

ON THE EFFECTIVE ALGEBRAIC GEOMETRY OF DETERMINANTAL VARIETIES

BY

SRIRAM GOPALAKRISHNAN

A THESIS

PRESENTED TO THE UNIVERSITY OF WATERLOO

IN FULFILMENT OF THE

THESIS REQUIREMENT FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

COMPUTER SCIENCE

WATERLOO, ONTARIO, CANADA, 2026

© SRIRAM GOPALAKRISHNAN 2026

EXAMINING COMMITTEE MEMBERSHIP

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

- External Examiners:
- Laurent Busé, Directeur de recherche (Reporter)
Inria Centre, Université Côte d'Azur
 - Carlos D'Andrea, Professor Catedràtic
Departament de Matemàtiques i Informàtica, Universitat de Barcelona
 - Emre Sertöz, Assistant Professor
Mathematical Institute, Universiteit Leiden
 - Gregory Smith, Professor (Reporter)
Department of Mathematics and Statistics, Queen's University
- Supervisors:
- Vincent Neiger, Maître de Conférences
LIP6, Sorbonne Université
 - Ludovic Perret, Professor
EPITA
 - Éric Schost, Professor
Cheriton School of Computer Science, University of Waterloo
- Internal-External Member: Stephen Melczer, Associate Professor
Department of Combinatorics and Optimization, University of Waterloo
- Other Member: Mohab Safey El Din, Professor
LIP6, Sorbonne Université

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

All of the results of this thesis appear in papers that I have (co)authored, as well as works in preparation.

- The content of Chapter 2 is based on joint work with Vincent Neiger and Mohab Safey El Din [GNS23].
- The content of Chapter 3 is based on [Gop25].
- The content of Chapter 4 is based on joint work with Vincent Neiger and Mohab Safey El Din [GNS24].
- The content of Chapter 6 is in preparation for submission.

ABSTRACT

The central objects of study in this thesis are varieties defined by rank deficiencies of matrices with polynomial entries, which are known as determinantal varieties. We consider effective questions about these varieties from two distinct perspectives. The first part of this thesis concerns computational results in the arithmetic complexity model, where basic field operations have unit cost. From classical results on free resolutions of determinantal ideals, we extract information about the syzygy modules of determinantal ideals, and use this information to adapt existing general-purpose Gröbner basis algorithms to determinantal ideals. This leads us to new algorithms to solve zero-dimensional determinantal polynomial systems and polynomial optimisation problems. We give complexity analyses of our algorithms, and in so doing, show that they improve upon the state-of-the-art. The central problem considered in the second part of this thesis is to bound heights of determinantal varieties. By way of new constructions in arithmetic integral geometry, we give exact values for Mahler measures of determinantal resultants. Coupled with a determinantal analogue of the standard u -resultant, this enables us to bound heights of Chow forms of determinantal varieties.

Les objets centraux de cette thèse sont des variétés définies par une chute de rang dans des matrices à entrées polynomiales, appelées « variétés déterminantielles ». Nous abordons les questions effectifs relatives à ces variétés sous deux angles distincts. La première partie de cette thèse porte sur des résultats dans le modèle de complexité arithmétique, où les opérations de base sur les corps ont un coût unitaire. À partir de résultats classiques sur les résolutions libres d'idéaux déterminantiels, nous extrayons des informations sur les modules des syzygies des idéaux déterminantiels, et utilisons ces informations pour adapter des algorithmes existant de bases de Gröbner généralistes aux idéaux déterminantiels. Cela nous conduit à de nouveaux algorithmes permettant de résoudre des systèmes déterminantiels d'équations polynomiales zéro-dimensionnels et des problèmes d'optimisation polynomiale. Nous analysons la complexité de nos algorithmes et démontrons ainsi qu'ils constituent une avancée par rapport à l'état de l'art. Le problème central abordé dans la deuxième partie de cette thèse consiste à borner les hauteurs des variétés déterminantielles. À l'aide de nouvelles constructions en géométrie intégrale arithmétique, nous donnons des valeurs exactes pour les mesures de Mahler des résultants déterminantiels. En y associant un analogue déterminantiel du u -résultant standard, cela nous permet de borner les hauteurs des formes de Chow des variétés déterminantielles.

ACKNOWLEDGEMENTS

First and foremost, thank you to the members of my examining committee for taking the time to read my thesis. My gratitude in particular to Laurent Busé and Greg Smith for reviewing my thesis.

As I would imagine is the case with any kind of academic pursuit, mathematics research is an inherently collaborative process. This is the case not only insofar as the expertise of others is invaluable in gaining insight into difficult problems, but also (and perhaps even more so) in the sense that it would simply not be possible without the personal support of friends, family, advisers, and colleagues – support that I have been undeservedly fortunate to have had over the past several years.

None of the work in this thesis would have been remotely possible had I not had been introduced to symbolic computation and computer algebra by Mohab and Vincent. I consider myself incredibly privileged to have been able to learn such wonderful mathematics from them. I must give particular thanks to Vincent for instilling in me a love for running which I did not know existed, and to Mohab for introducing me to Le Pantalon, where I made memories I will forever look fondly upon.

Research in mathematics, in my experience, is more often than not running headlong into brick walls, an activity that can be incredibly demoralising. I cannot imagine that many advisers would have been willing to allow their students to blindly dive down the rabbit hole of arithmetic intersection theory with little hope of emerging in possession of meaningful new results. I am certain that even fewer advisers would have been as encouraging and supportive as Éric was after over a year had passed with no substantial progress. I remember countless meetings which I entered feeling as though my time spent trying to learn about arithmetic geometry was time wasted, only to leave with a renewed excitement for the subject thanks to Éric's unwavering confidence that something would pan out. Without those meetings, not to mention those in which I spewed incoherent mathematics at Éric on which he diligently took notes, I doubt that my two years at Waterloo would have produced any interesting results, and I am certain that they would have been quite disheartening.

I owe special thanks to Rémi Prébet for many adventures, both in Norway and Marseilles, and to Pierre Pébèreau for being a good friend and always having interesting new ideas to discuss. My gratitude also to those other members of the PolSys team at Sorbonne with whom I had the good fortune of crossing paths: Lorenzo Baldi, Andrew Ferguson, Jorge García Fontán, Robin Kouba, Georgy Scholten, Kevin Tran, Trung Hieu Vu and Thi Xuan Vu.

In Waterloo, I was extremely lucky to have shared a lab with the algorithms and complexity group. In particular, I owe a debt of gratitude to Robert Andrews (and Oliver), whose advice and encouragement were indispensable during the last year of my program, to Enver Aman, Abhibhav Garg, Parth Mittal, Parth Gupta, and Vihan Shah for being wonderful rock climbing partners, to Raymond Liu, John Smith, and Helia Yazdanyar for making 2306H a great place to work, and to the rest of the members of the A&C group for making the lab a friendly and welcoming environment: Arkaprava Choudhury, Mohammad Hossein Ebtehaj, Nosawaru Efemwonkieke, Tom Iagovet, Alfred Mikhael, Matthew Regehr, Remy El Sabeh, Cameron Seth, and Janani Sundaresan.

To my parents, thank you for your constant love and support. To Allison (and Serena), it is impossible to adequately express the gratitude I feel for your support through thick and thin. Without you, this thesis simply would not exist.

TABLE OF CONTENTS

Examining Committee Membership	iii
Author's Declaration	iv
Statement of Contributions	v
Abstract	vi
Acknowledgements	vii
List of Figures	xii
List of Tables	xiii
Introduction	1
Introduction (en français)	9

I Arithmetic complexity

1 Preliminaries	19
1.1 Basic constructions	19
1.1.1 Polynomials and matrices	19
1.1.2 Graded modules	19
1.1.3 Algebra constructions	20
1.1.4 Hilbert functions	20
1.1.5 Syzygies and free resolutions	21
1.2 Signature Gröbner bases	22
1.2.1 Gröbner bases	22
1.2.2 Macaulay matrices	23
1.2.3 The matrix- F_5 algorithm	23
1.3 Genericity	24
1.3.1 Notation	24
1.3.2 Properties	26
2 Comaximal determinantal ideals	27
2.1 Syzygies of determinantal ideals	27
2.1.1 The Gulliksen-Negård complex	27
2.1.2 The case $r = p - 2$	28
2.1.3 The general case	30
2.2 Determinantal matrix- F_5 algorithm	30

2.3	The case $r = p - 2$	32
2.3.1	Higher syzygy modules	32
2.3.2	A refined F_5 algorithm	34
2.4	Complexity in the case $r = p - 2$	35
2.5	Experimental results	36
3	A refined complexity analysis	38
3.1	An explicit Hilbert series	38
3.2	Reverse lexicographic ideals	39
3.2.1	The grevlex staircase of a homogeneous reverse lexicographic ideal . . .	40
3.2.2	Reverse lexicographic determinantal ideals	41
3.3	Determinantal ideals and the Lefschetz properties	43
3.4	Complexity analysis	44
3.4.1	Bounding $\#(\text{LM}_{\prec}(G_{d+1}) \setminus \text{LM}_{\prec}(G_d))$	44
3.4.2	Lower bounds	45
3.4.3	Upper bounds	46
3.4.4	The asymptotic behaviour of $f_{\omega}(p)$	50
4	Maximal minors and critical points	52
4.1	The first syzygies of maximal minors	52
4.1.1	The Eagon-Northcott complex	52
4.1.2	Leading terms of syzygies	53
4.2	Critical points	55
4.3	Complexity analysis	56
4.3.1	New complexity bound	56
4.3.2	Comparison with Lazard's algorithm	60
II Bit complexity		
5	Preliminaries	67
5.1	Algebraic constructions	67
5.1.1	The algebraic Chow ring	67
5.1.2	Functoriality	68
5.1.3	Algebraic vector bundles	69
5.1.4	Grassmann bundles	70
5.1.5	Algebraic Chern classes	71
5.2	Arithmetic constructions	72
5.2.1	Forms and currents	72
5.2.2	The arithmetic Chow ring	74
5.2.3	Arithmetic Chern classes	75
5.2.4	Degree maps	76
5.2.5	The cycle pairing	77
5.2.6	Heights	78
5.2.7	Arithmetic Schubert calculus	79
6	Heights of determinantal varieties	82

6.1	The determinantal resultant	82
6.1.1	Busé's construction	82
6.1.2	A different perspective	83
6.1.3	An example	85
6.1.4	The proof of Theorem 6.1.2	87
6.1.5	The determinantal u -resultant	88
6.2	Principal determinantal resultants	89
6.2.1	Pulling back the quotient bundle	89
6.2.2	Consequences	92
6.2.3	An example	96
6.3	Higher corank conditions	96
6.3.1	Pulling back the quotient bundle	96
6.3.2	Consequences	97
6.3.3	An example	100
6.3.4	Heights of determinantal varieties	103

Bibliography	104
---------------------	------------

LIST OF FIGURES

4.1	Speedup of Algorithm 4. Top: $p = 3$; bottom: $p = 4$	62
4.2	Speedup of an algorithm which computes full-rank Macaulay matrices. Top: $p = 3$; bottom: $p = 4$	63
4.3	Speedup of Algorithm 4. Top: $d_0 = 3$; bottom: $d_0 = 4$	64
4.4	Speedup of an algorithm which computes full-rank Macaulay matrices. Top: $d_0 = 3$; bottom: $d_0 = 4$	65

LIST OF TABLES

2.1	Reductions to zero in standard F_5 (there is none in determinantal- F_5) as well as ratio of timings for standard F_5 compared to determinantal- F_5 , when computing a D -Gröbner basis for the system of $(r + 1)$ -minors of a generic $p \times p$ matrix of homogeneous linear forms in n variables over $\mathbb{k} = \mathbb{F}_{65521}$	37
3.1	The asymptotics of $f_\omega(p)$ compared to $p^{2\omega+3}$ for various $2 \leq \omega \leq 3$	51

INTRODUCTION

For as long as humans have been sentient, we have sought to understand the universe and our place in it. Why is there something rather than nothing? Does free will exist? Is cereal a soup? Finding these questions far too difficult to answer, we instead turn our attention, in this thesis, to the effective algebraic geometry of determinantal varieties. Algebraic geometry concerns itself, broadly speaking, with the study of solutions to polynomial equations and polynomial maps between such sets. Effective algebraic geometry concerns itself with algorithms to compute properties of such solutions sets. This thesis concerns itself with the design and analysis of algorithms to solve polynomial systems which arise as the minors of a fixed size of a matrix of polynomials.

Data structures and algorithms to compute numerically with algebro-geometric objects are an active area of research, and numerical methods to solve polynomial systems have shown remarkable efficiency in practice (see e.g. [BT18, Ver99, BSHW13, SVW05]). Such methods however, are, by their very nature, susceptible to error, and cannot work over fields of positive characteristic.

On the other side of the coin is symbolic computation, which treats constants as exact, symbolic values. As such, it incurs a potentially much higher computational cost, though it is not susceptible to error and works over fields of arbitrary characteristic. Our focus in this thesis is on the design and analysis of symbolic algorithms to solve polynomial systems.

The main contributions of this thesis can be most naturally divided into two distinct parts – results concerning the arithmetic complexity of solving determinantal polynomial systems, and those concerning the bit sizes of solutions to such systems.

DETERMINANTAL POLYNOMIAL SYSTEMS

Let $\mathbb{k}$ be a field, and fix an algebraic closure $\overline{\mathbb{k}}$ of $\mathbb{k}$. Let $\mathbb{k}[x_1, \dots, x_n]$ be the ring of polynomials in n variables with coefficients in $\mathbb{k}$. Consider a $p \times q$ matrix of polynomials

$$M = \begin{pmatrix} f_{1,1} & f_{1,2} & \cdots & f_{1,q} \\ f_{2,1} & f_{2,2} & \cdots & f_{2,q} \\ \vdots & \vdots & \ddots & \vdots \\ f_{p,1} & f_{p,2} & \cdots & f_{p,q} \end{pmatrix} \in \mathbb{k}[x_1, \dots, x_n]^{p \times q}.$$

Let $0 \leq r < \min\{p, q\}$ be an integer. An $((r+1) \times (r+1))$ -*minor* (or simply $(r+1)$ -*minor*) of M is the determinant of an $(r+1) \times (r+1)$ submatrix of M :

$$\det \begin{pmatrix} f_{i_1, j_1} & f_{i_1, j_2} & \cdots & f_{i_1, j_{r+1}} \\ f_{i_2, j_1} & f_{i_2, j_2} & \cdots & f_{i_2, j_{r+1}} \\ \vdots & \vdots & \ddots & \vdots \\ f_{i_{r+1}, j_1} & f_{i_{r+1}, j_2} & \cdots & f_{i_{r+1}, j_{r+1}} \end{pmatrix}.$$

The collection $F_{r+1}(M)$ of all $(r+1)$ -minors of M is a *determinantal system*. The ideal $\mathcal{I}_{r+1}(M)$ generated by $F_{r+1}(M)$ is called a *determinantal ideal*. If, for $\alpha = (\alpha_1, \dots, \alpha_n) \in \overline{\mathbb{k}}^n$,

we denote

$$M(\alpha) = \begin{pmatrix} f_{1,1}(\alpha_1, \dots, \alpha_n) & f_{1,2}(\alpha_1, \dots, \alpha_n) & \cdots & f_{1,q}(\alpha_1, \dots, \alpha_n) \\ f_{2,1}(\alpha_1, \dots, \alpha_n) & f_{2,2}(\alpha_1, \dots, \alpha_n) & \cdots & f_{2,q}(\alpha_1, \dots, \alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_{p,1}(\alpha_1, \dots, \alpha_n) & f_{p,2}(\alpha_1, \dots, \alpha_n) & \cdots & f_{p,q}(\alpha_1, \dots, \alpha_n) \end{pmatrix},$$

then there is an equality of sets

$$V(F_{r+1}(M)) = \{\alpha \in \overline{\mathbb{K}}^n : \forall f \in F_{r+1}(M), f(\alpha) = 0\} = \{\alpha \in \overline{\mathbb{K}}^n : \text{rank}(M(\alpha)) \leq r\}.$$

It is easy to see that $F_{r+1}(M)$ has cardinality precisely $\binom{p}{r+1} \binom{q}{r+1}$, which, in general, exceeds n . Before proceeding further, it seems prudent, then, to ask if the sets $V(F_{r+1}(M))$ are even nonempty. This depends, of course, on the entries of M , and on n , but in the most general case, there is a simple expression for the dimension of $V(F_{r+1}(M))$ as an algebraic set.

THEOREM ([BV88, Proposition 1.1]). — Let $M = (x_{i,j})_{i,j} \in \mathbb{K}[\{x_{i,j} : 1 \leq i \leq p, 1 \leq j \leq q\}]$ be a matrix of variables. Then for any $0 \leq r < \min\{p, q\}$

$$\text{codim}(V(F_{r+1}(M))) = (p - r)(q - r).$$

This equality turns out to hold even with arbitrary polynomials in place of the variables, provided the polynomials are chosen *generically*.

The natural determinantal analogue of square systems of polynomials is then $n = (p - r)(q - r)$. In this situation, the set $V(F_{r+1}(M))$ is generically finite. In this thesis, we will study systems of the form $F_{r+1}(M)$, with an eye towards improving algorithms for computing $V(F_{r+1}(M))$ – when it is finite – and understanding their complexity.

GRÖBNER BASES

We refer to [CLO15] for a reference textbook on the theory of Gröbner bases. Let $F = (f_1, \dots, f_m) \subseteq \mathbb{K}[x_1, \dots, x_n]$ be a sequence polynomials, let $\mathcal{I}$ be the ideal that they generate, and let $V = V(\mathcal{I})$ be the corresponding variety.

When V is zero-dimensional, it can be computed via the classical two-step polynomial systems solving strategy. This consists in first computing a Gröbner basis for $F_{r+1}(M)$ with respect to the graded reverse lexicographic (grevlex) order, and then using a change of order algorithm to obtain a lexicographic Gröbner basis for $F_{r+1}(M)$, from which the solutions to $F_{r+1}(M)$ can be read off. The focus of the first part of this thesis is on the first part of this process. It is frequently the most expensive of the two (see [FM17, BNS22]).

Evolutions of Buchberger's original Gröbner basis algorithm (see [Buc65]) have led to linear algebra-based algorithms, which originate from the algorithm of Lazard in [Laz83] and include the now standard F_4 and F_5 algorithms (see [Fau99, Fau02]) which have shown their practical efficiency.

These algorithms work by row echelonization of *Macaulay matrices*, whose columns are indexed by the monomials of $\mathbb{K}[x_1, \dots, x_n]$ up to some degree d and sorted in decreasing order (left to right) by the grevlex order, and whose rows store the coefficients of the input polynomials multiplied by the monomials required to reach the degree d . If d is large enough, the echelon form of the corresponding Macaulay matrix yields a Gröbner basis (see [Laz83]). Any bound

INTRODUCTION

on the maximum degree of a polynomial in the reduced grevlex Gröbner basis for $\mathcal{I}$ therefore gives, immediately, a bound on the arithmetic complexity of Lazard's algorithm. Unfortunately, as shown by an example of [MM82, Lemma 8] (see also [Yap91]) this maximum degree can be doubly exponential in n ¹:

THEOREM ([BM93, Proposition 3.11],[Yap91]). — For any n , there exists an ideal of $\mathbb{k}[x_1, \dots, x_n]$ generated by polynomials of degree at most d whose reduced grevlex Gröbner basis contains polynomials of degree $d^{2^{\Omega(n)}}$.

Fortunately for us, the situation is exponentially less dire for Cohen-Macaulay ideals:

THEOREM ([Laz83, Theorem 2]). — If $\mathcal{I} \subseteq \mathbb{k}[x_1, \dots, x_n]$ is a homogeneous ideal generated by m polynomials of degrees $d_1, \dots, d_m$ such that $\mathbb{k}[x_1, \dots, x_n]/\mathcal{I}$ is Cohen-Macaulay, then, after a (generic) linear change of variables, every polynomial of the reduced grevlex Gröbner basis of $\mathcal{I}$ has degree bounded from above by $d_1 + \dots + d_m - m + 1$.

It is worth mentioning that the maximum degree of a polynomial in the reduced grevlex Gröbner basis of $\mathcal{I}$ can be bounded by the *Castelnuovo-Mumford regularity* of the initial ideal of $\mathcal{I}$ (see [Eis05, Chapter 4]). Moreover, by [Eis05, Corollary 4.8], when $\mathcal{I}$ is Cohen-Macaulay, the Castelnuovo-Mumford regularity of $\mathcal{I}$ agrees, up to an additive correction by the dimension of $\mathcal{I}$, with the lowest degree at which the Hilbert function of $\mathcal{I}$ agrees with its Hilbert polynomial. Putting this fact together with the fact that determinantal ideals are generically Cohen-Macaulay (see [BV88, Theorem 2.5]) enables the extraction of a bound on the maximum degree of a polynomial in the grevlex Gröbner basis of a generic determinantal ideal from its Hilbert function.

Successive enhancements of the linear algebra approach to Gröbner basis computations have culminated with the F_5 algorithm [Fau02] (see also [EF16]), which manages to, a priori, discard some rows of the Macaulay matrices which are in the linear span of others, and thus reduce to zero in the echelonization. It has been shown that for regular sequences of polynomials, the so-called F_5 -criterion detects all reductions to zero and F_5 thus computes only full-rank Macaulay matrices.

Reductions to zero in Macaulay matrices are in one-to-one correspondence with syzygies of the input system, and the F_5 criterion precisely captures the Koszul syzygies, coming from the commutativity of polynomial multiplication. This yields asymptotically faster Gröbner basis computations for ideals of complete intersections [BFS15].

Of course, it is not the case that the F_5 -criterion eliminates all reductions to zero on classes of structured polynomial systems, including determinantal ones. Indeed, determinantal varieties are, in general, not complete intersections. This presents both an opportunity (the F_5 algorithm can be adapted to determinantal ideals) and a hint (superfluous computations in F_5 come from syzygies of determinantal ideals).

MAIN RESULTS (PART I)

Within the realm of arithmetic complexity, the research exposited in this thesis has given rise to three articles, all of which in some sense serve to provide partial answers to the following questions:

¹though not much worse than doubly exponential, thanks to [Dub90, Theorem 8.2]

- (i) What shape do the syzygies (or algebraic relations) between the minors of a fixed order of a polynomial matrix take?
- (ii) How can we exploit this structure to create Gröbner basis algorithms which are adapted specifically to determinantal systems?
- (iii) What is the arithmetic complexity of the resulting algorithms we obtain?

First, in [GNS23], an article published at ISSAC 2023, we concentrate on the case of square matrices of linear forms. We analyse the complex of Gulliksen and Negård (see [GN72]), which is a free resolution for $\mathcal{I}_{p-1}(M)$ (provided it is Cohen-Macaulay) to describe the syzygy modules of $\mathcal{I}_{p-1}(M)$. For $r < p - 2$, we use [Kur89, Theorem 5.1] to lift syzygies between the r -minors of the $(r + 1) \times (r + 1)$ submatrices to syzygies between the r -minors of A , thereby reducing the problem of computing syzygies between r -minors in general to the case $r = p - 2$. Equipped with our understanding of these syzygy modules, we then introduce new criteria which avoid reductions to zero when computing Gröbner bases of determinantal ideals of square matrices.

In particular, when $r = p - 2$, $p = q$, and the ideal $\mathcal{I}_{p-1}(M)$ is Cohen-Macaulay, all reductions to zero are avoided. This implies that all linearly redundant rows in the Macaulay matrices can be pruned a priori, leading to faster echelonization. A subsequent complexity bound is given (see Proposition 2.4.2 or [GNS23, Proposition 6.2] for a precise statement and proof):

THEOREM. — Let M be a $p \times p$ matrix of homogeneous linear forms in four variables with coefficients in a field $\mathbb{k}$. There exists an algorithm (see [GNS23, Algorithm 3] or Algorithm 3) to compute the reduced grevlex Gröbner basis of $\mathcal{I}_{p-1}(M)$ which, under suitable genericity assumptions, performs $O(p^{4\omega-1})$ arithmetic operations in $\mathbb{k}$.

This upper bound compares favourably with the best previously-known bound of $O(p^{5\omega+2})$ from [FSS13, Theorem 20].

In [Gop25], a subsequent article published in the Journal of Algebra, we provide an exact formula for the size of the reduced grevlex Gröbner basis of $\mathcal{I}_{p-1}(M)$ (see [Gop25, Theorem 8.3] or Theorem 3.4.3 for a precise statement and proof):

THEOREM. — Let M be a $p \times p$ matrix of homogeneous linear forms in four variables over a field $\mathbb{k}$. Under suitable genericity assumptions and assuming that the ideal $\mathcal{I}_{p-1}(M)$ is reverse lexicographic, the number of elements of $\mathbb{k}$ in the dense representation for the reduced grevlex Gröbner basis of $\mathcal{I}_{p-1}(M)$ is in $\Theta(p^6)$.

In this article, we also sharpen the complexity analysis of the algorithm [GNS23, Algorithm 3] taking into account the specific structure of the Macaulay matrices encountered (see [Gop25, Theorem 8.10] or Theorem 3.4.10) for the precise statement and proof):

THEOREM. — Let M be a $p \times p$ matrix of homogeneous linear forms in four variables over a field $\mathbb{k}$. Under certain genericity assumptions and assuming that the ideal $\mathcal{I}_{p-1}(M)$ is reverse lexicographic, the number of arithmetic operations in $\mathbb{k}$ performed by [GNS23, Algorithm 3] when computing the reduced grevlex Gröbner basis for $\mathcal{I}_{p-1}(M)$ is in $O(p^{2\omega+3})$.

Noting that $2 \leq \omega \leq 3$, we see that the upper bound $O(p^{2\omega+3})$ that we obtain on [GNS23, Algorithm 3] is subquadratic in the size of the output. However, taking, optimistically, $\omega = 2$, which corresponds to being able to compute row-echelon forms of matrices over $\mathbb{k}$ in linear

INTRODUCTION

time, we also see that our upper bound becomes $O(p^7)$, while the size of the output is still p^6 . This suggests that our complexity analysis is still not as sharp as it could be.

Finally, in [GNSED24], an article published at ISSAC 2024, we consider a sequence $F = (f_1, \dots, f_p)$ of polynomials and another polynomial g , all of them in $\mathcal{R}$, and the Jacobian matrix $\text{jac}(g, F)$ associated to g and F . We denote by $\langle F \rangle$ the ideal of $\mathcal{R}$ generated by F . We consider the problem of computing a grevlex Gröbner basis of the ideal

$$\mathcal{I}(g, F) = \langle F \rangle + \mathcal{I}_{p+1}(\text{jac}(g, F)).$$

When $\langle F \rangle$ is radical, is equidimensional of codimension p , and defines a smooth algebraic set $V(F)$ in $\overline{\mathbb{k}}^n$, the algebraic set $V(\mathcal{I}(g, F))$ in $\overline{\mathbb{k}}^n$ defined by $\mathcal{I}(g, F)$ is the set of critical points of the restriction of the polynomial map defined by g to $V(F)$.

We analyse the first syzygy module of the Eagon-Northcott complex (see [EN62]) and exhibit a submodule of its leading terms (with respect to some module order induced by the grevlex monomial order). This has a simple algorithmic consequence: by incrementally computing Gröbner bases of ideals generated by the leftmost entries of the matrix $\text{jac}(g, F)$, one obtains enough information to easily identify a submodule of the one generated by the leading terms of the first syzygy module of $\mathcal{I}(g, F)$. When combined with the syzygy criterion of F_5 (see [EF16, Lemma 6.4] or Proposition 1.2.2), this allows us to, a priori, discard a significant number of rows in the Macaulay matrices that arise when computing critical points. We provide a corresponding complexity analysis and compare it to the best previously known bound given in [Spa14]. Experimental evidence suggests that our new complexity bound could, asymptotically, improve on that given in [Spa14] by a polynomial factor.

ARITHMETIC GEOMETRY

Suppose $F = (f_1, \dots, f_m) \subseteq \mathbb{Q}[x_1, \dots, x_n]$ is a sequence of polynomials defining a variety V of dimension zero. A *rational univariate representation* of V , introduced in [ABRW96, Rou99], is a tuple of polynomials

$$(\nu(t), q(t), p_1(t), \dots, p_n(t)) \subseteq \mathbb{Q}[t]$$

such that, if $\alpha_1, \dots, \alpha_{\deg(\nu(t))}$ denote the (possibly repeated) roots of the *separating polynomial* $\nu(t)$ in an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, then

$$V = \left\{ \left(\frac{p_1(\alpha_j)}{q(\alpha_j)}, \dots, \frac{p_n(\alpha_j)}{q(\alpha_j)} \right) : 1 \leq j \leq \deg(\nu(t)) \right\}.$$

Rational univariate representations are a ubiquitous, efficient data structure used in practice (see, e.g., [BES21, MGH⁺05]) to represent solutions to zero-dimensional polynomial systems. Of note is the fact that the number of points of V is $\deg(V) = \deg(\nu(t))$. This degree is already a good first measure of the complexity of V . Indeed, an algorithm which outputs V must, at a minimum, compute $\deg(\nu(t))$ points. This measure of complexity fits nicely within the arithmetic complexity model that we consider in the first part of this thesis, since we bound the number of arithmetic operations over $\mathbb{k}$ performed by the algorithms that we present, and we treat each such arithmetic operation as having unit cost. In the most general situation, the Thom-Porteous formula (see [Ful98a, Theorem 14.4]) gives an effective way to compute fundamental classes of degeneracy loci, and this can be applied to deduce degree bounds on determinantal varieties (see, e.g., [FSS13, Corollary 11]).

INTRODUCTION

In practice, however, the complexity of V is not completely captured by its size alone. Each point of V may not necessarily be representable, in a computer, using the same number of bits. The main goal of the second part of this thesis is to understand the number of bits required to encode the separating polynomial of a zero-dimensional determinantal variety. This leads to bounds on bit sizes of rational points on determinantal varieties.

