Quantum programming and synthesis: Internalizing Clifford operations and beyond

by

Sam Winnick

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Combinatorics and Optimization

Waterloo, Ontario, Canada, 2025

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner: Ross Duncan
Lecturer, Computer Science
Strathclyde University

Supervisor(s): Jon Yard
Associate Professor, Combinatorics and Optimization,
University of Waterloo
Michele Mosca
Professor, Combinatorics and Optimization,
University of Waterloo

Internal Member: Karen Yeats
Professor, Combinatorics and Optimization,
University of Waterloo

Internal-External Member: William Slofstra
Associate Professor, Pure Mathematics, University of Waterloo

Other Member: Ben Webster
Associate Professor, Pure Mathematics, University of Waterloo

Author's Declaration

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Statement of Contributions

With the exception of Sec. 2.4, Ch. 2 comprises of joint work with Jennifer Paykin, which can be found in [WP24]. In Ch. 3, we present joint work with Jennifer Paykin from [PW24]. Lastly in Ch. 4, we present joint work with Amolak Ratan Kalra, Manimugdha Saikia, Dinesh Valluri, and Jon Yard [Kal+24]. I am the sole author of the rest of the work.

Abstract

Clifford operations are a subset of quantum operations used extensively in quantum error correction and classical simulation of quantum circuits.

The first part of the thesis is motivated by the problem of programming with generalized Clifford operations, such as the quantum Fourier transform. We delve into the algebraic complications that arise for systems of even dimension d, and we are particularly interested in the case when d is a power of 2. We apply our results in the design of a quantum functional programming language, in which the user does not have to worry about these irrelevant complications.

Later, we consider the problem of compiling circuits over universal gate sets. In particular, we study the problem of multi-qutrit exact synthesis over a variety of gate sets including Clifford gates.

Lastly, we present a framework for defining a symplectic form on an object in a sufficiently structured category, and lay out the theory, generalizing the theory of symplectic forms on a finite dimensional vector space or locally compact abelian group. In the process, we develop new results and perspectives on operations defined on categories.

Acknowledgements

First and foremost, I cannot overstate my gratitude to my supervisor Jon Yard for his guidance, and for sharing his profound insights and wealth of knowledge. I am extremely grateful for his availability and endless patience.

I am also very grateful for Michele Mosca's support and guidance.

Next, I would like to thank my examining committee for generously offering their time and expertise as readers on my thesis and providing me with detailed feedback.

I would also like to thank my collaborators, especially Jennifer Paykin, who patiently got me up to speed with type theory, Dinesh Valluri, who walked me through many number-theoretic calculations, and Amolak Ratan, who has taught me a lot about circuit synthesis. Thanks to Jon, Jennifer, and Amolak, as well as Nathan Haydon, Vikraman Choudhury, and Ben Plotke for their help reading the draft, and for many insightful discussions.

I have learned from many others along the way. In particular, Connor Paddock has also taught me a lot over the years.

I am deeply thankful of Alfred Menezes for his kindness. I would also like to express my gratitude to the all teachers and mentors who I have had along the way.

Over the last three years, I have benefited immensely from the energetic enthusiasm of the students I have tutored, including Matteo Mortensen, Bodhi Kovalenko, and Sebi Pintea.

Finally, I would like to thank my family. I could not have done it without their support.

Dedication

This is dedicated to my family.

Table of Contents

Chapter 1

Introduction

The *canonical commutation relations* of quantum mechanics are mathematically encoded by an object called the *symplectic form*. This is a structure defined on a vector space, module, or locally compact abelian group, called the *phase space*. Since there are several such variants, it is reasonable to ask what they have in common. In order to pose the question of what *kind* of objects may be used to form a mathematical phase space object, we turn to category theory. Thus, we seek to *internalize* the notion of *symplectic form* in a sufficiently structured category.

The same approach has been taken to study the role of the quantum Hilbert space by way of dagger compact categories [AC07][CD11]. One natural question is then to classify such categories up to equivalence. Analogous such classification problems are seen throughout mathematics, and tend to be nontrivial [Con86]. For example, the classification of finite simple groups is famously nontrivial. Another question is whether a given model is complete for the equational theory. In the case of dagger compact categories, several examples are known, and Selinger proved that the category of finite dimensional Hilbert spaces is complete [Sel12]. One may ask the same questions about preabelian star-autonomous categories admitting limits and colimits; these are the categories in which we give a definition of *symplectic form*.

The Curry-Howard-Lambek correspondence provides further motivation for the category-theoretic approach [Joh02]. If $\mathscr{C}$ is a category of phase space objects, the types of its internal language are phase space objects. In the case of finitely generated $\mathbb{Z}/d\mathbb{Z}$-modules, maps that respect the symplectic form are closely related to projective Clifford operations, and after making some changes, we arrive at a category $\mathscr{P}_{\mathrm{C}}$ whose internal language $\lambda^{\mathscr{P}_{\mathrm{C}}}$ specifies a functional programming language with native support for projective Clifford operations. In the design of the programming language, we only need to consider *free* finitely generated modules, whereas in the abstract framework for studying symplectic forms that we develop in Ch. 6, all finitely generated modules are considered in order to reason about kernels and cokernels. Nevertheless, quantum systems of composite dimension d are taken into account both in the programming language and in the mathematical framework. A projective Clifford operation on a system with phase space V is encoded as a pair (μ, ψ) consisting of a linear functional $\psi \in V^*$ and a symplectomorphism $\psi \in \mathsf{Sp}(V)$. Roughly speaking, objects in the category $\mathscr{P}_{\mathrm{C}}$ are more like Pauli groups, as opposed to the phase space objects of $\mathscr{C}$. This corresponds to a multilayer type system, where $\lambda^{\mathscr{P}_{\mathrm{C}}}$ types are built from types of an underlying linear-algebraic type system $\lambda^{\mathscr{C}}$ much like in [DD24].

The programming language application, combined with the importance of qubits, draws our attention to n qu*d*it projective Clifford operations where $d = 2^t$. In the $n = 1$ case, the t-qubit quantum Fourier transform is such an example [HDM05]. The encoding scheme for projective Clifford operations becomes much more complicated when d is even, since there is no longer an isomorphism between the n qu*d*it projective Clifford group $\mathbf{PCl}_{d,n}$ and the affine symplectic group $((\mathbb{Z}/d\mathbb{Z})^{2n})^* \rtimes \mathsf{Sp}((\mathbb{Z}/d\mathbb{Z})^{2n})$ [Mas23]. Nevertheless, there still exists a canonical bijection between the underlying sets, and the analysis of the even case turns out to be very interesting. Concerning $\lambda^{\mathscr{P}_{\mathrm{C}}}$, the subtleties of the even case are hidden from the user. The complicated formulas for composition, inversion, and evaluation of projective Clifford operations in the even case are all pushed into the semantics. The results on $\lambda^{\mathscr{P}_{\mathrm{C}}}$ and the projective Clifford group are in collaboration with Jennifer Paykin [PW24] [WP24].

The problem of compilation is closely related to that of circuit synthesis. In a separate collaboration with Amolak Ratan, Manimugdha Saikia, Dinesh Valluri, and Jon Yard, we derive a synthesis algorithm for multiqutrit Clifford operations over the ring $\mathbb{Z}[\frac{1}{3}, e^{2\pi i/9}]$ [Kal+24].[1] The result echoes the case of multiqubit synthesis conjectured in [KMM13] and proved in [GS13]. The problem is first reduced to synthesis over $\mathbb{Z}[\frac{1}{3}, e^{2\pi i/3}]$ by catalytic embedding (c.f. [Amy+23]), at which point we show that exact synthesis can be achieved with the Clifford+R gateset by iteratively reducing a parameter called *the smallest denominator exponent* to zero. In the end, three-level Clifford+R unitaries are converted into single qutrit gates using Gray codes, and synthesized using results of [YW22]. In the end, exact synthesis is achieved with Clifford+T gates using two ancillas and a reusable magic

[1] Similar results were independently established by Andrew N. Glaudell, Neil J. Ross, John van de Wetering, and Lia Yeh in [Gla+24].

state (catalyst).

In Ch. 6, we formulate the theory of symplectic forms in an arbitrary sufficiently structured category, in analogy to the theory of *abelian categories*, which generalizes the theory of homological algebra beyond concrete categories of modules [Buc55; Mac78; Gro57]. The theory of symplectic forms requires an internal notion of duality as well as notions of kernel, cokernel, and so on. In more technical terms, the category must be star-autonomous and pre-abelian. Parts of the theory work out when the category is only linearly distributive (weaker than *star-autonomous*), but other parts only hold in the category's nucleus.

In order to lay out the framework of Ch. 6, we first introduce the relevant concepts (*star-autonomy*, *linear distributivity*, *nucleus*, etc.) in Sec. 5.2. We view the relationship between nuclearity and reflexivity in a linearly distributive category as an instance of the microcosm principle [BD97], relating the internal duality to an external notion of duality, namely, the negation adjunction of Sec. 5.2.5. More philosophically, we argue that linear distributivity is to duality what associativity is to composition, and we give evidence for this claim by laying out the theory of star-autonomous categories without making any use of associativity in Sec. 5.3. Along the same lines, instead of working with monoidal categories, we consider a non-associative variant in Sec. 5.2, *magmal categories.* Categorification to one level higher has been achieved in Kelly's work on *doctrinal adunction* [Kel74], and we note how the theory of magmal categories, just like that of monoidal categories, is an instance of this meta-theory.

Chapter 2

Heisenberg groups and projective Clifford groups

The *Heisenberg group* provides a mathematical foundation for studying the famous canonical commutation relations of quantum mechanics. Several variants of the Heisenberg group exist, each with its own applications. Most famously, the *real Heisenberg group* refers to a particular Lie group relevant to quantum systems with continuous degrees of freedom. In more general usage, the Pauli group $\mathbf{P}_{d,n}$ for a system of n qu$d$its also qualifies as a Heisenberg group. Of related interest is the projective Clifford group $\mathbf{PCl}_{d,n}$, consisting of the center-fixing automorphisms of $\mathbf{P}_{d,n}$. Explicit definitions for these groups will be given below. In odd dimensions d, $\mathbf{PCl}_{d,n}$ is isomorphic to the affine symplectic group $V^* \rtimes \mathsf{Sp}(V,\omega)$, but this is false when d is even. Still, there is a bijection between the underlying sets:

$$\textsf{condensed encoding} : \mathbf{PCl}_{d,n} \xrightarrow{\sim} V^* \times \mathsf{Sp}(V,\omega) \qquad \text{(in S}\small{\text{ET}}\text{)} \tag{2.1}$$

The existence of such a bijection follows by applying Lagrange's Theorem to the structure theorem (Thm. 2.2.14) for $\mathbf{PCl}_{d,n}$, but working out an explicit bijection is less straightforward. We first consider encoding projective Clifford operations in terms of their action on Weyl operators $D_{q,p} = X^q Z^p$, but this is problematic when d is even. To solve this, we instead use Weyl operators of a slightly different form, $\Delta_{q,p} = \tau^{q \cdot p} X^q Z^p$. This trick for taming the even case is well known and has been used for example in [App+17] and [GNW21], though we take it in a different direction. We show that projective Cliffords admit a neat *condensed encoding* in terms of these Δ operators. This involves first considering *extended encodings* where the parameter d is replaced by $2d$. The price we pay for the condensed encodings is that the formulas for evaluating, composing, and inverting projective Cliffords involve complicated phase correction functions.

We find, however, that this encoding scheme is applicable in the design of a quantum functional programming language, as shown in Ch. 3. In fact, this is our motivation for working out the details. In this application, the operations of evaluation, composition, and inversion are only ever computed meta-theoretically or by a (future) compiler, and are thus out of the sight and mind of the programmer. We also feel that the results about condensed and extended encodings are interesting in their own right, and in particular, we find interesting connections between projective Clifford operations on a system of size $d = 2^t$ and $2d = 2^{t+1}$, that is, where one qubit is added.

Rather than focusing on a given Heisenberg group itself, we tend to instead focus on the associated phase space. For some variants of the Heisenberg group, the phase space is a locally compact abelian group equipped with a symplectic form, which encodes the same structure as the Heisenberg group itself [Mum06]. The Stone-von Neumann-Mackey Theorem classifies the faithful finite dimensional projective unitary representations of such a space, and these lift to ordinary unitary representations of the Heisenberg group. These representations are relevant in physics, since they pertain to the Hilbert space of an associated quantum system. There are several variants of the construction, for example involving finite dimensional real vector spaces in place of locally compact abelian groups, and unifying these motivates our study of the *category* of such objects. In Ch. 6, we give criteria for this category, and in order to make the locally compact abelian group example work, one has to iron out some topological pathologies. For this, we cite a construction of Barr and Kleisli, [BK01][Bar09].

Acknowledgments and author contributions in Ch. 2 The contents of Sec. 2.1.1, Sec. 2.2, and Sec. 2.3 (except Sec. 2.3.3 and the last example in Sec. 2.3.4) are joint work with Jennifer Paykin [WP24]. Many thanks to Jon Yard and Albert Schmitz for numerous fruitful discussions about this work.

2.1 The Pauli group and the projective Clifford group

2.1.1 Notation

Fix an integer $d > 1$ and let τ be a primitive d'th root of unity, where

$$d' = \begin{cases} 2d & : d \text{ is even} \\ d & : d \text{ is odd} \end{cases}$$

Then $\zeta = \tau^2$ has order d, and the other square root of ζ is $-\tau$, which has order d'. We are especially interested in the even case, which typically receives less attention, despite the relevance of quantum systems of dimension $d = 2^t$. It is well-known that the even case is harder to analyze. In this chapter, we write $R = \mathbb{Z}/d\mathbb{Z}$ for the finite cyclic ring of order d, and denote its elements by $0, \cdots, d-1$. Likewise, we write $R' = \mathbb{Z}/d'\mathbb{Z}$ for the finite cyclic ring of order d'. We find it convenient to introduce a group $\frac{1}{2}R'$, which is isomorphic to the underlying additive group of R', but whose elements are taken to be "halves" of the elements of R'. Explicitly, $\frac{1}{2}R'$ has the following abelian group presentations:

$$\frac{1}{2}R' = \left(\frac{1}{2} \;\middle|\; \underbrace{\frac{1}{2} + \cdots + \frac{1}{2}}_{d'} = 0 \right) = \left(1, \frac{1}{2} \;\middle|\; \underbrace{1 + \cdots + 1}_{d} = 0 \text{ and } \frac{1}{2} + \frac{1}{2} = 1 \right)$$

In other words, $\frac{1}{2}R'$ is obtained from R by formally adjoining $\frac{1}{2}$ if it doesn't already exist (i.e. in the even case), much like how $\mathbb{Q}(\tau) = \mathbb{Q}(\zeta, \tau)$ is obtained from $\mathbb{Q}(\zeta)$ by adjoining a square root of ζ. The point of introducing $\frac{1}{2}R'$ is that the canonical mutually inverse group isomorphisms $2 : \frac{1}{2}R' \xrightarrow{\sim} R'$ and $\frac{1}{2} : R' \xrightarrow{\sim} \frac{1}{2}R'$ amount to a formal device that allows us to carry out certain calculations thats would ordinarily involve multipliation or division by 2. The notation also allows us to treat the even and odd cases simultaneously, and by doing so, it underscores where the oddities of the even case enter the picture. If $t \in \frac{1}{2}R'$, then we interpret the expression ζ^t as meaning τ^{2t}, where 2 is the aforementioned isomoprhism.

Now, given a positive integer n, we set:

$$V = R^{2n} \qquad\qquad V' = (R')^{2n}$$

We call V the *phase space* and V' the *extended phase space*. Each is equipped with a *standard symplectic form*:

$$\begin{aligned} \omega : V \otimes V &\to R & \omega' : V' \otimes V' &\to R' \\ \omega((q_1, p_1), (q_2, p_2)) &= p_1 \cdot q_2 - p_2 \cdot q_1 & \omega'((q_1, p_1), (q_2, p_2)) &= p_1 \cdot q_2 - p_2 \cdot q_1 \end{aligned} \tag{2.2}$$

Here $\otimes$ denotes the tensor product of R-modules or R'-modules, respectively, and the $\cdot$ notation stands for the standard dot product of the appropriate type. The theory involves an interplay between R and R', or V and V'. This is mediated by an "adjunction" between the setwise inclusion $V \subseteq V'$ and the quotient map $V' \to V$. We pay strict attention to these *typecasting operations*, which are indicated by an underline or overline, respectively:[1]

$$\begin{array}{cc} \underline{\cdot} : V \to V' & \overline{\cdot} : V' \to V \\ (\text{in } \textsc{Set}) & (\text{in } \textsc{fgf-}R'\textsc{-Mod}) \end{array}$$

Occasionally, we write an expression involving both operations, $\overline{\underline{v}}$. It will always be possible to infer from the type whether this is intended as an element of V or V', though typically this notation will be used for an element of V', since $\underline{\cdot}$ is a section of $\overline{\cdot}$, i.e. $\overline{\cdot} \circ \underline{\cdot} = \mathsf{id}_V$. We also use the underline and overline notation for moving between R and R'. In contrast, when we identify R as a subgroup of $\frac{1}{2}R'$ (in the obvious way), we do **not** emphasize the inclusion with an underline or any other notation. Note that $R \leq \frac{1}{2}R'$ is a subgroup inclusion as opposed to just a subset inclusion, in contrast with $R \subseteq R'$ and $V \subseteq V'$.

In order to treat the even and odd cases simultaneously, let us introduce:

$$F_2 = \begin{cases} \mathbb{F}_2 & : d \text{ is even} \\ 0 & : d \text{ is odd} \end{cases}$$

In the even case, we frequently encounter elements $v_1, v_2 \in V'$ related by:

$$v_1 + v_2 = d\epsilon \tag{2.3}$$

for some $\epsilon \in F_2^{2n}$. Then the following quantity ends up playing a central role:

$$\langle \epsilon \rangle_{v_1, v_2} = \frac{1}{d} \omega'(v_1, v_2) \in F_2 \tag{2.4}$$

[1] We write $\textsc{Set}$ for the category of sets and $\textsc{fgf-}R'\textsc{-Mod}$ for the category of free finitely generated R'-modules. The inclusion function $\underline{\cdot}$ is not a homomorphism, hence only a morphism in $\textsc{Set}$.

Since any two of the quantities v_1, v_2, and ϵ determines the third via Eq. (2.3), we sometimes write $\langle\epsilon\rangle_{v_1}$ in place of $\langle\epsilon\rangle_{v_1,v_2}$. For example, since ω' is bilinear, $\langle\epsilon\rangle_0 = 0$ for any ϵ. Also, given v_1 and v_2, we sometimes implicitly *define* ϵ in terms of v_1 and v_2 by including it in an expression $\langle\epsilon\rangle_{v_1,v_2}$. Finally, if the context is clear, we might even write $\langle\epsilon\rangle$ as a shorthand for $\langle\epsilon\rangle_{v_1,v_2}$ in order to maintain precision but also to avoid overemphasizing v_1, v_2, and ϵ.

2.1.2 The Pauli group and the Clifford group

Let X and Z be the single-qu*d*it Pauli matrices. In the standard basis for $\mathbb{C}^d$, also called the *computational basis*, which we write with *ket* notation, their action is given by:

$$X\,|r\rangle = |r+1\rangle \qquad\qquad Z\,|r\rangle = \zeta^r\,|r\rangle \qquad\qquad r \in R$$

We also set $Y = \tau XZ$. The *n-qudit Pauli matrices* are defined in terms of the Kronecker product:

$$X^q = X^{q_1} \otimes \cdots \otimes X^{q_n} \qquad\qquad Z^p = Z^{p_1} \otimes \cdots \otimes Z^{p_n} \qquad\qquad q, p \in R^n$$

Two kinds of *Weyl operators* will be considered. For each $v = (q,p) \in V$ we set $D_v = X^q Z^p$, and on the other hand, for each $v = (q,p) \in V'$, we set $\Delta_v = \tau^{p \cdot q} D_{\overline{v}}$. In the latter case, the subscript v must be taken from V' in order for the phase $\tau^{p \cdot q}$ to be well-defined. These operations have the same conjugation action, and indeed define the same projective representation of the phase space:

$$[\Delta] : V \to \mathrm{PU}((\mathbb{C}^d)^{\otimes n})$$

Note that $[\Delta]$ is faithful only because we took the domain to be V, as opposed to the extended phase space V', and that this is legal, despite the previous remark. This is due to the fact that $\overline{v}_1 = \overline{v}_2$ if and only if Δ_{v_1} and Δ_{v_2} are proportional with constant ± 1:

$$\Delta_{v_2} = (-1)^{\langle \epsilon \rangle_{v_1, v_2}} \Delta_{v_1}$$

Faithfulness is needed in order for a projective unitary representation of V, such as $[\Delta]$, to lift to an ordinary unitary representation of the Heisenberg-Weyl group. As we will see, there are trade-offs between the D operators and the Δ operators, but overall, we find that the Δ operators lead to a more tractable analysis of the details that arise in the even case. Our preference of the Δ operators over the D operators leads us to prefer the larger version of the Pauli group, which has order $d'd^{2n}$ (as opposed to d^{2n+1}):

$$\mathbf{P}_{d,n} = \{\zeta^t D_v \,|\, t \in \tfrac{1}{2}R' \text{ and } v \in V\} = \langle \Delta_v \,|\, v \in V' \rangle = \langle X, Y, Z \rangle = \langle \tau, X, Z \rangle \tag{2.5}$$

We use the notations $\langle X, Y, Z\rangle$ and $\langle \tau, X, Z\rangle$ above as shorthands, where operators may act on all subsystems. In the even case, $\langle X, Z\rangle$ is an index 2 subgroup of the Pauli group (as we define it), and there are various other index 2 subgroups. In the single-qubit case,

$\langle X, Z\rangle$, $\langle X, Y\rangle$, and $\langle Y, Z\rangle$ are each isomorphic to the dihedral group of order 8, and $\langle iX, iZ\rangle = \langle iX, iY\rangle = \langle iY, iZ\rangle$ is isomorphic to the quaternion group. Each of these is a subgroup of the *Heisenberg-Weyl group*, which is obtained by enlarging the center to $\mathsf{U}(1)$:

$$\mathbf{HW}_{d,n} = \{cD_v \mid c \in \mathsf{U}(1) \text{ and } v \in V\}$$

The Stone-von Neumann-Mackey Theorem states that up to isomorphism, $\mathbf{HW}_{d,n}$ has a unique irreducible finite dimensional center-respecting unitary representation $\delta : \mathbf{HW}_{d,n} \to \mathsf{U}(\mathcal{H})$, where by *center-respecting* we mean that $\delta(cI) = c\,\mathsf{id}_{\mathcal{H}}$ for all $c \in \mathsf{U}(1)$. Note that the center of $\mathbf{HW}_{d,n}$ is $\mathsf{Z}(\mathbf{HW}_{d,n}) = \{cI \mid c \in \mathsf{U}(1)\}$. Equivalently, $[\Delta]$ is the unique irreducible finite dimensional faithful projective unitary representation of $V \cong \mathbf{HW}_{d,n}/\mathsf{Z}(\mathbf{HW}_{d,n})$ up to isomorphism. The projective Clifford group consists of the center-fixing automorphisms:

$$\mathbf{PCl}_{d,n} = \{\gamma \in \mathsf{Aut}\,\mathbf{P}_{d,n} \mid \gamma(P) = P \text{ for all } P \in \mathsf{Z}(\mathbf{P}_{d,n})\} \tag{2.6}$$

By the Stone-von Neumann-Mackey Theorem (or by the Skolem-Noether Theorem), it follows that each $\gamma \in \mathbf{PCl}_{d,n}$ is given by conjugation by a unitary U. On the other hand, each projective unitary $[U]$ that preserves $\mathbf{P}_{d,n}$ under conjugation uniquely defines a center-fixing automorphism of $\mathbf{P}_{d,n}$, and we obtain a group isomorphism:

$$\begin{aligned} \{[U] \in \mathsf{PU}(d^n) \mid UPU^\dagger \in \mathbf{P}_{d,n} \text{ for all } P \in \mathbf{P}_{d,n}\} &\xrightarrow{\sim} \mathbf{PCl}_{d,n} \\ [U] &\mapsto (P \mapsto UPU^\dagger) \end{aligned} \tag{2.7}$$

We tend to view this isomorphism as an identification. In the theory to follow, characterization Eq. (2.6) ends up being more useful, but when working through specific examples, characterization Eq. (2.7) ends up being easier. For example, in the single-qubit case, the second characterization may be used to see that the *projective S gate* $[S]$ (where $S = \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right)$) is projective Clifford. Note that this would be false if we had used $\langle X, Z\rangle$ as our definition of the Pauli group in place of the larger group $\mathbf{P}_{d,n} = \langle X, Y, Z\rangle$, as it appears in Eq. (2.7). Interestingly, replacing $\mathbf{P}_{d,n}$ by $\mathbf{HW}_{d,n}$ in Eq. (2.7) does not change the contents of $\mathbf{PCl}_{d,n}$.

2.1.3 Comparison of the D and Δ operators

If we use the D operators, each element of $\mathbf{P}_{d,n}$ may be expressed as $\zeta^t D_v$ for a unique pair $(t,v) \in \frac{1}{2}R' \times V$, and when expressed in terms of such pairs, the group law reads:

$$(t_1, v_1)(t_2, v_2) = (t_1 + t_2 + c(v_1, v_2), v_1 + v_2) \qquad t_i \in \tfrac{1}{2}R' \text{ and } v_i \in V$$

where $c : V \otimes V \to R$ is defined in terms of the dot product: $c((q_1,p_1),(q_2,p_2)) = p_1 \cdot q_2$. The group commutator involves the symplectic form on V:

$$(t_1, v_1)(t_2, v_2)(t_1, v_1)^{-1}(t_2, v_2)^{-1} = (\omega(v_1, v_2), 0) \qquad v_i \in V$$

This at first seems more convenient than the situation with the Δ operators. With the Δ operators, each element of $\mathbf{P}_{d,n}$ may be expressed as a pair $(t,v) \in \frac{1}{2}R' \times V'$, but these expressions are non-unique. Nevertheless, we can still express the group law in terms of the non-unique expressions, and this time, it involves the extended symplectic form:

$$(t_1, v_1)(t_2, v_2) = (t_1 + t_2 + \tfrac{1}{2}\omega'(v_1, v_2), v_1 + v_2) \qquad t_i \in \tfrac{1}{2}R' \text{ and } v_i \in V'$$

Here, $\frac{1}{2}$ denotes the group isomorphism $R' \xrightarrow{\sim} \frac{1}{2}R'$ from Sec. 2.1.1. The group commutator is given by:

$$(t_1, v_1)(t_2, v_2)(t_1, v_1)^{-1}(t_2, v_2)^{-1} = (\overline{\omega'(v_1, v_2)}, 0) = (\omega(\overline{v}_1, \overline{v}_2), 0) \qquad v_i \in V'$$

Note that the commutator expressions for the D and Δ notations both implicitly use the inclusion $R \leq \frac{1}{2}R'$. The Δ operators are quite strange. Despite being parameterized by a larger set (V') than the D operators, the Δ operators still only comprise a proper subset of $\mathbf{P}_{d,n}$ when d is even. In the single-qubit case, for example, we have:

$$\begin{array}{lll}
\Delta_{00} = \Delta_{20} = \Delta_{02} = \Delta_{22} = I & \Delta_{10} = \Delta_{30} = X & \Delta_{12} = \Delta_{32} = -X \\
 & \Delta_{01} = \Delta_{03} = Z & \Delta_{21} = \Delta_{23} = -Z \\
 & \Delta_{11} = \Delta_{33} = Y & \Delta_{13} = \Delta_{31} = -Y
\end{array}$$

Nevertheless, the Pauli group is *generated* by the Δ operators, as in Eq. (2.5). One advantage the Δ operators have over the D operators is the property that $\Delta_v^{\bar{t}} = \Delta_{tv}$ for all $t \in R'$ and $\Delta_v^d = I$, so each has order at most d. In the multi-qubit case, this means that Δ_v is always Hermitian. On the other hand, D_v has order d' for some v.

Each projective Clifford $\gamma \in \mathbf{PCl}_{d,n}$ has a unique D-*encoding*, that is, a pair (r, ψ) consisting of functions $r : V \to \frac{1}{2}R'$ and $\psi : V \to V$ satisfying $\gamma(D_v) = \zeta^{rv} D_{\psi v}$ for all $v \in V$. One finds that ψ is a symplectomorphism by extracting the exponent of the following:

$$\zeta^{\omega(v_1,v_2)} = \gamma(D_{v_1} D_{v_2} D_{v_1}^{-1} D_{v_2}^{-1}) = \gamma(D_{v_1})\gamma(D_{v_2})\gamma(D_{v_1})^{-1}\gamma(D_{v_2})^{-1} = \zeta^{\omega(\psi v_1, \psi v_2)}$$

On the other hand, the structure of r is less clear. Not every function $r : V \to \frac{1}{2}R'$ arises in some D-encoding, and in some cases, r might not even be a homomorphism. For example, if $\gamma = [S]$, then $r(0,0) = r(0,1) = 0$ and $r(1,0) = r(1,1) = \frac{1}{2}$, so $r(1,0) + r(1,0) \neq r((1,0) + (1,0))$. Nevertheless, r is still determined[2] by its action on the standard basis for V, once ψ is provided, due to the identity:

$$rv_1 + rv_2 - r(v_1 + v_2) = c(v_1, v_2) - c(\psi v_1, \psi v_2) \in \tfrac{1}{2}R' \tag{2.8}$$

The issue of r not being a homomorphism ends up making projective Clifford operations harder to analyze in terms of the D operators, so from this point on, we will shift our focus to the Δ operators. We would like to understand the sense in which a projective Clifford $\gamma \in \mathbf{PCl}_{d,n}$ can be encoded by a pair (λ, ϕ) of functions $\lambda : V' \to \frac{1}{2}R'$ and $\phi : V' \to V'$, in the sense that $\gamma(\Delta_v) = \zeta^{\lambda v} \Delta_{\phi v}$. Towards answering this, suppose that $\gamma(\Delta_{v_1}\Delta_{v_2}) = \gamma(\Delta_{v_1})\gamma(\Delta_{v_2})$. Then:

$$\begin{aligned}
\gamma(\Delta_{v_1}\Delta_{v_2}) &= \zeta^{\lambda(v_1+v_2)+\frac{1}{2}\omega'(v_1,v_2)} \Delta_{\phi(v_1+v_2)} \\
\gamma(\Delta_{v_1})\gamma(\Delta_{v_2}) &= \zeta^{\lambda v_1+\lambda v_2+\frac{1}{2}\omega'(\phi v_1,\phi v_2)} \Delta_{\phi v_1+\phi v_2}
\end{aligned}$$

It does not follow that $\phi(v_1 + v_2) = \phi v_1 + \phi v_2$ since there exist distinct $v_1, v_2 \in V'$ such that $\Delta_{v_2} = \pm\Delta_{v_1}$. However, the function taking each $v \in V$ to $\{\pm\Delta_{\underline{v}+d\epsilon}\}$ is a well-defined injective function that does not depend on the constant $\epsilon \in F_2^{2n}$. It follows that the function $\overline{\phi} : V' \to V$ obtained by reducing the output mod d is R'-linear, which then allows us to reduce the *input* mod d as well. We use the following double-overline notation for the R-linear map obtained from ϕ by reducing both the input and output mod d:

$$\psi = \overline{\overline{\phi}} : V \to V$$

[2]In fact, rv can be calculated efficiently in this way because V has the following *grammar*: each $v \in V$ is either 0 or has the form $w + e$ for some standard basis vector e and some $w \in V$ with $\mathsf{size}(w) < \mathsf{size}(v)$ for some function $\mathsf{size} : V \to \mathbb{N}_0$. Namely, we may take size to be the monoid homomorphism given by $\mathsf{size}(e) = 1$ for each standard basis vector e. Efficient calculation is all that is needed in some applications.

Finally, analysis of the phase exponent yields a formula in analogy to Eq. (2.8):

$$\lambda v_1 + \lambda v_2 - \lambda(v_1 + v_2) = \tfrac{d}{2}\langle\epsilon\rangle_{\phi(v_1+v_2),\phi v_1+\phi v_2} + \tfrac{1}{2}\omega'(v_1, v_2) - \tfrac{1}{2}\omega'(\phi v_1, \phi v_2) \in \tfrac{1}{2}R' \tag{2.9}$$

Note that the "$\frac{1}{2}$"s appearing here are applications of the isomorphism $\frac{1}{2} : R' \xrightarrow{\sim} \frac{1}{2}R'$. Now, if ϕ is R'-linear, then $\langle\epsilon\rangle = 0$, and in such a case, λ is a homomorphism if and only if $\phi \in \mathsf{Sp}(V', \omega')$. In deducing this, we have made use of the fact that γ is a homomorphism. If we now "multiply" Eq. (2.9) by $2 : \frac{1}{2}R' \xrightarrow{\sim} R'$ and then reduce mod d, we obtain:

$$\overline{2\lambda v_1 + 2\lambda v_2 - 2\lambda(v_1 + v_2)} = \omega(\overline{v}_1, \overline{v}_2) - \omega(\psi\overline{v}_1, \psi\overline{v}_2) \in R \qquad \text{for all } v_1, v_2 \in V' \tag{2.10}$$

The left-hand-side of Eq. (2.10) is symmetric and the right-hand-side is alternating, hence skew-symmetric, but assuming d is even, this is not enough to conclude that ψ is alternating, and then (by nondegeneracy) that $\psi \in \mathsf{Sp}(V, \omega)$. However, we may observe that ψ is the same map involved in the D-encoding of γ. From this, it follows that $\psi \in \mathsf{Sp}(V, \omega)$. From this we see that λ is "almost" a homomorphism, in the sense that for each $v_1, v_2 \in V'$, there exists $\alpha \in F_2$ such that $\lambda v_1 + \lambda v_2 - \lambda(v_1 + v_2) = d\alpha$.

2.2 Extended Δ-encodings

Describing the action of a projective Clifford operation in terms of the Δ operators turns out to be a lot harder than describing it in terms of the D operators, but ultimately more fruitful, since it leads us to the theory of *condensed Δ-encodings*. We proceed in steps. First we define *extended Δ-encodings*. In contrast with D-encodings, which are unique, a projective Clifford operation has multiple extended Δ-encodings. Further, a pair (λ, ϕ) of functions $\lambda : V' \to \frac{1}{2}R'$ and $\phi : V' \to V'$ is not necessarily an extended Δ-encoding of any projective Clifford operation, though as we will see, it will always encode a right-definite[3] center-respecting binary relation on $\mathbf{P}_{d,n}$. By considering these less-structured pairs (λ, ϕ), which we call *extended pre-Δ-encodings*, we will arrive at the following characterization:

Theorem 2.2.1 *A right-definite center-respecting binary relation on $\mathbf{P}_{d,n}$ is a projective Clifford operation if and only if it admits an R-valued symplectic extended pre-Δ-encoding.*

Explicit definitions for the terminology will be given in Sec. 2.2.1, but as an introduction, we shall now briefly explain the content of Thm. 2.2.1, and in doing so, give an informal survey of various kinds of encodings that arise. By *R-valued symplectic extended pre-Δ-encoding*, we refer to a pair (λ, ϕ) consisting of a homomorphism $\lambda : V' \to R$ and a symplectomorphism $\phi : V' \to V'$ of the extended phase space (V', ω'), relating to the binary relation in question in a way that we will soon define. The "R-valued" part indicates that the phase function λ in this definition is valued in the subgroup $R \leq \frac{1}{2}R'$. By Thm. 2.2.1, it will follow that such (λ, ϕ) is a symplectic extended Δ-encoding (without the "pre"), again with these terms being defined explicitly in Sec. 2.2.1. Then Thm. 2.2.1 will arise as the combination of Thm. 2.2.8 and Thm. 2.2.11. In Sec. 2.3, we will use Thm. 2.2.1 to show that projective Clifford operations are in canonical bijection with pairs (μ, ψ) where $\mu : V \to R$ is a homomorphism and $\psi : V \to V$ is a symplectomorphism, which we call *condensed Δ-encodings*.

We have alluded to multiple variants of encodings, and the terminology has already become burdensome. To address this, we may leave off the descriptors "extended" and "Δ-" in this section, since as the title suggests, this section is only about (variants of) extended Δ-encodings. Thus, we will use the term *Δ-encoding* or simply *encoding* as an abbreviation for *extended Δ-encoding*. Likewise, we will abbreviate *extended pre-Δ-encoding* by *pre-Δ-encoding* or even just *pre-encoding*. In later sections, we will use the term *extended*

[3]Relevant terminology about relations and some basic facts are given in Appx. A.

encoding to refer to a symplectic extended Δ-encoding. This is because (i) pre-encodings are only considered as an intermediate step in this section in order to state and prove Thm. 2.2.1 and (ii) symplectic encodings are the best-structured (extended) encodings, and we will never need to consider the less-structured ones outside of this section. We will also use the term *condensed encoding* in place of *condensed* Δ*-encoding* in later sections, and thus make a three-way distinction between D*-encodings*, *condensed encodings*, and *extended encodings*, where the latter two implicitly refer to Δ-encodings.

2.2.1 Existence and refinement

We now give explicit definitions for the various kinds of encodings as we need them.

An endofunction $\gamma : \mathbf{P}_{d,n} \to \mathbf{P}_{d,n}$ is *center-respecting* if $\gamma(\zeta^t \Delta_v) = \zeta^t \gamma(\Delta_v)$ for all $t \in \frac{1}{2}R'$ and $v \in V'$. A center-respecting endofunction is equivalently specified by its restriction to the subset $\{\Delta_v \mid v \in V'\}$ of the domain $\mathbf{P}_{d,n}$. On the other hand, since there exist $v_1, v_2 \in V'$ with $\Delta_{v_2} = -\Delta_{v_1}$, not every function $\gamma_0 : \{\Delta_v \mid v \in V'\} \to \mathbf{P}_{d,n}$ extends to a center-fixing endofunction. Due to the non-uniqueness of the expressions Δ_v, it is not immediately clear that each projective Clifford, let alone each center-respecting endofunction, is encoded (non-uniquely) by a pair (λ, ϕ) of functions $\lambda : V' \to \frac{1}{2}R'$ and $\phi : V' \to V'$, in the sense that $\gamma(\Delta_v) = \zeta^{\lambda v} \Delta_{\phi v}$ for all $v \in V'$. The following lemma asserts the existence of such encodings. All that is clear from the offset is that the hypothesis of the lemma is satisfied.

Lemma 2.2.2 *Let $\gamma : \mathbf{P}_{d,n} \to \mathbf{P}_{d,n}$ be a center-respecting endofunction and let $\phi : V' \to V'$ be a function such that for any $v \in V'$ there exists $t \in \frac{1}{2}R'$ such that $\gamma(\Delta_v) = \zeta^t \Delta_{\phi v}$. Then there exists a unique function $\lambda : V' \to \frac{1}{2}R'$ such that (λ, ϕ) is a Δ-encoding of γ.*

By considering the restricted function $\gamma_0 : \{\Delta_v \mid v \in V'\} \to \mathbf{P}_{d,n}$, it is clear that every center-respecting endofunction γ has such a ϕ. Hence by Lem. 2.2.2, there exists a pair (λ, ϕ) that encodes γ. Intuitively, the lemma asserts that the "t"s in $\gamma(\Delta_v) = \zeta^t \Delta_{\phi v}$ can be conglomerated into a function λ–a nontrivial fact, since distinct v may yield equal $\Delta_{\phi v}$.

Proof The relation $v \mapsto \Delta_v$ restricted to the subset $V \subseteq V'$ is an injective function, which allows us to define a function $\lambda_0 : V \to \frac{1}{2}R'$ by $\gamma(\Delta_v) = \zeta^{\lambda_0 v} \Delta_{\phi v}$ for all $v \in V \subseteq V'$. We want to extend λ_0 to a function $\lambda : V' \to \frac{1}{2}R'$ satsifying this property but for all $v \in V'$, not just V. Now, for each $v \in V'$ and $\epsilon \in F_2^{2n}$, there exist $s, t \in \frac{1}{2}R'$ such that:

$$\zeta^s \Delta_{\phi(v+d\epsilon)} = \gamma(\Delta_{v+d\epsilon}) = \gamma((-1)^{\langle \epsilon \rangle_v} \Delta_v) = (-1)^{\langle \epsilon \rangle_v} \gamma(\Delta_v) = \zeta^t \Delta_{\phi v}$$

There also exists unique $\delta \in F_2^{2n}$ with $d\delta = \phi v - \phi(v + d\epsilon)$. Now for $v \in V \subseteq V'$, set:

$$\lambda(v + d\epsilon) = \lambda_0 v + \frac{d}{2}(\langle \epsilon \rangle_v + \langle \delta \rangle_{\phi v}) \tag{2.11}$$

This defines λ on all of V', extending λ_0. Now for each $v + d\epsilon \in V'$, we have:

$$\zeta^{\lambda(v+d\epsilon)} \Delta_{\phi(v+d\epsilon)} = (-1)^{\langle \epsilon \rangle_v} \zeta^{\lambda v} \Delta_{\phi v}$$

as intended. Uniqueness is obvious: if $\zeta^{\lambda_1 v} \Delta_{\phi v} = \zeta^{\lambda_2 v} \Delta_{\phi v}$ for all $v \in V'$ then $\lambda_1 = \lambda_2$. ■

Given a center-respecting endofunction $\gamma : \mathbf{P}_{d,n} \to \mathbf{P}_{d,n}$, we have considered the domain-restricted function γ_0. Another point of view is that the restricted action $\Delta_v \mapsto \gamma(\Delta_v)$ just as well defines a binary relation on $\mathbf{P}_{d,n}$, which is right-definite but not left-total. Lemma Lem. 2.2.2 asserts that there exists a pair (λ, ϕ) such that this relation is given by $\Delta_v \mapsto \zeta^{\lambda v}\Delta_{\phi v}$. More generally, we call any pair (λ, ϕ) of functions $\lambda : V' \to \frac{1}{2}R'$ and $\phi : V' \to V'$ a *pre-Δ-encoding*. Each pre-Δ-encoding (λ, ϕ) defines a relation $\Delta_v \mapsto \zeta^{\lambda v}\Delta_{\phi v}$, which is not necessarily right-definite.[4] This relation extends to a center-respecting left-total relation γ on $\mathbf{P}_{d,n}$, which may or may not be right definite (i.e. an endofunction). Then a Δ-encoding is just a pre-Δ-encoding whose relation extends to a projective Clifford operation.

Lemma 2.2.3 *For any functions $\lambda_0 : V \to \frac{1}{2}R'$ and $\phi : V' \to V'$, there exists a unique function $\lambda : V' \to \frac{1}{2}R'$ extending λ_0 (with respect to the set inclusion $V \subseteq V'$) such that the relation $\Delta_v \mapsto \zeta^{\lambda v}\Delta_{\phi v}$ is right-definite, or equivalently, is the pre-Δ-encoding of some center-respecting endofunction γ.*

The proofs of Lem. 2.2.2 and Lem. 2.2.3 use the same calculation.

Proof Let λ be a function extending λ_0. Right-definiteness of $\Delta_v \mapsto \zeta^{\lambda v}\Delta_{\phi v}$ means:

$$\Delta_{v_1} = \Delta_{v_2} \implies \zeta^{\lambda v_1}\Delta_{\phi v_1} = \zeta^{\lambda v_2}\Delta_{\phi v_2} \qquad \text{for all } v_1, v_2 \in V'$$

This is achieved if and only if Eq. (2.11) is satisfied for all $v \in V \subseteq V'$ and $\epsilon \in F_2^{2n}$. ■

Two pre-Δ-encodings (λ_1, ϕ_1) and (λ_2, ϕ_2) are *equivalent*, written $(\lambda_1, \phi_1) \sim (\lambda_2, \phi_2)$, if they yield the same relation on $\mathbf{P}_{d,n}$. A pre-Δ-encoding (λ, ϕ) is *linear* if ϕ is R'-linear and *symplectic* if $\phi \in \mathsf{Sp}(V', \omega')$. By Eq. (2.9), a Δ-encoding (but not a pre-Δ-encoding) is symplectic if and only if λ is linear.

Lemma 2.2.4 *If (λ_0, ϕ_0) is a pre-Δ-encoding and $\overline{\phi}_0 : V' \to V$ is R'-linear, then there exists a canonical linear pre-Δ-encoding (λ, ϕ) such that $(\lambda_0, \phi_0) \sim (\lambda, \phi)$.*

As we saw in Sec. 2.1.2, if (λ_0, ϕ_0) is a Δ-encoding, then $\overline{\phi}_0$ is always R'-linear.

[4] We abuse the notation $\mapsto$ to indicate membership in the relation. It may be that $\Delta_{v_1} = \Delta_{v_2}$ but $\zeta^{\lambda v_1}\Delta_{\phi v_1} \neq \zeta^{\lambda v_2}\Delta_{\phi v_2}$. In this case, (λ, ϕ) defines a non-right-definite relation on $\mathbf{P}_{d,n}$. For definitions concerning relations, see Appx. A.

Proof We call this process *linearization*. Let $\phi : V' \to V'$ be the unique R'-linear map satisfying $\phi e = \phi_0 e$ for each standard basis vector e of V'. Since $\overline{\phi}_0$ is linear, $\overline{\phi v} = \overline{\phi_0 v}$ for all $v \in V'$, allowing us to define $\lambda v = \lambda_0 v + \frac{d}{2}\langle\delta\rangle_{\phi v, \phi_0 v}$. Then by construction, $(\lambda, \phi) \sim (\lambda_0, \phi_0)$, and ϕ is linear. ■

Proposition 2.2.5 *Each* $\psi \in \mathsf{Sp}(V, \omega)$ *lifts to some* $\phi \in \mathsf{Sp}(V', \omega')$.

By a *symplectic lift* we mean that $\phi \in \mathsf{Sp}(V', \omega')$ and $\psi = \overline{\overline{\phi}}$.

Proof See Theorem 1 on page 85 of [NS64].

Computing the matrix entries of a symplectic lift ϕ of a given $\psi \in \mathsf{Sp}(V, \omega)$ is not so straightforward, but by use of condensed encodings and some auxiliary formulas, we will never actually need to do so. Symplectic lifts can be used to evaluate $\gamma(\Delta_v)$ or $\gamma^{-1}(\Delta_v)$, but these other formulas will let us perform such evaluations without a symplectic lift. Thus, the existence of symplectic lifts is only used in proofs. Still, we note that symplectic lifts can be computed by solving a system of $4n^2$ equations and variables over F_2. To see why, start by lifting ψ to an R'-linear map ϕ_0, and let Φ_0 and Ω' be the R'-matrices for ϕ_0 and ω_0 in the standard basis. Then:

$$\Phi_0^T \Omega' \Phi_0 = \Omega' + dA$$

for some F_2-matrix A. Then solve for an F_2-matrix $E = \left(\begin{smallmatrix} E_1 & E_2 \\ E_3 & E_4 \end{smallmatrix}\right)$ such that:

$$A = \begin{pmatrix} D_1^T E_3 + D_3^T E_1 + E_3^T D_1 + E_1^T D_3 & D_1^T E_4 + D_3^T E_2 + E_3^T D_2 + E_1^T D_4 \\ D_2^T E_3 + D_4^T E_1 + E_4^T D_1 + E_2^T D_3 & D_2^T E_3 + D_4^T E_2 + E_4^T D_2 + E_2^T D_4 \end{pmatrix} \in F_2^{2n \times 2n} \tag{2.12}$$

where $\overline{\overline{\Phi}}_0 = \left(\begin{smallmatrix} D_1 & D_2 \\ D_3 & D_4 \end{smallmatrix}\right) \in F_2^{2n \times 2n}$. Then Eq. (2.12) is a linear system in the entries of E. By design, $A = E^T \Omega' \Phi_0 + \Phi_0^T \Omega' E$, so setting $\Phi = \Phi_0 + dE$, the following equation shows that a solution to the linear system yields a symplectomorphism:

$$\Phi^T \Omega' \Phi = \Phi_0^T \Omega' \Phi_0 + d(E^T \Omega' \Phi_0 + \Phi_0^T \Omega' E) = \Phi_0^T \Omega' \Phi_0 + dA = \Omega'$$

Since the reduction mod d of Φ is the R-matrix Ψ for ψ, Prop. 2.2.5 guarantees a solution.

Lemma 2.2.6 *Let* (λ_0, ϕ_0) *be a linear pre-*Δ*-encoding such that* $\psi = \overline{\overline{\phi}}_0 \in \mathsf{Sp}(V, \omega)$*. Then* (λ_0, ϕ_0) *is equivalent to a symplectic pre-*Δ*-encoding* (λ, ϕ)*.*

As seen in Sec. 2.1.2, if (λ_0, ϕ_0) is a Δ-encoding, then it is always the case that $\psi \in \mathsf{Sp}(V, \omega)$.

Proof By Prop. 2.2.5, there exists a linear map $\epsilon : F_2^{2n} \to F_2^{2n}$ such that $\phi = \phi_0 + d\epsilon \in \mathsf{Sp}(V', \omega')$. Then set:

$$\lambda v = \lambda_0 v + \frac{d}{2} \langle \epsilon v \rangle_{\phi_0 v, \phi v}$$

Then $(\lambda_0, \phi_0) \sim (\lambda, \phi)$ and $\phi \in \mathsf{Sp}(V', \omega')$.

Lemma 2.2.7 *Let $\gamma \in \mathbf{PCl}_{d,n}$ and suppose $\lambda : V' \to \frac{1}{2}R'$ and $\phi : V' \to V'$ are functions satisfying $\gamma(\Delta_v) = \zeta^{\lambda v} \Delta_{\phi v}$ for all $v \in V'$. Then the image of λ is contained in $R \leq \frac{1}{2}R'$.*

In contrast, the phase function $r : V \to \frac{1}{2}R'$ of the D-encoding (r, ψ) of some $\gamma \in \mathbf{PCl}_{d,n}$ may take half-element values. We have observed this behavior already when $\gamma = [S]$. This lemma establishes the better behavior of Δ-encodings in this way, but note that it applies to projective Cliffords only, not more generally to center-respecting endofunctions.

Proof Let $v \in V'$. By the property $\Delta_v^t = \Delta_{tv}$ and since γ is a homomorphism, we have:

$$I = \gamma(I) = \gamma(\Delta_v^d) = (\gamma(\Delta_v))^d = \zeta^{d\lambda v} \Delta_{d\phi v} = \zeta^{d\lambda v + \frac{d}{2}\langle \overline{\phi v} \rangle_0} I = \zeta^{d\lambda v} I$$

which implies $d\lambda v = 0$, and thus $\lambda v \in R \leq \frac{1}{2}R'$. ∎

Theorem 2.2.8 *Each $\gamma \in \mathbf{PCl}_{d,n}$ has a symplectic Δ-encoding (λ, ϕ), and λ is R-valued.*

Proof This follows from Lem. 2.2.2, Lem. 2.2.4, Lem. 2.2.6, and Lem. 2.2.7 applied to the case of Δ-encodings.

2.2.2 Sufficiency of the symplectic encodings

Our next goal is to prove the converse: given (λ, ϕ) where $\lambda : V' \to R$ is a homomorphism and $\phi \in \mathsf{Sp}(V', \omega')$, Thm. 2.2.11 establishes that (λ, ϕ) encodes some $\gamma \in \mathbf{PCl}_{d,n}$. Notice that λ is R-valued by assumption. The statement would otherwise be false, due to Lem. 2.2.7. Still, we find it interesting to consider a counterexample: let $\lambda : V' \to \frac{1}{2}R'$ be the homomorphism given by $\lambda(0,1) = \frac{1}{2}$ and $\lambda(1,0) = 0$, and $\phi = \mathsf{id}_{V'}$ in the single-qubit case. Then (λ, ϕ) is not the Δ-encoding of any projective Clifford, for if it were, it would follow that:

$$+I = \gamma(\Delta_{01}^2) = (\gamma(\Delta_{01}))^2 = -I$$

One way to understand the problem is that the relation $\Delta_v \mapsto \zeta^{\lambda v}\Delta_{\phi v}$ is not right definite. If it were, it would automatically define a homomorphism, hence a projective Clifford:

Lemma 2.2.9 *Let $\gamma : \mathbf{P}_{d,n} \to \mathbf{P}_{d,n}$ be a center-respecting endofunction satisfying $\gamma(\Delta_v) = \zeta^{\lambda v}\Delta_{\phi v}$ for some homomorphism $\lambda : V' \to \frac{1}{2}R'$ and $\phi \in \mathsf{Sp}(V', \omega')$. Then $\gamma \in \mathbf{PCl}_{d,n}$.*

Proof Since γ is center-respecting, the following calculation shows γ is an endomorphism:

$$\gamma(\Delta_{v_1})\gamma(\Delta_{v_2}) = \zeta^{\lambda v_1 + \lambda v_2 + \frac{1}{2}\omega'(\phi v_1, \phi v_2)}\Delta_{\phi v_1 + \phi v_2} = \zeta^{\lambda(v_1+v_2) + \frac{1}{2}\omega'(v_1, v_2)}\Delta_{\phi(v_1+v_2)} = \gamma(\Delta_{v_1}\Delta_{v_2})$$

Since ϕ is surjective and elements of $\mathbf{P}_{d,n}$ have the form $\zeta^t\Delta_v$, it follows that $\gamma : \mathbf{P}_{d,n} \to \mathbf{P}_{d,n}$ is surjective. Finally, since $\mathbf{P}_{d,n}$ is finite, γ is a bijection, and hence projective Clifford. ■

Lemma 2.2.10 *Let $\lambda : V' \to R$ be a homomorphism and $\phi \in \mathsf{Sp}(V', \omega')$. Then the relation γ given by $\Delta_v \mapsto \zeta^{\lambda v}\Delta_{\phi v}$ is right-definite, so extends to a center-respecting endofunction.*

Proof Consider the converse relation of the center-respecting endofunction γ on $\mathbf{P}_{d,n}$:

$$\gamma^{-1} = \left\{ (\zeta^{t+\lambda v}\Delta_{\phi v}, \zeta^t\Delta_v) \;\middle|\; t \in \tfrac{1}{2}R' \text{ and } v \in V' \right\}$$

Then observe that γ^{-1} is a homomorphic relation (i.e. a relation internal to GRP): (i): $(I, I) \in \gamma^{-1}$; (ii): the inverse of $(\zeta^{t+\lambda v}\Delta_{\phi v}, \zeta^t\Delta_v)$ is $(\zeta^{-t-\lambda v}\Delta_{-\phi v}, \zeta^{-t}\Delta_{-v}) \in \gamma^{-1}$; and (iii) if $(\zeta^{t_1+\lambda v_1}\Delta_{\phi v_1}, \zeta^{t_1}\Delta_{v_1}) \in \gamma^{-1}$ and $(\zeta^{t_2+\lambda v_2}\Delta_{\phi v_2}, \zeta^{t_2}\Delta_{v_2}) \in \gamma^{-1}$, then their product is:

$$\begin{aligned}
(\zeta^{t_3+\lambda v_3}\Delta_{\phi v_3}, \zeta^{t_3}\Delta_{v_3}) &= (\zeta^{t_1+t_2+\frac{1}{2}\omega'(\phi v_1, \phi v_2)+\lambda v_1+\lambda v_2}\Delta_{\phi v_1+\phi v_2}, \zeta^{t_1+t_2+\frac{1}{2}\omega'(v_1,v_2)}\Delta_{v_1+v_2}) \\
&= (\zeta^{t_1+t_2+\frac{1}{2}\omega'(v_1,v_2)+\lambda(v_1+v_2)}\Delta_{\phi(v_1+v_2)}, \zeta^{t_1+t_2+\frac{1}{2}\omega'(v_1,v_2)}\Delta_{v_1+v_2}) \in \gamma^{-1}
\end{aligned}$$

These facts establish that γ^{-1} is a subgroup of $\mathbf{PCl}_{d,n} \times \mathbf{PCl}_{d,n}$, or in other words, is a homomorphic relation on $\mathbf{PCl}_{d,n}$. Now, to see that γ is right-definite, we equivalently show that γ^{-1} is left-definite. By elementary properties of homomorphic relations, it suffices to show that $\mathsf{ker}\ \gamma^{-1}$ is trivial. Let $x \in \mathsf{ker}\ \gamma^{-1}$. This means $x = \zeta^{t+\lambda v}\Delta_{\phi v}$ for some $t \in \frac{1}{2}R'$ and $v \in V'$ such that $\zeta^t \Delta_v = I$. This implies that $v = d\epsilon$ for some $\epsilon \in F_2^{2n}$ and $t = \frac{d}{2}\langle\epsilon\rangle_0 = 0$. Then $x = \zeta^{\lambda d\epsilon}\Delta_{\phi d\epsilon} = \zeta^{d\lambda\epsilon}\Delta_{d\phi\epsilon}$ since λ and ϕ are homomorphisms. Since λ is valued in $R \leq \frac{1}{2}R'$, $\lambda d\epsilon = 0$, so $x = \Delta_{d\phi\epsilon} = \zeta^{\frac{d}{2}\langle\phi\epsilon\rangle_0} I = I$. So $\mathsf{ker}\ \gamma^{-1}$ is trivial. ■

Theorem 2.2.11 *Let $\lambda : V' \to R$ be a homomorphism and let $\phi \in \mathsf{Sp}(V', \omega')$. Then the relation $\Delta_v \mapsto \zeta^{\lambda v}\Delta_{\phi v}$ is right-definite and extends to a projective Clifford $\gamma \in \mathbf{PCl}_{d,n}$.*

Proof This follows from Lem. 2.2.9 and Lem. 2.2.10. ■

Now that we have the main theorem out of the way, we note a few corollaries. It would be nice to know whether the relation γ encoded by a pair (λ, ϕ) is projective Clifford. Better yet, we would like to know (1) whether γ is right-definite, and (2) assuming γ is right-definite, whether it is projective Clifford. By linearization, (1) is addressed as follows:

Corollary 2.2.12 *Let $\lambda : V' \to \frac{1}{2}R'$ be a function and let $\phi : V' \to V'$ be a homomorphism. Then the relation $\Delta_v \mapsto \zeta^{\lambda v}\Delta_{\phi v}$ is right definite if and only if*

$$\langle\epsilon\rangle_v = \langle\overline{\phi}\epsilon\rangle_{\phi v}$$

for all $v \in V'$ and $\epsilon \in F_2^{2n}$.

For question (2), we may start by assuming λ is R-valued, by Lem. 2.2.7. Then the answer is:

Corollary 2.2.13 *Let $\lambda : V' \to R$ and $\phi : V' \to V'$ be a pair of functions whose relation $\Delta_v \mapsto \zeta^{\lambda v}\Delta_{\phi v}$ is right-definite, or equivalently, whose relation extends to a center-repsecting endofunction γ on $\mathbf{P}_{d,n}$. Also let $\lambda_0 : V \to R$ be the restriction of λ to $V \subseteq V'$. Then γ is projective Clifford if and only if λ_0 is a homomorphism, $\overline{\phi} : V' \to V$ is R'-linear (so that $\psi = \overline{\overline{\phi}} : V \to V$ is well-defined), and ψ is a symplectomorphism, i.e. $\psi \in \mathsf{Sp}(V, \omega)$.*

Proof If either of λ_0 or $\overline{\phi}$ is not linear or ψ is not a symplectomorphism, then by preliminary observations in Sec. 2.1.2, $\gamma \notin \mathbf{PCl}_{d,n}$, so assume otherwise. Then by Lem. 2.2.4 and Lem. 2.2.6, without loss of generality, $\phi \in \mathsf{Sp}(V, \omega)$. Then since λ_0 is a homomorphism extending to λ, by the "uniqueness" part of Lem. 2.2.3, λ is a homomorphism. So by Thm. 2.2.11, $\gamma \in \mathbf{PCl}_{d,n}$. ■

2.2.3 A structure theorem for the projective Clifford group

We now present a structure theorem for the projective Clifford group, which provides a group isomoprhism $\mathsf{Sp}(V, \omega) \cong \mathbf{PCl}_{d,n}/V^*$ for all d. Although this isomorphism exists for all d, the exact sequence is not split in the even case, or in other words, $\mathbf{PCl}_{d,n} \ncong V^* \rtimes \mathsf{Sp}(V, \omega)$.

The case where d is odd was treated in [Gro06]. Results of the $d = 2$ case are contained in [GH12]. For general d and $n = 1$, a different approach was taken in [App05], which focuses on the special linear group rather than the symplectic group. The $d = 2$ case was also treated in [Mas23], and representation theory of the projective Clifford group was developed.

Theorem 2.2.14 *The function $\gamma \mapsto \psi = \overline{\overline{\phi}}_0$ for any Δ-encoding (λ_0, ϕ_0) of γ is a surjective group homomorphism $\pi : \mathbf{PCl}_{d,n} \to \mathsf{Sp}(V, \omega)$, independent of the encoding (λ_0, ϕ_0), with kernel $i : V^* \to \mathbf{PCl}_{d,n}$ identifying $\mu \in V^*$ with the projective Clifford encoded by $(\lambda, \mathsf{id}_{V'})$ for the unique homomorphism $\lambda : V' \to R \leq \frac{1}{2}R'$ satisfying $\lambda v = \mu\overline{v}$ for all $v \in V'$.*

$$1 \longrightarrow V^* \xrightarrow{i} \mathbf{PCl}_{d,n} \xrightarrow{\pi} \mathsf{Sp}(V, \omega) \longrightarrow 1 \tag{2.13}$$

Proof If (λ_1, ϕ_1) and (λ_2, ϕ_2) are Δ-encodings of $\gamma \in \mathbf{PCl}_{d,n}$, then for each $v \in V'$ there exists $\epsilon \in F_2^{2n}$ such that $\phi_1 v = \phi_2 v + d\epsilon$, so $\gamma \mapsto \psi$ is independent of the encoding. Now if γ and γ' have Δ-encodings (λ, ϕ) and (λ', ϕ') respectively, then their composition acts by:

$$\gamma\gamma'(\Delta_v) = \zeta^{\lambda' v + \lambda\phi' v}\Delta_{\phi\phi' v} \tag{2.14}$$

Reducing subscripts mod d, we see that $\gamma \mapsto \psi$ is multiplicative. It follows that $\gamma \mapsto \psi$ is a group homomorphism $\pi : \mathbf{PCl}_{d,n} \to \mathsf{Sp}(V, \omega)$. To see that π is surjective, by Prop. 2.2.5, lift an arbitrary $\psi \in \mathsf{Sp}(V, \omega)$ to some $\phi \in \mathsf{Sp}(V', \omega')$. By Thm. 2.2.11, the relation $\Delta_v \mapsto \Delta_{\phi v}$ is right-definite and extends to a projective Clifford, and since it has Δ-encoding $(0, \phi)$, it follows that $\pi\gamma = \psi$.

We now describe the kernel. Every $\gamma \in \ker \pi$ has a Δ-encoding of the form $(\lambda, \mathsf{id}_{V'})$, since by Lem. 2.2.2 it has a Δ-encoding (λ_0, ϕ_0), and then $(\lambda_0, \phi_0) \sim (\lambda, \mathsf{id}_{V'})$ where $\lambda = \lambda_0 + \frac{d}{2}\langle\epsilon\rangle_{\phi_0 v, v}$. Since $\mathsf{id}_{V'} \in \mathsf{Sp}(V', \omega')$, it follows that λ is a homomorphism. Since λ is a homomorphism and is valued in $R \leq \frac{1}{2}R'$ by Lem. 2.2.7, there exists unique $\mu \in V^*$

such that $\lambda v = \mu \overline{v}$ for all $v \in V'$. Conversely, if λ corresponds in this way to an arbitrary $\mu \in V^*$, then $(\lambda, \mathsf{id}_{V^*})$ is a Δ-encoding of some $\gamma \in \ker \pi$. This can be seen directly or by Thm. 2.2.11. ■

By Lagrange's Theorem, $|\mathbf{PCl}_{d,n}| = |V^*||\mathsf{Sp}(V, \omega)|$. Recall that one proves Lagrange's Theorem by constructing a bijection between the subgroup in question and an arbitrary coset. This doesn't immediately give us a bijection between the sets $\mathbf{PCl}_{d,n}$ and $V^* \times \mathsf{Sp}(V, \omega)$, but it does imply that one exists. The proof of Thm. 2.2.14 does hint towards a particular a bijection. One complication is that symplectic Δ-encodings are generally **not** unique, as seen in Sec. 2.3.4. Abstractly, finding such a bijection may be achieved by way of group cohomology, which we now recall.

Note that Eq. (2.13) is a short exact sequence of groups

$$1 \longrightarrow A \longrightarrow B \xrightarrow{\pi} G \longrightarrow 1$$

where A is abelian and equipped with a right G-action $\cdot : A \times G \to A$. (The right action is just pullback: $\mu \cdot \gamma = \mu\gamma$.) In such a case, each set-theoretic section $s : G \to B$ of π yields a bijection:

$$\begin{aligned} B = \bigsqcup_{g \in G} As(g) &\to A \times G \\ as(g) &\mapsto (a, g) \end{aligned}$$

With respect to this bijection, the group law is determined by a function $c : G \times G \to A$:

$$(a_1, g_1)(a_2, g_2) = (a_1 + a_2 + c(g_1, g_2), g_1 g_2)$$

By associativity, one finds that c is a group 2-cocycle. It is then routine to check that different sections s, s' yield cohomologous cocycles $c \sim c'$, and the 2-cohomology classes $[c]$ correspond to isomorphism classes of extensions $A \to B \to G$.

In the case of Eq. (2.13), the standard basis on $V = (\mathbb{Z}/d\mathbb{Z})^{2n}$ gives a canonical section, which we explore in Sec. 2.3, where we also present the formula for the cocycle c.

2.3 Condensed Δ-encodings

2.3.1 Construction and properties of condensed encodings

The following theorem gives the bijection claimed in Eq. (2.1).

Theorem 2.3.1 *There is a bijection* $\mathbf{PCl}_{d,n} \to V^* \times \mathsf{Sp}(V, \omega)$ *such that for any symplectic encoding* (λ, ϕ) *of* $\gamma \in \mathbf{PCl}_{d,n}$*, the corresponding pair* $(\mu, \psi) \in V^* \times \mathsf{Sp}(V, \omega)$ *uniquely satisfies:*

$$\psi = \overline{\overline{\phi}} \qquad \text{and} \qquad \lambda\underline{b} - \mu b = \frac{d}{2}\langle\epsilon\rangle_{\underline{\psi b}, \phi\underline{b}} \tag{2.15}$$

for all standard basis vectors $b \in V$*.*

Proof Given $\gamma \in \mathbf{PCl}_{d,n}$, we define (μ, ψ) as follows. By Thm. 2.2.8, let (λ, ϕ) be a symplectic encoding of γ. Then for each $v \in V'$, we have:

$$\gamma(\Delta_v) = \zeta^{\lambda v}\Delta_{\phi v} = \zeta^{\lambda v + \frac{d}{2}\langle\epsilon\rangle_{\underline{\psi\overline{v}}, \phi v}}\Delta_{\underline{\psi\overline{v}}}$$

where $\psi = \overline{\overline{\phi}} \in \mathsf{Sp}(V, \omega)$. Now define $\mu \in V^*$ by its action on standard basis vectors $b \in V$:

$$\mu b := \lambda\underline{b}$$

By construction, μ is R-linear ($\mu \in V^*$), and we obtain the following formula for evaluating $\gamma(\Delta_{\underline{b}})$ for basis vectors $b \in V$. Note that elements $\Delta_{\underline{b}}$ together with τ generate $\mathbf{P}_{d,n}$.

$$\gamma(\Delta_{\underline{b}}) := \zeta^{\mu b}\Delta_{\underline{\psi b}} \tag{2.16}$$

We now argue in two ways that the function $\gamma \mapsto (\mu, \psi)$ just described is a bijection. First, injectivity is straight-forward. Since the $\Delta_{\underline{b}}$ together with τ generate $\mathbf{P}_{d,n}$, we have:

$$(\mu_1, \psi_1) = (\mu_2, \psi_2) \implies \gamma_1(\Delta_{\underline{b}}) = \gamma_2(\Delta_{\underline{b}}) \text{ for standard basis vecs. } b \in V \implies \gamma_1 = \gamma_2$$

The result follows, since by Thm. 2.2.14, $|\mathbf{PCl}_{d,n}| \geq |V^*||\mathsf{Sp}(V, \omega)|$.

Alternately, we construct the inverse as follows. By Prop. 2.2.5, given (μ, ψ), we may lift ψ to $\phi \in \mathsf{Sp}(V', \omega')$, at which point for standard basis vectors $b \in V$ we have:

$$\zeta^{\mu b} \Delta_{\underline{\psi b}} = \zeta^{\mu b + \frac{d}{2}\langle \epsilon \rangle_{\underline{\psi b}, \phi \underline{b}}} \Delta_{\phi \underline{b}}$$

Then define $\lambda : V' \to R$ by R'-linearly extending its action on the standard basis vectors:

$$\lambda \underline{b} = \mu b + \frac{d}{2} \langle \epsilon \rangle_{\underline{\psi b}, \phi \underline{b}}$$

By Thm. 2.2.11, (λ, ϕ) is a symplectic encoding of some (unique) $\gamma \in \mathbf{PCl}_{d,n}$, and Eq. (2.16) is satisfied. Since Eq. (2.16) uniquely determines both γ and (μ, ψ), these constructions are mutually inverse.

Our goal is now to extend Eq. (2.16) to a formula for evaluating $\gamma(\Delta_v)$ for any $v \in V'$ rather than just for standard basis vectors $\underline{b} \in V'$. Recall that we factored the Xs and Zs *separately* in our definition $\Delta_v := \tau^{z \cdot x} X^x Z^z$. The evaluation formula is more readily obtained using the *interlaced* factorization:

$$\Delta_v = \prod_{i=1}^{n} \Delta_{(x_i e_i, z_i e_i)} = \tau^{z \cdot x} \prod_{i=1}^{n} X_i^{x_i} Z_i^{z_i} = \tau^{z \cdot x} X_1^{x_1} Z_1^{z_1} \cdots X_n^{x_n} Z_n^{z_n}$$

where $X_i := X^{e_i}$ and $Z_i := Z^{e_i}$.

Theorem 2.3.2 *Let $\gamma \leftrightarrow (\mu, \psi)$ correspond as in Thm. 2.3.1. Then for each $v \in V'$ we have:*

$$\gamma(\Delta_v) = \zeta^{\mu \overline{v} + \frac{d}{2}\kappa' v} \Delta_{\underline{\psi \overline{v}}} \tag{2.17}$$

where the function $\kappa' : V' \to F_2$ is defined by:

$$\frac{d}{2}\kappa' v = \frac{1}{2} z \cdot x + \frac{1}{2} \sum_{i=1}^{n} \omega'(x_i \underline{\psi(e_i, 0)}, z_i \underline{\psi[0, e_i]}) + \frac{d}{2} \sum_{i=1}^{n} \langle \epsilon \rangle_{x_i \underline{\psi(e_i,0)} + z_i \underline{\psi(0,e_i)}, \underline{\psi \overline{v}}}$$

Sometimes it is also helpful to introduce the function $\kappa : V \to F_2$ given by $\kappa v = \kappa' \underline{v}$.

Proof Using the interlaced factorization for Δ_v we obtain:

$$\begin{aligned}\gamma(\Delta_v) &= \tau^{z\cdot x}\prod \gamma(X_i)^{x_i}\gamma(Z_i)^{z_i}\\ &= \tau^{z\cdot x}\prod(\zeta^{x_i\mu(e_i,0)}\Delta_{x_i\underline{\psi(e_i,0)}})(\zeta^{z_i\mu(0,e_i)}\Delta_{z_i\underline{\psi(0,e_i)}})\\ &= \zeta^{\frac{1}{2}z\cdot x+\mu v+\frac{1}{2}\sum\omega'(x_i\underline{\psi(e_i,0)},z_i\underline{\psi(0,e_i)})}\prod\Delta_{x_i\underline{\psi(e_i,0)}+z_i\underline{\psi(0,e_i)}}\end{aligned}$$

On the other hand, for each $v \in V'$ there exists unique $k \in F_2$ such that $\gamma(\Delta_v) = \zeta^{\mu\overline{v}+\frac{d}{2}k}\Delta_{\underline{\psi\overline{v}}}$. Since the subscripts to the Δ operator agrees with Eq. (2.17), $\kappa' v = k$ is as in the theorem statement. ■

Corollary 2.3.3 *Let $\gamma \leftrightarrow (\mu,\psi)$ as in Thm. 2.3.1, let (λ,ϕ) be any symplectic encoding of γ, and let κ' be its phase correction function as in Thm. 2.3.2. Then for each $v \in V'$ we have:*

$$\lambda v - \mu\overline{v} = \frac{d}{2}\langle\epsilon\rangle_{\underline{\psi\overline{v}},\phi v} + \frac{d}{2}\kappa' v \tag{2.18}$$

Eq. (2.18) generalizes Eq. (2.15) by allowing for vectors beyond just standard basis vectors.

Proof Compare the phases of the left- and right-hand-sides of the following equation:

$$\zeta^{\lambda v+\frac{d}{2}\langle\epsilon\rangle_{\underline{\psi\overline{v}},\phi v}}\Delta_{\underline{\psi\overline{v}}} = \zeta^{\lambda v}\Delta_{\phi v} = \zeta^{\mu\overline{v}+\frac{d}{2}\kappa' v}\Delta_{\underline{\psi\overline{v}}}$$

■

Eq. (2.18) does not give a canonical symplectic encoding in terms of κ', since for example, both symplectic encodings of CNOT seen in Sec. 2.3.4 satisfy Eq. (2.18). Conversely, however, not only can a symplectic encoding (λ,ϕ) be used to directly compute $\gamma(\Delta_v) = \zeta^{\lambda v}\Delta_{\phi v}$, but Cor. 2.3.3 provides an alternate way to compute κ' in terms of (λ,ϕ). As noted before, a symplectic encoding can be obtained by solving a linear system. Still, we find it easier to use Thm. 2.3.2 for the purpose of evaluation.

Corollary 2.3.4 *Let (μ_1,ψ_1) and (μ_2,ψ_2) be condensed encodings of γ_1 and γ_2, respectively. Then the condensed encoding of the composition $\gamma_2\gamma_1$ is (μ_3,ψ_3), where $\psi_3 = \psi_2\psi_1$ and μ_3 is defined by R-linearly extending its action on standard basis vectors $b \in V$:*

$$\mu_3 b := \mu_1 b + \mu_2\psi_1 b + \frac{d}{2}\kappa_2\psi_1 b$$

We caution that $\mu_3 v$ must be computed using linearity by expanding v in the standard basis for V, rather than using the function $\tilde{\mu}$ below, which might not be linear. Also note that $\mu_3 - \mu_1 - \mu_2$ is the 2-cocycle c mentioned in Sec. 2.2.3.

Proof Here we use κ instead of κ'. The evaluation formula reads $\gamma(\Delta_{\underline{v}}) = \zeta^{\mu v + \frac{d}{2}\kappa v}\Delta_{\underline{\psi v}}$ for $v \in V$. Now extract the canonically determined functions $\tilde{\mu}_3$ and ψ_3 from $\zeta^{\tilde{\mu}_3 v}\Delta_{\underline{\psi_3 v}} := \gamma_2\gamma_1(\Delta_{\underline{v}})$:

$$\tilde{\mu}_3 v = \mu_1 v + \mu_2\psi_1 v + \frac{d}{2}\kappa_1 v + \frac{d}{2}\kappa_2\psi_1 v \tag{2.19}$$

In particular, Eq. (2.19) holds for standard basis vectors $b \in V$, and together with $\psi_3 = \psi_2\psi_1$, determines the condensed encoding as in Eq. (2.16). Also, $\kappa_1 b = 0$. ■

Corollary 2.3.5 *The operation* $((\mu_2, \psi_2), (\mu_1, \psi_1)) \mapsto (\mu_3, \psi_3)$ *makes the set* $V^* \times \mathsf{Sp}(V, \omega)$ *into a group isomorphic to* $\mathbf{PCl}_{d,n}$.

Proof This follows from Cor. 2.3.4 and the bijection of Thm. 2.3.1. ■

Corollary 2.3.6 *The identity element is* $(0, \mathsf{id}_V)$ *and the inverse of* (μ, ψ) *is* $(\mu_{\text{inv}}, \psi^{-1})$, *where:*

$$\mu_{\text{inv}} b = -\mu\psi^{-1}b + \frac{d}{2}\kappa\psi^{-1}b$$

for all standard basis vectors $b \in V$.

Proof This follows from Cor. 2.3.4. ■

2.3.2 The condensed product

Consider the center-respecting function $\star : \mathbf{P}_{d,n} \odot \mathbf{P}_{d,n} \to \mathbf{P}_{d,n}$ defined for $u, v \in V$ by

$$\Delta_{\underline{u}} \star \Delta_{\underline{v}} = \tau^{-\underline{\omega(u,v)}} \Delta_{\underline{u}} \Delta_{\underline{v}} = (-1)^{s(u,v)} \Delta_{\underline{u+v}} \tag{2.20}$$

where $s(u,v) = \frac{1}{d}(\omega'(\underline{u}, \underline{v}) - \underline{\omega(u,v)})$. This equation extends to all $u, v \in V'$ as follows:

$$\Delta_u \star \Delta_v = (-1)^{\langle \rho \rangle} \Delta_{\overline{u}} \star \Delta_{\overline{v}} = (-1)^{\langle \rho \rangle + s(\overline{u}, \overline{v})} \Delta_{\overline{u}+\overline{v}} = (-1)^{s(\overline{u}, \overline{v})} \Delta_{u+v}$$

Observe that for each $t_1, t_2 \in R$, the phase exponent of $\zeta^{t_1} \Delta_u \star \zeta^{t_2} \Delta_v$ is still in R:

$$\zeta^{t_1} \Delta_{\underline{u}} \star \zeta^{t_2} \Delta_{\underline{v}} = \zeta^{t_1 + t_2 + \frac{d}{2} s(u,v) + \frac{d}{2} \langle \rho \rangle_{\underline{u+v}, \underline{u+v}}} \Delta_{\underline{u+v}} \tag{2.21}$$

This implies that the following subsets of $\mathbf{P}_{d,n}$ are closed under $\star$:

$$\mathbf{Q}_{d,n} = \{\zeta^t \Delta_{\underline{v}} \,|\, t \in R \text{ and } v \in V\} \qquad \mathbf{\Sigma}_{d,n} = \{\pm \Delta_v \,|\, v \in V'\} = \{\pm \Delta_{\underline{v}} \,|\, v \in V\}$$

Notice that $\mathbf{Q}_{d,n}$ is in obvious bijection with the set $R \times V$. In applications, this encoding scheme for Paulis works well with the condensed encoding scheme for projective Cliffords.

Now let $R'_+ = \{0, \cdots, d-1\}$ and $R'_- = \{d, \cdots, d'-1\}$ so $R' = R'_+ \sqcup R'_-$. We write $\mathrm{sgn}(t) = 0$ if $t \in R'_+$ and $\mathrm{sgn}(t) = 1$ if $t \in R'_-$. For example, $s(u,v) = \mathrm{sgn}(\omega'(\underline{u}, \underline{v}))$. Then consider the function:

$$f : \mathbf{P}_{d,n} \to \mathbf{\Sigma}_{d,n} \qquad\qquad f(\tau^t \Delta_v) = (-1)^{\mathrm{sgn}(t)} \Delta_v$$

Then f is well-defined, $f(\tau^{t + \frac{d}{2}\langle \epsilon \rangle_v} \Delta_v) = (-1)^{\mathrm{sgn}(t) + \langle \epsilon \rangle_v} \Delta_v$. Though f does not respect the center (for a single qubit, $-I = f(-I) \neq f(iI) \star f(iI) = I \star I = I$), it satisfies:

$$f(\Delta_u) \star f(\Delta_v) = (-1)^{s(\overline{u}, \overline{v})} \Delta_{u+v} = f(\tau^{\omega'(u,v)} \Delta_{u+v}) = f(\Delta_u \Delta_v)$$

This prompts us to define the following equivalence relation $\sim$ on $\mathbf{P}_{d,n}$ and operation $\star$ on the quotient set $\mathbf{P}_{d,n}/\sim$, from which we obtain an isomorphism $\tilde{f} : \mathbf{P}_{d,n}/\sim \to \mathbf{\Sigma}_{d,n}$:

$$\tau^s \Delta_v \sim \tau^t \Delta_{v + d\epsilon} \text{ iff } \mathrm{sgn}(s) + \mathrm{sgn}(t) = \langle \epsilon \rangle_v \qquad [\tau^s \Delta_u] \star [\tau^t \Delta_v] = [\tau^r (-1)^{s(\overline{u}, \overline{v})} \Delta_{u+v}]$$

where r satisfies $\mathrm{sgn}(s) + \mathrm{sgn}(t) = \mathrm{sgn}(r)$. The intuition of the condensed product is therefore to only remember the "sign" of the phase exponent. When d is even, the $\star$ operations defined on $\mathbf{P}_{d,n}$ and $\mathbf{P}_{d,n}/\sim$ are non-associative:

$$X \star (Y \star Y) = X \star I = X \neq -X = -Z \star Y = (X \star Y) \star Y$$

There are many other such examples, and more for even $d > 2$:

$$(X \star Y) \star Z = -Z \star Z = -Z^2 \neq -X^2 = -X \star X = X \star (Y \star Z)$$

In the $d = 2$ case, $\mathbf{Q}_{d,n} = \mathbf{\Sigma}_{d,n} = \{\pm I, \pm X, \pm Y, \pm Z\}$ with multiplication table:

$\star$	I	X	Y	Z
I	I	X	Y	Z
X	X	I	Z	Y
Y	Y	$-Z$	I	X
Z	Z	$-Y$	$-X$	I

(respecting ± 1 phases)

The $\star$ operation extends to a well-defined $\mathbb{C}$-linear map $\mathbb{C}^{N\times N} \otimes \mathbb{C}^{N\times N} \to \mathbb{C}^{N\times N}$ (where $N = d^n$), which in the even case, is different from the matrix product.

Theorem 2.3.7 *Let $\gamma \in \mathrm{PCl}'_{d,n}$ and $u, v \in V'$. Then:*

$$\gamma(\Delta_u \star \Delta_v) = \gamma(\Delta_u) \star \gamma(\Delta_v)$$

Proof It suffices to just show the result holds for $\underline{v_1}$ and $\underline{v_2}$ with $v_1, v_2 \in V$. Let (μ, ψ) be the condensed encoding for γ and let κ be its correction function. Then,

$$\begin{aligned}
\gamma(\Delta_{\underline{u}} \star \Delta_{\underline{v}}) &= \zeta^{-\frac{1}{2}\underline{\omega(u,v)}}\gamma(\Delta_{\underline{u}})\gamma(\Delta_{\underline{v}}) \\
&= \zeta^{\mu u + \mu v + \frac{d}{2}(\kappa u + \kappa v) - \frac{1}{2}\underline{\omega(u,v)}}\Delta_{\underline{\psi u}}\Delta_{\underline{\psi v}} \\
&= \zeta^{\mu u + \mu v + \frac{d}{2}(\kappa u + \kappa v) - \frac{1}{2}\underline{\omega(u,v)} + \frac{1}{2}\underline{\omega(\psi u, \psi v)}}\Delta_{\underline{\psi u}} \star \Delta_{\underline{\psi v}} \\
&= \zeta^{\mu u + \mu v + \frac{d}{2}(\kappa u + \kappa v)}\Delta_{\underline{\psi u}} \star \Delta_{\underline{\psi v}} \\
&= \gamma(\Delta_{\underline{u}}) \star \gamma(\Delta_{\underline{v}})
\end{aligned}$$

■

Corollary 2.3.8 *For all $u, v \in V$ and $\psi \in \mathrm{Sp}(V, \omega)$, we have $s(u, v) = s(\psi u, \psi v)$.*

In other words, symplectomorphisms $\psi \in \mathrm{Sp}(V, \omega)$ preserve the sign of $s(u, v)$.

Proof Pick some $\mu \in V^*$ (eg. $\mu = 0$), and let (λ, ϕ) be a symplectic Δ-encoding of the $\gamma \in \mathrm{PCl}'_{d,n}$ whose condensed encoding is (μ, ψ). Then:

$$\gamma(\Delta_u \star \Delta_v) = (-1)^{s(\overline{u},\overline{v}) + s(\overline{\phi u}, \overline{\phi v})}\gamma(\Delta_u) \star \gamma(\Delta_v)$$

■

2.3.3 Dimension doubling

We now examine a relationship between condensed encodings and extended (symplectic) encodings in the case of a single qu$d$it with $d = 2^n$. The projective Clifford operations are the nodes of a tree (Fig. 2.1), as we will show, where n indicates the distance from the root node. The nodes are addressed by a sequence of *bias operators*. For simplicity, we do not consider composite systems here, though the results readily generalize. We first set:

$$\begin{array}{lll} d = 2^n > 1 & d' = 2d & d'' = 4d \\ \zeta_d = e^{2\pi i/d} & \zeta_{d'} = e^{2\pi i/d'} & \zeta_{d''} = e^{2\pi i/d''} \\ V = (\mathbb{Z}/d\mathbb{Z})^2 & V = (\mathbb{Z}/d'\mathbb{Z})^2 & V = (\mathbb{Z}/d''\mathbb{Z})^2 \end{array}$$

We denote set inclusions $V \subseteq V' \subseteq V''$ by an underline and module quotients with an overline. For example, if $v \in V$ then we write $\underline{v} \in V'$ and $\underline{\underline{v}} \in V''$. Next we set:

$$\begin{array}{ll} \Delta_{(x,z)} = \zeta_{d'}^{zx} X_d^{\overline{x}} Z_d^{\overline{z}} & (x, z) \in V' \\ \Delta'_{(x,z)} = \zeta_{d''}^{zx} X_{d'}^{\overline{x}} Z_{d'}^{\overline{z}} & (x, z) \in V'' \end{array}$$

Subscripts on X and Z indicate the dimension of the relevant Hilbert space. The qu$d$it system is related to the qud'it system by the following *squaring homomorphism*:

$$\begin{array}{lll} & \mathsf{sq} : \mathbf{P}_{d'} \to \mathbf{P}_d & \\ & c\Delta'_{\underline{v}} \mapsto c^2 \Delta_v & v \in V' \\ \text{or just as well} & c\Delta'_v \mapsto c^2 \Delta_{\overline{v}} & v \in V'' \end{array}$$

For example, in the $d = 2$ case, we have:

$$X_4 = \begin{pmatrix} & & & 1 \\ 1 & & & \\ & 1 & & \\ & & 1 & \end{pmatrix} \mapsto \begin{pmatrix} & 1 \\ 1 & \end{pmatrix} = X_2$$

sq restricts to a (non-homomorphic) bijection out of the *non-negative subset*:

$$\mathbf{P}_{d'}^{\geq 0} = \left\{ \zeta_{d''}^{t} \Delta'_{\underline{\underline{v}}} \,\middle|\, t \in \mathbb{Z}/d'\mathbb{Z} \text{ and } v \in V \right\}$$

We denote the inverse function of the restricted squaring function by:

$$\sqrt[\star]{-} : \mathbf{P}_d \xrightarrow{\sim} \mathbf{P}_{d'}^{\geq 0}$$

Now suppose $\gamma' \in \mathbf{PCl}_{d'}$, and let $(\mu, \psi) \in (V')^* \times \mathsf{Sp}\, V'$ be its condensed encoding. Then (μ, ψ) is an extended encoding of some unique $\gamma \in \mathbf{PCl}_d$, and evaluation is given by:

$$\begin{aligned} \gamma'(\Delta'_{\underline{v}}) &= (-1)^{\kappa v} \zeta_{d'}^{\mu v} \Delta'_{\underline{\psi v}} && v \in V' \\ \gamma(\Delta_v) &= \zeta_d^{\overline{\mu v}} \Delta_{\psi v} && v \in V' \end{aligned}$$

This describes the aforementioned tree structure. From this, we obtain the following *recursive evaluation formula*:

$$\gamma'(\Delta'_{\underline{v}}) = B_{\gamma', v} \sqrt[\star]{\gamma(\Delta_v)} \qquad v \in V'$$

where the *bias* is the Hermitian matrix

$$B_{\gamma', v} = (-1)^{\kappa v + \beta + \delta} i^{\underline{\langle \epsilon \rangle}} (X_2^\alpha \otimes I_d)(I_d \otimes Z_2^\beta) \tag{2.22}$$

and the bits α, β, δ, and $\langle \epsilon \rangle$ are defined by:

$$\begin{aligned} \psi v &= \underline{\overline{\psi v}} + d(\alpha, \beta) \in V' \\ \mu v &= \underline{\overline{\mu v}} + d\delta \in \mathbb{Z}/d'\mathbb{Z} \\ \langle \epsilon \rangle &= \langle \epsilon \rangle_{\psi v, \underline{\overline{\psi v}}} = \frac{1}{d} \omega'(\psi v, \underline{\overline{\psi v}}) \in \mathbb{Z}/2\mathbb{Z} \end{aligned}$$

In order to derive the bias formula Eq. (2.22), we have used the identities:

$$X_{d'}^d = X_2 \otimes I_d \qquad \text{and} \qquad Z_{d'}^d = I_d \otimes Z_2 \tag{2.23}$$

which embed $\mathbf{P}_2$ into $\mathbf{P}_{d'}$.