The fundamental measure of the complexity of a rational number is its *naïve, logarithmic height*. For $\frac{a}{b} \in \mathbb{Q}$ with $\gcd(a, b) = 1$, $h\left(\frac{a}{b}\right) = \log \max\{|a|, |b|\}$. The degree of V cannot be bounded purely in terms of m and n . Bézout's theorem gives us the bound $\deg(V) \leq \prod_{i=1}^m \deg(f_i)$, and this bound is as sharp as one could hope for in the sense that it is an equality as soon as V is a complete intersection (which generically, it is). Analogously, it is too much to hope for that the maximum naïve logarithmic height of the rational points of V can be bounded in terms of m, n , and $\deg(f_1), \dots, \deg(f_m)$, and the bounds we give additionally take as input a bound τ on the naïve logarithmic heights of the coefficients of the f_i .

The naïve logarithmic height of V makes little sense if V is positive dimensional. It is thus a somewhat unwieldy quantity to work with directly. Instead, we will consider the *Faltings height* of V , first defined in the enormously influential [Fal83]. There are a few equivalent definitions of this height, the most concrete of which is in terms of the Mahler measure of a Chow form of V . Let $\bar{V} \subseteq \mathbb{P}^n$ be the projective closure of V , and let $d = \dim(\bar{V})$. The intersection of $\bar{V}$ with $d + 1$ hyperplanes is generically empty, and the collection of $(d + 1)$ -tuples of hyperplanes whose intersection with $\bar{V}$ is nonempty is a codimension one Zariski closed subset of $(\mathbb{P}^n)^d$. Any polynomial defining this hypersurface is called a *Chow form* of V .

The *Faltings height* of V can then be defined in the following way². Let Φ_V be a Chow form of V , defined over an algebraic extension K of $\mathbb{Q}$ with maximal order $\mathcal{O}_K$. For each maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$, let $u_{\mathfrak{p}}$ be the minimum $\mathfrak{p}$ -adic valuation of the coefficients of Φ_V , and let p be the prime of $\mathbb{Z}$ over which $\mathfrak{p}$ lies. Then

$$h_{\text{Faltings}}(V) = \sum_{\sigma: K \hookrightarrow \mathbb{C}} \int_{(\mathbb{P}_{\mathbb{C}}^n)^d} \log |\Phi_V^{\sigma}| \mu_n^d - \sum_{\mathfrak{p}} u_{\mathfrak{p}} \log |p| + \frac{(d + 1)[K : \mathbb{Q}] \deg(V)}{2} \sum_{i=1}^n \frac{1}{i}$$

where μ_n is the standard probability measure on $\mathbb{P}_{\mathbb{C}}^n$ (that is, the pushforward of the Haar measure on the complex unit sphere $\mathbb{S}^{n+1} \subseteq \mathbb{C}^{n+1}$ under its natural quotient map to $\mathbb{P}_{\mathbb{C}}^n$). This definition is, as one would hope, independent of the choice of Φ_V , as can be seen by routine application of the product formula. The integral appearing in the definition of the Faltings height above is called the *Mahler measure* of Φ_V . The maximum of the naïve logarithmic heights of the coefficients of a polynomial over $\mathbb{Q}$ can be bounded in terms of its Mahler measure (see [KPS01, Lemma 1.1]³), and it is precisely this link which allows us to bound the maximum naïve logarithmic height of a rational point on a zero-dimensional determinantal variety in terms of its Faltings height. Of course, what remains is to bound the Mahler measure of the Chow form of a determinantal variety. This is accomplished via the classical link between the Chow form and the u -resultant, together with a new construction of the determinantal resultant, first defined in [Bus04].

²That this definition agrees with the definition of the Faltings height in terms of the first arithmetic Chern class of the tautological line bundle follows from [BGS94, Theorem 4.3.2] and [BGS94, Lemma 4.3.3]. That it agrees with the original Arakelov-theoretic definition of [Fal83] is essentially the content of [BGS94, Lemma 2.3.2]

³For the case $n = 1$, this is a consequence of Jensen's formula.

INTRODUCTION

MAIN RESULTS (PART II)

The main problem motivating the work in the second part of this thesis is that of bounding the naïve logarithmic height of rational points on determinantal varieties. We approach this problem, as explained above, by giving a bound on the Faltings height of determinantal varieties. Let e, f, r be integers, with $r \leq \min\{e, f\}$. For integers $d_1, \dots, d_f$, and N , let

$$\mathcal{E} = \mathcal{O}_{\mathbb{P}^N}^{\oplus e} \text{ and } \mathcal{F} = \bigoplus_{j=1}^f \mathcal{O}_{\mathbb{P}^N}(d_j).$$

A morphism of vector bundles $\phi \in \text{Hom}(\mathcal{E}, \mathcal{F})$ can be given by an $f \times e$ matrix, the (i, j) entry of which is a homogeneous polynomial in $N + 1$ variables of degree d_j (i.e. a section of $\mathcal{O}_{\mathbb{P}^N}(d_j)$). The locus $M_r(\phi)$ at which ϕ has rank at most r is called a *degeneracy locus*. Its degree is well-understood, thanks to the Thom-Porteous formula (see [Ful98a, Theorem 14.4]). It is evident from its definition (see above) that the crucial missing ingredient required to understand the Faltings height of $M_r(\phi)$ is the Mahler measure of its Chow form. In Chapter 6, we introduce a new object, which we call the *determinantal Chow divisor*. This construction associates, to a cycle Z on $\mathbb{P}^N$, a cycle $\text{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(Z)$ which parametrises morphisms in $\text{Hom}(\mathcal{E}, \mathcal{F})$ which drop in rank to at most r at some point of Z^4 . We link this construction to the determinantal resultant of [Bus04]:

THEOREM (Theorem 6.1.2). — The determinantal Chow divisor of projective space is the divisor of the determinantal resultant of [Bus04].

Next, we introduce a *determinantal u -resultant*, which adapts the standard u -resultant construction to the setting of determinantal varieties. The key (easy) theorem which we prove is that this u -resultant is in fact a Chow form of $M_r(\phi)$ (see Theorem 6.1.6).

The main technical content of Chapter 6 lies in computing the Mahler measure of the determinantal resultant. In the case when $r = e - 1$ and $e \leq f$, this is quite straightforward. The incidence correspondence which we use in our construction of the determinantal Chow divisor is the same as that used to define the usual (generalised) Chow divisor (see [BGS94, 4.3.1, Proposition 4.3.3]). This enables us to prove

THEOREM (Proposition 6.2.3). — For any cycle Z on $\mathbb{P}_{\mathbb{Z}}^N$ of dimension $f - e + 1$,

$$\begin{aligned} h(\text{Ch}_{e,f,e-1,(d_1,\dots,d_f)}^{\det}(Z)) &= \text{esym}_{f-e+1}(d_1, \dots, d_f) h_{\text{Faltings}}(Z) \\ &\quad + \text{esym}_{f-e}(d_1, \dots, d_f) \deg(Z) \sigma_{e-1} \end{aligned}$$

where esym_p is the p^{th} elementary symmetric polynomial, $h(\cdot)$ is the *normalised multiprojective height* (see [BGS94, Definition 4.1.1]), and σ_p , the p^{th} *Stoll number*, is the Faltings height of p -dimensional projective space (see, e.g., [BGS94, Lemma 3.3.1]).

From this theorem, we can deduce exact values for Mahler measures of determinantal resultants. For example, in Section 6.2.3, we show that the exact value of the Mahler measure of the determinantal resultant associated to the maximal minors of a 3×4 matrix of linear forms is $-\frac{57}{10}$.

⁴In particular, when $e = 1$ and $r = 0$, then the determinantal Chow divisor is just the usual (generalised) Chow divisor.

For general r , the situation is more complicated. In this case, the incidence correspondence is no longer the same one as is used to define the usual generalised Chow divisor. Understanding this new incidence correspondence requires us to prove Theorem 6.3.1, which is a generalisation of [BGS94, Proposition 4.3.3].

Using this, we are able to give a (non-closed, but easily computable) formula for the degree (see Proposition 6.3.2) and height (see Proposition 6.3.3) of the determinantal resultant in general. Finally, we apply the general results of [KPS01] to deduce, in Theorem 6.3.6, bounds on heights of rational points on determinantal varieties.

PERSPECTIVES

It is worth mentioning two natural continuations of the work in this thesis.

First, in the realm of arithmetic complexity, some of the work done in [Gop25] to use generic grevlex staircases to analyse the structure of Macaulay matrices could be applied to the situation of regular sequences as well. The F_5 algorithm works by successively row-reducing highly structured matrices. The sharpest existing analysis of the F_5 algorithm is that of [BFS15]. This analysis proceeds first by finding a bound on the number of unreduced rows of each matrix encountered in F_5 (see [BFS15, Theorem 2]), then by finding a bound on the cost of reducing each of these rows. As explained in [BFS15, Section 4], the second step of this analysis is far from sharp. In particular, it does not take into account the sparsity of the rows of the matrices being reduced. This sparsity is closely related to the structure of the Gröbner bases being computed. As such, under the same genericity assumptions of [BFS15], carrying out an analysis similar to the one performed in [Gop25] could yield a finer estimate of the complexity of F_5 . Preliminary work shows that this avenue of research is quite promising, potentially leading to an arithmetic complexity estimate of F_5 which accurately captures its *subcubic* behaviour with respect to the Bézout bound. It remains, however, to find tight closed-form asymptotic bounds on these new sharper estimates – a highly nontrivial step, considering the intricacy of the asymptotic analysis carried out in [BFS15].

Second, our work on heights leaves open many questions. Akin to the way the Schubert calculus which leads to formulæ for the degrees of determinantal varieties can be generalised to prove the Thom-Porteous-Giambelli formula for degrees of degeneracy loci, one might hope that the work in this thesis on heights of determinantal varieties could be used to derive formulæ for heights of degeneracy loci in general. An arithmetic Schubert calculus already exists (see [Mai95, Tam99]), and is a crucial ingredient in our existing work on heights. Moreover, the construction of the determinantal resultant in [Bus04] – which yields the same resultant as our construction in the appropriate setting – already works in remarkable generality and shows that a resultant exists for degeneracy loci under quite mild assumptions. By combining these two, a priori quite disjoint bodies of work, one could hope that an arithmetic analogue of the Thom-Porteous-Giambelli formula might exist. While this generalisation may seem, at first glance, to yield little in the way of practical complexity bounds, the flexibility provided by allowing for arbitrary degeneracy loci would result in bit-size bounds for determinantal varieties built from a more general class of matrices than the ones considered in this work. In particular, this general result could lead to sharp bounds for bit sizes of the outputs of a wide array of polynomial optimisation tasks arising from real-world applications.

INTRODUCTION (EN FRANÇAIS)

Depuis que les humains sont dotés de conscience, nous avons cherché à comprendre l'univers et notre place en son sein. Pourquoi y a-t-il quelque chose plutôt que rien ? Le libre arbitre existe-t-il ? Les céréales au lait sont-elles une soupe ? Trouvant ces questions bien trop difficiles à résoudre, nous tournons plutôt notre attention, dans cette thèse, vers la géométrie algébrique effective des variétés déterminantielles. La géométrie algébrique s'intéresse, en général, à l'étude des solutions d'équations polynomiales et des applications polynomiales entre de tels ensembles. La géométrie algébrique effective s'intéresse aux algorithmes permettant de calculer des propriétés de ces ensembles de solutions. Cette thèse porte sur la conception et l'analyse d'algorithmes permettant de résoudre des systèmes polynomiaux qui apparaissent comme les mineurs d'une taille fixée d'une matrice de polynômes.

Les structures de données et les algorithmes permettant de calculer numériquement avec des objets algébro-géométriques constituent un domaine de recherche actif, et les méthodes numériques de résolution de systèmes polynomiaux ont démontré une efficacité remarquable en pratique (voir par exemple [BT18, Ver99, BSHW13, SVW05]). De telles méthodes sont cependant, par leur nature même, sujettes à des erreurs, et ne fonctionnent pas sur des corps de caractéristique positive.

À l'opposé se trouve le calcul symbolique, qui traite les constantes comme des valeurs exactes et symboliques. Il entraîne ainsi un coût de calcul potentiellement bien plus élevé, mais n'est pas sujet à l'erreur et fonctionne sur des corps de caractéristique arbitraire. Notre attention, dans cette thèse, se porte sur la conception et l'analyse d'algorithmes symboliques pour la résolution de systèmes polynomiaux.

Les contributions principales de cette thèse se répartissent le plus naturellement en deux parties distinctes – des résultats concernant la complexité arithmétique de la résolution de systèmes polynomiaux déterminantiels, et ceux concernant la taille en bits des solutions de tels systèmes.

SYSTÈMES POLYNOMIAUX DÉTERMINANTIELS

Soit $\mathbb{k}$ un corps, et fixons une clôture algébrique $\overline{\mathbb{k}}$ de $\mathbb{k}$. Soit $\mathbb{k}[x_1, \dots, x_n]$ l'anneau des polynômes en n variables à coefficients dans $\mathbb{k}$. Considérons une matrice de polynômes de taille $p \times q$

$$M = \begin{pmatrix} f_{1,1} & f_{1,2} & \cdots & f_{1,q} \\ f_{2,1} & f_{2,2} & \cdots & f_{2,q} \\ \vdots & \vdots & \ddots & \vdots \\ f_{p,1} & f_{p,2} & \cdots & f_{p,q} \end{pmatrix} \in \mathbb{k}[x_1, \dots, x_n]^{p \times q}.$$

INTRODUCTION

Soit $0 \leq r < \min\{p, q\}$ un entier. Un *mineur* $((r+1) \times (r+1))$ (ou simplement *mineur* $(r+1)$) de M est le déterminant d'une sous-matrice $(r+1) \times (r+1)$ de M :

$$\det \begin{pmatrix} f_{i_1, j_1} & f_{i_1, j_2} & \cdots & f_{i_1, j_{r+1}} \\ f_{i_2, j_1} & f_{i_2, j_2} & \cdots & f_{i_2, j_{r+1}} \\ \vdots & \vdots & \ddots & \vdots \\ f_{i_{r+1}, j_1} & f_{i_{r+1}, j_2} & \cdots & f_{i_{r+1}, j_{r+1}} \end{pmatrix}.$$

L'ensemble $F_{r+1}(M)$ de tous les mineurs $(r+1)$ de M est un *système déterminantiel*. L'idéal $\mathcal{I}_{r+1}(M)$ engendré par $F_{r+1}(M)$ est appelé un *idéal déterminantiel*. Si, pour $\alpha = (\alpha_1, \dots, \alpha_n) \in \bar{\mathbb{k}}^n$, on note

$$M(\alpha) = \begin{pmatrix} f_{1,1}(\alpha_1, \dots, \alpha_n) & f_{1,2}(\alpha_1, \dots, \alpha_n) & \cdots & f_{1,q}(\alpha_1, \dots, \alpha_n) \\ f_{2,1}(\alpha_1, \dots, \alpha_n) & f_{2,2}(\alpha_1, \dots, \alpha_n) & \cdots & f_{2,q}(\alpha_1, \dots, \alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_{p,1}(\alpha_1, \dots, \alpha_n) & f_{p,2}(\alpha_1, \dots, \alpha_n) & \cdots & f_{p,q}(\alpha_1, \dots, \alpha_n) \end{pmatrix},$$

alors on a une égalité d'ensembles

$$V(F_{r+1}(M)) = \{\alpha \in \bar{\mathbb{k}}^n : \forall f \in F_{r+1}(M), f(\alpha) = 0\} = \{\alpha \in \bar{\mathbb{k}}^n : \text{rank}(M(\alpha)) \leq r\}.$$

Il est facile de voir que $F_{r+1}(M)$ a pour cardinal exactement $\binom{p}{r+1} \binom{q}{r+1}$, ce qui, en général, excède n . Avant d'aller plus loin, il semble donc prudent de se demander si les ensembles $V(F_{r+1}(M))$ sont ne serait-ce que non vides. Cela dépend, bien entendu, des coefficients de M , ainsi que de n , mais dans le cas le plus général, il existe une expression simple pour la dimension de $V(F_{r+1}(M))$ en tant qu'ensemble algébrique.

THÉORÈME ([BV88, Proposition 1.1]). — Soit $M = (x_{i,j})_{i,j} \in \mathbb{k}[\{x_{i,j}\} : 1 \leq i \leq p, 1 \leq j \leq q]$ une matrice de variables. Alors pour tout $0 \leq r < \min\{p, q\}$

$$\text{codim}(V(F_{r+1}(M))) = (p-r)(q-r).$$

Cette égalité se trouve rester vraie même en remplaçant les variables par des polynômes arbitraires, pourvu que ces polynômes soient choisis de manière *générique*.

L'analogue déterminantiel naturel des systèmes polynomiaux carrés est alors donné par $n = (p-r)(q-r)$. Dans cette situation, l'ensemble $V(F_{r+1}(M))$ est génériquement fini. Dans cette thèse, nous étudierons des systèmes de la forme $F_{r+1}(M)$, dans le but d'améliorer les algorithmes de calcul de $V(F_{r+1}(M))$ – lorsque cet ensemble est fini – et de comprendre leur complexité.

BASES DE GRÖBNER

Nous renvoyons à [CLO15] pour un ouvrage de référence sur la théorie des bases de Gröbner. Soit $F = (f_1, \dots, f_m) \subseteq \mathbb{k}[x_1, \dots, x_n]$ une suite de polynômes, soit $\mathcal{I}$ l'idéal qu'ils engendrent, et soit $V = V(\mathcal{I})$ la variété correspondante.

Lorsque V est de dimension zéro, elle peut être calculée au moyen de la stratégie classique en deux étapes de résolution de systèmes polynomiaux. Celle-ci consiste à calculer d'abord une base de Gröbner de $F_{r+1}(M)$ relativement à l'ordre lexicographique gradué inverse (grevlex), puis

INTRODUCTION

à utiliser un algorithme de changement d'ordre pour obtenir une base de Gröbner lexicographique de $F_{r+1}(M)$, à partir de laquelle les solutions de $F_{r+1}(M)$ peuvent être lues directement. La première partie de cette thèse porte sur la première étape de ce processus. C'est fréquemment la plus coûteuse des deux (voir [FM17, BNS22]).

Les évolutions de l'algorithme original de Buchberger pour le calcul de bases de Gröbner (voir [Buc65]) ont donné naissance à des algorithmes fondés sur l'algèbre linéaire, issus de l'algorithme de Lazard dans [Laz83], et incluant les algorithmes désormais classiques F_4 et F_5 (voir [Fau99, Fau02]), qui ont fait la preuve de leur efficacité pratique.

Ces algorithmes procèdent par échelonnement des *matrices de Macaulay*, dont les colonnes sont indexées par les monômes de $\mathbb{k}[x_1, \dots, x_n]$ jusqu'à un certain degré d et triées par ordre décroissant (de gauche à droite) selon l'ordre grevlex, et dont les lignes contiennent les coefficients des polynômes d'entrée multipliés par les monômes nécessaires pour atteindre le degré d . Si d est suffisamment grand, la forme échelonnée de la matrice de Macaulay correspondante fournit une base de Gröbner (voir [Laz83]). Toute borne sur le degré maximal d'un polynôme de la base de Gröbner grevlex réduite de $\mathcal{I}$ donne donc, immédiatement, une borne sur la complexité arithmétique de l'algorithme de Lazard. Malheureusement, comme le montre un exemple de [MM82, Lemma 8] (voir aussi [Yap91]), ce degré maximal peut être doublement exponentiel en n^5 :

THÉORÈME ([BM93, Proposition 3.11],[Yap91]). — Pour tout n , il existe un idéal de $\mathbb{k}[x_1, \dots, x_n]$ engendré par des polynômes de degré au plus d dont la base de Gröbner grevlex réduite contient des polynômes de degré $d^{2^{\Omega(n)}}$.

Heureusement pour nous, la situation est exponentiellement moins dramatique pour les idéaux de Cohen-Macaulay :

THÉORÈME ([Laz83, Theorem 2]). — Si $\mathcal{I} \subseteq \mathbb{k}[x_1, \dots, x_n]$ est un idéal homogène engendré par m polynômes de degrés $d_1, \dots, d_m$ tels que $\mathbb{k}[x_1, \dots, x_n]/\mathcal{I}$ soit Cohen-Macaulay, alors, après un changement de variables linéaire (générique), tout polynôme de la base de Gröbner grevlex réduite de $\mathcal{I}$ a un degré majoré par $d_1 + \dots + d_m - m + 1$.

Il convient de mentionner que le degré maximal d'un polynôme de la base de Gröbner grevlex réduite de $\mathcal{I}$ peut être majoré par la *régularité de Castelnuovo-Mumford* de l'idéal initial de $\mathcal{I}$ (voir [Eis05, Chapter 4]). De plus, d'après [Eis05, Corollary 4.8], lorsque $\mathcal{I}$ est Cohen-Macaulay, la régularité de Castelnuovo-Mumford de $\mathcal{I}$ coïncide, à une correction additive près liée à la dimension de $\mathcal{I}$, avec le plus petit degré à partir duquel la fonction de Hilbert de $\mathcal{I}$ coïncide avec son polynôme de Hilbert. En combinant ce fait avec celui que les idéaux déterminantiels sont génériquement Cohen-Macaulay (voir [BV88, Theorem 2.5]), on peut extraire une borne sur le degré maximal d'un polynôme de la base de Gröbner grevlex d'un idéal déterminantiel générique à partir de sa fonction de Hilbert.

Les améliorations successives de l'approche par algèbre linéaire du calcul de bases de Gröbner ont culminé avec l'algorithme F_5 [Fau02] (voir aussi [EF16]), qui parvient, a priori, à écarter certaines lignes des matrices de Macaulay se trouvant dans l'espace engendré par les autres, et donc à se réduire à zéro lors de l'échelonnement. Il a été démontré que, pour des suites régulières de polynômes, le critère dit de F_5 détecte toutes les réductions à zéro, de sorte que F_5 ne calcule que des matrices de Macaulay de rang plein.

⁵bien que pas beaucoup plus grand que doublement exponentiel, grâce à [Dub90, Theorem 8.2]

Les réductions à zéro dans les matrices de Macaulay sont en bijection avec les syzygies du système d'entrée, et le critère F_5 capture précisément les syzygies de Koszul, issues de la commutativité de la multiplication polynomiale. Cela conduit à des calculs de bases de Gröbner asymptotiquement plus rapides pour les idéaux d'intersections complètes [BFS15].

Bien entendu, il n'est pas vrai que le critère F_5 élimine toutes les réductions à zéro pour les classes de systèmes polynomiaux structurés, y compris les systèmes déterminantiels. En effet, les variétés déterminantielles ne sont, en général, pas des intersections complètes. Cela constitue à la fois une opportunité (l'algorithme F_5 peut être adapté aux idéaux déterminantiels) et un indice (les calculs superflus dans F_5 proviennent des syzygies des idéaux déterminantiels).

RÉSULTATS PRINCIPAUX (PARTIE I)

Dans le domaine de la complexité arithmétique, les travaux de recherche exposés dans cette thèse ont donné lieu à trois articles, qui contribuent tous, dans une certaine mesure, à apporter des réponses partielles aux questions suivantes :

- (i) Quelle forme prennent les syzygies (ou relations algébriques) entre les mineurs d'un ordre fixé d'une matrice polynomiale ?
- (ii) Comment exploiter cette structure pour créer des algorithmes de calcul de bases de Gröbner spécifiquement adaptés aux systèmes déterminantiels ?
- (iii) Quelle est la complexité arithmétique des algorithmes que nous obtenons ainsi ?

Tout d'abord, dans [GNS23], un article publié à ISSAC 2023, nous nous concentrons sur le cas des matrices carrées de formes linéaires. Nous analysons le complexe de Gulliksen et Negård (voir [GN72]), qui est une résolution libre de $\mathcal{I}_{p-1}(M)$ (à condition qu'il soit Cohen-Macaulay) permettant de décrire les modules de syzygies de $\mathcal{I}_{p-1}(M)$. Pour $r < p - 2$, nous utilisons [Kur89, Theorem 5.1] pour relever les syzygies entre les mineurs d'ordre r des sous-matrices $(r + 1) \times (r + 1)$ en des syzygies entre les mineurs d'ordre r de A , réduisant ainsi le problème du calcul des syzygies entre mineurs d'ordre r en général au cas $r = p - 2$. Munis de cette compréhension des modules de syzygies, nous introduisons alors de nouveaux critères permettant d'éviter les réductions à zéro lors du calcul de bases de Gröbner d'idéaux déterminantiels de matrices carrées.

En particulier, lorsque $r = p - 2$, $p = q$, et que l'idéal $\mathcal{I}_{p-1}(M)$ est Cohen-Macaulay, toutes les réductions à zéro sont évitées. Cela implique que toutes les lignes linéairement redondantes des matrices de Macaulay peuvent être élaguées a priori, ce qui accélère l'échelonnement. Une borne de complexité s'ensuit (voir Proposition 2.4.2 ou [GNS23, Proposition 6.2] pour un énoncé et une preuve précis) :

THÉORÈME. — Soit M une matrice $p \times p$ de formes linéaires homogènes en quatre variables à coefficients dans un corps $\mathbb{k}$. Il existe un algorithme (voir [GNS23, Algorithm 3] ou Algorithm 3) permettant de calculer la base de Gröbner grevlex réduite de $\mathcal{I}_{p-1}(M)$ qui, sous des hypothèses de généricité adéquates, effectue $O(p^{4\omega-1})$ opérations arithmétiques dans $\mathbb{k}$.

Cette borne supérieure se compare favorablement à la meilleure borne précédemment connue, à savoir $O(p^{5\omega+2})$, issue de [FSS13, Theorem 20].

Dans [Gop25], un article ultérieur publié dans le Journal of Algebra, nous fournissons une formule exacte pour la taille de la base de Gröbner grevlex réduite de $\mathcal{I}_{p-1}(M)$ (voir [Gop25, Theorem 8.3] ou Theorem 3.4.3 pour un énoncé et une preuve précis) :

INTRODUCTION

THÉORÈME. — Soit M une matrice $p \times p$ de formes linéaires homogènes en quatre variables sur un corps $\mathbb{k}$. Sous des hypothèses de généricité adéquates, et en supposant que l'idéal $\mathcal{I}_{p-1}(M)$ soit lexicographique inverse, le nombre d'éléments de $\mathbb{k}$ dans la représentation dense de la base de Gröbner grevlex réduite de $\mathcal{I}_{p-1}(M)$ est dans $\Theta(p^6)$.

Dans cet article, nous affinons également l'analyse de complexité de l'algorithme [GNS23, Algorithm 3] en tenant compte de la structure spécifique des matrices de Macaulay rencontrées (voir [Gop25, Theorem 8.10] ou Theorem 3.4.10 pour un énoncé et une preuve précis) :

THÉORÈME. — Soit M une matrice $p \times p$ de formes linéaires homogènes en quatre variables sur un corps $\mathbb{k}$. Sous certaines hypothèses de généricité, et en supposant que l'idéal $\mathcal{I}_{p-1}(M)$ soit lexicographique inverse, le nombre d'opérations arithmétiques dans $\mathbb{k}$ effectuées par [GNS23, Algorithm 3] lors du calcul de la base de Gröbner grevlex réduite de $\mathcal{I}_{p-1}(M)$ est dans $O(p^{2\omega+3})$.

En remarquant que $2 \leq \omega \leq 3$, on voit que la borne supérieure $O(p^{2\omega+3})$ que nous obtenons sur [GNS23, Algorithm 3] est sous-quadratique en la taille de la sortie. Cependant, en prenant, optimistement, $\omega = 2$, ce qui correspond à pouvoir calculer les formes échelonnées de matrices sur $\mathbb{k}$ en temps linéaire, on voit également que notre borne supérieure devient $O(p^7)$, alors que la taille de la sortie reste p^6 . Cela suggère que notre analyse de complexité n'est pas encore aussi fine qu'elle pourrait l'être.

Enfin, dans [GNS24], un article publié à ISSAC 2024, nous considérons une suite $F = (f_1, \dots, f_p)$ de polynômes ainsi qu'un autre polynôme g , tous appartenant à $\mathcal{R}$, et la matrice jacobienne $\text{jac}(g, F)$ associée à g et F . Nous notons $\langle F \rangle$ l'idéal de $\mathcal{R}$ engendré par F . Nous considérons le problème du calcul d'une base de Gröbner grevlex de l'idéal

$$\mathcal{I}(g, F) = \langle F \rangle + \mathcal{I}_{p+1}(\text{jac}(g, F)).$$

Lorsque $\langle F \rangle$ est radiciel, équidimensionnel de codimension p , et définit un ensemble algébrique lisse $V(F)$ dans $\overline{\mathbb{k}}^n$, l'ensemble algébrique $V(\mathcal{I}(g, F))$ dans $\overline{\mathbb{k}}^n$ défini par $\mathcal{I}(g, F)$ est l'ensemble des points critiques de la restriction à $V(F)$ de l'application polynomiale définie par g .

Nous analysons le premier module de syzygies du complexe d'Eagon-Northcott (voir [EN62]) et exhibons un sous-module de ses termes dominants (relativement à un certain ordre de module induit par l'ordre monomial grevlex). Cela a une conséquence algorithmique simple : en calculant de manière incrémentale les bases de Gröbner des idéaux engendrés par les entrées les plus à gauche de la matrice $\text{jac}(g, F)$, on obtient suffisamment d'information pour identifier facilement un sous-module de celui engendré par les termes dominants du premier module de syzygies de $\mathcal{I}(g, F)$. Combiné au critère de syzygie de F_5 (voir [EF16, Lemma 6.4] ou Proposition 1.2.2), cela nous permet d'écarter a priori un nombre significatif de lignes dans les matrices de Macaulay qui apparaissent lors du calcul des points critiques. Nous fournissons une analyse de complexité correspondante et la comparons à la meilleure borne précédemment connue, donnée dans [Spa14]. Les résultats expérimentaux suggèrent que notre nouvelle borne de complexité pourrait, asymptotiquement, améliorer celle de [Spa14] d'un facteur polynomial.

GÉOMÉTRIE ARITHMÉTIQUE

Supposons que $F = (f_1, \dots, f_m) \subseteq \mathbb{Q}[x_1, \dots, x_n]$ soit une suite de polynômes définissant une variété V de dimension zéro. Une *représentation univariée rationnelle* de V , introduite dans [ABRW96, Rou99], est un uplet de polynômes

$$(\nu(t), q(t), p_1(t), \dots, p_n(t)) \subseteq \mathbb{Q}[t]$$

tel que, si $\alpha_1, \dots, \alpha_{\deg(\nu(t))}$ désignent les racines (éventuellement répétées) du *polynôme séparant* $\nu(t)$ dans une clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$, alors

$$V = \left\{ \left(\frac{p_1(\alpha_j)}{q(\alpha_j)}, \dots, \frac{p_n(\alpha_j)}{q(\alpha_j)} \right) : 1 \leq j \leq \deg(\nu(t)) \right\}.$$

Les représentations univariées rationnelles constituent une structure de données efficace et omniprésente, utilisée en pratique (voir, par exemple, [BES21, MGH⁺05]) pour représenter les solutions de systèmes polynomiaux de dimension zéro. Il convient de noter que le nombre de points de V est $\deg(V) = \deg(\nu(t))$. Ce degré constitue déjà une bonne première mesure de la complexité de V . En effet, un algorithme qui calcule V doit, au minimum, calculer $\deg(\nu(t))$ points. Cette mesure de complexité s'inscrit naturellement dans le modèle de complexité arithmétique que nous considérons dans la première partie de cette thèse, puisque nous bornons le nombre d'opérations arithmétiques sur $\mathbb{k}$ effectuées par les algorithmes que nous présentons, et que nous traitons chaque opération arithmétique comme ayant un coût unitaire. Dans la situation la plus générale, la formule de Thom-Porteous (voir [Ful98a, Theorem 14.4]) fournit un moyen effectif de calculer les classes fondamentales des lieux de dégénérescence, ce qui peut être utilisé pour en déduire des bornes de degré sur les variétés déterminantielles (voir, par exemple, [FSS13, Corollary 11]).

En pratique, cependant, la complexité de V n'est pas entièrement capturée par sa seule taille. Chaque point de V n'est pas nécessairement représentable, dans un ordinateur, à l'aide du même nombre de bits. L'objectif principal de la seconde partie de cette thèse est de comprendre le nombre de bits nécessaires pour encoder le polynôme séparant d'une variété déterminantielle de dimension zéro. Cela conduit à des bornes sur la taille en bits des points rationnels des variétés déterminantielles.

La mesure fondamentale de la complexité d'un nombre rationnel est sa *hauteur logarithmique naïve*. Pour $\frac{a}{b} \in \mathbb{Q}$ avec $\gcd(a, b) = 1$, $h\left(\frac{a}{b}\right) = \log \max\{|a|, |b|\}$. Le degré de V ne peut être borné uniquement en fonction de m et n . Le théorème de Bézout fournit la borne $\deg(V) \leq \prod_{i=1}^m \deg(f_i)$, et cette borne est aussi fine que possible, en ce sens qu'elle est atteinte dès que V est une intersection complète (ce qui, génériquement, est le cas). De même, il est illusoire d'espérer que la hauteur logarithmique naïve maximale des points rationnels de V puisse être bornée uniquement en fonction de m, n , et $\deg(f_1), \dots, \deg(f_m)$, et les bornes que nous donnons prennent également en entrée une borne τ sur les hauteurs logarithmiques naïves des coefficients des f_i .

La hauteur logarithmique naïve de V n'a guère de sens si V est de dimension strictement positive. C'est donc une quantité quelque peu malcommode à manipuler directement. Nous considérerons plutôt la *hauteur de Faltings* de V , définie pour la première fois dans l'article, d'une influence considérable, [Fal83]. Il existe plusieurs définitions équivalentes de cette hauteur, la plus concrète étant en termes de la mesure de Mahler d'une forme de Chow de V . Soit $\overline{V} \subseteq \mathbb{P}^n$ la fermeture projective de V , et soit $d = \dim(\overline{V})$. L'intersection de $\overline{V}$ avec $d + 1$ hyperplans est génériquement vide, et l'ensemble des $(d + 1)$ -uplets d'hyperplans dont l'intersection avec $\overline{V}$ est non vide forme un sous-ensemble de Zariski fermé de codimension un de $(\mathbb{P}^n)^d$. Tout polynôme définissant cette hypersurface est appelé une *forme de Chow* de V .

La *hauteur de Faltings* de V peut alors être définie de la manière suivante⁶. Soit Φ_V une

⁶Le fait que cette définition coïncide avec la définition de la hauteur de Faltings en termes de la première classe de Chern arithmétique du fibré en droites tautologique découle de [BGS94, Theorem 4.3.2] et [BGS94, Lemma 4.3.3]. Le fait qu'elle coïncide avec la définition arakelovienne originale de [Fal83] constitue essentiellement le contenu de [BGS94, Lemma 2.3.2]

INTRODUCTION

forme de Chow de V , définie sur une extension algébrique K de $\mathbb{Q}$ d'anneau des entiers $\mathcal{O}_K$. Pour chaque idéal maximal $\mathfrak{p}$ de $\mathcal{O}_K$, soit $u_{\mathfrak{p}}$ la valuation $\mathfrak{p}$ -adique minimale des coefficients de Φ_V , et soit p le nombre premier de $\mathbb{Z}$ au-dessus duquel se trouve $\mathfrak{p}$. Alors

$$h_{\text{Faltings}}(V) = \sum_{\sigma: K \hookrightarrow \mathbb{C}} \int_{(\mathbb{P}_{\mathbb{C}}^n)^d} \log |\Phi_V^\sigma| \mu_n^d - \sum_{\mathfrak{p}} u_{\mathfrak{p}} \log |p| + \frac{(d+1)[K : \mathbb{Q}] \deg(V)}{2} \sum_{i=1}^n \frac{1}{i}$$

où μ_n désigne la mesure de probabilité standard sur $\mathbb{P}_{\mathbb{C}}^n$ (c'est-à-dire l'image directe de la mesure de Haar sur la sphère unité complexe $\mathbb{S}^{n+1} \subseteq \mathbb{C}^{n+1}$ par son application quotient naturelle vers $\mathbb{P}_{\mathbb{C}}^n$). Cette définition est, comme on l'espère, indépendante du choix de Φ_V , comme on peut le voir par une application de routine de la formule du produit. L'intégrale apparaissant dans la définition de la hauteur de Faltings ci-dessus est appelée la *mesure de Mahler* de Φ_V . Le maximum des hauteurs logarithmiques naïves des coefficients d'un polynôme sur $\mathbb{Q}$ peut être borné en fonction de sa mesure de Mahler (voir [KPS01, Lemma 1.1]⁷), et c'est précisément ce lien qui nous permet de borner la hauteur logarithmique naïve maximale d'un point rationnel d'une variété déterminantielle de dimension zéro en fonction de sa hauteur de Faltings. Bien entendu, il reste alors à borner la mesure de Mahler de la forme de Chow d'une variété déterminantielle. Cela est accompli grâce au lien classique entre la forme de Chow et le u -résultant, ainsi qu'à une nouvelle construction du résultant déterminantiel, défini pour la première fois dans [Bus04].

RÉSULTATS PRINCIPAUX (PARTIE II)

Le problème principal motivant les travaux de la seconde partie de cette thèse est celui de borner la hauteur logarithmique naïve des points rationnels sur les variétés déterminantielles. Nous abordons ce problème, comme expliqué ci-dessus, en établissant une borne sur la hauteur de Faltings des variétés déterminantielles. Soient e, f, r des entiers, avec $r \leq \min\{e, f\}$. Pour des entiers $d_1, \dots, d_f$, et N , posons

$$\mathcal{E} = \mathcal{O}_{\mathbb{P}^N}^{\oplus e} \text{ et } \mathcal{F} = \bigoplus_{j=1}^f \mathcal{O}_{\mathbb{P}^N}(d_j).$$

Un morphisme de fibrés vectoriels $\phi \in \text{Hom}(\mathcal{E}, \mathcal{F})$ peut être donné par une matrice $f \times e$, dont le coefficient (i, j) est un polynôme homogène en $N+1$ variables de degré d_j (c'est-à-dire une section de $\mathcal{O}_{\mathbb{P}^N}(d_j)$). Le lieu $M_r(\phi)$ où ϕ est de rang au plus r est appelé un *lieu de dégénérescence*. Son degré est bien compris, grâce à la formule de Thom-Porteous (voir [Ful98a, Theorem 14.4]). Il ressort clairement de sa définition (voir ci-dessus) que l'ingrédient crucial manquant pour comprendre la hauteur de Faltings de $M_r(\phi)$ est la mesure de Mahler de sa forme de Chow. Dans Chapter 6, nous introduisons un nouvel objet, que nous appelons le *diviseur de Chow déterminantiel*. Cette construction associe, à un cycle Z de $\mathbb{P}^N$, un cycle $\text{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(Z)$ qui paramètre les morphismes de $\text{Hom}(\mathcal{E}, \mathcal{F})$ dont le rang chute à au plus r en un point de Z ⁸. Nous relierons cette construction au résultant déterminantiel de [Bus04] :

THÉORÈME (Theorem 6.1.2). — Le diviseur de Chow déterminantiel de l'espace projectif est le diviseur du résultant déterminantiel de [Bus04].

⁷Pour le cas $n = 1$, ceci est une conséquence de la formule de Jensen.

⁸En particulier, lorsque $e = 1$ et $r = 0$, le diviseur de Chow déterminantiel n'est autre que le diviseur de Chow (généralisé) usuel.

INTRODUCTION

Ensuite, nous introduisons un *u-résultant déterminantiel*, qui adapte la construction usuelle du *u-résultant* au cadre des variétés déterminantielles. Le théorème clé (facile) que nous démontrons est que ce *u-résultant* est en fait une forme de Chow de $M_r(\phi)$ (voir Theorem 6.1.6).

Le contenu technique principal du Chapter 6 réside dans le calcul de la mesure de Mahler du résultant déterminantiel. Dans le cas où $r = e - 1$ et $e \leq f$, ce calcul est assez direct. La condition d'incidence que nous utilisons dans notre construction du diviseur de Chow déterminantiel est la même que celle utilisée pour définir le diviseur de Chow (généralisé) usuel (voir [BGS94, 4.3.1, Proposition 4.3.3]). Cela nous permet de démontrer

THÉORÈME (Proposition 6.2.3). — Pour tout cycle Z de $\mathbb{P}_{\mathbb{Z}}^N$ de dimension $f - e + 1$,

$$h(\text{Ch}_{e,f,e-1,(d_1,\dots,d_f)}^{\det}(Z)) = \text{esym}_{f-e+1}(d_1, \dots, d_f) h_{\text{Faltings}}(Z) \\ + \text{esym}_{f-e}(d_1, \dots, d_f) \deg(Z) \sigma_{e-1}$$

où esym_p désigne le $p^{\text{ième}}$ polynôme symétrique élémentaire, $h(\cdot)$ désigne la *hauteur multiprojective normalisée* (voir [BGS94, Definition 4.1.1]), et σ_p , le $p^{\text{ième}}$ *nombre de Stoll*, est la hauteur de Faltings de l'espace projectif de dimension p (voir, par exemple, [BGS94, Lemma 3.3.1]).

De ce théorème, nous pouvons déduire des valeurs exactes pour les mesures de Mahler de résultants déterminantiels. Par exemple, dans Section 6.2.3, nous montrons que la valeur exacte de la mesure de Mahler du résultant déterminantiel associé aux mineurs maximaux d'une matrice 3×4 de formes linéaires est $-\frac{57}{10}$.

Pour r général, la situation est plus compliquée. Dans ce cas, la condition d'incidence n'est plus la même que celle utilisée pour définir le diviseur de Chow généralisé usuel. Comprendre cette nouvelle condition d'incidence nous oblige à démontrer Theorem 6.3.1, qui est une généralisation de [BGS94, Proposition 4.3.3].

Grâce à cela, nous parvenons à donner une formule (non close, mais aisément calculable) pour le degré (voir Proposition 6.3.2) et la hauteur (voir Proposition 6.3.3) du résultant déterminantiel en général. Enfin, nous appliquons les résultats généraux de [KPS01] pour déduire, dans Theorem 6.3.6, des bornes sur les hauteurs des points rationnels des variétés déterminantielles.

PERSPECTIVES

Il convient de mentionner deux prolongements naturels des travaux de cette thèse.

Premièrement, dans le domaine de la complexité arithmétique, une partie des travaux menés dans [Gop25], qui utilisent des escaliers grevlex génériques pour analyser la structure des matrices de Macaulay, pourrait également être appliquée au cas des suites régulières. L'algorithme F_5 procède par réductions successives par lignes de matrices hautement structurées. L'analyse la plus fine existante de l'algorithme F_5 est celle de [BFS15]. Cette analyse procède d'abord en trouvant une borne sur le nombre de lignes non réduites de chaque matrice rencontrée dans F_5 (voir [BFS15, Theorem 2]), puis en trouvant une borne sur le coût de réduction de chacune de ces lignes. Comme expliqué dans [BFS15, Section 4], la seconde étape de cette analyse est loin d'être optimale. En particulier, elle ne tient pas compte de la parcimonie des lignes des matrices réduites. Cette parcimonie est étroitement liée à la structure des bases de Gröbner calculées. Ainsi, sous les mêmes hypothèses de généricité que [BFS15], mener une analyse similaire à celle réalisée dans [Gop25] pourrait fournir une estimation plus fine de la complexité de F_5 . Des travaux préliminaires montrent que cette piste de recherche est très prometteuse, et pourrait conduire à une estimation de la complexité arithmétique de F_5 capturant avec précision son

INTRODUCTION

comportement *sous-cubique* par rapport à la borne de Bézout. Il reste néanmoins à trouver des bornes asymptotiques closes et fines pour ces nouvelles estimations plus précises – une étape hautement non triviale, compte tenu de la complexité de l’analyse asymptotique menée dans [BFS15].

Deuxièmement, nos travaux sur les hauteurs laissent de nombreuses questions ouvertes. À l’instar de la manière dont le calcul de Schubert, qui conduit aux formules pour les degrés des variétés déterminantielles, peut être généralisé pour démontrer la formule de Thom-Porteous-Giambelli pour les degrés des lieux de dégénérescence en général, on pourrait espérer que les travaux de cette thèse sur les hauteurs des variétés déterminantielles puissent être utilisés pour établir des formules pour les hauteurs des lieux de dégénérescence en général. Un calcul de Schubert arithmétique existe déjà (voir [Mai95, Tam99]), et constitue un ingrédient essentiel de nos travaux existants sur les hauteurs. De plus, la construction du résultant déterminantiel dans [Bus04] – qui produit le même résultant que notre construction dans le cadre approprié – fonctionne déjà avec une généralité remarquable et montre qu’un résultant existe pour les lieux de dégénérescence sous des hypothèses assez faibles. En combinant ces deux corps de travaux, a priori assez disjoints, on pourrait espérer qu’un analogue arithmétique de la formule de Thom-Porteous-Giambelli existe. Bien que cette généralisation puisse sembler, à première vue, n’apporter que peu de bornes de complexité pratiques, la flexibilité offerte par la prise en compte de lieux de dégénérescence arbitraires conduirait à des bornes sur la taille en bits pour des variétés déterminantielles construites à partir d’une classe de matrices plus générale que celles considérées dans ce travail. En particulier, ce résultat général pourrait conduire à des bornes fines pour la taille en bits des sorties d’un large éventail de tâches d’optimisation polynomiale issues d’applications concrètes.

PART I

ARITHMETIC COMPLEXITY

PRELIMINARIES

The notation used throughout the first part of this thesis is introduced here. We begin by recalling some basic notions coming from commutative algebra. We then turn our attention to *signature Gröbner bases*, which enrich regular Gröbner bases with some extra data identifying the input polynomial from which each element of the Gröbner basis came from. We conclude with the (unfortunately rather onerous) framework we use to formalise the notion of *genericity*.

1.1 BASIC CONSTRUCTIONS

1.1.1 POLYNOMIALS AND MATRICES

We denote by $\mathcal{R}_n = \mathbb{k}[x_1, \dots, x_n]$ the ring of polynomials in n indeterminates over $\mathbb{k}$. For a module $\mathcal{M}$ over a ring $\mathcal{R}$ and a subset $F \subseteq \mathcal{M}$, we denote by $\langle\langle F \rangle\rangle$ the $\mathcal{R}$ -submodule of $\mathcal{M}$ generated by F . In particular, if $\mathcal{M} = \mathcal{R}$, so that $F \subseteq \mathcal{R}$ is a collection of elements of $\mathcal{R}$, the $\mathcal{R}$ -submodule $\langle\langle F \rangle\rangle$ of $\mathcal{R}$ is the ideal $\langle F \rangle$ of $\mathcal{R}$ generated by F .

For $\alpha \in \mathbb{Z}_{\geq 0}^n$, we take $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in \mathcal{R}_n$. For $d \in \mathbb{Z}_{\geq 0}$, we denote by $\text{Mon}_d(\mathcal{R}_n)$ the set of monomials of $\mathcal{R}_n$ of degree d .

For a ring $\mathcal{R}$, we will denote by $\mathcal{R}^{p \times q}$ the set of matrices with p rows and q columns with entries in $\mathcal{R}$; this is a free $\mathcal{R}$ -module of rank $p \cdot q$. Let $M \in \mathcal{R}^{p \times q}$, and let $r \in \{1, \dots, \min(p, q)\}$. Let $1 \leq i_1 < \dots < i_r \leq p$ and $1 \leq j_1 < \dots < j_r \leq q$ be two strictly increasing sequences of integers. We denote by $[i_1 \cdots i_r \mid j_1 \cdots j_r]_A$ the $r \times r$ submatrix of M with rows indexed by $(i_1, \dots, i_r)$ and columns indexed by $(j_1, \dots, j_r)$. We denote by $F_{r+1}(M)$ the subset of $\mathcal{R}$ consisting of the minors of M of size $r \times r$, and by $\mathcal{I}_{r+1}(M) = \langle F_{r+1}(M) \rangle$ the ideal of $\mathcal{R}$ generated by $F_{r+1}(M)$.

1.1.2 GRADED MODULES

A ring $\mathcal{R}$ is called *graded* if, for each integer $d \geq 0$, there exist additive abelian groups $\mathcal{R}_{[d]}$ such that $\mathcal{R} = \bigoplus_{d=0}^{\infty} \mathcal{R}_{[d]}$ and $\mathcal{R}_{[d]} \mathcal{R}_{[e]} \subseteq \mathcal{R}_{[d+e]}$. The elements of $\mathcal{R}_{[d]}$ are called the *homogeneous elements of degree d* . Our prototypical example of a graded ring will be the ring $\mathcal{R}_n$. Here, $\mathbb{k}[x_1, \dots, x_n]_{[d]}$ consists of the homogeneous polynomials of degree d (together with 0, which is, by definition, homogeneous of every degree).

A module $\mathcal{M}$ over a graded ring $\mathcal{R}$ is called *graded* if, for each $d \geq 0$, there exist abelian groups $\mathcal{M}_{[d]}$ such that $\mathcal{M} = \bigoplus_{d=0}^{\infty} \mathcal{M}_{[d]}$ and $\mathcal{R}_{[d]} \mathcal{M}_{[e]} \subseteq \mathcal{M}_{[d+e]}$. For an integer $s \geq 1$, $\mathcal{R}^s$ naturally carries the structure of a free $\mathcal{R}$ -module of rank s . We take as a basis for $\mathcal{R}^s$ the standard basis vectors $\{e_i : 1 \leq i \leq s\}$. If $\mathcal{R}$ is graded, it induces a natural grading on all free modules $\mathcal{R}^s$. For a graded module $\mathcal{M}$ and $e \in \mathbb{Z}$, we denote by $\mathcal{M}(e)$ the module $\mathcal{M}$ with the grading such that $\mathcal{M}(e)_{[d]} = \mathcal{M}_{[d+e]}$.

For $s \in \mathbb{Z}_{>0}$, we call an element of $\mathcal{R}_n^s$ a *monomial* if it takes the form $x^\alpha e_i$ for some $\alpha \in \mathbb{Z}_{\geq 0}^n$ and $1 \leq i \leq s$. Note that $\mathcal{R}_n$ is naturally graded by degree and thus so is $\mathcal{R}_n^s$. We denote by $\text{Mon}_d(\mathcal{R}_n^s)$ the set of all monomials of $\mathcal{R}_n^s$ of degree d .

1.1.3 ALGEBRA CONSTRUCTIONS

The *tensor algebra* of a module $\mathcal{M}$ over a ring $\mathcal{R}$ is denoted $T(\mathcal{M})$ and is defined by $T(\mathcal{M}) = \bigoplus_{d=0}^{\infty} \mathcal{M}^{\otimes d}$. Explicitly, for pure tensors $f_1 \otimes \cdots \otimes f_d \in \mathcal{M}^{\otimes d}$ and $g_1 \otimes \cdots \otimes g_e \in \mathcal{M}^{\otimes e}$ of ranks d and e respectively, we have

$$(f_1 \otimes \cdots \otimes f_d) \cdot (g_1 \otimes \cdots \otimes g_e) = f_1 \otimes \cdots \otimes f_d \otimes g_1 \otimes \cdots \otimes g_e \in \mathcal{M}^{\otimes(d+e)}.$$

The algebra $T(\mathcal{M})$ carries a natural grading as a ring, wherein its homogeneous part of degree d is precisely the $\mathcal{R}$ -module $\mathcal{M}^{\otimes d}$.

PROPOSITION 1.1.1 ([Eis95, Corollary A2.3]). — Let $\mathcal{R}$ be a ring and let $\mathcal{M}$ be a finite free $\mathcal{R}$ -module with basis $e_1, \dots, e_s$. Then for any integer $d \geq 1$, $\mathcal{M}^{\otimes d}$ is a free module of rank s^d and the set $\{e_{i_1} \otimes \cdots \otimes e_{i_d} : 1 \leq i_1, \dots, i_d \leq s\}$ is an $\mathcal{R}$ -basis for $\mathcal{M}^{\otimes d}$.

The *symmetric algebra* $\text{Sym}(\mathcal{M})$ of a module $\mathcal{M}$ over a ring $\mathcal{R}$ is simply the quotient $T(\mathcal{M})/\langle u \otimes v - v \otimes u : u, v \in \mathcal{M} \rangle$. The grading on $T(\mathcal{M})$ naturally induces a grading on $\text{Sym}(\mathcal{M})$, wherein the homogeneous part of degree d of $\text{Sym}(\mathcal{M})$ is called the *d-th symmetric power of $\mathcal{M}$* and is denoted $\text{Sym}_d(\mathcal{M})$.

The *exterior algebra* of a module $\mathcal{M}$ over a ring $\mathcal{R}$ is denoted $\bigwedge(\mathcal{M})$ and is defined by $\bigwedge(\mathcal{M}) = T(\mathcal{M})/\langle x \otimes x : x \in \mathcal{M} \rangle$. We denote by $f_1 \wedge \cdots \wedge f_d$ the image of the pure tensor $f_1 \otimes \cdots \otimes f_d$ in $\bigwedge(\mathcal{M})$. The grading on $T(\mathcal{M})$ described above naturally induces a grading on $\bigwedge(\mathcal{M})$. In this case, the homogeneous part of degree d of $\bigwedge(\mathcal{M})$ is called the *d-th exterior power of $\mathcal{M}$* and is denoted $\bigwedge^d(\mathcal{M})$. As in the case of $\mathcal{M}^{\otimes d}$, the abelian group $\bigwedge^d(\mathcal{M})$ naturally carries the structure of an $\mathcal{R}$ -module.

PROPOSITION 1.1.2 ([Eis95, Corollary A2.3]). — Let $\mathcal{R}$ be a ring and let $\mathcal{M}$ be a finite free $\mathcal{R}$ -module with basis $e_1, \dots, e_s$. Then for any integer $d \geq 1$, $\bigwedge^d(\mathcal{M})$ is a free module of rank $\binom{s}{d}$ and the set $\{e_{i_1} \otimes \cdots \otimes e_{i_d} : 1 \leq i_1 < \cdots < i_d \leq s\}$ is an $\mathcal{R}$ -basis for $\bigwedge^d(\mathcal{M})$.

For a module $\mathcal{M}$ over a ring $\mathcal{R}$, we denote by $\mathcal{M}^\vee = \text{Hom}(\mathcal{M}, \mathcal{R})$ the *dual module* of $\mathcal{M}$. A sequence $(f_1, \dots, f_s) \subseteq \mathcal{R}$ is said to be *$\mathcal{M}$ -regular* if f_1 is not a zero-divisor in $\mathcal{M}$, for all $2 \leq i \leq s$, f_i is not a zero-divisor in $\mathcal{M}/\langle f_1, \dots, f_{i-1} \rangle$, and $(f_1, \dots, f_s)\mathcal{M} \neq \mathcal{M}$. If $\mathcal{I}$ is an ideal of $\mathcal{R}$, the *grade of $\mathcal{I}$ with respect to $\mathcal{M}$* , denoted $\text{grade}(\mathcal{I}, \mathcal{M})$ is the length of a maximal $\mathcal{M}$ -regular sequence of elements of $\mathcal{I}$. We take $\text{grade}(\mathcal{I}) = \text{grade}(\mathcal{I}, \mathcal{R})$.

1.1.4 HILBERT FUNCTIONS

For a graded module $\mathcal{M}$ over $\mathcal{R}_n$ equipped with its natural grading by degree, the *Hilbert function* of $\mathcal{M}$ is defined by $\text{HF}_{\mathcal{M}}(d) = \dim_{\mathbb{k}}(\mathcal{M}_d)$. The *Hilbert series* $H_{\mathcal{M}}(t) = \sum_{d \geq 0} \text{HF}_{\mathcal{M}}(d)t^d \in \mathbb{Z}[[t]]$ of $\mathcal{M}$ is the generating function of $\text{HF}_{\mathcal{M}}(d)$.

THEOREM 1.1.3. — [Eis95, Theorem 1.1] If $\mathcal{M}$ is a finitely generated graded module over $\mathcal{R}_n$, then $\text{HF}_{\mathcal{M}}(d)$ is, for sufficiently large d , a polynomial $P_{\mathcal{M}}(d)$ of degree at most $n - 1$.

Pursuant to Theorem 1.1.3, the polynomial $P_{\mathcal{M}}(d)$ is called the *Hilbert polynomial* of d . The *Hilbert regularity* of $\mathcal{M}$, is the smallest integer d such that for all $d' \geq d$, $\text{HF}_{\mathcal{M}}(d') = P_{\mathcal{M}}(d')$.

PRELIMINARIES

1.1.5 SYZYGIES AND FREE RESOLUTIONS

Free resolutions are a fundamental construction, with many general properties [Eis95, Part III] [CLO15, Chapter 6]. Again, we recall below only what we need for our purposes.

Let $\mathcal{R}$ be a ring and $\mathcal{M}$ a finite $\mathcal{R}$ -module. An exact sequence

$$\cdots \xrightarrow{\partial_{j+1}} \mathcal{E}_j \xrightarrow{\partial_j} \cdots \xrightarrow{\partial_2} \mathcal{E}_1 \xrightarrow{\partial_1} \mathcal{E}_0 \xrightarrow{\epsilon} \mathcal{M} \rightarrow 0$$

is a *left resolution* of $\mathcal{M}$. The maps ∂_i are *boundary homomorphisms*, and the map ϵ is an *augmentation homomorphism*. If for each i , the module $\mathcal{E}_i$ is free, then the resolution is a *free resolution*. For the sake of brevity, we will often refer to a resolution as above simply by $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathcal{M}, \partial_\bullet)$. We call $\sup\{i \in \mathbb{Z} : \mathcal{E}_i \neq 0\}$ the *length* of the resolution $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathcal{M}, \partial_\bullet)$. The length of $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathcal{M}, \partial_\bullet)$ could be infinite and free resolutions of finite length are *finite free resolutions*.

THEOREM 1.1.4 (Hilbert's syzygy theorem, [Eis95, Corollary 19.7]). — Let $\mathcal{M}$ be a finitely generated $\mathbb{K}[x_1, \dots, x_n]$ -module. There exists a free resolution $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathcal{M}, \partial_\bullet)$ of length at most n .

When $\mathcal{R}$ is graded and $\mathcal{M}$ is a graded $\mathcal{R}$ -module, $\mathcal{M}$ possesses a free resolution $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathcal{M}, \partial_\bullet)$ where each $\mathcal{E}_i$ is graded so that the boundary maps ∂_i and the augmentation map ϵ are graded $\mathcal{R}$ -module homomorphisms. Such free resolutions are called *graded free resolutions*. Graded free resolutions $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathcal{M}, \partial_\bullet)$ such that the ranks of each of the $\mathcal{E}_i$ are minimal are *minimal free resolutions*.

Let $\mathcal{R}$ be a ring, and $F = (f_1, \dots, f_s) \subseteq \mathcal{R}^t$ a sequence of elements of the free module $\mathcal{R}^t$. We define the *syzygy module* of F to be the $\mathcal{R}$ -module

$$\text{Syz}(F) = \{(g_1, \dots, g_s) \in \mathcal{R}^s : g_1 f_1 + \cdots + g_s f_s = 0\}.$$

The syzygy module can be read off from a free resolution.

PROPOSITION 1.1.5. — If $F = (f_1, \dots, f_s) \subseteq \mathcal{R}^t$, $\mathcal{M} = \langle\langle F \rangle\rangle$, and $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathcal{M}, \partial_\bullet)$ is a free resolution of length ℓ such that $\epsilon(e_i) = f_i$ for all $1 \leq i \leq s$, then

$$\text{Syz}(F) = \text{Syz}(\epsilon(e_1), \dots, \epsilon(e_{r_0})) = \ker(\epsilon) = \text{im}(\partial_1)$$

where $\text{rank}(\mathcal{E}_i) = r_i$.