Theorem 2.3.9 *Let $\gamma' \in \mathbf{PCl}_{d'}$, let ρ_{in} be a density matrix on $\mathbb{C}^{d'}$, and let $\rho_{\mathsf{in}} = \gamma'(\rho_{\mathsf{out}})$. Then the probability of reading out $j = 0, 1$ upon performing a computational basis measurement on the last qubit is:*

$$p_j = \frac{1}{2}(1 + (-1)^j \langle B_{\gamma', (0,d)} \rangle_{\rho_{\mathsf{in}}}) \tag{2.24}$$

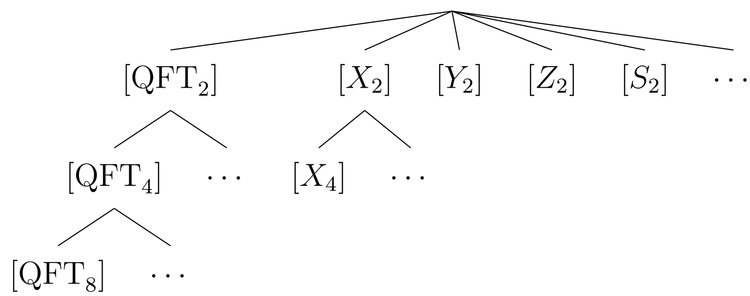


Figure 2.1: Here we visualize the rooted tree structure of single qu$d$it projective Clifford operations when d is a power of 2. The condensed encoding of a node is an extended encoding of its parent, and every such operation is reached. Level $d = 2^1$ has 24 nodes, and $\mathbf{PCl}_{2,1}$ is isomorphic to the octahedral group.

Equation Eq. (2.24) explains why we call $B_{\gamma',v}$ the *bias operator*. Note that it is illegal to permute the qubits so that a different one becomes the "last" qubit: if γ' is conjugation by some unitary U, and Σ represents a permutation of the qubit-by-qubit subsystems, then conjugation by $\Sigma U \Sigma^{-1}$ is no longer necessarily in $\mathbf{PCl}_{d'}$. For an explicit counterexample, take Σ to be the 2-qubit swap gate and U to be the 2-qubit quantum Fourier transform.

Proof The POVM for measuring the last qubit is $\{\Pi_1, \Pi_2\}$ where $\Pi_i = I_d \otimes |i\rangle \langle i|$. Now, we may decompose ρ_{out} as follows:

$$\rho_{\mathsf{out}} = p_0 \rho_{\mathsf{out},0} \otimes |0\rangle \langle 0| + p_1 \rho_{\mathsf{out},1} \otimes |1\rangle \langle 1|$$

Measurement of ρ_{out} leaves the system in post-measurement state:

$$\frac{\Pi_i \rho_{\mathsf{out}} \Pi_i}{p_i} = \rho_{\mathsf{out},i} \otimes |i\rangle \langle i|$$

with probability:

$$p_i = \mathrm{Tr}(\rho_{\mathsf{out}} \Pi_i) = \mathrm{Tr}(\rho_{\mathsf{in}} \gamma'(\Pi_i)) = \langle \gamma'(\Pi_i) \rangle_{\rho_{\mathsf{in}}}$$

On the other hand, $\Pi_i = \frac{1}{2}(I_{d'} + (-1)^i Z_{d'}^d)$, so by the recursive evaluation formula:

$$\gamma'(\Pi_i) = \frac{1}{2}(I_{d'} + (-1)^i \gamma'(\Delta'_{0,d})) = \frac{1}{2}(I_{d'} + (-1)^i B_{\gamma',(0,d)})$$

We obtain Eq. (2.24) by taking the expectation of this equation value at ρ_{in}. ∎

This phenomenon about measuring the last qubit is due to the coincidental equality between elements of the operator bases corresponding to $\mathbb{Z}_2^{n+1}$ and $\mathbb{Z}_{2^{n+1}}$. The result cannot be applied repeatedly, since the post-measurement state, which is generally mixed, cannot be realized as the result of applying a projective Clifford to the remaining n qubits. We are currently exploring possible connections with semantic security.

2.3.4 Examples of condensed and extended Δ-encodings

Example Let $d = 2$ and let γ be conjugation by CNOT. By considering the Pauli tableau ($X \otimes I \mapsto X \otimes X$, $I \otimes X \mapsto I \otimes X$, $Z \otimes I \mapsto Z \otimes I$, $I \otimes Z \mapsto Z \otimes Z$), the obvious way to get a Δ-encoding is to start with the following R'-linear map (written as a matrix in the standard basis):

$$\phi_0 = \begin{pmatrix} 1 & & & \\ 1 & 1 & & \\ & & 1 & 1 \\ & & & 1 \end{pmatrix}$$

By Lem. 2.2.2, there exists unique λ_0 such that (λ_0, ϕ_0) is an encoding of γ, but it is not symplectic, since by considering the action on basis vectors, we would have $\lambda_0 = 0$, but $\lambda_0(e_1 + e_4) \neq \lambda_0 e_1 + \lambda_0 e_4$. The following matrix calculation shows directly that $\phi_0 \notin \mathrm{Sp}(V', \omega')$:

$$[\phi_0^*(\omega') - \omega'] = [\phi_0]^T[\omega'][\phi_0] - [\omega'] = dA = 2\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Two symplectic encodings for CNOT (which both use $\lambda = 0$) are given by:

$$\phi = \begin{pmatrix} 1 & & & \\ 3 & 1 & & \\ & & 1 & 1 \\ & & & 1 \end{pmatrix} \qquad \text{or} \qquad \phi = \begin{pmatrix} 1 & & & \\ 1 & 1 & & \\ & & 1 & 3 \\ & & & 1 \end{pmatrix} \tag{2.25}$$

The condensed encoding for CNOT is $(0, \psi)$ where $\psi = \overline{\overline{\phi}} = \overline{\overline{\phi}}_0$. Note that ψ is R-linear as opposed to R'-linear.

Example Either of $\phi_1 = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \in \mathrm{Sp}(V', \omega')$ or $\phi_2 = \left(\begin{smallmatrix} 1 & 0 \\ 3 & 1 \end{smallmatrix}\right) \in \mathrm{Sp}(V', \omega')$ can be used in symplectic Δ-encodings of (conjugation by) either S or S^{-1}, each with the appropriate λ. The condensed encodings both of S and S^{-1} use $\psi = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \in \mathrm{Sp}(V, \omega)$, and the respective phase functions are $\mu_S = 0$ and $\mu_{S^{-1}}\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = 1$ and $\mu_{S^{-1}}\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) = 0$. The associated "correction functions" κ_S and $\kappa_{S^{-1}}$ are nonlinear. For example, $\kappa_S\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) = 1$ (since $SYS^{-1} = -X$) and $\kappa_S v = 0$ for $v \neq \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$.

Example The quantum Fourier transform acts on a single qudit by $X \mapsto Z$ and $Z \mapsto X^{-1}$. A symplectic encoding is $\lambda = 0$ and $\phi = \left(\begin{smallmatrix} & -1 \\ 1 & \end{smallmatrix}\right) \in \mathrm{Sp}(V', \omega')$. For $d = 2$ this is the Hadamard gate. The condensed encoding is just $\mu = 0$ and $\psi = \left(\begin{smallmatrix} & -1 \\ 1 & \end{smallmatrix}\right) \in \mathrm{Sp}(V, \omega)$.

Example Lastly, we give an example of dimension doubling in the $d = 2$ case. The non-negative part of the Pauli group is:

$$\mathbf{P}_{d'}^{\geq 0} = \{cP \mid c \in \{1, \zeta_8, i, \zeta_8^3\} \text{ and } P \in \{I_4, X_4, Y_4, Z_4\}\}$$

where

$$\begin{aligned} I_4 &= \Delta'_{00} = \Delta'_{40} = \Delta'_{04} = \Delta'_{44} & \qquad Y_4 &= \Delta'_{11} = \Delta'_{55} \\ X_4 &= \Delta'_{10} = \Delta'_{50} & \qquad Z_4 &= \Delta'_{01} = \Delta'_{05} \end{aligned}$$

The relevant square root calculations are:

$$\sqrt[\star]{I_2} = I_4 \qquad \sqrt[\star]{X_2} = X_4 \qquad \sqrt[\star]{Y_2} = Y_4 \qquad \sqrt[\star]{Z_2} = Z_4$$

Now let $\gamma'(P) = UPU^\dagger$ and $\gamma(Q) = HQH^\dagger$ where:

$$U = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \qquad H = H^\dagger = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Then the recursive formula lets us recover the conjugation action of U from that of H:

$$\begin{aligned} \gamma'(X_4) &= \sqrt[\star]{\gamma(X_2)} = \sqrt[\star]{Z_2} = Z_4 \\ \gamma'(Z_4) &= B\sqrt[\star]{\gamma(Z_2)} = X_4^2 \sqrt[\star]{X_2} = X_4^3 = X_4^\dagger \end{aligned}$$

The bias operator is $B = X_2 \otimes I_2 = X_4^2$, and the bias of measuring the last qubit is zero: $\langle t| B |t\rangle = 0$, from which it follows that $|\langle t| U |t\rangle|^2 = \frac{1}{2}$, for all $t \in \mathbb{Z}/4\mathbb{Z}$. These calculations generalize, and one may recover the tableau for the Fourier transform by induction. If γ_n is the projective quantum Fourier transform of size $d = 2^n$, then for example, we have:

$$\gamma_n(Z_{2^n}) = X_{2^n}^{2^{n-1}} \sqrt[\star]{X_{2^{n-1}}^{2^{n-2}} \sqrt[\star]{X_{2^{n-2}}^{2^{n-3}} \sqrt[\star]{\cdots}}} = X_{2^n}^{2^{n-1}} X_{2^n}^{2^{n-2}} X_{2^n}^{2^{n-3}} \cdots = X_{2^n}^{2^n - 1} = X_{2^n}^\dagger$$

as expected.

2.4 The category of locally compact abelian groups

2.4.1 Motivation

The *real Heisenberg group with center* $\mathbb{R}$ is the following matrix Lie group:

$$\mathbf{H}(\mathbb{R}^{2n}, \mathbb{R}) = \left\{ M_{t,(q,p)} = \begin{pmatrix} 1 & p^T & t \\ 0 & \mathbb{1}_n & q \\ 0 & 0 & 1 \end{pmatrix} \;:\; t \in \mathbb{R} \text{ and } q, p \in \mathbb{R}^n \right\} \tag{2.26}$$

$\mathbf{H}(\mathbb{R}^{2n}, \mathbb{R})$ is a central extension of Lie groups, i.e. a solution G to the extension problem

$$1 \longrightarrow Z \longrightarrow G \longrightarrow V \longrightarrow 1 \tag{2.27}$$

where $V = \mathbb{R}^{2n}$ and $Z = \mathbb{R}$. In other words, Eq. (2.27) is an exact sequence such that Z maps into the center of G. Regarded as a vector space, V has standard symplectic form:

$$\begin{gathered} \omega : V \otimes V \to Z = \mathbb{R} \\ \omega((q_1, p_1), (q_2, p_2)) = p_1 \cdot q_2 - p_2 \cdot q_1 \end{gathered} \tag{2.28}$$

The value $\omega(v_1, v_2)$ appears in the top-right entry of the group commutator:

$$M_{t_1,v_1} M_{t_2,v_2} M_{t_1,v_1}^{-1} M_{t_2,v_2}^{-1} = M_{\omega(v_1,v_2),0}$$

In this sense, G "remembers" the symplectic form. Conversely, since $2 \in \mathbb{R}$ is invertible, the group law can be expressed in terms of ω, since the matrices $M_{t,(q,p)} \in G$ are in bijection with pairs $(t - \frac{1}{2} p \cdot q, (q, p)) \in \mathbb{R} \times V$. The group law in this format is given by:

$$(s_1, v_1)(s_2, v_2) = (s_1 + s_2 + \tfrac{1}{2}\omega(v_1, v_2), v_1 + v_2) \tag{2.29}$$

In this way we may move between the phase space (V, ω) and the Heisenberg group G. There is also a coordinate-free analog, where given a finite dimensional real symplectic vector space (V, ω), we define a Lie group $\mathbf{H}((V, \omega), \mathbb{R})$ with underlying manifold $\mathbb{R} \times V$ and group law given by Eq. (2.29). As before, $\mathbf{H}((V, \omega), \mathbb{R})$ is a central extension of V by $\mathbb{R}$, and ω is recovered from the group commutator. We may again denote the elements of $\mathbf{H}((V, \omega), \mathbb{R})$ by symbols $M_{t,v}$ instead of pairs (s, v), where if $v = (q, p)$ then $t = s + \frac{1}{2}\omega((q, 0), (0, p))$.

The *Heisenberg Lie algebra* is:

$$\mathfrak{h}(\mathbb{R}^{2n}) = \left\{ m_{s,(q,p)} = \begin{pmatrix} 0 & p^T & s \\ 0 & 0 & q \\ 0 & 0 & 0 \end{pmatrix} \;:\; s \in \mathbb{R} \text{ and } q, p \in \mathbb{R}^n \right\}$$

Since $\mathfrak{h}(\mathbb{R}^{2n})$ is nilpotent, its exponential map is a diffeomorphism onto the unique corresponding simply connected Lie group, namely $\mathbf{H}(\mathbb{R}^{2n}, \mathbb{R})$. One easily checks that the exponential map is given by $m_{s,v} \mapsto M_{t,v}$ where $v = (q,p)$ and $t = s + \frac{1}{2} p \cdot q$. The only nonzero entry of the Lie bracket

$$m_{s_1,v_1} m_{s_2,v_2} - m_{s_2,v_2} m_{s_1,v_1} = m_{\omega(v_1,v_2),0} \tag{2.30}$$

is the top-right entry, which has value $\omega(v_1, v_2)$. In this way we find that the Lie algebra also encodes the same structure as the phase space. We may define $\mathfrak{h}(V, \omega)$ as the real vector space $\mathbb{R} \times V$ equipped with Lie bracket given by Eq. (2.30). Again the exponential map is given by $(s, v) = m_{s,v} \mapsto M_{t,v}$, and its well-definedness follows from the invertibility of 2.

There is another interesting Lie group $\mathbf{H}(\mathbb{R}^{2n}, \mathsf{U}(1))$ with Lie algebra $\mathfrak{h}(\mathbb{R}^{2n})$. It is also a central extension of $V = \mathbb{R}^{2n}$, meaning it lies in a short exact sequence like Eq. (2.27), but this time the center is $Z = \mathsf{U}(1)$, which makes $\mathbf{H}(\mathbb{R}^{2n}, \mathsf{U}(1))$ *not* simply connected. As before, $\mathbf{H}(\mathbb{R}^{2n}, \mathsf{U}(1))$ is diffeomorphic to $Z \times V$, so we may define the group law along the lines of Eq. (2.29). In order for this definition to make sense, we find that it is only appropriate that the symplectic form be valued in $\mathsf{U}(1)$ instead of $\mathbb{R}$. Thus, we use the exponentiated symplectic form (defined in terms of some $h \in \mathbb{R}^\times$):

$$\begin{aligned} \Omega : V \otimes V &\to Z = \mathsf{U}(1) \\ \Omega(v_1, v_2) &= e^{2\pi i h \omega(v_1, v_2)} \end{aligned} \tag{2.31}$$

The exponentiated symplectic form is no longer $\mathbb{R}$-bilinear, so at first it seems wrong to write the domain as $V \otimes V$. However, Ω is a homomorphism in both arguments, so this could be seen as a tensor product of $\mathbb{Z}$-modules, i.e. abelian groups. This seems strange since occurences of $\mathbb{R}$ from the previous example are now either staying as $\mathbb{R}$ (as in $V = \mathbb{R}^{2n}$) or being replaced by $\mathbb{Z}$ or $\mathsf{U}(1)$. What is really going on is that Ω is a morphism of locally compact abelian groups, and $\mathbb{Z}$ and $\mathsf{U}(1)$ are the monoidal unit $\top$ and comonoidal unit $\perp$. Thus, we should regard $V = \mathbb{R}^{2n}$ as a locally compact abelian group rather than a real vector space. In contrast, the symplectic form ω on $\mathbf{H}(\mathbb{R}^{2n}, \mathbb{R})/\mathbb{R}$ was just a morphism of finite dimensional real vector spaces, and in that category, $\top \cong \bot \cong \mathbb{R}$.

In the locally compact abelian group setting, notice that $\mathbb{Z}^{2n}$ is a Lagrangian subgroup (when we set $h = \frac{1}{2\pi}$). Consequently, we obtain the following realization of the representation promised by the Stone-von Neumann-Mackey theorem. Namely,

$$\rho : G \to \mathsf{U}(L^2(\mathbb{R}^{2n}/\mathbb{Z}^{2n}))$$
$$(\rho(C, v)f)(x) = C\sqrt{\Omega(v, x)}f(x + v)$$

where $L^2(\mathbb{R}^{2n}/\mathbb{Z}^{2n})$ consists of certain quasiperiodic functions $f : \mathbb{R}^{2n} \to \mathbb{C}$ as seen in [Mum06]. This result follows from the theory of symplectic forms on locally compact abelian groups, and thus demonstrates the utility in internalizing the theory of symplectic forms to categories other than that of finite dimensional real vector spaces.

One may also consider matrices as in Eq. (2.26) but with $q, p \in R^n$ and $t \in \frac{1}{2}R'$ where $R = \mathbb{Z}/d\mathbb{Z}$ and $\frac{1}{2}R'$ is defind as in Sec. 2.1.1. Then the Pauli group $G = \mathbf{P}_{d,n}$ is a central extension of $V = R \oplus R$ with center $Z = \mathbb{Z}/d'\mathbb{Z}$. Each $h \in (\mathbb{Z}/d'\mathbb{Z})^\times$ defines an isomorphism $\mathbb{Z}/d'\mathbb{Z} \xrightarrow{\sim} \langle\tau\rangle$, given by $t \mapsto \tau^{ht}$, where τ is a d'th root of unity. Then even though G is finite, one may define an object $\mathfrak{p}_{d,n}$ with similar properties to the Lie algebra, where again the top-right entry has to be taken from $\frac{1}{2}R'$. As we have seen in Sec. 2.2, the symplectic form $\omega : V \otimes V \to R$ remembers the group commutator of $\mathbf{P}_{d,n}$ but not the group law in the even case, and changing the codomain of ω from R to $\frac{1}{2}R'$ does nothing here. Instead, one must consider an extended phase space and symplectic form $\omega' : V' \otimes V' \to R'$, so $\mathbf{P}_{d,n}$ should only be studied from the perpective of R-modules if d is odd. The subgroups $\mathbf{P}^{(0)}_{d,n} = \langle X, Z\rangle$ and $\mathbf{P}^{(1)}_{d,n} = \langle \tau X, \tau Z\rangle$ have issues of their own in the even case. For instance, since we keep $Z = R$ instead of R', the exponential map $\mathfrak{g} \to G$ is not well-defined. Nevertheless, $\mathbf{P}_{d,n}$, $\mathbf{P}^{(0)}_{d,n}$, and $\mathbf{P}^{(1)}_{d,n}$ will qualify as *Heisenberg groups* per the definition in Sec. 2.4.4.

In both the even and odd case, we may consider the central extension $G = \mathbf{WH}_{d,n}$ of $V = (\mathbb{Z}/d\mathbb{Z})^{2n}$ by $\mathsf{U}(1)$, where V is regarded as a locally compact abelian group. In some cases, such when applying the Stone-von Neumann-Mackey theorem, it is sufficient to extend the center all the way up to $\mathsf{U}(1)$ and work in $\widehat{\mathrm{LCA}}$. More along the lines of the real Heisenberg group, another variant that may be interesting to consider is a number field such as $\mathbb{Q}(e^{2\pi i/d})$ in place of $\mathbb{R}$.

One way to get a better behaved Lie algebra and translation between the Heisenberg group and phase space when d is a power of 2 (the most interesting and important case where d is even) may be to treat all powers of 2 uniformly using Prüfer 2-group:

$$\mathbb{Z}[\tfrac{1}{2}]/\mathbb{Z} = \{0, \tfrac{1}{2}, \tfrac{1}{4}, \tfrac{3}{4}, \tfrac{1}{8}, \tfrac{3}{8}, \tfrac{5}{8}, \tfrac{7}{8}, \cdots\}$$

This (locally compact) group has the structure relevant to the dimension doubling phenomenon studied in Sec. 2.3.3. Namely, each group $\mathbb{Z}/2^m\mathbb{Z}$ is included in $\mathbb{Z}[\frac{1}{2}]/\mathbb{Z}$ by sending 1 to $\frac{1}{2^m}$. The relevant phase space is $(\mathbb{Z}[\frac{1}{2}]/\mathbb{Z})^{2m}$ and the (Δ-style) Weyl operators may be realized as follows:

$$\Delta_{t;q,p} = \begin{pmatrix} 1 & p^T & t + \frac{1}{2}p\cdot q \\ 0 & \mathbb{1}_m & q \\ 0 & 0 & 1 \end{pmatrix} \qquad\qquad t \in \mathbb{Z}[\tfrac{1}{2}]/\mathbb{Z} \text{ and } (q,p) \in (\mathbb{Z}[\tfrac{1}{2}]/\mathbb{Z})^{2m}$$

These generate a group $\mathbf{P}_{2^\star,m}$ that includes $\mathbf{P}_{2^n,m}$ for each n. Likewise we may define $\mathbf{PCl}_{2^\star,m}$ as the group of center-fixing automorphisms of $\mathbf{P}_{2^\star,m}$. We leave serious consideration of the Prüfer 2-group for future work.

2.4.2 Characters on locally compact abelian groups

In this thesis, we will use *locally compact* to mean *locally compact Hausdorff*.

A *complex unitary representation* of a locally compact group G is a continuous group homomorphism of the form

$$\rho : G \to \mathsf{U}(\mathcal{H})$$

for some complex Hilbert space $\mathcal{H}$. For now we will only concern ourselves with representations where $\mathcal{H}$ is finite dimensional. Such representations and the intertwining operators between them form a category $\textsc{Rep}(G)$. The *degree* $\mathsf{deg}\,\rho = \mathsf{dim}\,\mathcal{H}$ of ρ depends on ρ only up to isomorphism. One calls ρ *irreducible* if $\mathcal{H}$ has no proper invariant subspace, i.e. no subspace $\mathcal{H}_0$ such that $\rho(g)f \in \mathcal{H}_0$ for all $g \in G$ and $f \in \mathcal{H}_0$. If $\mathsf{deg}\,\rho = 1$ then ρ is irreducible, and the converse holds if G is abelian. The *character* of ρ is the function:

$$\begin{aligned} \chi_\rho : G &\to \mathbb{C} \\ g &\mapsto \mathsf{Tr}\,\rho(g) \end{aligned}$$

The degree satisfies $\mathsf{deg}\,\rho = \chi_\rho(1)$, and so we may speak of the *degree* of a character χ. If $\mathsf{deg}\,\rho = 1$, then χ_ρ is a continuous homomorphism into the unit circle $\mathsf{U}(1)$ and may be identified with ρ. If H is a closed subgroup of G, then we obtain a *restriction functor*:

$$\begin{aligned} \textsc{Rep}(G) &\to \textsc{Rep}(H) \\ \rho &\mapsto \rho \downarrow^G_H \end{aligned}$$

given by $\rho \downarrow^G_H (h) = \rho(h)$ for all $h \in H$. The restriction of an intertwining map (a morphism of representations) is just as easy to define. If G is compact or locally compact abelian, then restriction has a left adjoint (which is also its right adjoint), called *induction*:

$$\begin{aligned} \textsc{Rep}(H) &\to \textsc{Rep}(G) \\ \rho &\mapsto \rho \uparrow^G_H \end{aligned}$$

The *induced character* $\chi \uparrow^G_H$, i.e. the character of $\rho \uparrow^G_H$, is given by:

$$\chi \uparrow^G_H (g) = \int_{\{t \in G \,|\, tgt^{-1} \in H\}} \chi(tgt^{-1}) d\mu(t) \tag{2.32}$$

where χ is the character of ρ and μ is the Haar measure normalized so that $\mu(H) = 1$. The reason for assuming that G is compact or locally compact abelian is that in either case, the left and right Haar measures coincide, which enables the standard averaging arguments found in the character theory of finite groups, thereby leading to Eq. (2.32). In the case that G is locally compact abelian and H has finite index in G, it follows that:

$$\chi \uparrow_H^G (g) = \begin{cases} [G : H]\chi(g) & : g \in H \\ 0 & : g \in G \setminus H \end{cases} \tag{2.33}$$

The irreducible characters of G form another locally compact abelian group G^* under pointwise multipliation, called the *Pontryagin dual*. In Sec. 2.4.5, we note that the category of locally compact abelian groups is very nearly a star-autonomous category, where Pontryagin duality is the *negation*. A fragment of the character theory exists internally to this category, or better yet, to a replacement star-autonomous category $\widetilde{\mathrm{LCA}}$, which to be introduced in Sec. 2.4.5. Namely, given an inclusion

$$x : H \to G$$

of a closed subgroup H in G, $\widetilde{\mathrm{LCA}}$ also includes the restriction morphism:

$$\begin{aligned} x^* : G^* &\to H^* \\ \chi &\mapsto \chi \downarrow_H^G = \chi x \end{aligned}$$

In contrast, induction does not take irreducible characters on H to irreducible characters on G unless $H = G$. This can be seen by Eq. (2.33) and noting that $0 \notin \mathsf{U}(1)$. Sometimes, however, there exists a morphism $x_! : H^* \to G^*$ satisfying $x^* x_! = \mathsf{id}_{H^*}$. In fact, such $x_!$ exists if and only if there exists $\pi : G \to H$ satisfying $\pi x = \mathsf{id}_H$, in which case we may take $x_! = \pi^*$. By the splitting lemma for abelain groups, this is equivalent to the condition that H has a complement, i.e. $G = H \oplus K$ for some K. Note that x^* and $x_!$ are morphisms, not to be confused with functors between the categories of representations.

We will see that the existence or non-existence of $x_!$ plays a role in the theory of symplectic forms, first in Sec. 2.4.3 and then more generally in Ch. 6.

Consider the locally compact abelian group $G = \mathbb{R}^m$ and the closed subgroup $H = \mathbb{Z}^m$. Then the inclusion $x : H \to G$ does not admit a left inverse (homomorphism), and so the restriction $x^* : G^* \to H^*$ does not admit a right inverse $x_!$. This Lagrangian subgroup has no complement, though as we will see, the Lagrangan quotient G/H still plays a crucial role in the abstract theory of symplectic forms.

2.4.3 Symplectic forms on a locally compact abelian group

Previously, we have considered the canonical $\mathbb{Z}/d\mathbb{Z}$-linear symplectic form on $(\mathbb{Z}/d\mathbb{Z})^{2n}$, the canonical $\mathbb{R}$-linear symplectic form on $\mathbb{R}^{2n}$, and its exponentiated version (Eqs. (2.2), (2.28) and (2.31)). So far we have seen how these arise in the study of the corresponding Heisenberg groups, and in the first case, of the projective Clifford group. We now seek to lay out the main properties of symplectic forms, and for this, we limit ourselves to the third case, that of locally compact abelian groups. An analogous story may be told in the case of modules, but the version for locally compact abelian groups highlights some more interesting aspects. Abstractly, symplectic forms are defined as follows.

Let V be a locally compact abelian group with group law written additively. A *symplectic form* on V is a $\mathsf{U}(1)$-valued continuous function Ω on the product of the underlying locally compact topological space with itself, $V \times V$, subject to:

$$\begin{array}{rclr} \Omega(u_1+u_2,v) &=& \Omega(u_1,v)\Omega(u_2,v) & \\ \Omega(u,v_1+v_2) &=& \Omega(u,v_1)\Omega(u,v_2) & \text{biadditivity} \\ & & & \\ \Omega(v,v) &=& 1 & \text{alternation} \\ & & & \\ \forall u \in V \,.\, (\forall v \in V \,.\, \Omega(u,v) = 1) &\implies& u = 0 & \text{nondegeneracy} \end{array} \tag{2.34}$$

Skew-symmetry $\Omega(u,v)\Omega(v,u) = 1$ follows from alternation. Since Ω is continuous, it is continuous in each variable, and currying yields continuous homomorphisms:[5]

$$\begin{aligned} \lceil\Omega\rceil : V &\to V^* & \qquad\qquad \lfloor\Omega\rfloor = \frac{1}{\lceil\Omega\rceil} : V &\to V^* \\ v &\mapsto \Omega(v,-) & v &\mapsto \Omega(-,v) \end{aligned}$$

Given $v \in V$, we write $v^\flat = \lceil\Omega\rceil(v)$, and given $\alpha \in V^*$, we write $\alpha^\sharp = \lceil\Omega\rceil^{-1}(\alpha)$. We sometimes require Ω to satisfy a property stronger than nondegeneracy, namely that $\lceil\Omega\rceil$ and $\lfloor\Omega\rfloor$ be isomorphisms, which we call *nuclearity*. If nuclearity holds, then:

$$\mathsf{ev}_V = \lceil\Omega\rceil^\triangle \lfloor\Omega\rfloor : V \to V^{**}$$

[5] Later we will write the type of right currying as $V \to {}^*V$ instead of $V \to V^*$, but we avoid introducing such notations for now since they are redundant in LCA. Currying is defined abstractly in Sec. 5.2.1.

where $f^{\triangle} = (f^*)^{-1} = (f^{-1})^*$ and $\mathsf{ev}_V : V \to V^{**}$ denotes the canonical injection into the double dual. Thus, nuclearity implies ev_V is an isomorphism. See Thm. 6.1.1.

Next, the *symplectic orthogonal* or *perp* of a subset $S \subseteq V$ is given by:

$$S^{\Omega} = \{v \in V \mid \Omega(S, v) = 1\}$$

The *annihilator* of a subgroup $Q \leq V$ is the subgroup:

$$\mathsf{ann}_V(Q) = \{\chi \in V^* \mid \chi(Q) = 1\}$$

If (and only if) Q is closed, then V/Q is Hausdorff, hence again locally compact (Hausdorff) abelian. One transports the topology of $(V/Q)^*$ to $\mathsf{ann}_V(Q)$ via the canonical isomorphism $\mathsf{ann}_V(Q) \xrightarrow{\sim} (V/Q)^*$. For this reason it is safest to only consider *closed* subgroups Q to remain in the category LCA. In fact, we have only defined G^* when G is locally compact (Hausdorff) abelian. Erring on the side of caution, we may sometimes assume closedness even when it is not necessary. The following proposition shows that closedness is preserved by the perp operation. The proof uses the fact that a subset of a topological space is closed if and only if it contains all its limit points. The proposition happens to apply to closed subsets as well as closed subgroups of V. For these two reasons, one should not expect the result to generalize to the abstract framework of Ch. 6. Nevertheless, there we give an entirely different proof of the weaker statement Thm. 6.9.6, which applies only to closed subgroups.

Proposition 2.4.1 *Let S be a closed subset of a locally compact abelian group V with symplectic for Ω. Then S^{Ω} is closed.*

Proof Let p be a limit point of S^{Ω} in V. Then there is a sequence $p_1, p_2, p_3, \cdots$ in S^{Ω} converging to p. Now let $q \in S$. Since $q^{\flat} : V \to V^*$ is continuous and V is Hausdorff,[6]

$$1 = \lim_{i\to\infty} q^{\flat}(p_i) = q^{\flat}\left(\lim_{i\to\infty} p_i\right) = q^{\flat}(p)$$

Since this holds for any $q \in S$, it follows that $p \in S^{\Omega}$, and so S^{Ω} is closed. ∎

Proposition 2.4.2 *Let (V, Ω) be a locally compact abelian group with symplectic form and let $Q \leq V$ be a closed subgroup. Then $\lfloor\Omega\rfloor^{-1}\mathsf{ann}_V(Q) = Q^{\Omega}$.*

[6]Limits are unique in a Hausdorff space.

Thus, for a closed subgroup Q, $\lfloor \Omega \rfloor : V \to V^*$ restricts to an isomorphism $\lfloor \Omega \rfloor_{Q^\Omega} : Q^\Omega \xrightarrow{\sim} \mathsf{ann}_V(Q)$. Then by composition, we obtain a canonical isomorphism $Q^\Omega \xrightarrow{\sim} (V/Q)^*$. By skew-symmetry, the same result of course also holds about $\lceil \Omega \rceil$.

Proof Let $q \in Q$. Then

$$q \in \lfloor \Omega \rfloor^{-1} \mathsf{ann}_V(Q) \iff \Omega(Q, q) = 1 \iff q \in Q^\Omega$$

as claimed. ■

A subset $S \subseteq V$ is *isotropic* if $S \subseteq S^\Omega$, or equivalently, $\Omega(s, s) = 1$ for all $s \in S$. Likewise, S is *coisotropic* if $S^\Omega \subseteq S$, which implies $S^\Omega \subseteq S^{\Omega\Omega}$, or equivalently, $\Omega(t, t) = 1$ for all $t \in S^\Omega$. A subset is *Lagrangian* if it is isotropic and coisotropic, i.e. $S = S^\Omega$. We are primarily concerned with closed subgroups (as opposed to subsets) with these properties.

Example Consider the symplectic form $\Omega((q_1, p_1), (q_2, p_2)) = e^{2\pi i(p_1 q_2 - p_2 q_1)}$ on the locally compact abelian group $\mathbb{R}^2$. The following table doesn't come close to listing all kinds of locally compact abelian groups, but shows some simple yet interesting examples:

isotropy	Q	Q^Ω	comment
zero	$0 \oplus 0$	$\mathbb{R} \oplus \mathbb{R}$	
isotropic	$0 \oplus \mathbb{Z}$	$\mathbb{Z} \oplus \mathbb{R}$	
Lagrangian	$0 \oplus \mathbb{R}$	$0 \oplus \mathbb{R}$	
Lagrangian	$\mathbb{Z} \oplus \mathbb{Z}$	$\mathbb{Z} \oplus \mathbb{Z}$	quotient (torus) is not complement
coisotropic	$\mathbb{Z} \oplus \mathbb{R}$	$\mathbb{R} \oplus 0$	
symplectic	$\mathbb{R} \oplus \mathbb{R}$	$0 \oplus 0$	
isotropic	$0 \oplus \frac{a}{b}\mathbb{Z}$	$\frac{b}{a}\mathbb{Z} \oplus \mathbb{R}$	
coisotropic	$\frac{b}{a}\mathbb{Z} \oplus \mathbb{R}$	$0 \oplus \frac{a}{b}\mathbb{Z}$	
depends	$\frac{a}{b}\mathbb{Z} \oplus \frac{c}{d}\mathbb{Z}$	$\frac{d}{c}\mathbb{Z} \oplus \frac{b}{a}\mathbb{Z}$	

Notice that in each row, $Q = Q^{\Omega\Omega}$. Moreover, for any (V, Ω), all de Morgan laws hold:

$$Q^\Omega \cup P^\Omega = (P \cap Q)^\Omega \qquad\qquad (Q \cup P)^\Omega = P^\Omega \cap Q^\Omega$$

Furthermore, $(-)^\Omega$ is inclusion-reversing: $Q \leq P$ implies $P^\Omega \leq Q^\Omega$. These fundamental properties of $(-)^\Omega$ enable the theory of symplectic forms to follow, and are abstracted in Ch. 6.

Definition Given an isotropic closed subgroup $Q \leq V$, there is a homomorphism:

$$\begin{aligned} \widetilde{\lceil \Omega \rceil}^Q &: V/Q \to Q^* \\ p + Q &\mapsto p^\flat \downarrow_Q \end{aligned}$$

Note $\widetilde{\lceil \Omega \rceil}^Q$ is only well-defined on account of Q being isotropic.

Theorem 2.4.3 *Let V be a locally compact abelian group with symplectic form Ω, and let Q be a closed subgroup. Then the following are equivalent:*

(i) Q is a maximally isotropic subgroup.

(ii) Q is Lagrangian (i.e. $Q = Q^\Omega$).

(iii) Q is isotropic and $\lfloor \Omega \rfloor_Q : Q \to \mathsf{ann}_V Q$ is an isomorphism.

(iv) Q is isotropic and $\widetilde{\lceil \Omega \rceil}^Q : V/Q \to Q^*$ is an isomorhpism (assuming nuclearity).

Note that characterization (iii) involves the restriction to Q not just Q^Ω, so if Q is not isotropic, the map is well-defined but not surjective. The implication ($i \implies ii$) ends up being hard to prove in the abstract framwork of Ch. 6. In fact, this is what leads to our investigation of enriched global elements in Sec. 5.1.2 and Sec. 5.1.3.

Proof ($i \implies ii$): For any $p \in Q^\Omega$ and $q_1, q_2 \in Q$ and $p_1, p_2 \in \mathbb{Z}p$, we have:

$$\Omega(q_1 + p_1, q_2 + p_2) = \cancel{\Omega(q_1, q_2)} \cancel{\frac{\Omega(q_1, p_2)}{\Omega(q_2, p_1)}} \cancel{\Omega(p_1, p_2)} = 1$$

Note that we used skew-symmetry to cancel the cross-terms, and $\Omega(p_1, p_2) = n_1 n_2 \Omega(p, p) = 1$ follows by alternation for $p_1 = n_1 p$ and $p_2 = n_2 p$ for $n_1, n_2 \in \mathbb{Z}$. Then by maximality, $Q \leq Q + \mathbb{Z}p \leq Q$, which implies $p \in Q$. ($ii \implies iii$) follows directly from Prop. 2.4.2. ($iii \iff iv$ assuming nuclearity): If Ω is nuclear, then we obtain an isomorphism:

$$(\lceil \Omega \rceil^\triangle \lfloor \Omega \rfloor)_Q = (\widetilde{\lceil \Omega \rceil}^Q)^\triangle \lfloor \Omega \rfloor_Q : Q \xrightarrow{\sim} Q^{**}$$

($iii \implies i$): If $Q \leq P \leq P^\Omega$, then $Q \leq P \leq P^\Omega \leq Q^\Omega \cong \mathsf{ann}_V Q \cong Q$ where the second-to-last isomorphism is $\lfloor \Omega \rfloor_{Q^\Omega}$ and the last is $\lfloor \Omega \rfloor_Q$. ■

We note that Q is Lagrangian even if it is only maximally isotropic among *closed* subgroups. For this one takes arbitrary $p \in Q^{\Omega}$ and $u, v \in \mathsf{cl}(Q + \mathbb{Z}p)$ and proves that $\Omega(u, v) = 1$ as before, and then constraints $Q \leq \mathsf{cl}(Q + \mathbb{Z}p) \leq Q$ in order to conclude $p \in Q$.

Finally, we would like to investigate how Lagrangian complements work for locally compact abelian groups. We have already noted that $\mathbb{Z}^{2n} \leq \mathbb{R}^{2n}$ has no complement, let alone a Lagrangian complement. Our proof is basis-independent and avoids a Gram-Schmidt style argument such as the proof of Theorem 1.1 of [da 08].

Lemma 2.4.4 *Let V be a locally compact abelian group equipped with a symplectic form Ω, let $x : Q \to V$ be the inclusion of an isotropic subgroup, and let $p \in Q^*$. Set $r = (x_! p)^\sharp$. Then the following are equivalent:*

i. $r \in Q$.

ii. p *is the trivial character.*

iii. $r = 0$.

Proof ($i \implies ii$): Let $q \in Q$. Then $pq = \Omega(r, q) = 1$ by isotropy. ($ii \implies iii$) holds because $x_! p$ is the trivial representation of V. ($iii \implies i$) is obvious. ■

Definition If Q is a locally compact abelian group, then define

$$\Omega_0 : (Q \oplus Q^*) \times (Q \oplus Q^*) \to \mathsf{U}(1)$$
$$\Omega_0(q_1 \oplus p_1, q_2 \oplus p_2) = \frac{p_1 q_2}{p_2 q_1}$$

Then Ω_0 is the *canonical symplectic form* on $Q \oplus Q^*$. Note that $\lceil \Omega \rceil$ is injective, but it might not be an isomorphism, so Ω_0 might not be a *nuclear* symplectic form.

Theorem 2.4.5 *Let V be a locally compact abelian group with nuclear symplectic form Ω. Let $x : Q \to V$ be the inclusion of an isotropic closed subgroup Q. Suppose further that Q is a direct summand of V with projection π and set $x_! = \pi^* : Q^* \to V^*$. Then*

$$\Phi_Q : Q \oplus Q^* \to V$$
$$q \oplus p \mapsto xq + (x_! p)^\sharp$$

is a symplectic embedding. Moreover, if Q is Lagrangian, then Φ_Q is a symplectomorphism.

In particular, if a Lagrangian subgroup Q has a complement, then it has a Lagrangian complement. In that case, Ω_0 is also a nuclear symplectic form on $Q \oplus Q^*$.

Proof Clearly Φ_Q is a continuous homomorphism, and by Lem. 2.4.4, $\mathsf{ker}\,\Phi_Q = 0$, so Φ_Q is injective. Let $R = (x_! Q^*)^\sharp$ and denote its inclusion map by $y : R \to V$. Consider an arbitrary element $r = (x_! p)^\sharp \in R$. By Prop. 2.4.2, $r = (x_! p)^\sharp \in Q^\Omega$ if and only if $x_! p \in \mathsf{ann}_V Q$, or equivalently, $p = x^* x_! p$ is the trivial character on Q. It follows that $Q \cap R = 0$, and so Φ_Q maps onto $Q \oplus R \leq V$. Its inverse from the image $Q \oplus R$ factors through the projection maps onto Q and R, and is thereby decomposed into continuous maps, so Φ_Q is an embedding. Similarly, $y^* x_! = (\pi y)^* = 0^* = 0 : Q^* \to V^*$, which implies that $y^* x_! p$ is the trivial character on R, or equivalently, $x_! p \in \mathsf{ann}_V R$. By another application of Prop. 2.4.2, this means $r \in P^\Omega$, so R is isotropic. To see that Φ_Q is symplectic, let $q_i \oplus p_i \in Q \oplus Q^*$ and set $r_i = (x_! p_i)^\sharp$ for $i = 1, 2$. Then

$$\begin{aligned}
\Omega(\Phi_Q(q_1 \oplus p_1), \Phi_Q(q_2 \oplus p_2)) &= \Omega(q_1 + r_1, q_2 + r_2) \\
&= \cancel{\Omega(q_1, q_2)} \frac{\Omega(r_1, q_2)}{\Omega(r_2, q_1)} \cancel{\Omega(r_1, r_2)} \\
&= \frac{(x_! p_1)(x q_2)}{(x_! p_2)(x q_1)} \\
&= \frac{p_1 q_2}{p_2 q_1} \\
&= \Omega_0(q_1 \oplus p_1, q_2 \oplus p_2)
\end{aligned}$$

as claimed. Now suppose Q is Lagrangian. To see that Φ_Q is an isomorphism, it suffices to show that it is surjective, since we have seen that it is an embedding. Note that the following diagram commutes and has exact columns:

$$\begin{tikzcd}
& 0 \arrow[d] & \\
& Q \arrow[dl] \arrow[dr] & \\
Q \oplus Q^* \arrow[rr, "\Phi_Q"] \arrow[d] & & V \arrow[d] \\
Q^* \arrow[dr] & & V/Q \arrow[ll, "\widetilde{\lceil \Omega \rceil}^Q"'] \arrow[dl] \\
& 0 &
\end{tikzcd}$$

Since Q is Lagrangian, by Thm. 2.4.3, $\widetilde{\lceil \Omega \rceil}^{Q}$ is an isomorphism. Then Φ_Q is surjective (hence an isomorphism) by Lem. G.0.8. ■

2.4.4 Heisenberg groups with center in $\mathsf{U}(1)$ and the Stone-von Neumann-Mackey theorem

In this section, we define Heisenberg groups along the lines of [Mum06], but allow for central extensions of a subgroup of $\mathsf{U}(1)$, and then state the Stone-von Neumann-Mackey theorem. Except for the Heisenberg group with center $\mathbb{R}$, the groups discussed in Sec. 2.4.1 qualify as Heisenberg groups in this sense.

Suppose that V is an abelian group lying in a central extension of locally compact groups

$$1 \longrightarrow Z \xrightarrow{i} G \xrightarrow{\pi} V \longrightarrow 1 \tag{2.35}$$

where $Z \leq \mathsf{U}(1)$ (and $i(Z) \leq \mathsf{Z}(G)$). Note that Mumford requires $Z = \mathsf{U}(1)$. Further assume that π admits a topological splitting, not to be confused with a splitting of topological groups. That is, assume there exists a continuous function $\sigma : V \to G$ such that $\pi\sigma = \mathsf{id}_V$, or equivalently, that (the underlying topological space of) G is homeomorphic to $Z \times V$. By representing elements of G as pairs (t, v), the group law takes the form:

$$(t_1, v_1)(t_2, v_2) = (t_1 t_2 C(v_1, v_2), v_1 + v_2)$$

for some function $C : G \times G \to Z$. By projecting out the first coordinate and dividing by $t_1 t_2$ we find that C is continuous. Now lift $v_1, v_2 \in V$ to some $D_{v_1}, D_{v_2} \in G$. Then since the commutator $[G, G]$ is the unique minimal $N \trianglelefteq G$ such that G/N is abelian, define:

$$\Omega(v_1, v_2) = D_{v_1} D_{v_2} D_{v_1}^{-1} D_{v_2}^{-1} \in [G, G] \leq Z \leq \mathsf{U}(1)$$

It follows that:

$$\Omega(v_1, v_2) = \frac{C(v_1, v_2)}{C(v_2, v_1)} \tag{2.36}$$

From this, it follows that Ω is continuous and satisfies $\Omega(v, v) = 1$. Now, associativity of the group law of G implies that C is a group 2-cocycle:

$$C(v_1, v_2)C(v_1 + v_2, v_3) = C(v_1, v_2 + v_3)C(v_2, v_3) \tag{2.37}$$

Using the commutativity of V and three applications of Eq. (2.37), one finds that Ω is a homomorphism in one coordinate and then the other. We call the extension Eq. (2.35) a

Heisenberg group if $\lceil\Omega\rceil$ is an isomorphism, i.e. if Ω is a nuclear symplectic form.

According to our definition, the Pauli group $\mathbf{P}_{d,n}$ qualifies as a Heisenberg group, since it lies in the central extension:

$$1 \longrightarrow \langle\tau\rangle \longrightarrow \mathbf{P}_{d,n} \longrightarrow (\mathbb{Z}/d\mathbb{Z})^{2n} \longrightarrow 1$$

where ζ is a dth root of unity and $\tau = \sqrt{\zeta}$ is a d'th root of unity and $d' = 2d$ or d, depending on whether d is even or odd. The index 2 subgroups $\mathbf{D}_{d,n} = \langle X, Z\rangle$ and $\mathbf{Q}_{d,n} = \langle \tau X, \tau Z\rangle$ also qualify, and lie in subextensions, each with center $\langle\zeta\rangle$. These are all subextensions of the Heisenberg group with $\mathsf{U}(1)$ center:

$$1 \longrightarrow \mathsf{U}(1) \longrightarrow \mathbf{WH}_{d,n} \longrightarrow (\mathbb{Z}/d\mathbb{Z})^{2n} \longrightarrow 1$$

One may form new Heisenberg groups as central products. For example, the Pauli group relevant for a composite system consisting of n_1 qu$d_1$its and n_2 qu$d_2$its is:

$$1 \longrightarrow \langle e^{2\pi i/\mathsf{lcm}(d_1', d_2')}\rangle \longrightarrow \mathbf{P}_{d_1,n_1} \odot \mathbf{P}_{d_2,n_2} \longrightarrow (\mathbb{Z}/d_1\mathbb{Z})^{n_1} \oplus (\mathbb{Z}/d_2\mathbb{Z})^{n_2} \longrightarrow 1$$

Proposition 2.4.6 *Let $Z \xrightarrow{i} G \xrightarrow{\pi} V$ be a Heisenberg group. A subgroup $Q \le V$ is isotropic if and only if π splits over Q as a (discrete) group (not just as a set), that is, if and only if there exists a homomorphism $\sigma : Q \to G$ satisfying $(\pi|_{\pi^{-1}(Q)})\sigma = \mathsf{id}_Q$.*

Proof ($\Longrightarrow$): Since Q is isotropic, $\pi^{-1}(Q)$ is a abelian subgroup of G. Now since $i(Z) = \pi^{-1}\{0\} \le \pi^{-1}(Q)$ and $i(t) = (t, 0)$ (in the above notation), Eq. (2.35) restricts to an exact sequence of abelian groups that is (still) left split:

$$1 \longrightarrow Z \xrightarrow{\ i\ } \pi^{-1}(Q) \xrightarrow{\pi|_{\pi^{-1}(Q)}} Q \longrightarrow 1$$

By the splitting lemma for abelian groups, the sequence is also right-split, as claimed. ($\Longleftarrow$): If $v_1, v_2 \in Q$, then $\sigma(v_1), \sigma(v_2) \in \sigma(Q) \le G$. Since $\sigma(Q)$ is abelian, $\Omega(v_1, v_2) = 1$ by Eq. (2.36), so Q is isotropic. ■

Theorem 2.4.7 (Stone-von Neumann-Mackey) *Let $\mathsf{U}(1) \to G \to V$ be a Heisenberg group with center $\mathsf{U}(1)$. Then up to isomorphism, there exists a unique irreducible finite dimensional unitary representation*

$$\rho : G \to \mathsf{U}(\mathcal{H})$$

that respects the center, in the sense that $\rho(e^{i\theta}) = e^{i\theta}\mathsf{id}_{\mathcal{H}}$ for all $\theta \in \mathbb{R}$. Moreover, for any Lagrangian subgroup $Q \leq V$, we may use the Hilbert space

$$\mathcal{H} = \left\{ \textit{measurable } \psi : V \to \mathbb{C} \;\middle|\; \psi(x+v) = \frac{\psi(x)}{\alpha(v)C(v,x)} \textit{ and } \int_{V/Q} |\psi(x)|^2 d\mu x < \infty \right\}$$

and define ρ by $(\rho(e^{i\theta}, v)f)(x) = e^{i\theta}C(x,v)f(x+v)$.

2.4.5 Pathologies

The definition of *symplectic form* given at the beginning of Sec. 2.4.3 is satisfactory in the sense that it lets us develop the theory of symplectic forms on a locally compact abelian group, and ultimately leads to the Stone-von Neumann-Mackey Theorem (Thm. 2.4.7). However, we would like to make the story of Sec. 2.4.3 less *ad-hoc* by showing that LCA, or correctly, a close relative $\widetilde{\mathrm{LCA}}$ (to be defined in Thm. 2.4.8), fits into the framework we develop in Ch. 6. To do so, one needs to recharacterize the symplectic form as a morphism in $\widetilde{\mathrm{LCA}}$ itself, rather than a continuous function (hence a morphism in Top) out of the Cartesian product $V \times V$ formed from the underlying topological space V.

The *tensor product* $X \otimes Y$ of abelian groups X and Y is just their tensor product as $\mathbb{Z}$-modules, (not to be confused with the direct sum $X \oplus Y$). To bring up a more familiar example, in the case of (discrete) vector spaces over a field k, the bilinear forms on a vector space V correspond canonically with morphisms $V \otimes V \to k$, and properties such as *alternation* and *nondegeneracy* carry over to properties of this morphism in a straight-forward way.[7] On the other hand, with various kinds of topological vector spaces (e.g. Hilbert spaces, Banach spaces, etc.), the situation is more subtle, as there tend be multiple ways to define a topological tensor product.

The situation with discrete abelian groups is similar to that with discrete vector spaces, though it is perhaps more natural in that case to use the integers $\mathbb{Z}$ as the dualizing object rather than the discrete circle $\mathsf{U}(1)^{\mathsf{disc}}$. Naively, our first task is thus to give a topology to the tensor product $X \otimes Y$ of the abelian groups underlying a pair of locally compact abelian groups X and Y, check that the result is again locally compact, and ensure that it gives the desired correspondence of biadditive forms. After that, we would like to check that $(\mathrm{LCA}, \otimes)$ is star-autonomous.

Towards this goal, given locally compact abelian groups X and Y, one gives the abelian group $X \multimap Y$ of continuous homomorphisms $f : X \to Y$ the topology of pointwise convergence and checks that $X \multimap Y$ is again Hausdorff. It may be, however, that $X \multimap Y$ is not locally compact. For instance, $\mathbb{Z}^\kappa \multimap \mathbb{R} \cong \mathbb{R}^\kappa$ is locally compact if and only if the cardinal κ is finite [van22]. We don't care about such examples, and would be satisfied replacing LCA by another category $\widetilde{\mathrm{LCA}}$ that excludes such pathologies. This aside, one may show that the *Pontryagin dual* $X^* = X \multimap \mathsf{U}(1)$ of any locally compact abelian group

[7] By *discrete*, we mean *without a topology*. For instance, $\mathbb{R}^n$ is discrete if we do not equip a topology.

X is again locally compact. In particular, $\mathsf{U}(1)^* \cong \mathbb{Z}$ and $\mathbb{Z}^* \cong \mathsf{U}(1)$. Furthermore, the *Pontryagin duality theorem* [Pon34] states that every locally compact abelian group X is isomorphic to its double dual X^{**} (via the curried evaluation map $x \mapsto (\chi \mapsto \chi(x))$).

In Sec. 5.3, we will give an in-depth discussion of *star-autonomous categories*. If $\multimap$, as we have defined it, is the restriction of the internal hom in some (symmetric) star-autonomous category $(\mathscr{C}, \otimes)$ that contains LCA as a subcategory, then the tensor product of locally compact groups is not necessarily locally compact either, since in any star-autonomous category, it turns out that we have a natural isomorphism:

$$(X \otimes Y)^* \cong X \multimap Y^*$$

This is all saved by a construction of Barr and Kleisli [Bar09; BK01]:

Theorem 2.4.8 (Barr-Kleisli) *There exists a category* $\widetilde{\mathrm{LCA}}$ *satisfying the following:*

(i) $\widetilde{\mathrm{LCA}}$ *is star-autonomous.*

(ii) $\widetilde{\mathrm{LCA}}$ *is complete and cocomplete.*

(iii) $\widetilde{\mathrm{LCA}}$ *is a category of topological abelian groups containing* LCA *as a full subcategory.*

(iv) The underlying abelian group of the internal hom $X \multimap Y$ *is* $\mathsf{hom}_{\widetilde{\mathrm{LCA}}}(X, Y)$*.*

Properties (i), (ii), and (iv) explain why the framework we develop in Ch. 6 generalizes the situation of symplectic forms on locally compact abelian groups. That is, they show that $\widetilde{\mathrm{LCA}}$ is star-autonomous and pre-abelian. A counterexample given in [van22], showing that LCA is not abelian, still applies to $\widetilde{\mathrm{LCA}}$. Namely, the inclusion $\mathbb{R}^{\mathsf{disc}} \to \mathbb{R}$ is monic and epic but not an isomorphism.[8] Property (iii), roughly speaking, allows us to give concrete (element-wise) calculations just as if we were dealing with LCA, but without worrying about analytical technicalities. (Instead of verifying the analytical details, one verifies that a desired property follows from (iii).) Property (iv) ensures that currying works in the expected way. Namely, by currying a morphism $f : X \otimes Y \to Z$, one obtains:

$$\begin{aligned} \lceil f \rceil : X &\to Y \multimap Z \\ x &\mapsto (y \mapsto f(x, y)) \end{aligned}$$

[8] See Appx. G for facts about abelian and preabelian categories.

It follows that the underlying abelian group of $X \otimes Y$ is the tensor product of the underlying abelian groups, i.e. the tensor product of $\mathbb{Z}$-modules. Furthermore, for each object V, the biadditive forms $\Omega : V \times V \to \mathsf{U}(1)$ defined as in Eq. (2.34) are in bijective correspondence with morphisms $\tilde{\Omega} : V \otimes V \to \mathsf{U}(1)$, and the correspondence is characterized by the identity:

$$\Omega(u, v) = \tilde{\Omega}(u \otimes v) \qquad\qquad \text{for all } u, v \in V$$

In particular, *nondegeneracy* is captured by the injectivity of $\lceil\tilde{\Omega}\rceil : V \to V^*$, though as we have noted, we may sometimes require that $\lceil\tilde{\Omega}\rceil$ be an isomorphism.[9]

Finally, note that $\widetilde{\mathrm{LCA}}$ has two monoidal products: $\otimes$ and its de Morgan dual $\boxtimes$, defined by $Y \boxtimes X = (X^* \otimes Y^*)^*$. Monoidal categories are discussed in Sec. 5.2. The monoidal unit of $\otimes$ is $\mathbb{Z}$ and that of $\boxtimes$ is $\mathsf{U}(1)$. This makes $\widetilde{\mathrm{LCA}}$ markedly different from the category of free finitely generated R-modules, in which $\otimes \cong \boxtimes$ and both monoidal units are R. The example of $\widetilde{\mathrm{LCA}}$ is why we need to consider star-autonomous categories, and not just autonomous categories in Ch. 6.

[9]Note that our use of the *tilde* notation here is temporary and we write $\tilde{\omega}$ to mean something else in Ch. 6.

Chapter 3

A functional programming language for generalized projective Clifford operations

In joint work with Jennifer Paykin [PW24], we construct a functional programming language $\lambda^{\mathscr{P}_\mathrm{C}}$ for programming with multiqu*d*it projective Clifford operations. In the resulting *Pauli-based programming* abstraction, the user describes projective Clifford operations by their conjugation action on Paulis, rather than their action on state vectors. In this way, $\lambda^{\mathscr{P}_\mathrm{C}}$ is more in line with the Schrödinger picture (at least in the $d = 2$ case where the Pauli matrices are Hermitian) rather than the Heisenberg picture.

Pauli-based data structures have already been used in compilers [WPR23],[Pay+23b], simulation [AG04],[Li+22], circuit synthesis [SBW23],[Sch+24], and equivalence checking [Amy19],[KW20],[BPV21]. The novelty of $\lambda^{\mathscr{P}_\mathrm{C}}$ is that it allows for *programming* with Paulis. This is achieved by constructing a new type system resembling a linear type system modified to keep track of phases. The system relies on the condensed encodings defined in Sec. 2.3, and as a result, the language supports multiqu*d*it generalized Clifford operations for all d, most notably when d is even (such as a power of 2). The language thereby supports a vast array of quantum operations, including the standard quantum Fourier transform on a system of n qubits, which qualifies as a single qu*d*it projective Clifford for $d = 2^n$, (not to be confused with a multiqubit projective Clifford).

Expressions in $\lambda^{\mathscr{P}_\mathrm{C}}$ may be composed in various ways, using familiar abstractions from functional programming. The most primitive of these is pattern-matching, which essentially allows the user to define a projective Clifford by its tableau:

```
hadamard :: ⌈ Pauli ⊸ Pauli ⌉
hadamard ⌈X = Z⌉
hadamard ⌈Z = X⌉
```

The type signature ⌈ `Pauli` ⊸ `Pauli` ⌉ indicates that `hadamard` expresses a single qu$d$it projective Clifford operation. We hard code the constraint of being a valid projective Clifford operation directly into the typing rule for generating such expressions. We prove metatheoretically that this (syntactic) constraint translates over to the categorical semantics, using the fact that the operational semantics is sound with respect to the categorical semantics. In the present exposition, we start with the categorical semantics, and build up $\lambda^{\mathscr{P}_{\mathrm{C}}}$ as its internal language. To this end, we first define a category $\mathscr{C}$ equivalent to FGF-$\mathbb{Z}/d\mathbb{Z}$-MOD, whose concrete description is more suitable for the programming consideration. This description lets us inductively define a canonical symplectic form on each module of even rank. We then extend these to a category $\mathscr{P}_{\mathrm{C}}$ whose objects are either analogous to the loop $(\mathbf{Q}_{d,n}, \star)$ defined in Sec. 2.3 or the stage of definition $\mathbb{Z}/d\mathbb{Z}$ for global elements. Morphisms in $\mathscr{P}_{\mathrm{C}}$ are either projective Clifford operations, global elements, or scalars.

Under the hood, projective Clifford expressions in $\lambda^{\mathscr{P}_{\mathrm{C}}}$ correspond to condensed encodings (μ, ψ) as defined in Sec. 2.3. Instead of the matrix product, Pauli operations are composed using the condensed product $\star$. This makes it so that when d is even, the user only ever deals with roots of unity of order d, as opposed to $2d$. The complications associated with dealing with condensed encodings are out of sight and mind of the user, and instead are diverted to the operational and categorical semantics.

The type system is built up in steps. First we define a linear type system $\lambda^{\mathscr{C}}$ similar to [AD17], then define symplectic types, and next Pauli types. The resulting type system $\lambda^{\mathscr{P}_{\mathrm{C}}}$ is augmented with a Cartesian layer, which is integrated with the underlying Pauli type system, thereby forming a linear-nonlinear (LNL) type system. The categorical semantics of $\lambda^{\mathscr{C}}$ lies in the category $\mathscr{C}$, whereas that of the Pauli type system lies in $\mathscr{P}_{\mathrm{C}}$. The Pauli type system, roughly speaking, accounts for the noncommutativity of quantum mechanics by attaching phase components to $\mathscr{C}$-expressions. $\mathscr{P}_{\mathrm{C}}$ is not a model for linear logic,[1] and in particular, lacks a monoidal product interpreting the "$\otimes$" operation of linear logic (not to be confused with the tensor product of Hilbert spaces). For this reason, we are only able

[1]The Pauli type system $\lambda^{\mathscr{P}_{\mathrm{C}}}$ (without the LNL layer) is nevertheless still considered a *linear* type system, characterized by the fact that it doesn't have weakening or contraction.

to account for a single free Pauli variable. This is one reason (among others) our system does not currently support higher Clifford operations.

Specifying the language and its properties takes a lot of work, and some details have been omitted, including some inductive arguments that range over all typing rules. For further detail, the reader is referred to [PW24].

The language design is based on its categorical semantics, and so before delving into the syntax, we begin laying out the relevant mathematical structure in Sections 3.1 and 3.2. With a view towards the language, we give the category $\mathscr{C}$ an inductive definition that is nearly identical to the typing rules given in Sections 3.3 and 3.5. After specifying each type system $\lambda^{\mathscr{C}}$ and $\lambda^{\mathscr{P}_{\mathrm{C}}}$, we describe the operational semantics in Sections 3.4 and 3.6. Next, add a nonlinear layer to $\lambda^{\mathscr{P}_{\mathrm{C}}}$, which allows for auxiliary functions and is where we finally give support for lifted projective Clifford opertions. Pseudocode examples are given in Sec. 3.8, and lastly, we discuss future work in Sec. 3.9.

3.1 A nearly skeletal subcategory of free finitely generated modules

The category of free finitely generated R-modules, FGF-R-MOD, for a commutative ring R, is far better behaved than LCA, due to the lack of a topology. Namely, FGF-R-MOD is a compact category (i.e. autonomous and with a symmetric structure) with respect to the tensor product $\otimes = \otimes_R$ of R-modules, so there is no need for a theorem along the lines of Thm. 2.4.8 in order to use it in Ch. 6. On the other hand, FGF-R-MOD is not preabelian unless R is a field, since it does not include kernels or cokernels (quotients). This means we cannot plug it into the framework of Ch. 6 unless R is a field, but that is ok, since we can use $\widetilde{\mathrm{LCA}}$ to treat the other examples we are interested in. Still, we have a need to consider FGF-R-MOD (or something similar) when $R = \mathbb{Z}/d\mathbb{Z}$ and d is not necessarily prime. Better yet, we will define a nearly skeletal subcategory MAT(R) by specifying some inductive rules for generating objects, and this will serve as the categorical semantics for the type system $\lambda^{\mathscr{C}}$ to be defined in Sec. 3.3, with the inductive definition of the category matching the typing rules for the language.

If $R = \mathbb{Z}/d\mathbb{Z}$, then we use phase space $V = Q \oplus Q$ (or $Q \oplus Q^*$) with $Q = R^n$, and the relevant Hilbert space is $\mathbb{C}Q$. The configuration space of a composite quantum system is a direct sum $Q = Q_1 \oplus Q_2$ and the Hilbert space is $\mathbb{C}(Q_1 \oplus Q_2) \cong \mathbb{C}Q_1 \otimes_{\mathbb{C}} \mathbb{C}Q_2$. We encounter the tensor product of R-modules $\otimes = \otimes_R$ in the formation of the symplectic form $\omega : V \otimes V \to R$ and in the semantics of linear typing contexts $[\![\Delta; x : \alpha]\!] = [\![\Delta]\!] \otimes [\![\alpha]\!]$. Internal homs $Q \multimap P$ also arise in the semantics, and so we need to consider a subcategory MAT(R) that contains R^n and is closed under $\oplus$, $\otimes$, and $\multimap$. As one does, we build the language up inductively, and so it is convenient to work with a category MAT(R) whose definition roughly follows the same grammatical structure.

The category MAT(R) is defined as follows. Objects are certain pairs (V, E), which we inductively specify below, consisting of a free finitely generated R-module V equipped with ordered basis E, and whose morphisms are given by:

$$\mathsf{hom}_{\mathrm{MAT}(R)}((U,E),(V,F)) = \mathsf{hom}_{\mathrm{FGF}\text{-}R\text{-}\mathrm{MOD}}(U,V)$$

We will inductively combine objects with the operations $\oplus$, $\otimes$, and $\multimap$ (explained below). This creates some redundancy, since for example, $R^{\oplus 4} \cong R^{\oplus 2} \otimes R^{\oplus 2}$, meaning the objects of MAT(R) work strictly more like expressions than numbers, e.g. $1+1+1+1$ is distinguished from $(1+1)(1+1)$. This redundancy is intentional, similar to how in logic one often defines a language of propositions using an over-complete set of logical connectives. We note that $\textsc{Mat}(R)$ is nevertheless *equivalent* to the category whose objects are natural numbers and morphisms are matrices.

A morphism $h : (U, E) \to (V, F)$ in $\textsc{Mat}(R)$ is uniquely specified by a matrix with annotations for the ordered bases E resp. F of the domain and codomain. We could have just as well defined $\textsc{Mat}(R)$ as its image in R-$\textsc{Mod}$ under the forgetful functor and then noted that each module V gets inductively assigned a canonical basis. In a way, we are just pointing out that "coordinate-based linear algebra" is generated by a categorified (context-free) grammar.

Finally, we give the inductive definition. There are two base cases. First, $(0, ()) \in \mathsf{ob}(\textsc{Mat}(R))$ where 0 is the trivial R-module and $()$ is the empty sequence. Second, $(R, (1)) \in \mathsf{ob}(\textsc{Mat}(R))$, where $1 \in R$ is the ring identity included in R as an R-module over itself. So far, $\textsc{Mat}(R)$ only has two objects; we now specify more objects by requiring $\textsc{Mat}(R)$ to be closed under $\oplus$, $\otimes$, and $\multimap$.

Whenever $(U, E), (V, F) \in \mathsf{ob}(\textsc{Mat}(R))$, we shall now require that $\textsc{Mat}(R)$ contain the object $(U \oplus V, E \sqcup F)$, where $U \oplus V$ is the "outer direct sum" of the modules U and V and $E \sqcup F$ is the "concatenated basis". In other words, elements of $U \oplus V$ are symbols $u \oplus v$ indexed by $u \in U$ and $v \in V$, with the usual module structure, and $E \sqcup F$ is the *concatenation of sequences* formed from E and F:

$$E \sqcup F = (e \oplus 0 \,|\, e \in E) \frown (0 \oplus f \,|\, f \in F)$$

Since objects are inductively constructed with the direct sum, we inductively obtain the following canonical morphisms:

$$\begin{aligned} \iota^U_{U\oplus V} : U &\to U \oplus V & \iota^V_{U\oplus V} : V &\to U \oplus V & \pi^{U\oplus V}_U : U \oplus V &\to U & \pi^{U\oplus V}_V : U \oplus V &\to V \\ u &\mapsto u \oplus 0 & v &\mapsto 0 \oplus v & u \oplus v &\mapsto u & u \oplus v &\mapsto v \end{aligned}$$

These are seen to satisfy the relations and two universal properties of the biproduct. One may also easily show that each is natural in U and V. Note that by slight abuse of notation, we have written $U \to U \oplus V$ above in place of $(U, E) \to (U, E) \oplus (V, F)$, and so on. We will continue with this pattern when it doesn't cause confusion.

Next, given $(U, E), (V, F) \in \mathsf{ob}(\textsc{Mat}(R))$, we require $\textsc{Mat}(R)$ to contain the Kronecker product $(U \otimes V, E \times F)$, where $U \otimes V$ is the module of formal linear combinations of elements of the Kronecker basis $E \times F$, i.e. the dictionary-ordered sequence of symbols:

$$E \times F = (e \otimes f \,|\, e \in E, f \in F)$$

We then extend the $\otimes$ notation so that $u \otimes v$ is defined for each $u \in U$ and $v \in V$ by forcing it to satisfy bilinearity. We then obtain a very suspicious canonical map:

$$\begin{aligned} \Delta_V : V &\to V \otimes V \\ e &\mapsto e \otimes e \end{aligned}$$

This is defined for each $(V, E) \in \mathsf{ob}(\textsc{Mat}(R))$, where Δ_V is defined by linearly extending its action on basis vectors $e \in E$. It is of course not the case that $v \mapsto v \otimes v$ for arbitrary $v \in V$, since this would not be linear. Despite being defined canonically, i.e. given a "uniform" definition for each V, Δ_V is not *natural* in V. Naturality would require the following diagram to commute for all $h : U \to V$:

$$\begin{tikzcd} U \arrow[r, "\Delta_U"] \arrow[d, "h"'] & U \otimes U \arrow[d, "h \otimes h"] \\ V \arrow[r, "\Delta_V"'] & V \otimes V \end{tikzcd}$$

If R has an element λ that satisfies $\lambda \neq \lambda^2$, then the diagram does not commute when $U = V = R$ and h is multiplication by λ, but notice that this counterexample does not work over $\mathbb{F}_2$. A better counterexample, which works over any commutative ring R, is that naturality fails when $U = V = R^{\oplus 2}$ and $h = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$. When $R = \mathbb{C}$, this is the (rescaled) Hadamard matrix. Indeed, one path takes $|0\rangle$ to $|00\rangle + |11\rangle$ and the other takes it to $(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$. In fact, there is no natural transformation $\Delta : \mathsf{id}_{\textsc{Mat}(R)} \Rightarrow \otimes$ that is cocommutative and coassociative, as defined in [Abr09], since this would imply that every endomorphism $f : V \to V$ is a homothety $f = \lambda \mathsf{id}_V$ by a theorem of Abramsky:

Theorem 3.1.1 ***(Near collapse of cloning [Abr09])*** *In a category with a natural monoidal transformation $\Delta_V : V \to V \otimes V$ that is coassociative and cocommutative, every endomorphism $f : V \to V$ is a homothety $f = \lambda \mathsf{id}_V$ (where $\mathsf{tr}(f)$).*

The next surprise is that there is a canonical deletion map:

$$\begin{aligned} \nabla_V : V &\to R \\ e &\mapsto 1 \end{aligned}$$

taking each basis vector $e \in E$ of a given $(V, E) \in \mathsf{ob}(\textsc{Mat}(R))$ to the basis vector $1 \in R$. As with cloning, we find that deletion is unnatural, again by considering the naturality square for the Hadamard map h. Again, there is no natural deletion map $\nabla : \mathsf{id}_{\textsc{Mat}(R)} \Rightarrow R$ by the following theorem of Abramsky, this time because $\textsc{Mat}(R)$ is not a preorder:

Theorem 3.1.2 ***(No deleting [Abr09])*** *Any compact closed category with a natural transformation $\nabla_V : V \Rightarrow \mathbb{1}$ (to the constant functor valued at the monoidal unit $\mathbb{1}$) is a preorder.*

Lastly, given $(U, E), (V, F) \in \mathsf{ob}(\textsc{Mat}(R))$, we give $\textsc{Mat}(R)$ the object $(U \multimap V, E \triangleright F)$, where $U \multimap V$ is the R-module of linear maps $h : U \to V$, and where $E \triangleright F$ consists of:

$$\begin{aligned} e \multimap f : U &\to V \\ e' &\mapsto \delta_{e,e'} f \end{aligned}$$

ranging over each $f \in F$ and then $e \in E$, where $\delta_{e,e'} = 1$ if $e = e'$ or else 0. In particular, $V^* = V \multimap R$ is the dual module and $E^* = E \triangleright R$ is the dual basis. It is no coincidence that the sequence $E \triangleright F$ is (canonically) isomorphic to the Kronecker basis $F \times (E \triangleright R)$, and indeed, this isomorphism underlies the nuclear structure of $\textsc{Mat}(R)$.

Let us define the *rank* of $(V, E) \in \mathsf{ob}(\textsc{Mat}(R))$ as the length of the sequence E. Then since R is commutative, it satisfies the invariant basis number (IBN) property [Coh66], and by induction (on the constructors $\oplus$, $\otimes$, and $\multimap$), this is the usual notion of *rank* of a finitely generated free module over a ring with IBN property. Now, using the ordering on the bases, we may define canonical isomorphisms, such as the following, by their basis action:

$$\begin{aligned} \mathsf{distr}_{A,B,C,D} : (A \oplus B) \otimes (C \oplus D) &\xrightarrow{\sim} A \otimes B \;\oplus\; A \otimes D \;\oplus\; B \otimes C \;\oplus\; B \otimes D \\ \mathsf{nuc}_{U,V} : V \otimes U^* &\xrightarrow{\sim} U \multimap V \\ \mathsf{unit}_V : R \otimes V &\xrightarrow{\sim} V \\ \mathsf{sym}_{U,V} : U \otimes V &\xrightarrow{\sim} V \otimes U \end{aligned}$$

As we have seen above, canonically defined families of morphisms are not always natural. The isomoprhisms listed above, however, are indeed natural. It is a tedious exercise to check that they are the restrictions of a compact closed structure on $\textsc{fgf}$-R-$\textsc{Mod}$. Ultimately, by this strategy, one shows that not just $\textsc{fgf}$-R-$\textsc{Mod}$ but also $\textsc{Mat}(R)$ is compact closed. For example, one begins by showing that the operations $\oplus$, $\otimes$, and $\multimap$ are the restrictions to $\text{MAT}(R)$ of analogous operations on $\text{FGF-}R\text{-MOD}$, establishes the adjunction $- \otimes (V, E) \dashv (V, E) \multimap -$, and shows that distr is the natural isomorphism obtained from the fact that left adjoints (such as $- \otimes (V, E)$) preserve limits (such as $\oplus$). We have defined Δ_V and ∇_V by their action on the canonically generated basis of V, so as one might expect, there are equivalent formuations of Δ_V and ∇_V that use induction directly rather than referencing these bases. Interestingly, they involve some of the natural maps above. For example,

$$\Delta_{U \oplus V} = \mathsf{distr}^{-1}_{U,V,U,V}(\iota^{U^{\otimes 2}}_{U^{\otimes 2} \,\oplus\, U \otimes V} \oplus \iota^{V^{\otimes 2}}_{V \otimes U \,\oplus\, V^{\otimes 2}})(\Delta_U \oplus \Delta_V) \tag{3.1}$$

One must additionally provide inductive formulas for $\Delta_{U \otimes V}$ and $\Delta_{U \multimap V}$ to complete the inductive definition of Δ, much like exhausting all cases of a *pattern matching* definition in functional programming. It is tempting to try to prove naturality of Δ by induction on these formulas, or likewise to try to prove naturality of ∇, but this doesn't work. For example, why can't we conclude from Eq. (3.1) that Δ is a natural transformation over $\mathbb{F}_2$? In both base cases (where $V = 0$ or $V = \mathbb{F}_2$), the naturality square for Δ_V commutes, so why doesn't it follow by induction that $\Delta_{U \oplus V}$ commutes for all U and V, at least in the $\oplus$-fragment of $\text{MAT}(\mathbb{F}_2)$? In particular, how do we reconcile this with the Hadamard example, where the naturality square for $\Delta_{\mathbb{F}_2^2}$ fails to commute despite the base case working out? The answer is that if η_1 and η_2 are natural transformations, then although $\eta_1 \oplus \eta_2$ is natural, $\eta_1 \otimes \eta_2$ might not be. In the case of Δ, the tensors appearing in subexpressions of the right-hand-side of Eq. (3.1) end up destroying the naturality and hence the induction.

The direct sum $\oplus$ also admits a canonical duplication, called the *diagonal map*, which (unlike Δ) is natural:

$$\begin{aligned} \mathsf{diag}_V : V &\to V \oplus V \\ v &\mapsto v \oplus v \end{aligned}$$

Note that $v \mapsto v \oplus v$ holds for all $v \in V$, not just for basis vectors as with Δ. Next, $\oplus$ has a (natural) coduplication map, namely, the *vector addition* part of the module structure:

$$\begin{aligned} +_V : V \oplus V &\to V \\ v_1 \oplus v_2 &\mapsto v_1 + v_2 \end{aligned}$$

One may check that diag and $+$ arise from the universal properties of the biproduct. Likewise, we may realize scalar multiplication as an R-module homomorphism:

$$\cdot_V : R \otimes V \to V$$

These observations, that the module structure is described internally to the category $\mathscr{C}$, also apply to R-MOD and other variants. From here, one may easily verify that the module structure already defined on $U \oplus V$ satisfies an inductive formula, which we sketch now. Using the canonical associative and symmetric structures for $\oplus$ to reorganize terms, one checks that $+_{U\oplus V}$ is alternately given by the following (natural) inductive formula:

$$(U \oplus V) \oplus (U \oplus V) \xrightarrow{\text{(reorganize)}} (U \oplus U) \oplus (V \oplus V) \xrightarrow{+_U \oplus +_V} U \oplus V$$

Likewise, scalar multiplication on $U \oplus V$ is seen to satisfy the inductive formula:

$$R \otimes (U \oplus V) \xrightarrow{\mathsf{distr}_{R,0,U,V}} R \otimes U \;\; \oplus \;\; R \otimes V \xrightarrow{\cdot_U \oplus \cdot_V} U \oplus V$$

We also note that $\mathscr{C}$ is enriched in R-MOD (and hence also in AB). Accordingly, we have *pointwise scalar multiplication* and *pointwise vector addition* operations for appropriately typed morphisms. As in any additive category, if $f, g : U \to V$ are morphisms, then their sum $f + g : U \to V$ (the pointwise sum) factors through the biproduct:

$$U \xrightarrow{\mathsf{diag}_U} U \oplus U \xrightarrow{f \oplus g} V \oplus V \xrightarrow{\cdot_V} V$$

Likewise, pointwise scalar multiplication of $r : U \to R$ and $v : W \to V$ factors as:

$$U \otimes W \xrightarrow{r \otimes v} R \otimes V \xrightarrow{\cdot_V} V$$

These inductive characterizations of the module structure arise when defining the interpretation of well-typed judgments in Sec. 3.3.

Ultimately, the only phase spaces we wish to consider are $V = (\mathbb{Z}/d\mathbb{Z})^{2n}$ and $\mathbb{R}^{2n}$. These are treated by FGF-R-MOD using $R = \mathbb{Z}/d\mathbb{Z}$ or $\mathbb{R}$, respectively, or just as well by MAT(R). Recall that our reason for considering LCA is that $V = \mathbb{R}^{2n}$ has an interesting Lagrangian subgroup that is not an ($\mathbb{R}$-linear) Lagrangian sub*space*, namely $\mathbb{Z}^{2n}$, which leads to the quasiperiodic representation of the Heisenberg group. This required us to find a star-autonomous substitute for LCA that includes such examples. Another strategy would be to generate a nearly-skeletal subcategory of LCA, along the same lines as we have done here for FGF-R-MOD, involving only the objects we actually care about. This, at a glance, seems like it would be substantially harder, since we would need to include non-free $\mathbb{Z}$-modules, such as $\mathbb{Z}/d\mathbb{Z}$, and it would involve analytical subtleties. We would then have to ensure that the resulting category is a *feasible solution* to our problem, in the sense of being star-autonomous and preabelian. The Barr-Kleiseli construction [Bar09; BK01] let us avoid this entirely, which was better for the theoretical application, but for the programming language application, it is far easier to work with $\textsc{Mat}(\mathbb{Z}/d\mathbb{Z})$.

3.2 Categories $\mathscr{C}$, $\mathscr{S}$, and $\mathscr{P}_{\mathrm{C}}$

Let $R = \mathbb{Z}/d\mathbb{Z}$. We now define categories $\mathscr{C}$, $\mathscr{S}$, and $\mathscr{P}_{\mathrm{C}}$, towards describing the categorical semantics of $\lambda^{\mathscr{P}_{\mathrm{C}}}$. First, set $\mathscr{C} = \textsc{Mat}(R)$. Next, objects in $\mathscr{S}$ are *symplectic modules*, that is, pairs (V, ω_V) where V is an object of $\mathscr{C}$ and $\omega : V \otimes V \to R$ is a symplectic form. Morphisms in $\mathscr{S}$ are *symplectic maps*, that is, R-linear maps $\psi : U \to V$ satisfying $\omega_V(\psi u_1, \psi u_2) = \omega_U(u_1, u_2)$ for all $u_1, u_2 \in U$. Every symplectic map ψ is injective, and ψ is bijective if and only if it has an inverse, which is a symplectic map, in which case ψ is called a *symplectomorphism*. If $\psi : (U, \omega_U) \to (V, \omega_V)$ is a symplectic map, then $\mathsf{rk}\, U \leq \mathsf{rk}\, V$ with equality if and only if ψ is a symplectomorphism. We usually write ω instead of ω_V. Endomorphisms of (V, ω) are therefore automorphisms, and comprise the *symplectic group* $\mathsf{Sp}(V, \omega)$. This tells us $\mathscr{S}$ an *oidification* of the symplectic group.

Using the canonical basis that comes with each object $Q \in \mathsf{ob}(\mathscr{C})$, the module $Q \oplus Q^*$ comes with a canonical symplectic form, defined by $\omega((q_1, p_1), (q_2, p_2)) = p_2 q_1 - p_1 q_2$. For convenience, by the dual basis construction $Q \cong Q^*$, we instead use the corresponding canonical symplectic form $\tilde{\omega}_{Q \oplus Q}$ on $Q \oplus Q$. In matrix form, $\tilde{\omega}_{Q \oplus Q} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \otimes I_Q$. On the other hand, there is also an *interlaced* symplectic form on $Q \oplus Q$ with matrix $\omega_{Q \oplus Q} = I_Q \otimes \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. These are equivalent by the change of basis:

$$(q_1, \cdots, q_n, p_1, \cdots, p_n) \leftrightsquigarrow (q_1, p_1, \cdots, q_n, p_n)$$

The interlaced symplectic form also arises as follows: if U and V are symplectic modules, then $U \oplus V$ gets a canonical symplectic form by setting $\omega_{U \oplus V} = \omega_U + \omega_V$. Note that $\tilde{\omega}$ and ω are two different symplectic forms on $(Q \oplus Q) \oplus (Q \oplus Q)$. We prefer ω over $\tilde{\omega}$ in the specification of $\lambda^{\mathscr{P}_{\mathrm{C}}}$, so we tend to focus on $(R^{\oplus 2})^{\oplus n}$ over $(R^{\oplus n})^{\oplus 2}$.