Moreover, for each $1 \leq i \leq \ell$,

$$\text{Syz}(\partial_i(e_1), \dots, \partial_i(e_{r_i})) = \ker(\partial_i) = \text{im}(\partial_{i+1}).$$

Constructing free resolutions of a given finitely generated $\mathcal{R}$ -module is a straightforward process. Let $\mathcal{M}$ be a finitely generated $\mathcal{R}$ -module. Fix a set of generators $F = (\mathbf{f}_1^{(0)}, \dots, \mathbf{f}_{s_0}^{(0)})$ for $\mathcal{M}$. Let $\mathcal{E}_0 = \mathcal{R}^{s_0}$, and let $\epsilon : \mathcal{E}_0 \rightarrow \mathcal{M}$ be the map which sends $e_i \mapsto \mathbf{f}_i^{(0)}$. Next, let $(\mathbf{f}_1^{(1)}, \dots, \mathbf{f}_{s_1}^{(1)})$ be a set of generators for $\ker(\epsilon)$ and $\mathcal{E}_1 = \mathcal{R}^{s_1}$ and let $\partial_1 : \mathcal{E}_1 \rightarrow \mathcal{E}_0$ be the map which sends $e_i \mapsto \mathbf{f}_i^{(1)}$. Iterating this process, we obtain a free resolution $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathcal{M}, \partial_\bullet)$ of $\mathcal{M}$ with fixed generating sets for the images (resp. kernels) of each boundary morphism. We will call

$$\text{Syz}_j(F) = \text{Syz}(\partial_j(e_1), \dots, \partial_j(e_{r_j}))$$

the j^{th} syzygy module of F .

REMARK 1.1.6. — The way we define syzygy modules here is quite ad-hoc. In particular, as defined here, the syzygy modules of a given module $\mathcal{M}$ depend on the choices of a free resolution of $\mathcal{M}$ and generating sets for the images of each of the boundary homomorphisms in the chosen free resolution. In our setting this suffices, since we will define the free resolutions which we consider, and take explicit generating sets for the images of their boundary homomorphisms.

It is frequent that $\mathcal{M}$ is the ideal generated by polynomials $F = (f_1, \dots, f_\ell) \subseteq \mathcal{R}_n$. Then, the first syzygy module of F contains the Koszul syzygies, which are those following from the commutativity of polynomial multiplication: $f_i f_j - f_j f_i = 0$. In fact, they generate $\text{Syz}(F)$ in the case of *regular sequences* (that is, when f_i is not a zero-divisor in $\mathcal{R}_n / \langle f_1, \dots, f_{i-1} \rangle$ for any $2 \leq i \leq \ell$):

THEOREM 1.1.7 ([Eis05, Theorem A.2.49]). — If $(f_1, \dots, f_\ell)$ is a regular sequence, then $\text{Syz}(F) = \langle f_i e_j - f_j e_i : 1 \leq i, j \leq \ell, i \neq j \rangle$ where e_i is i -th standard basis vector.

In the context of $F_{r+1}(M)$, while the Koszul syzygies are among the syzygies of the minors of M , they do not generate $\text{Syz}(F_{r+1}(M))$.

The following consequence of Hilbert's syzygy theorem elucidates the connection between free resolutions and Hilbert series.

COROLLARY 1.1.8. — [CLO05, Theorem 4.4] Let $\mathcal{R}$ be a graded ring, let $\mathcal{M}$ be a finitely generated graded $\mathcal{R}$ -module, and let $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathcal{M}, \partial_\bullet)$ be a finite graded free resolution of $\mathcal{M}$ of length ℓ . For any $1 \leq i \leq \ell$, let $s_i = \text{rank}(\mathcal{E}_i)$ and write $\mathcal{E}_i = \bigoplus_{j=1}^{s_i} \mathcal{R}(-d_i^{(j)})$. Then

$$\text{HF}_{\mathcal{M}}(d) = \sum_{i=0}^{\ell} (-1)^i \sum_{j=1}^{s_i} \binom{k + d - d_i^{(j)} - 1}{k - 1}.$$

1.2 SIGNATURE GRÖBNER BASES

1.2.1 GRÖBNER BASES

A wealth of general theory about Gröbner bases can be found, for example, in [CLO05] and the references therein. We recall here only what is necessary for our purposes.

We denote by $\succ$ an admissible monomial order on $\mathcal{R}_n$. That is, $\succ$ is a total order on $\text{Mon}_d(\mathcal{R}_n)$ such that if σ, τ are monomials with $\sigma \succ \tau$, then for any monomial $m \in \text{Mon}_d(\mathcal{R}_n)$, $m\sigma \succ m\tau$, and for which there is no infinitely decreasing sequence of monomials. Given a polynomial $f \in \mathcal{R}_n$, we use $\text{LM}_{\prec}(f)$ to denote the leading monomial of f with respect to $\succ$, and $\text{LT}_{\prec}(f)$ to denote the leading term of f with respect to $\succ$, that is, $\text{LM}_{\prec}(f)$ multiplied by its coefficient in f . Given a set $F \subseteq \mathcal{R}$ of polynomials, we define the sets

$$\text{LM}_{\prec}(F) := \{\text{LM}_{\prec}(f) : f \in F\} \quad \text{and} \quad \text{LT}_{\prec}(F) := \{\text{LT}_{\prec}(f) : f \in F\}.$$

When $\succ$ is clear from the context, we remove it as a subscript.

From here on, we take $\prec$ to be the *graded reverse lexicographic* (or *grevlex*) order on $\mathcal{R}_n$, and $\prec_{\text{pot}}$ to be the corresponding *position over term* (or *POT*) order on $\mathcal{R}_n^s$ (see e.g. [CLO05, Def. 2.4, p211]).

By Proposition 1.1.2, if $\mathcal{M}$ is a free $\mathcal{R}_n$ -module of rank s , then $\bigwedge^d(\mathcal{M})$ is also a free $\mathcal{R}_n$ -module of rank $\binom{s}{d}$. Since the basis we fix on $\bigwedge^d(\mathcal{M})$ is not indexed by the integers

PRELIMINARIES

$1, \dots, \binom{s}{d}$ we slightly generalise the definition of the POT order: for $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$ and two strictly increasing sequences $1 \leq i_1 < \dots < i_d \leq s$, $1 \leq i'_1 < \dots < i'_d \leq s$, we take $x^\alpha(e_{i_1} \otimes \dots \otimes e_{i_d}) \prec_{\text{pot}} x^\beta(e_{i'_1} \otimes \dots \otimes e_{i'_d})$ if and only if $(i_1, \dots, i_d) \succ_{\text{lex}} (i'_1, \dots, i'_d)$ or $(i_1, \dots, i_d) = (i'_1, \dots, i'_d)$ and $x^\alpha \prec x^\beta$.

The set of all monomials of $\mathcal{R}_n$ (resp. $\mathcal{R}_n^s$) forms a basis for $\mathcal{R}_n$ (resp. $\mathcal{R}_n^s$) as an infinite-dimensional $\mathbb{k}$ -vector space. The *leading monomial* of an element $f \in \mathcal{R}_n$ (resp. $f \in \mathcal{R}_n^s$), denoted $\text{LM}_\prec(f)$ (resp. $\text{LM}_{\prec_{\text{pot}}}(f)$) is the largest monomial, with respect to $\prec$ (resp. $\prec_{\text{pot}}$), which appears in the unique representation of f in this $\mathbb{k}$ -basis. We naturally extend the leading monomial notation to sets: for a set $F \subseteq \mathcal{R}_n^s$, $\text{LM}_{\prec_{\text{pot}}}(F) = \{\text{LM}_{\prec_{\text{pot}}}(f) : f \in F\}$.

For some $s \in \mathbb{Z}_{>0}$, a $\prec_{\text{pot}}$ -Gröbner basis of a submodule $\mathcal{M} \subseteq \mathcal{R}_n^s$ is a set $G \subseteq \mathcal{M}$ such that $\langle\langle \text{LM}_{\prec_{\text{pot}}}(G) \rangle\rangle = \langle\langle \text{LM}_{\prec_{\text{pot}}}(\mathcal{M}) \rangle\rangle$. When $s = 1$ so that $\prec_{\text{pot}}$ coincides with $\prec$ and $\mathcal{M}$ is an ideal of $\mathcal{R}_n$, we call a $\prec_{\text{pot}}$ -Gröbner basis of $\mathcal{M}$ a $\prec$ -Gröbner basis.

1.2.2 MACAULAY MATRICES

For $s, n \in \mathbb{Z}_{>0}$ and a set $\mathbf{F} = \{\mathbf{f}_1, \dots, \mathbf{f}_t\} \subseteq \mathcal{R}_n^s$ of homogeneous elements, the *Macaulay matrix of $\mathbf{F}$ in degree d with respect to $\prec_{\text{pot}}$* , denoted $\mathcal{M}_d(\mathbf{F})$, is constructed as follows: its rows are indexed by the set $\bigcup_{i=1}^s \{\tau e_i : \tau \in \text{Mon}_{d-\deg \mathbf{f}_i}(\mathcal{R}_n)\}$, its columns are indexed by $\text{Mon}_d(\mathcal{R}_n^s)$, ordered decreasingly by $\prec_{\text{pot}}$, and for some $1 \leq i, j \leq s$ and $\tau \in \text{Mon}_{d-\deg \mathbf{f}_i}(\mathcal{R}_n)$, $\sigma \in \text{Mon}_d(\mathcal{R}_n^s)$, the entry of the row indexed by τe_i in the column indexed by σe_j is the coefficient of σe_j in $\tau \mathbf{f}_i$. The monomial τe_i is the *signature* of the row of $\mathcal{M}_d(\mathbf{F})$ which it indexes. For $1 \leq i \leq t$, we abbreviate $\mathcal{M}_{d,i}(\mathbf{F}) = \mathcal{M}_d(\{\mathbf{f}_1, \dots, \mathbf{f}_i\})$.

A *valid elementary row operation* on a Macaulay matrix $\mathcal{M}_d(\mathbf{F})$ consists in adding to a row of $\mathcal{M}_d(\mathbf{F})$ with signature τe_i a $\mathbb{k}$ -multiple of a row with some signature σe_j , where $\tau e_i \prec_{\text{pot}} \sigma e_j$. Finally, we denote by $\widetilde{\mathcal{M}}_d(\mathbf{F})$ a row-echelon form of $\mathcal{M}_d$ computed via a sequence of valid elementary row operations.

Each row of $\mathcal{M}_d(\mathbf{F})$ can be interpreted as an element of $\mathcal{R}_n^s$ by multiplying the entry in a given column by the monomial which indexes that column and taking the sum over all columns. We refer to rows of $\mathcal{M}_d(\mathbf{F})$ (resp. $\widetilde{\mathcal{M}}_d(\mathbf{F})$) as elements of $\mathcal{R}_n^s$, denoting them by $\text{rows}(\mathcal{M}_d(\mathbf{F}))$ (resp. $\text{rows}(\widetilde{\mathcal{M}}_d(\mathbf{F}))$).

For some $D \in \mathbb{Z}_{>0}$, we call $(D, \prec_{\text{pot}})$ -Gröbner basis of $\langle \mathbf{F} \rangle$ the union of the sets $\text{rows}(\widetilde{\mathcal{M}}_d(\mathbf{F}))$ for $d = \{\min_{1 \leq i \leq t} \{\deg \mathbf{f}_i\}, \dots, D\}$. This is justified by the following.

PROPOSITION 1.2.1 ([Laz83, Sec. 3]). — Let $\mathbf{F} = \{\mathbf{f}_1, \dots, \mathbf{f}_t\} \subseteq \mathcal{R}_n^s$, for $s, n \in \mathbb{Z}_{>0}$, be homogeneous elements with respect to the standard grading on $\mathcal{R}_n^s$. Then there exists $D \in \mathbb{Z}_{>0}$ such that a $(D, \prec_{\text{pot}})$ -Gröbner basis of $\langle \mathbf{F} \rangle$ is a $\prec_{\text{pot}}$ -Gröbner basis of $\langle \mathbf{F} \rangle$.

Moreover, it is shown in [Laz83, Sec. 3] that generically (in the sense of Section 1.3), the integer D in Proposition 1.2.1 satisfies the bound $D \leq 1 + \sum_{i=1}^t (\deg(\mathbf{f}_i) - 1)$.

1.2.3 THE MATRIX- F_5 ALGORITHM

Proposition 1.2.1 leads to an algorithm to compute Gröbner bases using linear algebra. This algorithm, known as Lazard's algorithm, is described in [Laz83]. Informally, given a polynomial system $F \subseteq \mathcal{R}_n$ and a degree bound $D \in \mathbb{Z}_{>0}$, it works by building the matrices $\mathcal{M}_d(F)$ and computing from them $\widetilde{\mathcal{M}}_d(F)$, for each degree $\min_{1 \leq i \leq t} \{\deg(f_i)\} \leq d \leq D$.

The following proposition, known as the syzygy criterion, lies at the core of the MatrixF₅ algorithm, which improves upon Lazard's algorithm by building Macaulay matrices with fewer rows.

PROPOSITION 1.2.2 (Syzygy Criterion, [EF16, Lemma 6.4]). — Let $s \in \mathbb{Z}_{>0}$, $F = (\mathbf{f}_1, \dots, \mathbf{f}_t) \subseteq \mathcal{R}_n^s$ be homogeneous elements and let $h = (h_1, \dots, h_\ell)$ be a homogeneous syzygy of F with $\text{LM}_{\succ_{\text{pot}}}(h) = \tau e_i$.

1. The row of $\mathcal{M}_{\deg \tau + d_i}$ with signature τe_i is a linear combination of rows of $\mathcal{M}_{\deg \tau + \deg \mathbf{f}_i}$ of smaller signature.
2. For any monomial $\sigma \in \mathcal{R}_n$, the row of $\mathcal{M}_{\deg \tau + \deg \sigma + \deg \mathbf{f}_i}$ with signature $\sigma \tau e_i$ is a linear combination of rows of $\mathcal{M}_{\deg \tau + \deg \sigma + \deg \mathbf{f}_i}$ of smaller signature.

Suppose now that $F = (f_1, \dots, f_t) \subseteq \mathcal{R}_n$ is a polynomial system. Then for each $1 \leq i, j \leq t$, $f_i e_j - f_j e_i \in \text{Syz}(F)$. Syzygies of this form are called *Koszul syzygies* and the MatrixF₅ algorithm exploits precisely these syzygies to improve upon Lazard's algorithm.

THEOREM 1.2.3 (F_5 Criterion, [Fau02, Theorem 1]). — Let $F = (f_1, \dots, f_t)$ be a polynomial system in $\mathcal{R}_n$. Then for any $d \in \mathbb{Z}_{>0}$, any $1 \leq i \leq t$, any $\tau \in \text{LM}_{\prec}(\text{rows}(\widetilde{\mathcal{M}}_{d,i}(F)))$, and any $i < j \leq t$, the row of $\mathcal{M}_{d+\deg(f_j)}(F)$ with signature τe_j is a linear combination of rows of $\mathcal{M}_{d+\deg(f_j)}(F)$ with smaller signature.

Proposition 1.2.2 leads naturally to Algorithm 1, which is a slightly modified version of the standard MatrixF₅ algorithm [BFS15] (see also [EF16, Sec. 3]) permitting the input of precomputed syzygies.

1.3 GENERICITY

1.3.1 NOTATION

Several of our results rely on genericity assumptions. As usual, let $\text{Mon}_d(\mathcal{R}_n)$ be the set of monomials in $\mathcal{R}_n$ of degree d . For $n, d \in \mathbb{Z}_{>0}$, and a set $\mathbf{c} = \{\mathbf{c}_\tau : \tau \in \text{Mon}_d(\mathcal{R}_n)\}$ of indeterminates, we call the polynomial

$$\mathbf{f}_{(n,d)}^{\mathbf{c}} = \sum_{\tau \in \text{Mon}_d(\mathcal{R}_n)} \mathbf{c}_\tau \tau \in \mathcal{R}_n[\mathbf{c}]$$

the *generic homogeneous polynomial in n variables of degree d* . A point $c = (c_\tau : \tau \in \text{Mon}_d(\mathcal{R}_n)) \in \mathbb{A}_{\mathbb{k}}^{\binom{n+d-1}{n-1}}$ defines a map

$$\phi_{\mathbf{c}} : \mathcal{R}_n[\mathbf{c}] \rightarrow \mathcal{R}_n; \quad \mathbf{c}_\tau \mapsto c_\tau$$

which maps $\mathbf{f}_{(n,d)}^{\mathbf{c}}$ to a homogeneous polynomial of degree d , with coefficients in $\mathbb{k}$.

Let $(d_1, \dots, d_s) \in \mathbb{Z}_{>0}^s$ and let $\mathbf{c}^{(1)}, \dots, \mathbf{c}^{(s)}$ be sets of indeterminates, with $\mathbf{c}^{(i)} = \{\mathbf{c}_\tau^{(i)} : \tau \in \text{Mon}_{d_i}(\mathcal{R}_n)\}$ for each $1 \leq i \leq s$. For a point $c = (c^{(1)}, \dots, c^{(s)}) \in \prod_{i=1}^s \mathbb{A}_{\mathbb{k}}^{\binom{n+d_i-1}{n-1}}$, the map

$$\phi_c : \mathcal{R}_n[\mathbf{c}^{(1)}, \dots, \mathbf{c}^{(s)}] \rightarrow \mathcal{R}_n; \quad \mathbf{c}_\tau^{(i)} \mapsto c_\tau^{(i)}$$

Algorithm 1 MatrixF₅(F, S, D)

Input: A sequence $F = (f_1, \dots, f_t)$ of homogeneous elements of degrees $d_1 \leq \dots \leq d_t$ in $\mathbb{K}[x_1, \dots, x_n]^s$; a degree bound D ; a set S of syzygies of F .

Output: A $(D, \prec_{\text{pot}})$ -Gröbner basis for $\langle\langle F \rangle\rangle$.

```

1: for  $i$  from 1 to  $t$  do  $G_i \leftarrow \emptyset$ 
2: for  $d$  from  $d_1$  to  $D$  do
3:    $\mathcal{M}_{d,0} \leftarrow \emptyset$ ;  $\text{Crit} \leftarrow \text{LM}_{\succ_{\text{pot}}}(S)$ 
4:   for  $i$  from 1 to  $t$  do
5:     if  $d < d_i$  then  $\mathcal{M}_{d,i} \leftarrow \mathcal{M}_{d,i-1}$ 
6:     else if  $d = d_i$  then  $\mathcal{M}_{d,i} \leftarrow$  concatenate the row  $f_i$  to  $\widetilde{\mathcal{M}}_{d,i-1}$  with signature  $e_i$ 
7:     else
8:        $\widetilde{\mathcal{M}}_{d,i} \leftarrow \widetilde{\mathcal{M}}_{d,i-1}$ 
9:       if  $s = 1$  then
10:        for  $\tau \in \text{LM}_{\prec}(\text{rows}(\mathcal{M}_{d-d_i,i-1}))$  do
11:           $\text{Crit} \leftarrow \text{Crit} \cup \{\tau e_i\}$ 
12:        for  $f \in \text{rows}(\widetilde{\mathcal{M}}_{d-1,i}) \setminus \text{rows}(\widetilde{\mathcal{M}}_{d-1,i-1})$  do
13:           $\tau e_i \leftarrow$  signature of  $f$ 
14:          if  $f = 0$  then
15:            for  $j$  from 1 to  $k$  do
16:               $\text{Crit} \leftarrow \text{Crit} \cup \{\tau x_j e_i\}$ 
17:          for  $f \in \text{rows}(\mathcal{M}_{d-1,i}) \setminus \text{rows}(\mathcal{M}_{d-1,i-1})$  do
18:             $\tau e_i \leftarrow$  signature of  $f$ 
19:            for  $j \in \{\max\{j' : x_{j'} \mid \tau\}, \dots, k\}$  do
20:              if  $\tau x_j e_i \notin \text{Crit}$  then  $\mathcal{M}_{d,i} \leftarrow$  concatenate the row  $x_j f$  to  $\mathcal{M}_{d,i}$  with
signature  $\tau x_j e_i$ 
21:           $\widetilde{\mathcal{M}}_{d,i} \leftarrow$  reduced row echelon form of  $\mathcal{M}_{d,i}$  obtained via a sequence of valid
elementary row operations
22:           $G_i \leftarrow G_i \cup \{f \in \text{rows}(\widetilde{\mathcal{M}}_{d,i}) : f \notin \langle \text{LM}_{\succ_{\text{pot}}}(G_i) \rangle\}$ 
23: return  $G_1, \dots, G_t$ 

```

defines a sequence of polynomials $\left(\phi_c \left(\mathfrak{f}_{(n,d_1)}^{c(1)}\right), \dots, \phi_c \left(\mathfrak{f}_{(n,d_s)}^{c(s)}\right)\right)$, with $\phi_c \left(\mathfrak{f}_{(n,d_i)}^{c(1)}\right)$ homogeneous of degree d_i , for each $1 \leq i \leq s$. Given such a point c , we will simply denote by $\phi_c \left(\mathfrak{f}_{(n,d_1,\dots,d_s)}\right)$ the sequence of polynomials defined by c in this way.

Similarly, let $p, q \in \mathbb{Z}_{>0}$ with $q \geq p$ and for $1 \leq i \leq p$, $1 \leq j \leq q$, let $d_{i,j} \in \mathbb{Z}_{>0}$ and let $\mathbf{c}^{(i,j)} = \left\{ \mathbf{c}_{\tau}^{(i,j)} : \tau \in \text{Mon}_{d_{(i,j)}}(\mathcal{R}_n) \right\}$ be a set of indeterminates. For a sequence of points $c = (c^{(1,1)}, \dots, c^{(p,q)})$ with $c^{(i,j)} \in \mathbb{A}_{\mathbb{K}}^{\binom{n+d_{i,j}-1}{n-1}}$, the map

$$\phi_c : \mathcal{R}_n[\mathbf{c}^{(1,1)}, \dots, \mathbf{c}^{(p,q)}] \rightarrow \mathcal{R}_n; \quad \mathbf{c}_{\tau}^{(i,j)} \mapsto c_{\tau}^{(i,j)}$$

defines a matrix $\left(\phi_c \left(\mathfrak{f}_{(n,d_{i,j})}^{(i,j)}\right)\right)_{i,j} \in \mathcal{R}_n^{p \times q}$. Again, given such a sequence of points $c = (c^{(1,1)}, \dots, c^{(p,q)})$, we will simply denote by $\phi_c \left(\mathfrak{f}_{(n,d_{i,j})}\right) \in \mathcal{R}_n^{p \times q}$ the $p \times q$ matrix defined by c in this way.

The following important fact is one which will be central to our ability to use well-known

free resolutions for generic determinantal ideals to compute syzygies of determinantal ideals of polynomial matrices.

PROPOSITION 1.3.1 ([BV88, Theorem 2.5]). — Let $n, p, q, d_0, r \in \mathbb{Z}_{>0}$ with $q \geq p \geq r$. Then there exists a Zariski open subset $U \subseteq \mathbb{A}^{pq \binom{n+d_0-1}{n-1}}$ such that for all $c \in U$,

$$\text{grade}(\mathcal{I}_r(\phi_c(\mathfrak{f}_{(n,d_0)}))) = (q - r + 1)(p - r + 1).$$

1.3.2 PROPERTIES

The notation pertinent to genericity used in Chapters 2 and 3 differ slightly from that used in Chapter 4. In the former, we take notation from [FSS13, Sec. 2 and 3], which we recall here.

In what follows, we use $\mathcal{A}_p^d$ to denote the $p \times p$ matrix of generic homogeneous polynomials of degree d , whose i, j entry is

$$\mathfrak{f}_{(n,d,\dots,d)}^{(i,j)} = \sum_{\tau \in \text{Mon}_d(\mathcal{R}_n)} \mathfrak{c}_{ij}^{(\tau)} \tau \in \mathcal{R}_n [\{\mathfrak{c}_{ij}^{(\tau)} : \tau \in \text{Mon}_d(\mathcal{R}_n)\}].$$

A map

$$\mathcal{P} : \{\text{Ideals of } \mathcal{R}_n\} \rightarrow \{\text{true}, \text{false}\}$$

is called a *property*.

A property $\mathcal{P}$ is (n, r, p, d) -generic if there exists a nonempty Zariski open subset $U \subseteq \mathbb{A}^{\binom{n+d-1}{n-1} \cdot p^2}$ such that for all $c \in U$,

$$\mathcal{P}(\mathcal{I}_{r+1}(\phi_c(\mathcal{A}_p^d))) = \text{true}.$$

One important property is the notion of Cohen-Macaulayness. Let $\mathcal{I}$ be an ideal of $\mathcal{R}_n$. A sequence $(f_1, \dots, f_\ell) \subseteq \mathcal{R}_n$ is called an $\mathcal{I}$ -regular sequence if for all $1 \leq i \leq \ell$, f_i is not a zero-divisor in the module $\mathcal{I}/\langle f_1, \dots, f_{i-1} \rangle$. The ideal $\mathcal{I}$ is called *Cohen-Macaulay* if there exists an $\mathcal{I}$ -regular sequence $(f_1, \dots, f_\ell)$ such that $\ell = \dim(\mathcal{I})$ (here $\dim(\mathcal{I})$ is the Krull dimension of $\mathcal{I}$ in $\mathcal{R}_n$).

REMARK 1.3.2. — If $(f_1, \dots, f_\ell)$ is an $\mathcal{I}$ -regular sequence, then $\ell \leq \dim(\mathcal{I})$. Hence, Cohen-Macaulayness requires that there exists an $\mathcal{I}$ -regular sequence of maximal possible length in $\mathcal{R}$.

The following proposition is a fundamental result on determinantal ideals.

PROPOSITION 1.3.3. — Let CM be the property given by

$$\text{CM}(I) = \begin{cases} \text{true} & \text{if } I \text{ is Cohen-Macaulay} \\ \text{false} & \text{otherwise} \end{cases}$$

Then for any $p, d \in \mathbb{Z}_{>0}$, $r < p$, CM is $((p - r)^2, r, p, d)$ -generic.

Proof. By [BV88, Theorem 2.5], the depth of $\mathcal{I}_{r+1}(\phi_c(\mathcal{A}_p^d))$ is at most $(p - r)^2$. By [FSS13, Theorem 10], there exists a Zariski open subset $U \subseteq \mathbb{A}_{\mathbb{k}}^{\binom{n+d-1}{n-1} \cdot p^2}$ such that for all $c \in U$, $\mathcal{I}_{r+1}(\phi_c(\mathcal{A}_p^d))$ has codimension $(p - r)^2$, and is therefore Cohen-Macaulay. $\square$

COMAXIMAL DETERMINANTAL IDEALS

We begin by considering the case of a square matrix of polynomials. That is, the case where M is a $p \times p$ matrix. By [Kur89, Theorem 5.1], the module $\text{Syz}(F_{r+1}(M))$ is generated by syzygies between minors of order $r + 1$ of submatrices of M of size $(r + 2) \times (r + 2)$. This allows us to reduce the problem of computing generators for $\text{Syz}(F_{r+1}(M))$ from the general case to the case $r = p - 2$. The Gulliksen-Negård complex (see [GN72, BV88]) is a free resolution of $\mathcal{I}_{p-1}(M)$. We will exploit this complex to obtain $\text{Syz}(F_{r+1}(M))$ first when $r = p - 2$, then in full generality. The content and results of this chapter come from the paper [GNS23], which was published in the proceedings of the International Symposium of Symbolic and Algebraic Computation (ISSAC) 2023.

2.1 SYZYGIES OF DETERMINANTAL IDEALS

2.1.1 THE GULLIKSEN-NEGÅRD COMPLEX

The Gulliksen-Negård complex is a free resolution of $\mathcal{I}_{p-1}(M)$,

$$0 \rightarrow \mathcal{E}_3 \xrightarrow{d_3} \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \mathcal{I}_{p-1}(M) \rightarrow 0.$$

As such, we can use Proposition 1.1.5 to compute the first syzygy module of the set of generators $F_{p-1}(M)$ as the kernel of the augmentation map ϵ of this complex. We recall the construction of the complex here; details and proofs can be found in [BV88, 2.D].

We denote by $M_p(\mathcal{R}_n)$ the set of $p \times p$ matrices over $\mathcal{R}_n$, with the structure of a free $\mathcal{R}_n$ -module of rank p^2 . We will denote by $\mathbf{E}_{i,j}$ the standard (i, j) -th basis matrix of $M_p(\mathcal{R}_n)$. In this section we will take as generators for $\mathcal{I}_{p-1}(M)$ the cofactors of M . To that end, let $M^C = (M_{i,j}^C)_{i,j} \in M_p(\mathcal{R}_n)$ be the matrix of these cofactors.

THE MODULES

We begin by defining the component modules $\mathcal{E}_3, \mathcal{E}_2, \mathcal{E}_1, \mathcal{E}_0$. Let $\mathcal{E}_0 = M_p(\mathcal{R}_n)$. Consider the sequence

$$\mathcal{R}_n \xrightarrow{\iota} M_p(\mathcal{R}_n) \oplus M_p(\mathcal{R}_n) \xrightarrow{\pi} \mathcal{R}_n$$

with $\iota(a) = (aI_p, aI_p)$, where I_p is the identity matrix in $M_p(\mathcal{R}_n)$ and $\pi(X, Y) = \text{trace}(X - Y)$ is the trace of $X - Y$. The module $\ker(\pi)$ is generated by the union of the following sets:

- $\{(0, \mathbf{E}_{i,j}) \in M_p(\mathcal{R}_n) \oplus M_p(\mathcal{R}_n) : 1 \leq i, j \leq n, i \neq j\},$
- $\{(\mathbf{E}_{i,j}, 0) \in M_p(\mathcal{R}_n) \oplus M_p(\mathcal{R}_n) : 1 \leq i, j \leq n, i \neq j\},$
- $\{(\mathbf{E}_{i,i}, \mathbf{E}_{1,1}) \in M_p(\mathcal{R}_n) \oplus M_p(\mathcal{R}_n) : 1 \leq i \leq n\},$ and
- $\{(0, \mathbf{E}_{i,i} - \mathbf{E}_{1,1}) \in M_p(\mathcal{R}_n) \oplus M_p(\mathcal{R}_n) : 2 \leq i \leq n\}.$

On the other hand, $\text{im}(\iota)$ is generated by

$$(I_p, I_p) = (\mathbf{E}_{1,1}, \mathbf{E}_{1,1}) + \sum_{i=2}^p (\mathbf{E}_{i,i}, \mathbf{E}_{1,1}) + \sum_{i=2}^p (0, \mathbf{E}_{i,i} - \mathbf{E}_{1,1}).$$

This shows that $\mathcal{E}_1 = \ker(\pi)/\text{im}(\iota)$ is a free module. Finally, let $\mathcal{E}_2 = M_p(\mathcal{R}_n)$ and $\mathcal{E}_3 = \mathcal{R}_n$.