Next we define a category $\mathscr{P}_{\mathrm{C}}$ whose objects are essentially the subsets $\mathbf{Q}_{d,n} \subseteq \mathbf{P}_{d,n}$ defined in Sec. 2.3, and whose morphisms include projective Clifford operations between such objects. Before we defined projective Clifford operations as center-fixing automorphisms of the Pauli group $\mathbf{P}_{d,n}$, which are seen to be automorphisms of $\mathbf{Q}_{d,n}$ and bijectively correspond with pairs $(\mu, \psi) \in V^* \times \mathsf{Sp}(V)$ where $V = R^{2n}$. It is a convenient programming abstraction to allow $\mu \in V^*$ to be paired with a symplectic map $\psi : U \to V$ rather than requiring $U = V$. This corresponds to a physically legal operation since such pairs may be regarded as projective Clifford operations on the output system. Since the semantics of our type system involves elements and characters of the phase space V, we also include these as morphisms. Thus, we include a unit object $\bullet$ as a "classical" stage of definition for global elements, and put:

$$\begin{aligned}\mathsf{ob}(\mathscr{P}_{\mathrm{C}}) &= \{\mathbf{Q}_V \,|\, V \in \mathsf{ob}(\mathscr{S})\} \sqcup \{\bullet\}\\ \mathsf{hom}_{\mathscr{P}_{\mathrm{C}}}(\mathbf{Q}_U, \mathbf{Q}_V) &= \mathsf{hom}_{\mathscr{C}}(U, R) \times \mathsf{hom}_{\mathscr{S}}(U, V) = U^* \times \mathsf{Sp}(U, V)\\ \mathsf{hom}_{\mathscr{P}_{\mathrm{C}}}(\bullet, \mathbf{Q}_V) &= \mathsf{hom}_{\mathscr{C}}(R, R) \times \mathsf{hom}_{\mathscr{C}}(R, V) = R \times V\\ \mathsf{hom}_{\mathscr{P}_{\mathrm{C}}}(\bullet, \bullet) &= \mathsf{hom}_{\mathscr{C}}(R, R) = R\end{aligned}$$

where the objects $\mathbf{Q}_V$ are symbols indexed by $V \in \mathsf{ob}(\mathscr{S})$. Composition of morphisms is defined as in Sec. 2.3. Namely, for $(\mu_2, \psi_2) \in \mathsf{hom}_{\mathscr{P}_{\mathrm{C}}}(\mathbf{Q}_U, \mathbf{Q}_V)$ and $(\mu_1, \psi_1) \in \mathsf{hom}_{\mathscr{P}_{\mathrm{C}}}(A, \mathbf{Q}_U)$ for arbitrary $A \in \mathsf{ob}(\mathscr{P}_{\mathrm{C}})$, we define:

$$(\mu_2, \psi_2)(\mu_1, \psi_1) = (\mu_3, \psi_2\psi_1)$$

where $\mu_3 \in \mathsf{hom}_{\mathscr{C}}(A, R)$ is defined by its action on standard basis elements by:

$$\mu_3 b = \mu_1 b + \mu_2\psi_1 b + \kappa^{\psi_2}\psi_1 b$$

where $\kappa^{\psi_2} : V \to F_2$ is the phase correction function defined in Sec. 2.3. In the remaining case, given $(t, v) \in \mathsf{hom}_{\mathscr{P}_{\mathrm{C}}}(\bullet, \mathbf{Q}_V)$ and $r \in \mathsf{hom}_{\mathscr{P}_{\mathrm{C}}}(\bullet, \bullet)$, define:

$$(t, v)r = (t', rv)$$

where t' is defined in terms of the *sign* function introduced in Sec. 2.3:

$$t' = rt + \frac{d}{2}\mathsf{sgn}(\underline{r}\,\underline{v})$$

The idea is that (t, v) encodes $\zeta^t\Delta_{\underline{v}}$, and we want evaluation at r to be like exponentiation:

$$(\zeta^t\Delta_{\underline{v}})^{\underline{r}} = \zeta^{rt}\Delta_{\underline{r}\,\underline{v}} = \zeta^{rt+\frac{1}{2}\mathsf{sgn}(\underline{r}\,\underline{v})}\Delta_{\underline{rv}}$$

We may at times write $\langle a\rangle$ for a morphism of the form (a, id).

3.3 Typing rules and categorical semantics for $\lambda^{\mathscr{C}}$

The type system $\lambda^{\mathscr{C}}$ consists of disjoint sets:

$$\mathsf{ctxs}(\mathscr{C}) \qquad \mathsf{types}(\mathscr{C}) \qquad \mathsf{exprs}(\mathscr{C}) \qquad \mathsf{vars}(\mathscr{C})$$

together with a ternary relation $\vdash^{\mathscr{C}} \subseteq \mathsf{ctxs}(\mathscr{C}) \times \mathsf{types}(\mathscr{C}) \times \mathsf{exprs}(\mathscr{C})$, called the *$\mathscr{C}$-typing judgment*. We begin by defining *$\mathscr{C}$-types* by the following grammar:

$$\alpha ::= \mathtt{Unit} \mid \alpha_1 \oplus \alpha_2 \mid \alpha_1 \multimap \alpha_2$$

This notation indicates that $\mathsf{types}(\mathscr{C})$ is the intersection of all sets X subject to: (i), X contains the symbol $\mathtt{Unit}$; and (ii), if $\alpha_1, \alpha_2 \in X$, then X contains the syntactical expressions $\mathtt{(}\alpha_1 \oplus \alpha_2\mathtt{)}$ and $\mathtt{(}\alpha_1 \multimap \alpha_2\mathtt{)}$. For example, $\mathtt{(}\alpha_1 \oplus \alpha_2\mathtt{)}$ consists of a left parenthesis symbol $\mathtt{(}$ followed by substring α_1, then the $\oplus$ symbol, then α_2, and lastly, the right parenthesis symbol $\mathtt{)}$. For ease of exposition we omit parentheses whenever possible.

Next, *$\mathscr{C}$-expressions* are defined by the grammar:

$$\begin{aligned} a ::=\ & x \mid \mathtt{let}\ x = a\ \mathtt{in}\ a' & & x \in \mathsf{vars}(\mathscr{C}) \\ & \mid \mathbf{0}_\alpha \mid r \mid a \cdot a' \mid a_1 + a_2 & & r \in \mathbb{Z}/d\mathbb{Z} \\ & \mid [a_1, a_2] \mid \mathtt{case}\ a\ \mathtt{of}\ \{\iota_1(x_1) \to a_1 \mid \iota_2(x_2) \to a_2\} & & \\ & \mid \lambda x.a \mid aa' & & \end{aligned}$$

We have expressed the grammar for $\mathscr{C}$-expressions using a notation called *Backus-Naur form* (BNF) [Knu64]. Vertical bars delineate options for the kind of expression being defined, and the expressions between the bars implicitly contain inductively-defined subexpressions when the same symbol is used (e.g. a) or a slight variant indicating another such subexpression (e.g. a'). As is standard in the field of programming languages (PL), we subsequently leave quantification of pieces of syntax implicit in the metatheoretical analysis.

Intuitively, $\mathscr{C}$-types correspond to objects in (the $\oplus$,$\multimap$-fragment of) $\mathscr{C}$ and $\mathscr{C}$-expressions involve *linear variables* x and evaluate to elements of these objects. In order to follow standard conventions for linear type systems, we use the square bracket syntax $[a_1, a_2]$ for ordered pairs, since round parentheses are traditionally used for tensors. The *$\mathscr{C}$-linear typing contexts* may also be regarded syntactically as follows:

$$\Delta ::= \cdot \mid \Delta, x : \alpha \qquad\qquad x \in \mathsf{vars}(\mathscr{C}) \text{ and } \alpha \in \mathsf{types}(\mathscr{C})$$

However, these are subject to the constraint that each linear variable $x \in \mathsf{vars}(\mathscr{C})$ may appear at most once in Δ. Another way to view a linear typing context Δ is as a partial function $\Delta : \mathsf{vars}(\mathscr{C}) \to \mathsf{types}(\mathscr{C})$ (with ordered domain). In that sense, the syntax Δ, Δ' stands for the relational union of Δ and Δ' viewed as partial functions, and is only defined when their domains are disjoint. We write $\Delta(x)$ for the $\mathscr{C}$-type assigned to the variable x.

We have again used the BNF form to define a formal language, this time the language of contexts. The context $\cdot$, for example, is just a meaningless piece of syntax–a chicken scratch. It is called the *emtpy context*.

Next, we define some formal expressions $\Delta \vdash^{\mathscr{C}} a : \alpha$, called *$\mathscr{C}$-typing derivations*, which collectively specify the $\mathscr{C}$-typing judgment $\vdash^{\mathscr{C}}$. Explicitly, the *$\mathscr{C}$-typing derivations* are precisely those expressions $\Delta \vdash^{\mathscr{C}} a : \alpha$ inductively reached by the following *$\mathscr{C}$-typing rules*:

$$\frac{}{x : \alpha \vdash^{\mathscr{C}} x : \alpha} \qquad \frac{\Delta, x : \alpha \vdash^{\mathscr{C}} a' : \alpha' \qquad \Delta' \vdash^{\mathscr{C}} a : \alpha}{\Delta, \Delta' \vdash^{\mathscr{C}} \texttt{let } x = a \texttt{ in } a' : \alpha'}$$

$$\frac{}{\cdot \vdash^{\mathscr{C}} r : \texttt{Unit}} \qquad \frac{\Delta \vdash^{\mathscr{C}} r : \texttt{Unit} \qquad \Delta' \vdash^{\mathscr{C}} a : \alpha}{\Delta, \Delta' \vdash^{\mathscr{C}} r \cdot a : \alpha} \qquad \frac{}{\Delta \vdash^{\mathscr{C}} \mathbf{0} : \alpha}$$

$$\frac{\Delta \vdash^{\mathscr{C}} a_1 : \alpha \qquad \Delta \vdash^{\mathscr{C}} a_2 : \alpha}{\Delta \vdash^{\mathscr{C}} a_1 + a_2 : \alpha} \qquad \frac{\Delta \vdash^{\mathscr{C}} a_1 : \alpha_1 \qquad \Delta \vdash^{\mathscr{C}} a_2 : \alpha_2}{\Delta \vdash^{\mathscr{C}} [a_1, a_2] : \alpha_1 \oplus \alpha_2}$$

$$\frac{\Delta, x_1 : \alpha_1 \vdash^{\mathscr{C}} a_1 : \alpha' \qquad \Delta, x_2 : \alpha_2 \vdash^{\mathscr{C}} a_2 : \alpha' \qquad \Delta' \vdash^{\mathscr{C}} a : \alpha_1 \oplus \alpha_2}{\Delta, \Delta' \vdash^{\mathscr{C}} \texttt{case } a \texttt{ of } \{\iota_1(x_1) \to a_1 \mid \iota_2(x_2) \to a_2\} : \alpha'}$$

$$\frac{\Delta, x : \alpha \vdash^{\mathscr{C}} a : \alpha'}{\Delta \vdash^{\mathscr{C}} \lambda x.a : \alpha \multimap \alpha'} \qquad \frac{\Delta_1 \vdash^{\mathscr{C}} a_1 : \alpha \multimap \alpha' \qquad \Delta_2 \vdash^{\mathscr{C}} a_2 : \alpha}{\Delta_1, \Delta_2 \vdash^{\mathscr{C}} a_1 a_2 : \alpha'}$$

Here $\cdot \vdash^{\mathscr{C}} r : \texttt{Unit}$ is typed for each $r \in \mathbb{Z}/d\mathbb{Z}$. In standard usage, $\mathscr{C}$-derivations are also called *well-formed judgments*. It is standard to simply write "$\Delta \vdash^{\mathscr{C}} a : \alpha$" as a meta-proposition asserting, "$\Delta \vdash^{\mathscr{C}} a : \alpha$ is a well-formed judgment". This is read as indicating that a $\mathscr{C}$-expression a involving the linear variables in Δ has type α.

Intuitively, $\lambda^{\mathscr{C}}$ is a λ-calculus for working in the category of free finitely generated $\mathbb{Z}/d\mathbb{Z}$-modules, similar to [DD24]. Towards making this into a more precise statement, we now give $\lambda^{\mathscr{C}}$ a categorical semantics. As an intermediate step, note that the data specifying $\lambda^{\mathscr{C}}$, namely the $\mathscr{C}$-expressions, $\mathscr{C}$-types, $\mathscr{C}$-contexts, and $\mathscr{C}$-derivations, equivalently specify a category whose objects are the $\mathscr{C}$-types or $\mathscr{C}$-contexts (remembering which) and whose morphisms are the well-formed typing judgments $\Delta \vdash^{\mathscr{C}} a : \alpha$. Reusing the notation $\lambda^{\mathscr{C}}$ to refer to this category, the *categorical semantics* of $\lambda^{\mathscr{C}}$ is then defined as a functor:

$$[\![-]\!]^{\mathscr{C}} : \lambda^{\mathscr{C}} \to \mathscr{C}$$

Explicitly, the *interpretation* $[\![-]\!]^{\mathscr{C}}$ of a type or context (object) is given by:

$$\begin{array}{cc} \text{types:} & \text{contexts:} \\ [\![\texttt{Unit}]\!]^{\mathscr{C}} = \mathbb{Z}/d\mathbb{Z} & [\![\cdot]\!]^{\mathscr{C}} = \mathbb{Z}/d\mathbb{Z} \\ [\![\alpha_1 \oplus \alpha_2]\!]^{\mathscr{C}} = [\![\alpha_1]\!]^{\mathscr{C}} \oplus [\![\alpha_2]\!]^{\mathscr{C}} & [\![\Delta, x : \alpha]\!]^{\mathscr{C}} = [\![\Delta]\!]^{\mathscr{C}} \otimes [\![\alpha]\!]^{\mathscr{C}} \\ [\![\alpha_1 \multimap \alpha_2]\!]^{\mathscr{C}} = [\![\alpha_1]\!]^{\mathscr{C}} \multimap [\![\alpha_2]\!]^{\mathscr{C}} & \end{array}$$

Notice that both the context $x : \alpha$ and the type α get mapped to the same object of $\mathscr{C}$. This allows us to define:

$$[\![x : \alpha \vdash^{\mathscr{C}} x : \alpha]\!]^{\mathscr{C}} = \mathsf{id}_{[\![\alpha]\!]^{\mathscr{C}}} \tag{3.2}$$

When defining the interpretation of a typing judgment (morphism), we often abuse notation and write a in place of $\Delta \vdash^{\mathscr{C}} a : \alpha$. So Eq. (3.2) becomes $[\![x]\!]^{\mathscr{C}} = \mathsf{id}_{[\![\alpha]\!]^{\mathscr{C}}}$. Next, consider the `let` rule, which is like a "judgmental modus ponens". We define $[\![\texttt{let}\ x = a\ \texttt{in}\ \alpha']\!]^{\mathscr{C}}$ by:

$$[\![\Delta, \Delta']\!]^{\mathscr{C}} = [\![\Delta]\!]^{\mathscr{C}} \otimes [\![\Delta']\!]^{\mathscr{C}} \xrightarrow{\mathsf{id}_{[\![\Delta]\!]^{\mathscr{C}}} \otimes [\![a]\!]^{\mathscr{C}}} [\![\Delta]\!]^{\mathscr{C}} \otimes [\![\alpha]\!]^{\mathscr{C}} \xrightarrow{[\![a']\!]^{\mathscr{C}}} [\![\alpha']\!]^{\mathscr{C}}$$

For each $r \in \mathbb{Z}/d\mathbb{Z}$, $[\![r]\!]^{\mathscr{C}} : \mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ is given by $a \mapsto ra$. Next, given well-typed judgments $\Delta \vdash^{\mathscr{C}} r : \texttt{Unit}$ and $\Delta' \vdash^{\mathscr{C}} a : \alpha$, we define $[\![r \cdot a]\!]^{\mathscr{C}}$ as pointwise scalar multiplication:

$$[\![\Delta, \Delta']\!]^{\mathscr{C}} = [\![\Delta]\!]^{\mathscr{C}} \otimes [\![\Delta']\!]^{\mathscr{C}} \xrightarrow{[\![r]\!]^{\mathscr{C}} \otimes [\![a]\!]^{\mathscr{C}}} \mathbb{Z}/d\mathbb{Z} \otimes [\![\alpha]\!]^{\mathscr{C}} \xrightarrow{\cdot_{[\![\alpha]\!]^{\mathscr{C}}}} [\![\alpha]\!]^{\mathscr{C}}$$

Note that $\mathscr{C}$ is enriched in $\mathbb{Z}/d\mathbb{Z}$-Mod. For empty context (the *constant* case), $[\![r \cdot a]\!]^{\mathscr{C}} = [\![r]\!]^{\mathscr{C}}\, [\![a]\!]^{\mathscr{C}}$ is just composition (up to unitor coherences), which corresponds to ordinary scalar multiplication, in the sense that the global element $[\![r]\!]^{\mathscr{C}}$ corresponds to an element (in the traditional sense) of $\mathbb{Z}/d\mathbb{Z}$. Next, we set $[\![\mathbf{0}]\!]^{\mathscr{C}} = 0 : [\![\Delta]\!]^{\mathscr{C}} \to [\![\alpha]\!]^{\mathscr{C}}$ (the zero morphism), and interpret $+$ as pointwise addition of morphisms: $[\![a_1 + a_2]\!]^{\mathscr{C}} = [\![a_1]\!]^{\mathscr{C}} + [\![a_2]\!]^{\mathscr{C}}$. Equivalently, $+$ is interpreted as the following composition of morphisms, as one would expect by applying the Curry-Howard correspondence to the relevant typing rule:

$$[\![\Delta]\!]^{\mathscr{C}} \xrightarrow{\mathsf{diag}_{[\![\Delta]\!]^{\mathscr{C}}}} [\![\Delta]\!]^{\mathscr{C}} \oplus [\![\Delta]\!]^{\mathscr{C}} \xrightarrow{[\![a_1]\!]^{\mathscr{C}} \oplus [\![a_2]\!]^{\mathscr{C}}} [\![\alpha]\!]^{\mathscr{C}} \oplus [\![\alpha]\!]^{\mathscr{C}} \xrightarrow{+_{[\![\alpha]\!]^{\mathscr{C}}}} [\![\alpha]\!]^{\mathscr{C}}$$

For $[\![[a_1, a_2]]\!]$, we do the same thing, but without adding the two components together at the end, and without requiring the two entries to have the same type:

$$[\![\Delta]\!]^{\mathscr{C}} \xrightarrow{\mathsf{diag}_{[\![\Delta]\!]^{\mathscr{C}}}} [\![\Delta]\!]^{\mathscr{C}} \oplus [\![\Delta]\!]^{\mathscr{C}} \xrightarrow{[\![a_1]\!]^{\mathscr{C}} \oplus [\![a_2]\!]^{\mathscr{C}}} [\![\alpha_1]\!]^{\mathscr{C}} \oplus [\![\alpha_2]\!]^{\mathscr{C}} = [\![\alpha_1 \oplus \alpha_2]\!]^{\mathscr{C}}$$

The categorical semantics helps explain the intuition of the case rule. One may be more familiar with the `case` syntax in a language like Haskell, whose categorical semantics Hask is very similar to Set. There, the coproduct is the disjoint union, and its elimination rule (the `case` rule) returns one branch or the other. In $\mathscr{C}$, however, the coproduct is the direct sum $\oplus$, and so the case rule returns a linear combination. Explicitly, $[\![\texttt{case}\ a\ \texttt{of}\ \{\iota_1(x_1) \to a_1 \mid \iota_2(x_2) \to a_2\}]\!]^{\mathscr{C}}$ is defined as the following composition:

$$\begin{tikzcd}
{[\![\Delta, \Delta']\!]^{\mathscr{C}}} \arrow[r, equal] & {[\![\Delta]\!]^{\mathscr{C}} \otimes [\![\Delta']\!]^{\mathscr{C}}} \arrow[r, "\mathsf{id}_{[\![\Delta]\!]^{\mathscr{C}}} \otimes [\![a]\!]^{\mathscr{C}}"] & {[\![\Delta]\!]^{\mathscr{C}} \otimes ([\![\alpha_1]\!]^{\mathscr{C}} \oplus [\![\alpha_2]\!]^{\mathscr{C}})} \arrow[d] \\
& & {[\![\Delta]\!]^{\mathscr{C}} \otimes [\![\alpha_1]\!]^{\mathscr{C}} \oplus [\![\Delta]\!]^{\mathscr{C}} \otimes [\![\alpha_2]\!]^{\mathscr{C}}} \arrow[d, equal] \\
{[\![\alpha']\!]^{\mathscr{C}}} & {[\![\alpha']\!]^{\mathscr{C}} \oplus [\![\alpha']\!]^{\mathscr{C}}} \arrow[l, "+_{[\![\alpha']\!]^{\mathscr{C}}}"'] & {[\![\Delta, x : \alpha_1]\!]^{\mathscr{C}} \oplus [\![\Delta, x : \alpha_2]\!]^{\mathscr{C}}} \arrow[l, "[\![a_1]\!]^{\mathscr{C}} \oplus [\![a_2]\!]^{\mathscr{C}}"']
\end{tikzcd}$$

Next, λs are just partially evaluated `let`s so their interpretation is given by (left) currying $[\![a]\!]^{\mathscr{C}} : [\![\Delta, x : \alpha]\!]^{\mathscr{C}} = [\![\Delta]\!]^{\mathscr{C}} \otimes [\![\alpha]\!]^{\mathscr{C}} \to [\![\alpha']\!]^{\mathscr{C}}$ in order to obtain a morphism:

$$[\![\lambda x.a]\!]^{\mathscr{C}} : [\![\Delta]\!]^{\mathscr{C}} \to [\![\alpha]\!]^{\mathscr{C}} \multimap [\![\alpha']\!]^{\mathscr{C}} = [\![\alpha \multimap \alpha']\!]^{\mathscr{C}}$$

Finally, the interpretation $[\![a_1 a_2]\!]^{\mathscr{C}}$ of application resembles the modus ponens rule:

$$\begin{tikzcd}
{[\![\Delta_1, \Delta_2]\!]^{\mathscr{C}}} \arrow[r, equal] & {[\![\Delta_1]\!]^{\mathscr{C}} \otimes [\![\Delta_2]\!]^{\mathscr{C}}} \arrow[r, "[\![a_1]\!]^{\mathscr{C}} \otimes [\![a_2]\!]^{\mathscr{C}}"] & {[\![\alpha \multimap \alpha']\!]^{\mathscr{C}} \otimes [\![\alpha]\!]^{\mathscr{C}}} \arrow[d, equal] \\
& {[\![\alpha']\!]^{\mathscr{C}}} & {([\![\alpha]\!]^{\mathscr{C}} \multimap [\![\alpha']\!]^{\mathscr{C}}) \otimes [\![\alpha]\!]^{\mathscr{C}}} \arrow[l, "\mathsf{lefteval}^{[\![\alpha]\!]^{\mathscr{C}}}_{[\![\alpha']\!]^{\mathscr{C}}}"']
\end{tikzcd}$$

This completes our definition of the categorical semantics $[\![-]\!]^{\mathscr{C}}$. Functorality of $[\![-]\!]^{\mathscr{C}}$ is imposed *by definition*. It is evident from the construction that $[\![-]\!] : \lambda^{\mathscr{C}} \to \mathscr{C}$ is essentially surjective, and one can show that it is full, but it is not faithful since distinct judgments, e.g. $\Delta \vdash^{\mathscr{C}} r \cdot (a_1 + a_2) : \alpha$ and $\Delta \vdash^{\mathscr{C}} r \cdot v_1 + r \cdot v_2 : \alpha$, may map to the same morphism. This is intended, of course, since users of the programming langauge are permitted to use different expressions that encode the same morphism. We are less concerned with the functorial relationship between the language $\lambda^{\mathscr{C}}$ and its categorical semantics $\mathscr{C}$, and moreso with the relationship between the categorical semantics and the *operational* semantics, which we describe in the next section.

If one is more familiar with category theory than type theory, then the way one arrives at the type system is by starting with the categorical semantics written in terms of morphism composition as above, though the role of the contexts arguably becomes a lot clearer from the type theory point of view. There is another way to view the categorical side of the correspondence. Since the more familiar way of working with module homomorphisms is in terms of their action on elements, we can rewrite the interpretations above concretely. Alternately, these formulas can also be directly gleaned from the typing rules:

$$
\begin{aligned}
[\![x]\!]^{\mathscr{C}}(s) &= s \\
[\![\texttt{let } x = a \texttt{ in } a']\!]^{\mathscr{C}}(s \otimes s') &= [\![a']\!]^{\mathscr{C}}(s' \otimes [\![a]\!]^{\mathscr{C}}(s)) \\
[\![r]\!]^{\mathscr{C}}(s) &= r \cdot s \\
[\![r \cdot a]\!]^{\mathscr{C}}(s \otimes s') &= [\![r]\!]^{\mathscr{C}}(s) \cdot [\![a]\!]^{\mathscr{C}}(s') \\
[\![\mathbf{0}]\!]^{\mathscr{C}}(s) &= 0 \\
[\![a_1 + a_2]\!]^{\mathscr{C}}(s) &= [\![a_1]\!]^{\mathscr{C}}(s) + [\![a_2]\!]^{\mathscr{C}}(s) \\
[\![[a_1, a_2]]\!]^{\mathscr{C}}(s) &= [\![a_1]\!]^{\mathscr{C}}(s) \oplus [\![a_2]\!]^{\mathscr{C}}(s) \\
[\![\texttt{case } a \texttt{ of } \{\iota_1(x_1) \to a_1 \mid \iota_2(x_2) \to a_2\}]\!]^{\mathscr{C}}(s \otimes s') &= [\![a_1]\!]^{\mathscr{C}}(s' \oplus c_1) + [\![a_2]\!]^{\mathscr{C}}(s' \oplus c_2) \\
&\qquad (\text{where } [\![a]\!]^{\mathscr{C}}(s) = c_1 \oplus c_2) \\
[\![\lambda x.a]\!]^{\mathscr{C}}(s)(s') &= [\![a]\!]^{\mathscr{C}}(s \otimes s') \\
[\![a_1 a_2]\!]^{\mathscr{C}}(s \otimes s') &= ([\![a_1]\!]^{\mathscr{C}}(s))([\![a_2]\!]^{\mathscr{C}}(s'))
\end{aligned}
$$

3.4 Operational semantics for $\lambda^{\mathscr{C}}$

In Sec. 3.3, we noted that the functor $[\![-]\!]^{\mathscr{C}}$ is not faithful. Working with equality of typing judgments is unreasonably strict, but there is something similar to faithfulness that we do need. For one thing, when closed expressions a_1 and a_2 normalize to the same value v, we would like them to be interpreted as the same morphism $[\![a_1]\!]^{\mathscr{C}} = [\![a_2]\!]^{\mathscr{C}} = [\![v]\!]^{\mathscr{C}}$.

$$\begin{tikzcd}
& \text{closed judgments in } \lambda^{\mathscr{C}} \arrow[dl, "\text{operational semantics } \downarrow"'] \arrow[dr, "\text{categorical semantics } [\![-]\!]^{\mathscr{C}}"] & \\
\text{values in } \lambda^{\mathscr{C}} \arrow[rr, dashed, "\text{(soundness required here)}"'] & & \text{morphisms in } \mathscr{C}
\end{tikzcd}$$

This is not good enough, though, as this property (*soundness*) should apply more generally to *open* expressions. However, since the step rule will only apply to closed expressions, we need to phrase the soundness condition in terms of value context mappings (models). Thus, we need to provide an operational semantics that is *sound* in the sense that whenever two equivalent value context mappings δ_1 and δ_2 map terms a_1 and a_2 to equivalent values, morphism equality holds:

$$(\text{for all}\,(\delta_1, \delta_2) \in \mathcal{V}_\Delta,\ (\delta_1(a_1), \delta_2(a_2)) \in \mathcal{E}_\alpha) \implies [\![\Delta \vdash^{\mathscr{C}} a_1 : \alpha]\!]^{\mathscr{C}} = [\![\Delta \vdash^{\mathscr{C}} a_2 : \alpha]\!]^{\mathscr{C}} \quad (3.3)$$

The operational semantics will consist of a strongly normalizing step rule. Strong normalization means that closed expressions eventually normalize to a unique *value*, and that they reach this value regardless of the path taken. This latter point (confluence) is trivial since the step rule we define will be deterministic. The sets $\mathcal{V}_\Delta$ and $\mathcal{E}_\alpha$ referenced in Eq. (3.3) are then *logical relations* defined in terms of this set of values.

Note that we don't require $\delta_1(a_1)$ and $\delta_2(a_2)$ to normalize to *equal* values, but to *equivalent* values (defined by the logical relations below). For example, $\lambda x.(2 \cdot x)$ is equivalent but not equal to $\lambda x.(x + x)$.

To begin, given a $\mathscr{C}$-context Δ, a *value context mapping* (*model*) for Δ is a function δ with the same domain as Δ, taking each $x : \alpha$ to a $\mathscr{C}$-value v of type α, i.e. a value v satisfying $\cdot \vdash v : \alpha$, where *$\mathscr{C}$-values* are certain $\mathscr{C}$-expressions, defined as follows:

$$v ::= r \,|\, [v_1, v_2] \,|\, \lambda x.a \qquad\qquad r \in \mathbb{Z}/d\mathbb{Z},\ a \in \mathsf{exprs}(\mathscr{C}),\ \text{and } v_1, v_2 \in \mathsf{vals}(\mathscr{C})$$

A *closed expression (of type α)* is an expression a such that $\cdot \vdash^{\mathscr{C}} a : \alpha$. We thus have a three-way distinction between (open) expressions, closed expressions, and values. Values are always closed. We will soon define an equivalence relation $\equiv$ internal to $\lambda^{\mathscr{C}}$ using the characterization on the left side of Eq. (3.3). By soundness, this will have the effect of pulling the notion of *morphism equality* back to the language. Thus, we will extend $\lambda^{\mathscr{C}}$ to include some judgments of the form $\Delta \vdash^{\mathscr{C}} a_1 \equiv a_2 : \alpha$, which certify morphism equality $[\![a_1]\!]^{\mathscr{C}} = [\![a_2]\!]^{\mathscr{C}}$. This has tremendous utility in the language. Namely, the characterization on the left side of Eq. (3.3) satisfies an inductive compatibility property with the typing rules, making it far more convenient to deal with on the language side than morphism equality. Judgments of the form $\Delta \vdash a_1 \equiv a_2 : \alpha$ will arise as hypotheses in some of the typing rules for $\lambda^{\mathscr{P}_{\mathrm{C}}}$. In particular, projective Clifford operations specified by the user are required to satisfy an algebraic relation, namely, the vanishing of the symplectic form. By encoding this relation as a hypothesis using $\equiv$, the relation check for a user-specified projective Clifford will be delegated to the typechecker. This is our main reason for introducing $\equiv$, and a technical rationale for the definition of *soundness*.

If a and a' are expressions and x is a variable, then $a\{a'/x\}$ denotes the expression obtained from a by replacing substituting a' for occurrences of x in a non-capturing way. We define the operational semantics as follows. First define the *beta reduction* rule $\rightarrow_\beta$ by:

$$\begin{array}{cc}
r_1 \cdot r_2 \rightarrow_\beta r_1 \cdot r_2 \in \mathbb{Z}/d\mathbb{Z} & r_1 + r_2 \rightarrow_\beta r_1 + r_2 \in \mathbb{Z}/d\mathbb{Z} \\
r \cdot [v_1, v_2] \rightarrow_\beta [r \cdot v_1, r \cdot v_2] & [v_1, v_2] + [v_1', v_2'] \rightarrow_\beta [v_1 + v_1', v_2 + v_2'] \\
r \cdot \lambda x.a \rightarrow_\beta \lambda x.r \cdot a & (\lambda x_1.a_1) + (\lambda x_2.a_2) \rightarrow_\beta \lambda x.a_1\{x/x_1\} + a_2\{x/x_2\}
\end{array}$$

$$\begin{aligned}
\texttt{let } x = v \texttt{ in } a' &\rightarrow_\beta a'\{v/x\} \\
\texttt{case } [v_1, v_2] \texttt{ of } \{\iota_1(x_1) \rightarrow a_1 \mid \iota_2(x_2) \rightarrow a_2\} &\rightarrow_\beta a_1\{v_1/x_1\} + a_2\{v_2/x_2\} \\
(\lambda x.a)v &\rightarrow_\beta a\{v/x\}
\end{aligned}$$

In the top row, on the left side of each $\rightarrow_\beta$, $r_1 \cdot r_2$ and $r_1 + r_2$ are $\mathscr{C}$-expressions involving the symbols $\cdot$ or $+$, whereas on the right side they are elements of $\mathbb{Z}/d\mathbb{Z}$ where $\cdot$ and $+$ are the ring operations. Note that only *certain closed expressions* appear to the left of $\rightarrow_\beta$.

We now extend $\to_\beta$ to a new step operation $\to$ in the *call-by-value* style:

$$\frac{a \to_\beta a'}{a \to a'} \qquad \frac{a \to a'}{\texttt{let } x = a \texttt{ in } a'' \to \texttt{let } x = a' \texttt{ in } a''}$$

$$\frac{a \to a'}{a \cdot a'' \to a' \cdot a''} \qquad \frac{a \to a'}{r \cdot a \to r \cdot a'}$$

$$\frac{a_1 \to a_1'}{a_1 + a_2 \to a_1' + a_2} \qquad \frac{a_2 \to a_2'}{v_1 + a_2 \to v_1 + a_2'}$$

$$\frac{a_1 \to a_1'}{[a_1, a_2] \to [a_1', a_2]} \qquad \frac{a_2 \to a_2'}{[v_1, a_2] \to [v_1, a_2']}$$

$$\frac{a \to a'}{\texttt{case } a \texttt{ of } \{\iota_1(x_1) \to a_1 \mid \iota_2(x_2) \to a_2\} \to \texttt{case } a' \texttt{ of } \{\iota_1(x_1) \to a_1 \mid \iota_2(x_2) \to a_2\}}$$

$$\frac{a_1 \to a_1'}{a_1 a_2 \to a_1' a_2} \qquad \frac{a_2 \to a_2'}{v a_2 \to v a_2}$$

Notice that the rules are designed to be deterministic, that is, at most one rule may be applied to a given closed expression. Two expressions are said to be α-*equivalent* if one can be transformed into the other by renaming bound variables in a non-capturing way.

Theorem 3.4.1 (Strong normalization) *If* $\cdot \vdash^{\mathscr{C}} a : \alpha$ *then there exists a unique value* v*, up to* α*-equivalence, such that* $a = a_1 \to \cdots \to a_n = v$*. (In such a case, we write* $a \downarrow v$*.)*

Proving strong normalization involves proving some technical lemmas by induction on the typing rules and step rules. For the proofs, see [PW24].

The operational semantics also satisfies type preservation ($\cdot \vdash^{\mathscr{C}} a : \alpha$ and $a \to a'$ implies $\cdot \vdash^{\mathscr{C}} a' : \alpha$) and behaves well under variable substitution ($\cdot \vdash^{\mathscr{C}} v : \alpha$ and $\Delta, x : \alpha \vdash^{\mathscr{C}} a : \alpha'$ implies $\Delta \vdash^{\mathscr{C}} a\{v/x\} : \alpha'$). These are also proved by induction.

In order to state the soundness condition, we introduce the following logical relations:

$$\begin{aligned}
\mathcal{V}_{\texttt{Unit}} &= \{(r,r) \mid r \in \mathbb{Z}/d\mathbb{Z}\} \\
\mathcal{V}_{\alpha_1 \oplus \alpha_2} &= \{([v_1,v_2],[v_1',v_2']) \mid (v_1,v_1') \in \mathcal{V}_{\alpha_1} \text{ and } (v_2,v_2') \in \mathcal{V}_{\alpha_2}\} \\
\mathcal{V}_{\alpha \multimap \alpha'} &= \{(\lambda x_1.a_1, \lambda x_2.a_2) \mid \text{for all } (v_1,v_2) \in \mathcal{V}_\alpha,\ (a_1\{v_1/x_1\}, a_2\{v_2/x_2\}) \in \mathcal{E}_{\alpha'}\} \\
\mathcal{E}_\alpha &= \left\{ (a_1,a_2) \;\middle|\; \begin{array}{l} \cdot \vdash^{\mathscr{C}} a_1 : \alpha,\ \cdot \vdash^{\mathscr{C}} a_2 : \alpha,\ \text{ and whenever } a_1 \downarrow v_1 \text{ and} \\ a_2 \downarrow v_2, \text{ it follows that } (v_1,v_2) \in \mathcal{V}_\alpha \end{array} \right\} \\
\mathcal{V}_\Delta &= \{(\delta_1,\delta_2) \mid \text{for all } x \in \mathsf{dom}(\Delta),\ (\delta_1(x),\delta_2(x)) \in \mathcal{V}_{\Delta(x)}\}
\end{aligned}$$

Now, given a context value mapping δ for $\Delta = x_1 : \alpha_1, \cdots, x_n : \alpha_n$ and an expression a, we write:

$$\delta(a) = a\{\delta(x_1)/x_1, \cdots, \delta(x_n)/x_n\}$$

Definition (of $\equiv$) Suppose $\Delta \vdash^{\mathscr{C}} a_1 : \alpha$ and $\Delta \vdash^{\mathscr{C}} a_2 : \alpha$. Then if for all $(\delta_1,\delta_2) \in \mathcal{V}_\Delta$ it follows that $(\delta(a_1),\delta(a_2)) \in \mathcal{E}_\alpha$, then we declare $\Delta \vdash^{\mathscr{C}} a_1 \equiv a_2 : \alpha$.

Thus, $\equiv$ is defined by the left-hand-side of Eq. (3.3).

Theorem 3.4.2 *The equivalence relation is compatible with the typing rules for $\lambda^{\mathscr{C}}$, in the sense that one derives the following rules:*

$$\frac{}{x : \alpha \vdash^{\mathscr{C}} x \equiv x : \alpha} \qquad \frac{\Delta_1 \vdash^{\mathscr{C}} a_1 \equiv a_1' : \alpha \qquad \Delta_2, x : \alpha \vdash^{\mathscr{C}} a_2 \equiv a_2' : \alpha'}{\Delta_1, \Delta_2 \vdash^{\mathscr{C}} \texttt{let } x = a_1 \texttt{ in } a_2 \equiv \texttt{let } x = a_1' \texttt{ in } a_2' : \alpha'}$$

$$\frac{r \in \mathbb{Z}/d\mathbb{Z}}{\cdot \vdash^{\mathscr{C}} r \equiv r : \texttt{Unit}} \qquad \frac{\Delta_1 \vdash^{\mathscr{C}} a_1 \equiv a_1' : \texttt{Unit} \qquad \Delta_2 \vdash^{\mathscr{C}} a_2 \equiv a_2' : \alpha}{\Delta_1, \Delta_2 \vdash^{\mathscr{C}} a_1 \cdot a_2 \equiv a_1' \cdot a_2' : \alpha}$$

$$\frac{}{\Delta \vdash^{\mathscr{C}} \mathbf{0} \equiv \mathbf{0} : \alpha} \qquad \frac{\Delta \vdash^{\mathscr{C}} a_1 \equiv a_1' : \alpha \qquad \Delta \vdash^{\mathscr{C}} a_2 \equiv a_2' : \alpha}{\Delta \vdash^{\mathscr{C}} a_1 + a_2 \equiv a_1' + a_2' : \alpha}$$

$$\frac{\Delta \vdash^{\mathscr{C}} a_1 \equiv a_1' : \alpha_1 \qquad \Delta \vdash^{\mathscr{C}} a_2 \equiv a_2' : \alpha_2}{\Delta \vdash^{\mathscr{C}} [a_1, a_2] \equiv [a_1', a_2'] : \alpha_1 \oplus \alpha_2}$$

$$\frac{\Delta \vdash^{\mathscr{C}} a \equiv a' : \alpha_1 \oplus \alpha_2 \qquad \Delta', x_1 : \alpha_1 \vdash^{\mathscr{C}} a_1 \equiv a_1' : \alpha' \qquad \Delta', x_2 : \alpha_2 \vdash^{\mathscr{C}} a_2 \equiv a_2' : \alpha'}{\Delta, \Delta' \vdash^{\mathscr{C}} \texttt{case } a \texttt{ of } \{\iota_1(x_1) \to a_1 \mid \iota_2(x_2) \to a_2\} \equiv \texttt{case } a' \texttt{ of } \{\iota_1(x_1) \to a_1' \mid \iota_2(x_2) \to a_2'\} : \alpha'}$$

$$\frac{\Delta, x : \alpha \vdash^{\mathscr{C}} a \equiv a' : \alpha'}{\Delta \vdash^{\mathscr{C}} \lambda x.a \equiv \lambda x.a' : \alpha \multimap \alpha'} \qquad \frac{\Delta_1 \vdash^{\mathscr{C}} a_1 \equiv a_1' : \alpha \multimap \alpha' \qquad \Delta_2 \vdash^{\mathscr{C}} a_2 \equiv a_2' : \alpha}{\Delta_1, \Delta_2 \vdash^{\mathscr{C}} a_1 a_2 \equiv a_1' a_2' : \alpha'}$$

From these rules, it follows that $\equiv$ is an internal equivalence relation:

$$\frac{\Delta \vdash^{\mathscr{C}} a : \alpha}{\Delta \vdash^{\mathscr{C}} a \equiv a : \alpha} \qquad \frac{\Delta \vdash^{\mathscr{C}} a_1 \equiv a_2 : \alpha}{\Delta \vdash^{\mathscr{C}} a_2 \equiv a_1 : \alpha} \qquad \frac{\Delta \vdash^{\mathscr{C}} a_1 \equiv a_2 : \alpha \qquad \Delta \vdash^{\mathscr{C}} a_2 \equiv a_3 : \alpha}{\Delta \vdash^{\mathscr{C}} a_1 \equiv a_3 : \alpha}$$

Towards proving soundness, we note the following:

Lemma 3.4.3 *Let* $(\mu, \psi) \in \mathsf{hom}_{\mathscr{P}_{\mathrm{C}}}(\alpha, \mathbf{Q}_V)$ *and* $(\mu', \psi') \in \mathsf{hom}_{\mathscr{P}_{\mathrm{C}}}(\mathbf{Q}_V, \mathbf{Q}_{V'})$*, and let* $a \in \mathsf{hom}_{\mathscr{C}}(V, \mathbb{Z}/d\mathbb{Z})$*. Then*

$$(\langle a\rangle(\mu', \psi')) \circ (\mu, \psi) = \langle a \circ \psi\rangle(\mu', \psi') \circ (\mu, \psi)$$

Proof First, $(\mu', \psi') \circ (\mu, \psi) = (\mu_0, \psi' \circ \psi)$ where μ_0 is defined on basis elements by

$$\mu_0(b) = \mu(b) + \mu'(\psi(b)) + \kappa^{\psi'}(\psi(b))$$

where $\kappa^{\psi'}$ is the phase correction function defined in Sec. 2.3. On the other hand,

$$(\langle a\rangle(\mu', \psi')) \circ (\mu, \psi) = (a + \mu', \psi') \circ (\mu, \psi) = (\mu_0', \psi' \circ \psi)$$

where by the composition law in $\mathscr{P}_{\mathrm{C}}$,

$$\mu_0'(b) = \mu(b) + (a + \mu')(\psi(b)) + \kappa^{\psi'}(\psi(b))$$

Thus $\mu_0' = \mu_0 + a \circ \psi$, which completes the proof. ∎

Theorem 3.4.4 (Soundness) *If* $\Delta \vdash^{\mathscr{C}} a_1 \equiv a_2 : \alpha$ *then* $[\![a_1]\!]^{\mathscr{C}} = [\![a_2]\!]^{\mathscr{C}}$*.*

Proof It suffices to prove: (i) $[\![a_i\{\delta_i(x_1)/x_1, \cdots, \delta_i(x_n)/x_n\}]\!]^{\mathscr{C}} = [\![a_i]\!]^{\mathscr{C}}([\![\delta_i(x_1)]\!]^{\mathscr{C}} \otimes \cdots \otimes [\![\delta_i(x_n)]\!]^{\mathscr{C}})$ where $\Delta = x_1 : \beta_1, \cdots, x_n : \beta_n$; (ii) if $\cdot \vdash^{\mathscr{C}} e_1 : \alpha$ and $e_1 \to e_2$ then $[\![e_1]\!]^{\mathscr{C}} = [\![e_2]\!]^{\mathscr{C}}$; and (iii) if $(v_1, v_2) \in \mathcal{V}_\alpha$ then $[\![v_1]\!]^{\mathscr{C}} = [\![v_2]\!]^{\mathscr{C}}$. Indeed, then let $(\delta_1, \delta_2) \in \mathcal{V}_\Delta$, and suppose that $\delta_1(a_1) \downarrow v_1$ and $\delta_2(a_2) \downarrow v_2$ with $(v_1, v_2) \in \Delta_\alpha$. Then by (ii) and (iii), it follows that $[\![\delta_1(a_1)]\!]^{\mathscr{C}} = [\![\delta_2(a_2)]\!]^{\mathscr{C}}$. Then $[\![\delta_i(a_i)]\!]^{\mathscr{C}} = [\![a_i\{\delta_i(x_1)/x_1, \cdots, \delta_i(x_n)/x_n\}]\!]^{\mathscr{C}}$. Since (i) applies to all value context mappings, it follows that the maps $[\![a_1]\!]^{\mathscr{C}}$ and $[\![a_2]\!]^{\mathscr{C}}$ agree on elements of the form $t_1 \otimes \cdots \otimes t_n \in [\![\Delta]\!]^{\mathscr{C}}$, so by linearity, we have $[\![a_1]\!]^{\mathscr{C}} = [\![a_2]\!]^{\mathscr{C}}$.

(i) It suffices to show that if $x : \alpha \vdash^{\mathscr{C}} a : \alpha'$ and $\cdot \vdash^{\mathscr{C}} v : \alpha$, then $[\![a\{v/x\}]\!]^{\mathscr{C}} = [\![a]\!]^{\mathscr{C}} \circ [\![v]\!]^{\mathscr{C}}$. This is done by induction over open expressions.

Case ($e = x$) Then $[\![a\{v/x\}]\!]^{\mathscr{C}} = [\![v]\!]^{\mathscr{C}}$ and $[\![a]\!]^{\mathscr{C}} = \mathsf{id}$, so $[\![a]\!]^{\mathscr{C}} \circ [\![v]\!]^{\mathscr{C}} = [\![v]\!]^{\mathscr{C}}$.

Case ($a = \texttt{let}\ y = a_1\ \texttt{in}\ a_2$) According to the typing rule for let statements, x must be in the domain of a_1. Thus, by the categorical semantics of let statements and by induction hypothesis, we have:

$$\begin{aligned}
[\![a\{v/x\}]\!]^{\mathscr{C}} &= [\![\texttt{let}\ y = a_1\{v/x\}\ \texttt{in}\ a_2]\!]^{\mathscr{C}} \\
&= [\![a_2]\!]^{\mathscr{C}} \circ [\![a_1\{v/x\}]\!]^{\mathscr{C}} \\
&= [\![a_2]\!]^{\mathscr{C}} \circ [\![a_1]\!]^{\mathscr{C}} \circ [\![v]\!]^{\mathscr{C}} \\
&= [\![\texttt{let}\ y = a_1\ \texttt{in}\ a_2]\!]^{\mathscr{C}} \circ [\![v]\!]^{\mathscr{C}}
\end{aligned}$$

Case ($e = \texttt{case}\ e'\ \texttt{of}\ \ \{\iota_1(x_1) \to e_1 \mid \iota_2(x_2) \to e_2\}$)

$$\begin{aligned}
[\![a\{v/x\}]\!]^{\mathscr{C}} &= [\![\texttt{case}\ a'\{v/x\}\ \texttt{of}\ \ \{\iota_1(x_1) \to a_1 \mid \iota_2(x_2) \to a_2\}\}]\!]^{\mathscr{C}} \\
&= (s \otimes s') \mapsto \big([\![a_1]\!]^{\mathscr{C}}(s' \oplus c_1) + [\![a_2]\!]^{\mathscr{C}}(s' \oplus c_2)\big) \\
&= (s'' \otimes s') \mapsto \big([\![a_1]\!]^{\mathscr{C}}(s' \oplus c_1') + [\![a_2]\!]^{\mathscr{C}}(s' \oplus c_2')\big)\, [\![a]\!]^{\mathscr{C}}\, [\![v]\!]^{\mathscr{C}} \\
&= [\![a]\!]^{\mathscr{C}} \circ [\![v]\!]^{\mathscr{C}}
\end{aligned}$$

where

$$[\![a']\!]^{\mathscr{C}} \circ [\![v]\!]^{\mathscr{C}} = [\![a'\{v/x\}]\!]^{\mathscr{C}}(s) = c_1 \oplus c_2 \qquad \text{and} \qquad [\![a']\!]^{\mathscr{C}}(s'') = c_1' \oplus c_2'$$

The other cases are similar.

(ii) It suffices to show the result for just the β-reduction rules.

Case ($\texttt{let}\ x = v\ \texttt{in}\ a' \to_\beta a'\{v/x\}$) Unfolding definitions, we have that

$$[\![\texttt{let}\ x = v\ \texttt{in}\ a']\!]^{\mathscr{C}}(1) = [\![a']\!]^{\mathscr{C}}(1 \otimes [\![v]\!]^{\mathscr{C}}(1)) = [\![a'\{v/x\}]\!]^{\mathscr{C}}(1)$$

Case ($\mathbf{0}_{\texttt{Unit}} \to_\beta 0$) Follows by unfolding definitions—both produce the zero map.

Case ($\mathbf{0}_{\alpha_1 \oplus \alpha_2} \to_\beta [\mathbf{0}_{\alpha_1}, \mathbf{0}_{\alpha_2}]$) It suffices to see that $[\![[\mathbf{0}_{\alpha_1}, \mathbf{0}_{\alpha_2}]]\!]^{\mathscr{C}}$ is the zero map on all inputs.

Case ($\mathbf{0}_{\alpha \multimap \alpha'} \to_\beta \lambda x.\mathbf{0}_{\alpha'}$) Similarly, it suffices to see that $[\![\lambda x.\mathbf{0}]\!]^{\mathscr{C}}(1)$ is the zero map.

Case ($r_1 \cdot r_2 \to_\beta r' = r_1 r_2 \in \texttt{Unit}$) Trivial.

Case $(r \cdot [v_1, v_2] \to_\beta [r \cdot v_1, r \cdot v_2])$

$$\begin{aligned}\llbracket r \cdot [v_1, v_2] \rrbracket^{\mathscr{C}}(1) &= r \cdot \big(\llbracket v_1 \rrbracket^{\mathscr{C}}(1) \oplus \llbracket v_2 \rrbracket^{\mathscr{C}}(1)\big) \\ &= \big(r \cdot \llbracket v_1 \rrbracket^{\mathscr{C}}(1)\big) \oplus \big(r \cdot \llbracket v_2 \rrbracket^{\mathscr{C}}(1)\big) \\ &= \llbracket [r \cdot v_1, r \cdot v_2] \rrbracket^{\mathscr{C}}(1)\end{aligned}$$

Case $(r \cdot \lambda x.a \to_\beta \lambda x.r \cdot a)$

$$\begin{aligned}\llbracket r \cdot \lambda x.a \rrbracket^{\mathscr{C}}(1) &= r \, \llbracket \lambda x.a \rrbracket^{\mathscr{C}}(1) \\ &= r \, \llbracket a \rrbracket^{\mathscr{C}} = \llbracket \lambda x.r \cdot a \rrbracket^{\mathscr{C}}(1)\end{aligned}$$

Case $(r_1 + r_2 \to_\beta r' = r_1 + r_2 \in \mathbb{Z}/d\mathbb{Z})$ Trivial.

Case $([v_1, v_2] + [v_1', v_2'] \to_\beta [v_1 + v_1', v_2 + v_2'])$

$$\begin{aligned}\llbracket [v_1, v_2] + [v_1', v_2'] \rrbracket^{\mathscr{C}}(1) &= \llbracket [v_1, v_2] \rrbracket^{\mathscr{C}}(1) + \llbracket [v_1', v_2'] \rrbracket^{\mathscr{C}}(1) \\ &= \big(\llbracket v_1 \rrbracket^{\mathscr{C}}(1) \oplus \llbracket v_2 \rrbracket^{\mathscr{C}}(1)\big) + \big(\llbracket v_1' \rrbracket^{\mathscr{C}}(1) \oplus \llbracket v_2' \rrbracket^{\mathscr{C}}(1)\big) \\ &= \big(\llbracket v_1 \rrbracket^{\mathscr{C}}(1) + \llbracket v_1' \rrbracket^{\mathscr{C}}(1)\big) \oplus \big(\llbracket v_2 \rrbracket^{\mathscr{C}}(1) + \llbracket v_2' \rrbracket^{\mathscr{C}}(1)\big) \\ &= \big(\llbracket v_1 + v_1' \rrbracket^{\mathscr{C}}(1)\big) \oplus \big(\llbracket v_2 + v_2' \rrbracket^{\mathscr{C}}(1)\big) \\ &= \llbracket [v_1 + v_1', v_2 + v_2'] \rrbracket^{\mathscr{C}}(1)\end{aligned}$$

Case $((\lambda x.a_1) + (\lambda x.a_2) \to_\beta \lambda x.a_1 + a_2)$

$$\begin{aligned}\llbracket (\lambda x.a_1) + (\lambda x.a_2) \rrbracket^{\mathscr{C}}(1) &= \big(b \mapsto \llbracket a_1 \rrbracket^{\mathscr{C}}(b)\big) + \big(b \mapsto \llbracket a_2 \rrbracket^{\mathscr{C}}(b)\big) \\ &= b \mapsto \llbracket a_1 \rrbracket^{\mathscr{C}}(b) + \llbracket a_2 \rrbracket^{\mathscr{C}}(b) \\ &= \llbracket a_1 + a_2 \rrbracket^{\mathscr{C}}(1)\end{aligned}$$

by linearity.

Case $(\texttt{case } [v_1, v_2] \texttt{ of } \{\iota_1(x_1) \to a_1 \mid \iota_2(x_2) \to a_2\} \to_\beta a_1\{v_1/x_1\} + a_2\{v_2/x_2\})$ From,

$$\llbracket \texttt{case } [v_1, v_2] \texttt{ of } \{\iota_1(x_1) \to a_1 \mid \iota_2(x_2) \to a_2\} \rrbracket^{\mathscr{C}}(1) = \llbracket a_1 \rrbracket^{\mathscr{C}}(c_1) + \llbracket a_2 \rrbracket^{\mathscr{C}}(c_2) \tag{3.4}$$

where $\llbracket [v_1, v_2] \rrbracket^{\mathscr{C}}(1) = \llbracket v_1 \rrbracket^{\mathscr{C}}(1) \oplus \llbracket v_2 \rrbracket^{\mathscr{C}}(1) = c_1 \oplus c_2$. Then

$$\llbracket a_i \rrbracket^{\mathscr{C}}(c_i) = \llbracket a_i \rrbracket^{\mathscr{C}}(\llbracket v_i \rrbracket^{\mathscr{C}}(1)) = \llbracket a_i\{v_i/x_i\} \rrbracket^{\mathscr{C}}(1)$$

Thus, Eq. (3.4) is equal to

$$\llbracket a_1\{v_1/x_1\} \rrbracket^{\mathscr{C}}(1) + \llbracket a_2\{v_2/x_2\} \rrbracket^{\mathscr{C}}(1) = \llbracket a_1\{v_1/x_1\} + a_2\{v_2/x_2\} \rrbracket^{\mathscr{C}}(1)$$

as expected.

Case $((\lambda x.a)v \to_\beta a\{v/x\})$

$$\begin{aligned}\llbracket(\lambda x.a)v\rrbracket^{\mathscr{C}}(1) &= \llbracket a\rrbracket^{\mathscr{C}}(\llbracket v\rrbracket^{\mathscr{C}}(1)) \\ &= \llbracket a\{v/x\}\rrbracket^{\mathscr{C}}(1)\end{aligned}$$

(iii) We proceed by induction on α. If $\alpha = \texttt{Unit}$ or $\alpha = \alpha_1 \oplus \alpha_2$, the result follows immediately from the definitions. The nontrivial case is where $\alpha = \alpha_1 \multimap \alpha_2$. Then $v_i = \lambda x.a_i$ such that, for all $(v_1', v_2') \in \mathcal{V}_{\alpha_1}$, we have $(a_1\{v_1'/x\}, a_2\{v_2'/x\}) \in \mathcal{V}_{\alpha_2}$. Then there exists $(v_1'', v_2'') \in \mathcal{V}_{\alpha_2}$ such that $a_i\{v_i'/x\} \to^* v_i''$. By the induction hypothesis, $\llbracket v_1''\rrbracket^{\mathscr{C}} = \llbracket v_2''\rrbracket^{\mathscr{C}}$, and so by (ii), we have:

$$\llbracket a_1\{v_1'/x\}\rrbracket^{\mathscr{C}} = \llbracket v_1''\rrbracket^{\mathscr{C}} = \llbracket v_2''\rrbracket^{\mathscr{C}} = \llbracket a_2\{v_2'/x\}\rrbracket^{\mathscr{C}}.$$

To show $\llbracket \lambda x.a_1\rrbracket^{\mathscr{C}} = \llbracket \lambda x.a_2\rrbracket^{\mathscr{C}}$, it suffices to show that for all basis elements b of $\llbracket \alpha_1\rrbracket^{\mathscr{C}}$, we have $\llbracket a_1\rrbracket^{\mathscr{C}}(b) = \llbracket a_2\rrbracket^{\mathscr{C}}(b)$. This follows from (i) and the fact that $(\lceil b\rceil, \lceil b\rceil) \in \mathcal{V}_{\alpha_1}$:

$$\llbracket a_1\rrbracket^{\mathscr{C}}(b) = \llbracket a_1\{\lceil b\rceil/x\}\rrbracket^{\mathscr{C}} = \llbracket a_2\{\lceil b\rceil/x\}\rrbracket^{\mathscr{C}} = \llbracket a_2\rrbracket^{\mathscr{C}}(b).$$

where $\lceil b\rceil$ is a valuation δ such that $\llbracket \delta\rrbracket^{\mathscr{C}}(1) = b$. ■

3.5 Typing rules and categorical semantics for $\lambda^{\mathscr{P}_{\mathrm{C}}}$

Among the $\mathscr{C}$-types, we also have $\mathscr{S}$*-types* or *symplectic types*, are defined as follows:

$$\sigma ::= \mathtt{Unit} \oplus \mathtt{Unit} \mid \sigma_1 \oplus \sigma_2 \qquad\qquad \sigma_1, \sigma_2 \in \mathsf{types}(\mathscr{S})$$

Lemma 3.5.1 *Each* $\mathscr{S}$*-type has a canonical symplectic form:*

$$\cdot \vdash^{\mathscr{C}} \omega_\sigma : \sigma \multimap \sigma \multimap \boldsymbol{Unit}$$

satisfying:

$$\cdot \vdash^{\mathscr{C}} \omega_{\boldsymbol{Unit} \oplus \boldsymbol{Unit}}[r_x, r_z][r'_x, r'_z] \equiv r'_x r_z - r_x r'_z : \boldsymbol{Unit}$$
$$\cdot \vdash^{\mathscr{C}} \omega_{\sigma_1 \oplus \sigma_2}[v_1, v_2][v'_1, v'_2] \equiv \omega_{\sigma_1} v_1 v'_1 - \omega_{\sigma_2} v_2 v'_2 : \boldsymbol{Unit}$$

Proof We define ω by induction on σ as follows:

$$\omega_{\mathtt{Unit}\oplus\mathtt{Unit}} = \lambda x.\ \lambda x'.\ \mathtt{case}\ x\ \mathtt{of} \begin{Bmatrix} \iota_1(x_x) \to \mathtt{case}\ x'\ \mathtt{of} \begin{Bmatrix} \iota_1(x'_x) \to \mathbf{0} \\ \iota_2(x'_z) \to -x_x x'_z \end{Bmatrix} \\ \iota_2(x_z) \to \mathtt{case}\ x'\ \mathtt{of} \begin{Bmatrix} \iota_1(x'_x) \to x_z x'_x \\ \iota_2(x'_z) \to \mathbf{0} \end{Bmatrix} \end{Bmatrix}$$

$$\omega_{\sigma_1\oplus\sigma_2} = \lambda x.\ \lambda x'.\ \mathtt{case}\ x\ \mathtt{of} \begin{Bmatrix} \iota_1(x_1) \to \mathtt{case}\ x'\ \mathtt{of} \begin{Bmatrix} \iota_1(x'_1) \to \omega_{\sigma_1} x_1 x'_1 \\ \iota_2(x'_2) \to \mathbf{0} \end{Bmatrix} \\ \iota_2(x_2) \to \mathtt{case}\ x'\ \mathtt{of} \begin{Bmatrix} \iota_1(x'_1) \to \mathbf{0} \\ \iota_2(x'_2) \to \omega_{\sigma_2} x_2 x'_2 \end{Bmatrix} \end{Bmatrix}$$

■

Next, $\mathscr{P}_{\mathrm{C}}$-types are defined by:

$$W ::= \mathtt{Pauli} \mid W \bullet W$$

Each $\mathscr{P}_{\mathrm{C}}$-type corresponds to a symplectic type:

$$\overline{\mathtt{Pauli}} = \mathtt{Unit} \oplus \mathtt{Unit} \qquad\qquad \overline{W \bullet W} = \overline{W} \oplus \overline{W}$$

The $\mathscr{P}_{\mathrm{C}}$-expressions are given by:

$$
\begin{aligned}
e ::= &\ x \mid \texttt{let}\ x = e\ \texttt{in}\ e' \\
&\mid a \mid \langle a \rangle e \mid e_1 \star e_2 \mid \texttt{pow}(e, r) \\
&\mid \texttt{case}\ e\ \texttt{of}\ \{\texttt{X} \to e_x \mid \texttt{Z} \to e_z\} \\
&\mid \iota_1(e) \mid \iota_2(e) \mid \texttt{case}\ e\ \texttt{of}\ \{\iota_1(x_1) \to e_1 \mid \iota_2(x_2) \to e_2\}
\end{aligned}
$$

Closed $\mathscr{P}_{\mathrm{C}}$-expressions normalize to values of the form $\cdot \vdash^{\mathscr{P}_{\mathrm{C}}} \langle r \rangle v : W$, corresponding to elements of the subset $\mathbf{Q}_{[\![\overline{W}]\!]^{\mathscr{C}}} \subseteq \mathbf{P}_{[\![\overline{W}]\!]^{\mathscr{C}}}$ of the Pauli group discussed in Sec. 2.3 and Sec. 3.2:

$$\zeta^{[\![r]\!]^{\mathscr{C}}(1)} \Delta_{\underline{[\![v]\!]^{\mathscr{C}}(1)}} \in \mathbf{Q}_{[\![W]\!]^{\mathscr{C}}}$$

The reason for the (1) in $[\![r]\!]^{\mathscr{C}}(1)$ and $[\![v]\!]^{\mathscr{C}}(1)$ is that $[\![r]\!]^{\mathscr{C}}$ and $[\![v]\!]^{\mathscr{C}}$ are technically global elements. Every $\mathscr{C}$-expression is also a $\mathscr{P}_{\mathrm{C}}$-expression with phase $\langle 0 \rangle$, and the $\star$ syntax implements the condensed product from Sec. 2.3. Since $\lambda^{\mathscr{P}_{\mathrm{C}}}$ lets us express elements of the Pauli loop $(\mathbf{Q}_W, \star)$, expressions in $\lambda^{\mathscr{P}_{\mathrm{C}}}$ are not limited to projective Clifford operations $\mathbf{Q}_W \to \mathbf{Q}_{W'}$. This is the motivation for including the other morphisms in the category $\mathscr{P}_{\mathrm{C}}$ in Sec. 3.2. Again the language itself is very similar to its categorical semantics:

$$[\![W]\!]^{\mathscr{P}_{\mathrm{C}}} = \mathbf{Q}_{[\![\overline{W}]\!]^{\mathscr{C}}} \qquad [\![\cdot]\!]^{\mathscr{P}_{\mathrm{C}}} = \bullet \qquad [\![x : W]\!]^{\mathscr{P}_{\mathrm{C}}} = [\![W]\!]^{\mathscr{P}_{\mathrm{C}}}$$

Currently, $\lambda^{\mathscr{P}_{\mathrm{C}}}$ only supports at most one variable, meaning we consider *Pauli contexts* of the form $\Theta = \cdot$ or $\Theta = x : Q$ only, with $[\![\cdot]\!]^{\mathscr{P}_{\mathrm{C}}} = \bullet$ and $[\![e : W]\!]^{\mathscr{P}_{\mathrm{C}}} = \mathbf{Q}_W$. Recall that concatenation of linear typing contexts corresponds to $\otimes$ in the categorical semantics. It is harder to imagine what the concatenation of Pauli contexts should correspond to in $\mathscr{P}_{\mathrm{C}}$. Larger contexts would be required in order to define quantum operations higher in the Clifford hierarchy, though we do not now how to encode the algebraic condition in terms of the condensed encodings, which would arise in the typing rule for such operations.

A judgment $x : W \vdash^{\mathscr{P}_{\mathrm{C}}} e : W'$ with a free variable is interpreted as a morphism $[\![e]\!]^{\mathscr{P}_{\mathrm{C}}} = (\mu, \psi)$ in $\mathscr{P}_{\mathrm{C}}$, as we detail after giving the typing rules below. We first define a $\mathscr{C}$-expression

e^ψ satisfying $x : \overline{W} \vdash^{\mathscr{C}} e^\psi : \overline{W'}$:

$$\begin{aligned}
x^\psi &= x \\
(\texttt{let}\ x = e\ \texttt{in}\ e')^\psi &= \texttt{let}\ x = e^\psi\ \texttt{in}\ (e')^\psi \\
a^\psi &= a \\
(\langle a \rangle e)^\psi &= e^\psi \\
(e_1 \star e_2)^\psi &= {e_1}^\psi + {e_2}^\psi \\
(\texttt{pow}(e,r))^\psi &= r \cdot e^\psi \\
(\texttt{case}\ e\ \texttt{of}\ \{\texttt{X} \to e_x \mid \texttt{Z} \to e_z\})^\psi &= \texttt{case}\ e^\psi\ \texttt{of}\ \{\iota_1(x_1) \to x_1 \cdot {e_x}^\psi \mid \iota_2(x_2) \to x_2 \cdot {e_z}^\psi\} \\
(\iota_i e)^\psi &= \iota_i e^\psi \\
(\texttt{case}\ e\ \texttt{of}\ \{\iota_1(x_1) \to e_1 \mid \iota_2(x_2) \to e_2\})^\psi &= \texttt{case}\ e^\psi\ \texttt{of}\ \{\iota_1(x_1) \to {e_1}^\psi \mid \iota_2(x_2) \to {e_2}^\psi\}
\end{aligned}$$

To simplify the notation in the typing rules, we write $\omega_W(e_1, e_2)$ in place of $\omega_{\overline{W}} {e_1}^\psi {e_2}^\psi$, and since the equivalences that arise are always of type `Unit`, and declare:

$$\frac{\Theta \vdash^{\mathscr{P}_c} e_1 : W \qquad \Theta \vdash^{\mathscr{P}_c} e_2 : W \qquad \overline{\Theta} \vdash^{\mathscr{C}} a : \texttt{Unit} \qquad \overline{\Theta} \vdash^{\mathscr{C}} \omega_{\overline{W}} {e_1}^\psi {e_2}^\psi \equiv a : \texttt{Unit}}{\Theta \vdash^{\mathscr{P}_c} \omega_W(e_1, e_2) \equiv a}$$

Finally, the typing rules for $\lambda^{\mathscr{P}_c}$ are:

$$\frac{\Theta = x : W}{\Theta \vdash^{\mathscr{P}_c} x : W} \qquad \frac{\Theta \vdash^{\mathscr{P}_c} e : W \qquad x : W \vdash^{\mathscr{P}_c} e' : W'}{\Theta \vdash^{\mathscr{P}_c} \texttt{let}\ x = e\ \texttt{in}\ e' : W'}$$

$$\frac{\cdot \vdash^{\mathscr{C}} a : \overline{W}}{\cdot \vdash^{\mathscr{P}_c} a : W} \qquad \frac{\overline{\Theta} \vdash^{\mathscr{C}} a : \texttt{Unit} \qquad \Theta \vdash^{\mathscr{P}_c} e : W}{\Theta \vdash^{\mathscr{P}_c} \langle a \rangle e : W}$$

$$\frac{\cdot \vdash^{\mathscr{P}_c} e_1 : W \qquad \cdot \vdash^{\mathscr{P}_c} e_2 : W}{\cdot \vdash^{\mathscr{P}_c} e_1 \star e_2 : W} \qquad \frac{\cdot \vdash^{\mathscr{P}_c} e : W \qquad r \in \texttt{Unit}}{\cdot \vdash^{\mathscr{P}_c} \texttt{pow}(e, r) : W}$$

$$\frac{\Theta \vdash^{\mathscr{P}_c} e : \texttt{Pauli} \qquad \cdot \vdash^{\mathscr{P}_c} e_x : W \qquad \cdot \vdash^{\mathscr{P}_c} e_z : W \qquad \cdot \vdash^{\mathscr{P}_c} \omega_W(e_z, e_x) \equiv 1}{\Theta \vdash^{\mathscr{P}_c} \texttt{case}\ e\ \texttt{of}\ \{\texttt{X} \to e_x \mid \texttt{Z} \to e_z\} : W}$$

$$\frac{\Theta \vdash^{\mathscr{P}_c} e : W_1}{\Theta \vdash^{\mathscr{P}_c} \iota_1(e) : W_1 \bullet W_2} \qquad \frac{\Theta \vdash^{\mathscr{P}_c} e : W_2}{\Theta \vdash^{\mathscr{P}_c} \iota_2(e) : W_1 \bullet W_2}$$

$$\frac{\Theta \vdash^{\mathscr{P}_c} e : W_1 \bullet W_2 \qquad x_i : W_i \vdash^{\mathscr{P}_c} e_i : W' \qquad x_1 : W_1, x_2 : W_2 \vdash^{\mathscr{P}_c} \omega_{W'}(e_1, e_2) \equiv \mathbf{0}}{\Theta \vdash^{\mathscr{P}_c} \texttt{case}\ e\ \texttt{of}\ \{\iota_1(x_1) \to e_1 \mid \iota_2(x_2) \to e_2\} : W'}$$

Notice that there is no λ introduction rule for Pauli types. This will be treated by the non-linear typing judgment. Pauli typing judgments are interpreted as follows (again using the shorthand $[\![e]\!]^{\mathscr{P}_c} = [\![\Theta \vdash^{\mathscr{P}_c} e : W]\!]^{\mathscr{P}_c}$):

$$\begin{aligned}
[\![x]\!]^{\mathscr{P}_c} &= (\mathbf{0}, \mathsf{id}_W) \\
[\![\mathtt{let}\ x = e\ \mathtt{in}\ e']\!]^{\mathscr{P}_c} &= [\![e']\!]^{\mathscr{P}_c} \circ [\![e]\!]^{\mathscr{P}_c} \\
[\![a]\!]^{\mathscr{P}_c} &= (\mathbf{0}, [\![a]\!]^{\mathscr{C}}) \\
[\![\langle a \rangle e]\!]^{\mathscr{P}_c} &= \langle [\![a]\!]^{\mathscr{C}} \rangle\, [\![e]\!]^{\mathscr{P}_c} \\
[\![e_1 \star e_2]\!]^{\mathscr{P}_c} &= [\![e_1]\!]^{\mathscr{P}_c} \star [\![e_2]\!]^{\mathscr{P}_c} \\
[\![\mathtt{pow}(e, r)]\!]^{\mathscr{P}_c} &= [\![e]\!]^{\mathscr{P}_c} \circ [\![r]\!]^{\mathscr{C}} \\
[\![\mathtt{case}\ e\ \mathtt{of}\ \{\mathtt{X} \to e_x \mid \mathtt{Z} \to e_z\}]\!]^{\mathscr{P}_c} &= \left([\![e_x]\!]^{\mathscr{P}_c} \boxplus [\![e_z]\!]^{\mathscr{P}_c}\right) \circ [\![e]\!]^{\mathscr{P}_c} \\
[\![\iota_i(e)]\!]^{\mathscr{P}_c} &= (\mathbf{0}, \iota_i) \circ [\![e]\!]^{\mathscr{P}_c} \\
[\![\mathtt{case}\ e\ \mathtt{of}\ \{\iota_1(x_1) \to e_1 \mid \iota_2(x_2) \to e_2\}]\!]^{\mathscr{P}_c} &= \left([\![e_1]\!]^{\mathscr{P}_c} \boxplus [\![e_2]\!]^{\mathscr{P}_c}\right) \circ [\![e]\!]^{\mathscr{P}_c}
\end{aligned}$$

where if $f_i : \alpha_i \to \alpha'$ is a morphism in $\mathscr{C}$ then $f_1 \boxplus f_2 : \alpha_1 \oplus \alpha_2 \to \alpha'$ is the map obtained from coproduct universality, $(f_1 \boxplus f_2)(e_1 \oplus e_2) = f_1 e_1 + f_2 e_2$.[2]

Then, soundness of $\lambda^{\mathscr{C}}$ is used to prove:

Theorem 3.5.2 *If $x : W \vdash^{\mathscr{P}_c} e : W'$ then $[\![e^{\psi}]\!]^{\mathscr{C}} \in \mathsf{hom}_{\mathscr{S}}(\overline{W}, \overline{W'})$.*

This theorem establishes that $\lambda^{\mathscr{P}_C}$ has the property we set out for: the non-phase part of an expression with free $\mathscr{P}_C$-variable is interpreted as a linear map that respects the symplectic forms. Invalid (non-Clifford) expressions will not typecheck. Soon we will define a closely-related nonlinear type $\lceil W \multimap W' \rceil$, the lifted type of projective Clifford operations. Furthermore, since (one may show that) $[\![e^{\psi}]\!]^{\mathscr{C}} = \psi$ where $[\![e]\!]^{\mathscr{P}_c} = (\mu, \psi)$, we verify that the categorical semantics $[\![-]\!]^{\mathscr{P}_c}$ is well-defined.

Proof It is clear that $[\![e^{\psi}]\!]^{\mathscr{C}} \in \mathsf{hom}_{\mathscr{C}}(\overline{W}, \overline{W'})$. Using properties of the equivalence relation, we prove below by induction on expressions $x : W \vdash^{\mathscr{P}_c} e : W'$ that for all values $\cdot \vdash^{\mathscr{C}} v_1 : \overline{W}$

[2] In other places in the thesis, we denote $f_1 \boxplus f_2$ by $[f_1, f_2]$, but we avoid that notation here, since it clashes with the ordered pair syntax in the language.

and $\cdot \vdash^{\mathscr{C}} v_2 : \overline{W}$ it follows that $\cdot \vdash^{\mathscr{C}} \omega_{\overline{W'}}(e^{\psi}\{v_1/x\}, e^{\psi}\{v_2/x\}) \equiv \omega_{\overline{W}}(v_1, v_2)$. Then by soundness for $\lambda^{\mathscr{C}}$, it follows that $[\![e^{\psi}]\!]^{\mathscr{C}}$ respects the symplectic forms.

Case ($e = x$) Trivial.

Case ($e = \mathtt{let}\ y = e'\ \mathtt{in}\ e''$) By Thm. 3.4.1, there exist values v_i' such that $(e')^{\psi}\{v_i/x\} \downarrow v_i'$. Then we get a string of equivalences:

$$\begin{aligned}
&\omega\left(\mathtt{let}\ y = (e')^{\psi}\{v_i/x\}\ \mathtt{in}\ (e'')^{\psi}, \mathtt{let}\ y = (e')^{\psi}\{v_i/x\}\ \mathtt{in}\ (e'')^{\psi}\right) \\
\equiv&\,\omega\left(\mathtt{let}\ y = v_1'\ \mathtt{in}\ (e'')^{\psi}, \mathtt{let}\ y = v_2'\ \mathtt{in}\ (e'')^{\psi}\right) \\
\equiv&\,\omega\left((e'')^{\psi}\{v_1'/y\}, (e'')^{\psi}\{v_2'/y\}\right) \\
\equiv&\,\omega\left(v_1', v_2'\right) \\
\equiv&\,\omega\left((e')^{\psi}\{v_1/x\}, (e')^{\psi}\{v_2/x\}\right) \\
\equiv&\,\omega\left(v_1, v_2\right)
\end{aligned}$$

by the induction hypothesis for e' and e''.

Case ($e = \langle a \rangle e'$) Since $(\langle a \rangle e')^{\psi} = (e')^{\psi}$, the result follows directly from the induction hypothesis.

Case ($e = \iota_i(e')$) Because $\omega_{\sigma_1 \oplus \sigma_2}\left(\iota_i(e_1), \iota_i(e_2)\right) \equiv \omega_{\sigma_i}\left(e_1, e_2\right)$, we can see that

$$\omega\left(\iota_i((e')^{\psi}\{v_1/x\}), \iota_i((e')^{\psi}\{v_2/x\})\right) \equiv \omega\left((e')^{\psi}\{v_1/x\}, (e')^{\psi}\{v_2/x\}\right) \equiv \omega\left(v_1, v_2\right)$$

by the induction hypothesis.

Case ($e = \mathtt{case}\ e'\ \mathtt{of}\ \{\mathtt{X} \to e_x \mid \mathtt{Z} \to e_z\}$)

Let $(e')^{\psi}\{v_i/x\} \downarrow [r_i^x, r_i^z]$. Then

$$\begin{aligned}
&\omega\left(e^{\psi}\{v_1/x\}, e^{\psi}\{v_2/x\}\right) \\
&\equiv \omega\left(\mathtt{case}\ (e')^{\psi}\{v_1/x\}\ \mathtt{of}\ \left\{\mathtt{X} \to {e_x}^{\psi} \mid \mathtt{Z} \to {e_z}^{\psi}\right\}, \mathtt{case}\ (e')^{\psi}\{v_2/x\}\ \mathtt{of}\ \left\{\mathtt{X} \to {e_x}^{\psi} \mid \mathtt{Z} \to {e_z}^{\psi}\right\}\right) \\
&\equiv \omega\left(\mathtt{case}\ [r_1^x, r_1^z]\ \mathtt{of}\ \left\{\mathtt{X} \to {e_x}^{\psi} \mid \mathtt{Z} \to {e_z}^{\psi}\right\}, \mathtt{case}\ [r_2^x, r_2^z]\ \mathtt{of}\ \left\{\mathtt{X} \to {e_x}^{\psi} \mid \mathtt{Z} \to {e_z}^{\psi}\right\}\right) \\
&\equiv \omega\left(r_1^x \cdot {e_x}^{\psi} + r_1^z \cdot {e_z}^{\psi}, r_2^x \cdot {e_x}^{\psi} + r_2^z \cdot {e_z}^{\psi}\right)
\end{aligned}$$

By bilinearity, this value is equivalent to:

$$\begin{aligned}
&r_1^x r_2^x \omega\left({e_x}^{\psi}, {e_x}^{\psi}\right) + r_1^x r_2^z \omega\left({e_x}^{\psi}, {e_z}^{\psi}\right) + r_1^z r_2^x \omega\left({e_z}^{\psi}, {e_x}^{\psi}\right) + r_1^z r_2^z \omega\left({e_z}^{\psi}, {e_z}^{\psi}\right) \\
\equiv&\, r_1^z r_2^x - r_1^x r_2^z \\
\equiv&\, \omega\left([r_1^x, r_1^z], [r_2^x, r_2^z]\right)
\end{aligned}$$

Because we assumed $(e')^{\psi}\{v_i/x\} \downarrow [r_i^x, r_i^z]$, this is equivalent to

$$\omega\left((e')^{\psi}\{v_1/x\}, (e')^{\psi}\{v_2/x\}\right) \equiv \omega\left(v_1, v_2\right)$$

by the induction hypothesis for e', as expected.

Case ($e = \texttt{case}\ e'\ \texttt{of}\ \{\iota_1(x_1) \to e_1 \mid \iota_2(x_2) \to e_2\}$)

Let $(e')^{\psi}\{v_i/x\} \downarrow [v_{i,1}, v_{i,2}]$. Then

$$\begin{aligned}
\omega\left(e^{\psi}\{v_1/x\}, e^{\psi}\{v_2/x\}\right) &\equiv \omega\Big(\texttt{case}\ (e')^{\psi}\{v_1/x\}\ \texttt{of}\ \left\{\iota_1(x_1) \to {e_1}^{\psi} \mid \iota_2(x_2) \to {e_2}^{\psi}\right\}, \\
&\qquad \texttt{case}\ (e')^{\psi}\{v_2/x\}\ \texttt{of}\ \left\{\iota_1(x_1) \to {e_1}^{\psi} \mid \iota_2(x_2) \to {e_2}^{\psi}\right\}\Big) \\
&\equiv \omega\Big(\texttt{case}\ [v_{1,1}, v_{1,2}]\ \texttt{of}\ \left\{\iota_1(x_1) \to {e_1}^{\psi} \mid \iota_2(x_2) \to {e_2}^{\psi}\right\}, \\
&\qquad \texttt{case}\ [v_{2,1}, v_{2,2}]\ \texttt{of}\ \left\{\iota_1(x_1) \to {e_1}^{\psi} \mid \iota_2(x_2) \to {e_2}^{\psi}\right\}\Big) \\
&\equiv \omega\left({e_1}^{\psi}\{v_{1,1}/x_1\} + {e_2}^{\psi}\{v_{1,2}/x_2\}, {e_1}^{\psi}\{v_{2,1}/x_1\} + {e_2}^{\psi}\{v_{2,2}/x_2\}\right)
\end{aligned}$$

By the linearity, this is equivalent to

$$\begin{aligned}
&\omega\left({e_1}^{\psi}\{v_{1,1}/x_1\}, {e_1}^{\psi}\{v_{2,1}/x_1\}\right) + \omega\left({e_1}^{\psi}\{v_{1,1}/x_1\}, {e_2}^{\psi}\{v_{2,2}/x_2\}\right) \\
&+ \omega\left({e_2}^{\psi}\{v_{1,2}/x_2\}, {e_1}^{\psi}\{v_{2,1}/x_1\}\right) + \omega\left({e_2}^{\psi}\{v_{1,2}/x_2\}, {e_2}^{\psi}\{v_{2,2}/x_2\}\right)
\end{aligned} \tag{3.5}$$

By the induction hypothesis of e_j, $\omega\left({e_j}^{\psi}\{v_{1,j}/x_j\}, {e_j}^{\psi}\{v_{2,j}/x_j\}\right) \equiv \omega\left(v_{1,j}, v_{2,j}\right)$. Furthermore, from the typing judgment we know that

$$\omega\left({e_1}^{\psi}\{v_{i,1}/x_1\}, {e_2}^{\psi}\{v_{i,2}/x_2\}\right) \equiv 0 \equiv -\omega\left({e_2}^{\psi}\{v_{i,2}/x_2\}, {e_1}^{\psi}\{v_{i,1}/x_1\}\right).$$

Thus Eq. (3.5) is equivalent to

$$\begin{aligned}
\omega\left(v_{1,1}, v_{2,1}\right) + \omega\left(v_{1,2}, v_{2,2}\right) &\equiv \omega\left([v_{1,1}, v_{1,2}], [v_{2,1}, v_{2,2}]\right) \\
&\equiv \omega\left((e')^{\psi}\{v_1/x\}, (e')^{\psi}\{v_2/x\}\right)
\end{aligned}$$

By the induction hypothesis, this is equivalent to $\omega\left(v_1, v_2\right)$, as expected.

$\blacksquare$

3.6 Operational semantics for $\lambda^{\mathscr{P}_{\mathrm{C}}}$

As we did with $\lambda^{\mathscr{C}}$, we now define a step rule for closed $\lambda^{\mathscr{P}_{\mathrm{C}}}$-expressions by specifying β-reductions and allowing for reduction inside call-by-value contexts. The β-rules are:

$$\begin{aligned}
\texttt{let } x = \langle r\rangle v \texttt{ in } e' &\rightarrow_\beta \langle r\rangle e'\{v/x\} \\
\langle r'\rangle\,(\langle r\rangle v) &\rightarrow_\beta \langle r'+r\rangle v \\
(\langle r_1\rangle v_1) \star (\langle r_2\rangle v_2) &\rightarrow_\beta \langle r_1+r_2+k\rangle (v_1+v_2) \\
& \qquad k = s(v_1,v_2) + \epsilon(\underline{v_1}+\underline{v_2}) \\
\texttt{pow}(\langle r\rangle v, r') &\rightarrow_\beta \langle r'r+k\rangle (r'\cdot v) \\
& \qquad k = \widetilde{\mathsf{sgn}}(\underline{r'}\ \underline{v}) \\
\texttt{case } \langle r\rangle[r_x,r_z] \texttt{ of } \{\texttt{X} \rightarrow e_x \mid \texttt{Z} \rightarrow e_z\} &\rightarrow_\beta \langle r+k\rangle \texttt{pow}(e_z,r_z) \star \texttt{pow}(e_x,r_x) \\
& \qquad k = \widetilde{\mathsf{sgn}}(\underline{r_x}\ \underline{r_z}) \\
\iota_i\langle r\rangle v &\rightarrow_\beta \langle r\rangle \iota_i(v) \\
\texttt{case } \langle r\rangle[v_1,v_2] \texttt{ of } \{\iota_1(x_1) \rightarrow e_1 \mid \iota_2(x_2) \rightarrow e_2\} &\rightarrow_\beta \langle r\rangle e_1\{v_1/x_1\} \star e_2\{v_2/x_2\} \\
v &\rightarrow_\eta \langle 0\rangle v
\end{aligned}$$

By slight abuse of notation, we have written v in place of $[\![v]\!]^{\mathscr{C}}(1)$ as inputs to the functions s and ϵ, and similarly for the inputs to $\widetilde{\mathsf{sgn}}$. If d is odd, s, ϵ, and $\widetilde{\mathsf{sgn}}$ (hence the phase corrections k) are trivial. If d is even, these functions $s : V \times V \to \{0, \frac{d}{2}\}$, $\epsilon : V' \to \{0, \frac{d}{2}\}$, and $\widetilde{\mathsf{sgn}} : \mathbb{Z}/d'\mathbb{Z} \to \{0, \frac{d}{2}\}$ are given as follows:

$$\widetilde{\mathsf{sgn}}(t) = \begin{cases} 0 & : t \in \{0, \cdots, d-1\} \\ \frac{d}{2} & : t \in \{d, \cdots, 2d-1\} \end{cases} \qquad\qquad \epsilon(w) = \frac{\omega'(w,\overline{w})}{2}$$

where V is the codomain of the interpretation $[\![v]\!]^{\mathscr{C}}$ of the relevant value v, V' is the extended phase space, and ω' is the extended symplectic form, as defined in Sec. 2.3. Lastly,

$$s(v_1,v_2) = \frac{\omega'(\underline{v_1},\underline{v_2}) - \underline{\underline{\omega(v_1,v_2)}}}{2} = \widetilde{\mathsf{sgn}}(\omega'(\underline{v_1},\underline{v_2})))$$

As in the case of $\lambda^{\mathscr{C}}$, we have:

Theorem 3.6.1 $\lambda^{\mathscr{P}_{\mathrm{C}}}$ *satisfies type preservation, strong normalization, and soundness.*

The normal forms for $\lambda^{\mathscr{P}_\mathrm{C}}$ have the form $\langle r\rangle v$ for $\mathscr{C}$-values $\cdot \vdash^{\mathscr{C}} r : \mathtt{Unit}$ and $\cdot \vdash^{\mathscr{C}} v : \alpha$.