THE MAPS

We next define the maps d_1, d_2, d_3, ϵ , as follows:

- $\epsilon : \mathcal{E}_0 \rightarrow \mathcal{I}_{p-1}(M), \quad N \mapsto \text{trace}(M^C N),$
- $d_1 : \mathcal{E}_1 \rightarrow \mathcal{E}_0, \quad \overline{(N_1, N_2)} \mapsto N_1 M - M N_2,$
- $d_2 : \mathcal{E}_2 \rightarrow \mathcal{E}_1, \quad N \mapsto \overline{(MN, NM)},$ and
- $d_3 : \mathcal{E}_3 \rightarrow \mathcal{E}_2, \quad x \mapsto x M^C,$

where for $(N_1, N_2) \in M_p(\mathcal{R}_n) \oplus M_p(\mathcal{R}_n)$, we denote by $\overline{(N_1, N_2)}$ its image under the canonical surjection $M_p(\mathcal{R}_n) \oplus M_p(\mathcal{R}_n) \twoheadrightarrow \mathcal{E}_1$.

PROPOSITION 2.1.1. — Let M be a matrix of homogeneous linear forms in $\mathcal{R}_n$. Assume $\mathcal{I}_{p-1}(M)$ is Cohen-Macaulay. With

$$\mathcal{E}_0, \mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3, \epsilon, d_1, d_2, d_3.$$

as defined above, the sequence

$$0 \rightarrow \mathcal{E}_3 \xrightarrow{d_3} \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \mathcal{I}_{p-1}(M) \rightarrow 0$$

is a free resolution of $\mathcal{I}_{p-1}(M)$.

Proof. Since $\mathcal{I} = \mathcal{I}_{p-1}(M)$ is Cohen-Macaulay, there exists an $\mathcal{I}$ -regular sequence of length equal to the Krull dimension of $\mathcal{I}$ in $\mathcal{R}_n$. By [FSS13, Theorem 10] and Proposition 1.3.3, the Krull dimension of $\mathcal{I}$ is exactly 4. Then, the result follows from [BV88, Theorem 2.26]. $\square$

2.1.2 THE CASE $r = p - 2$

We give generators for the first syzygy module in the case $r = p - 2$, assuming $\mathcal{I}_{p-1}(M)$ is Cohen-Macaulay.

THEOREM 2.1.2. — Let $M = (m_{i,j})$ be a matrix of homogeneous linear forms in $\mathcal{R}_n$. Suppose that $\mathcal{I}_{p-1}(M)$ is Cohen-Macaulay. Then the first syzygy module of $F_{p-1}(M)$ is generated by:

- (i) $\sum_{k=1}^p (-1)^{k+j} m_{k,i} \mathbf{E}_{k,j}$ for $i \neq j$;
- (ii) $\sum_{k=1}^p (-1)^{i+k} m_{j,k} \mathbf{E}_{i,k}$ for $i \neq j$;
- (iii) $\sum_{k=1}^p ((-1)^{i+k} m_{k,i} \mathbf{E}_{k,i} - (-1)^{k+1} m_{1,k} \mathbf{E}_{1,k})$ for $1 \leq i \leq p-1$;
- (iv) $\sum_{k=1}^p ((-1)^{j+k} m_{j,k} \mathbf{E}_{j,k} - (-1)^{k+1} m_{1,k} \mathbf{E}_{1,k})$ for $2 \leq j \leq p$.

Furthermore, the syzygies described by Items (i), (ii), (iii) and (iv) form a minimal generating set for the $\text{Syz}(F_{p-1}(M))$ of size $2p^2 - 2$.

Proof. By Proposition 1.1.5, $\ker(\epsilon)$ is the first syzygy module of the cofactors of M . By Proposition 2.1.1, since $\mathcal{I}_{p-1}(M)$ is Cohen-Macaulay, the Gulliksen-Negård complex is exact and $\ker(\epsilon) = \text{im}(d_1)$. The image $\text{im}(d_1)$ is generated by the images of generators for $\mathcal{E}_1$ under d_1 . Thus, by Section 2.1.1, the first syzygy module of $F_{p-1}(M)$ is generated by the following syzygies. For $i \neq j$,

$$d_1\left(\overline{(\mathbf{E}_{i,j}, 0)}\right) = \mathbf{E}_{i,j}M = \sum_{k=1}^p m_{k,i} \mathbf{E}_{k,j}. \quad (2.1)$$

Similarly, for $i \neq j$,

$$d_1\left(\overline{(0, \mathbf{E}_{i,j})}\right) = M\mathbf{E}_{i,j} = \sum_{k=1}^p m_{j,k} \mathbf{E}_{i,k}. \quad (2.2)$$

For any $1 \leq i \leq p-1$,

$$d_1\left(\overline{(\mathbf{E}_{i,i}, \mathbf{E}_{1,1})}\right) = \mathbf{E}_{i,i}M - M\mathbf{E}_{1,1} = \sum_{k=1}^p m_{k,i} \mathbf{E}_{k,i} - m_{1,k} \mathbf{E}_{1,k}. \quad (2.3)$$

Finally, for any $2 \leq j \leq p$,

$$d_1\left(\overline{(0, \mathbf{E}_{j,j} - \mathbf{E}_{1,1})}\right) = M\mathbf{E}_{j,j} - M\mathbf{E}_{1,1} = \sum_{k=1}^p m_{j,k} \mathbf{E}_{j,k} - m_{1,k} \mathbf{E}_{1,k}. \quad (2.4)$$

Since the generators for $\mathcal{I}_{p-1}(M)$ taken in the Gulliksen-Negård complex are the cofactors of M rather than the $(p-1)$ -minors of M , we obtain Items (i) to (iv) by pulling back each of Eqs. (2.1) to (2.4), respectively under the isomorphism $M_{i,j}^C \in \mathcal{I}_{p-1}(M) \mapsto (-1)^{(i+j)} M_{i,j}^C \in \mathcal{I}_{p-1}(M)$. There are $p^2 - p$ syzygies described by each of Item (i) and Item (ii), and $p-1$ syzygies described by each of Item (iii) and Item (iv). This gives a total of $2p^2 - 2$ syzygies.

We conclude by proving that these $2p^2 - 2$ syzygies form a minimal generating set for $\text{Syz}(F_{p-1}(M))$. Let $m_1, \dots, m_{2p^2-2} \in \text{Syz}(F_{p-1}(M))$ denote the generating set given by Item (i), Item (ii), Item (iii), Item (iv). Suppose that for some $1 \leq i \leq 2p^2 - 2$, m_i is generated by $\{m_1, \dots, m_{2p^2-2}\} \setminus \{m_i\}$. Then we can write $\sum_{j \neq i} a_j m_j = m_i$ for some $a_j \in \mathcal{R}_n$. Since the m_j are all homogeneous, this forces $a_j \in \mathbb{k}$ for all $j \neq i$. Subsequently, $a_j \in \text{im}(d_2) \cap \mathbb{k}^{2p^2-2}$ for all $j \neq i$.

Letting $a_i = 1$, and taking $N \in d_2^{-1}((a_1, \dots, a_{2p^2-2}))$, we find that $MN, NM \in M_p(\mathcal{R}_n)$ are matrices with entries in $\mathbb{k}$. For $1 \leq j \leq p$, the entries of the j -th row of MN are members of the ideal generated by the j -th row of M . The entries of M are homogeneous linear forms, so the only constant element contained in this ideal is 0. Similarly, for $1 \leq j \leq p$, the entries of the j -th row of NM are members of the ideal generated by the j -th column of M , and an analogous argument applies. Thus, $a_j = 0$ for each $1 \leq j \leq 2p^2 - 2$. $\square$

One can easily construct an algorithm, named `SyzCorankOne`, which, given a matrix M , computes the syzygies described in Theorem 2.1.2.

REMARK 2.1.3. — In both Theorem 2.1.2 and `SyzCorankOne`(M) we require that $F_{p-1}(M)$ is Cohen-Macaulay. This is necessary, as without it the Gulliksen-Negård complex need not be exact and subsequently we cannot compute $\text{Syz}(F_{p-1}(M))$ using its differential maps. However, since ϵ is defined by $\epsilon(N) = \text{trace}(M^C N)$, where $M^C = (M_{i,j}^C)$ is the matrix of cofactors of M , a matrix $N = (N_{i,j}) \in M_p(\mathcal{R}_n)$ is in the kernel of ϵ if and only if $\sum_{1 \leq i, j \leq p} N_{j,i} M_{i,j}^C = 0$. That is, $\ker(\epsilon)$ corresponds to $\text{Syz}(F_{p-1}(M))$ even if $\mathcal{I}_{p-1}(M)$ is not Cohen-Macaulay. Moreover, even if $\mathcal{I}_{p-1}(M)$ is not Cohen-Macaulay, the Gulliksen-Negård complex is still a complex.

Thus, in all cases, $\text{im}(d_1) \subseteq \ker \epsilon$, so if $\mathcal{I}_{p-1}(M)$ is not Cohen-Macaulay, Theorem 2.1.2 describes (and subsequently $\text{SyzCorankOne}(M)$ computes) a generating set for a submodule of $\text{Syz}(F_{p-1}(M))$.

REMARK 2.1.4. — If the entries of M are not homogeneous, then assuming $\mathcal{I}_{p-1}(M)$ is Cohen-Macaulay, the syzygies computed by Theorem 2.1.2 still generate $\text{Syz}(F_{p-1}(M))$, but they need no longer be a *minimal* generating set.

2.1.3 THE GENERAL CASE

THEOREM 2.1.5. — Let $p \geq 3$ and let $1 \leq r \leq p-2$. Then there exists a nonempty Zariski open set $U \subseteq \mathbb{A}^{np^2}$ such that for all $\mathbf{a} \in U$, taking $M = \varphi_{\mathbf{a}}(\mathcal{A}_p^1)$, the following holds: Let M' be the set of submatrices of size $(r+2) \times (r+2)$ of M . For each matrix $N \in M'$, let $S(N)$ be the set of syzygies of $F_{r+1}(N)$ computed using Theorem 2.1.2. Then $\text{Syz}(F_{r+1}(M)) = \bigcup_{N \in M'} S(N)$.

Proof. Let $\mathcal{U}$ be an $p \times p$ matrix of indeterminates over $\mathbb{k}$. Let $\mathcal{U}'$ be the set of $(r+2) \times (r+2)$ submatrices of $\mathcal{U}$. For each $\mathcal{N} \in \mathcal{U}'$, let $S(\mathcal{N})$ be the set of syzygies of $F_{r+1}(\mathcal{N})$ computed using Theorem 2.1.2. By [Kur89, Theorem 5.1], $\text{Syz}(F_{r+1}(\mathcal{A}_p^d)) = \bigcup_{\mathcal{N} \in \mathcal{U}'} S(\mathcal{N})$. Thus, by [FSS13, Lemma 3], there is a nonempty Zariski open subset $U_1 \subseteq \mathbb{A}^{np^2}$ such that for all $\mathbf{a} \in U_1$, the syzygies between the $(r+1)$ -minors of $\varphi_{\mathbf{a}}(\mathcal{A}_p^1)$ are those between the $(r+1)$ -minors of each $(r+2) \times (r+2)$ submatrix of $\varphi_{\mathbf{a}}(\mathcal{A}_p^1)$. We denote by $\mathcal{A}_p^{1'}$ the set of $(r+2) \times (r+2)$ submatrices of $\mathcal{A}_p^1$. By Proposition 1.3.3, for each submatrix N of $\mathcal{A}_p^{1'}$, there exists a nonempty Zariski open subset $U_N \subseteq \mathbb{A}^{np^2}$ such that for all $\mathbf{a} \in U_N$, the ideal generated by the $(r+1)$ -minors of N is Cohen-Macaulay, so that Theorem 2.1.2 applies. Thus, taking $U = \bigcap_{N \in \mathcal{A}_p^{1'}} U_N \cap U_1$, the result follows. $\square$

Consequently, using $\text{SyzCorankOne}(M)$ we obtain an algorithm $\text{SyzGen}(M, r)$ which constructs a set of generators for $\text{Syz}(F_{r+1}(M))$.

REMARK 2.1.6. — From Theorems 2.1.2 and 2.1.5, neither $\text{SyzGen}(M, r)$ nor $\text{SyzCorankOne}(M)$ require any arithmetic $\mathbb{k}$ -operations.

Again in the statement of Theorem 2.1.5 we require that $\mathcal{I}_{r+1}(M)$ is Cohen-Macaulay. This is necessary in order for $\text{Syz}(\mathcal{I}_{r+1}(M))$ to be computed via the syzygies of $(r+1)$ -minors of $(r+2) \times (r+2)$ submatrices. If $\mathcal{I}_{r+1}(M)$ is not Cohen-Macaulay, Theorem 2.1.5 gives a (possibly proper) subset of a generating set for $\text{Syz}(\mathcal{I}_{r+1}(M))$.

Finally, we require that the entries of M be homogeneous linear forms. Once again, the theorem holds if the entries are affine, as long as $\mathcal{I}_{r+1}(M)$ satisfies the stated genericity assumption.

Note that no claim is made as to the minimality of the generating set computed in Theorem 2.1.5. However, one can show that when the entries of M are homogeneous, a minimal generating set can be extracted from the set computed in Theorem 2.1.5 by throwing away any element which differs by multiplication by -1 from another element. This need no longer hold if the entries are affine.

2.2 DETERMINANTAL MATRIX- F_5 ALGORITHM

In this section, we use the syzygies returned by $\text{SyzGen}(M, r)$ to avoid reductions to zero when running Algorithm 1. As explained below, the following result will be instrumental.

PROPOSITION 2.2.1 ([EF16, Lemma 6.4]). — Let $(f_1, \dots, f_\ell) = F \subseteq \mathcal{R}_n^t$ be a system of homogeneous module elements. Let $D \in \mathbb{Z}_{\geq 0}$, and let $G = G_{D - \min_i \{\deg(f_i)\}}$ be the elements up to degree $D - \min_i \{\deg(f_i)\}$ of a POT-Gröbner basis for $\text{Syz}(F)$. Then,

1. If $\tau e_i \in \text{LT}_{\succ_{\text{pot}}}(G)$, the row of $\mathcal{M}_{\deg(\tau) + \deg(f_i), i}$ with signature (i, τ) is a linear combination of rows with smaller signature.
2. If a row with signature (i, τ) of $\mathcal{M}_{\deg(\tau) + \deg(f_i), i}$ reduces to zero, then τe_i is in the module generated by $\text{LT}_{\succ_{\text{pot}}}(G)$.

Proof. Item 1 is simply Proposition 1.2.2. We turn to Item 2. Fix $\min_i \{\deg(f_i)\} \leq d \leq D$ and $1 \leq i \leq \ell$. Suppose that the row with signature (i, τ) reduces to zero in $\mathcal{M}_{\deg(\tau) + \deg(f_i), i}$. Then there is a linear dependency $s_1 f_1 + \dots + s_\ell f_\ell = 0$. This corresponds to a syzygy $s = s_1 e_1 + \dots + s_\ell e_\ell \in \text{Syz}(F)$ with $\text{LT}_{\succ_{\text{pot}}}(s) = \tau e_i$. Finally,

$$\deg(s_i) = d - \deg(f_i) \leq D - \deg(f_i) \leq D - \min_i \{\deg(f_i)\}.$$

for each $1 \leq i \leq \ell$. Thus $\text{LT}_{\succ_{\text{pot}}}(s) = \tau e_i$ is in $\langle \text{LT}_{\succ_{\text{pot}}}(G) \rangle$. $\square$

Using Proposition 2.2.1, in order to remove all reductions to zero when running Algorithm 1 to compute a D -Gröbner basis for a graded module $F \subseteq \mathcal{R}_n^t$, we compute the leading terms of the elements up to degree $D - \min_{f \in F} \{\deg f\}$ of a Gröbner basis for $\text{Syz}(F)$. We can compute them by running Algorithm 1 on a set of chosen generators for $\text{Syz}(F)$ itself, with the appropriate degree bound given by Proposition 2.2.1. However, if $\text{Syz}_2(F) \neq \{0\}$, then Proposition 2.2.1 once again shows that reductions to zero will be encountered when computing the elements up to degree $D - \min_{f \in F} \{\deg f\}$ of a Gröbner basis for $\text{Syz}(F)$.

When $r = p - 2$, the Gulliksen-Negård complex allows us to explicitly compute generating sets for all higher syzygy modules. Thus, we can avoid all reductions to zero when computing a D -Gröbner basis for $F_{r+1}(M)$. When $r < p - 2$, we can only compute a generating set for the first syzygy module $\text{Syz}(F_{r+1}(M))$, and thus cannot efficiently remove all reductions to zero.

Now we are ready to describe an algorithm which exploits the syzygies computed by $\text{SyzGen}(M, r)$ to compute a grevlex Gröbner basis for $F_{r+1}(M)$ without reductions to zero in degree $r + 2$.

Algorithm 2 Determinantal-Matrix- $F_5(M, r, D)$

Input: An integer $1 \leq r \leq p - 2$, an $p \times p$ matrix M of homogeneous linear forms over $\mathbb{k}$ in $(p - r)^2$ variables such that $\mathcal{I}_{r+1}(M)$ is Cohen-Macaulay, and a degree bound D .

Output: A grevlex D -Gröbner basis for $\mathcal{I}_{r+1}(M)$.

- 1: $S \leftarrow \text{SyzGen}(M, r)$
 - 2: $S' \leftarrow \text{Matrix-F}_5(S, 1, \emptyset)$
 - 3: $G \leftarrow \text{Matrix-F}_5(F_{r+1}(M), D, S')$
 - 4: **return** G
-

PROPOSITION 2.2.2. — Algorithm 2 terminates and is correct.

Proof. Termination follows from that of $\text{SyzGen}(M, r)$ and Algorithm 1. To prove correctness, we need to show that the set S' of Algorithm 2 is indeed a set of syzygies between the elements of $\mathcal{I}_{r+1}(M)$. By Theorem 2.1.5, the set S computed on Algorithm 2 is a minimal generating set for $\text{Syz}(F_{r+1}(M))$. By the construction of this generating set, given in Theorem 2.1.5, each

element of S is homogeneous of degree one. Hence, according to correctness of Algorithm 1, the set S' consists of the elements of degree one of a POT-Gröbner basis for $\text{Syz}(F_{r+1}(M))$. $\square$

REMARK 2.2.3. — Both the number of rows and the number of columns of the Macaulay matrix in degree one for the set S on Algorithm 2 of Algorithm 2 is bounded by the number of rows of the Macaulay matrix for $F_{r+1}(M)$ in degree $r + 1$. Therefore, asymptotically, the arithmetic cost of Algorithm 2 is bounded by the arithmetic cost of its final step, computing the Gröbner basis of $F_{r+1}(M)$.

PROPOSITION 2.2.4. — Let $p \geq 3$, let $1 \leq r \leq p - 2$, let $D = r \cdot (p - r) + 1$, and let $n = (p - r)^2$. There exists a nonempty Zariski open set $U \subseteq \mathbb{A}^{n \cdot p^2}$ such that for all $\mathbf{a} \in U$, taking $M = \varphi_{\mathbf{a}}(\mathcal{A}_p^d)$, upon running Algorithm 2 with arguments M, r, D :

1. a full grevlex Gröbner basis is returned; and
2. for each $1 \leq i \leq \binom{p}{r+1}^2$, the matrix $\mathcal{M}_{r+2,i}$ has full rank.

Proof. By [FSS13, Lemma 18], there exists a Zariski open subset $U_1 \subseteq \mathbb{A}^{np^2}$ such that the maximal degree of a polynomial in the reduced grevlex Gröbner basis for $\mathcal{I}_{r+1}(M)$ is precisely D . Let U_2 be a nonempty Zariski open subset of $\mathbb{A}^{np^2}$ such that the results of Theorem 2.1.5 hold. Let $U = U_1 \cap U_2$. Item 1 follows immediately from the degree bound given in [FSS13]. We turn to Item 2. By Proposition 2.2.1, Item 2, it suffices to show that the leading terms of the set S' of Algorithm 2 consists of the elements of degree at most $r + 2$ of $\text{LT}_{\succ_{\text{pot}}}(\text{Syz}(\mathcal{I}_{r+1}(M)))$. This is immediate from Theorem 2.1.5 and correctness of Algorithm 1. $\square$

REMARK 2.2.5. — If we do not impose the genericity assumption on $\mathcal{I}_{r+1}(M)$ Algorithm 2 will still return a D -Gröbner basis for $\mathcal{I}_{r+1}(M)$, though $\mathcal{M}_{r+2,i}$ need no longer be full rank for all $1 \leq i \leq \binom{p}{r+1}^2$.

If the entries of M are affine, by Remark 2.1.6, there are two possibilities. First, $\text{SyzGen}(M, r)$ still returns a generating set for the first syzygy module of $F_{r+1}(M)$, and these may be used in the original F_5 algorithm which works on affine input to avoid reductions to zero. Alternatively, following [CLO15, Ch. 8, § 2, Prop. 7], one can simply homogenise $F_{r+1}(M)$ with respect to a variable h which is taken to be grevlex smaller than all other variables of $\mathcal{R}_n$, and specialise $h = 1$ upon termination of Algorithm 2.

2.3 THE CASE $r = p - 2$

Now, we describe an altered version of the F_5 algorithm which computes a Gröbner basis for $\mathcal{I}_{r+1}(M)$ when $r = p - 2$ without any reductions to zero. Note that Algorithm 2 does not require $r < p - 2$. Thus, we could simply compute a Gröbner basis for $\mathcal{I}_{r+1}(M)$ using Algorithm 2 when $r = p - 2$. However, only those reductions to zero arising from syzygies of degree $r + 2$ will be avoided. By Proposition 2.2.1, any syzygies of degree $d > r + 2$ which cannot be generated by the syzygies of degree $r + 2$ will manifest as reductions to zero in the Macaulay matrices in degree d .

2.3.1 HIGHER SYZGY MODULES

By Proposition 2.1.1, the Gulliksen-Negård complex is a free resolution of $\mathcal{I}_{r+1}(M)$ as soon as $\mathcal{I}_{r+1}(M)$ is Cohen-Macaulay. Thus, the kernels of its differential maps are precisely the syzygy

modules of $\mathcal{I}_{r+1}(M)$. The map d_3 is defined by $d_3(x) = xM^C$, where M^C is the matrix of cofactors of M . The third syzygy module $\text{Syz}_3(\mathcal{I}_{r+1}(M))$ is the image of d_3 , and is thus free of rank p^2 and principally generated by the entries of M^C .

PROPOSITION 2.3.1. — Let M be an $p \times p$ matrix of homogeneous linear forms in $\mathcal{R}_n$. Suppose $\mathcal{I}_{p-1}(M)$ is Cohen-Macaulay. In the $\mathcal{R}_n$ -basis for $\ker(\pi)/\text{im}(\iota)$ given in Section 2.1.1, the second syzygy module $\text{Syz}_2(F_{r+1}(M))$ is generated by the following syzygies:

(i) For $2 \leq i \leq p$ and $1 \leq j \leq p-1$,

$$\begin{aligned} & \sum_{k \neq j} m_{k,i} \overline{(E_{k,j}, 0)} + \sum_{k \neq i} m_{j,k} \overline{(0, E_{i,k})} \\ & + m_{j,i} \left(\overline{(E_{j,j}, E_{1,1})} + \overline{(0, E_{i,i} - E_{1,1})} \right). \end{aligned}$$

(ii) For $2 \leq i \leq p$,

$$\begin{aligned} & \sum_{k \neq p} m_{k,i} \overline{(E_{k,p}, 0)} + \sum_{k \neq i} m_{p,k} \overline{(0, E_{i,k})} \\ & - m_{p,i} \left(\sum_{j=1}^{p-1} \overline{(E_{j,j}, E_{1,1})} + \sum_{j=2}^{p-1} \overline{(0, E_{j,j} - E_{1,1})} \right) \end{aligned}$$

(iii) For $1 \leq j \leq p-1$,

$$\sum_{k \neq j} m_{k,1} \overline{(E_{k,j}, 0)} + \sum_{k \neq 1} m_{j,k} \overline{(0, E_{1,k})} + m_{j,1} \overline{(E_{j,j}, E_{1,1})}$$

(iv) Finally,

$$\begin{aligned} & \sum_{k \neq p} m_{k,1} \overline{(E_{k,p}, 0)} + \sum_{k \neq 1} m_{p,k} \overline{(0, E_{1,k})} \\ & - m_{p,1} \left(\sum_{j=1}^{p-1} \overline{(E_{j,j}, E_{1,1})} + \sum_{j=2}^p \overline{(0, E_{j,j} - E_{1,1})} \right) \end{aligned}$$

Proof. The second syzygy module $\text{Syz}_2(\mathcal{I}_{r+1}(M))$ is the image of d_2 , by Proposition 2.1.1. The map d_2 is defined by

$$d_2(N) = \overline{(MN, NM)}.$$

Taking $\mathbf{E}_{i,j}$, $1 \leq i, j \leq p$ to be the canonical $\mathcal{R}_n$ -basis for $M_p(\mathcal{R}_n)$, a basis for $\text{im}(d_2)$ is given by $\{\overline{(M\mathbf{E}_{i,j}, \mathbf{E}_{i,j}M)} \mid 1 \leq i, j \leq p\}$. We can express $M\mathbf{E}_{i,j}$ and $\mathbf{E}_{i,j}M$ in the canonical $\mathcal{R}_n$ -basis for $M_p(\mathcal{R}_n)$,

$$M\mathbf{E}_{i,j} = m_{j,i}\mathbf{E}_{j,j} + \sum_{k \neq j} m_{k,i}\mathbf{E}_{k,j}; \quad \mathbf{E}_{i,j}M = m_{j,i}\mathbf{E}_{i,i} + \sum_{k \neq i} m_{j,k}\mathbf{E}_{i,k}.$$

From this, we express generators for $\text{Syz}_2(\mathcal{I}_{r+1}(M))$ in the $\mathcal{R}_n$ -basis for $\ker(\pi)/\text{im}(\iota)$. Doing so gives precisely Items (i) to (iv). $\square$

Proposition 2.3.1 leads to an algorithm, which we will call $\text{Syz2GenCorankOne}(M)$ which constructs the set $\text{Syz}_2(F_{p-1}(M))$. We use this algorithm in the next section to design a dedicated F_5 -type algorithm which performs no reduction to zero when computing a Gröbner basis of $\mathcal{I}_{p-1}(M)$ when $\mathcal{I}_{p-1}(M)$ is Cohen-Macaulay and $n = 4$.

REMARK 2.3.2. — Analogous to Remark 2.2.5, if $\mathcal{I}_{p-1}(M)$ is not Cohen-Macaulay, the Gulliksen-Negård complex need not be a free resolution of $F_{p-1}(M)$, though it is still a complex. Thus, even if $\mathcal{I}_{p-1}(M)$ is not Cohen-Macaulay, $\text{im}(d_2) \subseteq \ker(d_1)$, so the syzygies described by Proposition 2.3.1 are a subset of a generating set for the syzygies between the generators for $\ker \epsilon$ given by Theorem 2.1.2.

2.3.2 A REFINED F_5 ALGORITHM

We combine Proposition 2.3.1, Theorem 2.1.2, and Proposition 2.2.1 to give an algorithm which computes a grevlex Gröbner basis for $F_{p-1}(M)$ without any reductions to zero, provided $\mathcal{I}_{p-1}(M)$ is Cohen-Macaulay. In order to obtain the leading terms of the first syzygy module, of $F_{p-1}(M)$, we must know which rows will reduce to zero when echelonizing the Macaulay matrices associated to the first syzygy module in various degrees. By Proposition 2.2.1, the signatures of these rows are precisely the leading terms of a Gröbner basis for the second syzygy module in the appropriate degree.

Subsequently, applying Proposition 2.2.1 once again, the leading terms of the first syzygy module in various degrees are precisely the signatures of the rows which reduce to zero when echelonizing the Macaulay matrices associated to $F_{p-1}(M)$.

Algorithm 3 Determinantal-Corank-One-Matrix- F_5

Input: An integer $p \geq 3$, an $p \times p$ matrix of generic homogeneous linear forms over $\mathbb{k}$ in 4 variables, and an integer $D \geq p - 1$

Output: The elements up to degree D of a grevlex Gröbner basis for $\mathcal{I}_{p-1}(M)$.

- 1: $S_1 \leftarrow \text{SyzCorankOne}(M)$
 - 2: $S_2 \leftarrow \text{Syz2GenCorankOne}(M)$
 - 3: $S'_2 \leftarrow \text{Matrix-}F_5(S_2, D - p, \emptyset)$
 - 4: $S'_1 \leftarrow \text{Matrix-}F_5(S_1, D - p + 1, S'_2)$
 - 5: $G \leftarrow \text{Matrix-}F_5(F_{p-1}(M), D, S'_1)$
 - 6: **return** G
-

PROPOSITION 2.3.3. — Algorithm 3 terminates and is correct.

Proof. Termination follows from termination of $\text{SyzCorankOne}(M)$, $\text{Syz2GenCorankOne}(M)$, and Algorithm 1. For correctness, it suffices to show that the set S'_1 computed on Algorithm 3 is indeed a set of syzygies of the polynomials in $F_{p-1}(M)$. This follows from Theorem 2.1.2. $\square$

PROPOSITION 2.3.4. — Let $D = 2p - 3$. Then there is a nonempty Zariski open subset U of $\mathbb{A}^{4p^2}$ such that for all $\mathbf{a} \in U$, upon running Algorithm 3 with arguments $\varphi_{\mathbf{a}}(\mathcal{I}_{p-1}(\mathcal{A}_p^d))$, D ,

1. a full grevlex Gröbner basis is returned; and
2. for each $1 \leq i \leq p^2$ and for each $p - 1 \leq d \leq 2p - 3$, the matrix $\mathcal{M}_{d,i}$ is full rank.