Example Consider the conjugation action of the single-qubit Hadamard gate $H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$. The projective H gate $[H]$ is projective Clifford, and is expressed as:

$$x : \mathtt{Pauli} \vdash^{\mathscr{P}_\mathrm{C}} \mathtt{case}\ x\ \mathtt{of}\ \{\mathtt{X} \to [0,1] \mid \mathtt{Z} \to [1,0]\} : \mathtt{Pauli} \tag{3.6}$$

This indicates that $HXH^\dagger = Z$ and $HZH^\dagger = X$. Expression Eq. (3.6) is well-typed because:

$$x : \mathtt{Unit} \oplus \mathtt{Unit} \vdash^{\mathscr{C}} \omega_{\mathtt{Unit}\oplus\mathtt{Unit}}[1,0][0,1] \equiv 1 : \mathtt{Unit}$$

since $-1 = 1$ in $\mathbb{Z}/2\mathbb{Z}$, from which it follows that:

$$x : \mathtt{Pauli} \vdash^{\mathscr{P}_\mathrm{C}} \omega_{\mathtt{Pauli}}([1,0],[0,1]) \equiv 1$$

as required for the formation of Eq. (3.6). Owing to the condensed encodings and condensed product, we may express the fact that $HYH^\dagger = -Y$ in $\lambda^{\mathscr{P}_\mathrm{C}}$. Since $Y = \Delta_{[1,1]}$, we express Y as $\langle 0\rangle[1,1]$, just as we express $X = \Delta_{[1,0]}$ by $\langle 0\rangle[1,0]$ and $Z = \Delta_{[0,1]}$ by $\langle 0\rangle[0,1]$. Recall also that $X \star Z = -Y$, which is expressed by $\langle 1\rangle[1,1]$. Then $HYH^\dagger$ is expressed as:

$$\begin{aligned}
\mathtt{case}\ \langle 0\rangle[1,1]\ \mathtt{of}\ \{\mathtt{X} \to [0,1] \mid \mathtt{Z} \to [1,0]\} &\to_\beta \langle \widetilde{\mathsf{sgn}}(1)\rangle \mathtt{pow}([1,0],1) \star \mathtt{pow}([0,1],1) \\
&= \mathtt{pow}([1,0],1) \star \mathtt{pow}([0,1],1) \\
&\to_\beta \langle k\rangle[1,1]
\end{aligned}$$

since $\widetilde{\mathsf{sgn}}(1) = 0$. The phase correction k is calculated as follows:

$$k = s([1,0],[0,1]) + \epsilon([1,1]) = 1 + 0 = 1$$

Therefore, the expression for $HXH^\dagger$ normalizes to $\langle 1\rangle[1,1]$, corresponding to $i^1X^1Z^1 = -Y$, as claimed. Notice how the annoying details about the phase correction are out of sight and mind of the programming language user.

3.7 Nonlinear types

Finally, we extend the $\mathscr{P}_\mathrm{C}$-type system to a linear-nonlinear (LNL) type system. This has two main benefits. For one, it allows for standard programming language features one expects to be available in any realistic programming language. These are needed, for example, to define auxiliary functions when coding up the error mitigation circuit for a stabilizer code. Secondly, allowing $\mathscr{P}_\mathrm{C}$-types to be *lifted* to nonlinear types is what we need to finally define *projective Clifford types*. We do not specify a categorical semantics for the full LNL system at this time, but we note that similar work has been done in this direction. The lowering and lifting operations become the left and right adjoints, respectively, in an adjunction between the linear and nonlinear semantic categories, and this idea has been incorporated into the QWIRE langauge [Pay18; PRZ17].

The non-linear types τ are given by:

$$\tau ::= \mathbf{Unit} \mid \tau_1 \times \tau_2 \mid \tau_1 + \tau_2 \mid \tau_1 \to \tau_2 \mid \lceil W \rceil \mid \lceil W_1 \multimap W_2 \rceil$$

The type $\lceil W \rceil$ is called a *lifted Pauli type* and $\lceil W_1 \multimap W_2 \rceil$ is called a *lifted projective Clifford type*. Note that $W_1 \multimap W_2$ is not a valid type of any kind. *Non-linear terms* t have the following syntax:

$$\begin{aligned} t ::= {} & () \mid t_1; t_2 \mid (t_1, t_2) \mid \pi_1 t \mid \pi_2 t \\ & \mid \iota_1(t) \mid \iota_2(t) \mid \texttt{case}\ t\ \texttt{of}\ \{\iota_1(x_1) \to t_1 \mid \iota_2(x_2) \to t_2\} \\ & \mid \lambda x.t \mid t_1 t_2 \mid \lceil e \rceil \mid \lceil \lambda x.e \rceil \end{aligned}$$

Nonlinear contexts have the form $\Gamma ::= \cdot \mid \Gamma, x : \tau$. The nonlinear typing judgment $\Gamma \vdash^{\mathtt{T}} t : \tau$ is given by the usual typing rules. We add new $\mathscr{P}_\mathrm{C}$-expressions:

$$e ::= \cdots \mid \texttt{let}\ x = t\ \texttt{in}\ e \mid t; e \mid \texttt{case}\ t\ \texttt{of}\ \{\iota_1(x_1) \to e_1 \mid \iota_2(x_2) \to e_2\} \mid t \mid te$$

where $\cdots$ indicates the $\mathscr{P}_\mathrm{C}$-expressions already defined. In addition to the nonlinear typing rules, we also add:

$$\frac{\Gamma; \cdot \vdash^{\mathscr{P}_\mathrm{C}} e : W}{\Gamma \vdash^{\mathtt{T}} \lceil e \rceil : \lceil W \rceil} \qquad \frac{\Gamma; x : W \vdash^{\mathscr{P}_\mathrm{C}} e : W'}{\Gamma \vdash^{\mathtt{T}} \lceil \lambda x.e \rceil : \lceil W \multimap W' \rceil}$$

$$\frac{\Gamma \vdash^{\mathtt{T}} t : \lceil W \rceil}{\Gamma; \cdot \vdash^{\mathscr{P}_\mathrm{C}} t : W} \qquad \frac{\Gamma \vdash^{\mathtt{T}} t : \lceil W_1 \multimap W_2 \rceil \qquad \Gamma; \Theta \vdash^{\mathscr{P}_\mathrm{C}} e : W_1}{\Gamma; \Theta \vdash^{\mathscr{P}_\mathrm{C}} te : W_2}$$

The $\mathscr{P}_{\mathrm{C}}$-typing judgment $\Theta \vdash^{\mathscr{P}_{\mathrm{c}}} e : W$ is updated to accomodate the new expressions e and a nonlinear typing context, so now has the form $\Gamma; \Delta \vdash^{\mathscr{P}_{\mathrm{c}}} e : W$. The $\mathscr{P}_{\mathrm{C}}$-typing rules are adjusted so that the context may always contain a nonlinear part Γ. For example:

$$\frac{\Gamma; \Theta \vdash^{\mathscr{P}_{\mathrm{c}}} e : \texttt{Pauli} \qquad \Gamma; \cdot \vdash^{\mathscr{P}_{\mathrm{c}}} e_x : W \qquad \Gamma; \cdot \vdash^{\mathscr{P}_{\mathrm{c}}} e_z : W \qquad \Gamma; \cdot \vdash^{\mathscr{P}_{\mathrm{c}}} \omega_W(e_z, e_x) \equiv 1}{\Gamma; \Theta \vdash^{\mathscr{P}_{\mathrm{c}}} \texttt{case } e \texttt{ of } \{\texttt{X} \to e_x \mid \texttt{Z} \to e_z\} : W} \tag{3.7}$$

The *non-linear values* are:

$$v^t ::= () \mid (v_1^t, v_2^t) \mid \iota_1(v^t) \mid \iota_2(v^t) \mid \lambda x.t \mid \lceil e \rceil \mid \lceil \lambda x.e \rceil$$

Note that for the values $\lceil e \rceil$ and $\lceil \lambda x.e \rceil$, the (closed) expressions e are not necessarily normalized. We add the β-reduction rules:

$$\lceil e \rceil \to_\beta e \qquad\qquad \lceil \lambda x.e \rceil(\langle r \rangle v) \to_\beta \langle r \rangle e\{v/x\}$$

3.8 Pseudocode examples

We now introduce some top-level syntax for the programming language. The syntax is inspired by that of Haskell. In the $d = 2$ case, the Pauli matrices are:

```
X :: ⌈Pauli⌉
X =  ⌈[1,0]⌉
```

```
Y :: ⌈Pauli⌉
Y =  ⌈[1,1]⌉
```

```
Z :: ⌈Pauli⌉
Z =  ⌈[0,1]⌉
```

```
I :: ⌈Pauli⌉
I =  ⌈[0,0]⌉
```

The projective S gate acts by $SXS^{\dagger} = Y$ and $SZS^{\dagger} = Z$. In $\lambda^{\mathscr{P}_{\mathrm{C}}}$ this is expressed:

```
1   S :: ⌈Pauli ⊸ Pauli⌉
2   S ⌈X = Y⌉
3   S ⌈Z = Z⌉
```

Lines 2 and 3 use *pattern match* syntax, which can be found in most functional programming languages, such as Haskell, and resembles the "piecewise function" notation in math. This program typechecks on account of the symplectic form condition being satisfied. On the other hand,

```
illTyped :: ⌈Pauli ⊸ Pauli⌉
illTyped ⌈X = X⌉
illTyped ⌈Z = X⌉
```

does not typecheck since it does not specify a projective Clifford operation. For a multiqubit example, consider the CNOT gate:

```
cnot :: ⌈ Pauli • Pauli ⊸ Pauli • Pauli ⌉
cnot ⌈ in1 X = in1 X ⋆ in2 X ⌉
cnot ⌈ in1 Z = in1 Z         ⌉
cnot ⌈ in2 X = in2 X         ⌉
cnot ⌈ in2 Z = in1 Z ⋆ in2 Z ⌉
```

P	$(CNOT)P(CNOT)^{\dagger}$
$X \otimes I$	$X \otimes X$
$Z \otimes I$	$Z \otimes I$
$I \otimes X$	$I \otimes X$
$I \otimes Z$	$Z \otimes Z$

Ultimately we will add support for polymorphism, so for example, the user will be able to define the following function uniformly for all `V1` and `V2`:

```
swap :: ⌈ V1 • V2 ⊸ V2 • V1 ⌉
swap ⌈ in1 q1 = in2 q1 ⌉
swap ⌈ in2 q2 = in1 q2 ⌉
```

The LNL type system allows for several useful constructs. For example, the projectivization of a Pauli P is projective Clifford, since $PQP^{\dagger} = \zeta^{\omega(P,Q)}Q$, and we may let Pauli operators act as Cliffords (by conjugation) using:

```
    pauliToClifford :: ⌈V⌉ → ⌈ V ⊸ V ⌉
    pauliToClifford p  ⌈ q = ⟨omega p q⟩ q ⌉
```

We may also compose projective Cliffords in sequence and parallel:

```
    compose :: ⌈ V1 ⊸ V2 ⌉ → ⌈ V2 ⊸ V3 ⌉ → ⌈ V1 ⊸ V3 ⌉
    compose f g ⌈ q = g (f q) ⌉

    parallel :: ⌈ V1 ⊸ V2 ⌉ → ⌈ V1' ⊸ V2' ⌉ → ⌈ V1 • V1' ⊸ V2 • V2' ⌉
    parallel f g ⌈ in1 q  = in1 (f q)  ⌉
    parallel f g ⌈ in2 q' = in2 (g q') ⌉
```

Example (Steane code) Finally, for a more complete example, we show how to code up the syndrome preparation circuit for the Steane code. Recall that the Steane code is a $[[7,1,3]]$-quantum error correction code. More specifically, it is a CSS code formed from using the Hamming code to correct both qubit flip and phase errors. The Hamming code, in turn, is a classical binary $[7,4,3]$-code with parity check matrix:

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

The following stabilizers generate the stabilizer group for the Steane code:

$$\begin{aligned} S_{\mathrm{x},1} &= I \otimes I \otimes I \otimes X \otimes X \otimes X \otimes X & \quad S_{\mathrm{z},1} &= I \otimes I \otimes I \otimes Z \otimes Z \otimes Z \otimes Z \\ S_{\mathrm{x},2} &= I \otimes X \otimes X \otimes I \otimes I \otimes X \otimes X & \quad S_{\mathrm{z},2} &= I \otimes Z \otimes Z \otimes I \otimes I \otimes Z \otimes Z \\ S_{\mathrm{x},3} &= X \otimes I \otimes X \otimes I \otimes X \otimes I \otimes X & \quad S_{\mathrm{z},3} &= Z \otimes I \otimes Z \otimes I \otimes Z \otimes I \otimes Z \end{aligned}$$

The logical qubits are:

$$\begin{aligned} |0\rangle_{\mathrm{L}} = \frac{1}{\sqrt{8}}(&|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ &+ |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle) \\ |0\rangle_{\mathrm{L}} = \frac{1}{\sqrt{8}}(&|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\ &+ |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle) \end{aligned}$$

Measurement of the observables $S_{\mathrm{x},1}$, $S_{\mathrm{x},1}$, and $S_{\mathrm{x},3}$ yields a 3-bit string $y = b_1 b_2 b_3 \in \mathbb{F}_2^3$. This is the *syndrome* for X errors. That is, an X error occurred on qubit $i \in \{1, \cdots, 7\}$ if and only if $He_i = y$. Likewise, the syndrome for Z errors is obtained by measuring $S_{z,1}$, $S_{z,2}$, and $S_{z,3}$.

Recall that an *ancilla* is an additional quantum register used as "workspace" during a quantum computation. In stabilizer coding, an ancilla qubit is added for each stabilizer generator, and measurement of the ancilla register is equivalent to that of the stabilizer generators, and hence encodes the syndrome.

In the case of the Steane code, in order to correct the errors, besides the seven physical qubits, one adds three ancillary qubits for the X error syndrome and three for the Z error syndrome. It is standard to write down the quantum circuit for the syndrome measurement on these $13 = 7 + 3 + 3$ qubits. Rather than using the quantum circuit model, we show how to code the same structure into $\lambda^{\mathscr{P}_{\mathrm{C}}}$.

First we make a new Pauli data type to keep track of the three registers:[3]

```
pdata steaneType =
  | Data      (i :: FinNat 7) (p :: Pauli) -- physical data qubits
  | BitFlip   (i :: FinNat 3) (p :: Pauli) -- bit-flip ancillae
  | PhaseFlip (i :: FinNat 3) (p :: Pauli) -- phase-flip ancillae
```

Here `FinNat n` is the (classical) type of natural numbers between 1 and n, inclusive. In standard functional programming style, `Data`, `BitFlip`, and `PhaseFlip` are *constructors*. There is no recursion here, and in this case they are essentially used as one uses an enum. So `steanType` is essentially syntactic sugar for:

$$(\texttt{Pauli} \bullet \cdots \bullet \texttt{Pauli}) \bullet (\texttt{Pauli} \bullet \texttt{Pauli} \bullet \texttt{Pauli}) \bullet (\texttt{Pauli} \bullet \texttt{Pauli} \bullet \texttt{Pauli})$$

Next, we define

```
hammingSyndrome :: FinNat 7 → Bool × Bool × Bool
hammingSyndrome 1 = (1, 0, 0)
hammingSyndrome 2 = (0, 1, 0)
hammingSyndrome 3 = (0, 0, 1)
hammingSyndrome 4 = (0, 1, 1)
hammingSyndrome 5 = (1, 1, 0)
hammingSyndrome 6 = (1, 0, 1)
hammingSyndrome 7 = (1, 1, 1)
```

[3] As in Haskell, `--` is the syntax for comments.

and

```
syndromeBitFlips :: Bool × Bool × Bool → ⌈ steaneType ⌉
syndromeBitFlips (b1, b2, b3) = (if b1 then BitFlip 1 X else I)
                              ⋆ (if b2 then BitFlip 2 X else I)
                              ⋆ (if b3 then BitFlip 3 X else I)
syndromePhaseFlips :: Bool × Bool × Bool → ⌈ steaneType ⌉
syndromePhaseFlips (b1, b2, b3) = (if b1 then PhaseFlip 1 X else I)
                                ⋆ (if b2 then PhaseFlip 2 X else I)
                                ⋆ (if b3 then PhaseFlip 3 X else I)
```

Finally, the ancilla preparation is given by:

```
steane :: ⌈ steaneType ⊸ steaneType ⌉
-- identity on X_a for ancillae a
steane ⌈BitFlip i X⌉   ⋆= I
steane ⌈PhaseFlip i X⌉ ⋆= I
-- maps Z_a to one of the six stabilizers
steane ⌈BitFlip 1 Z⌉   ⋆= Data 1 X ⋆ Data 4 X ⋆ Data 5 X ⋆ Data 6 X
steane ⌈BitFlip 2 Z⌉   ⋆= Data 2 X ⋆ Data 4 X ⋆ Data 6 X ⋆ Data 7 X
steane ⌈BitFlip 3 Z⌉   ⋆= Data 3 X ⋆ Data 5 X ⋆ Data 6 X ⋆ Data 7 X
steane ⌈PhaseFlip 1 Z⌉ ⋆= Data 1 Z ⋆ Data 4 Z ⋆ Data 5 Z ⋆ Data 6 Z
steane ⌈PhaseFlip 2 Z⌉ ⋆= Data 2 Z ⋆ Data 4 Z ⋆ Data 6 Z ⋆ Data 7 Z
steane ⌈PhaseFlip 3 Z⌉ ⋆= Data 3 Z ⋆ Data 5 Z ⋆ Data 6 Z ⋆ Data 7 Z
-- helper function describes whether an X or Z error occurred on d_i
steane ⌈Data i X⌉      ⋆= syndromeBitFlips   (hammingSyndrome i)
steane ⌈Data i Z⌉      ⋆= syndromePhaseFlips (hammingSyndrome i)
```

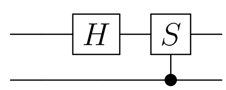
Note that this program does not *perform* the error correction or measurement. It only prepares the syndrome registers for measurement. The last two lines must be defined this way in order for the symplectic form relation to check out. On the one hand, proving that the program is correct seems to require additional pen-and-paper work. Namely, one verifies that the conjugation action on Paulis of the standard ancilla preparation circuit agrees with the tableau read off the program code. On the other hand, this design pattern could be employed for other CSS codes, and one might write programs for implementing families of codes using other features of the language, such as composability and polymorphism.

3.9 Future work

So far, $\lambda^{\mathscr{P}_{\mathrm{C}}}$ pertains to multiqu*d*it projective Clifford operations for a fixed choice of d. This means that it does not allow for universal quantum computation. One way to fix this is to allow for multiple values of d in the same program. By just allowing for $d = 2$ and $d = 4$, one would allow for universal quantum computation. To see why, note that:

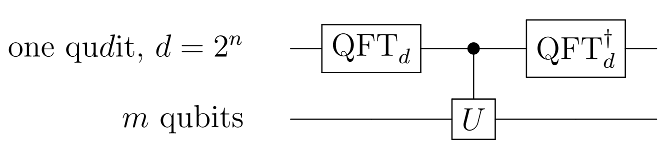
$$CS = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & i \end{pmatrix} \notin \mathbf{Cl}_{2,2}$$

So $\langle \mathbf{Cl}_{d=2}, CS \rangle$ is universal by [NRS00]. On the other hand, $\langle \mathbf{Cl}_{d=2}, \mathbf{Cl}_{d=4} \rangle = \langle \mathbf{Cl}_{d=2}, CS \rangle$, since the 2-qubit quantum Fourier transform may be synthesized as:



To achieve this, the system has to be regarded as consisting of two qubits at one time and as one ququart at another. It would be practical to allow for more values of d as well. By allowing for $d = 2$,4, and 8, the Toffoli gate is exactly synthesizable. Realizing a single qu*d*it system, with $d = 2^n$, instead as a system of n qubits amounts to taking a binary expansion of the basis vectors, i.e. working with a fixed bijection $\mathbb{Z}_{2^n} \to \mathbb{Z}_2^n$. Correspondingly, there is a change-of-basis between the two relevant operator bases for $\mathbb{C}^{2^n \times 2^n}$. The action of a projective Clifford operation for a single qu*d*it on a multiqubit Pauli operator may have exponentially many nonzero coefficients, and similarly in the other direction. The challenge is to divert any explosive computations to the (future) quantum compiler.

We also expect to be able to treat different registers as qu*d*its for different values of d, and this is actually a much easier task, involving the central product construction for Pauli groups. This functionality would be extremely practical for programming at a high level, since many quantum algorithms are best regarded as acting on such hybrid systems. For example, Shor's algorithm has the form:



In this case U is not in the m qubit Clifford group, let alone the m qubit Pauli group, so the controlled gate CU is not in the Clifford group of the composite system. In the case of Shor's algorithm, U is modular multiplication by a constant, which is classical. By allowing both generalizations, in which the change-of-basis can be applied to blocks of the computation bordered both spatially and temporally, a simple (though perhaps inefficient) way to synthesize U is with Toffoli gates, which are implemented by switching the second register between acting as multiple qu$d$its with d varying between 2, 4, and 8 throughout the computation.

Another future direction is to add polymorphism and/or dependent types. In fact, two kinds of polymorphism could be imagined. For one, we could allow for programs that are specified for all values of d simultaneously. Many quantum algorithms generalize along these lines, so it stands to reason that this would be a useful programming abstraction. For example, the constructors `X` and `Z` could stand for Paulis of the appropriate dimension, and the $\star$ product would also change depending on the type of data. Secondly, we could allow for the usual kind of polymorphism, for example allowing one to define a polymorphic swap operation.

We are also curious to explore what would be needed to allow more than one free variable in Pauli expressions. Ideally, we would like to be able to define operations higher in the Clifford hierarchy. For example, the projective T gate could be implemented as:

```
t :: ⌈ Pauli ⊸ Pauli ⊸ Pauli ⌉
t ⌈ Z q = pauliToClifford Z q  ⌉
t ⌈ X X = Y                    ⌉
t ⌈ X Z = ⟨1⟩Z                 ⌉
```

We are currently at a loss for how to certify these operations in terms of their condensed encodings analogous to how we certify projective Cliffords, but we are curious whether this could be achieved using results of Chen and de Silva [Cd24].

Finally, our language does not yet have an implementation. There are various ideas for compilers, for instance that integrate with PCOAST [Pay+23a].

Chapter 4

Multiqutrit exact synthesis

Until this point, the only quantum operations we have studied are (projective) Clifford operations, and our focus has not been on decomposing them, but on combining them using programming abstractions. We now turn to the problem of *circuit synthesis*, which asks how to decompose a given a unitary operation (not necessarily Clifford) over a given gate set. Specifically, we consider the synthesis problem for multiqutrit unitaries defined over the ring:

$$\mathbb{Z}[\tfrac{1}{3}, e^{2\pi i/9}]$$

The single qutrit case was done in [KVM24], where it was shown that $\mathbf{U}_3(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/9}])$ is equal to the group of single-qutrit Clifford+D gates. In analogy, it was first shown in [KMM13] that $\mathbf{U}_2(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$ equals single-qubit Clifford+T, and later extended to multiple qubits in [GS13].

Each of these results in exact synthesis establishes that a given set of quantum gates generates an arithmetic group. Such results are rare, and important connections between the problem of synthesis and the theory of maximal orders, particularly of quaternion algebras, have been established in [KY15], [Kli+15], and [PS18]. Beyond just an algebraic curiosity, exact synthesis has practical importance. In the Solovay-Kitaev approximate synthesis algorithm, the number of gates needed to approximate a unitary to precision ϵ was shown to be $O(\log^c \frac{1}{\epsilon})$ where $c \approx 3.98$. The Solovay-Kitaev algorithm does not give insight into the structure of the circuit, and the constant c is far higher than the information theoretic lower bound of 1. Since the Solovay-Kitaev algorithm is not exact and does not lead to a better bound for c, the exact synthesis program was born. Recent improvements lower c to around 1.7, and in practice, the best-known synthesis algorithms are a hybrid of approximate and exact synthesis, employing exact synthesis methods as subroutines by rounding off matrix entries into a ring.

Our method somewhat follows that of [GS13], but relies crucially on other ingredients, such as catalytic embedding, which was defined in [Amy+23]. Catalytic embedding eliminates 9th roots of unity in favor of 3rd roots, at the cost of introducing one ancilla:

$$\mathbf{U}_{3^n}(\mathbb{Z}[\tfrac{1}{3}, e^{2\pi i/9}]) \hookrightarrow \mathbf{U}_{3^{n+1}}(\mathbb{Z}[\tfrac{1}{3}, e^{2\pi i/3}])$$

This reduces the problem to synthesis over $\mathbb{Z}[\frac{1}{3}, e^{2\pi i/3}]$. We show that all such unitaries may be synthesized using multiqutrit Clifford+R gates. There is technically a question of synthesizing the *catalyst*, a magic state that must be initialized in the ancilla register. Since the catalyst comes out of the computation unaffected, it can be reused, thereby minimizing the problem. Then, we employ techniques developed in [KVM24]. We recall that localizing $\mathbb{Z}[\omega]$ at 3 is the same as localizing it at $\chi = 1 - \omega$. From there, we use the *smallest denominator exponent* for χ as a cost function on unitary matrices, which is reduced to zero by successive applications of 3-level unitaries from Clifford+R, (which have entries in $\mathbb{Z}[\frac{1}{3}, e^{2\pi i/3}]$). Then, as we show, this condition implies that the resulting matrix is essentially the identity.

The 3-level unitaries should not be confused with single-qutrit gates. Instead, these are unitaries acting nontrivially on a coordinate subspace of dimension at most 3. These are factored into multiply-controlled Clifford+R gates, for which results from [YW22] are employed to synthesize them over Clifford+T.

Thus, building on previous results, we prove:

Theorem 4.0.1 $\mathbf{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/9}])$ *is synthesizable over Clifford+T using 2 ancillas.*

We also note that the proof itself *is* the synthesis algorithm.

Author contributions The results in this chapter are joint work with Amolak Kalra, Manimugdha Saikia, Dinesh Valluri, and Jon Yard [Kal+24]. Each of the five authors made meaningful contributions to the work. The problem was suggested by Jon Yard. Most of the calculations were done as a group over Zoom, under the guidance of Dinesh Valluri.

Acknowledgment After the work was completed, it was brought to our attention that Andrew N. Glaudell, Neil J. Ross, John van de Wetering, and Lia Yeh independently established related results in [Gla+24].

4.1 Qutrit gatesets and controlled gates

Let $\zeta = e^{2\pi i/9}$ and $\omega = e^{2\pi i/3}$. We work the following single-qutrit gates previously considered in [Gla+24]:

$$H = \frac{1}{\sqrt{-3}}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \quad D_{a,b,c} = \begin{pmatrix} \zeta^a & 0 & 0 \\ 0 & \zeta^b & 0 \\ 0 & 0 & \zeta^c \end{pmatrix} \quad R_{u,v,w} = \begin{pmatrix} (-1)^u & 0 & 0 \\ 0 & (-1)^v & 0 \\ 0 & 0 & (-1)^w \end{pmatrix}$$

Among these, three important ones are $R = R_{0,0,1}$, $S = D_{1,1,2}$, and $T = D_{0,1,2}$. Then *Clifford+D* refers to the gateset consisting of H, $D_{a,b,c}$, and $R_{u,v,w}$ ranging over all values of $a, b, c; u, v, w$, or to the group generated by these gates. Next, *Clifford+T* comprises of H, S, and T, and finally, *Clifford+R* comprises of H, S, and R.

We now show some important gates generated by the Clifford+R gateset. First notice that H is $-i$ times the 3×3 quantum Fourier transform. So we obtain the X gate:

$$X = H^\dagger Z H = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Using X, we may cycle the rows and columns of any matrix, so we get the following 1-level gates of interest:

$$\begin{aligned} \mathsf{diag}(1,1,-1) &= R \qquad & \mathsf{diag}(-1,1,1) &= XRX^\dagger \qquad & \mathsf{diag}(1,-1,1) &= X^\dagger R X \\ \mathsf{diag}(1,1,\omega) &= S \qquad & \mathsf{diag}(\omega,1,1) &= XSX^\dagger \qquad & \mathsf{diag}(1,\omega,1) &= X^\dagger S X \end{aligned}$$

By multiplying across the diagonals, the product of the matrices on the top row above is $-I$. We then get the following 2-level gates:

$$-H^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \qquad -XH^2X^\dagger = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \qquad -X^\dagger H^2 X = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

The *multiqutrit* analogs of Clifford+D, Clifford+T, and Clifford+R are defined by letting the single-qutrit versions act on all registers and also including controlled X gates:

$$CX\,|x\rangle\,|y\rangle = |x\rangle\,|x+y\rangle \qquad CX = \begin{pmatrix} I & 0 & 0 \\ 0 & X & 0 \\ 0 & 0 & X^2 \end{pmatrix} = I \oplus X \oplus X^2$$

In Thm. 4.4.3 and elsewhere, we call for 3-level unitaries of type H or S, 2-level unitaries of type $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, and 1-level unitaries of type -1 and ω. The calculations above show that in this situation it suffices to consider unitaries from the (multiqutrit) Clifford+R gateset.

We will later also consider multiply-controlled U operations where $U \in \mathbf{U}_3$. These are defined analogously. Explicitly, the *multiply-controlled* U *operation* $C_t U \in \mathbf{U}_{3^{t+1}}$, which is controlled by the first t qutrits and targets the last qutrit, satisfies the inductive formula:

$$C_t U = I_{3^t} \oplus C_{t-1} U \oplus C_{t-1} U^2 \qquad\qquad C_0 U = U$$

We do indeed find it helpful (when dealing with Gray codes) to think of these in terms of block matrices. The constructions of qu*d*it controlled gates and multiply-controlled gates are standard, and can even be easily generalized to composite systems whose constituents have different dimensions from each other. As a small cautionary example, $\mathbb{C}^8$ could be viewed either as a 3-qubit system or a ququart-qubit system. The doubly-controlled U gate (Toffoli if $U = X$), pertaining to the first case, is different from the ququart-controlled U gate, pertaining to the second case. These are

$$\begin{pmatrix} I & & & \\ & I & & \\ & & I & \\ & & & U \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} I & & & \\ & U & & \\ & & U^2 & \\ & & & U^3 \end{pmatrix}$$

repsectively.

4.2 Catalytic embedding

One ingredient to multiqutrit exact synthesis is catalytic embedding. In this section we explore possible generalizations using standard tools from number theory.

Consider a tower of integral domains

$$R_1 \subseteq R_2 \subseteq R_3 \subseteq \cdots$$

with each R_k a finitely generated free R_{k-1}-module of degree d, where d is constant with respect to k. Suppose further that each R_k has a *primitive element* $z_k \in R_k$, that is:

$$R_k = R_{k-1}[z_k]$$

Since R_{k-1} is an integral domain, the minimal polynomial f_k of z_k over R_{k-1} is well-defined. It follows that $\{1, z_k, \cdots, z_k^{d-1}\}$ is an R_{k-1}-basis for R_k; it is called the *power basis*.

Recall that an *algebraic number field* is a finite extension of $\mathbb{Q}$. A *monogenic field* is an algebraic number field K for which there exists $z \in K$ such that $\mathcal{O}_K = \mathbb{Z}[z]$, where $\mathcal{O}_K$ is the ring of integers of K. For example, if ζ is a root of unity, then the *cyclotomic field* $\mathbb{Q}(\zeta)$ is monogenic, owing to the nontrivial fact that $\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$. Another example is the real subfield $\mathbb{Q}(\zeta + \zeta^{-1})$, since similarly, we have $\mathcal{O}_{\mathbb{Q}(\zeta+\zeta^{-1})} = \mathbb{Z}[\zeta + \zeta^{-1}]$. Now, if

$$K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots$$

is a tower of monogenic fields, then their rings of integers $R_k = \mathcal{O}_{K_k}$ satisfy the above property (provided the relative degrees are all d).

Now fix a positive integer N and unitaries $\Lambda_k \in \mathbf{U}_d(R_{k-1})$. Suppose each Λ_k has an eigenvector $|\lambda_k\rangle$, with corresponding eigenvalue z_k, and that for each k, we have a function:

$$\begin{aligned} \phi_k : \mathbf{U}_N(R_k) &\to \mathbf{U}_{dN}(R_{k-1}) \\ U &\mapsto \sum_{i=0}^{d-1} A_i \otimes \Lambda_k^i \end{aligned}$$

where, since each R_k is a free R_{k-1}-module, $A_1, \cdots, A_{d-1}$ are the unique matrices over R_{k-1} satisfying $U = \sum A_i z_i^k$. Then the data $((\phi_k, |\lambda_k\rangle))_{k=1}^{\infty}$ constitutes a *catalytic embedding* if:

$$\phi_k(U)(|\psi\rangle |\lambda_k\rangle) = (U |\psi\rangle) |\lambda_k\rangle \text{ for all } |\psi\rangle \in \mathbb{C}^N \tag{4.1}$$

Since z_k is an eigenvalue of a unitary, $z_k \in \mathsf{U}(1)$. So far we have only assumed that z_k is algebraic over K_{k-1}; it might not have finite *order*, but for simplicity, let us now assume that it does. Thus, we restrict our attention to the case where each ring is a cyclotomic extension of the previous. There is still flexibility in the base ring R_1, and figuring out what this ring "should" be is intimately related to the single qu*d*it exact synthesis problem.

The minimal polynomial for z_k over R_{k-1} is equal to the characteristic polynomial for Λ_k over R_{k-1} since each is a monic degree d polynomial f_k over R_{k-1} satisfying $f_k(z_k) = 0$, and the minimal polynomial is irreducible. Explicitly, by uniqueness, we have:

$$f_k(x) = x^d - z_k^d \in R_{k-1}[x]$$

It follows that $z_k^d \in R_{k-1}$. Due to the R_{k-1}-module isomorphism $R_k \cong R_{k-1}^d$, the *multiplication-by-z_k* endomorphism on R_k is represented by the companion matrix C_k for f_k:

$$C_k = \begin{pmatrix} & z_k^d \\ I & \end{pmatrix} \in R_{k-1}^{d\times d}$$

Now, C_k is diagonalized by the Vandermonde matrix, i.e. $C_k = V_k^{-1} D_k V_k$, where:

$$V_k = \begin{pmatrix} 1 & \lambda_{k,1} & \cdots & \lambda_{k,1}^{d-1} \\ 1 & \lambda_{k,2} & \cdots & \lambda_{k,2}^{d-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_{k,d} & \cdots & \lambda_{k,N}^{d-1} \end{pmatrix} \in R_k^{d\times d} \qquad D_k = \begin{pmatrix} \lambda_{k,1} & & & \\ & \lambda_{k,2} & & \\ & & \ddots & \\ & & & \lambda_{k,d} \end{pmatrix} \in R_k^{d\times d}$$

The roots of f_k are $\lambda_i = z_k \zeta_d^i$ where $\zeta_d = e^{2\pi i/d}$. Notice that V_k and D_k have entries in R_k whereas C_k has entries in R_{k-1}. Now, since z_k is a root of unity, the matrices C_k and D_k are unitary; $\frac{1}{\sqrt{\pm d}} V_k$ is unitary but the rescaling may mean that its coefficients are no longer in R_k. If d is an odd prime p, then the normalized Vandermonde matrix has coefficients in R_k provided that R_1 contain $1/p$, due to the Gauss sum:

$$\sum_{k=0}^{p-1} \zeta_p^{n^2} = \begin{cases} \sqrt{p} & : p \equiv 1 \bmod 4 \\ \sqrt{-p} & : p \equiv 3 \bmod 4 \end{cases}$$

In practice one may use C_k itself as the catalyzing matrix Λ_k provided that C_k satisfies the catalytic condition Eq. (4.1), and use $z_k = \zeta_{d^k} = e^{2\pi i/d^k}$. Related examples can be found in [Amy+23].

There might exist catalytic embeddings where z_k has infinite order, despite being an algebraic integer lying on the unit circle. Sadly, the ring $\mathbb{Z}[\zeta + \zeta^{-1}]$ cannot be involved in a catalytic embedding since it does not have a generator lying on the unit circle.

In this setting, it is convenient to define the norm and note a few of its properties. Let $R \subseteq A$ be integral domains, with A a free finitely generated R-module. Each $z \in A$ defines a *multiplication-by-z* map $m_z : A \to A$, allowing us to define the *norm* (and *trace*):

$$\mathsf{N}_{A/R}(z) = \mathsf{det}_R(m_z) \qquad\qquad \mathsf{Tr}_{A/R}(z) = \mathsf{Tr}_R(m_z)$$

Then $\mathsf{N}_{A/R} : A \to R$ is multiplicative and $\mathsf{N}_{A/R}(1) = 1$. It follows that if $u \in A^\times$ then $\mathsf{N}_{A/R}(u) \in R^\times$. The converse is also true. By the Cayley-Hamilton Theorem, each $z \in A$ satisfies its characteristic polynomial $x^d + c_{d-1}x^{d-1} + \cdots \mp c_1 x \pm \mathsf{N}_{A/R}(z) \in R[x]$, so if $\mathsf{N}_{A/R}(z) \in R^\times$, then,

$$1 = \frac{\pm z}{\mathsf{N}_{A/R}(z)}(z^{d-1} + c_{d-1}z^{d-2} + \cdots \mp c_1)$$

Hence $z \in A^\times$. In other words, units are detected by the norm function.

The rings we consider are always the rings of integers of algebraic number fields $R = \mathcal{O}_K$ and $A = \mathcal{O}_F$ with respect to a field extension F/K. Since the ring of integers is an order, i.e. $F = K \otimes_{\mathbb{Z}} \mathcal{O}_F$, it follows that $\mathsf{N}_{\mathcal{O}_F/\mathcal{O}_K}$ is just the restriction of the field norm $\mathsf{N}_{F/K}$.

We are of course most interested in cyclotomic fields, which are always Galois extensions. For a Galois extension F/K, the norm is the product of the Galois conjugates:

$$\mathsf{N}_{F/K}(z) = \prod_{\sigma \in \mathsf{Gal}(F/K)} z^\sigma$$

A coincidence relevant for qutrit exact synthesis is that $\mathsf{N}_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}$ is just the square of the ordinary absolute value function on $\mathbb{C}$ (restricted to $\mathbb{Q}(\zeta_3)$).

4.3 The cyclotomic polynomial

Let N be a positive integer, $\omega = e^{2\pi i/N}$, and $\chi = 1 - \omega$. The *Nth cyclotomic polynomial* Φ_N is the unique integer polynomial that divides $X^N - 1$ but not $x^k - 1$ for any $k < N$. Recall that $\mathbb{C}$ is an algebraically closed field, meaning we have the following factorization:

$$x^N - 1 = \prod_{k=1}^{N}(x - \omega^k)$$

The roots of Φ_N are precisely the principal Nth complex roots of unity, so:

$$\Phi_N(x) = \prod_{k \in (\mathbb{Z}/N\mathbb{Z})^\times} (x - \omega^k)$$

Putting these last two equations together, one arrives at:

$$X^N - 1 = \prod_{d|N} \Phi_d(x)$$

From here, one easily proves that:

$$\Phi_N(1) = \begin{cases} p & : N = p^n \text{ with } p \text{ prime} \\ 1 & : N \text{ has distinct prime factors} \end{cases}$$

We now specialize to the case that $N = p^n$ with p prime. It follows that

$$p = \Phi_N(1) = \chi^{\varphi(N)} u$$

where φ is the Euler totient function and u is defined as follows:

$$u = \prod_{k \in (\mathbb{Z}/N\mathbb{Z})^\times} \frac{1 - \omega^k}{1 - \omega} \in \mathbb{Z}[\omega]^\times$$

We see that u is a unit by checking that $\mathsf{N}_{\mathbb{Z}[\omega]/\mathbb{Z}}(u) = 1$. Then, since

$$\frac{1}{p} = \frac{u^{-1}}{\chi^{\varphi(N)}} \qquad \text{and} \qquad \frac{1}{\chi} = \frac{\chi^{\varphi(N)+1}}{p}$$

we have established the equality of the following localizations:

$$\mathbb{Z}\left[\tfrac{1}{p}, \omega\right] = \mathbb{Z}\left[\tfrac{1}{\chi}, \omega\right]$$

In the $N = 3$ case, pertinent to qutrits, these are also equal to $\mathbb{Z}[\frac{1}{\sqrt{-3}}, \omega]$, since $(\frac{\omega^2}{\chi})^2 = -\frac{1}{3}$.

4.4 The smallest denominator exponent

We now specialize to the qutrit case. Set $\omega = e^{2\pi i/3}$ and $\chi = 1 - \omega$.

The *smallest denominator exponent* $\mathsf{sde}(x)$ of $x \in \mathbb{Z}[\frac{1}{\chi}, \omega]$ is the least non-negative integer f such that $\chi^f x \in \mathbb{Z}[\omega]$. Since $\Phi_3(x) = x^2 + x + 1$, we have a well-defined homomorphism:

$$\begin{aligned} \mathcal{P} : \mathbb{Z}[\omega] &\to \mathbb{Z}/3\mathbb{Z} \\ g(\omega) &\mapsto g(1) \end{aligned}$$

Using the fact that $\mathbb{Z}[x]$ is an integral domain, it is easy to see that:

(*i*) $g \in \chi\mathbb{Z}[\omega]$ if and only if $\mathcal{P}(g) = 0$; and

(*ii*) $g \in \chi^2\mathbb{Z}[\omega]$ if and only if $\mathcal{P}(g) = 0$ and $\mathcal{P}(g') = 0$.

Technically, if $g \in R[\omega]$, its formal derivative g' with respect to ω is not well-defined, but if we first lift g to $\tilde{g} \in R[x]$, then we may define $\tilde{g}' \in R[x]$, and then $\tilde{g}'(1)$ doesn't depend on the lift modulo 3; this observation is required to make sense of the expression $\mathcal{P}(g')$. For a more general treatment of derivatives mod p in this setting, see [KVM24].

Since we work with unitary matrices, we make use of the complex conjugation and absolute value operations on $\mathbb{C}$. The squared absolute value restricted to the ring $\mathbb{Z}[\omega]$ is $\mathbb{Z}$-valued:

$$|-|^2 : \mathbb{Z}[\omega] \to \mathbb{Z}$$

Using the relation $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, one finds that (in the $N = 3$ case *only*) $|-|^2$ coincides with the norm $\mathsf{N}_{\mathbb{Z}[\omega]/\mathbb{Z}}$. The absolute value operation extends to vectors as usual. That is,

$$|v|^2 = |a|^2 + |b|^2 - a \cdot b \tag{4.2}$$

holds for all $v = a + b\omega \in \mathbb{Z}[\omega]^N$, where $\cdot$ is the dot product on $\mathbb{Z}^N$. We also extend the definition $\mathsf{sde}(v) = \mathsf{max}\{\mathsf{sde}(v_1), \cdots, \mathsf{sde}(v_N)\}$ from ring elements to vectors $v \in \mathbb{Z}[\frac{1}{\chi}, \omega]^N$.

Lemma 4.4.1 *For any $z = a + b\omega \in \mathbb{Z}[\omega]$, we have $\mathcal{P}(z)^2 = \mathcal{P}(z^2) = \mathcal{P}(|z|^2)$.*

However, the expression $\mathcal{P}(|z|)$ might be nonsensical since generally $|z| \notin \mathbb{Z}[\omega]$.

Proof The first equality holds since $\mathcal{P}$ is a ring homomorphism. For the second equality, let $z = a + b\omega \in \mathbb{Z}[\omega]$. Then:

$$z^2 - |z|^2 = 3ab\omega + b^2(\omega^2 - 1)$$

so the result follows by substituting $\omega \mapsto 1 \bmod 3$. ■

Lemma 4.4.2 *$v \in \mathbb{Z}[\omega]^N$ is a unit vector if and only if it has exactly one nonzero entry, which is a 6th root of unity.*

Proof Exhaust Eq. (4.2) and use the relation $1 + \omega + \omega^2 = 0$. ■

Definition $U \in \mathbf{U}_N$ is a *d-level unitary of type M* if it acts nontrivially on at most d standard basis vectors and the corresponding submatrix is $M \in \mathbf{U}_t$ for some $t \leq d$.

Theorem 4.4.3 *For all positive integers N and $U \in \mathbf{U}_N(\mathbb{Z}[\frac{1}{\chi}, \omega])$, there exists a sequence $U_1, \cdots, U_k$ of 3-level unitaries of type H, S, $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, -1 and ω, such that $U_1 \cdots U_k U = I$.*

For definitions of the matrices H and S, see Sec. 4.1.

Proof Let u be the first column of U and let f be a positive integer such that $v = \chi^f u \in \mathbb{Z}[\omega]^N$. Then since $f > 0$ and $\chi = 1 - \omega$, by Lem. 4.4.1, we have:

$$\sum_{i=1}^{m} \mathcal{P}(v_i)^2 = \mathcal{P}(|v|^2) = \mathcal{P}(|\chi|^{2f}) = 0 \in \mathbb{Z}/3\mathbb{Z} \tag{4.3}$$

It follows that the number of indices $i \in \{1, \cdots, N\}$ such that $\mathcal{P}(v_i) \neq 0$, i.e. such that $\mathsf{sde}(u_i) = f$, is a multiple of 3. If $\mathsf{sde}(u) = 0$, then by Lem. 4.4.2, u has a single nonzero entry, which is a 6th root of unity. Then by applying 2-level unitaries of type $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and 1-level unitaries of type ω, we may transform u into the first standard basis vector. This has the effect of transforming U into a block matrix with 1 in its top-left corner:

$$U_1 \cdots U_k U = \begin{pmatrix} 1 & \\ & U' \end{pmatrix}$$

It therefore suffices to transform u into a vector of smallest denominator exponent 0. We proceed by induction on $\lfloor \frac{N}{3} \rfloor$.

Base case: Since $N = 1$ or 2, it follows from Eq. (4.3) that $\mathcal{P}(v_i) = 0$ for each $i \in \{1, N\}$, and hence $f > \mathsf{sde}(u)$. Since f was an arbitrary positive integer, $\mathsf{sde}(u) = 0$.

Induction step: Now fix $f = \mathsf{sde}(u) > 0$. Without loss of generality, assume $f = \mathsf{sde}(u_i)$ for $i = 1, 2, 3$. We may force $\mathcal{P}(v_1) = \mathcal{P}(v_2) = \mathcal{P}(v_3) = 1$ by applying 1-level unitaries of type -1 if necessary. Now the truncated vector $u_{1,2,3} \in \mathbb{Z}[\frac{1}{\chi}, \omega]^3$ satisfies:

$$HS^a u_{1,2,3} = \frac{\omega^2}{\chi^{f+1}} \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \frac{\omega^2}{\chi^{f+1}} \begin{pmatrix} v_1 + v_2 + \omega^a v_3 \\ v_1 + v_2\omega + v_3^{a+2}\omega \\ v_1 + v_2\omega^2 + v_3^{a+1}\omega \end{pmatrix} \qquad a \in \mathbb{Z}/3\mathbb{Z}$$

Note that $w_1, w_2, w_3 \in \mathbb{Z}[\omega]$. Lift these to $g_1, g_2, g_2 \in \mathbb{Z}[x]$. By the Leibniz rule,

$$\begin{aligned} g_1' &= v_1' + v_2' + ax^{a-1}v_3 + x^a v_3' \\ g_2' &= v_1' + v_2 + xv_2' + (a+2)x^{a+1}v_3 + x^{a+2}v_3' \\ g_3' &= v_1' + 2xv_2 + x^2 v_2' + (a+1)x^a v_3 + +x^{a+1}v_3' \end{aligned}$$

It follows that:

$$\mathcal{P}(g_1') = \mathcal{P}(g_2') = \mathcal{P}(g_3') = a + \sum \mathcal{P}(v_i')$$

By choosing a to make these 0, we find that $w \in \chi^2\mathbb{Z}[\omega]$, and so:

$$\mathsf{sde}(HS^a u_{1,2,3}) = f - 1$$

We have only reduced the SDE of three entries that had the same SDE as u. If others remain, we repeat this process until we transform u into a vector u' with $\mathsf{sde}(u') = \mathsf{sde}(u) - 1$. Then we repeat the *entire* process in order to lower the SDE to 0. ■

4.5 Gray codes

We now show that a three-level unitary U of type $\tilde{U} = H$, S, $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, -1 or ω can be synthesized in terms of X gates, multiply-controlled X gates, and a single multiply-controlled $\tilde{U}$ operation on the last qutrit. To this end, we use Gray codes to obtain a factorization

$$U' = GUG^\dagger \tag{4.4}$$

where $U' = C_{n-1}\tilde{U}$ is the multiply-controlled $\tilde{U}$ operation targetting the last qutrit and controlled by the first $n-1$ qutrits, and G is a product of multiply-controlled X gates and single-qutrit X gates.

Given two n-trit strings $s, t \in (\mathbb{Z}/3\mathbb{Z})^n$, a *Gray code* taking s to t is simply a walk from s to t, where two strings in $(\mathbb{Z}/3\mathbb{Z})^n$ are deemed *adjacent* if differ in exactly one coordinate. Since U is a three-level unitary, let $r, s, t \in (\mathbb{Z}/3\mathbb{Z})^n$ be distinct such that if U acts nontrivially on computational basis vector $|u\rangle$ then $u \in \{r, s, t\}$. Then choose two Gray codes:

$$\begin{aligned} r = g_1 \mapsto \cdots \mapsto g_a = t \\ s = h_1 \mapsto \cdots \mapsto h_b = t \end{aligned}$$

Without loss of generality, ensure that $g_{a-1} \neq h_{b-1}$, and in fact, make it so that:

$$\begin{aligned} g_{a-1} &= (0, \cdots, 0, 0) \\ h_{b-1} &= (0, \cdots, 0, 1) \\ t &= (0, \cdots, 0, 2) \end{aligned}$$

Consider a step $g_i \mapsto g_{i+1}$ in the first walk. Then

$$g_i - g_{i+1} = ae_k = (0, \cdots, 0, a, 0, \cdots, 0) \in (\mathbb{Z}/3\mathbb{Z})^n$$

where the difference $a \in \mathbb{Z}/3\mathbb{Z} \setminus \{0\}$ occurs on the kth trit for some $1 \leq k \leq n$. Then let V_i be the unitary that fixes all computational basis states $|x\rangle$ except that it cycles:

$$|g_i\rangle \mapsto |g_i + ae_k = g_{i+1}\rangle \mapsto |g_i + 2ae_k\rangle \mapsto |g_i\rangle$$

A circuit for V_i is given in Fig. 4.1. Repeating this process, we obtain quantum Gray codes

$$\begin{aligned} |r\rangle = |g_1\rangle \mapsto \cdots \mapsto |g_a\rangle = |t\rangle \\ |s\rangle = |h_1\rangle \mapsto \cdots \mapsto |h_b\rangle = |t\rangle \end{aligned}$$

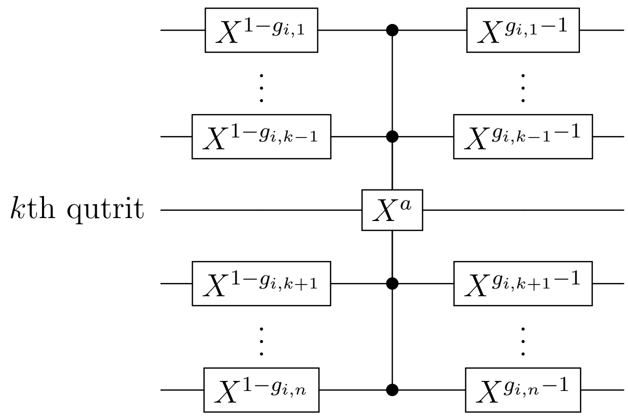


Figure 4.1: A unitary V_i fixing all except the kth qutrit, which it cycles mod 3.

implemented by unitaries $V = V_a \cdots V_1$ and $W = W_b \cdots W_1$, respectively, each composed of X gates and multiply-controlled X gates. By design, $G = WV$ satisfies Eq. (4.4).

Finally, [YW22] is used to synthesize the multiply-controlled X and $\tilde{U}$ gates over Clifford+T using at most one ancilla. It follows that every $U \in \mathbf{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/3}])$ can be exactly synthesized over Clifford+T using one ancilla, and finally that every $U \in \mathbf{U}_{3^n}(\mathbb{Z}[\frac{1}{3}, e^{2\pi i/9}])$, hence all Clifford+$D$ gates, can be exactly synthesized over Clifford+T with two ancillas provided the catalyst.

Chapter 5

Operations defined on categories

In Ch. 2 we investigated generalized Heisenberg groups and the equivalent structure encoded by their phase space through the symplectic form. Our goal is to show, in Ch. 6, that the theory of symplectic forms can be carried out in any sufficiently structured category. In this chapter, we study the structures and properties that such a category needs.

The *microcosm principle* [BD97] suggests that in order to internalize the notion of duality, one must first go to the appropriate categorification. Pontryagin duality is an example of the kind of internal duality we're after, due to its role in the theory of symplectic forms on locally compact abelian groups [Mum06]. Another example is the dual vector space construction. The former is more subtle, because the dualizing object for locally compact abelian groups is $\mathsf{U}(1)$, different from its tensor unit $\mathbb{Z}$. This leads us to consider star-autonomous categories (as in [Bar95]), particularly in the case where the linear distributors are isomorphisms.[1] We find that the theory of star-autonomous categories, at a high level, revolves around the negation adjunction; this is the categorified notion of duality in question.

Recall that in the definition of *group*, the associative law is motivated by abstracting this property of morphism composition; trivially, every group may be realized as the automorphism group of an object in some category. In analogy, linear distributivity is the key to formulating an abstract notion of duality. Associativity, as it turns out, is irrelevant to the theory of duality, despite what one might expect based on the presence of the associator in the definition of *adjunction*. Indeed, the more general concept of a *linear adjunction*, as

[1] From the perspective of linear logic, this case is sometimes considered degenerate.

defined in [CKS00], does not involve the associator. The associator in the definition of *adjunction* is just a degenerate case of the linear distributors when $\otimes \cong \parr$. With this insight, we carry out the theory of star-autonomous categories without relying on an associative structure. Our lack of reliance on associativity marks a major difference from existing accounts of monoidal and star-autonomous categories found for example in [Mac78] and [Bar95].

Negation is then seen to be a magmal adjunction in the ambient bicategory Cat. We mainly consider just magmal adjunctions, but note that Kelly's framework of *doctrinal adjunction* [Kel74] allows for several variants (magmal adjunctions, monoidal adjunctions, etc.) to be treated uniformly by realizing the corresponding *kind* of category (magmal, monoidal, etc.) as a 2-monad [Kel74]. Magmal adjunctions are a joint generalization of de Morgan duality and homomorphisms of (non-associative) algebraic structures. In our approach to linearly distributive categories, we find that three possible levels of coherence of the negation adjunction determine the important features of the category, relating for instance to finite dimensionality of vector spaces. Using Mac Lane's Parameter Theorem [Mac78], we find that an important currying formula arising in the theory of symplectic forms holds even without assuming the full level of coherence.

Dropping associativity highlights which parts of the theory *do* have interactions with associativity. These reveal, for instance, profound interactions with enrichment and the question of whether objects in a category are determined by their global elements. We formulate these concepts rigorously in order to instantiate the framework of Ch. 6 at our example categories of interest. Furthermore, although most of the theory of star-autonomous categories [Bar79; Bar91; Bar95] stays intact, we find a stratification between de Morgan duality and nuclearity. This implies that in the non-associative case, the category has separate left and right nuclei.

5.1 Subobjects and generalized elements

In this section we investigate subobjects, global elements, and connections between these concepts. The subobject preorder is a standard construction in category theory, so we mostly write about it here to provide context and introduce notation. We also note that if $\mathscr{C}$ is preabelian, then its subobject preorders are lattices and the two equivalent definitions of the direct sum (internal and external) are still present in the abstract setting. This relates the biproduct (direct sum) on $\mathscr{C}$ to the meet and join of its subobject preoders.

By the Yoneda lemma, every category $\mathscr{C}$ embeds into the category of presheaves on $\mathscr{C}$ [Mac78]. Intuitively, the presheaf $よ_{\mathscr{C}}(X) = \mathsf{Hom}_{\mathscr{C}}(-, X)$ for an object X collectively accounts for the *generalized elements* $x : Y \to X$ of X, naturally varying across all stages of definition Y. The theory in Ch. 6 involves an interplay between these generalized elements and so-called *global elements*. The latter are morphisms of the form $x : \top \to X$ where $\top$ is a fixed stage of definition. Fixing the stage of definition makes the functor $\mathsf{Hom}_{\mathscr{C}}(\top, -)$ too forgetful to be useful, but this can sometimes be fixed using enrichment. In Sec. 5.1.2 we give examples of the enriched functor $\mathsf{hom}_{\mathscr{C}}(\top, -)$ and explain how this can in some situations serve as a substitute for the Yoneda functor $よ_{\mathscr{C}}$.

In Sec. 5.1.3, we investigate the interaction between enriched global elements and subobjects. We also introduce various forms of a *subobject axiom*, which ends up arising in Ch. 6 in the proof that maximally isotropic subobjects are coisotropic.

5.1.1 Subobjects

Let W be an object in a category $\mathscr{C}$. An object in the *slice category* $\mathscr{C} \downarrow W$ is a morphism $x : Q \to W$ in $\mathscr{C}$, and a morphism in $\mathscr{C} \downarrow W$ from $x : Q \to W$ to $y : P \to W$ is a morphism $\phi : Q \to P$ in $\mathscr{C}$ subject to the commutativity of the following diagram:

$$\begin{tikzcd} Q \arrow[rr, "\phi"] \arrow[dr, "x"'] & & P \arrow[dl, "y"] \\ & W & \end{tikzcd}$$

It is convenient to identify a morphism $\phi : x \to y$ in $\mathscr{C} \downarrow W$ with its underlying morphism $\phi : Q \to P$ in $\mathscr{C}$. We often require x and y to be monic, and so we instead prefer the full subcategory $\textsc{Sub}_{\mathscr{C}}(W)$ of $\mathscr{C} \downarrow W$ on monic objects x, called the *category of subobjects of* W, whose name will be justified momentarily. Morphisms in $\textsc{Sub}_{\mathscr{C}}(W)$ are automatically monic, and we may alternately define $\textsc{Sub}_{\mathscr{C}}(W) = \mathsf{monos}(\mathscr{C}) \downarrow W$ where $\mathsf{monos}(\mathscr{C})$ is the subcategory of $\mathscr{C}$ consisting of the monomorphisms.

A *preorder* (or *preordered set* or *proset*) is a category in which for any two objects x and y, there is at most one morphism $x \to y$.[2] There are two conventional meanings for $\textsc{Sub}_{\mathscr{C}}(W)$, [Joh02]. We have chosen to define $\textsc{Sub}_{\mathscr{C}}(W)$ as a preorder, but it is also common to consider its partially ordered set (also known as a *poset* or *partial order*) of isomorphism classes [Joh02].

Because $\textsc{Sub}_{\mathscr{C}}(W)$ is a preorder and W is fixed, in the literature one may see an object $x : Q \to W$ abbreviated as Q [Joh02]. This will be too confusing in our application, but the notation $x : Q \to W$ is too cumbersome, so we will introduce an intermediate shorthand. Instead of $x : Q \to W$, let us write $x : [Q]_W$. Since given another $y : [Q]_W$, we necessarily have $x \cong y$, we usually may as well omit x from the notation. Moreover, we always fix W first and work within $\textsc{Sub}_{\mathscr{C}}(W)$, so we may also omit W. Thus, we write $[Q]_W$, $x : [Q]$, or even $[Q]$ in place of $x : [Q]_W$. Despite the omission of "x", the notation $[Q]$ implicitly refers to a *specific* monomorphism $x : Q \to W$ as opposed to an isomorphism class. Writing $[Q]$ is not too far from the conventional shorthand of writing Q, but it has the benefit of clarifying that we are working in $\textsc{Sub}_{\mathscr{C}}(W)$ rather than $\mathscr{C}$. This will be necessary because we will work both with objects of $\mathscr{C}$ and with objects of $\textsc{Sub}_{\mathscr{C}}(W)$.

[2] We are ignoring size issues, i.e. not distinguishing between *category* and *small category*, etc.

Along the same lines, instead of writing $\phi : x \to y$ for subobjects $x : [Q]$ and $y : [P]$, we write $\phi : [Q \subseteq P]$ or even just $[Q \subseteq P]$. This notation also stands for the statement that such a morphism in $\textsc{Sub}(V)$ exists. If $\phi : [Q \subseteq P]$ and $\psi : [P \subseteq Q]$ then ϕ and ψ are mutually inverse, and we write $[Q = P]$. This *equals* sign only indicates an isomorphism $[Q] \cong [P]$, but it is intended to remind us that when $\mathscr{C}$ is a familiar category, $[Q = P]$ means the subobjects are strictly equal. For instance, the groups $0 \oplus \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \oplus 0$ are isomorphic but non-equal subgroups of the Klein 4 group $G = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. They are isomorphic in $\textsc{Grp}$ but their inclusion maps are not isomorphic in $\textsc{Sub}_{\textsc{Grp}}(G)$.

The product of $[Q]$ and $[P]$ in $\textsc{Sub}_{\mathscr{C}}(W)$, if it exists, is called the *intersection* of subobjects in $\mathscr{C}$, and we denote it by $[Q \cap P]$. Thus, $Q \cap P$ is the domain of $[Q] \times [P]$, where $\times$ denotes the product in $\textsc{Sub}_{\mathscr{C}}(W)$. Likewise, the *union* is defined $[Q \cup P] \cong [Q] + [P]$, where $+$ is coproduct in $\textsc{Sub}_{\mathscr{C}}(W)$. Explicitly, these are defined by the universal diagrams:

$$\begin{tikzcd} & {[U]} \arrow[dl] \arrow[d, dashed] \arrow[dr] & \\ {[Q]} & {[Q \cap P]} \arrow[l] \arrow[r] & {[P]} \end{tikzcd} \qquad \begin{tikzcd} {[Q]} \arrow[r] \arrow[dr] & {[Q \cup P]} \arrow[d, dashed] & {[P]} \arrow[l] \arrow[dl] \\ & {[U]} & \end{tikzcd}$$

The following example requires some caution: in $\mathscr{C} = R$-$\textsc{fgfMod}$, $[Q \cap P] \cong [Q] \times [P]$ is the intersection of submodules $[Q]$ and $[P]$, just as one expects. However, $[Q \cup P] \cong [Q] + [P]$ is neither the union of submodules $[Q]$ and $[P]$ (which is not a submodule, hence ill-defined), nor the subobject whose domain is the coproduct of the domains Q and P (which is not only the coproduct, but the biproduct $Q \oplus P$ in $\mathscr{C}$, and more concretely is the direct sum). Rather, it is the R-span of the setwise union of the submodules $[Q]$ and $[P]$.

Unraveling definitions, the intersection can also be defined as a pullback in $\mathscr{C}$, as seen in the diagram on the left of Eq. (5.1) below. It is less immediate to see that the union is a pushout defined in terms of the intersection, when it exists, as seen in the diagram on the right of Eq. (5.1), but the proof is a standard exercise [Joh02; MM94]. Thus, from the perspective of $\mathscr{C}$, union and intersection aren't "dual" notions.[3] This is because we have already introduced some "bias" by considering subobjects as opposed to quotients. One may define dual notions of "co-union" and "co-intersection" in the category $\textsc{Quot}_{\mathscr{C}}(W)$

[3] A manifestation of this non-duality is that lists and streams (which are quite different) over an alphabet A are the inital algebra resp. final coalgebra of the combinatorial species $X \mapsto 1 + A \times X$ [Jac16; Joy81].

of quotients, the full subcategory of the coslice category $W \uparrow \mathscr{C}$ on epimorphisms.

$$
\begin{tikzcd}
U \arrow[dr, dashed] \arrow[drr, bend left] \arrow[ddr, bend right] & & \\
& Q \cap P \arrow[r] \arrow[d] & P \arrow[d] \\
& Q \arrow[r] & V
\end{tikzcd}
\qquad
\begin{tikzcd}
Q \cap P \arrow[r] \arrow[d] & P \arrow[d] \arrow[ddr, bend left] & \\
Q \arrow[r] \arrow[drr, bend right] & Q \cup P \arrow[dr, dashed] & \\
& & U
\end{tikzcd}
\tag{5.1}
$$

The existence of intersections therefore follows from the existence of pullbacks in $\mathscr{C}$, and the existence of unions follows from the existence of pullbacks *and* pushouts in $\mathscr{C}$.

Our primary interest is in categories $\mathscr{C}$ that support a good theory of symplectic forms. As we will later see, such categories are, among other things, preabelian. These categories have all finite limits and finite colimits, in particular finite pullbacks and finite pushouts. Therefore if $\mathscr{C}$ is preabelian, then $\textsc{Sub}_{\mathscr{C}}(W)$ is a lattice, and one finds that its top and bottom elements $[W]$ and $[0]$, respectively. Note that in our examples of interest, $\textsc{Sub}_{\mathscr{C}}(W)$ is not Cartesian closed, which implies $\mathscr{C}$ is not a topos (despite being fairly close).

Theorem 5.1.1 *Let $\mathscr{C}$ be a preadditive category with finite pullbacks and finite pushouts. Let $W \in \mathsf{ob}(\mathscr{C})$ and consider subobjects $[Q], [P] \in \mathsf{ob}(\textsc{Sub}_{\mathscr{C}}(W))$. Then $[W = Q \oplus P]$ if and only if $[Q \cup P = Q \oplus P]$ and $[Q \cap P = 0]$.*

Recall that there are two standard formulations the direct sum of R-modules, which are easily proved to be isomorphic. First, the *external direct sum* $Q \oplus P$ of R-modules Q and P is defined by giving the canonical R-module structure to the Cartesian product set $Q \times P = \{(q, p) \,|\, q \in Q \text{ and } p \in P\}$. Second, an R-module W is called the *internal direct sum* if they sum to the whole, i.e. $W = \{q + p \,|\, q \in Q \text{ and } p \in P\}$, and have trivial intersection $Q \cap P = 0$. The definition of the categorical biproduct $\oplus$ can be seen as an abstraction of the external direct sum. This theorem generalizes (internalizes) the equivalence of these two formulations of the direct sum under suitable hypotheses.[4]

Proof Assume $[W = Q \oplus P]$, i.e. that that $Q \oplus P \cong W$ in $\mathscr{C}$. We will show that $[Q \oplus P = Q \cup P]$. Uniqueness of inclusions implies that the composites of the arrows in the following

[4] Plenty of other such "internal vs. external" definitions exist, but the theorem may not apply, since $\mathscr{C}$ might not be preadditive with pushouts and pullbacks, e.g. disjoint union of sets, direct product of groups.

diagram are just the biproduct injections $i_1 : Q \to Q \oplus P$ and $i_2 : P \to Q \oplus P$:

$$\begin{tikzcd} [Q] \arrow[r] & [Q \cup P] \arrow[d] & [P] \arrow[l] \\ & [Q \oplus P] & \end{tikzcd}$$

Now take the underlying diagram in $\mathscr{C}$, and put in the biproduct projection maps:

$$\begin{tikzcd} Q \arrow[r, "j_1"] & Q \cup P \arrow[d, "u"] & P \arrow[l, "j_2"'] \\ & Q \oplus P \arrow[ul, "\pi_1"] \arrow[ur, "\pi_2"'] & \end{tikzcd}$$

By the biproduct property and preadditivity, $\mathsf{id}_{Q\oplus P} = uj_1\pi_1 + uj_2\pi_2 = u(j_1\pi_1 + j_2\pi_2)$, so u is a monic split epimorphism, hence an isomorphism in $\mathscr{C}$. It is of course also an isomorphism in $\textsc{Sub}_{\mathscr{C}}(V)$, that is, $[Q \cup P = Q \oplus P]$. To see that $[Q \cap P = 0]$, use the left square in Eq. (5.1), or since we have established that $[Q \cup P = Q \oplus P]$, the right square. With morphism names as in the following diagram (left side), left-multiply both sides of $i_1\tau_1 = i_2\tau_2$ by π_1 to get $\tau_1 = \pi_1 i_1 \tau_1 = \pi_1 i_2 \tau_2 = 0$ by the biproduct relations.

$$\begin{tikzcd} Q \cap P \arrow[r, "\tau_2"] \arrow[d, "\tau_1"'] & P \arrow[d, "i_2"] \\ Q \arrow[r, "i_1"'] & Q \oplus P \end{tikzcd} \quad \Longrightarrow \quad \begin{tikzcd} Q \cap P \arrow[r, "\tau_2"] \arrow[d, "\tau_1"'] & P \arrow[d, "i_2"] \\ Q & Q \oplus P \arrow[l, "\pi_1"] \end{tikzcd}$$

Since $\tau_1 = 0$, it follows that $[Q \cap P = 0]$. Conversely, suppose $[Q \cup P = W]$ and $[Q \cap P = 0]$. Then right diagram of Eq. (5.1) expresses that $W \cong Q + P$. Since $\mathscr{C}$ is prebelian, $Q + P \cong Q \oplus P$, and so $[W = Q \oplus P]$. ■

5.1.2 Global elements

One often finds that objects are "determined by their elements" in a given category. For instance, *extensionality* states that sets are determined by their elements. On the other hand, schemes do not have this property, (c.f. Example 4 below). We rigorously formulate the property of global elements being sufficient, and in doing so, we find that it is not a property of individual objects in a category, but is additional structure on $\mathscr{C}$ that applies collectively to all the objects of $\mathscr{C}$. To apply the result to a particular category $\mathscr{C}$, one must first identify an appropriate enrichment category $\mathscr{K}$ and forgetful functor $U : \mathscr{K} \to \textsc{Set}$. Typically, both U and the plain (unenriched) Hom functor $\mathsf{El} = \mathsf{Hom}_{\mathscr{C}}(\top, -) : \mathscr{C} \to \textsc{Set}$ are easily recognized to be faithful. In fact, faithfulness of El, which one might call *morphism extensionality with respect to global elementhood*, likely encapsulates one's intuitive understanding that "objects are determined by their elements" in a given category:

$$\forall x \in_\top X \,.\, fx = gx \qquad \Longrightarrow \qquad f = g \tag{5.2}$$

Here we have used the notation $x \in_\top X$ to refer to a morphism $x : \top \to X$. If Eq. (5.2) holds, each identity morphism id_X is "determined by its values" $\mathsf{id}_X x = x$ on global elements $x \in_\top X$. Since a morphism $f = (\mathsf{dom}\, f, \mathsf{codom}\, f, \mathsf{data}\, f)$ "remembers" its domain, intuitively we expect X to be "determined by its global elements". One finds, however, that faithfulness of El is not enough. Recall that a functor is full and faithful if and only if it is an embedding. This is the key property that enables proofs in which structure is *reflected* from a codomain category $\mathscr{K}$ back to a domain category $\mathscr{C}$. Intuitively, in order for $\mathscr{K}$ to be a suitable enrichment, the enriched hom functor $\mathsf{el} = \mathsf{hom}_{\mathscr{C}}(\top, -) : \mathscr{C} \to \mathscr{K}$ must be full and faithful.[5] The challenge is then to identify $\mathscr{K}$ and prove the fullness of el.

Let $\mathscr{K}$ be a monoidal category, $\mathscr{C}$ a category enriched over $\mathscr{K}$, and $\top \in \mathsf{ob}(\mathscr{C})$.

Suppose we have a full functor $\mathsf{el} : \mathscr{C} \to \mathscr{K}$ and faithful functors $\mathsf{El} : \mathscr{C} \to \textsc{Set}$ and $U : \mathscr{K} \to \textsc{Set}$, and that these satisfy the following commutative diagram:

$$\begin{tikzcd} \mathscr{C} \arrow[d, "\mathsf{el}"'] \arrow[dr, "\mathsf{El}"] & \\ \mathscr{K} \arrow[r, "U"'] & \textsc{Set} \end{tikzcd} \tag{5.3}$$

[5] In this way, the enrichment category $\mathscr{K}$ will play the same role as plays the category of presheaves $\mathsf{Hom}_{\mathrm{CAT}}(C^{\mathrm{op}}, \textsc{Set})$ in the context of the Yoneda lemma.

Then el is full and faithful. Typically, el is the enriched hom, El is the plain Hom, and U is a forgetful functor:

$$\mathsf{el} = \mathsf{hom}_{\mathscr{C}}(\top, -) : \mathscr{C} \to \mathscr{K} \qquad\qquad \mathsf{El} = \mathsf{Hom}_{\mathscr{C}}(\top, -) : \mathscr{C} \to \textsc{Set} \tag{5.4}$$

If el is the identity functor on $\mathscr{C} = \mathscr{K}$, one says that $\top$ *represents* U. In such a case, as we see in Examples 1-3 below, it still may be that El is not full, and is thus inadequate for our purposes. This is why we replace it by el. In concrete examples, we still expect a bijection between $\mathsf{El}\, X$ and the underlying set of X, and accept that $\top$ represents $U\mathsf{el}$ instead of U.

Example 1 Let $\mathscr{C}$ and $\mathscr{K}$ both be the category of R-modules, with $\top = R$. Let the monoidal product on $\mathscr{K}$ be the tensor product of R-modules, and let el and El be as in Eq. (5.4). The forgetful functor U is faithful since homomorphisms are just functions satisfying a property, and only this property (as opposed to structure) is forgotten. To see that el is full, let $\phi : \mathsf{el}\, X \to \mathsf{el}\, Y$, and define $f : X \to Y$ by $f(x) = \phi(1 \mapsto x)(1)$. As one may check, f is indeed a homomorphism. Then define $\alpha : X \to \mathsf{el}\, X$ and $\beta : \mathsf{el}\, Y \to Y$ by $\alpha(x)(1) = x$ and $\beta(\tilde{y}) = \tilde{y}(1)$, and note that α and β are isomorphisms, and $\beta(\mathsf{el}\, f)\alpha = f = \beta\phi\alpha$, from which we conclude that $\phi = \mathsf{el}\, f$. Therefore el is full. In contrast, El is **not** full, since not every function $\phi : \mathsf{El}\, X \to \mathsf{El}\, Y$ is a homomorphism, and indeed, one may **not** define $f : X \to Y$ by $f(x) = \phi(1 \mapsto x)(1)$ since this is not a homomorphism. El is faithful by noting that Eq. (5.2) holds.

Example 2 Let $\mathscr{C} = \mathscr{K} = \textsc{Top}$, with monoidal product $\times$ (the product) and global stage of definition $\top = \{\cdot\}$ (the singleton). Again the category is self-enriched, and the proof has a similar form. Let $\phi : \mathsf{el}\, X \to \mathsf{el}\, Y$ be continuous with respect to the topology of pointwise convergence, where $\mathsf{el}\, X = \mathsf{hom}_{\mathscr{C}}(\top, X)$. Like before, define $f : X \to Y$ by $f(x) = \phi(\cdot \mapsto x)(\cdot)$. This time one checks that the functions $\alpha : X \to \mathsf{el}\, X$ given by $\alpha(x)(\cdot) = x$ and $\beta : \mathsf{el}\, Y \to Y$ given by $\beta(\tilde{y}) = \tilde{y}(\cdot)$ are homeomorphisms by directly using the definition of pointwise convergence. Then from the fact that $f = \beta\phi\alpha$ it follows that f is continuous, so by the same reasoning, $\phi = \mathsf{el}\, f$, so el is full. Again one finds that El is faithful but not full.

Example 3 Since $\mathscr{C} = \widetilde{\mathrm{LCA}}$ is closed monoidal with respect to the tensor product $\otimes_{\mathbb{Z}}$ of $\mathbb{Z}$-modules, it is enriched over itself, so we use $\mathscr{K} = \mathscr{C}$ and must use $\otimes_{\mathbb{Z}}$ as the monoidal product rather than the (bi)product $\oplus$, making this more like Example 1 than Example 2. Rather than making a direct appeal to the topology, one may use Thm. 2.4.8 to prove fullness. Then the maps $\alpha : X \xrightarrow{\sim} \mathbb{Z} \multimap X = \mathsf{el}\, X$ and $\beta : \mathsf{el}\, Y = \mathbb{Z} \multimap Y \xrightarrow{\sim} Y$ come from the star-autonomous structure. Faithfulness of El is again obvious.

Example 4 The category of schemes $\mathscr{C} = \textsc{Sch}$ is not determined by its global $\textsc{Set}$-elements for a more dire reason. Recall that $T = \mathsf{Spec}\,\mathbb{Z}$ is terminal, that is, for any scheme Y, the set $\mathsf{Hom}_{\textsc{Sch}}(Y, T)$ is a singleton. It follows that the forgetful functor $U : \textsc{Sch} \to \textsc{Set}$ is not representable, since UT is infinite, hence not a singleton. Rather than changing enrichment, one expands the subcategory $\mathscr{Y} \subseteq \mathscr{C}$ of *stages of definition* from the terminal subcategory $\{Y\}$ to the category of affine schemes, $\mathscr{Y} = \textsc{AffSch}$, and considers the *functor of points* $X \mapsto \mathsf{Hom}_{\mathscr{C}}(-, X) : \mathscr{Y}^{\mathrm{op}} \to \textsc{Set}$, which is well-known to be full and faithful. A morphism $x : Y \to X$ in $\mathscr{C}$ is called a *generalized element* of X at *stage of definition* Y. One may always (in any category) extend the scope all the way to $\mathscr{Y} = \mathscr{C}$ in order to obtain a full and faithful functor よ$_{\mathscr{C}}$, the Yoneda embedding.

Finally, we precisely formulate the sufficiency of global elements:

Definition Let $\mathscr{K}$ be a monoidal category, let $\mathscr{C}$ be a $\mathscr{K}$-enriched category, and $\top \in \mathsf{ob}(\mathscr{C})$. Let $\mathsf{el} : \mathscr{C} \to \mathscr{K}$ and $U : \mathscr{K} \to \textsc{Set}$ be functors, and let $\mathsf{El} = \mathsf{Hom}_{\mathscr{C}}(\top, -) : \mathscr{C} \to \textsc{Set}$ be the plain Hom functor. We define $(\mathscr{C}, \mathscr{K}, \top, \mathsf{el}, U)$ to be *determined by its global elements* if $\mathsf{El} = U\mathsf{el}$ (i.e. Eq. (5.3) is satisfied), U and El are faithful, and el is full (and faithful).

Although this is a specification of additional *structure* on $\mathscr{C}$ satisfying some properties, rather than a mere *property*, we prefer a less precise phrasing that is more natural in English: we indicate such a structure by saying that $\mathscr{C}$ is *determined by its global $\mathscr{K}$-elements at stage of definition* $\top$ *with respect to* el *and* U, or use an abbreviation that leaves most of the data implicit, such as: *$\mathscr{C}$ is determined by its global elements.* Lastly, we note an important compatibility with monomorphisms:

Proposition 5.1.2 *Suppose $\mathscr{C}$ is determined by its global $\mathscr{K}$-elements. Then* el *restricts to a faithful functor* $\mathsf{elm} : \mathsf{monos}(\mathscr{C}) \to \mathscr{K}$. *If, furthermore,* el *is essentially surjective, then* $\mathsf{monos}(\mathscr{C})$ *is determined by its global* $\mathsf{monos}(\mathscr{K})$*-elements, and* elm *corestricts to a full, faithful, and essentially surjective functor* $\mathsf{monos}(\mathscr{C}) \xrightarrow{\sim} \mathsf{monos}(\mathscr{K})$.

Recall that a functor F lies in an equivalence of categories (F, G, η, ϵ) if and only if F is full, faithful, and essentially surjective. Thus, the "furthermore" part of Prop. 5.1.2 can be seen as showing that $\mathscr{C} \mapsto \mathsf{monos}(\mathscr{C})$ abides by the principle of equivalence: equivalent categories have equivalent subcategories of monomorphisms. The situation where el lies in an equivalence has more practical significance than is immediately obvious; in Examples 1, 2, and 3 above, we took el to be the self-enriched hom functor $\mathsf{hom}_{\mathscr{C}}(\top, -)$. In each case,

el is seen to be essentially surjective due to the existence of an isomorphism $\alpha : X \xrightarrow{\sim} \mathsf{el}\, X$, in addition to being full and faithful, hence an auto-equivalence. We will apply Prop. 5.1.2 to these and related examples in the next section.

Proof Since $\mathscr{C}$ is determined by its global $\mathscr{K}$-elements, $\mathsf{el} : \mathscr{C} \to \mathscr{K}$ is a full and faithful functor satisfying Eq. (5.3). Consider the restricted functor:

$$\mathsf{elm} = \mathsf{el}|_{\mathsf{monos}(\mathscr{C})} : \mathsf{monos}(\mathscr{C}) \to \mathscr{K} \tag{5.5}$$

Then elm clearly inherits faithfulness from el. If elm is full, we say $\mathscr{C}$ is *determined by its monic $\mathscr{K}$-elements*. Now suppose that el is essentially surjective in addition to being full and faithful. To see that elm is valued in $\mathsf{monos}(\mathscr{K})$ and that the resulting corestriction

$$\mathsf{monos}(\mathscr{C}) \to \mathsf{monos}(\mathscr{K})$$

is full, let $f : X \to Y$ be a morphism in $\mathsf{monos}(\mathscr{C})$. Then let $V \in \mathsf{ob}(\mathscr{K})$, let $t_1, t_2 : V \to \mathsf{elm}\, X$ be morphisms in $\mathscr{K}$ such that $(\mathsf{elm}\, f)t_1 = (\mathsf{elm}\, f)t_2$. Since el is essentially surjective, there exists $W \in \mathsf{ob}(\mathsf{monos}(\mathscr{C}))$ such that $\mathsf{elm}\, W \cong V$, so

$$\mathsf{elm}\, W \cong V \underset{t_2}{\overset{t_1}{\rightrightarrows}} \mathsf{elm}\, X \xrightarrow{\mathsf{elm}\, f} \mathsf{elm}\, Y$$

commutes. Since el is full, there exist $x_1, x_2 : W \to X$ in $\mathscr{C}$ such that $t_i = \mathsf{elm}\, x_i$, and since elm is faithful, the following diagram commutes:

$$W \underset{x_2}{\overset{x_1}{\rightrightarrows}} X \xrightarrow{f} Y$$

Finally, since f is monic, $x_1 = x_2$, and so $t_1 = t_2$, and is monic. Lastly, elm inherits essential surjectivity because monos defines a wide subcategory. ■

As we will see, there are far reaching consequences when a category is determined by its global elements. As one might expect, this "property" is invoked in a similar way as the Yoneda embedding: one does a calculation involving the hom objects and then *reflects* the calculation back through the embedding, in this case el. In such calculations, we will not get carried away in abstraction by *internalizing* arguments about global elements of the enriched hom objects themselves (internal morphisms), nor will be fully pedantic about enriched functors, but we note that making such changes would just be a formality anyway. Moreover, such detail is not really required for our enrichment categories of interest, since they are concrete. Enrichment, however, is required to apply the results of Ch. 6 to our categories of interest.

5.1.3 Monic global elements and the subobject axiom

Let $\mathscr{C}$ be a category and let $\top \in \mathsf{ob}(\mathscr{C})$.[6] We write $p \in_W P$ to indicate a morphism $p : W \to P$, that is, a *generalized element* at stage of definition $W \in \mathsf{ob}(\mathscr{C})$. A generalized element at stage of definition $\top$ is called a *global element*. In the previous section we considered the global elements of an object P, which make up the set $\mathsf{Hom}_{\mathscr{C}}(\top, P)$. This is somewhat analogous to the situation of the Yoneda embedding, where one considers generalized elements at all stages of definition W, which are conglomerated into a presheaf $\mathsf{Hom}_{\mathscr{C}}(-, P)$. The theory of symplectic forms ends up involving a delicate interplay between *monic global elements* and *monic generalized elements*, which are just global resp. generalized elements in the subcategory of monomorphisms, $\mathsf{monos}(\mathscr{C})$. The *subobject axiom*, which we introduce in this section, turns out to hold under the assumption that $\mathscr{C}$ is *determined by its monic global elements*, by which we mean that $\mathsf{monos}(\mathscr{C})$ is determined by its global elements. As the examples in the previous section illustrate, in practice we must therefore consider enriched categories in order to apply this result, and indeed this prompts us to consider an enriched version of the subobject axiom. Alternately, the plain (unenriched) subobject axiom can be verified directly in our categories of interest.

We procede in stages. First we characterize the *plain subobject axiom* in four equivalent ways. We would like to base our definition of the enriched subobject axiom on one of these. As an intermediate step, we define the *enriched slice axiom*, which becomes the desired *enriched subobject axiom* upon substituting $\mathsf{monos}(\mathscr{C})$ in place of $\mathscr{C}$. It is cleaner and more general to state and prove that the sufficiency of global elements entails the slice axiom, Thm. 5.1.4, and then to substitute $\mathsf{monos}(\mathscr{C})$ to get the desired corollary about subobjects. This is all possible due to a known construction by which if $\mathscr{C}$ is enriched in $\mathscr{K}$, then the slice category $\mathscr{C} \downarrow V$ is also enriched in $\mathscr{K}$. Then since $\textsc{Sub}_{\mathscr{C}}(V) = \mathsf{monos}(\mathscr{C}) \downarrow V$, the corollary pertains to when $\mathscr{C}$ is determined by its monic global $\mathscr{K}$-elements.

Thus, the story begins with a full and faithful functor el and a faithful functor U, whose composite is the plain Hom functor $\mathsf{El} = \mathsf{Hom}_{\mathscr{C}}(\top, -)$:

$$\begin{tikzcd} \mathscr{C} \arrow[d, "\mathsf{el}"'] \arrow[dr, "\mathsf{El} = \mathsf{Hom}_{\mathscr{C}}(\top, -)"] & \\ \mathscr{K} \arrow[r, "U"'] & \textsc{Set} \end{tikzcd} \tag{5.6}$$

[6] We use the notation $\top$ because in later sections, it will be the unit of a magmal product $\otimes$ on $\mathscr{C}$; it should not be confused with the top element $[V]$ of the subobject preorder $\textsc{Sub}_{\mathscr{C}}(V)$ for some $V \in \mathsf{ob}(\mathscr{C})$.

Given $P \in \mathsf{ob}(\mathscr{C})$, a set $\mathcal{P}$ of morphisms $W \to P$ (with the same codomain P but various domains W) is called *jointly epic over* $V \in \mathsf{ob}(\mathscr{C})$ if for all $y, y' : P \to V$, whenever $yp = y'p$ for all $p \in \mathcal{P}$ it follows that $y = y'$. $\mathcal{P}$ is called *jointly epic* if it is so for all $V \in \mathsf{ob}(\mathscr{C})$. Then $W \in \mathsf{ob}(\mathscr{C})$ is a *generator* (also called a *separator*) for $\mathscr{C}$ if for all $P \in \mathsf{ob}(\mathscr{C})$, the set $\mathsf{Hom}_{\mathscr{C}}(W, P)$ is jointly epic. Equivalently, W is a generator if $\mathsf{Hom}_{\mathscr{C}}(W, -)$ is faithful.