Proof. By [FSS13, Lemma 18], there is a Zariski dense subset U_1 of $\mathbb{A}^{4p^2}$ such that for all $\mathbf{a} \in U_1$, the maximal degree of a polynomial in the reduced grevlex Gröbner basis of $\mathcal{I}_{p-1}(M)$ is $2p - 3$. By Proposition 1.3.3, there is a nonempty Zariski open subset U_2 of $\mathbb{A}^{4p^2}$ such that for all $\mathbf{a} \in U_2$, the ideal $\varphi_{\mathbf{a}}(\mathcal{I}_{p-1}(\mathcal{A}_p^d))$ is Cohen Macaulay. Thus, taking $U = U_1 \cap U_2$, we obtain Item 1.

We turn to Item 2. By Proposition 2.2.1, Item 2, it suffices to show that the leading terms of the set S'_1 computed on Algorithm 3 consists of the elements of degree at most

$2p - 3$ of $\text{LT}_{\succ_{\text{pot}}}(\text{Syz}(\mathcal{I}_{p-1}(M)))$. This is immediate from Theorem 2.1.2 and correctness of Algorithm 1. $\square$

2.4 COMPLEXITY IN THE CASE $r = p - 2$

Throughout this section we focus on the dimension zero case. Thus, $n = (p - r)^2 = 4$. For a homogeneous ideal $\mathcal{I} \subseteq \mathcal{R}_n$, we take $\text{HF}_{\mathcal{I}}(d)$ to be the *Hilbert function* of $\mathcal{I}$. That is, for an integer $d \geq 0$, $\text{HF}_{\mathcal{I}}(d) = \dim_{\mathbb{k}} \mathcal{I}_d$. Further, we take $H_{\mathcal{I}}(t) = \sum_d \text{HF}_{\mathcal{I}}(d)t^d$ to be the *Hilbert series* of $\mathcal{I}$. We refer to [Eis95, 1.9] for further details.

When $r = p - 2$, we can use the results of the previous section to give explicit formulae for the coefficients of the Hilbert series $H_{\mathcal{I}_{r+1}(M)}(t)$. Subsequently, we can exactly compute the ranks of the Macaulay matrices in each degree computed by the F_5 algorithm, and bound the complexity of computing the reduced grevlex Gröbner basis of a matrix of generic homogeneous linear forms by that of computing the row reduction of each of these matrices.

First, note that for any $1 \leq d \leq r$, both the number of rows and the number of columns of the Macaulay matrix in degree d for the set S_2 (resp. S_1) computed by Algorithm 3 is bounded by the number of rows of the Macaulay matrix in degree $d + 1$ (resp. $d + r + 1$) for the set S_1 (resp. $F_{p-1}(M)$). Thus, the arithmetic cost of Algorithm 3 is bounded by the arithmetic cost of the final step, computing the grevlex Gröbner basis for $F_{p-1}(M)$.

PROPOSITION 2.4.1. — There exists a Zariski open set $U \subseteq \mathbb{A}^{4p^2}$ such that for all $\mathbf{a} \in U$, the Hilbert series $H_{\varphi_{\mathbf{a}}(\mathcal{I}_{r+1}(\mathcal{A}_p^d))}(t)$ for $\varphi_{\mathbf{a}}(\mathcal{I}_{r+1}(\mathcal{A}_p^d))$ is given by:

$$\sum_{d=r+1}^{2r+1} \left(p^2 \binom{d-r+2}{3} - (2p^2 - 2) \binom{d-r+1}{3} + p^2 \binom{d-r}{3} \right) t^d. \quad (2.5)$$

Proof. Let U be as in Proposition 2.3.4. If $\mathcal{M}$ is a free $\mathcal{R}_n$ -module of rank t , then the monomials of $\mathcal{M}$ of degree d form a basis for the finite-dimensional $\mathbb{k}$ -vector space of homogeneous elements of degree d of $\mathcal{M}$. Thus, $\text{HF}_{\mathcal{M}}(d) = t \cdot \binom{n+d-1}{d-1}$. The description of each free module in the Gulliksen-Negård complex given in Section 2.1.1 gives rise to

$$\begin{aligned} \text{rank } \mathcal{E}_0 &= \#F_{p-1}(M) = \binom{p}{p-1}^2 = p^2, & \text{rank } \mathcal{E}_1 &= 2p^2 - 2 \\ \text{rank } \mathcal{E}_2 &= p^2, & \text{rank } \mathcal{E}_3 &= 1 \end{aligned}$$

Thus, by [Eis95, Thm. 1.13], $\text{HF}_{\mathcal{I}_{p-1}(M)}(d) = \sum_{i=0}^3 (-1)^i \text{HF}_{\mathcal{E}_i}(d)$, which equals $p^2 \binom{d-r+2}{3} - (2p^2 - 2) \binom{d-r+1}{3} + p^2 \binom{d-r}{3} - \binom{d-r-1}{3}$. $\square$

In the following proposition, we take

$$\mathcal{B} = \sum_{d=r+1}^{2r+1} p^2 \binom{d-r+2}{3} - (2p^2 - 2) \binom{d-r+1}{3} + p^2 \binom{d-r}{3}.$$

PROPOSITION 2.4.2. — There is a Zariski dense subset U of $\mathbb{A}^{4p^2}$ such that for all $\mathbf{a} \in U$, the arithmetic cost of computing the reduced grevlex Gröbner basis for $\varphi_{\mathbf{a}}(\mathcal{I}_{p-1}(\mathcal{A}_p^d))$ using Algorithm 3 is in

$$O\left(\mathcal{B}^{\omega-1} \binom{2r+5}{5}\right) = O\left(p^{4(\omega-1)} \binom{2p}{3}\right).$$

Proof. Take U as in Proposition 2.4.1. Fix $\mathbf{a} \in U$ and let $M = \varphi_{\mathbf{a}}(\mathcal{I}_{p-1}(\mathcal{A}_p^d))$. The ideal $\mathcal{I}_{p-1}(M)$ is homogeneous, so the complexity of computing a grevlex Gröbner basis for $\mathcal{I}_{p-1}(M)$ is bounded by the complexity of reducing the intermediate Macaulay matrices encountered in the matrix- F_5 algorithm. The coefficient on t^d in the Hilbert series Eq. (2.5) gives the rank of the Macaulay matrix of $F_{r+1}(M)$ in degree d . The Macaulay matrices computed in Algorithm 3 have full row rank, allowing for the use of any echelonization algorithm when computing $\widetilde{\mathcal{M}}_{d,i}$. Hence, the result follows from the complexity of computing the reduced row echelon form [Sto00, Sec. 2.2] (see also [JPS13, App. A]) and the fact that the number of columns in the Macaulay matrix in degree $2p - 3$, the maximal degree of a polynomial in the grevlex Gröbner basis of $\mathcal{I}_{r+1}(M)$, is the number of monomials of degree $2p - 3$ in $\mathbb{k}[x_1, x_2, x_3, x_4]$. $\square$

Asymptotically, the bound given in [FSS13, Theorem 20] is in $O(p^{5\omega+2})$ whereas that given by Proposition 2.4.2 is in $O(p^{4\omega-1})$.

2.5 EXPERIMENTAL RESULTS

Here we present some experimental results on numbers of reductions to zero in our refinements of the F_5 algorithm compared to the standard F_5 algorithm. The systems used for these results were obtained by building square matrices of homogeneous linear forms with random coefficients over $\mathbb{k} = \mathbb{F}_{65521}$. This field is large enough that the genericity assumptions necessary for our results to hold do so with high probability when taking random coefficients.

All Gröbner basis computations were performed using an implementation of both standard F_5 and our refinements to F_5 written in SageMath (see [The22]) using the FFLAS-FFPACK library (see [Gro19]) for the linear algebra subroutines. When $r = p - 2$, we compute a full Gröbner basis for $F_{p-1}(M)$, whereas when $r < p - 2$, we only compute a Gröbner basis of $F_{r+1}(M)$ up to degree $r + 2$, as past this degree our algorithm performs no differently to standard F_5 .

When $r = p - 2$, all reductions to zero are avoided and thus all Macaulay matrices are full rank. By virtue of Proposition 1.2.2, if a row of $\mathcal{M}_{d,i}$ reduces to zero, then all multiples of this row in $\mathcal{M}_{d',i}$ for $d' > d$ reduce to zero as well, and the standard F_5 algorithm avoids these rows. Note however, that there are a significant number of reductions to zero which do not arise from reductions to zero in lower degree, as evidenced by the discrepancy between the size of the generating set for $\text{Syz}(F_{p-1}(M))$, which is $2p^2 - 2$ (when $r = p - 2$) and the number of reductions to zero encountered by the standard F_5 algorithm.

Note also that by [FSS13, Cor. 19], the largest degree of a polynomial in the reduced grevlex Gröbner basis for $\mathcal{I}_{p-1}(M)$ is $2p - 3$, which is strictly smaller than $2(r + 1) = 2p - 2$. Thus, Theorem 1.2.3 is never used when running either the standard F_5 algorithm, or our refined algorithm on $\mathcal{I}_{p-1}(M)$.

When $r < p - 2$, we avoid all reductions to zero in the Macaulay matrices $\mathcal{M}_{r+2,i}$ for all $1 \leq i \leq \binom{p}{r+1}^2$. As the data in Table 2.1 shows, this already allows us to avoid a significant number of reductions to zero. In fact, in all higher corank cases, over half of the reductions to zero overall appear in degree $r + 2$. The number of reductions to zero in degree $r + 2$ (and thus the size of a minimal generating set for $\text{Syz}(\mathcal{I}_{r+1}(M))$) appears to be

$$\binom{p}{r+2}^2 \left(\frac{2(r+2)(r+1)}{p-r-1} + 2r+2 \right).$$

From this quantity one could derive a refined estimate of the complexity of Algorithm 2.

Note that generically, in the case $r < p - 2$, the largest degree of a polynomial appearing in the reduced grevlex Gröbner basis for $\mathcal{I}_{r+1}(M)$ is $r \cdot (p - r) + 1$ again by [FSS13, Cor. 19]. Thus, in this case, Theorem 1.2.3 is used as soon as the degree exceeds $2(r + 1)$.

Finally, we observe that the speedups which can already be achieved using the results of this paper, within our software framework, increase when p grows and $p - r$ remains fixed. In the case where $p - r = 2$ we obtain a speedup which is close to a factor of 10. This clearly indicates the potential of these results with respect to practical computation times.

Table 2.1: Reductions to zero in standard F_5 (there is none in determinantal- F_5) as well as ratio of timings for standard F_5 compared to determinantal- F_5 , when computing a D -Gröbner basis for the system of $(r + 1)$ -minors of a generic $p \times p$ matrix of homogeneous linear forms in n variables over $\mathbb{k} = \mathbb{F}_{65521}$.

p	r	n	D	Red. to 0 (Std. F_5)	$\frac{(\text{Std. } F_5)}{(\text{Det. } F_5)}$
4	2	4	5	56	0.11
5	3	4	7	129	0.08
6	4	4	9	239	0.43
7	5	4	11	414	0.69
8	6	4	13	663	1.46
9	7	4	15	959	1.65
10	8	4	17	1387	2.26
11	9	4	19	1871	3.07
12	10	4	21	2525	3.99
13	11	4	23	3181	4.94
14	12	4	25	4032	6.00
15	13	4	27	4977	6.03
16	14	4	29	6213	7.93
17	15	4	31	7515	7.22
18	16	4	33	8845	7.99
19	17	4	35	10544	8.65
20	18	4	37	12969	10.59
4	1	9	3	160	1.27
5	2	9	4	450	1.77
6	3	9	5	1008	2.04
7	4	9	6	1960	2.16
8	5	9	7	3456	2.40
9	6	9	8	5670	2.50
5	1	16	3	800	1.34
6	2	16	4	3150	1.59
7	3	16	5	9408	1.72
6	1	25	3	2800	1.28
7	2	25	4	14700	1.39
7	1	36	3	7840	1.22

A REFINED COMPLEXITY ANALYSIS

The complexity analysis of Algorithm 3 in Proposition 2.4.2 is deficient in one key way. It does not take into account the structure of the Macaulay matrices built by the Matrix- F_5 algorithm. To understand this structure, we need insight into the grevlex staircase of determinantal ideals. This chapter is devoted to gaining that understanding. In particular, it seems to be the case that the initial ideal of the ideal of comaximal minors of a square matrix of linear forms is *reverse lexicographic*. We provide a general formula for the number of nonzero entries of Macaulay matrices for such ideals, and use this formula to refine our complexity analysis from Proposition 2.4.2 and, crucially, give a formula for the size of the dense representation of its output. The content and results of this chapter come from the paper [Gop25], which was published in the Journal of Algebra.

3.1 AN EXPLICIT HILBERT SERIES

One of the key inputs into our complexity analysis is the Hilbert series of determinantal ideals. Here, we give explicit formulæ for the Hilbert functions of determinantal ideals in the case $r = p - 2$, under certain genericity assumptions. We accomplish this by analysing a complex associated to these ideals called the Gulliksen-Negård complex, which under suitable genericity assumptions turns out to be a free resolution. This allows us to obtain the Hilbert series we require by computing the ranks of the component modules.

Applying Corollary 1.1.8, we extract from the Gulliksen-Negård complex the Hilbert series of $\mathcal{I}_{p-1}(M)$.

PROPOSITION 3.1.1. — For any $n \geq 3$, $D \geq 1$, let

$$H_{n,D}(t) = \sum_{d=D(n-1)}^{2Dn-3} \left(n^2 \binom{3+d-D(n-1)}{3} - (2n^2-2) \binom{3+d-Dn}{3} + n^2 \binom{3+d-D(n+1)}{3} \right) t^d.$$

Then the property

$$\text{HS}(I) = \begin{cases} \text{true} & \text{if } H_I(t) = H_{n,D}(t) \\ \text{false} & \text{otherwise} \end{cases}$$

is $(4, p-2, p, D)$ -generic.

Proof. By Proposition 1.3.3, there exists a Zariski open subset $U_{\text{CM}} \subseteq \mathbb{A}^{4p^2}$ such that for all $a \in U_{\text{CM}}$, $\mathcal{I}_{p-1}(\phi_a(\mathcal{A}_p^D))$ is Cohen-Macaulay. Subsequently, by Proposition 2.1.1, for any $a \in U_{\text{CM}}$, the Gulliksen-Negård complex is a free resolution of $\mathcal{I}_{p-1}(\phi_a(\mathcal{A}_p^D))$. In order to apply Corollary 1.1.8 on the Gulliksen-Negård complex, we must write, for each $0 \leq i \leq 3$, $\mathcal{E}_i = \bigoplus_{j=1}^{\text{rank}(\mathcal{E}_i)} \mathcal{R}_n(-d_i^{(j)})$.

A REFINED COMPLEXITY ANALYSIS

First, $\text{rank}(\mathcal{E}_0) = n^2$ and for each $1 \leq j \leq n^2$, the image of e_j under ϵ is an $(n-1)$ -minor of $\phi_a(\mathcal{A}_p^D)$. Such a minor is a polynomial of degree $D(n-1)$, so in order for ϵ to be graded, e_i must be a member of the $D(n-1)$ graded piece of $\mathcal{E}_0$. This gives $d_0^{(j)} = D(n-1)$ for all $1 \leq j \leq n^2$.

Next, $\text{rank}(\mathcal{E}_1) = 2n^2 - 2$. Consider the basis elements of $\mathcal{E}_1$ from Section 2.1.1 of the form $(\overline{\mathbf{E}_{i,j}}, 0)$ for $1 \leq i, j \leq n, i \neq j$. These map, under ∂_1 , to $\mathbf{E}_{i,j}\phi_a(\mathcal{A}_p^D)$. Each nonzero coefficient of $\mathbf{E}_{i,j}\phi_a(\mathcal{A}_p^D)$, written in terms of the standard basis elements of $\mathcal{E}_0 = M_p(\mathcal{R}_n)$, is an entry of $\phi_a(\mathcal{A}_p^D)$, and is thus a polynomial of degree D . Thus, in order for the map $\partial_1 : \mathcal{E}_1 \rightarrow \mathcal{E}_0(-D(n-1))$ to be graded, $(\overline{\mathbf{E}_{i,j}}, 0)$ must be a member of the Dn graded piece of $\mathcal{E}_1$. This gives $d_1^{(1)} = Dn$. A similar computation for the other basis elements of $\mathcal{E}_1$, described in Section 2.1.1 shows that, in fact, for all $1 \leq j \leq 2n^2 - 2$, $d_1^{(j)} = Dn$.

By construction, $\text{rank}(\mathcal{E}_2) = n^2$. For any basis element $\mathbf{E}_{i,j}$ of $\mathcal{E}_2$, each nonzero coefficient of $\partial_2(\mathbf{E}_{i,j}) = (\phi_a(\mathcal{A}_p^D)\mathbf{E}_{i,j}, \mathbf{E}_{i,j}\phi_a(\mathcal{A}_p^D))$, written in terms of the basis elements for $\mathcal{E}_1$ given in Section 2.1.1 is again an entry of $\phi_a(\mathcal{A}_p^D)$, and therefore a polynomial of degree D . In order for $\partial_2 : \mathcal{E}_2 \rightarrow \mathcal{E}_1(-Dn)$ to be graded, $\mathbf{E}_{i,j}$ must then be a member of the $D(n+1)$ graded piece of $\mathcal{E}_2$. This gives, for each $1 \leq j \leq n^2$, $d_2^{(j)} = D(n+1)$.

Finally, $\text{rank}(\mathcal{E}_3) = 1$, and $\partial_3(1) = \phi_a(\mathcal{A}_p^D)^C$. When written in terms of the standard basis of $\mathcal{E}_2 = M_p(\mathcal{R}_n)$, the nonzero coefficients of $\phi_a(\mathcal{A}_p^D)^C$ are precisely the cofactors of $\phi_a(\mathcal{A}_p^D)$, which have degree $D(n-1)$, giving $d_3^{(1)} = 2Dn$.

Putting these quantities together and applying Corollary 1.1.8 gives precisely $H_{n,D}(t)$. $\square$

We conclude this section with an auxiliary lemma regarding the structure of the Hilbert series given in Proposition 3.1.1 which will be necessary in order to perform the complexity analyses we give in later sections.

LEMMA 3.1.2. — For all $n-1 \leq d < 2n-3$, $h_{d+1} > h_d$.

Proof. Taking $D = 1$ in Proposition 3.1.1 and simplifying the summand, we find that

$$h_d = \frac{(2+d-n)(d^2 + (-2n+4)d + 4n^2 - 4n + 3)}{3}.$$

Let $f(d) = h_d$ and view f as a continuous function in one real variable. Then $f''(d) = 2d - 2n + 4$ has its unique root at $d = n - 2$. Thus, $f'(d)$ attains its minimum at $d = n - 2$, and f is therefore strictly increasing on the interval $[n-1, \infty)$. $\square$

3.2 REVERSE LEXICOGRAPHIC IDEALS

Reverse lexicographic ideals have been studied for the special place they hold amongst all ideals with a given Hilbert function (see e.g. [Dee96]). After recalling their definition in Section 3.2.1, we prove a general result about the structure of the grevlex leading monomials in the case of a homogeneous reverse lexicographic ideal (Proposition 3.2.2). In Section 3.2.2, we show that as long as a certain Zariski open subset that we make explicit is nonempty, this result can be applied to the determinantal ideals considered in this paper. In the following section, Section 3.3, we further investigate when the determinantal ideals that we consider are generically reverse lexicographic, and relate this property to the so-called *2-strong Lefschetz property*.

Recall that we have fixed our monomial order $\succ$ to be the graded reverse lexicographic order and suppressed the symbol $\succ$ from all relevant notation.

3.2.1 THE GREVLEX STAIRCASE OF A HOMOGENEOUS REVERSE LEXICOGRAPHIC IDEAL

Let $I \subseteq \mathcal{R}$ be a nonzero ideal. We call I *reverse lexicographic* if for all $\tau \in \text{LM}_{\prec}(I)$,

$$\{\sigma \in \text{Mon}_{\deg \tau}(\mathcal{R}_n) : \sigma \succ \tau\} \subseteq \text{LM}_{\prec}(I).$$

We begin with a simple and helpful observation about the grevlex staircase of a reverse lexicographic ideal.

LEMMA 3.2.1. — Let $I \subseteq \mathcal{R}_n$ be a reverse lexicographic ideal. Let $\tau \in \text{LM}_{\prec}(I)$ and x_j be the smallest variable in τ . For any variable $y \in \{x_1, \dots, x_n\}$ with $y \succ x_j$, the monomial $\sigma = \frac{\tau}{x_j}y \in \text{Mon}_{\deg \tau}(\mathcal{R}_n)$ is such that $\sigma \succ \tau$ and $\sigma \in \text{LM}_{\prec}(I)$.

We come now to the main result of this section, which provides a formula to calculate the number of polynomials of degree $d+1$ in a grevlex Gröbner basis of a homogeneous reverse lexicographic ideal whose leading monomials are not divisible by any leading monomial of degree d .

PROPOSITION 3.2.2. — Let $F \subseteq \mathbb{k}[x_1, \dots, x_n]$ be a sequence of homogeneous polynomials, all of degree d_0 . Suppose $I = \langle F \rangle$ is a reverse lexicographic ideal. Let $\text{HF}_I(d) = h_d$ be the Hilbert function of I and let D be the largest degree of a polynomial appearing in the reduced grevlex Gröbner basis of F . For any $d_0 \leq d \leq D$, let G_d be the set of elements of degree at most d in the reduced grevlex Gröbner basis for F and let ℓ_d be the largest integer such that

$$\binom{\ell_d + d - 1}{\ell_d - 1} < h_d.$$

Then for any $d_0 \leq d \leq D$,

$$\begin{aligned} \#(\text{LM}_{\prec}(G_{d+1}) \setminus \text{LM}_{\prec}(G_d)) &= h_{d+1} + (\ell_d - n)h_d \\ &\quad + \sum_{j=1}^{\ell_d} \binom{j + d - 2}{j - 1} (j - 1) \\ &\quad - \ell_d \binom{\ell_d + d - 1}{\ell_d - 1} \end{aligned}$$

Proof. We begin by noting that G_{d+1} can be obtained from G_d by multiplying each of the h_d nonzero rows of $\widetilde{\mathcal{M}}_d$ by each of the n variables to build $\mathcal{M}_{d+1}$, echelonizing to obtain $\widetilde{\mathcal{M}}_{d+1}$, then discarding zero rows and rows that are redundant because their leading terms are already divisible by those in $\text{LM}_{\prec}(G_d)$. Letting z_{d+1} (resp. r_d) be the number of these zero (resp. redundant) rows, we can write

$$\#(\text{LM}_{\prec}(G_{d+1}) \setminus \text{LM}_{\prec}(G_d)) = nh_d - z_{d+1} - r_{d+1}. \quad (3.1)$$

Note also that if the echelonization process alters the leading term of some row of $\mathcal{M}_{d+1}$ built in this way, then either that row reduces to zero, or its new leading term is no longer divisible by any monomial in $\text{LM}_{\prec}(G_d)$. Thus, denoting by c_{d+1} the number of rows of $\mathcal{M}_{d+1}$ which are to be reduced during the echelonization process, one has

$$c_{d+1} = z_{d+1} + \#(\text{LM}_{\prec}(G_{d+1}) \setminus \text{LM}_{\prec}(G_d)) \quad (3.2)$$

$$\text{and } r_{d+1} = nh_d - c_{d+1}. \quad (3.3)$$

Combining Eqs. (3.1) to (3.3) gives

$$\#(\text{LM}_{\prec}(G_{d+1}) \setminus \text{LM}_{\prec}(G_d)) = h_{d+1} - nh_d + c_{d+1}.$$

The rest of the proof consists in computing c_{d+1} . Fix $\tau \in \text{LM}_{\prec}(G_d)$, and let x_j be the grevlex smallest variable in τ . Then by Lemma 3.2.1, for each of the $j - 1$ variables larger than x_j , there exists some $\sigma \in \text{LM}_{\prec}(G_d)$ such that σx_j appears as the leading term of some row of $\mathcal{M}_{d+1}$ which can be reduced by a multiple of τ . Thus, the row of $\widetilde{\mathcal{M}}_d$ with leading term τ generates exactly $j - 1$ rows of $\mathcal{M}_{d+1}$ which are to be reduced. The number of monomials of degree d whose grevlex smallest variable is some x_j is simply

$$\underbrace{\binom{j+d-1}{j-1}}_{\substack{\text{number of monomials} \\ \text{of degree } d \text{ in } j \\ \text{variables}}} - \underbrace{\binom{j+d-2}{j-2}}_{\substack{\text{number of monomials} \\ \text{of degree } d \text{ in } j-1 \\ \text{variables}}} = \underbrace{\binom{j+d-2}{j-1}}_{\substack{\text{number of monomials} \\ \text{of degree } d \text{ with} \\ \text{grevlex smallest} \\ \text{variable } x_j}}$$

Finally, since the leading monomials of $\widetilde{\mathcal{M}}_d$ are simply the h_d grevlex largest monomials of degree d , we obtain the final result

$$\begin{aligned} \#(\text{LM}_{\prec}(G_{d+1}) \setminus \text{LM}_{\prec}(G_d)) &= h_{d+1} - nh_d + c_{d+1} \\ &= h_{d+1} - nh_d + \sum_{j=1}^{\ell_d} \binom{j+d-2}{j-1} (j-1) \\ &\quad + \ell_d \left(h_d - \binom{\ell_d+d-1}{\ell_d-1} \right) \\ &= h_{d+1} + (\ell_d - n)h_d + \sum_{j=1}^{\ell_d} \binom{j+d-2}{j-1} (j-1) \\ &\quad - \ell_d \binom{\ell_d+d-1}{\ell_d-1}. \end{aligned} \quad \square$$

3.2.2 REVERSE LEXICOGRAPHIC DETERMINANTAL IDEALS

With the hope of applying Proposition 3.2.2, we investigate here the conditions under which the determinantal ideals we consider are indeed reverse lexicographic. We begin by showing that the Macaulay matrices of reverse lexicographic ideals possess a certain structure. Next, we construct an explicit Zariski open subset whose points correspond to reverse lexicographic ideals of the form $\mathcal{I}_{p-1}(M)$. That this Zariski open subset is nonempty is left as a conjecture, which we give insight into in Section 3.3.

LEMMA 3.2.3. — Let $F \subseteq \mathcal{R}_n$ be a sequence of homogeneous polynomials. Then $I = \langle F \rangle$ is a reverse lexicographic ideal if and only if for any $d \in \mathbb{Z}_{>0}$, the first h_d columns of the Macaulay matrix in degree d , $\mathcal{M}_d$, have rank $h_d = \text{rank}(\mathcal{M}_d)$, or equivalently, the echelonized Macaulay matrix in degree d , $\widetilde{\mathcal{M}}_d$ takes the form

$$\widetilde{\mathcal{M}}_d = \left(I \mid X \right)$$

after having removed reductions to zero and up to a permutation of rows, where I is the identity matrix of size $h_d \times h_d$.

Proof. Fix $d \in \mathbb{Z}_{>0}$. Suppose I is reverse lexicographic, and let

$$\tau_0 = \min\{\tau \in \text{LM}_{\prec}(I) : \deg(\tau) = d\}.$$

Then τ_0 appears as the rightmost pivot of $\widetilde{\mathcal{M}}_d$. Since

$$\{\sigma \in \text{Mon}_d(\mathcal{R}_n) : \sigma \succ \tau\} \subseteq \text{LM}_{\prec}(I),$$

all columns to the left of that indexed by τ_0 contain a pivot.

Conversely, suppose $\widetilde{\mathcal{M}}_d$ takes the desired form. For any $\tau \in \text{LM}_{\prec}(I)$ of degree d , the column indexed by τ contains a pivot, and thus belongs to the left identity block. Thus, any column to the left of that indexed by τ must also contain a pivot. $\square$

We conclude by conjecturing that comaximal determinantal ideals of matrices of linear forms are indeed reverse lexicographic, and describing the appropriate Zariski open subset which must be nonempty in order for this to be true.

CONJECTURE 3.2.4. — Let RL be the property defined by

$$\text{RL}(I) = \begin{cases} \text{true} & \text{if } I \text{ is reverse lexicographic} \\ \text{false} & \text{otherwise} \end{cases}.$$

Then for any $p \geq 3$, RL is $(4, p-2, p, 1)$ -generic.

By Lemma 3.2.3, it is sufficient to prove that there exists some Zariski open subset $U \subseteq \mathbb{A}^{4p^2}$ such that for all $a \in U$, for any $d \in \mathbb{Z}_{>0}$, the reduced Macaulay matrix $\widetilde{\mathcal{M}}_d(F_{p-1}(\phi_a(\mathcal{A}_p^1)))$ takes the form

$$\widetilde{\mathcal{M}}_d(F_{p-1}(\phi_a(\mathcal{A}_p^1))) = (I \mid X)$$

after a suitable row permutation and removal of reductions to zero. Recall that the notation used here was introduced in Section 1.3.

By Proposition 3.1.1, there exists a Zariski open subset $U_{\text{HS}} \subseteq \mathbb{A}^{4p^2}$ such that for all $a \in U_{\text{HS}}$, the Hilbert series of $\mathcal{I}_{p-1}(\phi_a(\mathcal{A}_p^1))$ is the one given in Proposition 3.1.1. For any $d \in \mathbb{Z}_{>0}$, let $h_d = \text{HF}_{\mathcal{I}_{p-1}(\phi_a(\mathcal{A}_p^1))}(d)$.

Now fix some $d \in \mathbb{Z}_{>0}$, $n-1 \leq d \leq 2n-3$. The determinant of the square submatrix of the Macaulay matrix $\widetilde{\mathcal{M}}_d(F_{p-1}(\mathcal{A}_p^1))$ given by the first h_d columns after removing zero rows is a polynomial in $\mathbf{a}$, $g_d(\mathbf{a}) \in \mathbb{k}[\mathbf{a}]$.