Since $\mathrm{S{\scriptsize UB}}_{\mathscr{C}}(V)$ is a preoder, $\mathsf{Hom}_{\mathrm{S{\scriptsize UB}}_{\mathscr{C}}(V)}([\top], -)$ is faithful. Again, however, we find that faithfulness is not enough:

Subobject axiom (plain) Consider subobjects of some $V \in \mathsf{ob}(\mathscr{C})$. A pair of subobjects $x : [Q]$ and $y : [P]$ *satisfies the subobject axiom* at stage of definition $\top$ if the following equivalent conditions hold. We say that V *satisfies the subobject axiom* at $\top$ if all its pairs of subobjects do, and that $\mathscr{C}$ *satisfies the subobject axiom* at $\top$ if all its objects V do.

(i) If for all monic $p \in_\top P$ there exists monic $q \in_\top Q$ with $xq = yp$, then $[P \subseteq Q]$:

$$\begin{tikzcd}
& \top \arrow[dl, "\forall p"'] \arrow[dr, "\exists q"] & \\
P \arrow[rr, dashed] \arrow[dr, "y"'] & & Q \arrow[dl, "x"] \\
& V &
\end{tikzcd} \tag{5.7}$$

(ii) If there exists a function:

$$A_\top : \mathsf{Hom}_{\mathsf{monos}(\mathscr{C})}(\top, P) \to \mathsf{Hom}_{\mathsf{monos}(\mathscr{C})}(\top, Q)$$

such that $xq = yp$ for all monic $p \in_\top P$, where $q = A_\top p$, then $[P \subseteq Q]$.

(iii) If for all $\ell : [\top]$, there exists a function:

$$\mathsf{Hom}_{\mathrm{S{\scriptsize UB}}_{\mathscr{C}}(V)}([\top], [P]) \to \mathsf{Hom}_{\mathrm{S{\scriptsize UB}}_{\mathscr{C}}(V)}([\top], [Q])$$

then $[P \subseteq Q]$.

(iv) For all $\ell : [\top]$, the functor $\mathsf{Hom}_{\mathrm{S{\scriptsize UB}}_{\mathscr{C}}(V)}([\top], -)$ is full, (hence full and faithful).

It is straightforward to check that (i-iv) are equivalent under the (ambient) axiom of choice. In most concrete categories of interest, subobjects are defined by characterization (i), but without imposing that the (global) elements involved be monic: if Q contains all the (global) elements of P, then $P \subseteq Q$. As we discuss in the example below, the requirement that p and q be monic throws a wrench in things, but nevertheless, the subobject axiom as stated here is required in order to prove a theorem (namely, Thm. 6.8.3). For the enriched slice axiom, we modify formulation (ii):

Slice axiom (enriched) Let $\mathscr{C}$ be a $\mathscr{K}$-enriched category, let $\top, V \in \mathsf{ob}(\mathscr{C})$, and let el, El, and U be as in Eq. (5.6). Let $x : Q \to V$ and $y : P \to V$ be morphisms in the underlying plain category of $\mathscr{C}$, hence objects in the $\mathscr{K}$-enriched slice category $\mathscr{C} \downarrow V$. Then x and y *satisfy the slice axiom* if the following property holds:

Whenever there exists a morphism

$$\alpha_\top : \mathsf{el}\, P \to \mathsf{el}\, Q$$

in $\mathscr{K}$ such that $xq = yp$ for all $p \in_\top P$, where $q = A_\top p$, given in terms of the function

$$A_\top = U\alpha_\top : \mathsf{El}\, P \to \mathsf{El}\, Q$$

it follows that there exists a morphism $f : P \to Q$ such that $y = xf$.

Finally, the enriched subobject axiom is obtained by substituting $\mathsf{monos}(\mathscr{C})$ in place of $\mathscr{C}$ in the enriched slice axiom:

Subobject axiom (enriched) Let $\mathsf{monos}(\mathscr{C})$ be a $\mathscr{K}$-enriched category and let $\top, V \in \mathsf{ob}(\mathscr{C})$. Let $\mathsf{elm} : \mathsf{monos}(\mathscr{C}) \to \mathscr{K}$ be a full and faithful functor, and let $U : \mathscr{K} \to \textsc{Set}$ be a faithful functor satisfying $\mathsf{Elm} = U\mathsf{elm}$, where $\mathsf{Elm} = \mathsf{Hom}_{\mathsf{monos}(\mathscr{C})}(\top, -) : \mathsf{monos}(\mathscr{C}) \to \textsc{Set}$ is the plain Hom functor. Let $x : [Q]_V$ and $y : [P]_V$ be subobjects, that is, morphisms in the underlying plain category of $\mathsf{monos}(\mathscr{C})$ with the same codomain V, hence objects in the $\mathscr{K}$-enriched subobject category $\textsc{Sub}_{\mathscr{C}}(V) = \mathsf{monos}(\mathscr{C}) \downarrow V$. Then $[Q]$ and $[P]$ *satisfy the subobject axiom* if the following property holds:

Whenever there exists a morphism

$$\alpha_\top : \mathsf{elm}\, P \to \mathsf{elm}\, Q$$

in $\mathscr{K}$ such that $xq = yp$ for all **monic** $p \in_\top P$, where $q = A_\top p$, given in terms of the function

$$A_\top = U\alpha_\top : \mathsf{Elm}\, P \to \mathsf{Elm}\, Q$$

it follows that $[P \subseteq Q]$.

As with the plain subobject axiom, the enriched slice axiom and the enriched subobject axiom also have variants that apply to all pairs of slices/subobjects of an object V, or to the entire (enriched) category. It is clear that:

Proposition 5.1.3 *If $\mathscr{C}$ satisfies the plain subobject axiom, then it also satisfies the $\mathscr{K}$-enriched subobject axiom for any $(\mathscr{K}, \mathsf{el}, U)$.* ■

Finally, the sufficiency of global elements relates as follows:

Theorem 5.1.4 *If $\mathscr{C}$ is determined by its global $\mathscr{K}$-elements at $\top$, then $\mathscr{C}$ satisfies the $\mathscr{K}$-enriched slice axiom at $\top$.*

Proof Let $V \in \mathsf{ob}(\mathscr{C})$, $x : [Q]_V$, and $y : [P]_V$, and assume there exists a morphism

$$\alpha_\top : \mathsf{el}\, P \to \mathsf{el}\, Q$$

in $\mathscr{K}$ such that for all $p \in_\top P$, $xq = yp$, where $q = A_\top p$ and $A_\top = U\alpha_\top$. Since el is full, there exists $f : P \to Q$ in the underlying plain category of $\mathscr{C}$ such that $\alpha_\top = \mathsf{el}\, f$. Then:

$$q = A_\top p = (U\alpha_\top)(p) = U(\mathsf{el}\, f)(p) = (\mathsf{El}\, f)(p) = fp$$

It follows that $yp = xq = xfp$. Since El is faithful, for all $X, Y \in \mathsf{ob}(\mathscr{C})$, $\mathsf{El}\, X$ is jointly epic over Y. So $\mathsf{El}\, P$ is jointly epic over V, and the equation $yp = xfp$ yields $y = xf$. ■

Corollary 5.1.5 *If $\mathscr{C}$ is determined by its monic global $\mathscr{K}$-elements at $\top$, then $\mathscr{C}$ satisfies the $\mathscr{K}$-enriched subobject axiom at $\top$.*

Proof Substitute $\mathsf{monos}(\mathscr{C})$ in place of $\mathscr{C}$ in Thm. 5.1.4. ■

The following example illustrates these results.

Example Let $\mathscr{C} = R\text{-}\textsc{Mod}$. We noted previously that $\mathscr{C}$ is not determined by its plain elements, but is determined by its $\mathscr{K}$-enriched elements where $\mathsf{el} = \mathsf{hom}_{\mathscr{C}}(\top, -) : \mathscr{C} \to \mathscr{K}$ is the enriched hom functor and $\mathscr{C} = \mathscr{K}$. We can see that $\mathscr{C}$ satisfies the plain subobject axiom if and only if R is a field:

Suppose R is a field. Fix a vector space V and subspaces P and Q. Assume that for all $p : R \to P$ there exists $q : R \to Q$ such that $xq = yp$. If $P = 0$ then clearly $P \subseteq Q$ so assume otherwise, and let $\tilde{p} \in P \setminus \{0\}$. Then the map $p : R \to P$ given by $1 \mapsto p$ is injective (monic), so there exists $q : R \to Q$ with $xq = yp$, and so $\tilde{p} = p(1) = q(1) \in Q$, so $P \subseteq Q$. Now suppose R is not a field and let $P = R/I$ where I is a proper ideal. Then the kernel of any map $p : R \to P$ contains I, hence is non-injective. Then take $Q = R$ and $V = P \oplus Q$. Then vacuously, for all monic $p : R \to P$ there exists monic $q : R \to Q$ such that $xq = yp$, but there is no map $f : Q \to P$ satisfying $q = fp$ since q is monic and p is not.

Likewise, LCA is not determined by its plain monic global elements. On the other hand, in each case, $\mathscr{C}$ is determined by its $\mathsf{monos}(\mathscr{K})$-enriched monic global elements by Prop. 5.1.2, and so by Cor. 5.1.5, $\mathscr{C}$ satisfies the $\mathsf{monos}(\mathscr{K})$-enriched subobject axiom. Unfortunately, we later require the plain subobject axiom (in the proof of Thm. 6.8.3). It might be that Thm. 6.8.3 has an enriched variant, but we save this for future work.

We now consider the generalized element version. Recall that by the Yoneda lemma,

$$\begin{aligned} よ_{\mathscr{C}} : \mathscr{C} &\to [\mathscr{C}^{\mathrm{op}}, \textsc{Set}] \\ X &\mapsto \mathsf{Hom}_{\mathscr{C}}(-, X) : \mathscr{C}^{\mathrm{op}} \to \textsc{Set} \end{aligned}$$

is a full and faithful functor, where $[-,-] : \mathrm{CAT}^{\mathrm{op}} \times \mathrm{CAT} \to \mathrm{CAT}$ is the internal hom of the ambient CAT, (c.f. Appx. E. Now if $\mathscr{C}$ is enriched in $\mathscr{K}$ with enriched hom functor $\mathsf{hom}_{\mathscr{C}} : \mathscr{C}^{\mathrm{op}} \times \mathscr{C} \to \mathscr{K}$, and equipped with a faithful functor $U : \mathscr{K} \to \textsc{Set}$, then let us call

$$\begin{aligned} \mathsf{y} : \mathscr{C} &\to [\mathscr{C}^{\mathrm{op}}, \textsc{Set}] \\ X &\mapsto \mathsf{hom}_{\mathscr{C}}(-, X) : \mathscr{C}^{\mathrm{op}} \to \mathscr{K} \end{aligned}$$

the *enriched Yoneda embedding* if the following diagram commutes:

$$
\begin{tikzcd}
\mathscr{C} \arrow[d, "\mathsf{y}"'] \arrow[drr, "\text{よ}_{\mathscr{C}}"] & & \\
[\mathscr{C}^{\mathrm{op}}, \mathscr{K}] \arrow[rr, "{[\mathscr{C}^{\mathrm{op}}, U]}"'] & & [\mathscr{C}^{\mathrm{op}}, \mathrm{SET}]
\end{tikzcd}
\tag{5.8}
$$

Since U is faithful, so is $[\mathscr{C}^{\mathrm{op}}, U]$. Since $\text{よ}_{\mathscr{C}}$ is full, so is $[\mathscr{C}^{\mathrm{op}}, U]$. Then since $\text{よ}_{\mathscr{C}}$ and $[\mathscr{C}^{\mathrm{op}}, U]$ are each full and faithful, so is y. The following theorem shows that, owing to the Yoneda embedding, the generalized element analog of the enriched slice axiom is a tautology, and hence so is that of the subobject axiom by substituting $\mathsf{monos}(\mathscr{C})$.

Theorem 5.1.6 *Let $\mathscr{C}$ be a $\mathscr{K}$-enriched category, let $U : \mathscr{K} \to \mathrm{SET}$ be a faithful functor, and suppose the enriched Yoneda embedding y exists, i.e. Eq. (5.8) commutes. Let $V \in \mathsf{ob}(\mathscr{C})$, and let $x : Q \to V$ and $y : P \to V$ be morphisms in the underlying plain category of $\mathscr{C}$. Then if there exists a natural transformation*

$$\alpha : \mathsf{hom}_{\mathscr{C}}(-, P) \Rightarrow \mathsf{hom}_{\mathscr{C}}(-, Q) : \mathscr{C}^{\mathrm{op}} \to \mathscr{K} \tag{5.9}$$

such that $xq = yp$ for all W and $p \in_W P$, where $q = A_W p$ and $A = U\alpha$, then there exists a morphism $f : P \to Q$ such that $y = xf$.

Interestingly, if the theorem applies (i.e. there exists α such that...) in the enriched sense, then one may shed the enrichment by replacing $\mathscr{K}$, y, U, and α by SET, $\text{よ}_{\mathscr{C}}$, $\mathsf{id}_{\mathrm{SET}}$, and A, respectively, and apply it in the plain sense. If our goal is to apply the theorem in the plain sense, then an enrichment as in Thm. 5.1.6 serves as a certificate. This is sort of reversed from the global element version. In practice, the plain version may be easier to certify directly, which suggests that enrichment is more relevant to the global element setting.

Proof Since the *plain* Yoneda embedding is full, $A = \text{よ}_{\mathscr{C}} f$ for some $f : P \to Q$. For each W, A_W is the function $p \mapsto fp$. By assumption, $q = A_W p$, so the top triangle of the following diagram commutes:

$$
\begin{tikzcd}
& W \arrow[dl] \arrow[dr] & \\
P \arrow[rr, dashed] \arrow[dr] & & Q \arrow[dl] \\
& V &
\end{tikzcd}
\tag{5.10}
$$

In other words, $q = fp$. Since the square also commutes, $yp = xq = xfp$. In particular, plugging in $W = P$ and $p = \mathsf{id}_P$, we find that $y = xf$, as claimed. ■

Now, Thm. 5.1.6 trivializes in the case of plain subobjects. Then it states that if for all $[W]$, $[W \subseteq P]$ implies $[W \subseteq Q]$, then $[P \subseteq Q]$. This is obvious by substituting $[P]$ in for $[W]$. The enriched subobject case (which by the remarks above, entails the plain version) also undergoes a simplification, in which we find that naturality is automatic:

Lemma 5.1.7 *Let $\mathsf{monos}(\mathscr{C})$ be a $\mathscr{K}$-enriched category and let $U : \mathscr{K} \to \mathrm{S{\small ET}}$ be a faithful functor admitting an enriched Yoneda embedding. Let $V \in \mathsf{ob}(\mathscr{C})$, and consider subobjects $[Q]$ and $[P]$. Then and suppose that for all $[W]$ there exists a morphism*

$$\alpha_W : \mathsf{hom}_{\mathrm{S{\small UB}}_{\mathscr{C}}(V)}([W],[P]) \to \mathsf{hom}_{\mathrm{S{\small UB}}_{\mathscr{C}}(V)}([W],[Q])$$

in $\mathscr{K}$. Then α_W is natural in W.

If Lem. 5.1.7 applies, then Thm. 5.1.6 applies.

Proof For each W, consider the function:

$$A_W = U\alpha_W : \mathsf{Hom}_{\mathrm{S{\small UB}}_{\mathscr{C}}(V)}([W],[P]) \to \mathsf{Hom}_{\mathrm{S{\small UB}}_{\mathscr{C}}(V)}([W],[Q])$$

Since $\mathrm{S{\small UB}}(V)$ is a preorder, each Homset has cardinality 1 or 0, from which it follows by uniqueness of the terminal object (singleton $\bullet$) or uniqueness of the initial object (emptyset $\circ$) in $\mathrm{S{\small ET}}$, depending on the scenario, that any diagram of the following form commutes:

$$\begin{tikzcd}
\mathsf{Hom}_{\mathrm{S{\small UB}}_{\mathscr{C}}(V)}([W],[P]) \arrow[r] \arrow[d] & \mathsf{Hom}_{\mathrm{S{\small UB}}_{\mathscr{C}}(V)}([W],[Q]) \arrow[d] \\
\mathsf{Hom}_{\mathrm{S{\small UB}}_{\mathscr{C}}(V)}([W'],[P]) \arrow[r] & \mathsf{Hom}_{\mathrm{S{\small UB}}_{\mathscr{C}}(V)}([W'],[Q])
\end{tikzcd} \tag{5.11}$$

For reference, the relevant ($[W' \subseteq W]$) and possible scenarios for diagram Eq. (5.11) are:

$$\begin{array}{ccccc}
 & & \begin{tikzcd}[row sep=small, column sep=small] \circ \arrow[r] \arrow[d] & \circ \arrow[d] \\ \bullet \arrow[r] & \bullet \end{tikzcd} & & \\
\begin{tikzcd}[row sep=small, column sep=small] \bullet \arrow[r] \arrow[d] & \bullet \arrow[d] \\ \bullet \arrow[r] & \bullet \end{tikzcd} &
\begin{tikzcd}[row sep=small, column sep=small] \circ \arrow[r] \arrow[d] & \bullet \arrow[d] \\ \bullet \arrow[r] & \bullet \end{tikzcd} & &
\begin{tikzcd}[row sep=small, column sep=small] \circ \arrow[r] \arrow[d] & \circ \arrow[d] \\ \circ \arrow[r] & \bullet \end{tikzcd} &
\begin{tikzcd}[row sep=small, column sep=small] \circ \arrow[r] \arrow[d] & \circ \arrow[d] \\ \circ \arrow[r] & \circ \end{tikzcd} \\
 & & \begin{tikzcd}[row sep=small, column sep=small] \circ \arrow[r] \arrow[d] & \bullet \arrow[d] \\ \circ \arrow[r] & \bullet \end{tikzcd} & &
\end{array}$$

The remaining cases are irrelevant, because $[W' \not\subseteq W]$, or vacuous, because there is no function $\bullet \to \circ$. So A is natural. Finally, since U is faithful, α is natural. ■

If $\mathscr{C}$ is preabelian, it has a zero object 0 and is Ab-enriched. We take note of the following well-formed axiom, though we have no occasion to use it in any proof.

Global element inhabitation axiom If $[Q \neq 0]$ then there exists monic $q \in_\top Q$.

Note that every monomorphism is nonzero.

The generalized element version is again a tautology: a nonzero subobject $x : [Q]$ is automatically inhabited by a nonzero $q \in_W Q$ at *some* nonzero stage of definition W by the Ab-enriched Yoneda lemma, for otherwise, $よ_{\mathscr{C}} x$ would be the zero-valued functor, which would imply $x = 0$. Since $\mathscr{C}$ is preabelian, any nonzero morphism q may be factored as mq' with m monic, hence nonzero. Therefore, having a nonzero generalized element is equivalent to having a monic generalized element.

5.2 Magmal categories

In this section, we work out properties of de Morgan duality and nuclearity. Many of the proofs use the Yoneda embedding, and others hold only if the category is determined by its enriched global elements. The currying formulas and notation presented in Sec. 5.2.1 will be used throughout the rest of the thesis.

5.2.1 Currying

Let $(\mathscr{C}, \otimes)$ be a magmal category. This is more or less a monoidal category, but without associator or unit. See Appx. C for details. If the functor $- \otimes Y : \mathscr{C} \to \mathscr{C}$ has a right adjoint $Y \multimap - : \mathscr{C} \to \mathscr{C}$ (called the *left internal hom*), we say that $(\mathscr{C}, \otimes)$ is *left closed*. Likewise, if $Y \otimes - : \mathscr{C} \to \mathscr{C}$ has a right adjoint $- \multimapinv Y : \mathscr{C} \to \mathscr{C}$, we say that $(\mathscr{C}, \otimes)$ is *right closed*. If both conditions hold, $(\mathscr{C}, \otimes)$ is called *biclosed*. The adjunctions in question are called the *tensor-hom adjunctions* or *currying adjunctions*:

$$\underset{\text{left currying}}{- \otimes Y \dashv Y \multimap -} \qquad \text{and} \qquad \underset{\text{right currying}}{Y \otimes - \dashv - \multimapinv Y}$$

The notations $X \multimap Y$ and $Y \multimapinv X$, and sometimes the terms "left" and "right", are swapped when going from the physics convention, which we use, and the math convention, which we do not, c.f. Appx. F.2. The symbols $\multimap$ and $\multimapinv$ come from linear logic, and for this reason they usually connote *linearity*. Nevertheless, we use them to denote the left and right internal hom in any biclosed magmal category, simply because they are a standard notation for the internal hom that is *one-sided*. In contrast, the notation $[X, Y]$, often used in symmetric monoidal categories, is not suitable for the non-braided case. We occasionally use the notation Y^X in Cartesian monoidal categories, which are always symmetric. In Set and finSet, for example, Y^X is the set of functions from X to Y.

Assume $(\mathscr{C}, \otimes)$ is biclosed. The tensor-hom adjunctions are mediated by natural bijections:

$$\mathsf{leftcurry}^Y_{X,Z} : \mathsf{Hom}_{\mathscr{C}}(X \otimes Y, Z) \xrightarrow{\sim} \mathsf{Hom}_{\mathscr{C}}(X, Y \multimap Z)$$
$$\mathsf{rightcurry}^Y_{X,Z} : \mathsf{Hom}_{\mathscr{C}}(Y \otimes X, Z) \xrightarrow{\sim} \mathsf{Hom}_{\mathscr{C}}(X, Z \multimapinv Y)$$

By definition, naturality is in X and Z. Rather than introducing a plethora of morphism symbols $f, g, h, \cdots$, we often reuse symbols for morphisms of various different types; the types can be inferred from the situation. We also use the following shorthands for currying:

$$\lceil f \rceil = \mathsf{leftcurry}^{Y}_{X,Z}(f) \qquad \lfloor f \rfloor = \mathsf{rightcurry}^{Y}_{X,Z}(f)$$
$$\rceil g \lceil = (\mathsf{leftcurry}^{Y}_{X,Z})^{-1}(g) \qquad \rfloor g \lfloor = (\mathsf{rightcurry}^{Y}_{X,Z})^{-1}(g)$$

We do not assume an associative structure for $\otimes$, so technically the shorthand is well-defined, but we do sometimes equip a unital structure and elide the unitors, which introduces ambiguity. For instance, if $f : X \otimes Y \to Z$, then $\lceil f \rceil$ may either refer to the morphism of type $X \to Y \multimap Z$ or that of type $\top \to (X \otimes Y) \multimap Z$. It will always be clear from the situation which is intended.

The unit of each currying adjunction is called *coevaluation* and the counit is called *evaluation*. This unfortunate swap involving the *co-* prefix is present in both the math and physics conventions, and the terms *unit* and *counit* (of an adjunction) are firmly established in category theory [Mac78]. Coevaluation and evaluation are natural in X and Z. By the formulas for unit and counit of an adjunction in CAT (c.f. Appx. E), we have:

$$\lceil \mathsf{id}_{X\otimes Y} \rceil = \mathsf{leftcoeval}^{Y}_{X} : X \to Y \multimap (X \otimes Y) \qquad \rceil \mathsf{id}_{Y \multimap Z} \lceil = \mathsf{lefteval}^{Y}_{Z} : (Y \multimap Z) \otimes Y \to Z$$
$$\lfloor \mathsf{id}_{Y\otimes X} \rfloor = \mathsf{rightcoeval}^{Y}_{X} : X \to (Y \otimes X) \multimapinv Y \qquad \rfloor \mathsf{id}_{Z \multimapinv Y} \lfloor = \mathsf{righteval}^{Y}_{Z} : Y \otimes (Z \multimapinv Y) \to Z$$

We caution that $\mathsf{leftcurry}^{Y}_{X,Z}$ is a morphism-valued *function*, which takes a morphism of $\mathscr{C}$ as input, whereas $\mathsf{lefteval}^{Y}_{X}$ is itself a morphism in $\mathscr{C}$. The adjunct formulas read:

$$\begin{aligned}
f &= \mathsf{lefteval}^{Y}_{Z}(\lceil f \rceil \otimes Y) : X \otimes Y \to Z && \text{left adjunct formula for } -\otimes Y \dashv Y \multimap - \\
\lceil f \rceil &= (Y \multimap f)\mathsf{leftcoeval}^{Y}_{X} : X \to Y \multimap Z && \text{right adjunct formula for } -\otimes Y \dashv Y \multimap - \\
f &= \mathsf{righteval}^{Y}_{Z}(Y \otimes \lfloor f \rfloor) : Y \otimes X \to Z && \text{left adjunct formula for } Y \otimes - \dashv - \multimapinv Y \\
\lfloor f \rfloor &= (f \multimapinv Y)\mathsf{rightcoeval}^{Y}_{X} : X \to Z \multimapinv Y && \text{right adjunct formula for } Y \otimes - \dashv - \multimapinv Y
\end{aligned}$$

We use *whiskering* notation, so for instance, $\lceil f \rceil \otimes Y$ is shorthand for $\lceil f \rceil \otimes \mathsf{id}_Y$. (See Eq. (B.8) for details.) Next, we have the *currying formulas*, which relate currying and composition:

$$\lceil f(h \otimes Y) \rceil = \lceil f \rceil h \qquad \lfloor f(Y \otimes h) \rfloor = \lfloor f \rfloor h \tag{5.12}$$
$$(X \multimap g)\lceil f \rceil = \lceil g f \rceil \qquad (g \multimapinv X)\lfloor f \rfloor = \lfloor g f \rfloor \tag{5.13}$$

These formulas follow immediately from the adjunct formulas above. By the Parameter Theorem (IV.7 Theorem 3 of [Mac78]), the hom bijections of the currying adjunctions (and hence the evaluation and coevaluation maps) are natural not just in X and Z, but also in Y.[7] For left currying, this means that for all $g : W \to Y$, the following diagram commutes:

$$\begin{tikzcd}
\mathsf{hom}_{\mathscr{C}}(X \otimes Y, Z) \arrow[r] \arrow[d, "\mathsf{hom}_{\mathscr{C}}(X\otimes g,Z)"'] & \mathsf{hom}_{\mathscr{C}}(X, Y \multimap Z) \arrow[d, "\mathsf{hom}_{\mathscr{C}}(X,g\multimap Z)"] \\
\mathsf{hom}_{\mathscr{C}}(X \otimes W, Z) \arrow[r] & \mathsf{hom}_{\mathscr{C}}(X, W \multimap Z)
\end{tikzcd}$$

$$\begin{tikzcd}
f \arrow[r, mapsto] \arrow[d, mapsto] & \lceil f \rceil \arrow[d, mapsto] \\
f(X \otimes g) \arrow[r, mapsto] & \lceil f(X \otimes g) \rceil = (g \multimap Z)\lceil f \rceil
\end{tikzcd}$$

This implies that the **first currying formula** of Eq. (5.12) has the more general form:

$$\lceil f(h \otimes g) \rceil = (g \multimap Z)\lceil f \rceil h \qquad\qquad \lfloor f(g \otimes h) \rfloor = (Z \multimapinv g)\lfloor f \rfloor h \tag{5.14}$$

In later sections we will sometimes use the notation $g^{\neg}$ or ${}^{\neg}g$ for the morphisms $g \multimap Z$ or $Z \multimapinv g$, respectively. In Sec. 5.3 we derive the familiar "zigzag" formulas for $g^{\neg}$ and ${}^{\neg}g$, which are "internal to $\mathscr{C}$" in the sense that $g^{\neg}$ and ${}^{\neg}g$ are expressed purely in terms of morphism composition, rather than as the result of passing g through the functor $(-)^{\neg}$ or ${}^{\neg}(-)$, respectively. These zigzag formulas are not generally available, but we will show that they are assuming that $\mathscr{C}$ is a linearly distributive category (with invertible linear distributors), Z is the comonoidal unit $\perp$, and f is nuclear. We will also show that in such a case, the **second currying formula** of Eq. (5.13) genearlizes as follows:

$$(h \multimap g)\lceil f \rceil = \lceil gfh \rceil \qquad\qquad (g \multimapinv h)\lfloor f \rfloor = \lfloor gfh \rfloor \tag{5.15}$$

Note, however, that Eq. (5.15) **may not hold in general** unless $h = \mathsf{id}_X$. The failure of Eq. (5.15) might come as a suprise, since the equation is nevertheless always well-typed:

$$\begin{array}{lcc}
g : Y \to Z & gfh : W \to Z & \lceil f \rceil : \top \to X \multimap Y \\
f : X \to Y & \lceil gfh \rceil : \top \to W \multimap Z & (h \multimap g)\lceil f \rceil : \top \to W \multimap Z \\
h : W \to X & h \multimap g : X \multimap Y \to W \multimap Z & \checkmark
\end{array}$$

[7] Technically, for naturality in Y, one must regard Y as an object $\tilde{Y}$ in $\mathscr{C}^{\mathrm{op}}$ in one of the adjoints, e.g. $- \otimes Y \dashv \tilde{Y} \multimap -$, though in accordance with Appx. F.1, we avoid fixating on this issue.

This suggests a connection between nuclearity and coherence. Coherence in related settings has been considered in [DV19]. Lastly, we take note of a compatibility between currying and addition we will need later.

Proposition 5.2.1 *Let $f, g : X \otimes Y \to Z$ be morphisms in an additive category $\mathscr{C}$. Then left currying is an additive groupoid homomorphism:*

$$\lceil f + g \rceil = \lceil f \rceil + \lceil g \rceil : X \to Y \multimap Z \qquad \lceil 0 \rceil = 0 \qquad \lceil -f \rceil = -\lceil f \rceil$$

The analogous statement is of course true of right currying.

Proof As with group homomorphisms, it suffices to show $\lceil f + g \rceil = \lceil f \rceil + \lceil g \rceil$. Then,

$$\begin{aligned}
\lceil f + g \rceil &= \lceil \mathsf{lefteval}_Z^Y(\lceil f \rceil \otimes Y) + \mathsf{lefteval}_Z^Y(\lceil g \rceil \otimes Y) \rceil \\
&= \lceil \mathsf{lefteval}_Z^Y(\lceil f \rceil \otimes Y + \lceil g \rceil \otimes Y) \rceil \\
&= \lceil \mathsf{lefteval}_Z^Y((\lceil f \rceil + \lceil g \rceil) \otimes Y) \rceil \\
&= \lceil f \rceil + \lceil g \rceil
\end{aligned}$$

as claimed. ■

5.2.2 Associativity

Let $(\mathscr{C}, \otimes)$ be a biclosed magmal category.

Proposition 5.2.2 *The following structures are equivalent. That is, if a natural isomorphism of one of the following forms exists, then they all exist, and they canonically determine each other:*

$$\begin{aligned} \mathsf{associate}_{X,Y,Z} &: X \otimes (Y \otimes Z) \xrightarrow{\sim} (X \otimes Y) \otimes Z \\ \mathsf{internalleftcurry}_{X,Y,Z} &: (X \otimes Y) \multimap Z \xrightarrow{\sim} X \multimap (Y \multimap Z) \\ \mathsf{internalrightcurry}_{X,Y,Z} &: Z \multimapinv (Y \otimes X) \xrightarrow{\sim} (Z \multimapinv Y) \multimapinv X \\ \mathsf{lambek}_{X,Y,Z} &: (X \multimap Z) \multimapinv Y \xrightarrow{\sim} X \multimap (Z \multimapinv Y) \end{aligned}$$

In such a case, we say that $(\mathscr{C}, \otimes)$ is *pre-associative*, reserving the term *associative* to mean that in addition, $\mathsf{associate}$ satisfies the pentagon identity. We are not aware of any established name for fourth isomorphism. We call it the *Lambek law* since its earliest appearance that we are aware is in [Lam58]. In contrast, the following generally does *not* hold:

$$(X \multimapinv Z) \multimap Y \cong X \multimapinv (Z \multimap Y) \tag{5.16}$$

Consider the category of sets, for example. If X, Y, and Z are finite sets of cardinalities 1, 2, and 1, respectively, then the co-Lambek law is false, since $2^{1^1} = 2 \neq 1 = 1^{2^1}$.

Proof of Prop. 5.2.2 The natural isomorphisms are obtained by reflecting the appropriate isomorphisms of presheaves through the Yoneda embedding. ($i \implies ii$):

$$\begin{aligned} &\mathsf{hom}_{\mathscr{C}}(U, (X \otimes Y) \multimap Z) \\ \cong\; &\mathsf{hom}_{\mathscr{C}}(U \otimes (X \otimes Y), Z) \\ \cong\; &\mathsf{hom}_{\mathscr{C}}((U \otimes X) \otimes Y, Z) \\ \cong\; &\mathsf{hom}_{\mathscr{C}}(U \otimes X, Y \multimap Z) \\ \cong\; &\mathsf{hom}_{\mathscr{C}}(U, X \multimap (Y \multimap Z)) \end{aligned}$$

($i \implies iii$): Similar. ($ii \implies i$):

$$\begin{aligned}
&\mathsf{hom}_{\mathscr{C}}(X \otimes (Y \otimes Z), U)\\
\cong\ &\mathsf{hom}_{\mathscr{C}}(X, (Y \otimes Z) \multimap U)\\
\cong\ &\mathsf{hom}_{\mathscr{C}}(X, Y \multimap (Z \multimap U))\\
\cong\ &\mathsf{hom}_{\mathscr{C}}(X \otimes Y, Z \multimap U)\\
\cong\ &\mathsf{hom}_{\mathscr{C}}((X \otimes Y) \otimes Z, U)
\end{aligned}$$

($iii \implies i$): Similar, but involves $\mathsf{internalleftcurry}^{-1}$ instead of $\mathsf{internalleftcurry}$. ($i \implies iv$):

$$\begin{aligned}
&\mathsf{hom}_{\mathscr{C}}(U, (X \multimap Z) \mathrel{\circ\!\!-} Y)\\
\cong\ &\mathsf{hom}_{\mathscr{C}}(Y \otimes U, X \multimap Z)\\
\cong\ &\mathsf{hom}_{\mathscr{C}}((Y \otimes U) \otimes X, Z)\\
\cong\ &\mathsf{hom}_{\mathscr{C}}(Y \otimes (U \otimes X), Z)\\
\cong\ &\mathsf{hom}_{\mathscr{C}}(U \otimes X, Z \mathrel{\circ\!\!-} Y)\\
\cong\ &\mathsf{hom}_{\mathscr{C}}(U, X \multimap (Z \mathrel{\circ\!\!-} Y))
\end{aligned}$$

($iv \implies i$):

$$\begin{aligned}
&\mathsf{hom}_{\mathscr{C}}((X \otimes Y) \otimes Z, U)\\
\cong\ &\mathsf{hom}_{\mathscr{C}}(X \otimes Y, Z \multimap U)\\
\cong\ &\mathsf{hom}_{\mathscr{C}}(Y, (Z \multimap U) \mathrel{\circ\!\!-} X)\\
\cong\ &\mathsf{hom}_{\mathscr{C}}(Y, Z \multimap (U \mathrel{\circ\!\!-} X))\\
\cong\ &\mathsf{hom}_{\mathscr{C}}(Y \otimes Z, U \mathrel{\circ\!\!-} X)\\
\cong\ &\mathsf{hom}_{\mathscr{C}}(X \otimes (Y \otimes Z), U)
\end{aligned}$$

■

A pre-associative structure also induces *internal composition* natural transformations:

$$\begin{aligned}
&\mathsf{leftcomp}_{X,Y,Z} : (Y \multimap Z) \otimes (X \multimap Y) \to X \multimap Z\\
&\mathsf{leftcomp}_{X,Y,Z} = \lceil \mathsf{lefteval}^Y_Z((Y \multimap Z) \otimes \mathsf{lefteval}^X_Y)\mathsf{associate}^{-1}_{Y \multimap Z, X \multimap Y, X} \rceil
\end{aligned}$$

$$\begin{aligned}
&\mathsf{rightcomp}_{X,Y,Z} : (Y \mathrel{\circ\!\!-} X) \otimes (Z \mathrel{\circ\!\!-} Y) \to Z \mathrel{\circ\!\!-} X\\
&\mathsf{rightcomp}_{X,Y,Z} = \lfloor \mathsf{righteval}^Y_Z(\mathsf{righteval}^X_Y \otimes (Z \mathrel{\circ\!\!-} Y))\mathsf{associate}_{X, Y \mathrel{\circ\!\!-} X, Z \mathrel{\circ\!\!-} Y} \rfloor
\end{aligned}$$

Typically, when considering a pre-associative operator $\otimes$, one elides the associators, by which we mean the gray part of these last expressions is omitted.

5.2.3 Examples of magmal adjunctions

Consider a magmal category $(\mathscr{C}, \otimes)$, a category $\mathscr{D}$ with two unital magmal structures $\boxtimes_{\mathsf{L}}$ and $\boxtimes_{\mathsf{R}}$, as well as functors $L : \mathscr{C} \to \mathscr{D}$ and $R : \mathscr{D} \to \mathscr{C}$. These may additionally have unital structures, and we write $\top$ for the unit of $\otimes$ and $\perp_{\mathsf{L}}$ or $\perp_{\mathsf{R}}$ for the unit of $\boxtimes_{\mathsf{L}}$ or $\boxtimes_{\mathsf{R}}$, respectively. Typically, $\boxtimes_{\mathsf{L}} \cong \boxtimes_{\mathsf{R}}$, and hence $\perp_{\mathsf{L}} \cong \perp_{\mathsf{R}}$. Traditionally one also requires associative structures and studies *monoidal adjunctions*, though we can often do without imposing associativity or even unitality. Kelly's *doctrinal adjunction* covers all such variants by regarding the *kind of category* in question as a 2-monad. For the most part, we do not directly rely on Kelly's theorem, but we draw intuitions from this work [Kel74].

This setting of an adjunction between magmal categories allows us to study all instances of *de Morgan duality* we are aware of, and many instances of *homomomorphisms* between algebraic structures. In fact, the theory may be regarded as a joint generalization of these two concepts. We first list some motivating examples of de Morgan duality, which arise in Ch. 6. Star-autonomous categories will be introduced in Sec. 5.3. For pre-abelian categories, see Appx. G.

Example A Let L and R be the "perp" functors $(-)^{b_V} : \textsc{Sub}_{\mathscr{V}}(V) \to \textsc{Sub}_{\mathscr{V}}(V)^{\mathrm{op}}$ and ${}^{b_V}(-) : \textsc{Sub}_{\mathscr{V}}(V)^{\mathrm{op}} \to \textsc{Sub}_{\mathscr{V}}(V)$ determined by a nondegenerate bilinear form $b_V : V \otimes V \to \perp$ on an object V in a preabelian nuclear star-autonomous category $\mathscr{V}$ with comonoidal unit $\perp$. For example, if $\mathscr{V}$ is the category of finite dimensional vector spaces over a field $k \cong \perp$, then $\textsc{Sub}_{\mathscr{V}}$ is the lattice of subspaces of V. In this case, we have:

$$Q^{b_V} = \{v \in V \mid b_V(v, q) = 0 \;\forall\; q \in Q\} \qquad \{v \in V \mid b_V(q, v) = 0 \;\forall\; q \in Q\} = {}^{b_V}Q$$

One readily sees that $Q \subseteq {}^{b_V}(Q^{b_V})$. By *nondegenerate*, we mean that the curried bilinear form $\lceil b_V \rceil : V \to V^*$ is a monomorphism. The restriction $V \to Q^*$ of this map has kernel Q^{b_V}. In k-$\textsc{fdVect}$, it follows that $\dim Q^{b_V} + \dim Q = \dim V$ and so $Q = {}^{b_V}(Q^{b_V})$, so $(-)^{b_V} \dashv {}^{b_V}(-)$ is an adjoint equivalence.

In general, for a lattice $\textsc{Sub}_{\mathscr{V}}(V)$, we study the de Morgan duality between the *meet* $\cap$ and *join* $\cup$. When $\mathscr{V} \cong k$-$\textsc{fdVect}$, these are respectively the intersection of subspaces and the pointwise sum of subspaces, not to be confused with the union of their underlying sets, which is not a subspace, and is therefore not a well-defined subobject (subspace).

Similarly, we may take $\mathscr{V}$ to be the category $\widetilde{\mathrm{LCA}}$ from Sec. 2.4.5 and V to be the locally compact abelian group $\mathbb{R}^n$ with the symplectic form $\omega_V((q_1, p_1), (q_2, p_2)) = e^{2\pi i(p_1 q_2 - p_2 q_1)}$.

Note that the symplectic form is valued in the comonoidal unit $\perp \cong \mathsf{U}(1)$, not to be confused with the monoidal unit $\top \cong \mathbb{Z}$.

Example B Take L and R to be the left and right negations on a biclosed magmal category $(\mathscr{C}, \otimes)$ with respect to some object $\perp$. In other words, let $L = (-)^\neg = - \multimap \perp : \mathscr{C} \to \mathscr{C}^{\mathrm{op}}$ and $R = {}^\neg(-) = \perp \mathrel{\circ\!\!-} - : \mathscr{C}^{\mathrm{op}} \to \mathscr{C}$. These form the *negation adjunction* $(-)^\neg \dashv {}^\neg(-)$. In the braided case, $L^{\mathrm{op}} \cong R$, but braidedness has no say in whether $L \dashv R$ is an equivalence $\mathscr{C}^{\mathrm{op}} \simeq \mathscr{C}$. For example, $\mathscr{C}$ may be a Heyting algebra, where $\otimes$ is the product $\wedge$ and $\boxtimes$ is the coproduct $\vee$. Then $\mathscr{C}^{\mathrm{op}} \simeq \mathscr{C}$ if and only if $\mathscr{C}$ is actually a Boolean algebra. Symmetry of the product implies that negation is self-adjoint, that is, left and right negation are each other's opposite. For consistency, we continue to use separate notations: $L \cong (-)^\neg$ and $R \cong {}^\neg(-)$. In this case, the counit is the *double negation translation* judgment $\eta : \mathsf{Id}_{\mathscr{C}} \Rightarrow RL$. Since $L^{\mathrm{op}} \cong R$, the unit $\epsilon : LR \Rightarrow \mathsf{Id}_{\mathscr{C}^{\mathrm{op}}}$ is the opposite of η, not to be confused with *double negation elimination*, which is generally unavailable in a Heyting algebra. In intuitionistic logic, only three of the four de Morgan laws hold:

$$(Q \wedge P)^\neg \overset{\leftarrow}{\not\to} P^\neg \vee Q^\neg \quad (\text{in } \mathscr{C}) \qquad \text{and} \qquad {}^\neg P \wedge {}^\neg Q \cong {}^\neg(Q \vee P) \quad (\text{in } \mathscr{C}) \tag{5.17}$$

Caution Following our convention Appx. F.1, we write the arrows on the left of Eq. (5.17) in $\mathscr{C}$ by applying the oppositization 2-functor $\mathsf{op} : \mathrm{C{\scriptsize AT}}^{\mathrm{co}} \to \mathrm{C{\scriptsize AT}}$, since $L = (-)^\neg$ is valued in $\mathscr{C}^{\mathrm{op}}$. Originally it matches Eq. (5.19) where an arbitrary category $\mathscr{D}$ takes the place of $\mathscr{C}^{\mathrm{op}}$, and reads:

$$P^\neg \vee Q^\neg \overset{\leftarrow}{\not\to} (Q \wedge P)^\neg \quad (\text{in } \mathscr{C}^{\mathrm{op}}) \tag{5.18}$$

The category theory notation is slightly at odds with that of logic. Namely, the arrows in Eq. (5.17) and Eq. (5.18) indicate the existence of morphisms; they do not express implications (internal hom objects). Through the Curry-Howard correspondence, these morphisms correspond to judgments. For example, the judgment $P^\neg \vee Q^\neg \vdash (Q \wedge P)^\neg$ indicates that it is possible to form a natural deduction proof of $(Q \wedge P)^\neg$ with nondischarged hypothesis $P^\neg \vee Q^\neg$. A *de Morgan* Heyting algebra is one in which we also have a morphism $(Q \wedge P)^\neg \to P^\neg \vee Q^\neg$ in the other direction (in $\mathscr{C}$). There is a three-way distinction between non-de Morgan Heying algebras, in which the fourth de Morgan law does not generally hold; de Morgan non-classical Heyting algebras, in which all four de Morgan laws hold but double negation elimination still does not; and Boolean algebras.

Example B also covers the study of de Morgan duality in a star-autonomous category $\mathscr{V}$, not to be confused with its subobject preorders $\mathrm{S{\scriptsize UB}}_{k\text{-}\mathrm{FDV{\scriptsize ECT}}}(V)$.

5.2.4 Magmal adjunctions

Let $(\mathscr{C}, \otimes)$ be a magmal category, let $\mathscr{D}$ be a category equipped with two magmal structures $\boxtimes_{\mathsf{L}}$ and $\boxtimes_{\mathsf{R}}$, and consider a pair of functors $L : \mathscr{C} \to \mathscr{D}$ and $R : \mathscr{D} \to \mathscr{C}$.

We call $\boxtimes_{\mathsf{L}}$ a *left oplax de Morgan dual* of $\otimes$ if L is an oplax magmal functor, and $\boxtimes_{\mathsf{R}}$ a *right lax de Morgan dual* of $\otimes$ if R is a lax magmal functor. These respective conditions mean that a natural transformation of the appropriate form is equipped:

$$LX \boxtimes_{\mathsf{L}} LY \leftarrow L(Y \otimes X) \qquad \text{resp.} \qquad RX \otimes RY \to R(Y \boxtimes_{\mathsf{R}} X) \tag{5.19}$$

The functor L is called a *strong magmal functor* and we say that $\boxtimes_{\mathsf{L}}$ is a *strong* left de Morgan dual of $\otimes$ if the natural transformation on the left is an isomorphism, and dually.

Caution Our definition of magmal functors *reverses* the positions of X and Y. This differs from the standard convention for monoidal functors. Where we write $L : (\mathscr{C}, \otimes) \to (\mathscr{D}, \boxtimes)$, in the standard convention one would need to instead write $L : (\mathscr{C}, \otimes) \to (\mathscr{D}, \boxtimes^{\mathrm{rev}})$. This reversal in the defintion of magmal functors will allow us to follow the physics currying convention without having to write "$\boxtimes^{\mathrm{rev}}$" and to omit the adjective "reversed" from terms like "reversed left oplax magmal functor". See Appx. F for details.

Proposition 5.2.3 *If L is strong and essentially surjective, then $\boxtimes_{\mathsf{L}}$ is determined up to isomorphism by L and $\otimes$. Similarly, if R is strong, full, and faithful, then $\boxtimes_{\mathsf{R}}$ is determined up to isomorphism by R and $\otimes$. Furthermore, if L and R are both strong and constitute an equivalence, then $\boxtimes_{\mathsf{L}} \cong \boxtimes_{\mathsf{R}}$.*

When $\boxtimes_{\mathsf{L}} \cong \boxtimes_{\mathsf{R}}$, we call it the *strong bidirectional de Morgan dual* or simply *de Morgan dual* of $\otimes$. Given a magmal product $\otimes$ on $\mathscr{C}$ and a pair of functors L and R as above, we may always *define* a magmal product $\boxtimes$ on $\mathscr{D}$ by setting $Y \boxtimes X \cong L(RX \otimes RY)$. If $RL \cong \mathsf{id}_{\mathscr{C}}$, then $\boxtimes$ is a (hence, by Prop. 5.2.3, *the*) strong right de Morgan dual of $\otimes$. If both $RL \cong \mathsf{id}_{\mathscr{C}}$ and $LR \cong \mathsf{id}_{\mathscr{D}}$, or in other words, if L and R lie in an equivalence, then by Prop. 5.2.3, $\boxtimes$ is the strong bidirectional de Morgan dual of $\otimes$. Also note, so far we have not assumed adjointness. In the discrete case, $(\mathscr{C}, \otimes)$ is a magma, $\mathscr{D}$ is a set, L and R are mutually inverse bijections, and $\boxtimes$ is the magma structure thereby induced on $\mathscr{D}$.

Proof Suppose L is strong and essentially surjective, and let $A, B \in \mathsf{ob}(\mathscr{D})$. Since L is essentially surjective, there exist $X, Y \in \mathsf{ob}(\mathscr{C})$ such that $A \cong LX$ and $B \cong LY$. If

$\boxtimes_{\mathsf{L}}$ and $\boxtimes'_{\mathsf{L}}$ are two left de Morgan duals of $\otimes$, then since L is strong, it follows that $A \boxtimes_{\mathsf{L}} B \cong L(Y \otimes X) \cong A \boxtimes'_{\mathsf{L}} B$, so $\boxtimes_{\mathsf{L}} \cong \boxtimes'_{\mathsf{L}}$. Instead now suppose R is strong, full, and faithful, and let $X, Y \in \mathsf{ob}(\mathscr{C})$. Then if $\boxtimes_{\mathsf{R}}$ and $\boxtimes'_{\mathsf{R}}$ are right de Morgan duals of $\otimes$, then since R is strong, we have $R(Y \boxtimes_{\mathsf{R}} X) \cong RX \otimes RY \cong R(Y \boxtimes'_{\mathsf{R}} X)$. Then since R is full and faithful, it follows that $Y \boxtimes_{\mathsf{R}} X \cong Y \boxtimes'_{\mathsf{R}} X$, and so $\boxtimes_{\mathsf{R}} \cong \boxtimes'_{\mathsf{R}}$. Finally, suppose L and R are both strong and form an equivalence. Then:

$$X \boxtimes_{\mathsf{L}} Y \cong LRX \boxtimes_{\mathsf{L}} LRY \cong L(RY \otimes RX) \cong LR(X \boxtimes_{\mathsf{R}} Y) \cong X \boxtimes_{\mathsf{R}} Y$$

as claimed. ■

We call the natural transformations of Eq. (5.19) the *left* and *right de Morgan laws*. In total, there are four possible de Morgan laws, since left and right de Morgan duality may each be one- or two-sided. Regardless of whether L and R are strong, full and faithful, or essentially surjective, our applications typically only require us to consider a single magmal product $\boxtimes$ on $\mathscr{D}$, but require L and R to form an adjunction (in Cat):

$$\begin{tikzcd} \mathscr{D} \arrow[rr, bend right, "R"'] \arrow[rr, phantom, "\perp"] & & \mathscr{C} \arrow[ll, bend right, "L"'] \end{tikzcd}$$

Kelly's Theorem on doctrinal adjunctions, instantiated to the 2-monad whose 2-algebras are magmal categories, amounts to the following two facts: (1) If $L \dashv R$ is an (ordinary) adjunction, (that is, an adjunction in Cat, rather than the bicategory MagCat of magmal categories, oplax magmal functors, and oplax magmal natural transformaions), then L is oplax if and only if R is lax. In other words, if $L \dashv R$, then the two conditions of Eq. (5.19) are equivalent; (2) If L (or R) is both oplax and lax, it is strong, i.e. without loss of generality, one may take the oplax and lax structures to be mutually inverse, [Shu11]. We do not prove (2) in general, but we cite it in the proof of Thm. 5.3.2. We do prove (2) in a much simpler case (c.f. Prop. 5.2.6), which we also need, where $\otimes$ and $\boxtimes$ are the product and coproduct on $\mathscr{C}$. Part (1) of this instance of Kelly's Theorem is easy to see directly:

Proposition 5.2.4 *Let $L : \mathscr{C} \to \mathscr{D}$ and $R : \mathscr{C} \to \mathscr{D}$ be (ordinary) functors between magmal categories $(\mathscr{C}, \otimes)$ and $(\mathscr{D}, \boxtimes)$, and suppose there exist natural transformations $\eta : \mathsf{Id}_{\mathscr{C}} \Rightarrow RL$ and $\epsilon : LR \Rightarrow \mathsf{Id}_{\mathscr{D}}$. Then:*

(i) L is oplax if and only if R is lax. In other words, $\boxtimes$ is an oplax left de Morgan dual of $\otimes$ if and only if $\otimes$ is a lax right de Morgan dual of $\boxtimes$.

(ii) If η and ϵ are natural isomorphisms, then L is strong if and only if R is strong.

We don't even require the functors to form an adjunction $L \dashv R$ here, i.e. for η and ϵ to satisfy the zigzag laws. If they do, then the condition in (ii) means it is an adjoint equivalence.

We note that (i) is a self-dual statement, i.e. that the dual statement of (i) does not just swap the words *lax* and *oplax*, but also swaps L and R. In fact, the statement obtained by applying only one of these swaps is **false**, as indeed only three out of four de Morgan laws hold in every Heyting algebra.

Part (ii) and its proof (and technically, just as well part (i)) generalize the fact and proof, respectively, that the inverse of a bijective (i.e. SET-wise invertible) homomorphism of magmas, groups, Lie algebras, etc. is again a homomorphism.

Proof Suppose L is oplax. Then the following composition gives R a lax structure:

$$RX \otimes RY \xrightarrow{\eta_{RX \otimes RY}} RL(RX \otimes RY) \xrightarrow{R\mathsf{oplax}^L_{RX \otimes RY}} R(LRY \boxtimes LRX) \xrightarrow{R(\epsilon_Y \boxtimes \epsilon_X)} R(Y \boxtimes X) \tag{5.20}$$

Moreover, if η and ϵ are isomorphisms and L is strong, then Eq. (5.20) gives R a strong magmal structure. The proof that R being lax (or strong) implies L is oplax (or strong) is dual. ∎

It is possible to have an adjoint equivalence where L is oplax and R is lax without either being strong. Intuitively, this can happen by taking an ordinary adjoint equivalence, and equipping any old "incompatible" magmal products on $\mathscr{C}$ and $\mathscr{D}$. We give a more interesting example in Sec. 5.3, where we define *nuclearity* with respect to an operation $⅋$ that relates to $\otimes$ via invertible linear distributions. We then consider three levels of coherence of the adjunction of the negation functors, which go between $(\mathscr{C}, \otimes)$ and $(\mathscr{C}^{\mathrm{op}}, ⅋^{\mathrm{rev\,op}})$. In the intermediate case, the negation adjunction is an equivalence, but we do not require $⅋^{\mathrm{rev\,op}}$ to be the de Morgan dual $\boxtimes$ of $\otimes$, and thereby give a new perspective the role of de Morgan duality in star-autonomous categories, e.g. different from that of [CS97a].

It is also possible to have an adjunction $L \dashv R$ where L is strong and R is only lax. The negation adjunction for any non-de Morgan Heyting algebra is an example.

This phenomenon of three (but not necessarily all four) of the de Morgan laws holding, as in intuitionistic logic, holds more generally for all adjunctions in MagCat. Moreover, all four de Morgan laws hold if and only if the adjunction actually takes place in the bicategory StrongMagCat of strong magmal natural transformations.

In principle, one can apply different instances of Kelly's Theorem to see that the results discussed so far apply not just to magmal categories, but also to variants in which one imposes unitality, associativity, braidedness, and/or symmetry, including the case of monoidal categories. However, just as monoids are better-behaved than magmas, additional properties hold when imposing more structures and properties on the kind of category in question.

Consider an adjunction $L \dashv R$ with natural transformations as in Eq. (5.19). Then the adjuncts

$$Y \otimes X \to R(LX \boxtimes_{\mathsf{L}} LY) \qquad \text{resp.} \qquad Y \boxtimes_{\mathsf{R}} X \leftarrow L(RX \otimes RY) \tag{5.21}$$

might not be isomorphisms, even if the de Morgan laws are strong! This separation is witnessed by non-classical de Morgan Heyting algebras. Nevertheless, we see that:

Proposition 5.2.5 *Let $(\mathscr{C}, \otimes, \top)$ and $(\mathscr{D}, \boxtimes, \bot)$ be unital magmal categories, and let $L \dashv R$ be an adjunction equipped with natural transformations as in Eq. (5.19) as well as isomorphisms $L\top \xleftarrow{\sim} \bot$ and $R\bot \xrightarrow{\sim} \top$, satisfying the additional obvious coherences. (In other words, $L \dashv R$ is a unital magmal adjunction.) Then the following are equivalent:*

- *(i) The adjunction $L \dashv R$ is an equivalence.*
- *(ii) Both natural transformations in Eq. (5.21) are natural isomorphisms.*

Proof sketch ($i \implies ii$) is straight-forward. For ($ii \implies i$), substitute $\top$ and $\bot$ for Y on the left and right side of Sec. 5.2.4, respectively, and apply unitors to obtain natural isomorphisms $\eta_X : X \xrightarrow{\sim} RLX$ and $X \xleftarrow{\sim} LRX : \epsilon_X$. From the unitality coherence conditions, it should follow that these are the unit and counit of the underlying adjunction $L \dashv R$. The structure provided by hypothesis is enough to write down the unital magmal structure for $L \dashv R$. Finally, one checks that this induced structure is coherent. $\square$

When the equivalent conditions of Prop. 5.2.5 apply, all four de Morgan laws hold, generalizing the meta-theorem from logic that double negation elimination entails the fourth de

Morgan law. Classically, this is proved in Gentzen's *natural deduction* system (the classical version NK, which has double negation elimination, as opposed to the intuitionistic version NJ) by exhibiting a proof tree whose only nondischarged hypothesis is the proposition ${}^{\neg}(Y^{\neg} \vee X^{\neg})$ and whose output (root node) is the proposition $X \wedge Y$.[8] This is a construction of the inverse of the map on the left of Eq. (5.21):

$$\dfrac{\dfrac{[X^{\neg}]_2 \\ \vdots}{X} \qquad \dfrac{\dfrac{\dfrac{\dfrac{[Y^{\neg}]_1}{Y^{\neg} \vee X^{\neg}} \qquad {}^{\neg}(Y^{\neg} \vee X^{\neg})}{\perp}}{{}^{\neg}(Y^{\neg})}\ \neg\,\mathsf{intro}_{\text{discharge 1}}}{Y}\ \neg\neg\,\mathsf{elim}}{X \wedge Y}$$

In Ch. 6, we describe a contravariant endofunctor $(-)^{\omega}$ on the lattice $\mathrm{S{\scriptstyle UB}}_{\mathscr{V}}(V)$ of subobjects of an object V equipped with a symplectic form ω in a sufficiently-structure category $\mathscr{V}$, which takes a subobject X to its *symplectic orthogonal* X^{ω}. If $\mathscr{V} = \widetilde{\mathrm{LCA}}$, we find that $(-)^{\omega}$ is a self-adjoint monoidal adjunction and prove that three out of the four de Morgan laws hold. This example is different than the intuitionistic logic example in that $(-)^{\omega}$ is not a *negation*, that is, it is not an internal hom functor $- \multimap \perp$ on $\mathrm{S{\scriptstyle UB}}_{\mathscr{V}}(V)$ for any $\perp$.

Nevertheless, the symplectic orthogonal $(-)^{\omega}$ and the negation $(-)^{\neg}$ in intuitionistic logic do have something in common. In both cases, $\otimes$ is the product $\times$ on $\mathscr{C}$, and $\boxtimes$ is the coproduct $+$ on $\mathscr{C}$, i.e. the product in $\mathscr{D}$, which is taken to be $\mathscr{C}^{\mathrm{op}}$. Note that the coproduct $+$ on $\mathscr{C}$ is the product on $\mathscr{C}^{\mathrm{op}}$. The following proposition shows that for such adjunctions, at least three of the four de Morgan laws *always* hold.

Proposition 5.2.6 *Let $\mathscr{C}$ and $\mathscr{D}$ categories, each with finite products, and consider functors $L : \mathscr{C} \to \mathscr{D}$ and $R : \mathscr{D} \to \mathscr{C}$. Then L and R are* ***both oplax****, meaning there exist natural transformations of the form:*

$$LY \times LX \leftarrow L(X \times Y) \qquad\qquad R(X \times Y) \to RY \times RX \tag{5.22}$$

If, moreover, there exist natural transformations $\eta : \mathsf{Id}_{\mathscr{C}} \Rightarrow RL$ and $\epsilon : LR \Rightarrow \mathsf{Id}_{\mathscr{D}}$, then R is strong, that is, the natural transformation on the right of Eq. (5.22) is an isomorphism.

[8] For reference, we keep sidedness of $L = (-)^{\neg}$ and $R = {}^{\neg}(-)$ in our notation here despite symmetry.

If $\mathscr{C}$ has finite products and coproducts and we take $\mathscr{D}$ to be $\mathscr{C}^{\mathrm{op}}$ and R to be the opposite of L, then we only need to supply η for the second part of the theorem, since we may take ϵ to be its opposite. For example, suppose $\mathscr{C}$ is a lattice, and write $\cap$ for the product and $\cup$ for the coproduct. Then if $(-)^* : \mathscr{C} \to \mathscr{C}^{\mathrm{op}}$ is a contravariant endofunctor satisfying *double dualization translation* $X \subseteq {}^*(X^*)$ for all X, then it follows that $X^* \cap Y^* \subseteq (Y \cup X)^*$ and ${}^*(X \cup Y) = {}^*Y \cap {}^*X$ for all X and Y, where ${}^*(-) : \mathscr{C}^{\mathrm{op}} \to \mathscr{C}$ is the opposite of $(-)^*$. In such a case, $(-)^* \dashv {}^*(-)$, and *right double dualization translation* $X \subseteq ({}^*X)^*$ is also satisfied in $\mathscr{C}$ (as opposed to $\mathscr{C}^{\mathrm{op}}$), so at least six of eight de Morgan laws are satisfied.

Caution: At a glance, one might mistakenly believe that Prop. 5.2.6 contradicts the self-duality of Cat, the bicategory ambient to this adjunction (*a priori*, though we then see it is better MagCat). To understand why it does not, it is helpful to consider the example of a co-Heyting algebra, i.e. a model for *paraconsistent logic*. In this system, one has double negation elimination but not double negation translation, and so on. The key is that asymmetry is introduced by the types of η and ϵ, and indeed, *adjunction* is technically not a self-dual notion in Cat; it has a lesser-known dual notion, *co-adjunction*, not to be confused with the notion of the *opposite adjunction* $R^{\mathrm{op}} \dashv L^{\mathrm{op}}$ of a given adjunction $L \dashv R$. Whereas the data of an adjunction $L \dashv R$ is equivalent to that of its opposite $R^{\mathrm{op}} \dashv L^{\mathrm{op}}$, this is not so for a co-adjunction. *Co-adjunction* is defined the same as *adjunction*, but where the structure maps instead have the form $RL \Rightarrow \mathsf{Id}_{\mathscr{C}}$ and $\mathsf{Id}_{\mathscr{D}} \Rightarrow LR$. This swaps the roles of L and R, so a co-adjunction $L \vdash R$ is equivalently just an alias for an adjunction $R \dashv L$. Since co-adjunctions are just adjunctions in disguise, the concept is typically avoided. We only mention it here because it helps resolve the seeming asymmetry issue.

Proof The left and right oplax de Morgan laws are dual, so we just prove the left one:

$$\begin{tikzcd} & X \times Y \arrow[dl] \arrow[dr] & \\ X & & Y \end{tikzcd}$$

Pass this product diagram through L and set aside, as we will use it again in a moment:

$$\begin{tikzcd} & L(X \times Y) \arrow[dl] \arrow[d, dashed] \arrow[dr] & \\ LY & LY \times LX \arrow[l] \arrow[r] & LX \end{tikzcd}$$

This proves the left oplax de Morgan law. The proof of the right oplax law is dual. Assuming η and ϵ exist (without necessarily satisfying the triangle identities), we see that R is lax by part (i) of Prop. 5.2.4. Mutual inversehood of the oplax and lax de Morgan laws for R follows from the commutativity of the following two diagrams:

$$
\begin{tikzcd}
 & R(X) \times R(Y) \arrow[dl] \arrow[d] \arrow[dr] & \\
R(X) & R(Y \times X) \arrow[d] & R(Y) \\
 & R(X) \times R(Y) \arrow[ul] \arrow[ur] &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & R(Y \times X) \arrow[dl] \arrow[d] \arrow[dr] & \\
R(X) & R(X) \times R(Y) \arrow[d] & R(Y) \\
 & R(Y \times X) \arrow[ul] \arrow[ur] &
\end{tikzcd}
$$

Commutativity of each diagram, in turn, follows by universality of the product in $\mathscr{C}$. ■

5.2.5 Negation

Let $(\mathscr{C}, \otimes)$ be a biclosed magmal category and fix an arbitrary object $\perp \in \mathsf{ob}(\mathscr{C})$, to be called the *dualizing object*. Then consider the corresponding negation functors:

$$(-)^{\neg} = - \multimap \perp : \mathscr{C} \to \mathscr{C}^{\mathrm{op}} \qquad\qquad \perp \multimapinv - = {}^{\neg}(-) : \mathscr{C}^{\mathrm{op}} \to \mathscr{C}$$

left negation $\qquad\qquad$ right negation

We view left and right negation as having opposite type of each other, as above, so that they form an adjunction, the *negation adjunction* $(-)^{\neg} \dashv {}^{\neg}(-)$. Indeed, it follows that:

$$\mathsf{Hom}_{\mathscr{C}^{\mathrm{op}}}(\mathsf{Y}^{\neg}, X) := \mathsf{Hom}_{\mathscr{C}}(X, Y^{\neg}) \cong \mathsf{Hom}_{\mathscr{C}}(Y, {}^{\neg}X) \tag{5.23}$$

The := sign above indicates the identification of a morphism $f : X \to Y^{\neg}$ in $\mathscr{C}$ with the corresponding morphism $\tilde{f} : Y^{\neg} \to X$ in $\mathscr{C}^{\mathrm{op}}$ with respect to the defining identification of objects in $\mathscr{C}$ with those in $\mathscr{C}^{\mathrm{op}}$. See Appx. F.1 for remarks about conventions and shorthand notation concerning oppositization, e.g. for explanations of why write $Y^{\neg}$ rather than $Y^{\neg^{\mathrm{op}}}$ in the middle expression. The isomorphism in Eq. (5.23) is gotten by left uncurrying then right currying. One now computes the counit ϵ and unit η of $(-)^{\neg} \dashv {}^{\neg}(-)$:

$$({}^{\neg}X)^{\neg} \leftarrow X : \lceil \mathsf{righteval}_{\perp}^{X} \rceil = \epsilon_X \qquad\qquad \eta_X = \lfloor \mathsf{lefteval}_{\perp}^{X} \rfloor : X \to {}^{\neg}(X^{\neg})$$

We reversed the direction of the arrow for the counit in order to present it as being valued in $\mathscr{C}$, since originally (by definition) it is valued in $\mathscr{C}^{\mathrm{op}}$. The Triple Dual Problem [KM71] asks for which $(\mathscr{C}, \otimes, \perp)$ the following natural transformations Eq. (5.24) are identities. One may also ask whether an individual object $X \in \mathsf{ob}(\mathscr{C})$ satisfies the triple dual property. For example, in $(\mathscr{C}, \otimes, \perp) \cong (k\text{-}\textsc{Vect}, \otimes_k, k)$, infinite dimensional vector spaces do not.

$$\begin{gathered} ({}^{\neg}(X^{\neg}))^{\neg} \xleftarrow{\lceil \mathsf{righteval}_{\perp}^{X^{\neg}} \rceil} X^{\neg} \xleftarrow{\lfloor \mathsf{lefteval}_{\perp}^{X} \rfloor^{\neg}} ({}^{\neg}(X^{\neg}))^{\neg} \\ {}^{\neg}(({}^{\neg}X)^{\neg}) \xrightarrow{{}^{\neg}\lceil \mathsf{righteval}_{\perp}^{X} \rceil} {}^{\neg}X \xrightarrow{\lfloor \mathsf{lefteval}_{\perp}^{{}^{\neg}X} \rfloor} {}^{\neg}(({}^{\neg}X)^{\neg}) \end{gathered} \tag{5.24}$$

Recognizing these possible identities as the two canonical well-typed diagrams besides the zigzag identities for the negation adjunction $(-)^{\neg} \dashv {}^{\neg}(-)$, we see that one and hence both identities are satisfied if and only if $(-)^{\neg} \dashv {}^{\neg}(-)$ is an idempotent adjunction, c.f. [MS82].

Every closed semilattice is idempotent with respect to any dualizing object. The following NJ proof tree shows directly that triple negatives can be reduced to single negatives in intuitionistic logic. Again, we keep track of left versus right negation even though this is redundant due to the bradedness of $\wedge$ for comparison with the general case.

$$\dfrac{\dfrac{(^{\neg}(X^{\neg}))^{\neg} \qquad \dfrac{[X]}{^{\neg}(X^{\neg})}}{\perp}}{X^{\neg}}$$

Indeed, through the Curry-Howard-Lambek correspondence, this proof tree corresponds to the morphism to the left of the $=$ sign in Eq. (5.25). The simplification from the left-hand-side to the right-hand-side of the $=$ sign in Eq. (5.25) follows from the left currying formula.

$$\lceil \mathsf{lefteval}_{\perp}^{\neg(X^{\neg})}((^{\neg}(X^{\neg}))^{\neg} \otimes \lfloor \mathsf{lefteval}_{\perp}^{X} \rfloor) \rceil = \lfloor \mathsf{lefteval}_{\perp}^{X} \rfloor^{\neg} : (^{\neg}(X^{\neg}))^{\neg} \to X^{\neg} \tag{5.25}$$

Explicitly, the (left) double negation translation is given by $\lfloor \mathsf{lefteval}_{\perp}^{X} \rfloor$, the *modus ponens* rule corresponds to left evaluation, and the negation introduction in the final step corresponds to the entire morphism being left curried. We may also show directly that Eq. (5.25) is a left inverse of the (right) double negation translation map $\lceil \mathsf{righteval}_{\perp}^{X^{\neg}} \rceil$ evaluated at $X^{\neg}$:

$$(\lfloor \mathsf{lefteval}_{\perp}^{X} \rfloor^{\neg}) \lceil \mathsf{righteval}_{\perp}^{X^{\neg}} \rceil = \lceil \mathsf{righteval}_{\perp}^{X^{\neg}}(X^{\neg} \otimes \lfloor \mathsf{lefteval}_{\perp}^{X} \rfloor) \rceil = \lceil \mathsf{lefteval}_{\perp}^{X} \rceil = \mathsf{id}_{X^{\neg}}$$

The equalities above follow by the left and right currying formulas, respectively. Triple negatives are not generally isomorphic to single negatives, however. Indeed, $\lfloor \mathsf{lefteval}_{\perp}^{X} \rfloor^{\neg}$ is an isomorphism if and only if negation $(-)^{\neg} \dashv {}^{\neg}(-)$ is idempotent. In this way, propositions in intuitionistic logic behave differently from infinite dimensional vector spaces.

We call $(\mathscr{C}, \otimes, \perp)$ *left reflexive* if $\lfloor \mathsf{lefteval}_{\perp} \rfloor$ is a natural isomorphism, *left reflexive* if $\lceil \mathsf{righteval}_{\perp} \rceil$ is a natural isomorphism, and *bireflexive* if it is both left and right reflexive. In other words, $(\mathscr{C}, \otimes, \perp)$ is left reflexive if and only if $(-)^{\neg}$ is full and faithful, right reflexive if and only if ${}^{\neg}(-)$ is full and faithful, and bireflexive if and only if negation $(-)^{\neg} \dashv {}^{\neg}(-)$ is an adjoint equivalence. Again, we may also apply these terms to individual objects. When we ask if X is left reflexive, it is viewed as an object in $\mathscr{C}$, and when we ask if it is right reflexive, it is viewed as an object in $\mathscr{C}^{\mathrm{op}}$.

If $(-)^{\neg} \dashv {}^{\neg}(-)$ is idempotent, then the full subcategory of left reflexive objects of $\mathscr{C}$, (which is equivalent to the full subcategory of right reflexive objects of $\mathscr{C}^{\mathrm{op}}$,) is the full image of left negation [Gra18].

In logic, the unit $\lfloor \mathsf{lefteval}_{\perp} \rfloor$ of the *double negation monad* ${}^{\neg}((-)^{\neg}) : \mathscr{C} \to \mathscr{C}$ is the *double negation translation* judgment. Since negation is idempotent in that case, and since classical propositional logic NK is obtained from intuitionistic classical logic NJ by imposing the double negation elimination rule, we see that the *double negation translate* ${}^{\neg}(X^{\neg})$ of a classical tautology X is an intuitionistic tautology. In k-Vect and some relatives, this monad is called *double dualization* and its unit is often called the *canonical injection into the double dual*. In functional programming, e.g. if $\mathscr{C}$ is Haskell's type system Hask, ${}^{\neg}((-)^{\neg})$ is called the *continuation monad*, and $\perp$ is the return type of the continuation.

If $(\mathscr{C}, \otimes, \top)$ is a unital magmal category, and $\perp \in \mathsf{ob}(\mathscr{C})$ is a dualizing object, then by the Yoneda embedding we have $\top^{\neg} \cong \perp \cong {}^{\neg}\top$. Furthermore, if $\top$ is left reflexive, then ${}^{\neg}\perp \cong \top$ and if $\top$ is right reflexive, then $\perp^{\neg} \cong \top$. If $\mathscr{C}$ has a braiding, then $(-)^{\neg} \cong {}^{\neg^{\mathrm{op}}}(-)$.

5.2.6 Nuclearity and de Morgan Duality

Let $(\mathscr{C}, \otimes)$ be a biclosed magmal category, let $\perp$ be an arbitrary object in $\mathscr{C}$, and consider the corresponding negation adjunction:

$$
\begin{tikzcd}
\mathscr{C}^{\mathrm{op}} \arrow[rr, bend right, "\neg(-)"'] \arrow[rr, phantom, "\perp"] & & \mathscr{C} \arrow[ll, bend right, "(-)^{\neg}"']
\end{tikzcd}
\tag{5.26}
$$

If $\mathscr{C}^{\mathrm{op}}$ is equipped with a magmal product $\boxtimes$ as well as a (fixed choice of) natural isomorphism of the following form, which we call the *left* or *right pre-nuclearizer* for $\boxtimes$, respectively, then we call $(\mathscr{C}, \otimes)$ *left* or respectively *right pre-nuclear* with respect to $\boxtimes$:

$$
\overset{\text{left pre-nuclearizer}}{X \multimap Y^{\neg^{\mathrm{op}}} \cong Y^{\neg^{\mathrm{op}}} \boxtimes^{\mathrm{op}} X^{\neg^{\mathrm{op}}}} \qquad\qquad \overset{\text{right pre-nuclearizer}}{{}^{\neg}X \boxtimes^{\mathrm{op}} {}^{\neg}Y \cong {}^{\neg}Y \multimapinv X}
\tag{5.27}
$$

Morphisms are always casted into $\mathscr{C}$, never $\mathscr{C}^{\mathrm{op}}$. Moving forward, we do not use the $^{\mathrm{op}}$ superscript on functors such as $\otimes$, $\boxtimes$, $\multimap$, $\multimapinv$, $(-)^{\neg}$, and ${}^{\neg}(-)$. These superscripts can be inferred, but it is standard to omit them. See Appx. F.1 for remarks on this convention.

When switching from the physics convention to the math convention for de Morgan duality, left and right nuclearity each undergo a swap, where e.g. left pre-nuclearity would read $X \multimap Y^{\neg} \cong X^{\neg} \boxtimes Y^{\neg}$. We call $(\mathscr{C}, \otimes)$ *left nuclear*, *right nuclear*, or *binuclear* if it is equipped with a natural isomorphism of the following respective form:

$$
\overset{\text{left nuclearizer}}{X \multimap Y \cong Y \boxtimes X^{\neg}} \qquad\qquad \overset{\text{right nuclearizer}}{{}^{\neg}X \boxtimes Y \cong Y \multimapinv X}
\tag{5.28}
$$

In Sec. 5.3, we consider nuclearity as opposed to pre-nuclearity since the two end up being equivalent in that setting (assuming strong linear distributivity), but here, we focus on pre-nuclearity because it interacts more directly with the de Morgan laws, and thereby lets us avoid assuming *reflexivity* in certain proofs. This generality allows for most of these results to apply, for instance, to de Morgan Heyting algebras.

Recall that a *(strong) left de Morgan dual* of $\otimes$ is a magmal product $\boxtimes$ on $\mathscr{C}^{\mathrm{op}}$ that satisfies:

$$
(X \otimes Y)^{\neg} \cong Y^{\neg} \boxtimes X^{\neg}
\tag{5.29}
$$

If $(\mathscr{C}, \otimes)$ is left reflexive with respect to $\perp$, then such $\boxtimes$ exists, is unique up to isomorphism, and is given by $Y \boxtimes X \cong (^{\neg}X \otimes {}^{\neg}Y)^{\neg}$. We use the word *left* because Eq. (5.29) involves the left negation operation $(-)^{\neg}$ as opposed to the right, $^{\neg}(-)$. Also recall that if $(\mathscr{C}, \otimes)$ is left reflexive and $\boxtimes$ is the left de Morgan dual of $\otimes$, then $\otimes$ is a right de Morgan dual of $\boxtimes$:

$$^{\neg}(Y \boxtimes X) \cong {}^{\neg}((^{\neg}X \otimes {}^{\neg}Y)^{\neg}) \cong {}^{\neg}X \otimes {}^{\neg}Y$$

We use the word *strong*, in contrast to *oplax* or *lax*, in our terminology *strong left de Morgan dual* because Eq. (5.29) is an isomorphism as opposed to just a morphism. Thus $(\mathscr{C}, \otimes)$ is left reflexive if and only if $(-)^{\neg} : (\mathscr{C}, \otimes) \to (\mathscr{C}^{\mathrm{op}}, \boxtimes)$ is a full and faithful strong magmal functor,[9]. Furthermore, $(\mathscr{C}, \otimes)$ is bireflexive if and only if $(-)^{\neg} \dashv {}^{\neg}(-)$ is an equivalence of magmal categories $(\mathscr{C}^{\mathrm{op}}, \boxtimes) \simeq (\mathscr{C}, \otimes)$. Typically, the left and right de Morgan duals of $\otimes$ coincide. For example, by Prop. 5.2.3, this is true if $(\mathscr{C}, \otimes)$ is bireflexive.

The facts we have stated here have analogous forms in the case that $\mathscr{C}$ has a *unital* magmal structure $(\otimes, \top)$. In that case, one also obtains a canonical isomorphism $\perp \cong \top^{\neg}$ via the Yoneda embedding, as well as an induced unital magmal structure $(\boxtimes, \perp)$ on $\mathscr{C}^{\mathrm{op}}$.

Proposition 5.2.7 *Let $(\mathscr{C}, \otimes, \top)$ be a $\mathscr{K}$-enriched left-closed unital magmal category, let $\perp \in \mathsf{Ob}(\mathscr{C})$ be arbitrary, and assume $\mathscr{C}$ is determined*[10] *by its global $\mathscr{K}$-elements with respect to $\top$. Then there is a canonical natural isomorphism $(X \otimes Y)^{\neg} \cong X \multimap Y^{\neg}$.*

Thus, under these hypotheses, $\otimes$ is left nuclear with respect to an operation $\boxtimes$ if and only if $\boxtimes$ is a strong left de Morgan dual of $\otimes$.

Proof First note the natural bijection of sets of global elements:

$$\mathsf{hom}_{\mathscr{C}}(\top, Y^{\neg} \boxtimes X^{\neg}) \cong \mathsf{hom}_{\mathscr{C}}(\top, (X \otimes Y)^{\neg}) \cong \mathsf{hom}_{\mathscr{C}}(X \otimes Y, \perp) \cong \mathsf{hom}_{\mathscr{C}}(\top, X \multimap Y^{\neg})$$

Then reflect $\mathsf{hom}_{\mathscr{C}}(\top, -)$ since $\mathscr{C}$ is determined by its global $\mathscr{K}$-elements. ■

[9] A left adjoint in CAT is a full and faithful functor if and only if its unit is an isomorphism.

[10] See Sec. 5.1.2. Enrichment is required in order to apply this to examples such as $\mathbb{R}$-FDVECT and $\widetilde{\mathrm{LCA}}$, which are each self-enriched. Intuitively, an abelian group is not determined by its underlying set of global elements (since a the group law cannot be recovered), but by its underlying abelian group of global elements, so this is why we need enrichment.

Here we implicitly used the opposite $(-)^{\neg\mathrm{op}}$ of the left negation functor $(-)^{\neg}$, in adherence to our stated convention. This was necessary in order to uncurry in the middle isomorphism in the proof. This is why Prop. 5.2.7 requires $\mathscr{C}$, as opposed to $\mathscr{C}^{\mathrm{op}}$, to be determined by its global $\mathscr{K}$-elements. We will suppress further such remarks.

Proposition 5.2.8 *Let $(\mathscr{C}, \otimes, \top)$ be a $\mathscr{K}$-enriched left-closed magmal category, let $\perp \in \mathsf{Ob}(\mathscr{C})$ be an arbitrary object, and assume $\mathscr{C}$ is determined by its global $\mathscr{K}$-quotients with respect to $\perp$. Then each natural isomorphism $(X \otimes Y)^{\neg} \cong X \multimap Y^{\neg}$ determines a pre-associative structure on $(\mathscr{C}, \otimes)$.*

Combining this with Prop. 5.2.7, we see that if $\mathscr{C}$ is determined both by its global $\mathscr{K}$-elements and by its global $\mathscr{K}$-quotients, then $(\mathscr{C}, \otimes)$ is pre-associative, since the canonical natural isomorphism $(X \otimes Y)^{\neg} \xrightarrow{\sim} X \multimap Y^{\neg}$ gives $\otimes$ a pre-associative structure.

Proof Consider the natural isomorphism of $\mathscr{K}$-objects of global quotients:

$$\begin{aligned}
\mathsf{hom}_{\mathscr{C}}((X \otimes Y) \otimes Z, \perp) &\cong \mathsf{hom}_{\mathscr{C}}(X \otimes Y, Z^{\neg}) \\
&\cong \mathsf{hom}_{\mathscr{C}}(X, Y \multimap Z^{\neg}) \\
&\cong \mathsf{hom}_{\mathscr{C}}(X, (Y \otimes Z)^{\neg}) \\
&\cong \mathsf{hom}_{\mathscr{C}}(X \otimes (Y \otimes Z), \perp)
\end{aligned}$$

The result follows since $\mathscr{C}$ is determined by its global $\mathscr{K}$-quotients. ■

Proposition 5.2.9 *Let $(\mathscr{C}, \otimes, \top)$ be a left-closed unital magmal category, let $\perp \in \mathsf{Ob}(\mathscr{C})$ be an arbitrary object, and assume $(\mathscr{C}, \otimes)$ is left reflexive with respect to $\perp$. Then $\mathscr{C}$ is determined by its global $\mathscr{K}$-quotients with respect to $\perp$ if and only $\mathscr{C}$ is determined by its global $\mathscr{K}$-elements with respect to $\top$.*

Thus, if $(\mathscr{C}, \otimes, \top, \perp)$ is unital, left closed, left reflexive, and *globally determined* (by its global elements with respect to $\top$ or equivalently by its global quotients with respect to $\perp$), then $(\mathscr{C}, \otimes)$ is pre-associative. Note that this is different from the property of $\mathscr{C}^{\mathrm{op}}$ being globally determined, since the roles of $\top$ and $\perp$ get swapped, though the result about associativity holds in that case as well by a symmetry argument.

Proof Let $\mathscr{C}$ be determined by its global $\mathscr{K}$-elements, let X and Y be $\mathscr{C}$-valued functors, and suppose $\mathsf{hom}_{\mathscr{C}}(X, \perp) \cong \mathsf{hom}_{\mathscr{C}}(Y, \perp)$ is a ($\mathscr{K}$-valued) natural isomorphism. Then:

$$\mathsf{hom}_{\mathscr{C}}(\top, X^{\neg}) \cong \mathsf{hom}_{\mathscr{C}}(X, \perp) \cong \mathsf{hom}_{\mathscr{C}}(Y, \perp) \cong \mathsf{hom}_{\mathscr{C}}(\top, Y^{\neg})$$

By hypothesis, this reflects a natural isomorphism $X^\neg \cong Y^\neg$, and then by left reflexivity, we obtain a natural isomorphism $X \cong {}^\neg(X^\neg) \cong {}^\neg(Y^\neg) \cong Y$ whose image under $\mathsf{hom}_{\mathscr{C}}(-, \perp)$ is the original $\mathscr{K}$-isomorphism. The converse is similar. ■

Proposition 5.2.10 *Let $(\mathscr{C}, \otimes)$ be a pre-associative biclosed magmal category, and let $\perp \in \mathsf{Ob}(\mathscr{C})$ be arbitrary. Then there are canonical natural isomorphisms $(X \otimes Y)^\neg \cong X \multimap Y^\neg$ and ${}^\neg(Y \otimes X) \cong {}^\neg Y \mathbin{\circ\!\!-} X$.*

Thus, if $(\mathscr{C}, \otimes)$ is pre-associative, biclosed, and equipped with a strong left de Morgan dual $\boxtimes$, then $(\mathscr{C}, \otimes)$ is left nuclear with respect to $\boxtimes$. In particular, if $(\mathscr{C}, \otimes)$ is pre-associative, biclosed, and left reflexive, then there exists a magmal product $\boxtimes$ on $\mathscr{C}^{\mathrm{op}}$ that uniquely satisfies either and hence both of the following: (i) $\boxtimes$ is the strong left de Morgan dual of $\otimes$; and (ii) $(\mathscr{C}, \otimes)$ is left nuclear with respect to $\boxtimes$. Finally, if $(\mathscr{C}, \otimes)$ is pre-associative, biclosed, and bireflexive, then $\mathscr{C}$ is both left and right nuclear with respect to the bidirectional de Morgan dual $\boxtimes$.

Proof The isomorphisms are given by internally currying, c.f. Prop. 5.2.2. ■

Proposition 5.2.11 *Let $(\mathscr{C}, \otimes)$ be a pre-associative biclosed magmal category, and let $\perp \in \mathsf{Ob}(\mathscr{C})$ be arbitrary. Then if $(\mathscr{C}, \otimes)$ is left reflexive (with respect to $\perp$), then $X \multimap Y \cong X^\neg \mathbin{\circ\!\!-} Y^\neg$. Likewise, if $(\mathscr{C}, \otimes)$ is right reflexive, then $Y \mathbin{\circ\!\!-} X \cong {}^\neg Y \multimap {}^\neg X$. The converses to each of these statements hold in the presence of a unital structure $(\otimes, \top)$.*

Thus, if $\mathscr{C}$ is pre-associative and bireflexive, then the left and right internal homs, $\multimap$ and $\mathbin{\circ\!\!-}$, determine each other.