The distinguished Zariski open set $\mathbb{A}^{4p^2} \setminus V(g_d(\mathbf{a}))$ consists precisely of those $a \in \mathbb{A}^{4p^2}$ such that

$$\widetilde{\mathcal{M}}_d(F_{p-1}(\mathcal{A}_p^1)) = (I \mid X).$$

By [FSS13, Corollary 19], there exists a Zariski open subset $O \subseteq \mathbb{A}^{4p^2}$ such that the largest degree Macaulay matrix which needs to be reduced is $\mathcal{M}_{2n-3}$. Thus, letting

$$U_{\text{RL}} = O \cap U_{\text{HS}} \cap \bigcap_{d=n-1}^{2n-3} \left(\mathbb{A}^{4p^2} \setminus V_{\mathbb{k}}(g_d(\mathbf{a})) \right),$$

for any $a \in U_{\text{RL}}$, the ideal $\mathcal{I}_{p-1}(\phi_a(\mathcal{A}_p^1))$ is reverse lexicographic.

It is not clear, however, that the set U_{RL} is nonempty. Equivalently, it is not clear that the polynomials $g_d(\mathfrak{a}) \in \mathbb{k}[\mathfrak{a}]$ are nonzero.

In [Par10, Theorem 3] (see also the references therein), necessary and sufficient conditions are given in order for a given power series to be the Hilbert series of a reverse lexicographic ideal. By Lemma 3.1.2, these assumptions are satisfied by the Hilbert series given in Proposition 3.1.1.

In the following section, we relate Conjecture 3.2.4 to the Lefschetz properties (see [HMM⁺13b]), and show that under certain genericity assumptions, $\mathcal{I}_{p-1}(M)$ has the *weak Lefschetz property*.

3.3 DETERMINANTAL IDEALS AND THE LEFSCHETZ PROPERTIES

We devote this section to exploring conditions under which determinantal ideals possess the so-called Lefschetz properties, in the hope of shedding some light on Conjecture 3.2.4. These properties have been widely studied in various contexts, notably that of Artinian Gorenstein algebras.

This section is entirely self-contained, and for ease of exposition we do not provide definitions of several classical properties from commutative algebra (e.g. Artinian, Gorenstein). Such definitions and a wealth of related facts can be found, e.g., in [Mat87].

Let $A = \bigoplus_{d=0}^c A_d$ be a graded Artinian $\mathbb{k}$ -algebra with $A_c \neq 0$. The algebra A has the *weak Lefschetz property* (see [HMM⁺13b, Definition 3.1]), or simply WLP if there exists some $\ell \in A_1$ such that for all $0 \leq d \leq c-1$, the map of $\mathbb{k}$ -vector spaces

$$\times \ell : A_d \rightarrow A_{d+1}$$

given by multiplication by ℓ has full rank. Such an ℓ is called a *weak Lefschetz element*. If, in addition, for all $0 \leq d \leq c-1$ and $1 \leq s \leq c-d$, the map

$$\times \ell^s : A_d \rightarrow A_{d+s}$$

has full rank, then A is said to have the *strong Lefschetz property* (see [HMM⁺13b, Definition 3.8]), or simply SLP, and ℓ is called a *strong Lefschetz element*.

For some $t \geq 1$, A has the t -WLP (resp. t -SLP) if there are some $\ell_1, \dots, \ell_t \in A_1$ such that ℓ_1 is a weak (resp. strong) Lefschetz element for A and, for each $1 < i \leq t$, the linear form ℓ_i is a weak (resp. strong) Lefschetz element for $A/(\ell_1, \dots, \ell_{i-1})$ (see [HMM⁺13a, Definition 6.1]).

When A is an Artinian ideal of a polynomial ring over $\mathbb{k}$, the notion of the t -SLP has a useful description in terms of the Hilbert series of A .

PROPOSITION 3.3.1 ([HMM⁺13a, Remark 6.11]). — Let $I \subseteq \mathcal{R}_n$ be a graded Artinian ideal. Then ℓ is a strong Lefschetz element for $\mathcal{R}_n/I$ if and only if for all $s \geq 1$,

$$\text{HF}_{\mathcal{R}_n/(I+(\ell^s))}(d) = \max\{\text{HF}_{\mathcal{R}_n/I}(d) - \text{HF}_{\mathcal{R}_n/I}(d-s), 0\}.$$

If $I \subseteq \mathcal{R}_n$ is an Artinian ideal, then $\mathcal{R}_n/I$ has dimension zero. Thus, there is some D such that for all $d > D$, $\text{HF}_{\mathcal{R}_n/I}(d) = 0$. Clearly, one can restrict to $s \leq D$ in the above proposition.

THEOREM 3.3.2 ([HMM⁺13a, Corollary 6.30]). — Let $I \subseteq \mathbb{k}[x_1, x_2, x_3, x_4]$ be a graded Artinian ideal such that $\mathcal{R}_4/I$ has the 2-SLP. Then the generic initial ideal $\text{gin}(I)$ of I with respect to the grevlex order is the unique weakly reverse lexicographic ideal with Hilbert function $\text{HF}_{\mathcal{R}_4/I}$.

To establish Conjecture 3.2.4, it is therefore sufficient to prove, in our setting, that the 2-SLP is $(4, p - 2, p, 1)$ -generic. On the other hand, while it would not establish Conjecture 3.2.4, it would still be useful to discern whether or not the WLP is $(4, p - 2, p, 1)$ -generic.

THEOREM 3.3.3 ([MMR03, Remark 4.4]). — Let $I \subseteq \mathbb{k}[x_1, \dots, x_n]$ be a graded ideal. If I is Artinian and has no generator in degree 1, and if the quotient $\mathcal{R}_n/I$ is Gorenstein and compressed with even socle degree, then $\mathcal{R}_n/I$ has the weak Lefschetz property.

The socle degree of a zero-dimensional ideal $I \subseteq \mathbb{k}[x_1, \dots, x_n]$ is simply the degree of its Hilbert series, which is a polynomial. In this context, to be compressed simply means that $\text{HF}_{\mathcal{R}_n/I}(d) = \text{HF}_{\mathcal{R}_n}(d)$ for all $0 \leq d \leq \frac{s}{2}$, where $s = \deg(H_{\mathcal{R}_n/I}(t))$ is the socle degree of $\mathcal{R}_n/I$.

By [FSS13, Theorem 10], the property of being zero-dimensional is $(4, p - 2, p, 1)$ -generic, thus so is the property of being Artinian.

As soon as $p \geq 3$, the 2-minors of M are of degree at least 2 and generate $\mathcal{I}_{p-1}(M)$. Again by [FSS13, Theorem 10], the property that $\mathcal{R}_n/I$ has socle degree exactly $2p - 2$ is $(4, p - 2, p, 1)$ -generic.

If M is a matrix of linear forms the degree of the $(p - 1)$ -minors of M is $p - 1$. Thus, the property that $\mathcal{R}_n/I$ is compressed is also $(4, p - 2, p, 1)$ -generic.

Finally, by [BV88, Theorem 2.26], the Gulliksen-Negård complex is a free resolution of M as soon as $\mathcal{I}_{p-1}(M)$ is Cohen-Macaulay and the final module of this resolution has rank one (see Section 2.1.1). Thus, the property that $\mathcal{I}_{p-1}(M)$ is Gorenstein is also $(4, p - 2, p, 1)$ -generic.

3.4 COMPLEXITY ANALYSIS

We consider a matrix of the form $M = \phi_a(\mathcal{A}_p^1)$, where a is taken to be a point in some suitable Zariski open subset of $\mathbb{A}^{4p^2}$. We make precise which Zariski open subsets we must take a to lie in below, appealing to the various genericity statements we have established above (e.g. Propositions 1.3.3 and 3.1.1 and Conjecture 3.2.4). Our complexity analysis begins by computing the number of polynomials of each degree in the reduced grevlex Gröbner basis of $\mathcal{I}_{p-1}(M)$.

The coefficient of t^d in the Hilbert series of $\mathcal{I}_{p-1}(M)$ is, by definition, the dimension of the $\mathbb{k}$ -vector space of homogeneous polynomials in $\mathcal{I}_{p-1}(M)$ of degree d . This dimension is also precisely the rank of the Macaulay matrix of $F_{p-1}(M)$ in degree d . Combining these ranks with the aforementioned count of polynomials of degree d in the reduced grevlex Gröbner basis of $\mathcal{I}_{p-1}(M)$ allows us to compute tight bounds on the complexity of the overall Gröbner basis computation using fast linear algebra techniques.

3.4.1 BOUNDING $\#(\text{LM}_{\prec}(G_{d+1}) \setminus \text{LM}_{\prec}(G_d))$

The work of computing the number of polynomials of degree d in the reduced grevlex Gröbner basis for $\mathcal{I}_{p-1}(M)$ is already accomplished by our analysis of staircases of reverse lexicographic ideals in Section 3.2. The following proposition arises from plugging in the relevant quantities into the formula given in Proposition 3.2.2.

PROPOSITION 3.4.1. — Suppose Conjecture 3.2.4 is true. Fix $a \in U_{\text{RL}} \cap U_{\text{HS}} \subseteq \mathbb{A}^{4p^2}$. Let $M = \phi_a(\mathcal{A}_p^1)$. For any integer $p - 1 \leq d < 2p - 3$,

$$\#(\text{LM}_{\prec}(G_{d+1}) \setminus \text{LM}_{\prec}(G_d)) = \frac{(d - 2p + 3)(d - 2p + 2)}{2},$$

A REFINED COMPLEXITY ANALYSIS

where G_d is the reduced d -Gröbner basis for $\mathcal{I}_{p-1}(M)$ with respect to the grevlex order.

Proof. If Conjecture 3.2.4 is true, then the ideal $\mathcal{I}_{p-1}(M)$ is reverse lexicographic. Therefore, we can apply Proposition 3.2.2. We begin by showing that for all $d \geq p-1$, the integer ℓ_d is 3. Recall, from the statement of Proposition 3.2.2, that ℓ_d is defined to be the largest integer such that

$$\binom{\ell_d + d - 1}{\ell_d - 1} < h_d,$$

where $h_d = \text{HF}_{\mathcal{I}_{p-1}(M)}(d)$. For any $a \in U_{\text{HS}}$, the Hilbert series $H_{\mathcal{I}_{p-1}(M)}(t)$ is given by Proposition 3.1.1.

First, note that $h_{p-1} = p^2$ and

$$\binom{(p-1)+2}{2} = \frac{p^2 + p}{2}.$$

Since $p > 1$, this shows that $\ell_{p-1} \geq 3$. As $n = 4$, $\ell_{p-1} \leq 3$.

We proceed by induction. Suppose $\ell_d = 3$ for some $d \geq p-1$. Then there must be at least one monomial τ in which the variable x_4 appears in $\text{LM}_{\prec}(G_d)$. Subsequently for any variable x , $x\tau \in \text{LM}_{\prec}(G_{d+1})$ and $x\tau$ contains the variable x_4 as well, showing that $\ell_{d+1} = 3$.

Finally, applying Proposition 3.2.2, we obtain

$$\begin{aligned} \# \text{LM}_{\prec}(G_{d+1}) \setminus \text{LM}_{\prec}(G_d) &= h_{d+1} - h_d + \binom{d}{1} + 2\binom{d+1}{2} - 3\binom{d+2}{2} \\ &= h_{d+1} - h_d + d + 2\binom{d+1}{2} - 3\binom{d+2}{2} \\ &= \frac{(d-2p+3)(d-2p+2)}{2}. \end{aligned} \quad \square$$

3.4.2 LOWER BOUNDS

As a first application of Proposition 3.4.1, we establish an exact expression for the size of the reduced grevlex Gröbner basis of ideals of the form $\mathcal{I}_{p-1}(M)$ under certain genericity assumptions.

PROPOSITION 3.4.2. — Fix $a \in U_{\text{RL}} \subseteq \mathbb{A}^{4p^2}$. Let $M = \phi_a(\mathcal{A}_p^1)$. The total number of polynomials in the reduced grevlex Gröbner basis for $\mathcal{I}_{p-1}(M)$ is

$$\#G = \frac{p(p+1)(p+2)}{6}.$$

Proof. Enumerating the polynomials in the reduced grevlex Gröbner basis for $\mathcal{I}_{p-1}(M)$ is equivalent to enumerating the leading monomials of these polynomials. That is,

$$\#G = \# \text{LM}_{\prec}(G_{p-1}) + \sum_{d=p-1}^{2p-4} \#(\text{LM}_{\prec}(G_{d+1}) \setminus \text{LM}_{\prec}(G_d)).$$

Using Proposition 3.4.1,

$$\#G = p^2 + \sum_{d=p-1}^{2p-4} \frac{(d-2p+3)(d-2p+2)}{2} = \frac{p(p^2 + 3p + 2)}{6}. \quad \square$$

Recall that here, we consider the computation of a dense representation of the sought Gröbner basis, meaning that all coefficients in $\mathbb{k}$ of all elements in this basis are explicitly computed.

The expression obtained in Proposition 3.4.2 counts only the leading monomials of the polynomials in the reduced grevlex Gröbner basis of $\mathcal{I}_{p-1}(M)$, and not the smaller monomials in these polynomials. In the following theorem, we compute — under our genericity assumptions — the number of nonzero coefficients in each of these polynomials.

THEOREM 3.4.3. — Suppose Conjecture 3.2.4 is true. Fix $a \in U_{\text{RL}} \cap U_{\text{HS}} \subseteq \mathbb{A}^{4p^2}$. Let $M = \phi_a(\mathcal{A}_p^1)$. The number of elements of $\mathbb{k}$ in the dense representation of the reduced grevlex Gröbner basis of $\mathcal{I}_{p-1}(M)$ is asymptotically bounded from below by p^6 .

Proof. Since $a \in U_{\text{HS}}$, the Hilbert series of $\mathcal{I}_{p-1}(M)$ is the one given in Proposition 3.1.1. Let $h_d = \text{HF}_{\mathcal{R}/\mathcal{I}_{p-1}(M)}(d)$. The number of monomials appearing in a degree d polynomial in the reduced grevlex Gröbner basis for $\mathcal{I}_{p-1}(M)$ is

$$\binom{3+d}{3} - h_d + 1.$$

Therefore, using Proposition 3.4.1, we find that the number of nonzero monomials appearing in the grevlex Gröbner basis for $\mathcal{I}_{p-1}(M)$ is

$$N = n^2 \left(\binom{2+p}{3} - p^2 + 1 \right) + \sum_{d=p-1}^{2p-4} \frac{(d-2p+3)(d-2p+2)}{2} \left(\binom{3+d}{3} - h_d + 1 \right).$$

Expanding this gives

$$N = \frac{1}{72}p^6 + \frac{13}{120}p^5 - \frac{4}{9}p^4 + \frac{13}{24}p^3 + \frac{31}{72}p^2 + \frac{7}{20}p \quad \square$$

3.4.3 UPPER BOUNDS

For a given degree $d > p-1$, Algorithm 3 builds the Macaulay matrix in degree d by multiplying each row of the Macaulay matrix in degree $d-1$ by each variable, utilising the signatures attached to each row to avoid redundancies in rows. The reverse lexicographic property of determinantal ideals provides the unreduced Macaulay matrix in degree d with a precise structure, which we analyse to obtain complexity upper bounds.

PROPOSITION 3.4.4. — Suppose Conjecture 3.2.4 is true. Fix $a \in U_{\text{RL}} \subseteq \mathbb{A}^{4p^2}$. Let $M = \phi_a(\mathcal{A}_p^1)$ and let $d \in \mathbb{Z}_{>0}$, $p-1 \leq d < 2p-3$. Then after a suitable row permutation, the unreduced Macaulay matrix $\mathcal{M}_{d+1}$ of $\mathcal{I}_{p-1}(M)$ built by Algorithm 3 is of the form

$$\left(\begin{array}{c|c} T_{d+1} & X_{d+1} \\ \hline A_{d+1} & Y_{d+1} \end{array} \right)$$

where T_{d+1} is a square upper triangular block of size $h_{d+1} - \frac{(d-2p+3)(d-2p+2)}{2}$ and $h_{d+1} = \text{HF}_{\mathcal{I}_{p-1}(M)}(d+1)$ is the Hilbert function of $\mathcal{I}_{p-1}(M)$ evaluated at $d+1$.

A REFINED COMPLEXITY ANALYSIS

Proof. Let G be the reduced grevlex Gröbner basis of $\mathcal{I}_{p-1}(M)$. We partition the rows of $\widetilde{\mathcal{M}}_{d+1}$ into the following two sets

$$R_1 = \{f \in \text{rows}(\widetilde{\mathcal{M}}_{d+1}) : f \in G\} \quad R_2 = \{f \in \text{rows}(\widetilde{\mathcal{M}}_{d+1}) : f \notin G\}.$$

Let $\tau = \min_{f \in R_2} \{\text{LM}_{\prec}(f)\}$. Then there must exist some variable x_j such that $\frac{\tau}{x_j} \in \text{LM}_{\prec}(G)$. Fix $\sigma \in R_1$. In Proposition 3.4.1 it was shown that all monomials involving x_1, x_2, x_3 appear in $\text{LM}_{\prec}(G_{p-1})$. Thus, since $d+1 > p-1$, $x_4 \mid \sigma$. As G is a reduced Gröbner basis and $\sigma \in \text{LM}_{\prec}(G)$, the monomial $\frac{\sigma}{x_4}$ is not in $\text{LM}_{\prec}(G)$. Since we assume Conjecture 3.2.4, this forces $\frac{\tau}{x_j} \succ \frac{\sigma}{x_4}$. Subsequently, since $x_j \succ x_4$, we have that $\tau \succ \sigma$.

This shows that any monomial of $\text{LM}_{\prec}(R_1)$ is smaller than τ . On the other hand, assuming Conjecture 3.2.4, for any $\tau' \succ \tau$, there exists some $g \in R_2$ such that $\text{LM}_{\prec}(g) = \tau'$.

Now for any polynomial $g \in R_2$, there exists some $h \in \text{rows}(\widetilde{\mathcal{M}}_d)$ such that $\text{LM}_{\prec}(h) \mid \text{LM}_{\prec}(g)$. Since Algorithm 1 constructs the rows of $\mathcal{M}_{d+1}$ by multiplying the rows of $\widetilde{\mathcal{M}}_d$ by suitable variables, we see that there must be a row of $\mathcal{M}_{d+1}$ with leading monomial precisely $\text{LM}_{\prec}(g)$. Thus, the set of rows of $\mathcal{M}_{d+1}$ which, upon echelonization, are in R_2 form a submatrix of $\mathcal{M}_{d+1}$ of the form

$$\left(\begin{array}{c|c} T_{d+1} & X_{d+1} \end{array} \right)$$

with T_{d+1} upper triangular. The rows of T_{d+1} are in bijection with R_2 , and by Proposition 3.4.1, the set R_1 has cardinality $\frac{(d-2p+3)(d-2p+2)}{2}$. As $\mathcal{M}_{d+1}$ has exactly h_{d+1} rows, we see that T_{d+1} has $h_{d+1} - \frac{(d-2p+3)(d-2p+2)}{2}$ rows. $\square$

By Proposition 3.4.4, A_{d+1} is a matrix with $\alpha_{d+1} = \frac{(d-2p+3)(d-2p+2)}{2}$ rows, T_{d+1} is a matrix with $\beta_{d+1} = h_{d+1} - \alpha_{d+1}$ rows, and X_{d+1} is a matrix with $\gamma_{d+1} = \binom{4+d}{3} - \beta_{d+1}$ columns. We begin by establishing various useful facts about the behaviour of $h_{d+1}, \alpha_{d+1}, \beta_{d+1}, \gamma_{d+1}$.

LEMMA 3.4.5. — For all $p-1 < d < 2p-3$, $\alpha_{d+1} < \alpha_d$.

Proof. Let $f(d) = \alpha_d$ and view f as a continuous function in one real variable. Then $f'(d) = d - 2p + \frac{5}{2}$ has its unique root at $d = 2p - \frac{5}{2}$. Thus, f is strictly decreasing on the interval $(-\infty, 2p - \frac{5}{2}]$. $\square$

LEMMA 3.4.6. — For all $p-1 \leq d < 2p-3$, $\alpha_{d+1} < \beta_{d+1}$.

Proof. In view of Lemmas 3.1.2 and 3.4.5, it suffices to show that $\alpha_p < \frac{h_p}{2}$. We have $\alpha_p = p^{\frac{p^2-3p+2}{2}}$ and $h_p = 2p^2 + 2$. Thus, $\frac{h_p}{2} - \alpha_p = \frac{p^2+3p}{2}$, which is certainly positive for $p \geq 3$. $\square$

LEMMA 3.4.7. — For all $p-1 \leq d < 2p-3$, $\alpha_{d+1} \leq \gamma_{d+1}$.

Proof. For ease of exposition, in this proof we take $\mathcal{R} = \mathcal{R}_4$.

Recall that $h_{d+1} = \dim_{\mathbb{k}}(\mathcal{I}_{p-1}(M)_{d+1})$. The $\mathbb{k}$ -vector space $\mathcal{I}_{p-1}(M)_{d+1}$ is a sub- $\mathbb{k}$ vector space of $\mathcal{R}_{[d+1]}$. Since $\dim_{\mathbb{k}}(\mathcal{R}_{[d+1]}) = \binom{4+d}{3}$, we have that $h_{d+1} \leq \binom{4+d}{3}$. Finally,

$$\begin{aligned} \gamma_{d+1} &= \binom{4+d}{3} - \beta_{d+1} \\ &= \binom{4+d}{3} - h_{d+1} + \alpha_{d+1} \\ &\geq \alpha_{d+1} \end{aligned}$$

$\square$

Before turning to the complexity of echelonizing a Macaulay matrix in a fixed degree, we need one final auxiliary lemma regarding the cost of solving several triangular systems.

LEMMA 3.4.8 (see [DGP04, Lemma 3.1]). — Let $U \in \mathbb{k}^{p \times p}$ be an invertible $p \times p$ upper triangular matrix and $V \in \mathbb{k}^{p \times q}$ a $p \times q$ matrix. Let $C(p, q)$ be the arithmetic complexity of computing $U^{-1}V$ using [DGP04, ULeft-TRSM(U, V)]. Then

$$C(p, q) \in \begin{cases} O(qp^{\omega-1}) & \text{if } p \leq q \\ O(p^2q^{\omega-2}) & \text{if } p > q \end{cases}.$$

Proof. For $p \leq q$, this is precisely the statement of [DGP04, Lemma 3.1]. Assume then that $p > q$. In the following, we denote by C_ω the constant associated to rectangular matrix multiplication with exponent ω . That is, the cost of multiplying a $p \times q$ matrix by a $q \times s$ matrix (all with entries in $\mathbb{k}$) is bounded by $C_\omega \min\{p, q, s\}^{\omega-2} \max\{pq, ps, qs\}$. We use the case $p \leq q$ as a base case for the recursion. The complexity in this case is given directly by [DGP04, Lemma 3.1]. That is,

$$C(p, q) = \begin{cases} \frac{C_\omega}{2(2^{\omega-2}-1)} qp^{\omega-1} & \text{if } p \leq q \\ C(\lceil \frac{p}{2} \rceil, q) + C(\lfloor \frac{p}{2} \rfloor, q) + C_\omega p^2 q^{\omega-2} & \text{otherwise} \end{cases}.$$

By padding U with an identity block and V with zeroes, we may assume that $\frac{p}{q}$ is a power of two. Subsequently, we have

$$\begin{aligned} C(p, q) &= \frac{p}{q} C(q, q) + C_\omega p^2 q^{\omega-2} \sum_{j=0}^{\log_2(\frac{p}{q})-1} \frac{1}{2^j} \\ &= \frac{C_\omega}{2(2^{\omega-2}-1)} pq^{\omega-1} + 2C_\omega p^2 q^{\omega-2} \left(1 - \frac{q}{p}\right) \\ &= 2C_\omega p^2 q^{\omega-2} + \left(\frac{C_\omega}{2(2^{\omega-2}-1)} - 2C_\omega\right) pq^{\omega-1} \end{aligned}$$

as desired. □

Putting together Lemmas 3.1.2 and 3.4.5 to 3.4.7, we can compute an upper bound on the cost of echelonizing a Macaulay matrix in a fixed degree.

PROPOSITION 3.4.9. — For any $p-1 \leq d \leq 2p-3$, the number of arithmetic operations in $\mathbb{k}$ required to compute the matrix $\widetilde{\mathcal{M}}_{d+1}$ from $\mathcal{M}_{d+1}$ is in

$$O(\beta_{d+1}^2 \alpha_{d+1}^{\omega-2} + \alpha_{d+1}^{\omega-2} \beta_{d+1} \gamma_{d+1}).$$

Proof. The computation of $\widetilde{\mathcal{M}}_{d+1}$ from $\mathcal{M}_{d+1}$ can be broken up into four steps.

Step 1. First, we echelonize the upper block, which is of the form $\left(\begin{array}{c|c} T_{d+1} & X_{d+1} \end{array} \right)$, with T_{d+1} upper triangular. Applying Lemma 3.4.8, the cost of this step is $O(\beta_{d+1}^2 \alpha_{d+1}^{\omega-2})$.

Step 2. Next, we use the I_{d+1} block to eliminate A_{d+1} . The resulting matrix takes the form

$$\left(\begin{array}{c|c} I_{d+1} & X_{d+1} \\ \hline 0 & Y_{d+1} - A_{d+1}X_{d+1} \end{array} \right).$$

A REFINED COMPLEXITY ANALYSIS

The arithmetic complexity of this step is bounded by the cost of computing $A_{d+1}X_{d+1}$. The matrix A_{d+1} has α_{d+1} rows and β_{d+1} columns, while X_{d+1} has β_{d+1} rows and γ_{d+1} columns. By Lemmas 3.4.6 and 3.4.7,

$$\min\{\alpha_{d+1}, \beta_{d+1}, \gamma_{d+1}\} = \alpha_{d+1}.$$

Hence, by [Kni95, Section 2.1], the matrix $A_{d+1}X_{d+1}$ can be computed using $O(\alpha_{d+1}^{\omega-2}\beta_{d+1}\gamma_{d+1})$ arithmetic operations in $\mathbb{k}$.

Step 3. Next, we compute the reduced row echelon form of $Y_{d+1} - A_{d+1}X_{d+1}$ which has α_{d+1} rows and β_{d+1} columns. By Lemma 3.4.6, and using the general results of [Sto00, Section 2.2] (see also [JPS13, Appendix A]), this can be done using $O(\alpha_{d+1}^{\omega-1}\gamma_{d+1})$ operations in $\mathbb{k}$.

Step 4. The matrix after the previous step takes the form

$$\left(\begin{array}{c|c|c} I_{d+1} & X_{d+1}^{(1)} & X_{d+1}^{(2)} \\ \hline 0 & I^{(\alpha_{d+1})} & Y_{d+1} \end{array} \right),$$

where $X_{d+1} = \left(\begin{array}{c|c} X_{d+1}^{(1)} & X_{d+1}^{(2)} \end{array} \right)$ and $I^{(\alpha_{d+1})}$ is an identity matrix of size α_{d+1} . The final step of the echelonization process is then to reduce X_{d+1} using the identity block $I^{(\alpha_{d+1})}$. The resulting matrix takes the form

$$\left(\begin{array}{c|c|c} I_{d+1} & 0 & X_{d+1}^{(2)} - X_{d+1}^{(1)}Y_{d+1} \\ \hline 0 & I^{(\alpha_{d+1})} & Y_{d+1} \end{array} \right).$$

Similarly to above, the arithmetic complexity of this step is bounded by that of computing $X_{d+1}^{(1)}Y_{d+1}$. The matrix $X_{d+1}^{(1)}$ has β_{d+1} rows and α_{d+1} columns, while the matrix Y_{d+1} has α_{d+1} rows and $\binom{4+d}{3} - h_{d+1}$ columns. Therefore, by the general bound given in [Kni95, Section 2.1], the number of arithmetic $\mathbb{k}$ operations required to compute the matrix $X_{d+1}^{(1)}Y_{d+1}$ is in

$$\begin{cases} O\left(\left(\binom{4+d}{3} - h_{d+1}\right)^{\omega-2} \alpha_{d+1} \beta_{d+1}\right) & \text{if } \alpha_{d+1} > \binom{4+d}{3} - h_{d+1} \\ O\left(\left(\binom{4+d}{3} - h_{d+1}\right) \alpha_{d+1}^{\omega-2} \beta_{d+1}\right) & \text{otherwise} \end{cases}$$

In the first case,

$$O\left(\left(\binom{4+d}{3} - h_{d+1}\right)^{\omega-2} \alpha_{d+1} \beta_{d+1}\right) \subseteq O(\alpha_{d+1}^{\omega-1} \beta_{d+1}) \subseteq O(\alpha_{d+1}^{\omega-2} \beta_{d+1} \gamma_{d+1})$$

and in the second case, since $\binom{4+d}{3} - h_{d+1} \geq \gamma_{d+1}$,

$$O\left(\left(\binom{4+d}{3} - h_{d+1}\right) \alpha_{d+1}^{\omega-2} \beta_{d+1}\right) \subseteq O(\alpha_{d+1}^{\omega-2} \beta_{d+1} \gamma_{d+1})$$

so the complexity of the second step dominates. $\square$

Our main complexity upper bound, given in the following theorem, is now an easy consequence of Proposition 3.4.9.

THEOREM 3.4.10. — Fix $a \in U_{\text{RL}} \subseteq \mathbb{A}^{4p^2}$. Let $M = \phi_a(\mathcal{A}_p^1)$. The number of arithmetic operations in $\mathbb{k}$ performed by Algorithm 3 when computing the reduced grevlex Gröbner basis for $\mathcal{I}_{p-1}(M)$ is in $O(p^{2\omega+3})$.