Proof Assume $\mathscr{C}$ is left reflexive. Then we obtain a natural bijection:

$$\mathsf{hom}_{\mathscr{C}}(U, X \multimap Y) \cong \mathsf{hom}_{\mathscr{C}}(U, X \multimap {}^\neg(Y^\neg)) \cong \mathsf{hom}_{\mathscr{C}}(Y^\neg \otimes U \otimes X, \perp) \cong \mathsf{hom}_{\mathscr{C}}(U, X^\neg \mathbin{\circ\!\!-} Y^\neg)$$

So $X \multimap Y \cong X^\neg \mathbin{\circ\!\!-} Y^\neg$ by reflecting the Yoneda embedding. Conversely, given a natural isomorphism $X \multimap Y \cong X^\neg \mathbin{\circ\!\!-} Y^\neg$, substitute $\top$ for X and use unitality to obtain:

$$Y \cong \top \multimap Y \cong \perp \mathbin{\circ\!\!-} Y^\neg \cong {}^\neg(Y^\neg)$$

This shows that $\mathscr{C}$ is left reflexive. Right reflexivity works the same. ■

Proposition 5.2.12 *Let $(\mathscr{C}, \otimes)$ be a pre-associative biclosed magmal category that is bireflexive with respect to some $\perp \in \mathsf{Ob}(\mathscr{C})$. Then there exists $\top \in \mathsf{Ob}(\mathscr{C})$ and canonical unital structures $(\otimes, \top)$ and $(\boxtimes, \perp)$ for the primal and de Morgan dual operations, respectively.*

Proof It suffices to describe the canonical unital structure for $(\boxtimes, \perp)$. The right unitor is obtained by left reflexivity from the following string of canonical natural isomorphisms:

$$X \cong {}^{\neg}(X^{\neg}) \cong \perp \multimapinv X^{\neg} \cong {}^{\neg}(X^{\neg}) \boxtimes \perp \cong X \boxtimes \perp$$

Likewise, the left unitor for $(\boxtimes, \perp)$ is obtained using right reflexivity. Defining $\top$ as $\perp^{\neg}$ (or ${}^{\neg}\perp$), we obtain the canonical unital structure $(\otimes, \top)$ by de Morgan duality. ∎

Example Let $\mathscr{L}$ be a loop, that is, a unital magma in which for all $x, y \in \mathscr{L}$, there exist unique elements $x \multimap y$ and $y \multimapinv x$ satisfying $(x \multimap y)x = y$ (left evaluation) and $x(y \multimapinv x) = y$ (right evaluation). Viewed another way, $\mathscr{L}$ is precisely a discrete non-associative unital autonomous category (to be defined in Sec. 5.3) with product $\otimes$ and unit $\mathbb{1} = \top = \perp$. In particular, it is a biclosed magmal category, and the de Morgan dual $\boxtimes : \mathscr{L}^{\mathrm{op}} \times \mathscr{L}^{\mathrm{op}} \to \mathscr{L}^{\mathrm{op}}$ is the opposite of the primal magmal product $\otimes : \mathscr{L} \times \mathscr{L} \to \mathscr{L}$, not to be confused with the reverse-opposite. Explicitly, $\boxtimes = \otimes^{\mathrm{op}}$ is given by $x \boxtimes y = x \otimes y$ with respect to the defining identification of objects in $\mathscr{L}$ with objects in $\mathscr{L}^{\mathrm{op}}$. In the standard pattern of notational abuse, "$\otimes = \boxtimes$". This works in the expected way:

$$(xy)^{-1} = (x \otimes y)^{\neg} = y^{\neg} \boxtimes x^{\neg} = y^{-1}x^{-1}$$

A *group* is an associative loop.

Caution: In the math convention, the de Morgan dual would be (what in the physics convention we call) the reverse-opposite $\otimes^{\mathrm{rev\,op}}$, given by $y \otimes^{\mathrm{rev\,op}} x = x \otimes y$, not just the opposite, due to the swapped behavior of de Morgan duality. Thus, in the physics convention, we end up considering only the primal operation and applying the reversals manually (notationally), whereas in the math convention, this example is viewed in terms of the interaction of the primal operation and its reverse-opposite. In an unfortunate clash of terminology, in algebra (c.f. *opposite group*, *opposite algebra*), the operation $\otimes^{\mathrm{rev\,op}}$ is what is referred to as the *opposite* of the primal operation $\otimes$ (whereas $\otimes^{\mathrm{op}}$ is identified with $\otimes$).

The homset $\mathsf{hom}_{\mathscr{L}}(x, y)$ encodes (nothing more than) the boolean of whether $x = y$. Thus, the objects of $\mathscr{L}$ are not determined by their global elements or by their global quotients, (*i.e.* whether they equal $\mathbb{1}$) unless $\mathscr{L}$ has at most two elements. Then:

1. The existence of a group (such as $\mathbb{Z}/3\mathbb{Z}$) with more than two elements disproves the converses of Prop. 5.2.7 and Prop. 5.2.8.

2. Let $\mathscr{A}$ be a unital alternative algebra. Two-sided multiplicative inverses in $\mathscr{A}$ are unique when they exist, and these (bi-)invertible elements comprise the *unit loop* $\mathscr{A}^{\times}$. Inverses furthermore satisfy $y = (yx^{-1})x$, so it follows that $\mathscr{A}^{\times}$ is left nuclear: $x \multimap y = yx^{-1}$. The octonions $\mathbb{O}$ comprise a unital alternative algebra, and every nonzero octonion is invertible, i.e. $\mathbb{O}^{\times} = \mathbb{O} \setminus \{0\}$. This shows that it is possible to have nuclearity without associativity, let alone globally determined objects.

Example Building on Barr's example [Bar95], let $\mathscr{C} = \textsc{Sub}_{\textsc{Set}}(M)$ be the powerset of a magma M, and consider the magmal product given by $U \otimes V = \{uv \,|\, u \in U \text{ and } v \in V\}$. Then $(\mathcal{C}, \otimes)$ is biclosed, and $V \multimap W = \{u \in M \,|\, uV \subseteq W\}$ and $W \multimapinv V = \{u \in M \,|\, Vu \subseteq W\}$. If M has a unit 1 then $\top = \{1\}$ is the magmal unit of $\otimes$. An object $\perp$ is cyclic if and only if it is a normal subset: $m\perp = \perp m$ for all $m \in M$.

Example In Sec. 2.4.5 we noted that $\widetilde{\mathrm{LCA}}$ is a symmetric closed monoidal category. The de Morgan dual $\boxtimes$ of the tensor product $\otimes$ is defined in terms of Pontryagin duality. Some important isomorphisms are: $(\mathbb{Z}/d\mathbb{Z})^* \cong \mathbb{Z}/d\mathbb{Z}$, $\mathbb{R}^* \cong \mathbb{R}$, $\mathbb{Z}^* \cong \mathbb{T}$, $\mathbb{T}^* \cong \mathbb{Z}$, $0^* \cong 0$, and $(A \oplus B)^* \cong A^* \oplus B^*$. While $\mathbb{R}$-$\textsc{fdVect}$ is autonomous (the special case of star-autonomous where $\otimes \cong \boxtimes$), $\widetilde{\mathrm{LCA}}$ is properly star-autonomous. To see that $\otimes \ncong \boxtimes$, we use nuclearity and the fact that there are no group homomorphisms from the circle $\mathbb{T}$ to the integers $\mathbb{Z}$:

$$0 \cong \mathbb{T} \multimap \mathbb{Z} \cong \mathbb{Z} \boxtimes \mathbb{Z}$$

But $\mathbb{Z} \otimes \mathbb{Z} \cong \mathbb{Z}$. The de Morgan dual $\boxtimes$ coincides with the (opposite of the) 'par' operation, $\boxtimes \cong \parr^{\mathrm{op}}$, (not to be confused with $\parr^{\mathrm{rev\,op}}$, though of course this example is symmetric).

5.3 Star-autonomous categories

The theory of *star-autonomous categories* captures a general notion of *duality* internal to a category, including constructions such as the *dual vector space* in linear algebra as well as the *Pontryagin dual* of a locally compact abelian group. Star-autonomous categories, as defined by Barr, can be characterized as bireflexive biclosed monoidal categories [Bar79; Bar95]. Shortly after Barr's original paper, Cockett and Seely showed that a star-autonomous category is equivalently a linearly distributive category (LDC) that satisfies a property often called *nuclearity* [CS97a]. In this section, we approach the theory of star-autonomous categories from a different direction, without relying on associativity, and note some interactions with associativity and derive two formulas we believe to be new.

Traditionally, the linear distributors of an LDC are not required to be isomorphisms, and this is a major feature. Indeed, boolean algebras are a commonly cited first example where linear distribution is not invertible. The examples that motivate our interest in star-autonomous categories, however, have invertible linear distribution. These are the categories FGF-R-MOD and $\widetilde{\mathrm{LCA}}$. For this reason, in our approach, we start by assuming that the linear distributors are isomorphisms. In reality, this assumption is not used much, but even more interestingly, we find that in the associative case, the theory is no less general. This is because we do not require the $\parr$ operation (or technically $\parr^{\mathrm{op}}$) to be the de Morgan dual of $\otimes$. This leads to a three-way distinction for the various levels of coherence of the negation adjunction $^{\neg}(-) \dashv (-)^{\neg}$.

One goal of this exposition is to highlight when aspects of the theory of star-autonomous categories are instances of more general phenomena in category theory, for example by focusing on aspects of the adjunction $(-)^{\neg} \dashv {}^{\neg}(-)$, in order to defer calculations to the proofs of more powerful theorems. Another is to point out the different roles of associativity and linear distributivity. While the former is understood to generalize the associativity of function composition, the latter is intimately connected with duality. We do not require associativity when we lay out the theory of star-autonomous categories, with the exception of showing an interaction between associativity, de Morgan duality, and nuclearity. However, as we note in Appx. C, from invertible unitors and invertible linear distributors, one derives a canonical associative structure. We do not scrutinize the exact properties needed of the unitors for now, but we do not explicitly require associativity, and thus only call for a *non-associative LDC*. The irrelevance of associativity in the theory prompts us to find new formulas for the inverse nuclearizer and internal composition into the dualizing object.

5.3.1 Ordinary and linear distributivity

Let $(\mathscr{C}, \otimes)$ be a biclosed magmal category.

Since left adjoints preserve colimits, the coproduct $+$ (if available) distributes over $\otimes$:

$$(X+Y) \otimes Z \cong X \otimes Z + Y \otimes Z \qquad \text{and} \qquad X \otimes (Y+Z) \cong X \otimes Y + X \otimes Z$$

Dually, if $\mathscr{C}$ is equipped with a co-biclosed functor $\boxtimes : \mathscr{C}^{\mathrm{op}} \times \mathscr{C}^{\mathrm{op}} \to \mathscr{C}^{\mathrm{op}}$ and has coproducts, then:

$$(X \times Y) \boxtimes Z \cong X \boxtimes Z \times Y \boxtimes Z \qquad \text{and} \qquad X \boxtimes (Y \times Z) \cong X \boxtimes Y \times X \boxtimes Z$$

So far, we have not imposed de Morgan duality or any other relationship between $\otimes$ and $\boxtimes$, nor have we even fixed a dualizing object $\bot$. A classic example of distributivity is the powerset $\mathrm{S{\scriptsize UB}}_{\mathrm{S{\scriptsize ET}}}(V)$ of a set V, in which case $\otimes \cong \times \cong \cap$ is the product (intersection) and $\boxtimes \cong + \cong \cup$ is the coproduct (union). Another is $\mathrm{S{\scriptsize ET}}$, where $\otimes \cong \times$ is the Cartesian product and $\boxtimes \cong + \cong \sqcup$ is the disjoint union. Likewise, in $\mathrm{F{\scriptsize IN}S{\scriptsize ET}}$ and its decategorification, the natural numbers $\mathbb{N}_0$, the operations $\otimes$ and $\boxtimes$ are again the product and sum (coproduct). A familiar example where $\otimes$ is not just the product is the biclosed monoidal category k-$\mathrm{{\scriptsize FD}V{\scriptsize ECT}}$, in which $+ \cong \times$ is the biproduct (direct sum) $\oplus$ and $\otimes \cong \boxtimes$ is the tensor product of finite dimensional k-vector spaces. There are many related examples.

In Sec. 5.2.6, we fixed a dualizing object $\bot$ with which to form negations without imposing any sort of distributive law between the primal operation $\otimes$ and the left dual operation $\boxtimes$, defined either by left de Morgan duality or left nuclearity. It was shown in [CS97a] that, (assuming associativity,) a linear distributivity always holds:

Theorem 5.3.1 *Let $(\mathscr{C}, \otimes, \bot)$ be an associative biclosed magmal category. Then there exist canonical natural transformations, which we call "pre-linear distributors":*

$$X \otimes (Z \multimapinv Y^{\neg}) \to Z \multimapinv (X \otimes Y)^{\neg} \qquad ({}^{\neg}Y \multimap X) \otimes Z \to {}^{\neg}(Y \otimes X) \multimap X \tag{5.30}$$

Moreover, if $(\mathscr{C}, \otimes, \bot)$ is bireflexive, we obtain linear distributors:

$$X \otimes (Y \boxtimes Z) \to (X \otimes Y) \boxtimes Z \qquad (X \boxtimes Y) \otimes Z \to X \boxtimes (Y \otimes Z) \tag{5.31}$$

where $\boxtimes$ is the de Morgan dual of $\otimes$.

By the existence of non-associative unital loops (in which "$\boxtimes = \otimes$"), such as the nonzero octonions $\mathbb{O}^\times$, we see that this theorem makes crucial use of associativity. This demonstrates how Cockett and Seely's characterization of star-autonomous categories as bireflexive LDCs breaks down in the non-associative case.

Proof By Prop. 5.2.10, we have a natural isomorphism $(X \otimes Y)^\neg \xrightarrow{\sim} X \multimap Y^\neg$ (in $\mathscr{C}$), which we left uncurry to obtain a natural transformation $\phi_{YX} : (X \otimes Y)^\neg \otimes X \to Y^\neg$. Composing this with $\ulcorner \mathsf{righteval}_Z^{Y^\neg} \urcorner : Y^\neg \to (Z \multimapinv Y^\neg) \multimap Z$, we obtain a natural transformation $\psi_{ZYX} : (X \otimes Y)^\neg \otimes X \to (Z \multimapinv Y^\neg) \multimap Z$. Finally, by associativity, this may be recurried as $\rho_{ZYX} : X \otimes (Z \multimapinv Y^\neg) \to Z \multimapinv (X \otimes Y)^\neg$. The weak left linear distributor is obtained by applying right nuclearity and left reflexivity. The right version is similar. ■

The linear distributors guaranteed by Thm. 5.3.1 are not necessarily isomorphisms, though we are more interested in the case where they are. The classical example where the linear distributors are *not* isomorphisms is a Boolean lattice $\mathscr{B}$, such as a powerset $\textsc{Sub}_{\textsc{Set}}(V)$ for some set V. One takes $\otimes \cong \times \cong \cap$ to be the product (meet/intersection) and $\boxtimes \cong + \cong \cup$ to be the coproduct (join/union). Even though these satisfy the ordinary distributive law, they also satisfy weak linear distributivity, as can be verified directly (using Venn diagrams or natural deduction) or by applying Thm. 5.3.1. The currying adjunction and nuclearity are embodied by the following statement:

$$X \cap Y \subseteq Z \qquad \text{if and only if} \qquad X \subseteq Z \cup Y^\neg$$

where $Y^\neg = {}^\neg Y = V \smallsetminus Y$ is the set complement. Clearly, ${}^\neg(Y^\neg) = Y = ({}^\neg Y)^\neg$ and $\cap$ is associative, so the thoerem applies. This can be contrasted with the lattice $\textsc{Sub}_{k\text{-}\textsc{FDVect}}(V)$ of subspaces of a k-vector space V, which is not Cartesian closed.

5.3.2 Star-autonomous categories: overview

Let $(\mathscr{C}, \otimes, \parr)$ be a non-associative LDC with invertible linear distributors.

Each object X gives rise to a sequence of (linear) adjoints[11], which is either an n-cycle for some $n \in \{1, 2, \cdots\}$, or (by uniqueness of adjoints) has no repeated (isomorphic) terms and in each direction either eventually terminates or continues indefinitely:

$$\cdots X^{**} \dashv X^* \dashv X \dashv {}^*X \dashv {}^{**}X \dashv \cdots \tag{5.32}$$

We will soon see that if $(\mathscr{C}, \otimes, \perp)$ is associative, biclosed, and bireflexive, then X has a left adjoint X^* if and only if X has a right adjoint ${}^*X$, in which case the only way for Eq. (5.32) to terminate in either direction is if it consists of a single term X, not to be confused with the situation of a self-dual object (1-cycle).

Adjointness is one way to formulate the notion of *dual objects*. For another, since $(\mathscr{C}, \otimes)$ is biclosed, we may consider the left and right negations, defined by $X^\neg \cong X \multimap \perp$ and ${}^\neg X \cong \perp \multimapinv X$ for some dualizing object $\perp$. The natural question, then, is when these two notions of *dual* coincide: when is the left negation isomorphic to the left adjoint, $X^* \cong X^\neg$, or equivalently, when is $X^\neg \dashv X$? It turns out (very nontrivially) that assuming $(\mathscr{C}, \otimes)$ is biclosed (as always) and that X has a left adjoint X^*, then it follows that $X^* \cong X^\neg$.

Recall that an adjunction $X^* \dashv X$ consists of objects X^* and X together with morphisms $\eta : \top \to X \parr X^*$ and $\epsilon : X^* \otimes X \to \perp$ satisfying the zigzag identities:

$$\begin{tikzcd} X \arrow[r, "\eta\otimes X"] \arrow[dr, "X"'] & X \parr X^* \otimes X \arrow[d, "X\parr\epsilon"] \\ & X \end{tikzcd} \qquad \begin{tikzcd} X^* \arrow[r, "X^*\otimes\eta"] \arrow[dr, "X^*"'] & X^* \otimes X \parr X^* \arrow[d, "\epsilon\parr X^*"] \\ & X^* \end{tikzcd}$$

left zigzag $\qquad\qquad$ right zigzag

[11] The adjunction $X^* \dashv X$ takes place in the delooping linear bicategory $\mathbf{B}\mathscr{C}$, not to be confused with the negation adjunction $(-)^\neg \dashv {}^\neg(-)$, which takes place in the (ordinary) bicategory CAT. The left adjoint X^* of X has often been called a left negation (eg. in [CS97a]), but we use the word *negation* as in Sec. 5.2.5. Also, invertibility of the linear distributors isn't required for this definition to work, but we require it anyway.

It turns out that as soon as the left zigzag of $X^* \dashv X$ is satisfied, it follows that $X^\neg \dashv X$, so by uniqueness of left adjoints, the right zigzag is satisfied if and only if $X^* \cong X^\neg$. To see why, first assume that the left zigzag of $X^* \dashv X$ holds. Then by the currying identities, the following diagram commutes, showing that the left zigzag of $X^\neg \dashv X$ holds:

$$\begin{tikzcd}
X \arrow[r, "\eta\otimes X"] \arrow[dr, "X"'] & X \parr X^* \otimes X \arrow[r, "X \parr \lceil \epsilon \rceil \otimes X"] \arrow[d, "X \parr \epsilon"] & X \parr X^\neg \otimes X \arrow[d, "X \parr \mathsf{lefteval}_\perp^X"] \\
& X \arrow[r, equal] & X
\end{tikzcd}$$

The next step is to show that as soon as the left zigzag of $X^\neg \dashv X$ holds, so does the right, and so indeed $X^\neg \dashv X$. We prove this and the other things in the next subsection.

In Sec. 5.2.6, we began with a magmal product $\otimes$ on $\mathscr{C}$, an object $\perp$, and a magmal product $\boxtimes$ on $\mathscr{C}^{\mathrm{op}}$ called its left de Morgan dual. We then defined *left nuclearity with respect to* $\boxtimes$, and showed that if $(\mathscr{C}, \otimes)$ has unit $\top$, then left reflexivity implies left nuclearity with respect to $\boxtimes$. Now we start with a magmal product $\parr$ on $\mathscr{C}$, which is required to linearly distribute with $\otimes$ in the invertible sense, but is not required to be its de Morgan dual, and define *left nuclearity with respect to* $\parr$: X is *left nuclear* in this sense if it has a left adjoint. Note that left nuclearity with respect to $\parr$ is a property, not additional structure. For the moment it seems that we have just introduced a synonym for *left adjoint*, but we will review how nuclearity extends from a property of objects to one of morphisms [Row88; CS99]. Uniqueness of left adjoints can be used to show that left nuclearity with respect to $\parr$ implies left reflexivity, that is, that $\lfloor \mathsf{lefteval}_\perp^X \rfloor : X \to {}^\neg(X^\neg)$ is an isomorphism. Interestingly, the converse is not necessarily true. That is, it may be that X, or just as well the whole category $(\mathscr{C}, \otimes, \parr)$, is left reflexive but not left nuclear with respect to $\parr$.

For example, a nontrivial Boolean algebra $(\mathscr{C}, \otimes = \wedge, \parr = \wedge)$, such as $\mathbb{F}_2$, is a reflexive LDC with strong linear distributors that is not nuclear. The linear distributors are the associators, as we are in the degenerate $\otimes \cong \parr$ case. Yet $(\mathscr{C}, \otimes, \parr)$ is not nuclear because the de Morgan dual of $\otimes$ is $\boxtimes = \vee^{\mathrm{op}}$, not $\parr^{\mathrm{op}} = \wedge^{\mathrm{op}}$. Here the difference between our approach and Cockett and Seely's approach is clear. In [CS97a], the de Morgan dual $\boxtimes^{\mathrm{op}}$ is used as their second operation $\parr$, and indeed, $(\mathscr{C}, \otimes, \boxtimes)$ is nuclear. With this particular example, we can trade invertibility of the linear distributors for that of the nuclearizer by instead taking $\boxtimes^{\mathrm{op}} = \vee$ as the second operation.

The version of nuclearity we discuss here at first appears to be completely different from the version defined in Sec. 5.2.6. However, the left linear distributor (even in the non-invertible case) determines the *left nuclearizer* $\mathsf{leftnuc}_Y^X : Y \parr X^\neg \to X \multimap Y$. Although $\mathsf{leftnuc}_Y^X$ might not be invertible, we will show that X is left nuclear with respect to $\parr$ if and only if $\mathsf{leftnuc}_X^X$ is an isomorphism, relating back to our original definition of nuclearity in Sec. 5.2.6. In the other direction, we have already recounted Cockett and Seely's construction Thm. 5.3.1 of the weak linear distributors in terms of the de Morgan dual $\boxtimes$.

Conjecture Let $(\mathscr{C}, \otimes, \perp)$ be a bireflexive biclosed monoidal category and let $\boxtimes$ be the strong de Morgan dual. Suppose there exists a (weak) linearly distributive structure relating $\otimes$ and $\boxtimes^{\mathrm{op}}$, but forget the particular structure as well as the de Morgan duality structure. (So we only assume existence of these.) Then the constructions (*i*) of the (weak) nuclearizer, and thereby of the (weak) de Morgan laws, given a (weak) linearly distributive structure; and (*ii*) of the (weak) linearly distributive structure given a (strong) de Morgan structure, are mutually inverse in the case that everything is strong.

Each side of the negation adjunction for a biclosed magmal LDC $(\mathscr{C}, \otimes, \parr)$ with invertible linear distributors has three levels of coherence.[12]

$$\begin{tikzcd} \mathscr{C}^{\mathrm{op}} = (\mathscr{C}^{\mathrm{op}}, \parr^{\mathrm{op}}) \arrow[rr, bend right, "\neg(-)"'] \arrow[rr, phantom, "\perp"] & & (\mathscr{C}, \otimes) = \mathscr{C} \arrow[ll, bend right, "(-)^\neg"'] \end{tikzcd} \tag{5.33}$$

We always require $(\mathscr{C}, \otimes, \parr)$ to be biclosed with respect to $\otimes$. The first level involves nothing more. Second, left negation $(-)^\neg : \mathscr{C} \to \mathscr{C}^{\mathrm{op}}$ may or may not be full and faithful, which is equivalent to $(\mathscr{C}, \otimes)$ being left reflexive. Third, we may equip (if it exists) a strong magmal structure on $(-)^\neg$. In other words, we may equip a strong left de Morgan law (if it exists), imposing that $\parr^{\mathrm{op}}$ be the left de Morgan dual of $\otimes$. If there is a pre-associative structure on $\otimes$, then the specification of a strong left de Morgan law is equivalent to that of a strong left nuclearizer. The following theorem shows that, in the pre-associative case, the third level of coherence implies the second level. By the results of Sec. 5.2.4, if $(\mathscr{C}, \otimes, \perp)$ is bireflexive, then (regardless of associativity), the left and right versions of the third level of coherence merge, and $\parr^{\mathrm{op}}$ is the bidirectional de Morgan dual.

[12]Recall that our definition of magmal functors is "reversed" to simplify notation and terminology in teh physics convention. If it weren't, the object on the left of Eq. (5.33) would be $\mathscr{C}^{\mathrm{rev\,op}} = (\mathscr{C}^{\mathrm{op}}, \parr^{\mathrm{rev\,op}})$.

Theorem 5.3.2 *Let $(\mathscr{C}, \otimes, \parr)$ be a magmal LDC and assume $\otimes$ is biclosed. Then* (1) *if $(\mathscr{C}, \otimes, \perp)$ is (canonically) left nuclear with respect to $\parr$, then $(\mathscr{C}, \otimes, \perp)$ is left reflexive. Moreover,* (2) *if $\otimes$ is pre-associative, then there is a canonical oplax left de Morgan law (and lax right de Morgan law), and* (3) *the existence of* ***any*** *strong left nuclearizer (or equivalently that of a strong left de Morgan law) implies that $(\mathscr{C}, \otimes, \perp)$ is left reflexive.*

Since $\parr^{\text{op}}$ is not necessarily the de Morgan dual in Thm. 5.3.2, even if the the canonical weak linear distributors of Eq. (5.31) relating the de Morgan dual $\boxtimes$ and $\otimes$ are isomorphisms, it may still be that $\parr \ncong \boxtimes^{\text{op}}$. For example, we may artificially take the second operation $\parr$ on $\widetilde{\text{LCA}}$ to be $\otimes$ instead of the more natural choice, the de Morgan dual $\boxtimes^{\text{op}}$. Then the canonical (weak) linear distributors with the de Morgan dual are isomorphisms, and we have reflexivity without nuclearity. In the other direction, if we take $\otimes$ and $\parr$ to be the product $\wedge$ and coproduct $\vee$ on a Boolean algebra, then $\parr \cong \boxtimes$, so we have nuclearity and hence reflexivity, but the canonical linear distributors are not isomorphisms.

Proof Part (1) is Cor. 5.3.5, which we prove in the next section. For (2), observe that a canonical oplax left de Morgan law $\phi_{XY} : Y^{\neg} \parr X^{\neg} \to (X \otimes Y)^{\neg}$ is obtained by composing the natural isomoprhism $X \multimap Y^{\neg} \cong (X \otimes Y)^{\neg}$ (by pre-associativity) with the canonical weak left nuclearizer $\mathsf{leftnuc}^{X}_{Y^{\neg}} : Y^{\neg} \parr X^{\neg} \to X \multimap Y^{\neg}$. For (3), by the second part of doctrinal adjunction, the existence of any strong left de Morgan law implies ϕ itself is an isomorphism, and we may apply (1). ■

It is a nontrivial feature of the negation adjunction of a biclosed pre-associative magmal LDC that strong left de Morgan duality implies left reflexivity. That is, there exist strong magmal (or even monoidal) adjunctions that are not equivalences, as witnessed by the negation adjunction on any non-classical de Morgan Heyting algebra.

The *left nucleus* of a biclosed LDC with invertible linear distributors is the full subcategory on left nuclear objects. By results from the next section, the left nucleus is a two-sided ideal under composition, and $(\mathscr{C}, \otimes, \parr)$ is left nuclear if and only if it is equal to its left nucleus. As we have established, pre-associativity and bireflexivity are enough to make the left and right versions merge. In other words, if $(\mathscr{C}, \otimes, \parr)$ is associative and bireflexive, then the left and right nuclei coincide, in which case we simply call them the *nucleus*.

5.3.3 Nuclearity

Let $(\mathscr{C}, \otimes, \parr)$ be a biclosed magmal LDC with invertible linear distributors.

A morphism $f : X \to Y$ in $\mathscr{C}$ is *left nuclear* if it has a *left pseudoname*, that is, a morphism $p : \top \to Y \parr X^{\neg}$ such that the following diagram on the left commutes, and *right nuclear* if it has a *right pseudoname*, that is, a morphism $q : \top \to {}^{\neg}X \parr Y$ such that the following diagram on the right commutes:

$$\begin{tikzcd} X \arrow[r, "p \otimes X"] \arrow[dr, "f"'] & Y \parr X^{\neg} \otimes X \arrow[d, "Y \parr \mathsf{lefteval}^X_\perp"] \\ & Y \end{tikzcd} \qquad \begin{tikzcd} X \arrow[r, "X \otimes q"] \arrow[dr, "f"'] & X \otimes {}^{\neg}X \parr Y \arrow[d, "\mathsf{righteval}^X_\perp \parr Y"] \\ & Y \end{tikzcd} \tag{5.34}$$

Equivalently, nuclearity may be expressed in terms of the *left* and *right nuclearizer*, which are defined by left currying $Y \parr \mathsf{lefteval}^X_\perp$ or right currying $\mathsf{righteval}^X_\perp \parr Y$, respectively. The diagrams of Eq. (5.34) are respectively equivalent to the following curried versions:

$$\begin{tikzcd} \top \arrow[r, "p"] \arrow[dr, "\lceil f \rceil"'] & Y \parr X^{\neg} \arrow[d, "\mathsf{leftnuc}^X_Y"] \\ & X \multimap Y \end{tikzcd} \qquad \begin{tikzcd} \top \arrow[r, "q"] \arrow[dr, "\lfloor f \rfloor"'] & {}^{\neg}X \parr Y \arrow[d, "\mathsf{rightnuc}^X_Y"] \\ & Y \multimapinv X \end{tikzcd} \tag{5.35}$$

We call an object X *left* (resp. *right*) *nuclear* if id_X is. We will eventually show that if a left (resp. right) pseudoname exists then $\mathsf{leftnuc}^X_Y$ (resp. $\mathsf{rightnuc}^X_Y$) is invertible, which implies that pseudonames are unique if they exist. Before proving invertibility of the nuclearizer, the following theorem implies uniqueness of pseudonames of objects.

Theorem 5.3.3 *If X is left nuclear, then $X^{\neg} \dashv X$.*

In other words, as soon as the left zigzag of $X^{\neg} \dashv X$ is satisfied, so is the right. By uniqueness of the adjunction unit, the left pseudoname for X is then unique. The same applies for right nuclearity, and we denote the respective pseudonames, if they exist, by:

$$\widetilde{\mathsf{leftcoeval}}^X : \top \to X \parr X^{\neg} \qquad \widetilde{\mathsf{rightcoeval}}^X : \top \to {}^{\neg}X \parr X$$

Proof Let $L = - \otimes X$ and $R = X \multimap -$ so that $(L, R, \mathsf{leftcoeval}^X, \mathsf{lefteval}^X)$ is the left currying adjunction across X (in $\textsc{Cat}$). Let p be a pseudoname for id_X. Then consider:

$$
\begin{tikzcd}
 & X \parr X^{\neg} \otimes X \arrow[d, "\mathsf{leftnuc}_{X,X} \otimes X"] \\
L\top = X \arrow[ur, "p \otimes X"] \arrow[r, "\mathsf{leftcoeval}^X_\top \otimes X = L(\mathsf{leftcoeval}^X_\top)" description] \arrow[dr, "X"'] \arrow[ur, phantom, "\text{(1L)}" near end, shift right=4ex] \arrow[dr, phantom, "\text{(2L)}" near end, shift left=4ex] & (X \multimap X) \otimes X = LRL\top \arrow[d, "\mathsf{lefteval}^X_X = \mathsf{lefteval}^X_X L(\mathsf{id}_X)"] \\
 & X = L\top
\end{tikzcd}
\tag{5.36}
$$

(1L) commutes since it is $\mathcal{D} \otimes X$ where $\mathcal{D}$ is the left diagram in Eq. (5.35). Equation (2L) commutes since it is the left zigzag identity of $L \dashv R$ instantiated at $\top$. Next,

$$
\begin{tikzcd}
 & X^{\neg} \otimes X \parr X^{\neg} \arrow[d, "\mathsf{leftnuc}_{X, X^{\neg} \otimes X}"] \\
R\bot = X^{\neg} \arrow[ur, "X^{\neg} \otimes p"] \arrow[r, "\mathsf{leftcoeval}^X_{X^{\neg}} = \mathsf{leftcoeval}^X_{X^{\neg}} R(\mathsf{id}_X)" description] \arrow[dr, "X^{\neg}"'] \arrow[ur, phantom, "\text{(1R)}" near end, shift right=4ex] \arrow[dr, phantom, "\text{(2R)}" near end, shift left=4ex] & X \multimap (X^{\neg} \otimes X) = RLR\bot \arrow[d, "X \multimap \mathsf{lefteval}^X_\bot = R(\mathsf{lefteval}^X_\bot)"] \\
 & X^{\neg} = R\bot
\end{tikzcd}
\tag{5.37}
$$

(1R) commutes since it is obtained by left currying the following commutative diagram:

$$
\begin{tikzcd}
 & X^{\neg} \otimes X \parr X^{\neg} \otimes X \arrow[d, "X^{\neg} \otimes X \parr \mathsf{lefteval}^X_\bot"] \\
X^{\neg} \otimes X \arrow[ur, "X^{\neg} \otimes (p \otimes X) \overset{\mathrm{coh}}{=} (X^{\neg} \otimes p) \otimes X"] \arrow[r, phantom, "\text{(1R)}'"] \arrow[dr, "X^{\neg} \otimes X"'] & {} \\
 & X^{\neg} \otimes X
\end{tikzcd}
$$

The equality $\overset{\text{coh}}{=}$ is due to a coherence axiom. This diagram (1R)$'$, in turn, is just $X^\neg \otimes \mathcal{D}'$ where $\mathcal{D}'$ is the left diagram of Eq. (5.34). (2R) commutes because it is the right zigzag identity of $L \dashv R$ instantiated at $\perp$. The composite of the vertical arrows in Eq. (5.36) is:

$$\mathsf{lefteval}^X_X(\mathsf{leftnuc}_{X,X} \otimes X) = \mathsf{lefteval}^X_X(\lceil X \parr \mathsf{lefteval}^X_\perp \rceil \otimes X) = X \parr \mathsf{lefteval}^X_\perp$$

The composite of the vertical arrows in Eq. (5.37) is:

$$\begin{aligned}(\mathsf{id}_X \multimap \mathsf{lefteval}^X_\perp)\lceil X^\neg \otimes X \parr \mathsf{lefteval}^X_\perp \rceil &= \lceil \mathsf{lefteval}^X_\perp (X^\neg \otimes X \parr \mathsf{lefteval}^X_\perp)\rceil \\ &= \lceil \mathsf{lefteval}^X_\top (\mathsf{lefteval}^X_\perp \parr X^\neg \otimes X)\rceil \\ &= \mathsf{lefteval}^X_\perp \parr X^\neg\end{aligned}$$

Commutativity of Eq. (5.36) and Eq. (5.37) certifies the adjunction $(X^\neg, X, p, \mathsf{lefteval}^X_\perp)$ in $\mathbf{B}\mathscr{C}$. ∎

Proposition 5.3.4 *If X is left nuclear then $X^\neg$ is right nuclear with right pseudoname:*

$$\mathsf{right}\widetilde{\mathsf{coeval}}^X = (\lfloor \mathsf{lefteval}^X_\perp \rfloor \parr X^\neg)\mathsf{left}\widetilde{\mathsf{coeval}}^X \tag{5.38}$$

Proof Let X be left nuclear. It suffices to show that the right-hand-side q of Eq. (5.38) is a right pseudoname for $X^\neg$. The left zigzag certifying right nuclearity of $X^\neg$ is as follows:

$$\begin{tikzcd} X^\neg \arrow[r, "X^\neg \otimes q"] & X^\neg \otimes {}^\neg(X^\neg) \parr X^\neg \arrow[d, "\mathsf{righteval}^{X^\neg}_\perp \parr X^\neg"] \\ & X^\neg \end{tikzcd} = \begin{tikzcd} X^\neg \arrow[r, "X^\neg \otimes \mathsf{left}\widetilde{\mathsf{coeval}}^X"] & X^\neg \otimes X \parr X^\neg \arrow[d, "X^\neg \otimes \lfloor \mathsf{lefteval}^X_\perp \rfloor \parr X^\neg"] \\ & X^\neg \otimes {}^\neg(X^\neg) \parr X^\neg \arrow[d, "\mathsf{righteval}^{X^\neg}_\perp \parr X^\neg"] \\ & X^\neg \end{tikzcd}$$

$$= \begin{tikzcd} X^\neg \arrow[r, "X^\neg \otimes \mathsf{left}\widetilde{\mathsf{coeval}}^{X^\neg}"] & X^\neg \otimes X \parr X^\neg \arrow[d, "\mathsf{lefteval}^X_\perp \parr X^\neg"] \\ & X^\neg \end{tikzcd}$$

$$= \begin{tikzcd} X^\neg \arrow[r, "X^\neg"] & X^\neg \end{tikzcd}$$

The last step here by the right zigzag of the left nuclearity of X. ∎

Corollary 5.3.5 *If X is left nuclear then X is left reflexive, and furthermore:*

$$\lceil \mathsf{lefteval}_{\perp}^{X} \rceil = ({}^{\neg}(X^{\neg}) \parr \mathsf{lefteval}_{\perp}^{X})(\widetilde{\mathsf{rightcoeval}}^{X^{\neg}} \otimes X) : X \xrightarrow{\sim} {}^{\neg}(X^{\neg}) \tag{5.39}$$

$$\lceil \mathsf{lefteval}_{\perp}^{X} \rceil^{-1} = (X \parr \mathsf{righteval}_{\perp}^{X^{\neg}})(\widetilde{\mathsf{leftcoeval}}^{X} \otimes {}^{\neg}(X^{\neg})) : {}^{\neg}(X^{\neg}) \xrightarrow{\sim} X \tag{5.40}$$

Proof Uniqueness of right adjoints applied to the adjunctions $X^{\neg} \dashv X$ and $X^{\neg} \dashv {}^{\neg}(X^{\neg})$ asserts that the path along the top of the following diagram is an isomorphism:

$$\begin{tikzcd}
 & & {}^{\neg}(X^{\neg}) \parr X^{\neg} \otimes X \arrow[drr, "{}^{\neg}(X^{\neg}) \parr \mathsf{lefteval}_{\perp}^{X}"] & & \\
X \arrow[urr, "\widetilde{\mathsf{rightcoeval}}^{X^{\neg}} \otimes X"] \arrow[rr, "\widetilde{\mathsf{leftcoeval}}^{X} \otimes X"'] \arrow[drr, "X"'] & & X \parr X^{\neg} \otimes X \arrow[u, "\lceil \mathsf{lefteval}_{\perp}^{X} \rceil \parr X^{\neg} \otimes X"] \arrow[d, "X \parr \mathsf{lefteval}_{\perp}^{X}"] & & {}^{\neg}(X^{\neg}) \\
 & & X \arrow[urr, "\lceil \mathsf{lefteval}_{\perp}^{X} \rceil"'] & &
\end{tikzcd}$$

It also asserts that the inverse of the path along the top is the right-hand-side of Eq. (5.40). Finally, the path along the bottom is $\lceil \mathsf{lefteval}_{\perp}^{X} \rceil$, so X is left reflexive and Eq. (5.39) holds. ∎

Theorem 5.3.6 *Let $f : X \to Y$, $h : W \to X$, and $g : Y \to Z$. Assume f is left nuclear with left pseudoname p. Then gfh is left nuclear and has left pseudoname $(g \parr h^{\neg})p$, and we have the following currying formula:*

$$(h \multimap g)\lceil f \rceil = \lceil gfh \rceil : \top \to W \multimap Z \tag{5.41}$$

Besides giving a useful currying formula, this theorem shows that the left nuclear morphisms comprise not just a full subcategory, but a two-sided ideal, called the *left nucleus*. Recall that assuming bireflexivity and associativity, left and right nuclearity coincide, and thus so do the left and right nuclei, in which case one simply refers to the *nucleus*.

Proof The larger square part of the following diagram reduces to the naturality square of $\mathsf{id} \parr \mathsf{lefteval}_{\perp}$, which commutes since both id and $\mathsf{lefteval}_{\perp}$ are natural transformations–the latter by Mac Lane's parameter theorem. The smaller square commutes since $p \otimes -$ is natural, and the triangle commutes since p is a left pseudoname for f.

$$\begin{tikzcd}
W \arrow[r, "p\otimes W"] \arrow[d, "h"'] & Y \parr X^{\neg} \otimes W \arrow[rr, "g \parr h^{\neg} \otimes W"] \arrow[d, "Y \parr X^{\neg} \otimes h"] & & Z \parr W^{\neg} \otimes W \arrow[dd, "Z \parr \mathsf{lefteval}_{\perp}^{W}"] \\
X \arrow[r, "p\otimes X"] \arrow[dr, "f"'] & Y \parr X^{\neg} \otimes X \arrow[d, "Y \parr \mathsf{lefteval}_{\perp}^{X}"] & & \\
& Y \arrow[rr, "g"'] & & Z
\end{tikzcd}$$

This shows that $(g \parr h^{\neg})p$ is a left pseudoname for gfh. In other words (left currying):

$$\ulcorner gfh \urcorner = \mathsf{leftnuc}_{Z}^{W}(g \parr h^{\neg})p \tag{5.42}$$

Now, since naturality is preserved under adjunctions, in this case the left currying adjunction, $\mathsf{leftnuc}$ is natural in both arguments, and we obtain the following commutative diagram:

$$\begin{tikzcd}
\top \arrow[r, "p"] \arrow[dr, "\ulcorner f \urcorner"'] & Y \parr X^{\neg} \arrow[r, "g \parr h^{\neg}"] \arrow[d, "\mathsf{leftnuc}_{Y}^{X}"] & Z \parr W^{\neg} \arrow[d, "\mathsf{leftnuc}_{Z}^{W}"] \\
& X \multimap Y \arrow[r, "h \multimap g"'] & W \multimap Z
\end{tikzcd} \tag{5.43}$$

Putting this together with Eq. (5.42), we obtain the desired formula Eq. (5.41). ■

Corollary 5.3.7 *Let $f : X \to Y$ be a left nuclear morphism. Then*

1. *If f has a left inverse, then X is left nuclear.*
2. *If f has a right inverse, then Y is left nuclear.*

5.3.4 The inverse nuclearizer and internal composition into the dualizing object

By Thm. 5.3.8, if a morphism $\phi : X \to Y$ is left nuclear, then the $\mathsf{leftnuc}_Y^X$ is an isomorphism. A formula for $(\mathsf{leftnuc}_Y^X)^{-1}$, which we call the *inverse nuclearizer*, was given in Rowe's paper [Row88], and appeared shortly after in Higgs-Rowe [HR89], but in both cases, checking its correctness was left to the reader. The result has been cited subsequently, eg. in [ABP98], but we could not find a complete proof in the literature. Mac Lane had conjectured a coherence theorem should hold for symmetric monoidal categories, and this was later proved by Soloviev in [Sol97]. This theorem reduces certain equality checks between morphisms to type-checking, and certifies Rowe's formula for the inverse nuclearizer.

We work in slightly more generality than Higgs-Rowe, since we do not require $\otimes \cong \parr$, so Soloviev's coherence theorem does not apply. Rowe's formula generalizes in an obvious way, and we prove directly that it still holds, assuming associativity. However, we are intrigued by the fact that the formula involves associativity at all. The rest of the theory of star-autonomous categories does not, with the exception of some simplifications noted in Sec. 5.3.2, such as the merging of the left and right nuclei. We show that associativity is redundant by deriving a formula for the inverse nuclearizer that does not rely on an associative structure. We believe the formula was previously unknown. We also derive a formula for internal composition when the third object involved is the dualizing object. This formula does not use associativity either, and we also believe it is new. The key insight to deriving the new formula for the inverse nuclearizer is that the role of the internal composition in Rowe's formula can be replaced by this other internal composition map.

Theorem 5.3.8 *Let X be an object. Then the following are equivalent:*

(i). X is left nuclear.

(ii). For every object Y, $\mathsf{leftnuc}_Y^X$ is an isomorphism.

(iii). For every object Y, every morphism $\phi : X \to Y$ is left nuclear.

In such a case, the inverse left nuclearizer is given by:

$$(\mathsf{leftnuc}_Y^X)^{-1} = (\mathsf{lefteval}_Y^X \parr X^\neg)((X \multimap Y) \otimes \widetilde{\mathsf{leftcoeval}}^X) : X \multimap Y \to Y \parr X^\neg \tag{5.44}$$

Proof It is trivial to see that (ii) implies (iii) and that (iii) implies (i). Interestingly, by Theorem Thm. 5.3.6, we already have seen that (i) implies (iii), though it still remains to show that (i) implies (ii) and to derive the formula. Assume X is left nuclear. We temporarily denote the expression on the right-hand-side of Eq. (5.44) by N_Y^X. To see that N_Y^X is the inverse of $\mathsf{leftnuc}_Y^X$, first observe that the following diagram commutes, and that the counterclockwise path left curries to $\mathsf{leftnuc}_Y^X N_Y^X$, whereas the clockwise path left curries to $\mathsf{id}_{X \multimap Y}$. This shows that N_Y^X is a right inverse of $\mathsf{leftnuc}_Y^X$:

$$\begin{tikzcd}
 & & (X \multimap Y) \otimes X \arrow[dll, "(X\multimap Y)\otimes\widetilde{\mathsf{leftcoeval}}^X\otimes X"'] \arrow[dd, "(X\multimap Y)\otimes X"] \\
(X \multimap Y) \otimes X \parr X^\neg \otimes X \arrow[d, "\mathsf{lefteval}_Y^X \parr X^\neg \otimes X"'] \arrow[drr, "(X\multimap Y)\otimes X \parr \mathsf{lefteval}_\perp^X"] & & \\
Y \parr X^\neg \otimes X \arrow[d, "Y \parr \mathsf{lefteval}_\perp^X"'] & & (X \multimap Y) \otimes X \arrow[dll, "\mathsf{lefteval}_Y^X"] \\
Y & &
\end{tikzcd} \tag{5.45}$$

Commutativity of the upper triangle in Eq. (5.45) follows from the left nuclearity of X, and the lower triangle commutes by elementary properties. Next, commutativity of Eq. (5.46) directly shows (without currying) that N_Y^X is a right inverse of $\mathsf{leftnuc}_Y^X$:

$$\begin{tikzcd}
 & & Y \parr X^\neg \arrow[dll, "\mathsf{leftnuc}_Y^X"'] \arrow[d, "Y\parr X^\neg\otimes\widetilde{\mathsf{leftcoeval}}^X"] \arrow[drr, "Y\parr X^\neg"] & & \\
X \multimap Y \arrow[drr, "(X\multimap Y)\otimes\widetilde{\mathsf{leftcoeval}}^X"'] & & Y \parr X^\neg \otimes X \parr X^\neg \arrow[rr, "Y\parr\mathsf{lefteval}_\perp^X\parr X^\neg"'] \arrow[d, "\mathsf{leftnuc}_Y^X\otimes X\parr X^\neg"] & & Y \parr X^\neg \\
 & & (X \multimap Y) \otimes X \parr X^\neg \arrow[urr, "\mathsf{lefteval}_Y^X\parr X^\neg"'] & &
\end{tikzcd} \tag{5.46}$$

The top right subdiagram of Eq. (5.46) commutes by left nuclearity of X, and the left subdiagram commutes by elementary means. The bottom right subdiagram is obtained from:

$$
\begin{tikzcd}
Y \parr X^\neg \otimes X \arrow[r, "Y \parr \mathsf{lefteval}_\perp^X"] \arrow[d, "\mathsf{leftnuc}_Y^X \otimes X"'] & Y \\
(X \multimap Y) \otimes X \arrow[ur, "\mathsf{lefteval}_Y^X"'] &
\end{tikzcd}
\tag{5.47}
$$

Diagram Eq. (5.47) commutes, since both paths left curry to the same morphism $\mathsf{leftnuc}_Y^X$, due to the currying identities $\lceil f(h \otimes X)\rceil = \lceil f \rceil h$ and $\lceil Y \parr t\rceil = \mathsf{leftnuc}_Y^X(Y \parr \lceil t \rceil)$. ■

Corollary 5.3.9 (Rowe's formula) *Let Y be an object. If $(\mathscr{C}, \otimes)$ is coherently associative, then the following are equivalent:*

(i). Y is left nuclear.

(ii). For every object X, $\mathsf{leftnuc}_Y^X$ is an isomorphism.

(iii). For every object X, every morphism $\phi : X \to Y$ is left nuclear.

In such a case, the inverse left nuclearizer is given by Rowe's formula:

$$
(\mathsf{leftnuc}_Y^X)^{-1} = (Y \parr \mathsf{leftcomp}_{X,Y,\perp})(\widetilde{\mathsf{leftcoeval}}^Y \otimes (X \multimap Y)) \tag{5.48}
$$

Proof Again we prove the only nontrivial implication, $(i) \implies (ii)$ and derive the formula. By Theorem Thm. 5.3.8, it suffices to show that the right-hand-side M_Y^X of Eq. (5.48) is a left inverse to $\mathsf{leftnuc}_Y^X$ without verifying that it is a right inverse. Observe that the following diagram commutes. The top triangle commutes by the coherent associativity pentagon, the middle part by elementary properties, and the bottom triangle by left nuclearity of Y.

$$
\begin{tikzcd}
(Y \parr Y^\neg \otimes (X \multimap Y)) \otimes X \arrow[d, "\mathsf{assoc}^\otimes_{\dots}"] & (X \multimap Y) \otimes X \arrow[l, "(\widetilde{\mathsf{leftcoeval}}^Y \otimes (X \multimap Y)) \otimes X"'] \arrow[dl, "\widetilde{\mathsf{leftcoeval}}^Y \otimes ((X \multimap Y) \otimes X)"] \arrow[dd, "\mathsf{lefteval}_Y^X"] \\
Y \parr Y^\neg \otimes ((X \multimap Y) \otimes X) \arrow[dd, "Y \parr Y^\neg \otimes \mathsf{lefteval}_Y^X"'] & \\
 & Y \arrow[d, "Y"] \arrow[dl, "\widetilde{\mathsf{leftcoeval}}^Y \otimes Y"'] \\
Y \parr Y^\neg \otimes Y \arrow[r, "Y \parr \mathsf{lefteval}_\perp^Y"'] & Y
\end{tikzcd}
$$

Now, by the formulas $\lceil f(h \otimes X) \rceil = \lceil f \rceil h$ and $\lceil Y \parr t \rceil = \mathsf{leftnuc}_Y^X(Y \parr \lceil t \rceil)$, the counterclockwise path left curries to $\mathsf{leftnuc}_Y^X M_Y^X$. The clockwise path left curries to $\mathsf{id}_{X \multimap Y}$. ■

In Section Sec. 5.2.2, we defined internal composition in an associative biclosed magmal category. It turns out that a different formula for internal composition is available in a strong magmal LDC if the final object is $\perp$, even without assuming associativity. Namely, define

$$\widetilde{\mathsf{leftcomp}}_{X,Y} : Y^\neg \otimes (X \multimap Y) \to X^\neg$$

to be the composition:

$$\begin{array}{c} Y^\neg \otimes (X \multimap Y) \\ \downarrow{\scriptstyle Y^\neg \otimes ((X \multimap Y) \otimes \widetilde{\mathsf{leftcoeval}}^X)} \\ Y^\neg \otimes ((X \multimap Y) \otimes X \parr X^\neg) \\ \downarrow{\scriptstyle Y^\neg \otimes (\mathsf{lefteval}_Y^X \parr X^\neg)} \\ Y^\neg \otimes Y \parr X \\ \downarrow{\scriptstyle \mathsf{lefteval}_\perp^Y \parr X} \\ X^\neg \end{array}$$

By Theorem Thm. 5.3.8, internal composition is equivalently given by:

$$\widetilde{\mathsf{leftcomp}}_{X,Y} = (\mathsf{lefteval}_\perp^Y \parr X^\neg)(Y^\neg \otimes (\mathsf{leftnuc}_Y^X)^{-1}) \tag{5.49}$$

We also believe this to be a new formula. The insight that let us replace Rowe's formula for the inverse nuclearizer by Eq. (5.44) was that the internal composition in Rowe's formula can be replaced by Eq. (5.49), which does not use associativity. This is because the last object in the composition is the dualizing object $\perp$.

5.3.5 Formula for dual morphisms

Linear bicategories are the evident oidification of linearly distributive categories, and so in a sense, when we study nuclear objects, we are just studying the single object case of an adjunction, after also imposing biclosedness. Nuclearity is a bit more involved than this, however, since we consider nuclear *morphisms*, not just objects. In this way nuclearity is like an "internal oidification" of the notion of *adjunction* itself in an LDC. We have seen that biclosedness entails that once the left or right zigzag of $X^\neg \dashv X$ is satisfied, both are satisfied. It turns out that nuclear morphisms satisfy the analogous property. This is a high level interpretation of Thm. 5.3.10, but the practical essence is the well-known formula, Eq. (5.50).

Theorem 5.3.10 *Consider objects W and Y and a morphism $g : W \to Y$. Then if W is left nuclear, then $g^\neg = g \multimap \bot : Y^\neg \to W^\neg$ is just as well given by:*

$$Y^\neg \xrightarrow{Y^\neg\otimes\widetilde{\mathsf{leftcoeval}}^W} Y^\neg \otimes W \parr W^\neg \xrightarrow{Y^\neg\otimes g\parr W^\neg} Y^\neg \otimes Y \parr W^\neg \xrightarrow{\mathsf{lefteval}^Y_\bot \parr W^\neg} W^\neg \tag{5.50}$$

Proof By Thm. 5.3.6 or Thm. 5.3.8, g has a left pseudoname $p : \top \to Y \parr W^\neg$. Now consider:

$$\begin{tikzcd}
 & Y^\neg \otimes W \parr W^\neg \arrow[r, "Y^\neg\otimes g\parr W^\neg"] \arrow[d, "Y^\neg\otimes\mathsf{leftnuc}^W_W"] \arrow[dr, phantom, "(2)"] & Y^\neg \otimes Y \parr W^\neg \arrow[d, "Y^\neg\otimes\mathsf{leftnuc}^W_Y"'] \arrow[dr, "\mathsf{lefteval}^Y_\bot\parr W^\neg"] & \\
Y^\neg \arrow[ur, "Y^\neg\otimes\widetilde{\mathsf{leftcoeval}}^W"] \arrow[dr, "Y^\neg\otimes\mathsf{leftcoeval}^W_\top"'] \arrow[r, phantom, "(1)"] \arrow[urr, bend left=60, "Y^\neg\otimes p"] \arrow[urr, phantom, bend left=30, "(5)"] \arrow[drr, bend right=60, "Y^\neg\otimes\lceil g\rceil"'] \arrow[drr, phantom, bend right=30, "(4)"] & & & W^\neg \arrow[l, phantom, "(3)"] \\
 & Y^\neg \otimes (W \multimap W) \arrow[r, "Y^\neg\otimes(W\multimap g)"'] & Y^\neg \otimes (W \multimap Y) \arrow[ur, "\widetilde{\mathsf{leftcomp}}_{W,Y}"'] &
\end{tikzcd}$$

(1) commutes by left nuclearity of W. (2) commutes by naturality of $\mathsf{leftnuc}$. (3) commutes by formula Eq. (5.49). (4) commutes by definition of $\lceil g \rceil$. Next, since g is left nuclear, the top and bottom paths $Y^\neg \to Y^\neg \otimes (W \multimap Y)$ are equal, so (5) commutes by the invertibility of the nuclearizer. So far we have established that:

$$(\mathsf{lefteval}^W_\perp \parr W^\neg)(Y^\neg \otimes g \parr W^\neg)(Y^\neg \otimes \widetilde{\mathsf{leftcoeval}}^W) = (\mathsf{lefteval}^Y_\perp \parr W^\neg)(Y^\neg \otimes p)$$

We now show that the right-hand-side reduces to $g^\neg$. Since g is left nuclear, the following diagram commutes:

$$\begin{tikzcd}
W \arrow[r, "p \otimes W"] \arrow[dr, "g"'] & Y \parr W^\neg \otimes W \arrow[d, "Y \parr \mathsf{lefteval}^W_\perp"] \arrow[dr, bend left, "\lceil \mathsf{lefteval}^Y_\perp \rceil \parr \mathsf{lefteval}^W_\perp"] & \\
& Y \arrow[r, "\lfloor \mathsf{lefteval}^W_\perp \rfloor"'] & {}^\neg(Y^\neg)
\end{tikzcd}$$

Now right-uncurry this to obtain commutative diagram:

$$\begin{tikzcd}
Y^\neg \otimes W \arrow[r, "Y^\neg \otimes p \otimes W"] \arrow[dr, "(Y^\neg \otimes g)\mathsf{lefteval}^Y_\perp"'] & Y^\neg \otimes Y \parr W^\neg \otimes W \arrow[d, "\mathsf{lefteval}^Y_\perp \parr \mathsf{lefteval}^W_\perp"] \\
& \perp
\end{tikzcd}$$

Finally, left curry this to get the desired right zigzag for the left nuclearity of g:

$$\begin{tikzcd}
Y^\neg \arrow[r, "Y^\neg \otimes p"] \arrow[dr, "g^\neg = \lceil \mathsf{lefteval}^Y_\perp (Y^\neg \otimes g) \rceil"'] & Y^\neg \otimes Y \parr W^\neg \arrow[d, "\mathsf{lefteval}^Y_\perp \parr W^\neg"] \\
& W^\neg
\end{tikzcd} \tag{5.51}$$

The equality $g^\neg = \lceil \mathsf{lefteval}^Y_\perp (Y^\neg \otimes g) \rceil$ may either be seen by the first currying formula (i.e. by Mac Lane's parameter theorem) or by the nuclear currying formula Eq. (5.41). ■

We get another formula along the way:

Corollary 5.3.11 *If $g : W \to Y$ is left nuclear then $g^\neg = (\mathsf{lefteval}^Y_\perp \parr W^\neg)(Y^\neg \otimes p)$.*

Proof This follows by commutativity of Eq. (5.51). ■

In fact, we define the *left conuclearizer* by currying Eq. (5.51):

$$\begin{tikzcd}
\top \arrow[r, "p"] \arrow[dr, "\lfloor g^{\neg} \rfloor"'] & Y \parr W^{\neg} \arrow[d, "\mathsf{leftconuc}_Y^W"] \\
& W^{\neg} \multimapinv Y^{\neg}
\end{tikzcd}$$

Conjecture 5.3.12 *If $(\mathscr{C}, \otimes, \parr)$ is unital and associative, and $g : W \to Y$ is a left nuclear morphism with left pseudoname $p : \top \to Y \parr W^{\neg}$, then the left nuclearizer and left conuclearizer are related as indicated by the following commutative diagam:*

$$\begin{tikzcd}
\top \arrow[r, "p"] \arrow[dr, "\lfloor g^{\neg} \rfloor"'] \arrow[ddrr, bend right, "\lceil g \rceil"'] & Y \parr W^{\neg} \arrow[d, "\mathsf{leftconuc}_Y^W"] \arrow[ddr, bend left, "\mathsf{leftnuc}_Y^W"] & \\
& W^{\neg} \multimapinv Y^{\neg} \arrow[dr, "\sim"'] & \\
& & W \multimap Y
\end{tikzcd}$$

Such a relationship between the nuclearizer and conuclearizer is expected since the types check out, and because the assumption of nuclearity seems to be enough to achieve coherence. Without an actual coherence theorem or explicit proof for now, however, we leave this as a conjecture.

Chapter 6

Internalization of multilinear forms

A bilinear form ω_V on an R-module V is *nondegenerate* if for all nonzero $u \in V$, the map $v \mapsto \omega_V(u, v)$ is nonzero. One calls ω_V *symmetric* if $\omega_V(u, v) = \omega_V(v, u)$ for all $u, v \in V$, *skew-symmetric* if $\omega_V(u, v) + \omega_V(v, u) = 0$ for all $u, v \in V$, and *alternating* if $\omega_V(v, v) = 0$ for all $v \in V$. Every alternating form is skew-symmetric, but the converse holds if and only if R has odd or zero characteristic. Furthermore, symmetry and skew-symmetry coincide in characteristic 2. These and other kinds of multilinear forms can be defined *internally*, that is, they may be defined on an object in a magmal category $\mathscr{V}$ with sufficient structure and properties imposed. We also consider the *oidifications* of such forms, i.e. families $\omega = (\omega_V)_{V \in \mathsf{ob}(\mathscr{V}')}$ of forms varying naturally across a full subcategory $\mathscr{V}'$.

Starting with a biclosed preabelian magmal category with distinguished element $\perp$, the existence of a multilinear form of a given kind may imply that the *domain of oidification* $\mathscr{V}'$ satisfies some additional property, or the form itself might induce additional structure on $\mathscr{V}'$. For example, we consider bilinear forms that partially evaluate to an isomorphism (rather than just a monomorphism), and call these *nuclear* bilinear forms. These coincide with nondegenerate bilinear forms on finitely generated free R-modules. The existence of a naturally varying nuclear bilinear form, it turns out, implies that $\mathscr{V}'$ is star-autonomous. It is possible to define alternating, symmetric, and skew-symmetric bilinear forms with surprisingly little imposition on $\mathscr{V}$.

One technicality to keep in mind is that although R-Mod is abelian, fgf-R-Mod is not preabelian unless R is a field since it lacks kernels and cokernels. This is not a problem since we can work with the larger category R-Mod but restrict our focus to the nucleus.

6.1 Internalization and oidification of bilinear forms

Let $\mathscr{V}$ be a magmal category, and let $\perp$ be an object in $\mathscr{V}$. A *bilinear form on an object* V is a morphism $\omega_V : V \otimes V \to \perp$. A morphism of the form $\phi : U \to V$ *respects* bilinear forms ω_U and ω_V if Eq. (6.1) commutes. More generally, a *(naturally varying) bilinear form on a full subcategory* $\mathscr{V}'$ is a natural transformation $\omega : F \Rightarrow G$, where $F = \otimes \Delta_{\mathscr{V}} : \mathscr{V}' \to \mathscr{V}$ is given by $F\phi = \phi \otimes \phi$ and $G : \mathscr{V}' \to \mathscr{V}$ is the constant functor $G\phi = \mathsf{id}_\perp$. In other words, ω is a family of morphisms ω_V indexed by each object V of $\mathscr{V}'$ such that all morphisms of the form $\phi : U \to V$ respect ω_U and ω_V:

$$\begin{tikzcd} U \otimes U \arrow[r, "\omega_U"] \arrow[d, "\phi\otimes\phi"'] & \perp \arrow[d, "\mathsf{id}_\perp"] \\ V \otimes V \arrow[r, "\omega_V"'] & \perp \end{tikzcd} \tag{6.1}$$

A bilinear form ω_V on an object V is the same as a bilinear form ω on the full subcategory on the single object V. It is only a technicality that $\mathscr{V}$ must be larger than $\mathscr{V}'$ in this case, since $\mathscr{V}$ has to also contain the objects $V \otimes V$ and $\perp$, in addition to V. Let us write $\mathsf{End}(\mathscr{V}, \omega)$ for the subcategory of $\mathscr{V}'$ consisting of the morphisms $\phi : U \to V$ that respect ω_U and ω_V. Likewise, we define $\mathsf{End}(V, \omega_V)$ to be the monoid of endomorphisms $\phi : V \to V$ that respect ω_V. In the case that $\mathscr{V}'$ contains a single object, $\mathsf{End}(\mathscr{V}, \omega)$ is the delooping category of $\mathsf{End}(V, \omega_V)$. This style of generalization, whereby $\mathsf{End}(V, \omega_V)$ is upgraded to $\mathsf{End}(\mathscr{V}, \omega)$ is called an *oidification*. Likewise, the *automorphism groupoid* $\mathsf{Aut}(\mathscr{V}, \omega)$ is defined as the *core* (subcategory of isomorphisms) of $\mathsf{End}(\mathscr{V}, \omega)$, and this is the oidification of the automorphism group $\mathsf{Aut}(V, \omega_V)$, i.e. the group of invertible elements of $\mathsf{End}(V, \omega_V)$.

Now suppose that $\mathscr{V}$ is biclosed. Then by the first currying identity, Eq. (6.1) is equivalent to:

$$\begin{tikzcd} U \arrow[r, "\ulcorner \omega_U \urcorner"] \arrow[d, "\phi"'] & U^* \\ V \arrow[r, "\ulcorner \omega_V \urcorner"'] & V^* \arrow[u, "\phi^*"'] \end{tikzcd} \tag{6.2}$$

Note that $\phi^* := \phi \multimap \perp$ is another morphism in $\mathscr{V}$ (or originally, $\mathscr{V}^{\mathrm{op}}$), not to be confused with the closely related pullback operation $\phi^\star$ on bilinear forms, which is given by $\phi^\star(\omega_V) = \omega_U$. By focusing on ϕ^* instead of $\phi^\star$, we can express the pullback of a bilinear form *internally* via Eq. (6.2), whereas even just defining $\phi^\star$ takes us out of $\mathscr{V}$.

A bilinear form ω is *left nondegenerate* if $\lceil \omega_V \rceil : V \to V^*$ is a strict monomorphism for all $V \in \mathsf{ob}(\mathscr{V}')$. *Right nondegeneracy* is defined analogously, and ω is called *nondegenerate* if it is both left and right nondegenerate. This generalizes the familiar notion of nondegeneracy from k-VECT, in which (strict) monomorphism is equivalent to injectivity of a linear map. The nucleus of k-VECT consists of the finite dimensional k-vector spaces. By basic linear algebra, in the nucleus of k-VECT, left nondegeneracy is equivalent to $\lceil \omega \rceil$ (or $\lfloor \omega \rfloor$) being an isomorphism. The following theorem shows how this generalizes. Let us call a bilinear form ω *nuclear* if $\lceil \omega \rceil$ and $\lfloor \omega \rfloor$ are isomorphisms. Technically, this clashes with the term *nuclear morphism* in Sec. 5.3, but the following theorem justifies this new usage.

Theorem 6.1.1 *Let $\mathscr{V}$ be a magmal category, fix $\perp \in \mathsf{ob}(\mathscr{V})$, and let $\mathscr{V}'$ be a full subcategory. Let ω be a naturally varying bilinear form on $\mathscr{V}'$. Further assume that $\lceil \omega \rceil$ is a natural isomorphism. Then left double negation translation is given by:*

$$\lfloor \mathsf{lefteval}^V_\perp \rfloor = {}^*\lceil \omega_V \rceil^{-1} \lfloor \omega_V \rfloor : V \to {}^*(V^*) \tag{6.3}$$

for all $V \in \mathsf{ob}(\mathscr{V}')$, and the following are equivalent (formulations of star-autonomy):

i. $\lfloor \omega \rfloor$ is a natural isomorphism.

ii. $\mathscr{V}'$ is left reflexive.

iii. $\mathscr{V}'$ is right reflexive.

Conditions i, ii, and iii imply:

iv. $\otimes$ has two-sided strong de Morgan dual $\boxtimes$ on $\mathscr{V}'$.

Conditions i, ii, and iii are implied by condition v, which presumes associativity:

v. $(\mathscr{V}', \otimes, \otimes^{\mathrm{rev}})$ is a nuclear LDC, i.e. $\mathscr{V}'$ lies in the nucleus of the LDC $(\mathscr{V}, \otimes, \otimes^{\mathrm{rev}})$.

Finally, if $\mathscr{V}'$ is closed under $\otimes$, then $\boxtimes \cong \otimes^{\mathrm{rev\,op}}$ on $\mathscr{V}'$ (in the physics convention).[1] *Then if $\mathscr{V}'$ is closed under $\otimes$ and $\otimes$ is associative, then i, ii, iii, iv, and v are equivalent.*

[1] In the math convention, the de Morgan dual involved in the theorem and proof is $\otimes^{\mathrm{op}}$ instead of $\otimes^{\mathrm{rev\,op}}$, but everything is otherwise unaffected. Symmetry/braidedness is not relevant or required in either case.

Proof By the first currying identity, we have:

$$^*\lceil\omega_V\rceil\lfloor\mathsf{lefteval}^V_\perp\rfloor = \lfloor\mathsf{lefteval}^V_\perp(\lceil\omega_V\rceil\otimes V)\rfloor = \lfloor\omega_V\rfloor$$

Assume $\lceil\omega\rceil$ is a natural isomoprhism. Then so is $^*\lceil\omega\rceil$, by which we obtain Eq. (6.3), which shows that $\mathscr{V}'$ is left reflexive if and only if $\lfloor\omega\rfloor$ is a natural isomorphism. Likewise, if we start by assuming $\lfloor\omega\rfloor$ is a natural isomorphism, we find that $\mathscr{V}'$ is right reflexive if and only if $\lceil\omega\rceil$ is a natural isomorphism. This establishes the equivalence of i, ii, and iii. Using left and right reflexivity, one constructs the respective de Morgan duals $\boxtimes_{\mathsf{L}}$ and $\boxtimes_{\mathsf{R}}$, and then by Prop. 5.2.3, $\boxtimes_{\mathsf{L}}\cong\boxtimes_{\mathsf{R}}$, thereby establishing iv as a consequence of i, ii, and iii.

On the other hand, assuming v holds, (which gives $\otimes$ an associative structure), ii follows by Prop. 5.2.7 and Cor. 5.3.5. Finally, suppose $\mathscr{V}'$ is closed under $\otimes$. Then we have an isomorphism

$$(U\otimes V)^* \xrightarrow{\lceil\omega_{U\otimes V}\rceil^{-1}} U\otimes V \xrightarrow{\lceil\omega_U\rceil\otimes\lceil\omega_V\rceil} U^*\otimes V^*$$

natural in U and V, and so $\otimes^{\mathrm{rev\,op}}$ is the left de Morgan dual of $\otimes$. Therefore, if $\mathscr{V}'$ is closed under $\otimes$ and $\otimes$ is associative, then iv implies v, and so all five conditions are equivalent.■

6.2 Algebraic and geometric considerations of alternating forms

We now compare how alternating forms arise in differential geometry and in linear algebra either as elements of $\wedge^k V^*$ or $(\wedge^k V)^*$, respectively. We first consider the case of free finitely generated modules over a ring R and later specialize to $R = \mathbb{R}$ and review the construction of the Poincaré symplectic form on the cotangent bundle.

Given an R-module V, one defines

$$\wedge^k V = V^{\otimes k} / I^k V$$

where

$$I^k V = \operatorname{span}\{x_1 \otimes \cdots \otimes x_k \,|\, x_1, \cdots, x_k \in V \text{ and } x_i = x_j \text{ for some } i \neq j\}.$$

A *k-multilinear form* on V is first defined as a function $\omega_V : V^{\times k} \to R$ satisfying *k-multilinearity*, i.e. linearity in each argument. One finds that a k-multilinear form is equivalently specified by (and henceforth identified with) a linear map $\omega_V : V^{\otimes k} \to R$, i.e. a linear functional on $V^{\otimes k}$, and so $(V^{\otimes k})^*$ is the module of k-multilinear forms. A k-multilinear form, thought of in the first sense, is *alternating* if it annihilates the submodule $I^k V$. If I is a subset of an R-module W, then the submodule $\mathsf{ann}_W(I) \subseteq W^*$ consisting of the linear functionals that annihilate I is canonically isomorphic to the dual of the quotient:

$$\mathsf{ann}_W(I) \cong (W/I)^*$$

Thus, the module of alternating bilinear forms on V is identified with $(\wedge^k V)^*$. This contrasts with the perspective taken in differential geometry, where a *k-form* is a section of the bundle $\wedge^k T^* M \to M$. Nevermind the fact that it is a vector bundle rather than vector space; the "point" is that over $p \in M$ with tangent space $V = T_p M$, the k-form at p is an element of $\wedge^k T_p^* M = \wedge^2 (V^*)$ rather than $(\wedge^k V)^*$. This different perspective is useful in differential geometry because it gives the exterior derivative operator d a cleaner definition, but ultimately, in order to *evaluate* such a k-form, it must be converted back into the "algebra style" alternating k-multilinear form residing in $(\wedge^k V)^*$. This may be done as follows: each $\alpha \in V^*$ extends to an *interior product*, that is, an anti-derivation $\iota_\alpha : \wedge^k V \to \wedge^{k-1} V$ of degree -1, characterized by the the inductive formula:

$$\iota_\alpha (x \wedge y) = \iota_\alpha x \wedge y + (-1)^{\deg x} x \wedge \iota_\alpha y$$

with base cases $\iota_\alpha v = \alpha(v)$ for $v \in V$ and $\iota_\alpha(r) = 0$ for $r \in R$. It follows by induction that $\iota_\alpha \iota_\beta + \iota_\beta \iota_\alpha = 0$. Then, by a separate inductive proof, one also finds that $(\iota_\alpha)^2 = 0$. Both facts hold in all characteristics, but the latter can only be immediately concluded from the former in odd or zero characteristic. Using both of these facts, we may define $\iota_{\alpha_1 \wedge \cdots \wedge \alpha_k} = \iota_{\alpha_1} \cdots \iota_{\alpha_k}$, and by linear extension for each $m \in \{k, k+1, \cdots, n = \dim V\}$, we obtain a canonical pairing:

$$\iota : \wedge^k V^* \otimes \wedge^m V \to \wedge^{m-k} V \qquad\qquad \omega \otimes x \mapsto \iota_\omega x \tag{6.4}$$

Two special cases are when $m = n$, in which case ι is the *Hodge star*, and when $m = k$, where ι is the *Gram determinant*, which left curries to an isomorphism $\wedge^k V^* \xrightarrow{\sim} (\wedge^k V)^*$:[2]

$$\alpha_1 \wedge \cdots \wedge \alpha_k \mapsto (v_1 \wedge \cdots \wedge v_k \mapsto \det\, \alpha_i v_j) \tag{6.5}$$

In this way, the interior derivative is used to evaluate a "geometry style" k-form $\omega \in \wedge^k V^*$ as if it were instead an element of $(\wedge^k V)^*$. Notice how this isomorphism $\wedge^k V^* \cong (\wedge^k V)^*$ does not simply come from the de Morgan self duality $V^{*\otimes k} \cong V^{\otimes k *}$.

Example We first recall that the cotangent bundle $M = T^*Q$ of a smooth manifold Q is canonically a symplectic manifold. Let $q \in Q$ and $p \in T_q^*Q$, so that $m = (q, p)$ is an arbitrary point of M, and let $\pi : M \to Q$ be the projection map. Then the *tautological 1-form* $\theta \in \Omega^1 M$ is defined pointwise by:

$$\theta_m : T_m M \xrightarrow{d\pi_m} T_q Q \xrightarrow{\;p\;} \mathbb{R}$$

The *Poincaré symplectic form* is $\omega := -d\theta \in \Omega^2 M$. By construction, ω is a 2-form. To see that it is symplectic, we just need to verify nondegeneracy, which is a pointwise condition. Let $w = (u, v) \in T_m M$ and let $\gamma : \mathbb{R} \to M$ be a smooth curve with $\gamma(0) = m$ and $\gamma'(0) = w$. Writing $\gamma(t) = (q(t), p(t))$, we have that $q(0) = q$ and $q'(0) = u$. It follows that:

$$d\pi_m(w) = (\pi\gamma)'(0) = q'(0) = u$$

This gives the following coordinate-free expression for $\theta_m(w)$:

$$\theta_m(w) = p(d\pi_m(w)) = p(u)$$

[2] By currying some fixed nondegenerate bilinear form $\langle -, - \rangle$ on V, the entries $\alpha_i v_j$ of the Gram matrix may be viewed as inner products $\langle u_i, v_j \rangle$, related by $\alpha_i = \lceil \langle -, - \rangle \rceil u_i$. To see that Eq. (6.5) is an isomorphism, take $u_i = v_i$. By the Gram matrix theorem, for independent $\alpha_1, \cdots, \alpha_k$, $\det\langle v_i, v_j \rangle \neq 0$, so $\iota_{\alpha_1 \wedge \cdots \wedge \alpha_k} \neq 0$.

In a coordinate neighborhood around $q \in Q$ with coordinate functions $q^1, \cdots, q^n$ and cooresponding basis $dq^1_q, \cdots, dq^n_q$ of covectors in $T^*_q Q$, we may expand:

$$p = \sum_{i=1}^{n} p_i(q) dq^i_q \in T^*_q Q$$

Since $dq^i(v) = 0$, the pointwise evaluation of the tautological 1-form is given by the same expression (noting that $T^*_q Q$ is a subspace of $T^*_m M$):

$$\theta_m = \sum_{i=1}^{n} p_i(q) dq^i_q \in T^*_m M$$

Locally, we therefore have:

$$\theta = \sum_{i=1}^{n} p_i dq^i \qquad \text{and} \qquad \omega = \sum_{i=1}^{n} dq^i \wedge dp_i$$

Now consider $Q = \mathbb{R}^n$ so that $M = T^*Q \cong \mathbb{R}^{2n}$. Then we use the Gram determinant to evaluate the symplectic form:

$$\omega_m(w_1, w_2) = \det \begin{pmatrix} dq_m(w_1) & dq_m(w_2) \\ dp_m(w_1) & dp_m(w_2) \end{pmatrix} = v_2 \cdot u_1 - v_1 \cdot u_2$$

where $w_1 = (u_1, v_1)$ and $w_2 = (u_2, v_2)$. This is the standard symplectic form on $\mathbb{R}^{2n}$, but the construction made us first consider ω_m as an element of $\wedge^2((\mathbb{R}^n)^*)$, so in order to evaluate it, we had to do a calculation invovling a Gram matrix, which effectively converted it into an element of $(\wedge^2 \mathbb{R}^n)^*$.

In contrast, from the "linear algebra" point of view, the symplectic form starts as an element of $(\wedge^2 V)^*$ rather than $\wedge^2 V^*$. Indeed, for any finitely generated free R-module Q, there is a canonical symplectic form $\omega_V : V \otimes V \to R$ on $V = Q \oplus Q^*$ given by:

$$\omega_V((u_1, v_1), (u_2, v_2)) = v_2 u_1 - v_1 u_2 \tag{6.6}$$

A symmetric nondegenerate bilinear form $\cdot$ furnishes an isomoprhism $Q \cong Q^*$ for which the right-hand-side of Eq. (6.6) again becomes $v_2 \cdot u_1 - v_1 \cdot u_2$. Whereas in the differential geometry approach, the symplectic form arose as the derivative of the tautological 1-form θ, in the linear algebra approach, we view the symplectic form as arising from the group 1-cocycle c given by $c((q,p),(u,v)) = p(u)$. Namely, $\omega(w_1, w_2) = c(w_2, w_1) - c(w_1, w_2)$.

Our goal is to generalize the theory of symplectic forms on finite dimensional real vector spaces and locally compact abelian groups. For now, we are not concerned with geometrical aspects such as the differential d. As such, we consider alternating forms in the "linear algebra sense", i.e. as elements of $(\wedge^2 V)^*$. This is our starting point for internalization.

6.3 Internalization of alternating bilinear forms

Consider a unital magmal preabelian category $(\mathscr{V}, \otimes, \top)$. We will mimic the definition of $\wedge^2 V$ in R-Mod by defining $\wedge^2 V$ as a quotient of $I^2 V$, which we characterize by specifying enough of its generalized elements. We build up to the definition in stages for sake of motivation.

Let $V \in \mathsf{ob}(\mathscr{V})$. Recall that the notation $x \in_U V$ stands for a *generalized element of* V *at stage of definition* U, which is synonymous with a morphism $x : U \to V$. As a first attempt, suppose we define $i : I^2V \to V^{\otimes 2}$ (an object I^2V together with a morphism to $V^{\otimes 2}$) to be optimal ("smallest") with the property that for all $x \in_U V$, there exists unique $u_x \in_{U^{\otimes 2}} I^2V$ such that $iu_x = x^{\otimes 2}$. Optimality means that for any other such $j : I \to V^{\otimes 2}$ there exists a unique $\varphi : I^2V \to I$ such that for all $x \in_U V$, the following diagram commutes:

$$\begin{tikzcd} & & I \arrow[dl, bend left, "j"] \\ U^{\otimes 2} \arrow[r, dotted, "u_x"] \arrow[dr, "x^{\otimes 2}"'] \arrow[urr, dotted, bend left] & I^2V \arrow[d, "i"] \arrow[ur, dashed, "\varphi"'] & \\ & V^{\otimes 2} & \end{tikzcd} \tag{6.7}$$

This mocks the definition of $\mathrm{span}\{x^{\otimes 2} \mid x \in V\}$ from the $\mathscr{V} = R$-Mod case. We might expect naturality to be required in U in this definition in order to uncover the full theory. However we immediately see that imposing the defining condition on all generalized elements $x \in_U V$ is too strong, and so the question of naturality is a moot point. For example, consider the case $U := V$ and $x = \mathsf{id}_V$. Then it follows that $i : I^2V \to V^{\otimes 2}$ is an epimorphism, which is generally false in R-Mod. The solution is to restrict the requirement from generalized elements to global elements, (or even monic global elements). In this context, a *global element* is a generalized element at stage of definition $\top$. The reasoning is that the monoidal unit in our (concrete) categories of interest (eg. R-Mod, where $\top \cong R$) has a distinguished element (eg. $1 \in R$) in the usual sense of the word *element*; this distinguished element can be used to make the notion of *global element* correspond with the usual notion of *element*.

monoidal category	monoidal unit	strict monic gen. elt. x	global elt. x
$(R\text{-Mod}, \otimes)$	R	submodule $x(U)$	element (vector) $x(1)$
$(\mathrm{LCA}, \otimes)$	$\mathbb{Z}$	subgroup $x(U)$	element $x(1)$
$(\mathrm{Set}, \times)$	singleton $\{\cdot\}$	subset $x(U)$	element $x(\cdot)$

For our second attempt at defining I^2V, we revise Eq. (6.7) by using $\top$ as the only stage of definition. This also eliminates the question of naturality in the stage of definition.

$$\begin{tikzcd}
 & & I \arrow[ddl, bend left] \\
\top \cong \top \otimes \top \arrow[r, dotted, "u_x"] \arrow[urr, dotted, bend left] \arrow[dr, "x^{\otimes 2}"'] & I^2V \arrow[ur, dashed] \arrow[d, "i"] & \\
 & V^{\otimes 2} &
\end{tikzcd} \tag{6.8}$$

We will later prove that all *lines* (monomorphisms $\top \to V$) in an object V with symplectic form are isotropic, a fact that plays a key role in the theory of symplectic forms. Intuitively, the stage of definition $\top$ used in the definition of I^2V not only makes it so that lines are isotropic but also *generates* the rest of the isotropic subobjects. If we allowed too much flexibility in the stage of definition, too many subobjects would be deemed isotropic, and the theory would trivialize. Using the unit $\top$ of the unital magmal structure as the preferred stage of definition, as opposed to some other fixed object T, does not seem to make much of a difference in the theory, but we are motivated to use $\top$ due to our examples.

There is yet another problem. It does not appear automatic from our definition that $i : I^2V \to V^{\otimes 2}$ is monic. This is something we will need, because i will be the kernel of the quotient map $\pi : V^{\otimes 2} \to \wedge^2 V$. In fact, it would be ok to require *all* the arrows in Eq. (6.8) to be monic, since they represent either inclusions or global elements, and our categories of interest are determined by their *monic* global elements.

Two ways we can ensure that $i : I^2V \to V^{\otimes 2}$ is monic are as follows. We can either add to the definition the requirement that i be monic, otherwise leaving it undefined, or simply change the context of the definition from taking place in $\mathscr{V}$ to taking place in $\mathsf{monos}(\mathscr{V})$. In the former approach, we would not require the global elements involved in Eq. (6.8) to be monic, otherwise it would coincide with the latter. We shall ultimately take the latter approach, but for now, we put off substituting $\mathsf{monos}(\mathscr{V})$ in place of $\mathscr{V}$ for sake of generality.

Before replacing $\mathscr{V}$ by $\mathsf{monos}(\mathscr{V})$, one must carefully distinguish between generalized elements $x \in_U Q$, which are not necessarily monic, and subobjects $x : [Q]_V$, which are. Although this distinction dissolves after making the substitution, it is still helpful to keep both notations and accompanying terminologies, because subobjects and generalized elements do end up playing different roles.

Another complication with Diagram Eq. (6.8) as a definition for $i : I^2V \to V^{\otimes 2}$ is that it doesn't immediately appear to be a limit or colimit. However, it is in fact a colimit, just not in $\mathscr{V}$, but in $\mathscr{V} \downarrow V^{\otimes 2}$, or ultimately in $\mathsf{monos}(\mathscr{V}) \downarrow V^{\otimes 2} = \mathrm{S{\scriptsize UB}}_{\mathscr{V}}(V^{\otimes 2})$. As one may check, the logical quantifications imposed on Eq. (6.8) in our previous iteration of the definition can be packaged up into the following coproduct diagram Eq. (6.9) in $\mathscr{V} \downarrow V^{\otimes 2}$. Thus, we take $i : I^2V \to V^{\otimes 2}$ to be the coproduct of slices $x^{\otimes 2} : \top \to V^{\otimes 2}$ ranging over all $x \in_\top V$.

$$\begin{tikzcd} \left[\top \overset{x^{\otimes 2}}{\to} V^{\otimes 2}\right]_{x \in_\top V} \arrow[d, Rightarrow] \arrow[dr, Rightarrow] & \\ {[I^2V \to V^{\otimes 2}]} \arrow[r, dashed, "\exists!"'] & {[I' \to V^{\otimes 2}]} \end{tikzcd} \tag{6.9}$$

Lastly, it turns out that we will need i to be a **strict monomorphism**.[3] For this, we simply modify the definition so as to leave $i : I^2V \to \wedge^2 V$ undefined if the recipe results in a morphism that is not strict (or not a monomorphism). Let us finally now replace $\mathscr{V}$ by $\mathsf{monos}(\mathscr{V})$, so that the *monomorphism* part of this issue goes away. Note that strictness is still required in order to continue. Finally we rewrite Eq. (6.9) in a more readable notation. In accordance with standard conventions, we also strengthen the requirement of the existence of the coproduct from a property of objects to a property of the category itself.

Definition Let $(\mathscr{V}, \otimes, \top)$ be a unital magmal preabelian category and let $V \in \mathsf{ob}(\mathscr{V})$. Assume that $\mathscr{V} \downarrow V^{\otimes 2}$ has enough coproducts. Then define $i : I^2V \rightarrowtail V^{\otimes 2}$ by:

$$i : [I^2V]_{V^{\otimes 2}} \cong \sum_{x \in_\top V} x^{\otimes 2} \qquad \text{in} \qquad \mathrm{S{\scriptsize UB}}_{\mathscr{V}}(V^{\otimes 2}) \cong \mathsf{monos}(\mathscr{V}) \downarrow V^{\otimes 2} \tag{6.10}$$

By *enough coproducts* we mean that $\mathrm{S{\scriptsize UB}}_{\mathscr{V}}(V^{\otimes 2})$ is required to contain coproducts indexed by $\mathsf{hom}_{\mathsf{monos}(\mathscr{V})}(\top, V)$ for each $V \in \mathsf{ob}(\mathscr{V})$. As noted in Sec. 5.1.1, a convenient criterion for this is if $\mathscr{V}$ has enough limits and colimits, so that the union may arise as the pushout of a pullback, generalizing Eq. (5.1). Finally we define the *alternating square*:

$$\wedge^2 V \cong V^{\otimes 2} / I^2 V$$

[3]See the appendix (Section Appx. G) for the definition and properties of strictness.

More explicitly, we form the cokernel $\pi : V^{\otimes 2} \to \wedge^2 V$ of $i : I^2V \to V^{\otimes 2}$:

$$\begin{tikzcd}
\top \arrow[r, "u_x"] \arrow[dr, "x^{\otimes 2}"'] & I^2V \arrow[r] \arrow[d, "i"] & 0 \arrow[d] \\
& V^{\otimes 2} \arrow[r, "\pi"'] & \wedge^2 V
\end{tikzcd} \tag{6.11}$$

Notice that we do not require all objects V to have alternating square, since if $\sum_{x\in_\top V} x^{\otimes 2}$ is not strict, I^2V is undefined. Since the coproduct $\sum$ in $\textsc{Sub}_{\mathscr{V}}(V^{\otimes 2})$ is the "union", one may recognize that Eq. (6.10) looks like the definition $\mathrm{span}\{x^{\otimes 2} \,|\, x \in V\}$ of I^2V in R-$\textsc{Mod}$.

The definition of cokernel says that the square part of Diagram Eq. (6.11) is a pushout. Since i is strict by hypothesis, it follows that the square is also a pullback and π is a strict epimorphism. In other words, we have a strict short exact sequence:

$$0 \longrightarrow I^2V \xrightarrow{\ i\ } V^{\otimes 2} \xrightarrow{\ \pi\ } \wedge^2 V \longrightarrow 0 \tag{6.12}$$

Now assume further that $\mathscr{V}$ is star-autonomous. Then Eq. (6.12) may be dualized to obtain another strict short exact sequence:

$$0 \longleftarrow (I^2V)^* \xleftarrow{\ i^*\ } V^{\otimes 2*} \xleftarrow{\ \pi^*\ } (\wedge^2 V)^* \longleftarrow 0$$

Finally, an *alternating bilinear form* on V is a bilinear form $\omega_V : V \otimes V \to \perp$ of the form $\omega_V = \pi\omega'_V$ where $\omega'_V : \wedge^2 V \to \perp$ is obtained by left-uncurrying some $\tilde{\omega}_V \in_\top (\wedge^2 V)^*$. Each of ω_V, ω'_V, and $\tilde{\omega}_V$ arise in calculations.

Finally, we note that if the unital magmal structure on $\mathscr{V}$ is upgraded to a monoidal structure (by adding coherent associativity), then the construction here readily generalizes so that one may define I^kV and $\wedge^k V$. Ultimately, we only need $\wedge^k V$ since we are interested in symplectic forms, which are bilinear. Concrete definitions for I^kV and $\wedge^k V$ are given in Sec. 6.5.

6.4 Evaluation of bilinear forms

Let $\mathscr{V}$ be a star-autonomous preabelian category, and let $\omega : V^{\otimes 2} \to \bot$ be a bilinear form. Total evaluation of a bilinear form is straightforward when ignoring possible conditions imposed on ω, such as alternation. Following Sec. 5.2.1, each $w \in_U V^{\otimes 2}$ yields:

$$\mathsf{lefteval}_{\bot}^{V^{\otimes 2}}(\lceil\omega\rceil \otimes w) : \top \otimes U \to \bot$$

On many occasions, we will need to *partially evaluate* a bilinear form at a generalized element of a subobject. The setup is as follows: given a subobject $x : [Q]_V$ and a generalized element $q \in_U Q$, it follows that $xq \in_U V$. (Note that x and xq might not be monic.) For *left partial evaluation*, we define $\lceil q^\flat \rceil : U \to V^*$ by the following commutative diagram, and then left uncurry to obtain $q^\flat : U \otimes V \to \bot$ and right curry to obtain $\lfloor q^\flat \rfloor : V \to {}^*U$.

$$\begin{tikzcd} U \arrow[r, "\lceil q^\flat \rceil"] \arrow[d, "q"'] & V^* \\ Q \arrow[r, "x"'] & V \arrow[u, "\lceil\omega\rceil"'] \end{tikzcd} \tag{6.13}$$

In our categories of interest, the following *partial evaluation formula* says "$q^\flat = \omega(q, -)$".

Proposition 6.4.1 *Let $x : [Q]$, $y : [P]$, and $q \in_U Q$. Then $\lfloor q^\flat \rfloor y = \lfloor \omega(xq \otimes y) \rfloor : P \to {}^*U$.*

Combining this with the first currying identity, we obtain the identity:

$$\lfloor q^\flat \rfloor y = {}^*(xq)\lfloor\omega\rfloor y \tag{6.14}$$

Proof

$$\begin{aligned}
\lfloor \omega(xq \otimes y) \rfloor &= \lfloor \mathsf{lefteval}_{\bot}^{V}(\lceil\omega\rceil \otimes \mathsf{id}_V)(xq \otimes y) \rfloor && \text{left adjunct formula for } -\otimes V \dashv V \multimap - \\
&= \lfloor \mathsf{lefteval}_{\bot}^{V}(\lceil\omega\rceil xq \otimes y) \rfloor && \text{functorality of } \otimes \\
&= \lfloor \mathsf{lefteval}_{\bot}^{V}(\lceil q^\flat \rceil \otimes y) \rfloor && \text{definition of } q^\flat \\
&= \lfloor \mathsf{lefteval}_{\bot}^{V}(\lceil q^\flat \rceil \otimes \mathsf{id}_V)(\mathsf{id}_U \otimes y) \rfloor && \text{functorality of } \otimes \\
&= \lfloor q^\flat(\mathsf{id}_U \otimes y) \rfloor && \text{left adjunct formula for } -\otimes V \dashv V \multimap - \\
&= \lfloor \mathsf{righteval}_{\bot}^{U}(\mathsf{id}_U \otimes \lfloor q^\flat \rfloor)(\mathsf{id}_U \otimes y) \rfloor && \text{left adjunct formula for } U \otimes - \dashv - \multimapinv U \\
&= \lfloor \mathsf{righteval}_{\bot}^{U}(\mathsf{id}_U \otimes \lfloor q^\flat \rfloor y) \rfloor && \text{functorality of } \otimes \\
&= \lfloor q^\flat \rfloor y && \text{left adjunct formula for } U \otimes - \dashv - \multimapinv U
\end{aligned}$$

■

In some situations, more specialized formulas are needed to evaluate bilinear forms with additional properties such as alternation. Thus, let us now specialize to alternating bilinear forms. For this, we must assume that the object V has an alternating square, and consider an alternating form, with notation as in Sec. 6.3:

$$\omega : V^{\otimes 2} \to \bot \qquad\qquad \omega' : \wedge^2 V \to \bot \qquad\qquad \tilde{\omega} : \top \to (\wedge^2 V)^*$$

Since the alternating square $\wedge^2 V$ is defined as a cokernel, we end up needing to consider the transported exact sequence as seen in the left diagram below. The "geometry style" alternating forms (as in Sec. 6.2), i.e. global elements of $\wedge^2 V^*$ as opposed to $(\wedge^2 V)^*$, involve the de Morgan duality (contraction) map, and most naturally act not on the cokernel (quotient) $\wedge^2 V$ but on the kernel (subobject) $\mathsf{Alt}^2 V$, defined as follows:

$$\begin{tikzcd} I^2V \arrow[r] \arrow[d] & I^2V \cong {}^*((I^2V)^*) \arrow[d] \\ V^{\otimes 2} \arrow[r, "\mathsf{id}_{V^{\otimes 2}}"] \arrow[d, "\pi"'] & V^{\otimes 2} \cong {}^*(V^{\otimes 2 *}) \arrow[d] \\ \wedge^2 V \arrow[r] & \wedge^2 V \cong {}^*((\wedge^2 V)^*) \end{tikzcd} \qquad \begin{tikzcd} I^2V^* \arrow[r] \arrow[d] & (J^2V)^* \arrow[d] \\ V^{*\otimes 2} \arrow[r, "\text{de Morgan}"] \arrow[d] & V^{\parr 2 *} \arrow[d] \\ \wedge^2 V^* \arrow[r] & (\mathsf{Alt}^2 V)^* \end{tikzcd} \qquad \begin{tikzcd} J^2V \\ V^{\parr 2} \arrow[u] \\ \mathsf{Alt}^2 V \arrow[u] \end{tikzcd} \tag{6.15}$$

In the middle diagram, we use right reflexivity to define $(J^2V)^*$ and $(\mathsf{Alt}^2V)^*$ as the transported kernel and cokernel, which by duality, yields the short exact sequence on the right. In the diagram on the left we apply left reflexivity to the objects on the left so that we may right uncurry the bottom line:

$$\mathsf{lefteval}_{\bot}^{\wedge^2 V} : (\wedge^2 V)^* \otimes \wedge^2 V \to \bot \tag{6.16}$$

Composing with $(\wedge^2 V)^* \otimes \pi$ yields a pairing $(\wedge^2 V)^* \otimes V^{\otimes 2} \to \bot$ whereby an alternating bilinear form acts on $V^{\otimes 2}$ rather than on $\wedge^2 V$. This is the "algebra style" evaluation described in Sec. 6.2. The bottom arrow of the diagram on the right of Eq. (6.15) left uncurries to:

$$\mathsf{dMlefteval}^{V,2} : \wedge^2 V^* \otimes \mathsf{Alt}^2 V \to \bot \tag{6.17}$$

In order to get to the geometry style evaluation on $\wedge^2 V$, we either need an isomorphism between $(\wedge^2 V)^*$ and $\wedge^2 V^*$ to use with Eq. (6.16) or an isomorphism between $\mathsf{Alt}^2 V$ and

$\wedge^2 V$ to use with Eq. (6.17). We have already described the former in the case of R-Mod in Sec. 6.2, which uses the interior derivative. We give an (equivalent) calculation for the latter case in Sec. 6.5.

Shifting our attention back to the algebra style forms, we also have the following *total evaluation formula* for evaluating an alternating form on generalized elements of subobjects.

Proposition 6.4.2 *Let $\omega : V^{\otimes 2} \to \perp$ be an alternating form, let $x : [Q]_V$ and $y : [P]_V$, and let $q \in_U Q$ and $p \in_W P$. Then*

$$\omega(xq \otimes yp) = \mathsf{lefteval}_{\perp}^{\wedge^2 V}(\tilde{\omega} \otimes (xq \wedge yp)) : U \otimes W \to \perp$$

where $\omega = \pi\omega'$ and $\pi : V^{\otimes 2} \to \wedge^2 V$ is the alternating square, and $xq \wedge yp := \pi(xq \otimes yp)$.

Proof By the left adjunct formula for $- \otimes \wedge^2 V \dashv \wedge^2 V \multimap -$, we have:

$$\begin{aligned}
\omega(xq \otimes yp) &= \omega'(xq \wedge yp) \\
&= \omega'(\top \otimes (xq \wedge yp)) \\
&= \mathsf{lefteval}_{\perp}^{\wedge^2 V}(\tilde{\omega} \otimes \wedge^2 V)(\top \otimes (xq \wedge yp)) \\
&= \mathsf{lefteval}_{\perp}^{\wedge^2 V}(\tilde{\omega} \otimes (xq \wedge yp))
\end{aligned}$$

as claimed. ■

6.5 Sixteen flavors of multilinear tensors

Although we are more concerned with the evaluation of "algebra style" multilinear forms, transporting the defining exact sequence of the alternating powers $\wedge^k V$ across the de Morgan duality map yields interesting results, which we note here.

Let R be a ring with the invariant basis number (IBN) property. We consider the nuclear autonomous category FGF-R-MOD.[4] Recall that every alternating k-multilinear form on a finitely generated free R-module V is skew-symmetric, but the converse holds if and only if $d = \mathsf{char}\, V$ is odd or zero. We would like to investigate the modules of alternating and skew-symmetric forms, which we denote by $(\wedge^k V)^*$ and $(\tilde{\wedge}^k V)^*$, respectively. These "algebra style" forms have closely related "geometry style" forms, which comprise $\wedge^k V^*$ resp. $\tilde{\wedge}^k V^*$. By transporting the defining exact sequences of the latter across the de Morgan duality map, (which is full tensor contraction in FGF-R-MOD,) we find that a total of eight interesting objects are involved, seen on the corners of the following diagrams:

$$\begin{tikzcd}
\tilde{I}^k V^* \arrow[r] \arrow[d] & (\tilde{J}^k V)^* \arrow[d] \\
V^{*\otimes k} \arrow[r, "\text{de Morgan}"] \arrow[d] & V^{\parr k *} \arrow[d] \\
\tilde{\wedge}^k V^* \arrow[r] & (\widetilde{\mathsf{Alt}}^k V)^*
\end{tikzcd}
\qquad
\begin{tikzcd}
I^k V^* \arrow[r] \arrow[d] & (J^k V)^* \arrow[d] \\
V^{*\otimes k} \arrow[r, "\text{de Morgan}"] \arrow[d] & V^{\parr k *} \arrow[d] \\
\wedge^k V^* \arrow[r] & (\mathsf{Alt}^k V)^*
\end{tikzcd}
\tag{6.18}$$

These eight objects are defined by the property that each diagram is an isomorphism of (strict) short exact sequences, and in terms of $\tilde{I}^k V^*$ or $I^k V^*$, which in turn are given by:

$$\tilde{I}^k V = \mathsf{span}\{t + t\sigma \mid t \in V^{\otimes k} \text{ and } \sigma \in S_k \setminus A_k\} \quad \text{w.r.t. the right action } V^{\otimes k} \circlearrowleft S_k$$
$$I^k V = \mathsf{span}\{x_1 \otimes \cdots \otimes x_k \mid x_i \in V \text{ and } x_i = x_j \text{ for some } i \neq j\}$$

where $S_k \setminus A_k$ is the set of odd permutations. Notice that $\tilde{I}^k V \subseteq I^k V$, and for example, $2x^{\otimes k} \in \tilde{I}^k V$, whereas $x^{\otimes k} \in I^k V$ but $x^{\otimes k} \in \tilde{I}^k V$ if and only if d is odd or zero. Then:

$$(\wedge^k V)^* = \{\text{alternating forms}\} \subseteq \{\text{skew symmetric forms}\} = (\tilde{\wedge}^k V)^*$$

[4] Recall that an autonomous category is a star-autonomous category in which $\otimes \cong \parr$. We nevertheless keep track of $\otimes$ vs. $\parr$ since some of what we show here generalizes to other star-autonomous categories.

It is common to encounter $\mathsf{Alt}^k W$ identified with $\wedge^k V$ in the literature, and so on, which halves the number of objects in consideration. This is not done using any of the isomorphisms in Eq. (6.18), but by more concrete means. For example, consider the map:

$$\mathsf{Alt}_0 : V^{\otimes k} \to V^{\parr k} \qquad\qquad x_1 \otimes \cdots \otimes x_k \mapsto \sum_{\sigma \in S_k} \mathsf{sgn}(\sigma) x_{\sigma 1} \parr \cdots \parr x_{\sigma k} \tag{6.19}$$

This version of the Alt_0 map, which does not involve a factor of $\frac{1}{k!}$, descends to an isomorphism, regardless of k and d, whose image is $\mathsf{Alt}^k V$, (as we calculate below):

$$\mathsf{Alt} : \wedge^k V \xrightarrow{\sim} \mathsf{Alt}^k V \tag{6.20}$$

The important point here is that $\wedge^k V$ is a quotient (of $V^{\otimes k}$) whereas $\mathsf{Alt}^k V$ is a submodule (of $V^{\parr k}$). We keep the fairly general notation even though this situation is very concrete:

$$\begin{aligned}
\mathsf{Alt}^k V &\overset{\text{def}}{=} {}^*(V^{\parr k *}/(J^k V)^*) \qquad\qquad (6.21)\\
&\cong \{ w \in {}^*(V^{\parr k *}) \,|\, w(\omega) = 0 \text{ for all } \omega \in (J^k V)^* \}\\
&\cong \{ w \in V^{\parr k} \,|\, \omega(w) = 0 \text{ for all } \omega \in (J^k V)^* \}\\
&= \left\{ \sum c_i x_{i1} \parr \cdots \parr x_{ik} \,\middle|\, \begin{matrix} \sum c_i \alpha_1(x_{i1}) \cdots \alpha_k(x_{ik}) = 0 \text{ for all } \alpha_j \in V^* \\ \text{with } \alpha_{j_1} = \alpha_{j_2} \text{ for some } j_1 \neq j_2, \text{ and } x_{ij} \in V \end{matrix} \right\}
\end{aligned}$$

From this calculation we find that:

$$\mathsf{Alt}^k V \supseteq \mathsf{span} \left\{ \sum_{\sigma \in S_k} \mathsf{sgn}(\sigma) x_{\sigma_1} \parr \cdots \parr x_{\sigma_k} \,\middle|\, x_1, \cdots, x_k \in V \right\} \tag{6.22}$$

Since the modules are free and finitely generated, by the dual basis construction and Eq. (6.18), it follows that $\mathsf{Alt}^k V \cong (\mathsf{Alt}^k V)^* \cong \wedge^k V^* \cong \wedge^k V$, and so $\mathsf{rk}(\mathsf{Alt}^k V) = \mathsf{rk}(\wedge^k V) = \binom{n}{k}$, where $n = \mathsf{rk}(V)$. On the other hand, the right-hand-side of Eq. (6.22) has a basis of size $\binom{n}{k}$. Therefore, since R satisfies the IBN property, Eq. (6.22) is an equality, and Eq. (6.20) is established. For example, if $d = k = 2$, then the alternating case is as follows:

$$\mathsf{Alt}^2 \mathbb{F}_2^2 = \{0, |01\rangle + |10\rangle\} \qquad \text{and} \qquad (\wedge^2 \mathbb{F}_2^2)^* = \{0, \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\}$$

The skew-symmetric case, on the other hand, looks like this:

$$\widetilde{\mathsf{Alt}}^2 \mathbb{F}_2^2 = \mathsf{span}\{|00\rangle, |11\rangle, |01\rangle + |10\rangle\} \qquad \text{and} \qquad (\tilde{\wedge}^2 \mathbb{F}_2^2)^* = \mathsf{span}\{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\}$$

Eq. (6.20) induces an isomorphism $\wedge^k V^* \cong (\wedge^k V)^*$ via Eq. (6.18), which may be used to evaluate geometry style k-forms, and one easily shows that this is again the Gram determinant Eq. (6.5):

$$\begin{aligned} \wedge^k V^* &\to (\wedge^k V)^* \\ \alpha_1 \wedge \cdots \wedge \alpha_k &\mapsto x_1 \wedge \cdots \wedge x_k \mapsto \mathsf{det}(\alpha_i x_j)_{ij} \end{aligned}$$

Calculation Eq. (6.21) and the calculation in Sec. 6.2, which both tell us how to evaluate geometry style forms, are concrete elementwise arguments, and we do not bother trying to formulate them category theoretically. In fact, we actually find it very helpful to distinguish between $\wedge^k V$ and $\mathsf{Alt}^k V$, due to their different roles as a quotient or subobject, respectively. Finally, as far as the local theory of symplectic forms is concerned, we only need the algebra style forms anyway.

We point out that the four additional objects (with tildes) just introduced are generally not the *transposes* of the first four, in the sense of Young diagrams. The transposes, instead, yield eight more objects, for a grand total of sixteen! The remaining objects are seen in:

$$\begin{tikzcd} \tilde{A}^k V^* \arrow[r] \arrow[d] & (\tilde{B}^k V)^* \arrow[d] \\ V^{*\otimes k} \arrow[r, "\text{de Morgan}"] \arrow[d] & V^{\parr k *} \arrow[d] \\ \tilde{S}^k V^* \arrow[r] & (\widetilde{\mathsf{Sym}}^k V)^* \end{tikzcd} \qquad \begin{tikzcd} A^k V^* \arrow[r] \arrow[d] & (B^k V)^* \arrow[d] \\ V^{*\otimes k} \arrow[r, "\text{de Morgan}"] \arrow[d] & V^{\parr k *} \arrow[d] \\ S^k V^* \arrow[r] & (\mathsf{Sym}^k V)^* \end{tikzcd} \tag{6.23}$$

As before, these eight new objects are defined by the isomorphic short exact sequence property as soon as we define one kernel or cokernel in each diagram. For instance:

$$\begin{aligned} \tilde{A}^k V &= \{t - t\sigma \,|\, t \in V^{\otimes k} \text{ and } \sigma \in S_k\} \\ \mathsf{Sym}^k V &= \mathsf{span}\left\{ \sum_{\sigma \in S_k} x_{\sigma_1} \parr \cdots \parr x_{\sigma_k} \,\middle|\, x_1, \cdots, x_k \in V \right\} \end{aligned} \tag{6.24}$$

We are more interested in the quotients $\wedge^k V$, $\mathsf{Alt}^k V$, $\tilde{\wedge}^k V$, $\widetilde{\mathsf{Alt}}^k V$, $S^k V$, $\mathsf{Sym}^k V$, $\tilde{S}^k V$, and $\widetilde{\mathsf{Sym}}^V W$, than their kernels–eight out of the sixteen objects. Four of these are isomorphic to four others, by the same reasoning that $\wedge^k V \cong \mathsf{Alt}^k V$. There is a coincidence if $k = 2$ that halves it once again, since by autonomy ($\otimes \cong \parr$), we have:

$$\tilde{I}^2 V = \mathsf{span}\{x \otimes y + y \otimes x\} \cong \mathsf{span}\{x \parr y + y \parr x\} = \mathsf{Sym}^2 V$$

Without making the other identifications, the diagrams in the $k = 2$ case read:

$$\begin{tikzcd} \mathsf{Sym}^2 V^* \arrow[r] \arrow[d] & S^2 V^* \arrow[d] \\ V^{*\otimes 2} \arrow[r, "\text{de Morgan}"] \arrow[d] & V^{\parr 2*} \arrow[d] \\ \tilde{\wedge}^2 V^* \arrow[r] & (\widetilde{\mathsf{Alt}}^2 V)^* \end{tikzcd} \qquad \begin{tikzcd} \widetilde{\mathsf{Sym}}^2 V^* \arrow[r] \arrow[d] & \tilde{S}^2 V^* \arrow[d] \\ V^{*\otimes 2} \arrow[r, "\text{de Morgan}"] \arrow[d] & V^{\parr 2*} \arrow[d] \\ \wedge^2 V^* \arrow[r] & (\mathsf{Alt}^2 V)^* \end{tikzcd} \tag{6.25}$$

On the one hand, this "coincidence" is due to bias with the number 2 baked into the definitions of $\tilde{I}^k V$, $I^k V$, $\tilde{A}^k V$, and if we were to define it directly, $A^k V$. On the other hand, by the isomorphisms $\wedge^k V \cong \mathsf{Alt}^k V$ and $S^k V \cong \mathsf{Sym}^k V$, we may reformulate these definitions by the equalities Eq. (6.22) and Eq. (6.24), which do not appear biased with respect to 2.

Finally, if $k = 2$ and d is odd or zero, the two diagrams in Eq. (6.25) coincide:

$$\begin{tikzcd} \mathsf{Sym}^2 V^* \arrow[r] \arrow[d] & S^2 V^* \arrow[d] \\ V^{*\otimes 2} \arrow[r, "\text{de Morgan}"] \arrow[d] & V^{\parr 2*} \arrow[d] \\ \wedge^2 V^* \arrow[r] & (\mathsf{Alt}^2 V)^* \end{tikzcd} \tag{6.26}$$

6.6 Symmetry and skew-symmetry abstractly

Although our generalized theory of symplectic forms calls for alternating forms, we briefly note how one may define the other kinds of tensors in Sec. 6.5. We are mainly interested in skew-symmetric bilinear forms due to the fact that alternation still implies skew-symmetry in the abstract setting.

Let $\mathscr{V}$ be a preabelian star-autonomous category. In the $k > 2$ case, we require coherent associative structures for $\otimes$ and $\parr$, but in the $k = 2$ case one may use the non-associative (but still unital) generalization of star-autonomy. Just as in the concrete case, it suffices to define a single kernel or cokernel in each of the following diagrams in order to define all sixteen by transporting strict exact sequences across the de Morgan isomorphism:

$$\begin{tikzcd}
\tilde{I}^k V^* \arrow[r] \arrow[d] & (\tilde{J}^k V)^* \arrow[d] \\
V^{*\otimes k} \arrow[r, "\mathsf{dM}"] \arrow[d] & V^{\parr k *} \arrow[d] \\
\tilde{\wedge}^k V^* \arrow[r] & (\widetilde{\mathsf{Alt}}^k V)^*
\end{tikzcd}
\qquad
\begin{tikzcd}
I^k V^* \arrow[r] \arrow[d] & (J^k V)^* \arrow[d] \\
V^{*\otimes k} \arrow[r, "\mathsf{dM}"] \arrow[d] & V^{\parr k *} \arrow[d] \\
\wedge^k V^* \arrow[r] & (\mathsf{Alt}^k V)^*
\end{tikzcd}
\qquad
\begin{tikzcd}
\tilde{A}^k V^* \arrow[r] \arrow[d] & (\tilde{B}^k V)^* \arrow[d] \\
V^{*\otimes k} \arrow[r, "\mathsf{dM}"] \arrow[d] & V^{\parr k *} \arrow[d] \\
\tilde{S}^k V^* \arrow[r] & (\widetilde{\mathsf{Sym}}^k V)^*
\end{tikzcd}
\qquad
\begin{tikzcd}
A^k V^* \arrow[r] \arrow[d] & (B^k V)^* \arrow[d] \\
V^{*\otimes k} \arrow[r, "\mathsf{dM}"] \arrow[d] & V^{\parr k *} \arrow[d] \\
S^k V^* \arrow[r] & (\mathsf{Sym}^k V)^*
\end{tikzcd}$$

We define symmetric and skew-symmetric bilinear forms along the same lines as we defined alternating forms. That is, we define $[\tilde{I}^k V]$ and $[\tilde{A}^k V]$ as the following unions:

$$[\tilde{I}^k V]_{V^{\otimes 2}} \cong \sum_t \sum_{\sigma \in S_k \smallsetminus A_k} (t + t\sigma) \qquad [\tilde{A}^k V]_{V^{\otimes 2}} \cong \sum_t \sum_{\sigma \in S_k} (t - t\sigma) \tag{6.27}$$

where both summations range over all *pure states*, i.e. morphisms of the form $t = t_1 \otimes \cdots \otimes t_k$ with $t_1, \cdots, t_k \in_\top V$, and where $t\sigma = t_{\sigma 1} \otimes \cdots \otimes t_{\sigma k}$. As in Sec. 6.3, the corresponding multilinear forms are defined as monic global elements of the corresponding quotients. Notice that the action of S_k is defined without the use of a (naturally varying) symmetric structure on $(\mathscr{V}, \otimes)$, in the sense of *symmetric monoidal categories*. It may be that a naturally-varying symmetric or skew-symmetric form induces a symmetric structure on its domain of oidification, similar to how the existence of a naturally-varying nuclear form implies star-autonomy, but we leave this question for future work due to lack of time.

Although we won't need the following approach, one could also generalize Eq. (6.19) as follows. For simplicity assuming $\otimes \cong \parr$, we may on the other hand use the following definitions:

$$\mathsf{Alt}_0 : V^{\otimes k} \to V^{⅋ k} \qquad\qquad \mathsf{Alt}_0 = \sum_{\sigma \in S_k} \mathsf{sgn}(\sigma)\sigma$$

$$\mathsf{Sym}_0 : V^{\otimes k} \to V^{⅋ k} \qquad\qquad \mathsf{Sym}_0 = \sum_{\sigma \in S_k} \sigma$$

These maps are off by a factor of $\frac{1}{k!}$ from the projection maps, but this normalization is seen to be preferable in Sec. 6.5. Then one may define the alternating and symmetric subobjects as the images of these maps:

$$\mathsf{Alt}^k V := \mathsf{ker}\,\mathsf{coker}\,\mathsf{Alt}_0$$
$$\mathsf{Sym}^k V := \mathsf{ker}\,\mathsf{coker}\,\mathsf{Sym}_0$$

These definitions can likely be generalized to the star-autonomous case, where we do not necessarily have $\otimes \cong ⅋$, and the natural action by the symmetric group maps from $V^{\otimes k}$ to $V^{⅋ k}$, but we leave this for future work. We now have two ways to define $\wedge^2 V$, but we find that the characterization given in Sec. 6.3 is more accessible from the theory of symplectic forms. We will not use the version defined here in terms of $\mathsf{Alt}^k V$, so we don't bother proving the equivalence of the two characterizations at this time. We also have two ways to define skew-symmetric forms, and we use Eq. (6.27) as our working definition. We leave the definitions of the kernels and cokernels in the first or third diagram above to the reader.

Proposition 6.6.1 *Let $\mathscr{V}$ be a symmetric preabelian star-autonomous category. Then every alternating bilinear form $\omega : V \otimes V \to \perp$ is skew-symmetric.*

We omit the proofs of some basic properties about distributivity between $\oplus$ and $\otimes$.

Proof sketch Since $\oplus$ is the biproduct and $\mathscr{V}$ is closed with respect to $\otimes$, it follows (since right adjoints preserve limits) that $\oplus$ distributes over $\otimes$ in the appropriate sense. From this, one may show that $+$ distributes over $\otimes$, in the sense that for $r, s : W \to V$,

$$(r+s) \otimes (r+s) = r \otimes r \;+\; r \otimes s \;+\; s \otimes r \;+\; s \otimes s : W^{\otimes 2} \to V^{\otimes 2}$$

Composing with $\pi : V^{\otimes 2} \to \wedge^2 V$, we get:

$$(r+s) \wedge (r+s) = r \wedge r \;+\; r \wedge s \;+\; s \wedge r \;+\; s \wedge s : W^{\otimes 2} \to \wedge^2 V$$

Then plugging in monic global elements $q \in_\top Q$ and $p \in_\top P$ of subobjects $x : [Q]_V$ and $y : [P]_V$, by the definition of alternating form we have $xq \wedge xq = 0$ and $yp \wedge yp = 0$, (although note that $x \wedge x$ and $y \wedge y$ are generally nonzero). Moreover, $xq + yp$ is a monic global element, and so $(xq + yp) \wedge (xq + yp) = 0$. So:

$$0 = xq \wedge yp + yp \wedge xq : \top^{\otimes 2} \to \wedge^2 V$$

and so $\omega(xq \otimes yp) + \omega(yp \otimes xq) = 0$, as claimed. ■

6.7 Orthogonality

Let $\mathscr{V}$ be a preabelian star-autonomous category, let $\omega : V \otimes V \to \bot$ be a bilinear form. Recall that in the concrete case, one defines the *left* and *right orthogonal subobjects*, also called the *left* and *right perp*, as follows:

$$Q^\omega = \{v \in V \mid \omega(q, v) = 0 \text{ for all } q \in Q\} = \bigcap_{q \in Q} \mathsf{ker}\, q^\flat \tag{6.28}$$
$$^\omega P = \{v \in V \mid \omega(v, p) = 0 \text{ for all } p \in P\} = \bigcap_{p \in P} \mathsf{ker}\, {}^\flat p$$

For the abstract case, let $x : [Q]$ and $q \in_U Q$, and recall that we have defined (c.f. Eq. (6.13)):

$$\lceil q^\flat \rceil : U \to V^* \qquad\qquad q^\flat : U \otimes V \to \bot \qquad\qquad \lfloor q^\flat \rfloor : V \to {}^*U$$

Now, there are two conceivable ways to define the left orthogonal subobject, depending on whether we focus on global elements or generalized elements. First, we define the *left orthognal subobject at stage of definition* U as the following intersection:

$$Q^\omega_U = \textstyle\bigcap_{q \in_U Q} \mathsf{ker}\, \lfloor q^\flat \rfloor \xrightarrow{\pi_q} \mathsf{ker}\, \lfloor q^\flat \rfloor \xrightarrow{k_q} V \xrightarrow{\lfloor q^\flat \rfloor} {}^*U \tag{6.29}$$

Of particular importance is the *left global orthogonal subobject* $Q^\omega_\top$, which matches Eq. (6.28) when $\mathscr{V}$ is determined by its global elements. The second abstraction is the *generalized left orthogonal subobject*, which we define as an intersection over all stages of definition U:

$$\left[Q^\omega_{\mathsf{gen}} = \bigcap_U Q^\omega_U \right]$$

Clearly, $[Q^\omega_{\mathsf{gen}} \subseteq Q^\omega_U]$ for all U, and in particular $[Q^\omega_{\mathsf{gen}} \subseteq Q^\omega_\top]$. We now seek to prove:

Theorem 6.7.1 *Let $(-)^\omega = (-)^\omega_U$ or $(-)^\omega_{\mathsf{gen}}$. Then $(-)^\omega : \mathscr{V} \to \mathscr{V}^{\mathrm{op}}$ is a contravariant endofunctor and has a right adjoint, or equivalently,*[5] *there is another functor ${}^\omega(-) : \mathscr{V}^{\mathrm{op}} \to \mathscr{V}$ with which $(-)^\omega$ satisfies both left and right double dualization translation in* $\mathrm{Sub}_{\mathscr{V}}(V)$ *and hence at least six out of the following eight de Morgan laws:*

$$[Q^\omega \cup P^\omega \subseteq (P \cap Q)^\omega] \qquad\qquad [{}^\omega(Q \cup P) = {}^\omega P \cap {}^\omega Q]$$
$$[{}^\omega Q \cup {}^\omega P \subseteq {}^\omega(P \cap Q)] \qquad\qquad [(Q \cup P)^\omega = P^\omega \cap Q^\omega]$$

[5] This is because $\mathrm{Sub}_{\mathscr{V}}(V)$ is a preorder. The six de Morgan laws follow since it is a lattice, c.f. Prop. 5.2.6.

In the next section, we will see by example that $(-)^\omega$ does not necessarily have double dualization *elimination*. In this way, $\textsc{Sub}_{\mathscr{V}}(V)$ behaves similarly to a Heyting algebra, but generally is not one since dualization $(-)^\omega$ is generally not a negation and there is no implication, i.e. $\textsc{Sub}_{\mathscr{V}}(V)$ is not Cartesian-closed.

Lemma 6.7.2 *$(-)^\omega_U$ and $(-)^\omega_{\mathsf{gen}}$ are contravariant endofunctors on $\textsc{Sub}_{\mathscr{V}}(V)$.*

Proof To see that $(-)^\omega_U$ is a contravariant endofunctor, assume $\phi : [P \subseteq Q]$, let $p \in_U P$, and set $q = \phi p$ and $r : [Q^\omega_U]$. Then $q \in_U Q$, and the following diagram commutes:

$$\begin{tikzcd}
Q^\omega_U \arrow[d, "r"'] \arrow[dr, "0"] & & \\
V \arrow[r, "\lfloor q^\flat \rfloor"] \arrow[d, "\lfloor \omega \rfloor"'] & {}^*U & \\
{}^*V \arrow[r, "{}^*x"'] \arrow[rr, bend right, "{}^*y"'] & {}^*Q \arrow[u, "{}^*q"] \arrow[r, "{}^*\phi"'] & {}^*P \arrow[ul, "{}^*p"']
\end{tikzcd}$$

Note that the square commutes by Eq. (6.14). The outside path is $0 = {}^*(yp)\lfloor\omega\rfloor r = \lfloor p^\flat \rfloor r$, so by universality of the kernel, $[Q^\omega_U \subseteq \mathsf{ker}\lfloor p^\flat \rfloor]$. Since this holds for all $p \in_U P$, by universality of the intersection defining $[P^\omega_U]$, it follows that $[Q^\omega_U \subseteq P^\omega_U]$, so $(-)^\omega_U$ is a contravariant endofunctor. Now, since $[Q^\omega_{\mathsf{gen}} \subseteq Q^\omega_U \subseteq P^\omega_U]$ for all U, it follows by universality of the intersection defining $[P^\omega_{\mathsf{gen}}]$ that $[Q^\omega_{\mathsf{gen}} \subseteq P^\omega_{\mathsf{gen}}]$. ∎

For the right orthogonal subobject, we use the following dual version of diagram Eq. (6.13). Given $y : [P]$ and $p \in_U P$, define the *right partial evaluation* ${}^\flat p : V \otimes U \to \perp$ by:

$$\begin{tikzcd}
U \arrow[r, "\lfloor {}^\flat p \rfloor"] \arrow[d, "p"'] & {}^*V \\
P \arrow[r, "y"'] & V \arrow[u, "\lfloor \omega \rfloor"']
\end{tikzcd} \tag{6.30}$$

Then $[{}^\omega_U P]$ and $[{}^\omega_{\mathsf{gen}} P]$ are defined by putting $\lceil {}^\flat p \rceil$ in place of $\lfloor q^\flat \rfloor$ in Eq. (6.29). By convention, we view these as objects in $\textsc{Sub}_{\mathscr{V}}(V)$, never in $\textsc{Sub}_{\mathscr{V}}(V)^{\mathrm{op}}$. In analogy to Eq. (6.14), we have:

$$\lceil \omega(x \otimes yp) \rceil = \lceil {}^\flat p \rceil x \tag{6.31}$$

Then Eq. (6.14) and Eq. (6.31) yield the following identity, relating left and right partial evaluation:

$$\rfloor \lfloor q^\flat \rfloor yp \lfloor = \omega(xq \otimes yp) = \rceil \lceil^\flat p \rceil xq \lceil : U \otimes U \to \bot \tag{6.32}$$

Lemma 6.7.3 *$(-)^\omega_U$ and $(-)^\omega_{\text{gen}}$ have left double dualization translation. In other words:*

$$[Q \subseteq {}^{\omega}_{U}(Q^\omega_U)] \qquad\qquad \textit{and} \qquad\qquad [Q \subseteq {}^{\omega}_{\mathsf{gen}}(Q^\omega_{\mathsf{gen}})]$$

meaning ${}^{\omega}_{U}(-), {}^{\omega}_{\mathsf{gen}}(-) : \mathscr{V}^{\mathrm{op}} \to \mathscr{V}$ are the right adoints of $(-)^\omega_U$ resp. $(-)^\omega_{\mathsf{gen}} : \mathscr{V} \to \mathscr{V}^{\mathrm{op}}$.

Dually, $(-)^\omega_U$ and $(-)^\omega_{\mathsf{gen}}$ also have right double dualization translation.

Proof Introduce another subobject $[P]$ satisfying $[P \subseteq Q^\omega_U]$, and let $q \in_U Q$, $p \in_U P$, $x : [Q]$, and $y : [P]$. Since $[P \subseteq Q^\omega_U]$, $\lfloor q^\flat \rfloor y = 0$. Then using Eq. (6.32), we have:

$$\lceil^\flat p \rceil xq = \lceil \rfloor \lfloor q^\flat \rfloor yp \lfloor \rceil = \lceil \rfloor 0 \lfloor \rceil = 0 : U \to U^*$$

Now invoke the $\textsc{Ab}$-enriched Yoneda embedding $\text{よ}_{\mathscr{V}} : \mathscr{V} \rightarrowtail [\mathscr{V}^{\mathrm{op}}, \textsc{Ab}]$:

$$\begin{aligned} \text{よ}_{\mathscr{V}}(\lceil^\flat p \rceil x)(U) = \mathsf{hom}_{\mathscr{V}}(U, \lceil^\flat p \rceil x) : \mathsf{hom}_{\mathscr{V}}(U, Q) &\to \mathsf{hom}_{\mathscr{V}}(U, \bot) \\ q &\mapsto \lceil^\flat p \rceil xq = 0 \end{aligned}$$

Since $\text{よ}_{\mathscr{V}}(\lceil^\flat p \rceil x)(U) = (q \mapsto 0)$ for each U, $\text{よ}_{\mathscr{V}}(\lceil^\flat p \rceil x) : \mathscr{V}^{\mathrm{op}} \to \textsc{Ab}$ is naturally isomorphic to the zero-valued functor. This is the zero object in $[\mathscr{V}^{\mathrm{op}}, \textsc{Ab}]$, so since $\text{よ}_{\mathscr{V}}$ is full and faithful, $\lceil^\flat p \rceil x = 0$. By the universality of kernels and intersections, $[Q \subseteq {}^{\omega}_{U}P]$. For the $(-)^\omega_U$ case, substitute $P = Q^\omega_U$ (typically $U = \top$), and for the $(-)^\omega_{\mathsf{gen}}$ case, $P = Q^\omega_{\mathsf{gen}}$. Then

$$\begin{tikzcd}
 & & P \arrow[r] & Q^\omega_U \arrow[d] & \\
{}^{\omega}_{\mathsf{gen}}P \arrow[r] & {}^{\omega}_{U}P \arrow[r] & \mathsf{ker}\,\lceil^\flat p \rceil \arrow[r] & V \arrow[r, "\lceil^\flat p \rceil"] & {}^*U \\
 & U \arrow[r, "q"'] & Q \arrow[ull, dashed] \arrow[ul, dashed] \arrow[u, dashed] \arrow[ur, "x"'] & &
\end{tikzcd}$$

commutes, proving both claims. ■

Notice how even the statement about $(-)^{\omega}_{\top}$ required us to use $(-)^{\omega}_{\mathsf{gen}}$ in the proof so that we could apply the Yoneda embedding theorem. This is our original reason for introducing $(-)^{\omega}_{\mathsf{gen}}$, since our categories of interest are determined by their global elements anyway.

Proof of Thm. 6.7.1. Combine Lem. 6.7.2, Lem. 6.7.3, and the dual of Lem. 6.7.3 with Prop. 5.2.6. ■

Lastly, we note that in the case of a symmetric or skew-symmetric bilinear form, the left and right global orthogonal subobjects are naturally isomorphic in $\mathrm{S{\small UB}}_{\mathscr{V}}(V)$. This is generally false for bilinear forms that are not skew-symmetric or symmetric, even if $(\mathscr{V}, \otimes)$ has a symmetric structure. In other words, the following diagram may **not** commute:

$$\begin{tikzcd}
 & V^* & \\
U \arrow[ur, "\lceil r^\flat \rceil"] \arrow[dr, "\lfloor {}^\flat r \rfloor"'] \arrow[r, phantom, "?"] & & V \arrow[ul, "\lceil \omega \rceil"'] \arrow[dl, "\lfloor \omega \rfloor"] \\
 & {}^*V \arrow[uu, "\wr"] &
\end{tikzcd}$$

For example, in the category of finite dimensional vector spaces over $\mathbb{F}_2$, consider the subspace $Q = \mathsf{span}\{\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]\}$ of the vector space $\mathbb{F}_2^2$. Let $\omega = \left[\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right]$, which is not symmetric = skew-symmetric. Then $Q^\omega = \mathsf{span}\{\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]\}$ whereas ${}^\omega Q = \mathsf{span}\{\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right]\}$.

Proposition 6.7.4 *Let $\mathscr{V}$ be a symmetric preabelian star-autonomous category determined by its global* $\mathrm{A{\small B}}$*-enriched elements, and let ω be a symmetric or skew-symmetric bilinear form on an object V. Then for all subobjects $[Q]$, we have:*

$$[Q \subseteq (Q^{\omega}_{\top})^{\omega}_{\top}]$$

In such a case, by uniqueness of adjoints, $(-)^{\omega}_{\top}$ and ${}^{\omega}_{\top}(-)$ are (naturally isomorphic to) each other's opposite. In other words, the orthogonality adjunction is self-adoint:

$$[{}^{\omega}_{\top}Q = Q^{\omega}_{\top}]$$

This is sometimes expressed by saying that every subobject $[Q]$ is *cyclic*.

Proof Let $q \in_\top Q$, $p \in_\top Q^\omega_\top$, $x : [Q]$, and $y : [Q^\omega_\top]$, and consider $\lfloor p^\flat \rfloor xq : \top \to \bot$:

$$\begin{aligned}
\lfloor p^\flat \rfloor xq &= \lfloor \omega(yp \otimes xq) \rfloor && \text{by Prop. 6.4.1.}\\
&= \lfloor \pm\omega(xq \otimes yp) \rfloor && \text{by (skew-)symmetry (since } q \text{ and } p \text{ are global).}\\
&= \pm\lfloor \omega(xq \otimes yp) \rfloor && \text{by Prop. 5.2.1}\\
&= \pm\lfloor q^\flat \rfloor yp && \text{by Prop. 6.4.1.}\\
&= 0 && \text{Since } \lfloor q^\flat \rfloor y = 0, \text{ since } y : [Q^\omega_\top].
\end{aligned}$$

Let $\mathsf{el} = \mathsf{hom}_{\mathscr{V}}(\top, -) : \mathscr{V} \to \textsc{Ab}$ be the $\textsc{Ab}$-enriched hom functor at stage of definition $\top$. Then $\mathsf{el}(\lfloor p^\flat \rfloor x) : \mathsf{el}\, Q \to \mathsf{el}\, \bot$ is given by $q \mapsto \lfloor p^\flat \rfloor xq$, which by the above calculation, is the zero homomorphism. Since $\mathscr{V}$ is determined by its $\textsc{Ab}$-enriched elements, it follows that $\lfloor p^\flat \rfloor x = 0$. Then by the universality of kernels and intersections, $[Q \subseteq (Q^\omega_\top)^\omega_\top]$. ■

6.8 Isotropy

Let V be an object in a preabelian star-autonomous category $\mathscr{V}$. A contravariant endofunctor $(-)^\omega$ on $\mathrm{Sub}_{\mathscr{V}}(V)$ yields notions of *isotropic*, *coisotropic*, and *Lagrangian* subobjects:

$[Q \subseteq Q^\omega]$	$[Q \supseteq Q^\omega]$	$[Q = Q^\omega]$
$[Q]$ is isotropic	$[Q]$ is coisotropic	$[Q]$ is Lagrangian

Of course we consider these notions as they pertain to the operations $(-)^\omega_\top$ and $(-)^\omega_{\mathsf{gen}}$ defined in the previous section. As such, we refer to subobjects being *globally* resp. *generally* isotropic, and so on. Clearly, every Lagrangian subobject $[Q]$ is maximally isotropic, meaning if $[Q \subseteq P]$ and $[P]$ is also isotropic then $[Q = P]$. The reader is encouraged to take a moment to prove the converse, i.e. that every maximally isotropic subobject is Lagrangian, in the case that (V, ω) is a finite dimensional real symplectic vector space. Note that this converse is false if ω is an inner product instead of a symplectic form. The proof hinges on the fact that one-dimensional subspaces of a symplectic vector space, which for brevity we call *lines*, are isotropic. It also uses skew-symmetry, which follows from alternation. Assuming $\mathscr{V}$ satisfies the subobject axiom, maximal isotropic subobjects of an object with symplectic form (V, ω) turn out to be Lagrangian in the abstract setting as well, but as we shall see, proving this takes a considerable amount of effort.

Assume V has an alternating square, and let ω be an alternating form on V.

Proposition 6.8.1 $[V^\omega_{\mathsf{gen}} = 0]$ *if and only if* $\lfloor \omega \rfloor$ *is a monomorphism.*

As in the ordinary theory of symplectic vector spaces, we often need the property $[V^\omega_{\mathsf{gen}} = 0]$ (or equivalently $[V^\omega_{\mathsf{gen}} \cap V = 0]$), and therefore consider a *nondegenerate alternating form*, i.e. a *symplectic form*. For simplicity, we take *nondegeneracy* to mean something stronger: that $\lceil \omega \rceil$ and $\lfloor \omega \rfloor$ are isomorphisms. In the case of symplectic vector spaces, this means we restrict our attention to the finite dimensional ones. It may be possible to prove a global element analog if $\mathscr{V}$ satisfies the subobject axiom, but we don't need this for now anyway.

Proof In Eq. (6.13) let us set $Q = V$ and $x = \mathsf{id}_V : [V]$. Suppose $[V^\omega_{\mathsf{gen}} = 0]$. In order to show that $[\mathsf{ker}\,\lfloor \omega \rfloor = 0]$ (and hence $\lfloor \omega \rfloor$ is a monomorphism), by universality of intersections, it suffices to show $[\mathsf{ker}\,\lfloor \omega \rfloor \subseteq \mathsf{ker}\,\lfloor q^\flat \rfloor]$ for all U and $q \in_U V$. Denoting $y : [\mathsf{ker}\,\lfloor \omega \rfloor]$, we have:

$$\lfloor q^\flat \rfloor y = {}^*(xq) \lfloor \omega \rfloor y = 0$$

so the desired containment follows by universality of $\mathsf{ker}\,\lfloor q^\flat \rfloor$. Conversely, let $r : [V^\omega_{\mathsf{gen}}]$ and substitute $U = V$ and $q = x = \mathsf{id}_V$. Then $\lfloor \omega \rfloor r = \lfloor q^\flat \rfloor r = 0$, and so $[Q^\omega_{\mathsf{gen}} \subseteq \mathsf{ker}\,\lfloor \omega \rfloor = 0]$.■

Due to Prop. 6.8.1, we now assume that ω is a *symplectic form* on V. As noted above, a crucial ingredient of the theory of symplectic forms is the fact that lines are isotropic. Before we prove this abstractly, note that even in the concrete case, the morphism $\omega(x \otimes x) : Q \otimes Q \to \bot$ is *generally* nonzero when $x : [Q]$ is a subobject, which could also be viewed as a monic *generalized* element $x \in_Q V$. However, it is clear from our definition of *alternating bilinear form* that $\omega(x \otimes x) = 0$ when x is a subobject of the form $x : [\top]_V$, which we call a *line*. Thus, the definition of *alternating form* gives special treatment to monic *global* elements.

Proposition 6.8.2 *Each line $x : [\top]$ is isotropic both in the global element sense and in the generalized element sense.*

Proof Consider a monic generalized element $q \in_U \top$ of a line $x : [\top]$. Since $\omega(x \otimes x) = 0$,

$$\lfloor q^\flat \rfloor x = \lfloor \omega(xq \otimes x) \rfloor = \lfloor \omega(x \otimes x)(q \otimes \mathsf{id}_\top) \rfloor = \lfloor 0 \rfloor = 0 : \top \to {}^*U$$

Then by the universal property of the kernel, we have a factorization:

$$\begin{tikzcd} & \top \arrow[dl, dashed] \arrow[d, "x"] \\ \ker \lfloor q^\flat \rfloor \arrow[r] & V \end{tikzcd}$$

Since q was an arbitrary, $x : [\top]$ is generally (as well as globally) isotropic. ■

Finally, we arrive at the following nontrivial theorem.

Theorem 6.8.3 *Let $(-)^\omega \dashv {}^\omega(-)$ be a contravariant adjunction on $\mathrm{SUB}_{\mathscr{V}}(V)$ that deems all lines isotropic. Further assume that lines are cyclic, i.e. for any $z : [\top]$, $[\top^\omega = {}^\omega\top]$ where $z^\omega : [\top^\omega]$ and ${}^\omega z : [{}^\omega\top]$. Then a maximally isotropic subobject $[Q]$ is coisotropic if and only if the plain (i.e. unenriched) subobject axiom is satisfied for $[Q]$ and $[Q^\omega]$.*

For the *plain subobject axiom*, see Sec. 5.1.3. By *contravariant adjunction*, we mean that $(-)^\omega : \mathscr{V} \to \mathscr{V}^{\mathrm{op}}$ and ${}^\omega(-) : \mathscr{V}^{\mathrm{op}} \to \mathscr{V}$ satisfy left double dualization translation: $[Q \subseteq {}^\omega(Q^\omega)]$. Recall that if $\mathscr{V}$ is equipped with a symmetry, then alternating forms are skew-symmetric, which in turn implies that $(-)^\omega_\top \dashv {}^\omega_\top(-)$ is self-adjoint, i.e. that $[W^\omega_\top = {}^\omega_\top W]$ for all subobjects $[W]$. This property, as pertaining to the line $[\top^\omega = {}^\omega\top]$, generalizes the role of skew-symmetry as it enters the proof in the concrete setting.

Proof Let $x : [Q]$, $y : [Q^\omega]$, and consider a monic global element $p \in_\top Q^\omega$; if no such p exists, then the result holds vacuously. Now let $\phi : [Q \subseteq Q^\omega]$ be the isotropy witness. By Prop. 6.8.2, let $\ell : [\top \subseteq \top^\omega]$. Now let $\psi : [Q \subseteq {}^\omega\top]$ be the composite of $[{}^\omega\top = \top^\omega]$, ${}^\omega p : [{}^\omega(Q^\omega) \subseteq {}^\omega\top]$, and $[Q \subseteq {}^\omega(Q^\omega)]$. Then we get a commutative diagram:

$$\begin{tikzcd}
{[Q]} \arrow[r] \arrow[dr, "\langle\phi,\psi\rangle"'] & {[\top \cup Q]} \arrow[d, dashed] & yp : [\top] \arrow[l] \arrow[dl, "\langle p,\ell\rangle"] \\
 & {[Q^\omega \cap \top^\omega]} &
\end{tikzcd} \tag{6.33}$$

The dashed arrow in Eq. (6.33) is from universality of the union. The notation $\langle\cdot,\cdot\rangle$ refers to the dashed arrow gotten from applying universality of the intersection. Likewise, $[\cdot,\cdot]$ indicates the dashed arrow gotten from universality of a coproduct (union):

$$[\langle\phi,\psi\rangle, \langle p,\ell\rangle] : [\top \cup Q \subseteq Q^\omega \cap \top^\omega]$$

By the intuitionistic de Morgan law (which follows from double dualization translation), $[Q^\omega \cap \top^\omega \subseteq (\top \cup Q)^\omega]$, so $[\top \cup Q]$ is isotropic. By maximality, $[Q = \top \cup Q]$, which by composition yields $q : [\top \subseteq Q]$ with $xq = yp$. Since p was arbitrary, the desired containment $[Q^\omega \subseteq Q]$ is equivalent to the subobject axiom for $x : [Q]$ and $y : [Q^\omega]$. ∎

Some remarks are in order concerning the use of the subobject axiom in Thm. 6.8.3. Inconveniently, it is the plain subobject axiom, as opposed to the (weaker) enriched subobject axiom, that is required. If it were the enriched version, we could use Cor. 5.1.5, since our categories of interest are determined by their enriched monic global elements. We find it unclear, however, whether Thm. 6.8.3 admits an enriched generalization. If it does, we suspect that the proof would look very different. In a different direction, we have come to expect Yoneda style generalized element versions that hold without requiring enrichment.

Our proof of Thm. 6.8.3 assigns a $q \in_\top Q$ to each $p \in_\top Q^\omega$. In other words, it specifies a function

$$A_\top : \mathsf{Hom}_{\mathrm{SUB}_{\mathscr{V}}(V)}([\top], [Q^\omega]) \to \mathsf{Hom}_{\mathrm{SUB}_{\mathscr{V}}(V)}([\top], [Q])$$

For the generalized element version, we would instead need to construct a function of type

$$A_W : \mathsf{Hom}_{\mathrm{SUB}_{\mathscr{V}}(V)}([W], [Q^\omega]) \to \mathsf{Hom}_{\mathrm{SUB}_{\mathscr{V}}(V)}([W], [Q])$$

for each $[W] \in \mathsf{ob}(\mathrm{SUB}_{\mathscr{V}}(V))$ playing the role of $[\top]$. The problem is that in order to carry out the proof, we need to assume $[W]$ is isotropic from the outset. Although isotropy is preserved under inclusion, $[W]$ is only presumed to be a subobject of $[Q^\omega]$, which a priori is not isotropic. To state it another way, consider the preorder $\mathrm{ISO}_{\mathscr{V}}(V, \omega)$ of isotropic subobjects of V. Then only after proving Thm. 6.8.3 do we obtain:

$$A_W : \mathsf{Hom}_{\mathrm{ISO}_{\mathscr{V}}(V,\omega)}([W], [Q^\omega]) \to \mathsf{Hom}_{\mathrm{ISO}_{\mathscr{V}}(V,\omega)}([W], [Q]) \tag{6.34}$$

It is convenient to supplement $\mathrm{ISO}_{\mathscr{V}}(V, \omega)$ by giving it the maximum element $\mathsf{id}_V : [V]$ even though $[V]$ is not an isotropic (unless $[V = 0]$). Then $\mathrm{ISO}_{\mathscr{V}}(V, \omega)$ becomes a slice category:

$$\mathrm{ISO}_{\mathscr{V}}(V, \omega) = \mathscr{I}_{\mathscr{V}}(V, \omega) \downarrow V$$

where we temporarily define $\mathscr{I}_{\mathscr{V}}(V, \omega)$ to be the subcategory of $\mathscr{V}$ consisting of monomorphisms of the form $x : Q \to V$ for Q such that $[Q \subseteq Q^\omega]$, as well as monomorphisms of the form $f : Q \to P$ commuting with such $x : Q \to V$ and $y : P \to V$. This enables us to use Lem. 5.1.7 and Thm. 5.1.6 to see, only in retrospect, that maximally isotropic subobjects are coisotropic by reflecting the Yoneda embedding in Eq. (6.34).

Whether or not we include $[V]$, one may observe that $\mathrm{ISO}_{\mathscr{V}}(V, \omega)$ is a $\cap$-semilattice, but unions $[Q \cup P]$ of isotropic subobjects $[Q]$ and $[P]$ are of course not necessarily in $\mathrm{ISO}_{\mathscr{V}}(V, \omega)$.

In conclusion, we do not know whether the theorem can be proved without assuming the plain subobject axiom, either by assuming a (weaker) enriched version, or nothing at all, appealing to Yoneda-style arguments. Equivalently, we do not know whether the subobject axiom is always satisfied for pairs of subobjects of the form $([Q], [Q^\omega])$.

6.9 Isotropy, complementation, and topology

An important example of a Lagrangian subgroup of a locally compact abelian group is $Q = \mathbb{Z}^{2n}$ in $V = \mathbb{R}^{2n}$. Despite being Lagrangian, Q does not have a complement P, i.e. another subgroup satisfying $V = Q \oplus P$. This sets locally compact abelian groups apart from finite dimensional real vector spaces, in which Lagrangian subspaces always admit isomorphic Lagrangian complements. Nevertheless, the corresponding quotient $V/Q \cong \mathbb{T}^{2n}$ plays an important role. Namely, the unique irreducible center-respecting representation of the Heisenberg group for $\textsc{Heis}(V, \omega)$ can be realized on $L^2(V/Q)$ [Mum06]. Our goal in this section is to probe at some of these features in the abstract framework.

Theorem 6.9.1 *Let $\mathscr{V}$ be a preabelian star-autonomous category, let $\omega : V \otimes V \to \perp$ be a symplectic form in $\mathscr{V}$, let $x : [Q]_V$ be a subobject, and consider its generalized symplectic orthogonal $y : [Q^\omega_{\mathsf{gen}}]_V$. Then we have an isomorphism of exact sequences:*

$$
\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] \\
Q^\omega_{\mathrm{gen}} \arrow[r, "\lfloor\omega\rfloor\downarrow_{Q^\omega_{\mathsf{gen}}}", "\sim"'] \arrow[d, "y"'] & {}^*(V/Q) \arrow[d] \\
V \arrow[r, "\lfloor\omega\rfloor"] \arrow[d] & {}^*V \arrow[d, "{}^*x"] \\
V/Q^\omega_{\mathrm{gen}} \arrow[r, "\sim"] \arrow[d] & {}^*Q \arrow[d] \\
0 & 0
\end{tikzcd}
\tag{6.35}
$$

Equivalently, ${}^*(V/Q)$ is a subobject of V (via $\lfloor\omega\rfloor^{-1}$) and $[Q^\omega_{\mathrm{gen}} = {}^*(V/Q)]_V$.

This is evidence that $[Q^\omega_{\mathsf{gen}}]$, as opposed to $[Q^\omega_\top]$, is the better notion of symplectic orthogonal. Recall that this was unclear from the offset since our defnition of *alternating form* immediately introduces bias towards $\top$ as a relevant stage of definition.

Proof Start with the exact sequence on the left of Eq. (6.35). Since $\lfloor\omega\rfloor$ is an isomorphism, it is transported to an exact sequence with trivial image-coimage factorizations. Without loss of generality, there exists a subobject $z : [R]_V$ such that we have the following commutative diagram with exact columns:

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] \\
Q^\omega_{\mathsf{gen}} \arrow[r] \arrow[d, "y"'] & {}^*(V/R) \arrow[d] \\
V \arrow[r, "\lfloor\omega\rfloor"] \arrow[d] & {}^*V \arrow[d, "{}^*z"] \\
V/Q^\omega_{\mathsf{gen}} \arrow[r] \arrow[d] & {}^*R \arrow[d] \\
0 & 0
\end{tikzcd}$$

It thus suffices to show that $\mathsf{ker}\,{}^*x \cong \lfloor\omega\rfloor y$ in $\mathscr{C} \downarrow {}^*R$. First let us form the following commutative diagram for each object U and each $q \in_U Q$:

$$\begin{tikzcd}
Q^\omega_U = \bigcap_{q \in_U Q} \mathsf{ker}\,\lfloor q^\flat \rfloor \arrow[r] \arrow[d] & Q^\omega_{\mathsf{gen}} = \bigcap_U Q^\omega_U \arrow[r, dashed] \arrow[d, "y"'] & {}^*(V/Q) \arrow[d, "k"] \\
\mathsf{ker}\,\lfloor q^\flat \rfloor \arrow[r] & V \arrow[r, "\lfloor\omega\rfloor"] \arrow[d, "\lfloor q^\flat \rfloor"'] & {}^*V \arrow[d, "{}^*x"] \\
& {}^*U & {}^*Q \arrow[l, "{}^*q"]
\end{tikzcd} \tag{6.36}$$

A priori, we don't have the dashed arrow above, but using established properties, we find:

$$({}^*q)({}^*x)\lfloor\omega\rfloor y = {}^*(xq)\lfloor\omega\rfloor y = \lfloor\omega(xq \otimes y)\rfloor = \lfloor q^\flat \rfloor y = 0 : Q^\omega_{\mathsf{gen}} \to {}^*U$$

In particular, plugging in Q and id_Q for U and q, respectively, we find that ${}^*x\lfloor\omega\rfloor y = 0$, giving the dashed arrow in Eq. (6.36). Now since ${}^*xk = 0$, for each U and $q \in_U Q$, and since $0 = {}^*(xq)k = \lfloor q^\flat \rfloor \lfloor \omega \rfloor^{-1} k$, unwinding definitions, we get the following dashed arrows:

$$\begin{tikzcd}
Q^\omega_U \arrow[r] \arrow[d] & Q^\omega_{\mathsf{gen}} \arrow[r, dashed] \arrow[d, "y"] & {}^*(V/Q) \arrow[d, "k"] \arrow[l, dashed, bend right, "(3)"'] \arrow[ll, dashed, bend right, "(2)"'] \arrow[dll, dashed, bend right=80, "(1)"'] \\
\mathsf{ker}\,\lfloor q^\flat \rfloor \arrow[r] & V \arrow[r, "\lfloor \omega \rfloor"] \arrow[d, "\lfloor q^\flat \rfloor"'] & {}^*V \arrow[d, "{}^*x"] \\
 & {}^*U & {}^*Q \arrow[l, "{}^*q"]
\end{tikzcd} \tag{6.37}$$

Since the whole diagram commutes, this shows that $[Q^\omega_{\mathsf{gen}} = {}^*(V/Q)]$ as claimed. ∎

Corollary 6.9.2 *$[Q^\omega_{\mathsf{gen}} = 0]$ if and only if $[Q = V]$ and $[Q^\omega_{\mathsf{gen}} = V]$ if and only if $[Q = 0]$.*

Here we have already presumed that $\lceil \omega \rceil$ and $\lfloor \omega \rfloor$ are monic, unlike in Prop. 6.8.1.

Theorem 6.9.3 *Let $\mathscr{V}$ be a pre-abelian star-autonomous category, let $\omega : V \otimes V \to \perp$ be a symplectic form in $\mathscr{V}$, and let $x : [Q]_V$ be an isotropic subobject, in the generalized element sense ($[Q \subseteq Q^\omega_{\mathsf{gen}}]$). Then $\mathsf{coker}\, x$ is a subquotient of ${}^*x\lfloor \omega \rfloor$ over V.*

Proof Since $[Q]$ is isotropic, ${}^*x\lfloor \omega \rfloor x = \lfloor \omega(x \otimes x) \rfloor = \lfloor 0 \rfloor = 0$, so we get the following dashed arrow by universality of the cokernel:

$$\begin{tikzcd}
Q \arrow[d, "x"'] & \\
V \arrow[r, "\lfloor \omega \rfloor"] \arrow[d, "\pi = \mathsf{coker}\, x"'] & {}^*V \arrow[d, "{}^*x"] \\
V/Q \arrow[r, dashed, "\widetilde{\lfloor \omega \rfloor_Q}"'] & {}^*Q
\end{tikzcd} \tag{6.38}$$

∎

Combining Theorems Thm. 6.9.1 and Thm. 6.9.3, we find that:

Corollary 6.9.4 *The dashed arrow in Eq. (6.38) is an isomorphism, or in other words, we have an equality of quotients* $[V/Q = {}^*Q]^V$ *(i.e. an isomorphism in* $\textsc{Quot}_{\mathscr{C}}(V)$*) if and only if* $[Q]_V$ *is Lagrangian (in the generalized element sense), that is,* $[Q = Q^{\omega}_{\mathsf{gen}}]_V$*.*

In such a case, we call $[V/Q]^V$ the *Lagrangian quotient* corresponding to the Lagrangian subobject $[Q]_V$. For example, $\mathbb{T}^{2n}$ is the Lagrangian quotient corresponding to the Lagrangian subgroup $\mathbb{Z}^{2n}$ of the locally compact abelian group $\mathbb{R}^{2n}$. Notice that the inclusion $\mathbb{Z}^{2n} \to \mathbb{R}^{2n}$ does not have a left inverse.

Theorem 6.9.5 *Let* $\mathscr{V}$ *be a preabelian star-autonomous category with a nuclear symplectic form* ω *and let* $x : [Q]$ *be an isotropic direct summand such that* x *is strict. Then there are canonical strict monomorphisms* $y : [{}^*Q]$ *and* $\Phi_Q : [Q \oplus {}^*Q]$*. Furthermore, if* $[Q]$ *is Lagrangian and* Φ_Q *is strict, then* $\Phi_Q : [V = Q \oplus {}^*Q]$*.*

Furthermore, we conjecture that $\Phi_Q : Q \oplus Q^* \to V$ is symplectic, but we skip the proof due to a time constraint. The proof should be essentially the same as our coordinate-free proof in the concrete case, Thm. 2.4.5. We do not expect it to require the subobject axiom. Thus, we expect that in the case of a nuclear symplectic form, a Lagrangian subobject has a complement if and only if it has a Lagrangian complement. The *strictness* hypothesis is only used to prove that in the case of a Lagrangian subobject, Φ_Q is an isomorphism, not just a monic epic. Recall that in $\widetilde{\mathrm{LCA}}$, strict monomorphisms are the same as regular monomorphisms, and these are precisely *embeddings*.

Proof Since Q is a direcct summand, let ${}_!x$ be the dual of the projection $V \to Q$. Then

$$x : Q \to V \qquad\qquad {}^*x : {}^*V \to {}^*Q \qquad\qquad {}_!x : {}^*Q \to {}^*V$$

and the following diagram commutes.

$$\begin{tikzcd}
& Q \arrow[dl, "i=\langle \mathsf{id}_Q, 0_{Q,{}^*Q}\rangle"'] \arrow[dr, "x"] & & \\
Q \oplus {}^*Q \arrow[rr, "\Phi_Q = {[x, \lfloor\omega\rfloor^{-1}({}_!x)]}"'] \arrow[d, "\tau"'] & & V \arrow[r, "\lfloor\omega\rfloor"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\text{from Eq. (6.38)}"] & {}^*V \arrow[d, "{}^*x"] \\
{}^*Q \arrow[rr, dashed, "\phi"'] & & V/Q \arrow[r, "\psi = \widetilde{\lfloor\omega\rfloor_Q}"'] & {}^*Q
\end{tikzcd}$$

In particular, the triangle commutes by properties of the biproduct:

$$[x, \lfloor\omega\rfloor^{-1}({}_!x)]\langle \mathsf{id}_Q, 0_{Q,{}^*Q}\rangle = x\mathsf{id}_Q + \lfloor\omega\rfloor^{-1}({}_!x)0_{Q,{}^*Q} = x$$

The map ϕ is defined by universality of the cokernel τ since $\pi x = 0$. By uniqueness of the cokernel, $\psi\phi = \mathsf{id}_{{}^*Q}$. Since x is strict, so is ${}_!x$ and thus so is $y = \lfloor\omega\rfloor^{-1}({}_!x)$, and then $\Phi_Q = [x, y]$. Now, if $[Q]$ is Lagangian, then by Cor. 6.9.4, $\phi = \psi^{-1}$, and we obtain the following commutative diagram with exact columns:

$$\begin{tikzcd}
& 0 \arrow[d] & \\
& Q \arrow[dl] \arrow[dr] & \\
Q \oplus {}^*Q \arrow[rr, "\Phi_Q"] \arrow[d] & & V \arrow[d] \\
{}^*Q \arrow[rr, "\psi"] \arrow[dr] & & V/Q \arrow[dl] \\
& 0 &
\end{tikzcd}$$

Now Φ_Q is a strict monomorphism, and by Lem. G.0.8, is an epimorphism, hence an isomorphism. ∎

In Sec. 2.4.3, we saw that if S is a closed subset of a locally compact abelian group V with symplectic form ω, then S^ω is also closed in V. Our proof used limits and Hausdorffness, and S was not required to be a subgroup. We now give an entirely different proof by diagram chasing. In the case of locally compact abelian groups, we would require a subgroup Q rather than just a subset.

Theorem 6.9.6 (Topological closedness) *Let $[Q]$ be a subobject of an object V with a symplectic form. Then the following diagram commutes:*

$$\begin{tikzcd}
& Q \arrow[dl, "x"'] \arrow[dr, "{}^*(\widetilde{\lceil\omega\rceil_Q})\lfloor\mathsf{lefteval}^Q_\perp\rfloor"] & \\
V \arrow[dr, "{}^*\lceil\omega\rceil\lfloor\mathsf{lefteval}^V_\perp\rfloor"'] & & {}^*(V/Q) \arrow[dl, "{}^*\pi"] \\
& {}^*V &
\end{tikzcd}$$

Suppose $x : [Q]_V$ is a closed subgroup of a locally compact abelian group V. Note that ${}^*(\widetilde{\lceil\omega\rceil_Q})\lfloor\mathsf{lefteval}_\perp^Q\rfloor$ is an isomorphism. Closedness is equivalent to continuity of the inclusion map x. Then since ${}^*\lceil\omega\rceil\lfloor\mathsf{lefteval}_\perp^V\rfloor x$ is continuous, $[{}^*(V/Q)]_{{}^*V}$ is closed in ${}^*V$. Then using the isomorphism $Q_{\mathsf{gen}}^\omega \cong {}^*(V/Q)$ from Thm. 6.9.1, we see that $[Q_{\mathsf{gen}}^\omega]$ is a closed subgroup of V. Thus, Thm. 6.9.6 can be viewed as showing that if $[Q]$ is closed then so is $[Q_{\mathsf{gen}}^\omega]$.

Proof The following diagram commutes since all of its subdiagrams commute:

$$\begin{tikzcd}
 & & Q \arrow[lld, "x"'] \arrow[d, "\lfloor\mathsf{lefteval}_\perp^Q\rfloor"'] \arrow[rd] & \\
V \arrow[rd, "\lfloor\mathsf{lefteval}_\perp^V\rfloor"'] & \text{(A)} & {}^*(Q^*) \arrow[r, "{}^*(\widetilde{\lceil\omega\rceil_Q})"'] \arrow[ld, "{}^*(x^*)"] & {}^*(V/Q) \arrow[ld, "{}^*\pi"] \\
 & {}^*(V^*) \arrow[r, "{}^*\lceil\omega\rceil"'] & {}^*V & \text{(B)}
\end{tikzcd}$$

Subdiagram (A) commutes by naturality of $\lfloor\mathsf{lefteval}_\perp\rfloor$, and subdiagram (B) commutes because it is the right dual ${}^*\mathcal{D}$ of the "left" version $\mathcal{D}$ of the square subdiagram in Eq. (6.38).
$\blacksquare$

Chapter 7

Discussion

One topic we are excited to explore further is that of dimension doubling. Since the combination of multiqubit and multiququart Clifford operations is universal, we are interested to explore this case, as well as the case of allowing multiqu$d$it Clifford operations for varying $d = 2^t$. We expect that the Prüfer 2-group will play a key role in consolidating our understanding of this topic. Evaluating encoded projective Clifford operations at the standard qubit Pauli observables for different powers of 2 in the same circuit or program involves changing between operator bases, which can spawn an exponential number of nonzero coefficients. On the other hand, we have seen that there are some coincidental cases where there are fewer coefficients, and we are interested in exploring this connection with computational complexity. We are also eager to explore how such matters will factor into the design of a compiler if $\lambda^{\mathscr{P}_\mathrm{C}}$ is augmented to support various values of t in the same program.

We suspect there may be a connection between catalytic embedding for qubits and the dimension doubling phenomenon we have noted with the condensed and extended encodings. At a glance, the two phenomena have a lot in common. Both involve doubling of the dimension, and cyclotomic extensions. The evaluation formula relating condensed and extended encodings also has some similarities with the catalytic embedding property.

We have many questions to explore about the category theory work presented in the thesis. For one thing, we are interested to find more models (categories) that fit into the framework, and to classify them. We are also curious whether the Stone von-Neumann Theorem admits a generalization, whereby an object V with a symplectic form in a preabelian star-autonomous category with limits and colimits is represented on an object $\mathcal{H}$ in a dagger compact category. We would also like to better understand the separation of de Morgan duality and nuclearity in the non-associative case.

References

[ABP98] S. Abramsky, R. Blute, and P. Panangaden. *Nuclear and Trace Ideals in Tensored *-Categories*. June 1998. arXiv: math/9805102.

[Abr09] Samson Abramsky. "No-Cloning in Categorical Quantum Mechanics". In: *Semantic Techniques in Quantum Computation*. Ed. by Ian Mackie and Simon Gay. Cambridge: Cambridge University Press, 2009, pp. 1–28. ISBN: 978-0-521-51374-6. DOI: 10.1017/CBO9781139193313.002.

[AC07] Samson Abramsky and Bob Coecke. *A Categorical Semantics of Quantum Protocols*. Mar. 2007. DOI: 10.48550/arXiv.quant-ph/0402130. arXiv: quant-ph/0402130.

[AD17] Pablo Arrighi and Gilles Dowek. "Lineal: A linear-algebraic lambda-calculus". In: *Logical Methods in Computer Science* 13 (2017).

[AG04] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". In: *Physical Review A—Atomic, Molecular, and Optical Physics* 70.5 (2004), p. 052328. DOI: 10.1103/physreva.70.052328.

[Amy+23] M. Amy et al. *Catalytic Embeddings of Quantum Circuits*. May 2023. DOI: 10.48550/arXiv.2305.07720. arXiv: 2305.07720 [quant-ph].

[Amy19] Matthew Amy. "Towards Large-scale Functional Verification of Universal Quantum Circuits". In: *Electronic Proceedings in Theoretical Computer Science* 287 (Jan. 2019), pp. 1–21. ISSN: 2075-2180. DOI: 10.4204/eptcs.287.1.

[App+17] Marcus Appleby et al. "SICs and Algebraic Number Theory". In: *Foundations of Physics* 47.8 (Aug. 2017), pp. 1042–1059. ISSN: 0015-9018, 1572-9516. DOI: 10.1007/s10701-017-0090-7. arXiv: 1701.05200 [quant-ph].

[App05] D. M. Appleby. "SIC-POVMs and the Extended Clifford Group". In: *Journal of Mathematical Physics* 46.5 (May 2005), p. 052107. ISSN: 0022-2488, 1089-7658. DOI: 10.1063/1.1896384. arXiv: quant-ph/0412001.

[Bar09] Michael Barr. "On Duality of Topological Abelian Groups". Unpublished. Available at https://www.math.mcgill.ca/barr/papers/abgp.pdf. 2009.

[Bar79] Michael Barr. **-Autonomous Categories*. Vol. 752. Lecture Notes in Mathematics. Berlin, Heidelberg: Springer Berlin Heidelberg, 1979. ISBN: 978-3-540-09563-7 978-3-540-34850-4. DOI: 10.1007/BFb0064579.

[Bar91] Michael Barr. "*-Autonomous Categories and Linear Logic". In: *Mathematical Structures in Computer Science* 1.2 (July 1991), pp. 159–178. ISSN: 0960-1295, 1469-8072. DOI: 10.1017/S0960129500001274.

[Bar95] Michael Barr. "Nonsymmetric $*$-Autonomous Categories". In: *Theoretical Computer Science* 139.1-2 (Mar. 1995), pp. 115–130. ISSN: 03043975. DOI: 10.1016/0304-3975(94)00089-2.

[BD97] John C. Baez and James Dolan. *Higher-Dimensional Algebra III: N-Categories and the Algebra of Opetopes*. Feb. 1997. DOI: 10.48550/arXiv.q-alg/9702014. arXiv: q-alg/9702014.

[BK01] Michael Barr and Heinrich Kleisli. "On Mackey Topologies in Topological Abelian Groups". In: *Theory and Applications of Categories* 8.4 (2001).

[BPV21] Agustín Borgna, Simon Perdrix, and Benoît Valiron. "Hybrid quantum-classical circuit simplification with the ZX-calculus". In: *Programming Languages and Systems: 19th Asian Symposium, APLAS 2021, Chicago, IL, USA, October 17–18, 2021, Proceedings 19*. Springer. 2021, pp. 121–139.

[Buc55] D. A. Buchsbaum. "Exact Categories and Duality". In: *Transactions of the American Mathematical Society* 80.1 (1955), pp. 1–34. ISSN: 0002-9947, 1088-6850. DOI: 10.1090/S0002-9947-1955-0074407-6.

[CD11] Bob Coecke and Ross Duncan. "Interacting Quantum Observables: Categorical Algebra and Diagrammatics". In: *New Journal of Physics* 13.4 (Apr. 2011), p. 043016. ISSN: 1367-2630. DOI: 10.1088/1367-2630/13/4/043016.

[Cd24] Imin Chen and Nadish de Silva. *Characterising Semi-Clifford Gates Using Algebraic Sets*. May 2024. DOI: 10.48550/arXiv.2309.15184. arXiv: 2309.15184 [math-ph, physics:quant-ph].

[CKS00] J. R. B. Cockett, J. Koslowski, and R. A. G. Seely. "Introduction to Linear Bicategories". In: *Mathematical Structures in Computer Science* 10.2 (Apr. 2000). ISSN: 0960-1295, 1469-8072. DOI: 10.1017/S0960129520003047.

[Coh66] P.M. Cohn. “Some Remarks on the Invariant Basis Property”. In: *Topology* 5.3 (Sept. 1966), pp. 215–228. ISSN: 00409383. DOI: 10.1016/0040-9383(66)90006-1.

[Con07] John B. Conway. *A Course in Functional Analysis*. Vol. 96. Graduate Texts in Mathematics. New York, NY: Springer, 2007. ISBN: 978-1-4419-3092-7 978-1-4757-4383-8. DOI: 10.1007/978-1-4757-4383-8.

[Con86] John Horton Conway. *Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups*. Oxford Oxfordshire : New York: Oxford University Press, Jan. 1986. ISBN: 978-0-19-853199-9.

[CS97a] J. R. B. Cockett and R. A. G. Seely. “Weakly Distributive Categories”. In: *Journal of Pure and Applied Algebra* 114.2 (Jan. 1997), pp. 133–173. ISSN: 0022-4049. DOI: 10.1016/0022-4049(95)00160-3.

[CS97b] J. R. B. Cockett and R. a. G. Seely. “Proof Theory for Full Intuitionistic Linear Logic, Bilinear Logic, and MIX Categories.” In: *Theory and Applications of Categories [electronic only]* 3 (1997), pp. 85–131. ISSN: 1201-561X.

[CS99] J.R.B. Cockett and R.A.G. Seely. “Linearly Distributive Functors”. In: *Journal of Pure and Applied Algebra* 143.1-3 (Nov. 1999), pp. 155–203. ISSN: 00224049. DOI: 10.1016/S0022-4049(98)00110-8.

[da 08] Ana Cannas da Silva. *Lectures on Symplectic Geometry*. Vol. 1764. Lecture Notes in Mathematics. Berlin, Heidelberg: Springer, 2008. ISBN: 978-3-540-42195-5 978-3-540-45330-7. DOI: 10.1007/978-3-540-45330-7.

[DD24] Alejandro Díaz-Caro and Gilles Dowek. “A Linear Linear Lambda-Calculus”. In: *Mathematical Structures in Computer Science* (May 2024), pp. 1–35. ISSN: 0960-1295, 1469-8072. DOI: 10.1017/S0960129524000197. arXiv: 2201.11221 [cs].

[DV19] Lawrence Dunn and Jamie Vicary. *Coherence for Frobenius Pseudomonoids and the Geometry of Linear Proofs*. July 2019. DOI: 10.23638/LMCS-15(3:5)2019. arXiv: 1601.05372 [cs].

[GH12] Shamgar Gurevich and Ronny Hadani. “The Weil Representation in Characteristic Two”. In: *Advances in Mathematics* 230.3 (June 2012), pp. 894–926. ISSN: 0001-8708. DOI: 10.1016/j.aim.2012.03.008.

[Gir87] Jean-Yves Girard. “Linear Logic”. In: *Theoretical Computer Science* 50.1 (Jan. 1987), pp. 1–101. ISSN: 0304-3975. DOI: 10.1016/0304-3975(87)90045-4.

[Gla+24] Andrew N. Glaudell et al. “Exact Synthesis of Multiqutrit Clifford-Cyclotomic Circuits”. In: *Electronic Proceedings in Theoretical Computer Science* 406 (Aug. 2024), pp. 44–62. ISSN: 2075-2180. DOI: 10.4204/EPTCS.406.2. arXiv: 2405.08136 [quant-ph].

[GNW21] David Gross, Sepehr Nezami, and Michael Walter. “Schur-Weyl Duality for the Clifford Group with Applications: Property Testing, a Robust Hudson Theorem, and de Finetti Representations”. In: *Communications in Mathematical Physics* 385.3 (Aug. 2021), pp. 1325–1393. ISSN: 0010-3616, 1432-0916. DOI: 10.1007/s00220-021-04118-7. arXiv: 1712.08628 [math-ph, physics:quant-ph].

[Gra18] Marco Grandis. *Category Theory and Applications: a Textbook for Beginners: A TEXTBOOK FOR BEGINNERS*. Singapore: World Scientific Publishing Co Pte Ltd, Mar. 2018. ISBN: 978-981-323-106-1.

[Gro06] D. Gross. “Hudson’s Theorem for Finite-Dimensional Quantum Systems”. In: *Journal of Mathematical Physics* 47.12 (Dec. 2006), p. 122107. ISSN: 0022-2488. DOI: 10.1063/1.2393152.

[Gro57] Alexander Grothendieck. “Sur Quelques Points d’algèbre Homologique, I”. In: *Tohoku Mathematical Journal* 9.2 (Jan. 1957), pp. 119–221. ISSN: 0040-8735, 2186-585X. DOI: 10.2748/tmj/1178244839.

[GS13] Brett Giles and Peter Selinger. “Exact Synthesis of Multiqubit Clifford+T Circuits”. In: *Physical Review A* 87.3 (Mar. 2013), p. 032332. DOI: 10.1103/PhysRevA.87.032332.

[HDM05] Erik Hostens, Jeroen Dehaene, and Bart De Moor. “Stabilizer States and Clifford Operations for Systems of Arbitrary Dimensions, and Modular Arithmetic”. In: *Physical Review A* 71.4 (Apr. 2005), p. 042315. ISSN: 1050-2947, 1094-1622. DOI: 10.1103/PhysRevA.71.042315. arXiv: quant-ph/0408190.

[HR89] D.A. Higgs and K.A. Rowe. “Nuclearity in the Category of Complete Semilattices”. In: *Journal of Pure and Applied Algebra* 57.1 (Feb. 1989), pp. 67–78. ISSN: 00224049. DOI: 10.1016/0022-4049(89)90028-5.

[Jac16] Bart Jacobs. *Introduction to Coalgebra: Towards Mathematics of States and Observation*. Cambridge Tracts in Theoretical Computer Science. Cambridge: Cambridge University Press, 2016. ISBN: 978-1-107-17789-5. DOI: 10.1017/CBO9781316823187.

[Joh02] Peter T. Johnstone. *Sketches of an Elephant: A Topos Theory Compendium*. Oxford Logic Guides. Oxford, New York: Oxford University Press, Nov. 2002. ISBN: 978-0-19-853425-9.

[Joy81] André Joyal. "Une Théorie Combinatoire Des Séries Formelles". In: *Advances in Mathematics* 42.1 (Oct. 1981), pp. 1–82. ISSN: 0001-8708. DOI: 10.1016/0001-8708(81)90052-9.

[Kal+24] Amolak Ratan Kalra et al. *Multi-Qutrit Exact Synthesis*. May 2024. DOI: 10.48550/arXiv.2405.08147. arXiv: 2405.08147 [quant-ph].

[Kel69] G. M. Kelly. "Monomorphisms, Epimorphisms, and Pull-Backs". In: *Journal of the Australian Mathematical Society* 9.1-2 (Feb. 1969), pp. 124–142. ISSN: 1446-7887, 1446-8107. DOI: 10.1017/S1446788700005693.

[Kel74] G. M. Kelly. "Doctrinal Adjunction". In: *Category Seminar*. Ed. by Gregory M. Kelly. Berlin, Heidelberg: Springer, 1974, pp. 257–280. ISBN: 978-3-540-37270-7. DOI: 10.1007/BFb0063105.

[Kli+15] Vadym Kliuchnikov et al. *A Framework for Approximating Qubit Unitaries*. Oct. 2015. DOI: 10.48550/arXiv.1510.03888. arXiv: 1510.03888 [quant-ph].

[KM71] G. M. Kelly and S. Maclane. "Coherence in Closed Categories". In: *Journal of Pure and Applied Algebra* 1.1 (Jan. 1971), pp. 97–140. ISSN: 0022-4049. DOI: 10.1016/0022-4049(71)90013-2.

[KMM13] Vadym Kliuchnikov, Dmitri Maslov, and Michele Mosca. *Fast and Efficient Exact Synthesis of Single Qubit Unitaries Generated by Clifford and T Gates*. Feb. 2013. DOI: 10.48550/arXiv.1206.5236. arXiv: 1206.5236 [quant-ph].

[Kna07] Anthony W. Knapp. *Basic Algebra*. Springer Science & Business Media, July 2007. ISBN: 978-0-8176-4529-8.

[Knu64] Donald E. Knuth. "Backus Normal Form vs. Backus Naur Form". In: *Commun. ACM* 7.12 (Dec. 1964), pp. 735–736. ISSN: 0001-0782. DOI: 10.1145/355588.365140.

[Kop11] Yaroslav Kopylov. *The Two-Square Lemma and the Connecting Morphism*. Mar. 2011. DOI: 10.48550/arXiv.1103.5251. arXiv: 1103.5251 [math].

[KVM24] Amolak Ratan Kalra, Dinesh Valluri, and Michele Mosca. *Synthesis and Arithmetic of Single Qutrit Circuits*. Jan. 2024. DOI: 10.48550/arXiv.2311.08696. arXiv: 2311.08696 [quant-ph].

[KW20] AR Kissinger and JMM van de Wetering. "PyZX: Large Scale Automated Diagrammatic Reasoning". In: *Electronic Proceedings in Theoretical Computer Science* 318 (2020), pp. 229–241.

[KY15] Vadym Kliuchnikov and Jon Yard. *A Framework for Exact Synthesis*. Apr. 2015. DOI: 10.48550/arXiv.1504.04350. arXiv: 1504.04350 [quant-ph].

[Lam58] Joachim Lambek. "The Mathematics of Sentence Structure". In: *The American Mathematical Monthly* 65.3 (Mar. 1958), pp. 154–170. ISSN: 0002-9890. DOI: 10.1080/00029890.1958.11989160.

[Li+22] Gushu Li et al. "Paulihedral: A Generalized Block-Wise Compiler Optimization Framework for Quantum Simulation Kernels". In: *Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*. ASPLOS '22. Lausanne, Switzerland: Association for Computing Machinery, 2022, pp. 554–569. ISBN: 9781450392051. DOI: 10.1145/3503222.3507715.

[Mac78] Saunders Mac Lane. *Categories for the Working Mathematician*. Vol. 5. Graduate Texts in Mathematics. New York, NY: Springer, 1978. ISBN: 978-1-4419-3123-8 978-1-4757-4721-8. DOI: 10.1007/978-1-4757-4721-8.

[Mas23] Kieran Mastel. *The Clifford Theory of the n-Qubit Clifford Group*. July 2023. DOI: 10.48550/arXiv.2307.05810. arXiv: 2307.05810 [math-ph, physics:quant-ph].

[MM94] Saunders Mac Lane and Ieke Moerdijk. *Sheaves in Geometry and Logic: A First Introduction to Topos Theory*. Universitext. New York, NY: Springer, 1994. ISBN: 978-0-387-97710-2 978-1-4612-0927-0. DOI: 10.1007/978-1-4612-0927-0.

[MS82] John L. MacDonald and Arthur Stone. "The Tower and Regular Decomposition". In: *Cahiers de topologie et géométrie différentielle* 23.2 (1982), pp. 197–213. ISSN: 2681-2398.

[Mum06] David Mumford. *Tata Lectures on Theta III*. Boston: Birkhäuser Boston, Jan. 2006. ISBN: 978-0-8176-4570-0.

[NRS00] Gabriele Nebe, E. M. Rains, and N. J. A. Sloane. *The Invariants of the Clifford Groups*. Oct. 2000. DOI: 10.48550/arXiv.math/0001038. arXiv: math/0001038.

[NS64] M. Newman and J. Smart. "Symplectic Modulary Groups". In: *Acta Arithmetica* 9.1 (1964), pp. 83–89. ISSN: 0065-1036.

[Pay+23a] Jennifer Paykin et al. *PCOAST: A Pauli-based Quantum Circuit Optimization Framework*. May 2023. DOI: 10.48550/arXiv.2305.10966. arXiv: 2305.10966 [quant-ph].

[Pay+23b] Jennifer Paykin et al. *PCOAST: A Pauli-based Quantum Circuit Optimization Framework (extended Version)*. arXiv:2305.10966v2. 2023.

[Pay18] Jennifer Paykin. "Linear/non-linear types for embedded domain-specific languages". PhD thesis. University of Pennsyvlania, 2018.

[Pon34] L. Pontrjagin. "The Theory of Topological Commutative Groups". In: *Annals of Mathematics* 35.2 (1934), pp. 361–388. ISSN: 0003-486X. DOI: 10.2307/1968438. JSTOR: 1968438.

[PRZ17] Jennifer Paykin, Robert Rand, and Steve Zdancewic. "QWIRE: a core language for quantum circuits". In: *ACM SIGPLAN Notices* 52.1 (2017), pp. 846–858.

[PS18] Ori Parzanchevski and Peter Sarnak. "Super-Golden-Gates for PU(2)". In: *Advances in Mathematics* 327 (Mar. 2018), pp. 869–901. ISSN: 00018708. DOI: 10.1016/j.aim.2017.06.022. arXiv: 1704.02106 [math].

[PW24] Jennifer Paykin and Sam Winnick. *Qudit Quantum Programming with Projective Cliffords*. July 2024. DOI: 10.48550/arXiv.2407.16801. arXiv: 2407.16801 [quant-ph].

[Rie16] Emily Riehl. *Category Theory in Context*. Mineola, New York: Dover Publications, Nov. 2016. ISBN: 978-0-486-80903-8.

[Row88] K. A. Rowe. "Nuclearity". In: *Canadian Mathematical Bulletin* 31.2 (June 1988), pp. 227–235. ISSN: 0008-4395, 1496-4287. DOI: 10.4153/CMB-1988-035-5.

[Rud91] Walter Rudin. *Functional Analysis*. 2nd edition. New York: McGraw-Hill Science/Engineering/Math, Jan. 1991. ISBN: 978-0-07-054236-5.

[SBW23] Sarah Schneider, Lukas Burgholzer, and Robert Wille. "A SAT encoding for optimal Clifford circuit synthesis". In: *Proceedings of the 28th Asia and South Pacific Design Automation Conference*. 2023, pp. 190–195.

[Sch+24] Albert T Schmitz et al. "Graph optimization perspective for low-depth Trotter-Suzuki decomposition". In: *Physical Review A* 109.4 (2024), p. 042418.

[Sel12] Peter Selinger. "Finite Dimensional Hilbert Spaces Are Complete for Dagger Compact Closed Categories". In: *Logical Methods in Computer Science* Volume 8, Issue 3 (Aug. 2012), p. 1086. ISSN: 1860-5974. DOI: 10.2168/LMCS-8(3:6)2012. arXiv: 1207.6972 [quant-ph].

[Sha94] R. Shankar. *Principles of Quantum Mechanics, 2nd Edition*. 2nd edition. New York, NY: Plenum Press, Aug. 1994. ISBN: 978-0-306-44790-7.

[Shu11] Michael Shulman. *Comparing Composites of Left and Right Derived Functors*. Feb. 2011. arXiv: 0706.2868 [math].

[Sol97] S. Soloviev. "Proof of a Conjecture of S. Mac Lane". In: *Annals of Pure and Applied Logic* 90.1 (Dec. 1997), pp. 101–162. ISSN: 0168-0072. DOI: 10.1016/S0168-0072(97)00034-1.

[Stacks] The Stacks Project Authors. *Stacks Project*. https://stacks.math.columbia.edu. 2018.

[van22] Remy van Dobben de Bruyn. *Locally Compact Abelian Groups*. Unpublished notes for the Intercity Geometry Seminar on Condensed Mathematics. 2022.

[Wat18] John Watrous. *The Theory of Quantum Information*. 1st edition. Cambridge: Cambridge University Press, Apr. 2018. ISBN: 978-1-107-18056-7.

[WP24] Sam Winnick and Jennifer Paykin. *Condensed Encodings of Projective Clifford Operations in Arbitrary Dimension*. July 2024. DOI: 10.48550/arXiv.2407.16861. arXiv: 2407.16861 [quant-ph].

[WPR23] Xin-Chuan Wu, Shavindra Premaratne, and Kevin Rasch. "Introduction to Hybrid Quantum-Classical Programming Using C++ Quantum Extension". In: *2023 IEEE/ACM International Conference on Computer Aided Design (ICCAD)*. 2023, pp. 1–6. DOI: 10.1109/ICCAD57390.2023.10323946.

[YW22] Lia Yeh and John van de Wetering. "Constructing All Qutrit Controlled Clifford+T Gates in Clifford+T". In: vol. 13354. 2022, pp. 28–50. DOI: 10.1007/978-3-031-09005-9_3. arXiv: 2204.00552 [quant-ph].

APPENDICES

Appendix A

Relations in Set and Grp

A *relation* (of sets) is a triple (X, Y, γ) where X and Y are sets and $\gamma \subseteq X \times Y$ is called the *graph* of the relation. In other accounts, relations are sometimes defined as just the graph, but an identifiable *domain* X and *codomain* Y are required in order for relations to comprise (the morphisms of) a category $\textsc{Rel}$. As usual, we write $\gamma : X \to Y$ for (X, Y, γ).

A relation $\gamma : X \to Y$ is *left total* if for all $x \in X$ there exists $y \in Y$ such that $(x, y) \in \gamma$, and *right definite* if $(x, y_1), (x, y_2) \in \gamma$ implies $y_1 = y_2$. A *function* is a left total right definite relation. Right totality and left definiteness are defined dually. A function is *injective* if it is left definite and *surjective* if it is right total.

Relations can be defined internally to any category.For now, we do not need this generality, so we just give a concrete description of relations in the category of groups.

A *relation of groups* or *homomorphic relation* is a triple (X, Y, γ) where X and Y are groups and $\gamma \leq X \times Y$ is a subgroup. Left and right totality and definiteness are defined exactly as before. This time, a group homomorphism is precisely a left total right definite relation of groups. A homomorphism is injective if it is left definite and surjective if it is right definite.

One easily verifies that a homomorphic relation $\gamma : X \to Y$ is left definite if and only if the subgroup $\mathsf{ker}\,\gamma = \{x \in X \mid (x, 1) \in \gamma\} \leq X$ is trivial, as is the case with homomorphisms.

Appendix B

Bicategories and globe diagrams

Just as categories have objects and morphisms, a *bicategory* has objects, 1-morphisms, and 2-morphisms. These are also called 0-cells, 1-cells, and 2-cells, respectively. The 1-morphisms map between objects, and the 2-morphisms map between 1-morphisms:

$$\begin{tikzcd} A \arrow[r, bend left=50, "f"{name=U}] \arrow[r, bend right=50, "g"'{name=D}] & B \arrow[Rightarrow, from=U, to=D, "\eta"] \end{tikzcd} \tag{B.1}$$

First we note some foundational intuition: the definition of *category* involves (large) sets and functions, and so in retrospect, it is built from the categorical structure of S_{ET}. Likewise, the definition of *bicategory* involves (large) categories, functors, and natural transformations. These are actually just the objects, 1-morphisms, and 2-morphisms, respectively, of the strict bicategory C_{AT}.[1] This is an example of *categorification*. As it turns out, it is possible to guess what the definition of *bicategory* "should" be, following a few basic principles:

1. The *types* (domain and codomain) of morphisms and such guide the definitions. For example, one can compose $g : Y \to Z$ and $f : X \to Y$ thereby obtaining $g \,\square\, f : X \to Z$.

2. Abide by the *principle of equivalence*. For example, since adjointness is only defined up to natural isomorphism, if $L \dashv R$ and $L' \cong L$, then it should also be the case

[1] *Products* are also involved in these definitions. We give a little more detail in Appx. E.

that $L' \dashv R$, otherwise *adjointness* would be considered "evil". When reasoning abstractly about categories, we should never have strict equality of objects (except in definitions or meta-structure, e.g. the domain of a morphism $f : X \to Y$ is strictly equal to X). Likewise, with bicategories, we forbid strict equality of 1-morphisms.

3. Ensure some level of *coherence*. For example, one should impose enough constraints that different natural transformations $F \Rightarrow G$ formed from the canonical structure are equal. This rule is sometimes broken in related settings, for instance, with braided monoidal categories, which have less coherence than symmetric monoidal categories.

The defining data of a *bicategory* is given in Fig. B.1. The data is required to satisfy a slew of axioms, which can be guessed using the principles above. It is easier to figure them out with the aid of a graphical calculus. Two well-established graphical calculi for bicategories are *string diagrams* and *globe diagrams*. We give an informal overview of the latter.An *atomic globe diagram* in (the globe diagram language of) a bicategory $\mathbf{C}$, as in Eq. (B.1), consists of the following data from $\mathbf{C}$:

$$A, B \in \mathsf{Ob}(\mathbf{C}) \qquad\qquad f, g : A \to B \qquad\qquad \eta : f \Rightarrow g : A \to B$$

Obviously f and g have to have the same type $A \to B$ in order for this to make sense. In fact, 2-morphisms include the data of their domain and codomain, as do 1-morphisms, so the atomic globe diagram Eq. (B.1) actually *corresponds* to the 2-morphism η. Compatible globe diagrams can be concatenated, either vertically or horizontally. The following inductive definition on subdiagrams defines *equivalence* of globe diagrams:

$$\begin{tikzcd} A \arrow[r, bend left=60, "f"{name=F}] \arrow[r, "g"{name=G, description}] \arrow[r, bend right=60, "h"'{name=H}] & B \arrow[Rightarrow, from=F, to=G, "\eta_2"] \arrow[Rightarrow, from=G, to=H, "\eta_1"] \end{tikzcd} \quad \sim \quad \begin{tikzcd} A \arrow[r, bend left, "f"{name=F}] \arrow[r, bend right, "h"'{name=H}] & B \arrow[Rightarrow, from=F, to=H, "\eta_1 \circ \eta_2"] \end{tikzcd} \tag{B.2}$$

$$\begin{tikzcd} A \arrow[r, bend left, "f_2"{name=F2}] \arrow[r, bend right, "g_2"'{name=G2}] & B \arrow[r, bend left, "f_1"{name=F1}] \arrow[r, bend right, "g_1"'{name=G1}] & C \arrow[Rightarrow, from=F2, to=G2, "\beta"] \arrow[Rightarrow, from=F1, to=G1, "\alpha"] \end{tikzcd} \quad \sim \quad \begin{tikzcd} A \arrow[r, bend left, "f_1 \square f_2"{name=F}] \arrow[r, bend right, "g_1 \square g_2"'{name=G}] & C \arrow[Rightarrow, from=F, to=G, "\alpha \square \beta"] \end{tikzcd} \tag{B.3}$$

Figure B.1: Data defing a bicategory $\mathbf{C}$

$\mathsf{Ob}(\mathbf{C})$	a "set" of objects. For objects we use notations like A, B, X, Y, etc.
$1\text{-}\mathsf{Mor}(\mathbf{C})$	a "set" of 1-morphisms, which go from one object to another. For 1-morphisms we use notations like $f : A \to B$, etc.
$2\text{-}\mathsf{Mor}(\mathbf{C})$	a "set" of 2-morphisms, which go from one 1-morphism to another of the same type. For 2-morphisms, we use notations like $\alpha : f \Rightarrow g : A \to B$, etc.
$\mathsf{Hom}_{\mathbf{C}}(A, B)$	a *Hom category* for all objects A and B, whose objects are 1-morphisms and morphisms are 2-morphisms. For *2-identities*, we write $\mathsf{Id}_f : f \Rightarrow f$, and for composition (called *vertical composition*) we write $\alpha \circ \beta$.
$\mathsf{id}_A : A \to A$	for all objects A a distinguished 1-morphism called the *1-identity*
$\square_{A,B,C} : \mathsf{Hom}_{\mathbf{C}}(B, C) \times \mathsf{Hom}_{\mathbf{C}}(A, B) \to \mathsf{Hom}_{\mathbf{C}}(A, C)$,	a (covariant) functor for all objects A, B, C called *horizontal composition*. We write $\square$ in place of $\square_{A,B,C}$.
$\mathsf{leftunitor}(A, B)$	*left unitor*[2], a natural isomorphism $\lambda(A, B) \overset{\sim}{\Rightarrow} \mathsf{Id}_{\mathsf{Hom}_{\mathbf{C}}(A,B)}$, where $\lambda(A, B)$ is the endofunctor $f \mapsto \mathsf{id}_B \square f$ and $\theta \mapsto \mathsf{Id}_{\mathsf{id}_B} \square \theta$ on $\mathsf{Hom}_{\mathbf{C}}(A, B)$.
$\mathsf{rightunitor}(A, B)$	*right unitor*, a natural isomorphism $\rho(A, B) \overset{\sim}{\Rightarrow} \mathsf{Id}_{\mathsf{Hom}_{\mathbf{C}}(A,B)}$, where $\rho(A, B)$ is the endofunctor $f \mapsto f \square \mathsf{id}_A$ and $\theta \mapsto \theta \square \mathsf{Id}_{\mathsf{id}_A}$ on $\mathsf{Hom}_{\mathbf{C}}(A, B)$.
$\alpha(A, B, C, D) : (- \square -) \square - \overset{\sim}{\Rightarrow} - \square (- \square -)$,	natural transformations for all A, B, C, D, called *associators*, of the two association functors of the following type: $\mathsf{Hom}_{\mathbf{C}}(C, D) \times \mathsf{Hom}_{\mathbf{C}}(B, C) \times \mathsf{Hom}_{\mathbf{C}}(A, B) \to \mathsf{Hom}_{\mathbf{C}}(A, D)$ It is common practice to abbreviate $\alpha(A, B, C, D)$ by α.

Remarks (i) We are ignoring size issues; these are easy, yet tedious, to address. This is why we write *"set"* in quotation marks. (ii) Expressions like $\mathsf{Id}_{\mathsf{id}_B} \square \theta$ are often written as $\mathsf{id}_B \square \theta$ or even $B \square \theta$. This is an example of *whiskering* in the ambient bicategory CAT. Whiskering is introduced below (see Eq. (B.8)).

The following diagram can be collapsed in two ways to produce an atomic diagram:

$$
\begin{tikzcd}
A \arrow[r, bend left=60, "f_2"] \arrow[r, "g_2" description] \arrow[r, bend right=60, "h_2"'] \arrow[r, phantom, shift left=3ex, "\Downarrow\beta_2"] \arrow[r, phantom, shift right=3ex, "\Downarrow\beta_1"] & B \arrow[r, bend left=60, "f_1"] \arrow[r, "g_1" description] \arrow[r, bend right=60, "h_1"'] \arrow[r, phantom, shift left=3ex, "\Downarrow\alpha_2"] \arrow[r, phantom, shift right=3ex, "\Downarrow\alpha_1"] & C
\end{tikzcd}
\quad\sim\quad
\begin{tikzcd}
A \arrow[rr, bend left=40, "f_1\square f_2"] \arrow[rr, bend right=40, "g_1\square g_2"'] \arrow[rr, phantom, "\Downarrow(\alpha_1\circ\alpha_2)\square(\beta_1\circ\beta_2)=(\alpha_1\square\beta_1)\circ(\alpha_2\square\beta_2)"] & & C
\end{tikzcd}
\tag{B.4}
$$

We would like these to be the same, so we impose the *exchange property*:

i. $\mathsf{Id}_{f_1}\square\mathsf{Id}_{f_2}=\mathsf{Id}_{f_1\square f_2}$ for all $A\xrightarrow{f_2}B\xrightarrow{f_1}C$, and

ii. $(\alpha_1\square\alpha_2)\circ(\beta_1\square\beta_2)=(\alpha_1\circ\beta_1)\square(\alpha_2\circ\beta_2)$ for all $A\overset{f_2,g_2,h_2}{\rightarrow}B\overset{f_1,g_1,h_1}{\rightarrow}C$ etc.

Similarly, there are associative laws for Eq. (B.2) and Eq. (B.3). In order to abide by the principle of equivalence, the horizontal associativity must only hold *up to coherent isomorphism*. That is, up to natural isomorphism provided by the associators:

$$
\begin{tikzcd}
 & (f_1\square f_2)\square f_3 \arrow[d, Rightarrow, "(\alpha\square\beta)\square\gamma"] \arrow[rrr, Rightarrow, "\alpha(A,B,C,D)_{f_1,f_2,f_3}"] & & & f_1\square(f_2\square f_3) \arrow[d, Rightarrow, "\alpha\square(\beta\square\gamma)"] & \\
A \arrow[ur, no head] \arrow[dr, no head] & {} & D \arrow[r, phantom, "\sim"] & A \arrow[ur, no head] \arrow[dr, no head] & {} & D \\
 & (g_1\square g_2)\square g_3 \arrow[rrr, Rightarrow, "\alpha(A,B,C,D)_{g_1,g_2,g_3}"] & & & g_1\square(g_2\square g_3) &
\end{tikzcd}
\tag{B.5}
$$

Therefore the following diagram must be interpreted as one of the two associations $\alpha\square(\beta\square\gamma)$ or $(\alpha\square\beta)\square\gamma$, depending on the situation, but not both:

$$
\begin{tikzcd}
A \arrow[r, bend left=50, "f_3"] \arrow[r, bend right=50, "g_3"'] \arrow[r, phantom, "\Downarrow\gamma"] & B \arrow[r, bend left=50, "f_2"] \arrow[r, bend right=50, "g_2"'] \arrow[r, phantom, "\Downarrow\beta"] & C \arrow[r, bend left=50, "f_1"] \arrow[r, bend right=50, "g_1"'] \arrow[r, phantom, "\Downarrow\alpha"] & D
\end{tikzcd}
\tag{B.6}
$$

Intuitively, the diagrammatic calculus is only sound *up to coherence*. Because of this subtlety, it is incorrect to identify 2-morphisms in $\mathbf{C}$ with equivalence classes of globe diagrams. It is an entirely different matter that every bicategory is equivalent to a strict bicategory, for which the identification is legal.

It turns out that the requirements imposed so far are not enough for the coherence theorem for bicategories to hold. In particlar, imposing Eq. (B.5) does not imply that expressions like $f_1 \otimes \cdots \otimes f_n$ are unambiguous up to coherent isomorphism when $n > 3$, contrary to what one might expect from working with groups or monoids. However, this issue is resolved by imposing the following *coherence condition*: for all $A \xrightarrow{h} B \xrightarrow{g} C \xrightarrow{f} D \xrightarrow{e} E$, the following diagram commutes:

$$\begin{tikzcd}
 & (e \square f) \square (g \square h) \arrow[dr, Rightarrow, "\alpha(A,C,D,E)_{e,f,g \square h}"] & \\
((e \square f) \square g) \square h \arrow[ur, Rightarrow, "\alpha(A,B,C,E)_{e \square f,g,h}"] \arrow[d, Rightarrow, "\alpha(B,C,D,E)_{e,f,g} \square h"'] & & e \square (f \square (g \square h)) \\
(e \square (f \square g)) \square h \arrow[rr, Rightarrow, "\alpha(A,B,D,E)_{e,f \square g,h}"'] & & e \square ((f \square g) \square h) \arrow[u, Rightarrow, "e \square \alpha(A,B,C,D)_{f,g,h}"']
\end{tikzcd} \tag{B.7}$$

In Eq. (B.7), we wrote $\alpha(B,C,D,E)_{e,f,g} \square h$ in place of $\alpha(B,C,D,E)_{e,f,g} \square \mathsf{Id}_h$. This is called *whiskering*. This shorthand is also used in globe diagrams as follows:

$$\begin{tikzcd}
A \arrow[r, bend left, "f"] \arrow[r, bend right, "g"'] \arrow[r, phantom, "\Downarrow\beta"] & B \arrow[r, "h"] & C
\end{tikzcd} \quad \sim \quad \begin{tikzcd}
A \arrow[r, bend left, "f"] \arrow[r, bend right, "g"'] \arrow[r, phantom, "\Downarrow\beta"] & B \arrow[r, bend left, "h"] \arrow[r, bend right, "h"'] \arrow[r, phantom, "\Downarrow\mathsf{Id}_h"] & C
\end{tikzcd} \tag{B.8}$$

$$\begin{tikzcd}
A \arrow[r, "h"] & B \arrow[r, bend left, "f"] \arrow[r, bend right, "g"'] \arrow[r, phantom, "\Downarrow\alpha"] & C
\end{tikzcd} \quad \sim \quad \begin{tikzcd}
A \arrow[r, bend left, "h"] \arrow[r, bend right, "h"'] \arrow[r, phantom, "\Downarrow\mathsf{Id}_h"] & B \arrow[r, bend left, "f"] \arrow[r, bend right, "g"'] \arrow[r, phantom, "\Downarrow\alpha"] & C
\end{tikzcd}$$

Whiskering lets us form diagrams such as the following:

$$\begin{tikzcd}
A \arrow[rr, bend left, "f"] \arrow[dr, bend left, "g"] \arrow[dr, bend right, "f'"'] \arrow[dr, phantom, "\Downarrow\beta"] & \arrow[d, phantom, "\Downarrow\alpha"] & C \\
 & B \arrow[ur, bend right, "h"'] &
\end{tikzcd} \tag{B.9}$$

Further coherence is imposed between the unitors and associator.

Two main examples of bicategories are CAT and the delooping bicategory $\mathbf{B}\mathscr{C}$ of any monoidal category $\mathscr{C}$. In fact, a *monoidal category* may simply be defined as a bicategory $\mathbf{C}$ with exactly one object $\bullet$. Its underlying category $\mathsf{Hom}_{\mathbf{C}}(\bullet, \bullet)$ is called the *loop space*, and this is usually what is meant when referring to the monoidal category.

Appendix C

Linear bicategories and related structures

Linear bicategory is a generalization of *bicategory* defined in [CKS00], exactly like how *linearly distributive category* is a generalization of *monoidal category*. Linear bicategories still retain the full theory of adjunctions, and arguably, the separation of roles of the operations $\otimes$ and $\parr$ elucidates the theory. Examples include duality in star-autonomous categories as well as adjunctions in ordinary bicategories, such as CAT, i.e. adjoint functors.

A *linear bicategory* $\mathbf{C}$ consists of two bicategories $\mathbf{C}^{\otimes}$ and $\mathbf{C}^{\parr}$ with the same objects, 1-morphisms, 2-morphisms, and vertical composition, but different:

- horizontal composition $\otimes$ and $\parr$, respectively;
- identities $\top_A : A \to A$ and $\bot_A : A \to A$, resepectively;
- left unitors $\mathsf{lu}^{\otimes}(A,B)_f : f \overset{\sim}{\Rightarrow} A \otimes f$ and $\mathsf{lu}^{\parr}(B,A)_f : B \parr f \overset{\sim}{\Rightarrow} f$, respectively;
- right unitors $\mathsf{ru}^{\otimes}(B,A) : f \overset{\sim}{\Rightarrow} f \otimes A$ and $\mathsf{ru}^{\parr}(A,B)_f : f \parr B \overset{\sim}{\Rightarrow} f$, respectively.

Furthermore, $\mathbf{C}$ is equipped with:

- left linear distributor $\mathsf{lld}(A,B,C,D)_{f,g,h} : f \otimes (g \parr h) \Rightarrow (f \otimes g) \parr h$;
- right linear distributor $\mathsf{rld}(A,B,C,D)_{f,g,h} : (r \parr l) \otimes r \Rightarrow f \parr (g \otimes h)$.

$$
\begin{tikzcd}
 & & (e \otimes f) \parr (g \otimes h) & & \\
((e \otimes f) \parr g) \otimes h \arrow[urr, Rightarrow, "\mathsf{rld}(A,B,C,E)_{e\otimes f,g,h}"] & & & & e \otimes (f \parr (g \otimes h)) \arrow[ull, Rightarrow, "\mathsf{lld}(A,C,D,E)_{e,f,g\otimes h}"'] \\
 & (e \otimes (f \parr g)) \otimes h \arrow[ul, Rightarrow, "\mathsf{lld}(B,C,D,E)_{e,f,g}\otimes h"] \arrow[rr, Rightarrow, "\alpha^{\otimes}(A,B,D,E)_{e,f\parr g,h}"'] & & e \otimes ((f \parr g) \otimes h) \arrow[ur, Rightarrow, "e\otimes\mathsf{rld}_{f,g,h}"'] &
\end{tikzcd}
\tag{C.1}
$$

$$
\begin{tikzcd}
 & & (e \parr f) \otimes (g \parr h) \arrow[dll, Rightarrow, "\mathsf{lld}(A,B,C,E)_{e\parr f,g,h}"'] \arrow[drr, Rightarrow, "\mathsf{rld}(A,C,D,E)_{e,f,g\parr h}"] & & \\
((e \parr f) \otimes g) \parr h \arrow[dr, Rightarrow, "\mathsf{rld}(B,C,D,E)_{e,f,g}\parr h"'] & & & & e \parr (f \otimes (g \parr h)) \arrow[dl, Rightarrow, "e\parr\mathsf{lld}(A,B,C,D)_{f,g,h}"] \\
 & (e \parr (f \otimes g)) \parr h \arrow[rr, Rightarrow, "\alpha^{\parr}(A,B,D,E)_{e,f\otimes g,h}"'] & & e \parr ((f \otimes g) \parr h) &
\end{tikzcd}
\tag{C.2}
$$

Figure C.1: Pentagon identities relating linear distributivity and associativity

Additional coherences are imposed relating the linear distributors to the unitors and associator. Notice that the left and right linear distributor attracts $\otimes$ to the left or right, respectively. Also, the $\parr$s go into unitors and $\otimes$s come out. Among the new coherences are two new pentagon identities seen in Fig. C.1. There are other requirements besides these, which can be found in [CKS00].

A bicategory is just a linear bicategory where $\otimes$ and $\parr$ coincide, and the linear distributors coincide with the associator. A linear bicategory $\mathbf{C}$ has an *opposite* $\mathbf{C}^{\mathrm{op}}$ as well as a *converse* $\mathbf{C}^{\mathrm{co}}$. In $\mathbf{C}^{\mathrm{op}}$, the domain and codomain of 1-morphisms are interchanged, thereby reversing morphism composition for each of $\otimes$ and $\parr$. The reversed $\otimes$ operation $\otimes^{\mathrm{rev}}$, given by $Y \otimes^{\mathrm{rev}} X = X \otimes Y$, is the new *primal (horizontal) composition* (the new "$\otimes$") for $\mathbf{C}^{\mathrm{op}}$, and likewise for the *dual (horizontal) composition* "$\parr$". The left and right unitors for $\otimes$ are reversed, and likewise for $\parr$. The associators for $\otimes$ and $\parr$ are also each inverted.

In $\mathbf{C}^{\mathrm{co}}$, the domain and codomain of 2-morphisms are interchanged, thereby reversing vertical composition. Due to the symmetry in the roles of $\otimes$ and $\parr$, as seen in Fig. C.1, $\mathbf{C}^{\mathrm{co}}$ is made into a linear bicategory by reversing the roles of $\otimes$ and $\parr$. The linear bicategory $\mathbf{C}^{\mathsf{co}\ \mathsf{op}}$ has both the 1-morphisms and 2-morphisms interchanged, so for instance, its primal monoidal product is $\parr^{\mathrm{rev}}$.

A *linearly distributive category* is (the loop space of) a linear bicategory with exactly one object. A monoidal category is therefore just a linearly distributive category in the case that $\otimes$ and $\parr$ coincide. Confusingly, if $\mathscr{C}$ is a linearly distributive category with delooping $\mathbf{B}C$, then $\mathscr{C}^{\mathrm{op}}$ denotes the linearly distributive category with delooping $(\mathbf{B}\mathscr{C})^{\mathrm{co}}$. This makes the notation $\mathscr{C}^{\mathrm{op}}$ behave like the usual notion of opposite category. Its morphisms and monoidal structures are swapped.

There are several variations on the definition of *linear bicatgory* that one may wish to consider. For one thing, we can consider what happens when removing the associators $\alpha^{\otimes}$ and $\alpha^{\parr}$ as well as any coherence laws they are involved in, such as Fig. C.1. Furthermore, one may only require the unitors to be natural transformations, not necessarily isomorphisms, or even more severely, remove the unitors and units altogether. We work out the theory of star-autonomous categories without ever using the associators, and in particular, derive a new formula for the inverse nuclearizer that does not reference the associator. When working in these variations, it may be warranted to impose new coherences. For example, in a non-associative linearly distributive category, the following diagram is available:

$$\begin{tikzcd}
 & (V \otimes (W \parr X)) \otimes (Y \parr Z) \arrow[dl] \arrow[dr] & \\
((V \otimes (W \parr X)) \otimes Y) \parr Z \arrow[dr] & & ((V \otimes W) \parr X) \otimes (Y \parr Z) \arrow[dl] \\
 & (((V \otimes W) \parr X) \otimes Y) \parr Z &
\end{tikzcd}$$

By deleting the associators, we had to delete the four pentagon coherence laws of usual linearly distributive categories. The lazy way to procede is to simply make it part of the definition that "all well-formed diagrams commute". The work of checking coherence is then deferred to the part of plugging in a given category. Our present concern is not to find a complete set of coherence laws, serving a similar role to the pentagon laws, and prove the coherence theorem. Coherence is rarely invoked, though it is for example in the proof of Rowe's formula for the inverse nuclearizer Cor. 5.3.9, where we invoke the associativity pentagon directly (as opposed to a coherence theorem).

Once one assumes that the linear distributors and unitors are isomorphisms, these can be used to define canonical associative structures for $\otimes$ and $⅋$. We do not know whether the coherences involving these associative structures are inherited from those of the underlying unital non-associative linearly distributive structure. In Sec. 5.2.2, we explore associativity without coherence. For example, $\alpha^{\otimes}(A, B, C, D)$ is given by the following composition:

$$\begin{aligned}
(f \otimes g) \otimes h &\overset{\sim}{\Leftarrow} (f \otimes (\perp ⅋ g)) \otimes h \\
&\overset{\sim}{\Rightarrow} ((f \otimes \perp) ⅋ g) \otimes h \\
&\overset{\sim}{\Rightarrow} (f \otimes \perp) ⅋ (g \otimes h) \\
&\overset{\sim}{\Leftarrow} f \otimes (\perp ⅋ (g \otimes h)) \\
&\overset{\sim}{\Rightarrow} f \otimes (g \otimes h)
\end{aligned}$$

This derivation crucially relies on the invertibility of the left unitor for $⅋$ and left linear distributor.

Appendix D

Adjunctions in a linear bicategory

The notion of *adjoint functors* from category theory can be generalized in multiple ways. First, adjunctions can be defined in an arbitrary bicategory in place of Cat. The basic properties of adjunctions can still be proved, but one no longer has access to some of the neat Yoneda style proofs available in Cat. More generally, it turns out that we can define adjunctions in a linear bicategory. In fact, by analyzing the proofs below, one finds that associativity is never used in the elementary theory of adjunctions. Whereas associativity is used (e.g. in the definition of *category*) to give an abstract generalization of function composition, linear distributivity (but not associativity) is the key to abstractly formulating internal notions of *duality*.

The physics and math conventions for dualization result in two versions of the theory of star-autonomous categories. In the physics convention, the negation adjunction (de Morgan duality) involves a reversal, seen notationally as $(X \otimes Y)^* \cong Y^* \parr X^*$:

$$\begin{tikzcd}
\mathscr{C}^{\mathrm{rev\,op}} = (\mathscr{C}^{\mathrm{op}}, \parr^{\mathrm{rev}}) \arrow[rr, bend right, "{}^{\neg}(-)"'] \arrow[rr, phantom, "\perp"] & & (\mathscr{C}, \otimes) = \mathscr{C} \arrow[ll, bend right, "(-)^{\neg}"']
\end{tikzcd}$$

In the math convention, there is no reversal. Likewise, the definition of *linear adjunction* undergoes a reversal between the physics and math conventions. Note that the math convention is used in [CKS00], but we follow the physics convention. In the physics convention,

$$
\begin{tikzcd}
l \arrow[r, Rightarrow, "\mathsf{ru}^{\otimes}(A,B)_l"] \arrow[dddrrr, Rightarrow, "l"'] & l \otimes A \arrow[r, Rightarrow, "l\otimes\eta"] & l \otimes (r \parr l) \arrow[dr, Rightarrow, "\mathsf{lld}(B,A,B,A)_{l,r,l}"] & \\
 & & & (l \otimes r) \parr l \arrow[d, Rightarrow, "\epsilon \parr l"] \\
 & & & B \parr l \arrow[d, Rightarrow, "\mathsf{lu}^{\parr}(B,A)_l"] \\
 & & & l
\end{tikzcd}
$$

$$
\begin{tikzcd}
r \arrow[r, Rightarrow, "\mathsf{lu}^{\otimes}(A,B)_r"] \arrow[dddrrr, Rightarrow, "r"'] & A \otimes r \arrow[r, Rightarrow, "\eta\otimes r"] & (r \parr l) \otimes r \arrow[dr, Rightarrow, "\mathsf{rld}(A,B,A,B)_{r,l,r}"] & \\
 & & & r \parr (l \otimes r) \arrow[d, Rightarrow, "r \parr \epsilon"] \\
 & & & r \parr B \arrow[d, Rightarrow, "\mathsf{ru}^{\parr}(A,B)_r"] \\
 & & & r
\end{tikzcd}
$$

Figure D.1: Verbose zigzag identities for an adjunction in a linear bicategory

this directly generalizes the standard notion of *adjunction* from category theory, whereas in the math version, it generalizes the opposite (i.e. reversed) notion.

Let $\mathbf{C}$ be a linear bicategory. Then a pair of 1-morphisms $l : A \to B$ and $r : B \to A$, called the *left* and *right adjoint*, respectively, together with 2-morphisms $\eta : \top_A \Rightarrow r \parr l$ and $\epsilon : l \otimes r \Rightarrow \bot_B$, called the *unit* and *counit*, respectively, constitute a *linear adjunction* (in the physics convention) if the diagrams in Fig. D.1 commute. These are typically abbreviated by eliding the unitors and linear distributors:

$$
\begin{tikzcd}
l \arrow[r, Rightarrow, "l\otimes\eta"] \arrow[dr, Rightarrow, "l"'] & l \otimes r \parr l \arrow[d, Rightarrow, "\epsilon\parr l"] \\
 & l
\end{tikzcd}
\qquad
\begin{tikzcd}
r \arrow[r, Rightarrow, "\eta\otimes r"] \arrow[dr, Rightarrow, "r"'] & r \parr l \otimes r \arrow[d, Rightarrow, "r\parr\epsilon"] \\
 & r.
\end{tikzcd}
$$

For brevity, we refer to linear adjunctions simply as *adjunctions*. We caution that in the case of the tensor-hom adjunction, the counit is called *evaluation* whereas the unit is called *coevaluation*. Unfortunately, this inconsistency in the "co" prefix is well-established; it has nothing to do with the physics vs. math convention.

In a slight abuse of notation, we will use the globe diagrams we defined for bicategories also with linear bicategories. The zigzag identities are expressed by the diagrams:

$$
\begin{tikzcd}
B & A \arrow[l, "l"] & B \arrow[l, "r"] \arrow[ll, bend left=60, "\bot_B"] \arrow[ll, phantom, "\Downarrow\epsilon" below] & A \arrow[l, "l"] \arrow[ll, bend right=60, "\top_A"'] \arrow[ll, phantom, "\Downarrow\eta" above]
\end{tikzcd}
\qquad
\begin{tikzcd}
A & B \arrow[l, "r"] & A \arrow[l, "l"] \arrow[ll, bend right=60, "\top_A"'] \arrow[ll, phantom, "\Downarrow\eta" above] & B \arrow[l, "r"] \arrow[ll, bend left=60, "\bot_B"] \arrow[ll, phantom, "\Downarrow\epsilon" below]
\end{tikzcd}
\tag{D.1}
$$

Note that we also elide the unitors and linear distributors in the globe diagrams.

We noted previously that the principle of equivalence suggests that *adjunction* should only be considered a *well-defined* notion if it satisfies the following proposition. This is more than just a matter of beauty, since properties such as this are frequently invoked rigorously in the proofs of subseqeunt results.

Proposition D.0.1 (Well-definedness of the left-adjoint) *Let (l, r, η, ϵ) be an adjunction in a linear bicategory $\mathbf{C}$, and suppose that there exists a 2-isomorphism $\theta : l' \overset{\sim}{\Rightarrow} l$. Then $(l', r, \eta', \epsilon')$ is also an adjunction, where $\eta' = (r \parr \theta^{-1}) \circ \eta$ and $\epsilon' = \epsilon \circ (\theta \otimes \mathsf{Id}_r)$.*

Proof By the zigzag identities, the following diagrams collapse into Id_l and Id_r:

$$
\begin{tikzcd}
B & A \arrow[l, bend right, "l'"'] \arrow[l, bend left, "l"] \arrow[l, phantom, "\Downarrow\theta"] & B \arrow[l, "r"] \arrow[ll, bend left=60, "\bot_B"] \arrow[ll, phantom, "\Downarrow\epsilon" below] & A \arrow[l, bend right, "l'"'] \arrow[l, bend left, "l"] \arrow[l, phantom, "\Downarrow\theta^{-1}"] \arrow[ll, bend right=60, "\top_A"'] \arrow[ll, phantom, "\Downarrow\eta" above]
\end{tikzcd}
\qquad
\begin{tikzcd}
A & B \arrow[l, "r"] & A \arrow[l, bend right, "l'"'] \arrow[l, "l"] \arrow[l, bend left, "l'"] \arrow[ll, bend right=60, "\top_A"'] \arrow[ll, phantom, "\Downarrow\eta" above] & B \arrow[l, "r"] \arrow[ll, bend left=60, "\bot_B"] \arrow[ll, phantom, "\Downarrow\epsilon" below]
\end{tikzcd}
\tag{D.2}
$$

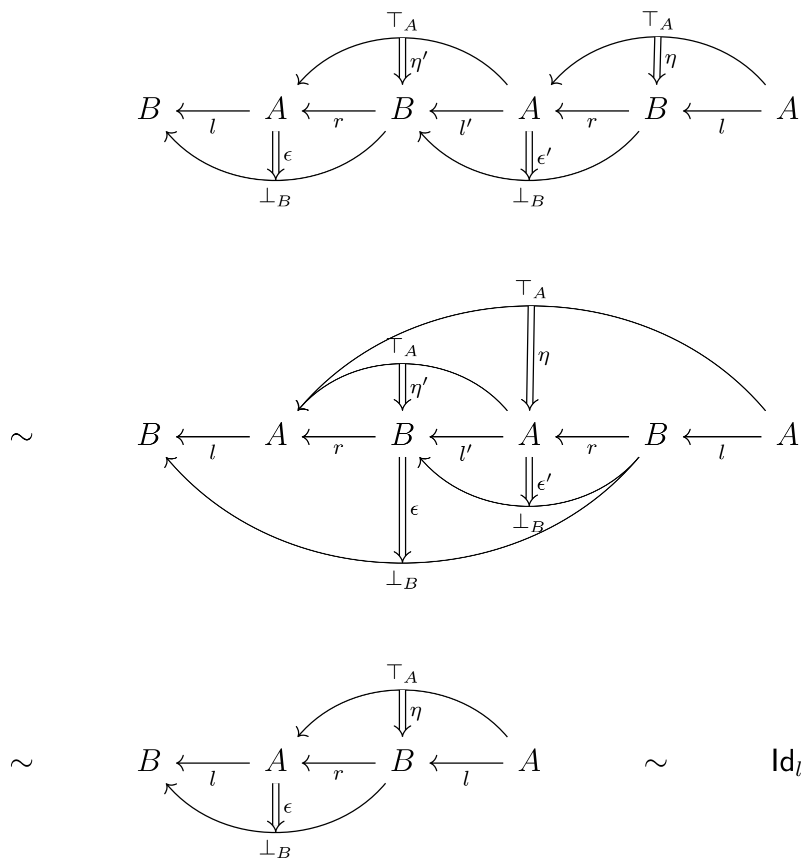
■

Proposition D.0.2 (Uniqueness of the left adjoint) *Let (l, r, η, ϵ) and $(l', r, \eta', \epsilon')$ be adjunctions in a linear bicategory $\mathbf{C}$. Then $l \simeq l'$.*

Proof By the left zigzag identity, we must show that the following diagram commutes.

$$\begin{tikzcd}
l \arrow[r, Rightarrow, "l\otimes\eta'"] \arrow[dd, Rightarrow, "l\otimes\eta"'] & l \otimes r \parr l' \arrow[d, Rightarrow, "\epsilon\parr l'"] & \\
 & l' \arrow[r, Rightarrow, "l'\otimes\eta"] & l' \otimes r \parr l \arrow[d, Rightarrow, "\epsilon'\parr l"] \\
l \otimes r \parr l \arrow[rr, Rightarrow, "\epsilon\parr l"'] & & l
\end{tikzcd} \tag{D.3}$$

It is easier to see this using globe diagrams:



(D.4)

The proof used the left zigzag identity for $l \dashv r$ and the right zigzag identity for $l' \dashv r$. ■

In the case of $\mathbf{C} = \textsc{Cat}$, Prop. D.0.1 and Prop. D.0.2 can also be proved using the Yoneda embedding. The Yoneda proofs, which we omit, are actually much simpler, as the work is diverted into the (very technical) proof of Prop. E.0.3.

Appendix E

The bicategory Cat

We now briefly describe the bicategorical structure of $\textsc{Cat}$. We skip all the proofs. These can be found in [Mac78] or a variety of other sources. The purpose of this section is to give some additional context to the calculations found throughout the thesis. For example, the formulas for evaluation and coevaluation are proved in the process of proving Prop. E.0.3. We also state the Yoneda lemma and its important corollary, that the Yoneda functor $よ_{\mathscr{C}}$ is full and faithful.

Objects in $\textsc{Cat}$ are categories, 1-morphisms are functors, and 2-morphisms are natural transformations. We assume the reader is familiar with categories and functors. If $\mathscr{A}, \mathscr{B}$ are categories and $F, G : \mathscr{A} \to \mathscr{B}$ are functors, then a *natural transformation* $\eta : F \Rightarrow G$ assigns a morphism $\eta_X : FX \to GX$ in $\mathscr{B}$ to each object X in $\mathscr{A}$, such that for any morphism $\phi : X \to Y$ in $\mathscr{A}$, the following diagram commutes:

$$\begin{tikzcd} F(X) \arrow[r, "\eta_X"] \arrow[d, "F(\phi)"'] \arrow[dr, dashed] & G(X) \arrow[d, "G(\phi)"] \\ F(Y) \arrow[r, "\eta_Y"'] & G(Y) \end{tikzcd} . \tag{E.1}$$

We have just given the *objectwise* definition, meaning η is an indexed family over $\mathsf{ob}(\mathscr{A})$. Natural transformations also act on morphisms, and these actions uniquely determine each other. Explicitly, η takes ϕ to the dashed diagonal morphism in Eq. (E.1), which is denoted $\eta(\phi)$.

The *vertical composition* $\eta^1 \circ \eta^2 : F \to H$ of compatible natural transformations $F \overset{\eta^2}{\Rightarrow} G \overset{\eta^1}{\Rightarrow} H$ of functors $F, G, H : \mathscr{A} \to \mathscr{B}$ takes a morphism $\phi : X \to Y$ in $\mathscr{A}$ to the dashed diagonal arrow $(\eta_1 \circ \eta_2)(\phi)$ in the following commutative diagram.

$$\begin{tikzcd} F(X) \arrow[r, "\eta^2_X"] \arrow[d, "F(\phi)"'] \arrow[drr, dashed] & G(X) \arrow[r, "\eta^1_X"] \arrow[d, "G(\phi)"] & H(X) \arrow[d, "H(\phi)"] \\ F(Y) \arrow[r, "\eta^2_Y"'] & G(Y) \arrow[r, "\eta^1_Y"'] & H(Y) \end{tikzcd} . \tag{E.2}$$

Equivalently, the vertical composition is given objectwise by $(\eta^1 \circ \eta^2)_X = \eta^1_X \circ \eta^2_X$. Next, the horizontal product of natural transformations $\alpha : F_1 \Rightarrow G_1$ and $\beta : F_2 \Rightarrow G_2$ is the *Godement product*: $\alpha \,\square\, \beta : \mathscr{A} \to \mathscr{C}$ is defined on $X \in \mathsf{ob}(A)$ by the formula:

$$(\alpha \,\square\, \beta)_X = \alpha(\beta_X). \tag{E.3}$$

The horizontal composition composition operations for functors and natural transformations, together with the vertical (Godement) composition operation makes $\textsc{Cat}$ into a strict bicategory. There is also a fourth composition operation to watch out for in $\textsc{Cat}$, which is the composition of morphisms within the objects of $\textsc{Cat}$ (categories) themselves.

Recall that the category of sets, $\textsc{Set}$, has a *factorization system* in which every morphism (function) $f : A \to B$ has the form $f = me$ where m is injective and e is surjective. The situation is a little bit more complicated with $\textsc{Cat}$. It has multiple factorization systems, but most importantly, every functor factors as an essentially surjective functor followed by a full and faithful functor. A functor $F : \mathscr{A} \to \mathscr{B}$ is called *full* if for all $X, Y \in \mathsf{ob}(\mathscr{A})$,

$$F_{X,Y} : \mathsf{Hom}_{\mathscr{A}}(X, Y) \to \mathsf{Hom}_{\mathscr{B}}(FX, FY)$$

is surjective and *faithful* if it is injective. F is *essentially surjective* if for all $X' \in \mathsf{ob}(\mathscr{B})$ there exists $X \in \mathsf{ob}(\mathscr{A})$ such that $X' \cong FX$. Every functor *preserves structure*, but:

Proposition E.0.1 *A functor reflects structure if and only if it is full and faithful.*

A functor $F : \mathscr{A} \to \mathscr{B}$ is defined to *preserve* or *reflect* structure if:

$$\underset{\text{(preservation)}}{G \cong G' \implies FG \cong FG'} \qquad\qquad \underset{\text{(reflection)}}{G \cong G' \impliedby FG \cong FG'}$$

respectively, ranging over all $G, G' : \mathscr{U} \to \mathscr{X}$ with the same domain. One proves that the Yoneda embedding (discussed below) is full and faithful, but in practice it is almost always used (e.g. in Sec. 5.2) in conjunction with Prop. E.0.1. The proofs of both of these facts are nontrivial. Next, an *equivalence of categories* consists of a pair of functors $F : \mathscr{A} \to \mathscr{B}$ and $G : \mathscr{B} \to \mathscr{A}$ and natural isomorphisms $GF : \mathsf{id}_{\mathscr{A}} \overset{\sim}{\Rightarrow} \eta$ and $\epsilon : FG \overset{\sim}{\Rightarrow} \mathsf{id}_{\mathscr{B}}$. Then:

Proposition E.0.2 *A functor $F : \mathscr{A} \to \mathscr{B}$ is full, faithful, and essentially surjective if and only if it lies in an equivalence (F, G, η, ϵ).*

Every equivalence can be upgraded to an adjoint equivalence. Also, in the bicategory Cat, adjunctions have a few more equivalent formulations than in the abstract case:

Proposition E.0.3 *Let $\mathscr{A}$ and $\mathscr{B}$ be categories, and let $L : \mathscr{A} \to \mathscr{B}$ and $R : \mathscr{B} \to \mathscr{A}$ be functors. Then the following additional structures, if they exist, uniquely determine each other:*

(i) a natural transformation $\eta : \mathsf{id}_{\mathscr{A}} \to RL$ such that for all $X \in \mathsf{Ob}(\mathscr{A})$, $Y \in \mathsf{Ob}(\mathscr{B})$, and $g : X \to RY$, there exists a unique $f : LX \to Y$ such that the following diagram commutes:

$$\begin{tikzcd} X \arrow[r, "\eta_X"] \arrow[dr, "g"'] & RLX \arrow[d, "Rf"] \\ & RY \end{tikzcd} . \tag{E.4}$$

This is called the universal factorization through the unit;

(ii) a natural transformation ϵ (counit) satisfying universal factorization dual to above;

(iii) natural transformations $\eta : \mathsf{id}_{\mathscr{A}} \to RL$ and $\epsilon : LR \to \mathsf{id}_{\mathscr{B}}$ such that (L, R, η, ϵ) form an adjunction;

(iv) a natural bijection of the following functors of type $\mathscr{A}^{\mathrm{op}} \times \mathscr{B} \to$ Set:

$$\iota : \mathsf{Hom}_{\mathscr{B}}(L(-), -) \overset{\sim}{\Rightarrow} \mathsf{Hom}_{\mathscr{A}}(-, R(-)),$$

called the adjunction isomorphism.

Characterization (*iv*) enables Yoneda style arguments and is often taken to be the definition of *adjunction* in $\textsc{Cat}$. We note, however, that the natural bijection of homsets for adjoint functors $L \vdash R$ is recovered from the unit and counit by the formulas:

$$\begin{aligned} \iota_{X,Y} : \mathsf{Hom}_{\mathscr{B}}(LX, Y) &\to \mathsf{Hom}_{\mathscr{A}}(X, RY) \\ f &\mapsto (Rf)\eta_X \end{aligned} \qquad \begin{aligned} \iota^{-1}_{X,Y} : \mathsf{Hom}_{\mathscr{A}}(X, RY) &\to Hom_{\mathscr{B}}(LX, Y) \\ g &\mapsto \epsilon_Y(Lg) \end{aligned}$$

Conversely, the unit and counit are given in terms of the hom bijection by:

$$\eta_X = \iota_{X,LX}(\mathsf{id}_{LX}) : X \to RLX \qquad \epsilon_Y = \iota^{-1}_{RY,Y}(\mathsf{id}_{RY}) : LRY \to Y \tag{E.5}$$

These formulas are used when working with the currying adjunctions.

Finally, we state the Yoneda Lemma and its important corollary. The *Yoneda embedding* for a category $\mathscr{C}$ is the functor:

$$\begin{aligned} よ_{\mathscr{C}} : \mathscr{C} &\to [\mathscr{C}^{\mathrm{op}}, \textsc{Set}] \\ F &\mapsto \mathsf{Hom}_{\mathscr{C}}(-, F) : \mathscr{C}^{\mathrm{op}} \to \textsc{Set} \end{aligned}$$

Here $[-,-]$ is the (large) Hom functor on the ambient CAT, and $\mathsf{Hom}_{\mathscr{C}}$ is the ordinary Hom functor for the category $\mathscr{C}$.

Theorem E.0.4 (Yoneda Lemma) *Given $X \in \mathsf{Ob}(\mathscr{C})$ and $F : \mathscr{C}^{\mathrm{op}} \to \textsc{Set}$, the function*

$$\begin{aligned} \ell_{X,F} : \mathsf{Nat}_{[\mathscr{C}^{\mathrm{op}},\textsc{Set}]}(よ_{\mathscr{C}} X, F) &\to FX \\ \eta &\mapsto \eta_X(\mathsf{id}_X) \end{aligned}$$

is natural in X and F, and in fact, conglomerates a natural bijection of functors of type $\mathscr{C} \times [\mathscr{C}^{\mathrm{op}}, \textsc{Set}] \to \textsc{Set}$.

Here, $\mathsf{Nat}_{[\mathscr{C}^{\mathrm{op}},\textsc{Set}]}$ temporarily denotes the (large) Hom functor for the (large) category $[\mathscr{C}^{\mathrm{op}}, \textsc{Set}]$ of presheaves on $\mathscr{C}$, whose morphisms are natural transformations.

Corollary E.0.5 *The Yoneda embedding $よ_{\mathscr{C}}$ is a full and faithful functor.*

In practice, the Yoneda embedding is used in conjunction with the nontrivial theorem that a functor is full and faithful if and only if it is an *embedding*, i.e. reflects structure. For example, if one can prove that there is a natural bijection:

$$\mathsf{Hom}_{\mathscr{C}}(-, F) \cong \mathsf{Hom}_{\mathscr{C}}(-, G)$$

then it follows that $F \cong G$ are naturally isomorphic functors. Typically we use a slightly different notation where objects are plugged in. That is, one writes that

$$\mathsf{Hom}_{\mathscr{C}}(U, FX) \cong \mathsf{Hom}_{\mathscr{C}}(U, GX)$$

is a bijection that is natural in U and X and concludes that $FX = GX$ is natural in X.

Appendix F

Conventions

F.1 Oppositization

Let $\mathscr{C}$ be a category. By definition (of *category*), we regard a morphism $f : X \to Y$ in $\mathscr{C}$ as a triple (X, Y, Γ) where X and Y are objects, and there is no general constraint on the additional data Γ. A triple is used in this definition so that we may recover the domain X, codomain Y, and data Γ of a morphism f.[1] Under this encoding, the *opposite category* $\mathscr{C}^{\mathrm{op}}$ is a new category whose objects are aliases $\tilde{X}$ for the objects X of $\mathscr{C}$, and whose morphisms $\tilde{f} = (\tilde{Y}, \tilde{X}, \Gamma)$ are in bijection with the morphisms $f = (X, Y, \Gamma)$ of $\mathscr{C}$.

$$f : X \to Y \qquad\qquad \tilde{f} : \tilde{Y} \to \tilde{X}$$

Composition is reversed, $\widetilde{gf} = \tilde{f}\tilde{g}$, and identities satisfy $\widetilde{\mathsf{id}_X} = \mathsf{id}_{\tilde{X}}$. In practice, the tilde notation is neither used for objects or morphisms. One simply writes X for $\tilde{X}$, but it would be confusing to write f as a shorthand when referring to the morphism $\tilde{f}$ in $\mathscr{C}^{\mathrm{op}}$ since the domain and codomain are swapped from those of the original morphism f in $\mathscr{C}$. We solve this by always recasting a morphism $\tilde{f}$ in $\mathscr{C}^{\mathrm{op}}$ back to $\mathscr{C}$ and working with f directly. Nevertheless, it is impossible to avoid $\mathscr{C}^{\mathrm{op}}$ entirely, due to the importance of contravariant functors. Recall that a *contravariant endofunctor* on $\mathscr{C}$ either has type $\mathscr{C} \to \mathscr{C}^{\mathrm{op}}$ or $\mathscr{C}^{\mathrm{op}} \to \mathscr{C}$. One also encounters functors of type $\mathscr{C}^{\mathrm{op}} \times \mathscr{C} \to \mathscr{C}$, and so on. This convention of recasting morphisms in $\mathscr{C}^{\mathrm{op}}$ to $\mathscr{C}$ is standard. Its main benefit is that it allows us to

[1] For example, if $\mathscr{C} = \textsc{Set}$, then Γ is the graph relation of the function f. Since Y cannot be recovered from Γ, the ordered triple encoding gives functions well-defined notions of *codomain* and *surjectivity*.

avoid having to constantly specify whether a morphism is in $\mathscr{C}$ or $\mathscr{C}^{\mathrm{op}}$.

Each functor $F : \mathscr{C} \to \mathscr{D}$ has an opposite $F^{\mathrm{op}} : \mathscr{C}^{\mathrm{op}} \to \mathscr{D}^{\mathrm{op}}$ defined by $F^{\mathrm{op}}(\tilde{f}) = \widetilde{F(f)}$. Likewise, each natural transformation $\alpha : F \Rightarrow G$ gives rise to $\alpha^{\mathrm{op}} : G^{\mathrm{op}} \Rightarrow F^{\mathrm{op}}$ by setting $\alpha^{\mathrm{op}}(f) = \widetilde{\alpha(f)}$. These satisfy properties making oppositization a 2-functor $(-)^{\mathrm{op}} : \textsc{Cat} \to \textsc{Cat}^{\mathrm{co}}$. The superscript $^{\mathrm{co}}$ indicates that oppositization acts covariantly on 1-morphisms (functors) but contravariantly on 2-morphisms (natural transformations) in the bicategory $\textsc{Cat}$. Due to this covariance on 1-morphisms, it is standard to write F in place of F^{op}, generalizing how one writes X in place of $\tilde{X}$, and we follow this convention.[2] A common example is seen in the *hom-bijection* formulation of adjunctions. To explain, first note that $\mathsf{Hom}_{\mathscr{C}}$ is a functor of type:

$$\mathsf{Hom}_{\mathscr{C}} : \mathscr{C}^{\mathrm{op}} \times \mathscr{C} \to \textsc{Set}$$

Then recall that an *adjunction* $L \dashv R$ consists of a pair of functors $L : \mathscr{C} \to \mathscr{D}$ and $R : \mathscr{D} \to \mathscr{C}$ together with a natural bijection ι of the following form:

$$\iota_{X,Y} : \mathsf{Hom}_{\mathscr{D}}(LX, Y) \to \mathsf{Hom}_{\mathscr{C}}(X, RY) \tag{F.1}$$

More correctly, one should write L^{op} instead of L in the above expression, since the left input of the hom functor is contravariant, but this would be highly unusual. We prefer to specify the precise type of L when first introducing it, but typically just write L (instead of distinguishing between L and L^{op}) in subsequent expressions, as we have done in Eq. (F.1). To do otherwise would spawn tedious typechecking exercises that don't shed light on the mathematical structure being considered, which is that of $\mathscr{C}$ rather than the ambient $\textsc{Cat}$.

Pedantically keeping track of F versus F^{op} is also awkward when working with multiple adjunctions that interact. For example, suppose $\mathscr{C}$ is biclosed monoidal. Then left negation $(-)^{\neg} = - \multimap \perp$ is contravariant, so its type must either be $\mathscr{C} \to \mathscr{C}^{\mathrm{op}}$ or $\mathscr{C}^{\mathrm{op}} \to \mathscr{C}$. Let us consider its interaction with the left currying adjunction $- \otimes Y \dashv Y \multimap -$. Consider the following morphisms in $\mathscr{C}$:

$$\lfloor \mathsf{lefteval}_{\perp}^{X} \rfloor : X \to {}^{\neg}(X^{\neg}) \tag{F.2}$$

$$\mathsf{lefteval}_{\perp}^{X} : X^{\neg} \otimes X \to \perp \tag{F.3}$$

$$\mathsf{id}_{X^{\neg}} : X^{\neg} \to X^{\neg} \tag{F.4}$$

[2] In fact, we are just applying the same convention to the functor category $\mathsf{Hom}_{\textsc{Cat}}(\mathscr{C}, \mathscr{D})$. To see why this extends the notational convention for objects, consider the identity functor id on $\mathscr{C}$: $\mathsf{id}_X^{\mathrm{op}} = \widetilde{\mathsf{id}_X} = \mathsf{id}_{\tilde{X}}$.

Since these are all morphisms in $\mathscr{C}$, Eq. (F.2) suggests that we should regard left negation as a functor of type $(-)^\neg : \mathscr{C} \to \mathscr{C}^{\mathrm{op}}$ and right negation as $^\neg(-) : \mathscr{C}^{\mathrm{op}} \to \mathscr{C}$. Indeed, we shall take this point of view, and note that they form the *negation adjunction* $(-)^\neg \dashv {}^\neg(-)$. But then $X \in \mathsf{Ob}(\mathscr{C})$ and $X^\neg \in \mathsf{Ob}(\mathscr{C}^{\mathrm{op}})$, so Eq. (F.3) is mistyped, since we should certainly either have $\otimes : \mathscr{C} \times \mathscr{C} \to \mathscr{C}$ or $\otimes : \mathscr{C}^{\mathrm{op}} \times \mathscr{C}^{\mathrm{op}} \to \mathscr{C}^{\mathrm{op}}$. Also, Eq. (F.4) is mistyped because it is a morphism in $\mathscr{C}$ but left negation is $\mathscr{C}^{\mathrm{op}}$-valued.

To solve this without resorting to the notational abuse, certain instances of $(-)^\neg$ would need to be replaced by $((-)^\neg)^{\mathrm{op}}$ (which we will temporarily denote by $(-)^{\neg^{\mathrm{op}}}$), and certain instances of X should really be $\tilde{X}$. Part of the issue is that left currying is more correctly of the form $- \otimes Y \dashv \tilde{Y} \multimap -$, and similarly for right currying. This detail can be seen by applying the same pedantic analysis to the proof of Mac Lane's parameter theorem [Mac78]. In the end, Eq. (F.2), Eq. (F.3), and Eq. (F.4) end up having respective types:

$$X \to {}^\neg(X^\neg) \qquad\qquad \tilde{X}^{\neg^{\mathrm{op}}} \otimes X \to \bot \qquad\qquad \tilde{X}^{\neg^{\mathrm{op}}} \to \tilde{X}^{\neg^{\mathrm{op}}} \tag{F.5}$$

Also, as if Eq. (F.5) weren't bad enough, the types of the domains of these morphisms will be swapped when writing out the hom bijections. Since this matter of bookkeeping does not contribute to our understanding, we choose not to distinguish between F and F^{op}, or in particular between X and $\tilde{X}$. However we note that in order for the negations to have types $(-)^\neg : \mathscr{C} \to \mathscr{C}^{\mathrm{op}}$ and $^\neg(-) : \mathscr{C}^{\mathrm{op}} \to \mathscr{C}$, the internal hom functors must be of types:

$$\begin{aligned} \multimap &: \mathscr{C} \times \mathscr{C}^{\mathrm{op}} \to \mathscr{C}^{\mathrm{op}} & \qquad \circ\!\!- &: \mathscr{C} \times \mathscr{C}^{\mathrm{op}} \to \mathscr{C} \\ \multimap^{\mathrm{op}} &: \mathscr{C}^{\mathrm{op}} \times \mathscr{C} \to \mathscr{C} & \qquad \circ\!\!-^{\mathrm{op}} &: \mathscr{C}^{\mathrm{op}} \times \mathscr{C} \to \mathscr{C}^{\mathrm{op}} \end{aligned} \tag{F.6}$$

We sometimes consider a functor $F : \mathscr{C} \to \mathscr{D}$ for arbitrary $\mathscr{C}$ and $\mathscr{D}$, only later to instantiate $\mathscr{C}^{\mathrm{op}}$ for $\mathscr{D}$. This is where the convention of replacing the discussion of a morphism $\tilde{f}$ in $\mathscr{C}^{\mathrm{op}}$ with that of its corresponding morphism f in $\mathscr{C}$ can be confusing. In the arbitrary $\mathscr{D}$ case, one may discuss a morphism $f : Y \to X$ in $\mathscr{D}$, but then when plugging in $\mathscr{C}^{\mathrm{op}}$ for $\mathscr{D}$, there is a swap in the subject of discussion, which becomes the morphism $f : X \to Y$ in $\mathscr{C}$ instead of the morphism $\tilde{f}$ in $\mathscr{C}^{\mathrm{op}}$. In order to alert the reader of this confusing swap of "subject", in the arbitrary $\mathscr{D}$ case, we write $X \leftarrow Y : f$ instead of $f : Y \to X$. Then when instantiating to $\mathscr{C}^{\mathrm{op}}$, the arrow reverses direction, and the notation becomes $f : X \to Y$.

Why not use the mirrored notation in the instantiated case instead of the uninstantiated case? Because in the instantiated case, the defining relationship between $\mathscr{C}$ and $\mathscr{C}^{\mathrm{op}}$ ultimately obscures whether a morphism "should" be regarded as being in $\mathscr{C}$ or $\mathscr{C}^{\mathrm{op}}$, as we have seen in above with Eq. (F.2), Eq. (F.3), and Eq. (F.4).

F.2 Currying convention

We now discuss a convention that manifests itself in a variety of ways. A familiar one of these concerns a sesquelinear form $\langle -, - \rangle$ on a complex vector space V. Physicists prefer linearity in the second argument, and mathematicians prefer it in the first:

$$\begin{array}{cc} \langle -, - \rangle : \overline{V} \otimes V \to \mathbb{C} & \langle -, - \rangle : V \otimes \overline{V} \to \mathbb{C} \\ \text{(physics convention)} & \text{(math convention)} \end{array} \tag{F.7}$$

We arbitrarily choose to follow the **physics** convention.

Here, $\overline{V}$ is the complex conjugate vector space, which has the same underlying set and addition of V but has scalar multiplication $\cdot$ given by $c \cdot v = \bar{c}v$. This effectively makes $\langle -, - \rangle$ *antilinear* in the argument of type $\overline{V}$.

Given finite dimensional complex inner product space V, a canonical isomorphism $\overline{V} \cong V^*$ is obtained by currying the inner product $\langle -, - \rangle$. Then Eq. (F.7) becomes the *natural pairing*:

$$\begin{array}{cc} \langle -, - \rangle : V^* \otimes V \to \mathbb{C} & \langle -, - \rangle : V \otimes V^* \to \mathbb{C} \\ f \otimes x \mapsto f(x) & x \otimes f \mapsto f(x) \\ \text{(physics convention)} & \text{(math convention)} \end{array} \tag{F.8}$$

We call both maps in Eq. (F.8) **left evaluation** maps. The physics vs. math distinction is **different** from the left vs. right distinction, and the physics and math conventions each have their own notions of left and right evaluation, currying, and so on. For example, the types indicated in Eq. (F.6) are consistent with the physics convention.

One finds that the physics vs. math convention for evaluation is equivalent to many other conventions when studying categories with sufficient structure, generalizing the case of $\mathbb{C}$-Vect, and so for lack of better terminology, we extend the terms *physics convention* and *math convention* to all of these. Given a functor $\otimes : \mathscr{C} \times \mathscr{C} \to \mathscr{C}$, such conventions must be chosen consistently. However, when $(\mathscr{C}, \otimes)$ is equipped with a braiding, that is, a natural isomorphism β of the form $\beta_{XY} : X \otimes Y \xrightarrow{\sim} Y \otimes X$, the distinction of left and right is less important since the left and right versions determine each other via the braiding. This is the case with $\mathbb{C}$-Vect, which has a *symmetry*, that is, a braiding s satisfying $s^2 = \mathsf{Id}_{\mathsf{id} \times \mathsf{id}}$.

The equivalence of various forms of the convention discussed here is often unobvious, and for historical reasons, the "wrong" convention is sometimes set in stone, and we don't dare to stray from it. For example, function evaluation is almost always written as "$f(x)$", never "$(x)f$", even though in the math convention, this results in a somewhat annoying swap in Eq. (F.8). We write $f(x)$ in red to indicate that the expected swap is not used.

	physics	math
left curry right curry	$\mathsf{hom}(X \otimes Y, Z) \cong \mathsf{hom}(X, Y \multimap Z)$ $\mathsf{hom}(X \otimes Y, Z) \cong \mathsf{hom}(Y, Z \multimapinv X)$	$\mathsf{hom}(X \otimes Y, Z) \cong \mathsf{hom}(Y, X \multimap Z)$ $\mathsf{hom}(X \otimes Y, Z) \cong \mathsf{hom}(X, Z \multimapinv Y)$
left int. curry right int. curry	$(X \otimes Y) \multimap Z \cong X \multimap (Y \multimap Z)$ $Z \multimapinv (X \otimes Y) \cong (Z \multimapinv X) \multimapinv Y$	$(X \otimes Y) \multimap Z \cong Y \multimap (X \multimap Z)$ $Z \multimapinv (X \otimes Y) \cong (Z \multimapinv Y) \multimapinv X$
left eval. right eval.	$(X \multimap Y) \otimes X \to Y$ $X \otimes (Y \multimapinv X) \to Y$	$X \otimes (X \multimap Y) \to Y$ $(Y \multimapinv X) \otimes X \to Y$
left nucl. right nucl.	$Y \parr X^* \cong X \multimap Y$ ${}^*X \parr Y \cong Y \multimapinv X$	$Y^* \parr X \cong X \multimap Y$ $Y \parr {}^*X \cong Y \multimapinv X$
de Morgan	$(X \otimes Y)^* \cong Y^* \parr X^*$ ${}^*(X \parr Y) \cong {}^*Y \otimes {}^*X$	$(X \otimes Y)^* \cong X^* \parr Y^*$ ${}^*(X \parr Y) \cong {}^*X \otimes {}^*Y$
left int. comp. right int. comp.	$(Y \multimap Z) \otimes (X \multimap Y) \to X \multimap Z$ $(Y \multimapinv X) \otimes (Z \multimapinv Y) \to Z \multimapinv X$	$(X \multimap Y) \otimes (Y \multimap Z) \to X \multimap Z$ $(Z \multimapinv Y) \otimes (Y \multimapinv X) \to Z \multimapinv X$
consistent with	bra-ket notation [Sha94] category theorists [Mac78; Rie16] various nlab pages Higgs, Rowe [Row88; HR89] Haskell Quantum info theory [Wat18][3]	functional analysis [Kna07; Con07; Rud91] category theorists various nlab pages Girard; Cocket, Seely; Barr [Gir87; CS99; CS97b; CS97b] [Bar79; Bar91; Bar95]

Table F.1: Some equivalent Formulations of the currying convention

We take some liberty with the placement of citations in Table F.1. The types of the unit of an arbitrary adjunction and counit are firmly established in category theory (e.g. in [Mac78; Rie16]), but it is usually ambiguous which currying convention is used since the monoidal structure is usually symmetric. That said, preference for one convention or the other can arguably be gleaned from the notational choices, for instance on pp.63-65, 129 of [Rie16].

Once one is accustomed to one convention, it is easy to mistakenly believe that braidedness is being assumed when coming across the other convention.

[3]The *vectorization* map is the inverse $X \multimap Y \xrightarrow{\sim} Y \parr X^*$ of the nuclearizer when X is a finite dimensional vector space, though *TQI* ([Wat18]) avoids mention of the dual space, so the map appears slightly differently.

One should choose a consistent convention not only with regard to the interal structure of $\mathscr{C}$, but also with higher categorical structure. Consider, for instance, the hom functor:

$$\mathsf{hom}_{\mathscr{C}} : \mathscr{C}^{\mathrm{op}} \times \mathscr{C} \to \textsc{Set} \qquad \qquad \mathsf{hom}_{\mathscr{C}} : \mathscr{C}^{\mathrm{op}} \times \mathscr{C} \to \textsc{Set}$$

(physics convention) (math convention)

This is similar to an evaluation map, so we expect consistency with Eq. (F.8). In the physics convention, it is the "left" version and in the math convention (assuming we use the "uncorrected" version as written above), it is the "right" version.

Composition of morphisms takes a pair (g, f) with $g : Y \to Z$ and $f : X \to Y$ to its composite $gf : X \to Z$ (often written $g \circ f$). This is "left composition" from the point of view of the physics convention and "right composition" from the point of view of the math convention. A frustration common to users of either convention is that composition runs opposite to the standard left-to-write format for arrows in commutative diagrams:

$$X \xrightarrow{f} Y \xrightarrow{g} Z \qquad \qquad X \xrightarrow{gf} Z$$

Two fixes are occasionally employed: either the diagrams can be drawn right-to-left or one introduces a new composition symbol ; and writes $f;g$ in place of gf. We would argue that the former is more in line with the rest of the "physics" conventions and the latter is more in line with the rest of the "math" conventions, including writing "$(x)f$" in place of $f(x)$. We do not apply either of these fixes and write diagrams as usual.

de Morgan duality is a helpful way to view the difference between the physics and math conventions. *Inversion* on a group is an instance of this abstract notion of de Morgan duality. A group may be thought of as a discrete autonomous category. The monoidal product $\otimes : \mathscr{G} \times \mathscr{G} \to \mathscr{G}$ is the group law. In the physics convention, the de Morgan dual $\boxtimes$ is "the same" as the original operation, by which we mean that we have a natural isomorphism $\boxtimes \cong \otimes^{\mathrm{op}}$. In the math convention, the de Morgan dual $\boxtimes$ is the "reverse" $\boxtimes \cong \otimes^{\mathrm{rev\,op}}$. In group theory, $\otimes^{\mathrm{rev\,op}}$ is called the *opposite group* law. Note the unfortunate terminology clash: the group law on the opposite group is not the opposite of the functor $\otimes$, but the reverse opposite.

Haskell is more consistent with the physics convention because out of the four versions of currying listed in the table, only *left* currying in the *physics* convention leaves the orders of the arguments X, Y, and Z unchanged, as does the `curry` function in Haskell.

Appendix G

Pre-abelian categories

Let $\mathscr{C}$ be a category with finite limits and finite colimits.

Consider a morphism $f : X \to Y$. The *kernel pair* of f is the pullback:

$$\begin{tikzcd} X \times_Y X \arrow[r, "t_2"] \arrow[d, "t_1"'] & X \arrow[d, "f"] \\ X \arrow[r, "f"'] & Y \end{tikzcd}$$

In $\mathscr{C} = \text{Set}$, we may define $X \times_Y X = \{(x_1, x_2) \in X \times X \mid fx_1 = fx_2\}$ with $t_i(x_1, x_2) = x_i$. That is, $X \times_Y X$ is the equivalence relation on X induced by f. One easily finds this satisfies universality. In $\mathscr{C} = \text{Grp}$, Ab, or various other similar examples, the kernel pair may be given the same material definition, and it is the (homomorphic) equivalence relation of membership in the same coset of the usual kernel $\mathsf{ker}\, f = \{x \in X \mid fx = 1_Y\}$.

The *regular coimage* of f is the coequalizer $\mathsf{coim}\, f$ of the kernel pair $X \times_Y X \rightrightarrows X$. In $\mathscr{C} = \text{Set}$, we may take it to be the set of equivalence classes $\{[x] \mid x \in X\}$ where $[x_1] = \{x_2 \in X \mid (x_1, x_2) \in X \times_Y X\}$. In $\mathscr{C} = \text{Grp}$, Ab, and so on, it is the quotient. The *regular image* is defined dually. In HausTop it is the closure of the range $\overline{f(X)}$. By construction, the regular coimage is a regular epimorphism and the regular image is a regular monomorphism. One then finds that there is an essentially unique factorization:

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d] & Y \\ \mathsf{coim}\, f \arrow[r, "\tilde{f}"'] & \mathsf{im}\, f \arrow[u] \end{tikzcd}$$

One calls f *strict* if $\tilde{f}$ is an isomorphism. We will see that a regular monomorphism is the same as a strict monomorphism, and dually. Although they are equivalent, they are not obviously so, and *strictness* is the characterization that ends up arising more directly in our application. The intuition for *regular monomorphism* is that in $\mathscr{C} = \textsc{HausTop}$, the monomorphisms are the injective continuous functions, whereas the regular monomorphisms are the embeddings. We omit the proofs and refer the reader to [Stacks] and [Kel69].

Proposition G.0.1 *If $f : X \to Y$ is a regular monomorphism, then $\mathsf{coim}\, f \cong \mathsf{id}_X$ (in the coslice category $\mathscr{C} \uparrow X$), and dually. Such morphisms are moreover strict.*

In other words, when $\mathscr{C}$ has finite limits and finite colimits, regular monomorphisms are the same as (what are elsewhere called) *effective monomorphisms.*

Now assume $\mathscr{C}$ is *preabelian.* This means $\mathscr{C}$ is $\textsc{Ab}$-enriched and has finite limits and finite colimits. Note that $\mathscr{C}$ is called *abelian* if every morphism is strict. The category of locally compact abelian groups LCA is preabelian, but not abelian, so for this reason, we do not assume that every morphism is strict. The *kernel* of $f : X \to Y$ is the pullback:

$$\begin{tikzcd} \mathsf{ker}\, f \arrow[r] \arrow[d, "\mathsf{ker}\, f"'] & 0 \arrow[d] \\ X \arrow[r, "f"'] & Y \end{tikzcd}$$

The kernel of f is unique up to isomoprhism in the slice category $\mathscr{C} \downarrow X$. Dually, the *cokernel* is defined by pushout, and is unique up to isomoprhism in $\mathscr{C} \uparrow Y$.

Proposition G.0.2 *A morphism $f : X \to Y$ is monic if and only if $\mathsf{ker}\, f \cong 0$, and dually.*

Proposition G.0.3 *For any f, we have $\mathsf{ker}\,\mathsf{coker}\,\mathsf{ker}\,f \cong \mathsf{ker}\,f$ over X, and dually.*

Proposition G.0.4 *The image and coimage of a morphism $f : X \to Y$, as defined above, are equivalently $\mathsf{im}\,f \cong \mathsf{ker}\,\mathsf{coker}\,f$ and $\mathsf{coim}\,f \cong \mathsf{coker}\,\mathsf{ker}\,f$, respectively.*

In fact these are usually taken to be the definitions of *image* and *coimage* when working with preabelian categories. It follows that every morphism $f : X \to Y$ admits an essentially unique canonical decomposition:

$$X \twoheadrightarrow \mathsf{coker}\,\mathsf{ker}\,f \xrightarrow{\tilde{f}} \mathsf{ker}\,\mathsf{coker}\,f \rightarrowtail Y \tag{G.1}$$

Thus, $f : X \to Y$ is strict if and only if $\tilde{f}$ in Eq. (G.1) is an isomorphism.

Proposition G.0.5 *A monomorphism is strict if and only if it is a kernel, and dually.*

Proposition G.0.6 *Every strict monomorphism is a regular monomorphism.*

Together with Prop. G.0.1, we see that in a preabelian category, a monomorphism is strict if and only if it is a regular monomorphism.

A sequence $\cdots \to X_i \overset{f_i}{\to} X_{i+1} \overset{f_{i+1}}{\to} X_{i+2} \to \cdots$ is *exact* if $\mathsf{ker}\,\mathsf{coker}\,f_i = \mathsf{ker}\,f_{i+1}$ for each i. A *co-exact sequence* is defined dually. An exact sequence is *strict* if each f_i is strict.

Proposition G.0.7 *Let $0 \to X \overset{f}{\to} Y \overset{g}{\to} Z \to 0$ be a short exact sequence and suppose f is strict. Then $f \cong \mathsf{ker}\,g$. Likewise if g is strict then $g \cong \mathsf{coker}\,f$.*

In particular if we assume that f is a strict monomorphism and define g to be its cokernel, then g is a strict epimorphism lying in such an exact sequence. We will later use this technique in order to define the *alternating square* $\wedge^2 V$ as $V^{\otimes 2}/I^2V$.

From Prop. G.0.7 we see that every strict short exact sequence is co-exact.

Next, we will need the dual of part (i) of Lemma 2.1 in [Kop11]:

Lemma G.0.8 *Consider a diagram of the following form in a preabelian category:*

$$\begin{tikzcd} A \arrow[r, equal] \arrow[d, "p_1"'] & A \arrow[d, "p_2"] \\ B_1 \arrow[r, "r"] \arrow[d, "q_1"'] & B_2 \arrow[d, "q_2 = \mathsf{coker}\, p_2"] \\ C \arrow[r, equal] & C \end{tikzcd}$$

Further assume that $p_1 q_1 = 0$ and that q_1 is epic. Then r is epic.

Note that the equalities can of course be replaced by isomorphisms without harm.

Proof Let $xr = 0$ for some $x : B_2 \to U$. Then $xp_2 = xrp_1 = 0$, and since $q_2 = \mathsf{coker}\, p_2$, there exists unique $y : C \to U$ such that $yq_2 = x$. Then $yq_1 = yq_2 r = xr = 0$. Since q_1 is epic, $y = 0$, which implies $x = yq_2 = 0$, and so r is epic. ■

Appendix H

Transporting an exact sequence

Consider a pair of composable morphisms in a preabelian category:

$$
\begin{tikzcd}
K \arrow[d, "k"'] & \\
X \arrow[r, "\phi"] & Y
\end{tikzcd}
$$

We may extend this to:

$$
\begin{tikzcd}
K \arrow[r] \arrow[dd, "k"'] & \mathsf{coker}\,\mathsf{ker}\,\phi k \arrow[dr] & \\
 & & \mathsf{ker}\,\mathsf{coker}\,\phi k \stackrel{\text{def}}{=} \mathsf{ker}\,\pi \arrow[d] \\
X \arrow[rr, "\phi"] \arrow[d] & & Y \arrow[dd, "\pi"] \\
\mathsf{coker}\,\mathsf{ker}\,\pi\phi \arrow[dr] & & \\
 & \mathsf{ker}\,\mathsf{coker}\,\pi\phi \arrow[r] & \mathsf{coker}\,\phi k
\end{tikzcd}
\tag{H.1}
$$

The left vertical sequence might not be exact, since we haven't even assumed that k is monic. The sequence on the right is automatically exact, however, since $\mathsf{ker}\,\mathsf{coker}\,\mathsf{ker}\,\pi \cong$

$\mathsf{ker}\,\pi$ by Proposition Prop. G.0.3. Now suppose that k is a strict monomorphism, which implies $k \cong \mathsf{ker}\,\mathsf{coker}\,k$. Then $k \cong \mathsf{ker}\,\pi\phi$ if and only if the sequence on the left is also exact, which is the middle isomorphism below:

$$k \cong \mathsf{ker}\,\mathsf{coker}\,k \cong \mathsf{ker}\,\mathsf{coker}\,\mathsf{ker}\,\pi\phi \cong \mathsf{ker}\,\pi\phi$$

Now, if ϕ is an isomorphism, then by Proposition Prop. G.0.5, the diagonal arrows in Eq. (H.1) are isomorphisms, and the diagram reduces to the following:

$$\begin{tikzcd}
K \arrow[r, "\phi|_K"] \arrow[d, "k"'] & \phi(K) \arrow[d] \\
X \arrow[r, "\phi"] \arrow[d] & Y \arrow[d] \\
X/K \arrow[r, "\phi'"'] & Y/\phi(K)
\end{tikzcd} \tag{H.2}$$

In this case one finds that $\phi|_K$ and ϕ' are also isomorphisms. To see why, first note that a strict short exact sequence is transported to itself across the identity map. It follows that the composites of the horizontal arrows in the following diagram are identities:

$$\begin{tikzcd}
K \arrow[r, "\phi|_K"] \arrow[d] & \phi(K) \arrow[r, "\phi^{-1}|_K"] \arrow[d] & K \arrow[d] \\
X \arrow[r, "\phi"] \arrow[d] & Y \arrow[r, "\phi^{-1}"] \arrow[d] & X \arrow[d] \\
X/K \arrow[r, "\phi'"'] & Y/\phi(K) \arrow[r, "(\phi^{-1})'"'] & X/K
\end{tikzcd}
\qquad
\begin{tikzcd}
\phi(K) \arrow[r, "\phi^{-1}|_K"] \arrow[d] & K \arrow[r, "\phi|_K"] \arrow[d] & \phi(K) \arrow[d] \\
Y \arrow[r, "\phi^{-1}"] \arrow[d] & X \arrow[r, "\phi"] \arrow[d] & Y \arrow[d] \\
Y/\phi(K) \arrow[r, "(\phi^{-1})'"'] & X/K \arrow[r, "\phi'"] & Y/\phi(K)
\end{tikzcd}$$

In other words, if k is a strict monomorphism and ϕ is an isomorphism, then the arrows $\phi|_K$ and ϕ' in Eq. (H.2) are also isomorphisms, i.e. Eq. (H.2) is an isomorphism of strict short exact sequences.