Proof. Note first that all arithmetic operations occur when computing the $\widetilde{\mathcal{M}}_d$ from the $\mathcal{M}_d$. Secondly, note that the complexity of the final step of Algorithm 3 bounds the complexity of the algorithm as a whole, since the number of rows to be reduced in the Macaulay matrix in degree d for the first (resp. second) syzygy module is precisely the number of (a priori) reductions to zero encountered in $\mathcal{M}_{d+1}$ (resp. the Macaulay matrix in degree $d+1$ of the first syzygy module). Note also that $\mathcal{M}_{p-1}$ has p^2 rows, and $\binom{p+2}{3}$ columns, and is of rank p^2 . Thus, by [Sto00, Section 2.2] (see also [JPS13, Appendix A]) the arithmetic complexity of computing $\widetilde{\mathcal{M}}_{p-1}$ from $\mathcal{M}_{p-1}$ is in

$$O\left(p^{2\omega-2}\binom{p+2}{3}\right) \subseteq O(p^{2\omega+1}).$$

It follows, by Proposition 3.4.9, that the total complexity of computing the reduced grevlex Gröbner basis for $\mathcal{I}_{p-1}(M)$ is in $O(p^{2\omega+1} + f_\omega(p))$, where

$$f_\omega(p) = \sum_{d=p-1}^{2p-4} \beta_{d+1}^2 \alpha_{d+1}^{\omega-2} + \alpha_{d+1}^{\omega-2} \beta_{d+1} \gamma_{d+1}.$$

By Lemma 3.4.5, for all $p-1 \leq d \leq 2p-4$, $\alpha_{d+1} \leq \alpha_p < p^2$, hence

$$f_\omega(p) \in O\left(p^{2\omega-4} \sum_{d=p-1}^{2p-4} \beta_{d+1} \gamma_{d+1} + \beta_{d+1}^2\right). \quad (3.4)$$

One can verify (e.g. using the Maple computer algebra system [MGH⁺05]) that

$$\sum_{d=p-1}^{2p-4} \beta_{d+1} \gamma_{d+1} + \beta_{d+1}^2 = \frac{619}{1260}p^7 - \frac{341}{360}p^6 - \frac{7}{360}p^5 + \frac{7}{36}p^4 - \frac{169}{360}p^3 - \frac{89}{360}p^2 - \frac{1}{420}p.$$

It follows that $f_\omega(p) \in O(p^{2\omega+3})$, which concludes the proof. $\square$

REMARK 3.4.11. — The upper bound on Algorithm 3 obtained in Theorem 3.4.10 is subquadratic in the size of the dense representation of the output Gröbner basis obtained in Theorem 3.4.3.

REMARK 3.4.12. — When $\omega = 2$, the bound $O(p^{2\omega+3})$ becomes $O(p^7)$, which still differs from the lower bound on the output size obtained in Theorem 3.4.3 by a factor of p . This suggests that there might still be room for improvement upon the bound obtained in Theorem 3.4.10. In experiments, when working on input of matrices of homogeneous linear forms in four variables with coefficients chosen uniformly at random from some large prime field, one can observe that the submatrices A_d defined in Proposition 3.4.4 are sparse. Perhaps by taking into account this sparsity, a tighter upper bound could be achieved.

3.4.4 THE ASYMPTOTIC BEHAVIOUR OF $f_\omega(p)$

In the proof of Theorem 3.4.10, only one upper bound is actually used — the bound $\alpha_{d+1} < p^2$. We conclude our complexity analysis by presenting precise asymptotics for $f_\omega(p)$ for various ω . Using the SageMath computer algebra system (see [The22]), we obtain the asymptotic data in Table 3.1. It suggests that the asymptotic result $f_\omega(p) = O(p^{2\omega+3})$ obtained in Theorem 3.4.10 is sharp.

Table 3.1: The asymptotics of $f_\omega(p)$ compared to $p^{2\omega+3}$ for various $2 \leq \omega \leq 3$.

ω	$f_\omega(p) \sim_{p \rightarrow \infty}$	$p^{2\omega+3}$
3	$\frac{401}{18144}p^9$	p^9
2.7	$\frac{2^{\frac{7}{10}} \cdot 76533282553747476335323}{2761171875000000000000000}p^{8.4}$	$p^{8.4}$
2.5	$\frac{29\sqrt{2}}{10080}p^8$	p^8
2.38	$\frac{2^{\frac{19}{50}} \cdot 3808710545424609640564981876343720387}{41658431291580200195312500000000000000}p^{7.76}$	$p^{7.76}$
2	$\frac{619}{1260}p^7$	p^7

MAXIMAL MINORS AND CRITICAL POINTS

Our next focus is on the case of maximal minors of a rectangular matrix of polynomials. First defined in [EN62], the Eagon-Northcott complex is a complex of free modules associated to a matrix with entries in any commutative ring with unity. We are specifically concerned with the first syzygies of maximal minors of a polynomial matrix. The Eagon-Northcott complex provides access to them, and in a similar fashion to Algorithm 2, we use these syzygies to adapt the Matrix- F_5 algorithm to determinantal polynomial systems of maximal minors. As a particular application of this adapted algorithm, we compute critical points of a polynomial map restricted to an algebraic set. The content and results of this chapter come from the paper [GNSD24], which was published in the proceedings of ISSAC 2025.

4.1 THE FIRST SYZYGIES OF MAXIMAL MINORS

4.1.1 THE EAGON-NORTHCOTT COMPLEX

THEOREM 4.1.1 ([EN62, Theorem 1], [Eis05, Theorem A2.60]). — Let $\mathcal{R}$ be a commutative ring with unity and let A be a $p \times q$ matrix with entries in $\mathcal{R}$, with $p \leq q$. For each $0 \leq i \leq q - p$, let

$$\mathcal{E}_i = \text{Sym}_i \mathcal{R}^{p^\vee} \otimes \bigwedge^{p+i} (\mathcal{R}^q).$$

Then there are graded morphisms $\partial_i : \mathcal{E}_i \rightarrow \mathcal{E}_{i-1}$, $1 \leq i \leq q - p$, such that the complex $\text{EN}(A) = (\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathcal{R}/\mathcal{I}_p(A), \partial_\bullet)$ is a free resolution if and only if $\text{grade}(\mathcal{I}_p(A)) = q - p + 1$.

We make explicit the first boundary morphism ∂_1 , whose image is precisely the first syzygy module of $\mathcal{I}_p(A)$. First, by the definition of the free modules $\mathcal{E}_i$, the map ∂_1 is a map

$$\partial_1 : \mathcal{R}^{p^\vee} \otimes \bigwedge^{p+1} (\mathcal{R}^q) \rightarrow \bigwedge^p (\mathcal{R}^q).$$

We take as a basis for $\mathcal{R}^{p^\vee}$ the standard basis functionals e_i for $1 \leq i \leq q$. It follows immediately from Propositions 1.1.1 and 1.1.2 that a basis for the $\mathcal{R}$ -module $\mathcal{R}^{p^\vee} \otimes \bigwedge^{p+1} (\mathcal{R}^q)$ is given by

$$\{e_i \otimes (e_{i_1} \wedge \cdots \wedge e_{i_p}) : 1 \leq i \leq p, 1 \leq i_1 < \cdots < i_p \leq q\}.$$

Subsequently, $\partial_1(e_i \otimes (e_{i_1} \wedge \cdots \wedge e_{i_p}))$ equals

$$\sum_{t=1}^{p+1} (-1)^{t-1} (e_{i_t} A^T e_i) (e_{i_1} \wedge \cdots \wedge \widehat{e_{i_t}} \wedge \cdots \wedge e_{i_{p+1}}).$$

The map $\epsilon : \bigwedge^p (\mathcal{R}^q) \rightarrow \mathcal{R}/\mathcal{I}_p(A)$ is given by

$$\epsilon(e_{i_1} \wedge \cdots \wedge e_{i_p}) = \det([1 \cdots p \mid i_1 \cdots i_p]_A).$$

The image of ∂_1 (and thus $\text{Syz}(F_p(A))$) then admits an explicit description. For each $p \times (p+1)$ submatrix A' of A , the determinant of the square matrix formed by duplicating any row of A' , computed via Laplace expansion around the duplicated row, is zero.

MAXIMAL MINORS AND CRITICAL POINTS

EXAMPLE 4.1.2. — Let $p = 2$, $q = 4$, and suppose

$$A = \begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \end{pmatrix} \in \mathcal{R}^{2 \times 4}.$$

We have

$$\partial_1(e_1 \otimes (e_2 \wedge e_3 \wedge e_4)) = f_{12}(e_3 \wedge e_4) - f_{13}(e_2 \wedge e_4) + f_{14}(e_2 \wedge e_3).$$

Note that the fact that $\partial_1(e_1 \otimes (e_2 \wedge e_3 \wedge e_4)) \in \ker \epsilon$ is precisely the statement that the determinant

$$\det \begin{pmatrix} f_{12} & f_{13} & f_{14} \\ f_{22} & f_{23} & f_{24} \end{pmatrix}$$

is zero. More explicitly, $\epsilon(\partial_1(e_1 \otimes (e_2 \wedge e_3 \wedge e_4)))$ is simply the determinant of this matrix, computed via Laplace expansion along its first row. Analogously, $\epsilon(\partial_1(e_2 \otimes (e_1 \wedge e_3 \wedge e_4)))$ is simply the determinant of the singular matrix

$$\begin{pmatrix} f_{21} & f_{23} & f_{24} \\ f_{11} & f_{13} & f_{14} \\ f_{21} & f_{23} & f_{24} \end{pmatrix}$$

computed via Laplace expansion along its first row.

4.1.2 LEADING TERMS OF SYZYGIES

We start with a consequence of the description of the first syzygy module provided by the Eagon-Northcott complex.

PROPOSITION 4.1.3. — Let $A = (a_{i,j})$ be an $p \times q$ matrix with entries in $\mathbb{k}[x_1, \dots, x_n]$, with $p \leq q$. For each $1 \leq k \leq q - p$, let $\mathcal{J}_k(A)$ be the ideal $\langle a_{i,j} : 1 \leq i \leq p, j \leq k \rangle$ of $\mathbb{k}[x_1, \dots, x_n]$. Let $\mathcal{H}$ be the set

$$\bigcup_{k=1}^{q-p} \bigcup_{k+1 < i_2 < \dots < i_p \leq q} \{ \text{LM}_{\prec}(g)(e_{k+1} \wedge e_{i_2} \wedge \dots \wedge e_{i_p}) : g \in \mathcal{J}_k(A) \}.$$

Then the module $\langle\langle \mathcal{H} \rangle\rangle$ is a submodule of $\text{LM}_{\succ_{\text{pot}}}(\text{Syz}(F_p(A)))$.

Proof. Fix $1 \leq k \leq q - p$. Let $i_2, \dots, i_p \in \mathbb{Z}_{>0}$ be integers such that $k + 1 < i_2 < \dots < i_p < q$, and let $g \in \mathcal{J}_k(A)$. Then there exist polynomials $h_{i,j} \in \mathcal{R}_n$ such that $g = \sum_{i,j} h_{i,j} a_{i,j}$. Let

$$G = \sum_{i,j} h_{i,j} \partial_1(e_i \otimes (e_j \wedge e_{k+1} \wedge e_{i_2} \wedge \dots \wedge e_{i_p})).$$

We claim that

$$\text{LM}_{\succ_{\text{pot}}}(G) = \text{LM}_{\prec}(g)(e_{k+1} \wedge e_{i_2} \wedge \dots \wedge e_{i_p}).$$

Now taking $\phi = (e_{k+1} \wedge \dots \wedge e_{i_p})^\vee$, we have

$$\phi(G) = \sum_{i,j} \phi(h_{i,j} \partial_1(e_i \otimes (e_j \wedge e_{k+1} \wedge e_{i_2} \wedge \dots \wedge e_{i_p})))$$

$$\begin{aligned}
 &= \sum_{i,j} h_{i,j} \phi(\partial_1(e_i \otimes (e_j \wedge e_{k+1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_p}))) \\
 &= \sum_{i,j} h_{i,j} a_{i,j} = g
 \end{aligned}$$

By the definition of ∂_1 , only those basis vectors of $\bigwedge^p(\mathcal{R}_n^q)$ of the form $e_j \wedge \cdots \wedge \widehat{e_{i_t}} \wedge \cdots \wedge e_{i_p}$ appear with nonzero coefficient in G . The largest of these basis vectors with respect to the lexicographic order is clearly $e_{k+1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_p}$, so our claim is proven. Having constructed an element of $\text{LM}_{\succ_{\text{pot}}}(\text{Syz}(F_p(A)))$ whose leading term is precisely $\text{LM}_{\prec}(g)(e_{k+1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_p})$, we are done. $\square$

REMARK 4.1.4. — We have seen, in Section 4.1.1, that the syzygies described by the Eagon-Northcott complex between the maximal minors of a $p \times q$ matrix A over $\mathcal{R}_n$ are given by choosing a $p \times (p+1)$ submatrix A' of A , duplicating any row of A' , and computing the determinant of this matrix by Laplace expansion over the duplicated row (see Example 4.1.2 for an example). The $\prec_{\text{pot}}$ -leading term of such a syzygy is simply the leading term of the leftmost entry of the duplicated row.

Upon fixing a maximal minor of A , the leading monomials of a ord-Gröbner basis of the polynomial system formed by the entries of the columns to the left of the leftmost column of this minor are leading monomials of syzygies amongst the maximal minors of A .

Proposition 4.1.3 leads directly to the following algorithm.

Algorithm 4 $\text{MaxDetMatrixF}_5(A, D)$

Input: A matrix $A = (a_{i,j}) \in \mathbb{k}[x_1, \dots, x_n]^{p \times q}$ of homogeneous polynomials, with $p \leq q$ and an integer D .

Output: A (D, ord) -Gröbner basis of $\mathcal{I}_p(A)$.

- 1: $C \leftarrow \{a_{1,1}, \dots, a_{p,1}, \dots, a_{1,q-p}, \dots, a_{p,q-p}\}$
 - 2: $G_1, \dots, G_{p(q-p)} \leftarrow \text{MatrixF}_5(C, \emptyset, D - \min_{f \in F_{r+1}(M)pA} \{\deg(f)\})$
 - 3: $H \leftarrow \emptyset$
 - 4: **for** $i \in \{1, \dots, p(q-p)\}$ **do**
 - 5: **for** $f \in F_{r+1}(M)p \left[1 \cdots p \mid \left(\left\lfloor \frac{i}{p} \right\rfloor + 1 \right) \cdots q \right]_A$ **do**
 - 6: $j \leftarrow \text{index of } f \text{ in } F_{r+1}(M)pA$
 - 7: $H \leftarrow H \cup \{\text{LM}_{\prec}(g)e_j : g \in G_i\}$
 - 8: **return** $\text{MatrixF}_5(F_{r+1}(M)pA, H, D)$
-

THEOREM 4.1.5. — Algorithm MaxDetMatrixF_5 is correct.

Proof. This follows from the correctness of MatrixF_5 [BFS15, Theorem 9], and from Proposition 4.1.3 which establishes that the set H input to MatrixF_5 on Algorithm 4 is a subset of $\text{LM}_{\succ_{\text{pot}}}(\text{Syz}(F_p(A)))$. Recall that here we use the slightly modified MatrixF_5 from [GNS23, Algorithm 1], whose description requires the input of a set of syzygies whose leading terms it immediately extracts. Instead, here we directly give it as input the set H , which is a set of leading terms of syzygies. $\square$

4.2 CRITICAL POINTS

Recall that for a set of homogeneous polynomials $F = (f_1, \dots, f_p) \subseteq \mathcal{R}_n$, and a homogeneous polynomial $g \in \mathcal{R}_n$, our goal is to compute a Gröbner basis for $\mathcal{I}(g, F) = \mathcal{I}_p(\text{jac}(g, F)) + \langle F \rangle$. Note that if g and the f_i 's are affine, by [CLO15, Chapter 8, Section 4, Theorem 4], one can simply homogenise them with respect to a variable h which is smaller than all of the x_i , apply the algorithms in this paper, then set $h = 1$.

Via a minor modification of Algorithm 4, we obtain an algorithm which computes a Gröbner basis for the ideal $\mathcal{I}(g, F)$.

Algorithm 5 CritGB(F, g, D)

Input: A system of homogeneous polynomials $F = (f_1, \dots, f_p) \subseteq \mathcal{R}_n$, a homogeneous polynomial $g \in \mathcal{R}_n$, and an integer D .

Output: A $(D, \succ)$ -Gröbner basis of $\mathcal{I}(g, F)$.

```

1:  $J \leftarrow \text{jac}(g, F)$ 
2:  $C \leftarrow \{J_{1,1}, \dots, J_{p+1,1}, \dots, J_{1,n-p-1}, \dots, J_{p,n-p-1}\}$ 
3:  $G_1, \dots, G_{(p+1)(n-p-1)} \leftarrow \text{MatrixF}_5\left(C, \emptyset, D - \min\left\{\deg\left(\frac{\partial f_i}{\partial x_j}\right)\right\}\right)$ 
4:  $H \leftarrow \emptyset$ 
5: for  $i \in \{1, \dots, (p+1)(n-p-1)\}$  do
6:   for  $f \in F_{r+1}(M)p+1\left[1 \cdots p+1 \mid \left(\left\lfloor \frac{i}{p+1} \right\rfloor + 1\right) \cdots n\right]_J$  do
7:      $j \leftarrow \text{index of } f \text{ in } F_{r+1}(M)p+1J$ 
8:      $H \leftarrow H \cup \{\text{LM}_{\prec}(g)e_j : g \in G_i\}$ 
9: return  $\text{MatrixF}_5(F \cup F_{r+1}(M)p+1J, H, D)$ 
    
```

PROPOSITION 4.2.1. — Algorithm CritGB is correct.

Proof. The only modification made to Algorithm 4 to obtain Algorithm 5 is to add the set F to the polynomial system upon which we run MatrixF_5 . Thus, the correctness follows immediately from that of Algorithm 4, proven in Theorem 4.1.5. $\square$

For a system of homogeneous polynomials $F = (f_1, \dots, f_p) \subseteq \mathcal{R}_n$ and a polynomial $g \in \mathcal{R}_n$, there may exist, a priori, nontrivial syzygies between the polynomials in F and the maximal minors of $\text{jac}(g, F)$. Generically, this does not occur.

PROPOSITION 4.2.2. — Let $n, p, d_0 \in \mathbb{Z}_{>0}$. There exists a nonempty Zariski open subset $U \subseteq \mathbb{A}^{(p+1)\binom{n+d_0-1}{n-1}}$ such that for all $c \in U$, taking $(g, f_1, \dots, f_p) = \phi_c(\mathbf{f}_{(n, (d_0, \dots, d_0))})$,

$$\text{Syz}(F \cup F_{p+1}(\text{jac}(g, F))) = \text{Syz}(F) \oplus \text{Syz}(F_{p+1}(\text{jac}(g, F)))$$

where $F = (f_1, \dots, f_p)$.

Proof. By [Spa14, Lemma 2.2], there exists a nonempty Zariski open subset $U \subseteq \mathbb{A}^{(p+1)\binom{n+d_0-1}{n-1}}$ such that for all $c \in U$, taking

$$(g, f_1, \dots, f_p) = \phi_c(\mathbf{f}_{(n, (d_0, \dots, d_0))}).$$

and $F = (f_1, \dots, f_p)$, the sequence $(f_1, \dots, f_p)$ is a $\mathcal{R}_n/\mathcal{I}_{p+1}(\text{jac}(g, F))$ -regular sequence. For such c , F is also a regular sequence in $\mathcal{R}_n$, so the Koszul complex associated to F , $\mathcal{K}(F)$,

is exact. By [ML95, Theorem 9.3], there is then an isomorphism

$$H_i(\mathbf{EN}(\mathrm{jac}(g, F)) \otimes_{\mathcal{R}_n} \mathcal{K}(F)) \cong \mathrm{Tor}_i^{\mathcal{R}_n}(\mathcal{R}_n/\langle F \rangle, \mathcal{R}_n/\mathcal{I}_{p+1}(\mathrm{jac}(g, F)))$$

between the homology of $\mathbf{EN}(\mathrm{jac}(g, F)) \otimes_{\mathcal{R}_n} \mathcal{K}(F)$ and the torsion products of $\mathcal{R}_n/\langle F \rangle$ and $\mathcal{R}_n/\mathcal{I}_{p+1}(\mathrm{jac}(g, F))$ as $\mathcal{R}_n$ -modules.

Now since F is an $\mathcal{R}_n/\mathcal{I}_{p+1}(\mathrm{jac}(g, F))$ -regular sequence, the complex

$$\mathcal{K}(F; \mathcal{R}_n/\mathcal{I}_{p+1}(\mathrm{jac}(g, F))) = \mathcal{K}(F) \otimes_{\mathcal{R}_n} \mathcal{R}_n/\mathcal{I}_{p+1}(\mathrm{jac}(g, F)).$$

is acyclic, and thus for all $i > 0$,

$$\mathrm{Tor}_i^{\mathcal{R}_n}(\mathcal{R}_n/\mathcal{I}_{p+1}(\mathrm{jac}(g, F)), \mathcal{R}_n/\langle F \rangle) = 0.$$

It follows that $\mathbf{EN}(\mathrm{jac}(g, F)) \otimes_{\mathcal{R}_n} \mathcal{K}(F)$ is a free resolution of the tensor product

$$\mathcal{R}_n/\langle F \rangle \otimes_{\mathcal{R}_n} \mathcal{R}_n/\mathcal{I}_{p+1}(\mathrm{jac}(g, F)) \cong \mathcal{R}_n/(\langle F \rangle + \mathcal{I}_{p+1}(\mathrm{jac}(g, F))). \quad \square$$

4.3 COMPLEXITY ANALYSIS

The complexity of linear-algebra based Gröbner basis algorithms is governed by the cost of echelonizing Macaulay matrices. The work that we have done thus far allows us to estimate these costs, since the sizes and ranks of the Macaulay matrices computed can be deduced from the Eagon-Northcott complex.

4.3.1 NEW COMPLEXITY BOUND

Recall that given a polynomial system $F \subseteq \mathcal{R}_n$, the columns of $\mathcal{M}_d(F)$, are indexed by the monomials of degree d in $\mathcal{R}_n$. We are left to compute the rank of $\mathcal{M}_d(F)$ and the number of rows of $\mathcal{M}_d(F)$ taken into account by our algorithm. We first count the number of syzygies from Proposition 4.1.3.

PROPOSITION 4.3.1. — Let $A = (a_{i,j})$ be a $p \times q$ matrix with entries homogeneous polynomials of degree d_0 in $\mathcal{R}_n$, with $q \geq p$. For each $1 \leq k \leq q - p$, let $\mathcal{J}_k(A) := \langle a_{i,j} : 1 \leq i \leq p, 1 \leq j \leq k \rangle \subseteq \mathcal{R}_n$. Then for any $D \in \mathbb{Z}_{>0}$ and any $d \in \{d_0 p, \dots, D\}$, the number of elements of degree $d - pd_0$ of the set H computed in Algorithm 4 is

$$\sum_{k=1}^{q-p} \mathrm{HF}_{\mathcal{J}_k(A)}(d - pd_0) \binom{q - k - 1}{p - 1}$$

Proof. Let $H_{d-pd_0} \subseteq H$ be the subset of the set H in Algorithm 4 consisting of elements of degree $d - pd_0$. This set H is precisely the set $\mathcal{H}$ defined in the statement of Proposition 4.1.3. We can therefore write

$$\begin{aligned} \#H_{d-pd_0} &= \sum_{k=1}^{q-p} \sum_{k+1 < i_2 < \dots < i_p \leq q} \# \{ \mathrm{LM}_{\prec}(g)(e_{k+1} \wedge e_{i_2} \wedge \dots \wedge e_{i_p}) : \\ &\quad g \in \mathcal{J}_k(A), \deg(g) = d - pd_0 \} \end{aligned}$$

MAXIMAL MINORS AND CRITICAL POINTS

$$= \sum_{k=1}^{q-p} \sum_{k+1 < i_2 < \dots < i_p \leq q} \text{HF}_{\mathcal{J}_k(A)}(d - pd_0).$$

The last equality follows from the fact that the number of monomials of $\text{LM}_{\prec}(\mathcal{J}_k(A))$ of degree $d - pd_0$ is $\text{HF}_{\mathcal{J}_k(A)}(d - pd_0)$. The result follows from the fact that for $1 \leq k \leq q - p$, there are $\binom{q-k-1}{p-1}$ sequences of the form $k + 1 < i_2 < \dots < i_p \leq q$. $\square$

Using Proposition 4.3.1, we are left to compute the Hilbert functions of the ideals $\mathcal{J}_k(A)$ of flattened columns, of course under certain genericity assumptions. To do this, we rely on Fröberg's conjecture [Frö85, Sec. 1], which we reformulate below.

In what follows, for polynomials $P(t), Q(t) \in \mathbb{Z}[t]$, we denote by $\left[\frac{P(t)}{Q(t)} \right]_+$ the power series expansion of $\frac{P(t)}{Q(t)}$, truncated at its first non-positive coefficient.

CONJECTURE 4.3.2 ([Frö85, Sec. 1], [Nic17, Conj. 1]). — For any $n \in \mathbb{Z}_{>0}$ and any sequence of integers $(d_1, \dots, d_m) \in \mathbb{Z}_{\geq 0}^m$, there exists a Zariski open subset $U \subseteq \prod_{i=1}^m \mathbb{A}^{\binom{n+d_i-1}{n-1}}$ such that for any $c \in U$,

$$H_{\mathcal{R}_n / \langle \phi_c(\mathbf{f}_{(n, d_1, \dots, d_m)}) \rangle}(t) = \left[\frac{\prod_{i=1}^m (1 - t^{d_i})}{(1 - t)^n} \right]_+.$$

PROPOSITION 4.3.3. — Let $m, n \in \mathbb{Z}_{>0}$ and let $F = (f_1, \dots, f_m) \subseteq \mathbb{k}[x_1, \dots, x_n]$ be a sequence of homogeneous polynomials, all of degree d_0 . Let D be the Hilbert regularity of $\langle F \rangle$. If F is a semi-regular sequence, and Conjecture 4.3.2 is true, then for any $0 \leq d < D$,

$$\text{HF}_{\mathcal{R}_n / \langle f_1, \dots, f_m \rangle}(d) = \sum_{j=0}^{\left\lfloor \frac{n+d-1}{d_0} \right\rfloor} (-1)^j \binom{n+d-d_0j-1}{n-1} \binom{m}{j}.$$

Proof. By Conjecture 4.3.2, the Hilbert series of $\mathcal{R}_n / \langle F \rangle$ is

$$H_{\mathcal{R}_n / \langle f_1, \dots, f_m \rangle}(t) = \left[\frac{(1 - t^{d_0})^m}{(1 - t)^n} \right]_+.$$

The numerator $(1 - t^{d_0})^m$ can be expanded as $\sum_{j=0}^m (-1)^j \binom{m}{j} t^{jd_0}$ while the reciprocal of the denominator has the classical expansion

$$\frac{1}{(1 - t)^n} = \sum_{j \geq 0} \binom{n+j-1}{n-1} t^j.$$

The result follows by taking the product of these expansions. $\square$

PROPOSITION 4.3.4. — Let $n \in \mathbb{Z}_{>0}$. For any $p \leq n$ and any $d_0 \in \mathbb{Z}_{>0}$, there exists a Zariski open set $U \subseteq \mathbb{A}^{(p+1)\binom{n+d_0-1}{n-1}}$ such that for all $c \in U$, taking $(g, f_1, \dots, f_p) = \phi_c(\mathbf{f}_{(n, d_0, \dots, d_0)})$, the sequence

$$\left(\frac{\partial g}{\partial x_1}, \frac{\partial f_1}{\partial x_1}, \dots, \frac{\partial f_p}{\partial x_1}, \dots, \frac{\partial g}{\partial x_{n-p-1}}, \frac{\partial f_1}{\partial x_{n-p-1}}, \dots, \frac{\partial f_p}{\partial x_{n-p-1}} \right)$$

formed by the leftmost $n - p - 1$ columns of $\text{jac}(g, f_1, \dots, f_p)$ is semi-regular.

Proof. Let $\mathbf{c}^{(1)}, \dots, \mathbf{c}^{(p+1)}$ be sets of indeterminates, with $\mathbf{c}^{(i)} = \{\mathbf{c}_\tau^{(i)} : \tau \in \text{Mon}_{d_0}(\mathcal{R}_n)\}$. For any $1 \leq i \leq p+1$ and for $1 \leq j \leq n-p-1$, the coefficients of the partial derivative $\frac{\partial \mathbf{f}_{(n,d_0)}^{(i)}}{\partial x_j}$ are polynomials in the indeterminate coefficients $\mathbf{c}^{(i)}$.

For any $d \geq d_0$, (upon fixing bases for the domain and codomain), the multiplication map by $\frac{\partial \mathbf{f}_{(n,d_0)}^{(i)}}{\partial x_j}$

$$\left(\frac{\mathcal{R}_n}{\langle \frac{\partial \mathbf{f}_{(n,d_0)}^{(1)}}{\partial x_1}, \dots, \frac{\partial \mathbf{f}_{(n,d_0)}^{(i-1)}}{\partial x_{j-1}} \rangle} \right)_{d-d_0} \rightarrow \left(\frac{\mathcal{R}_n}{\langle \frac{\partial \mathbf{f}_{(n,d_0)}^{(1)}}{\partial x_1}, \dots, \frac{\partial \mathbf{f}_{(n,d_0)}^{(i-1)}}{\partial x_{j-1}} \rangle} \right)_d$$

is represented by a matrix whose entries are rational functions in the indeterminate coefficients $\mathbf{c}^{(i)}$.

The points $c \in \mathbb{A}^{(p+1)\binom{n+d_0-1}{n-1}}$ such that this map is full-rank form a (possibly empty) Zariski open subset. By intersecting all such subsets for all $1 \leq i \leq p+1$ and $1 \leq j \leq n-p-1$, we obtain the set U we seek. $\square$

COROLLARY 4.3.5. — Let $n \in \mathbb{Z}_{>0}$ and assume Conjecture 4.3.2 is true. For any $p \leq n$ and any $d_0 \in \mathbb{Z}_{>0}$, there exists a Zariski open set $U \subseteq \mathbb{A}^{(p+1)\binom{n+d_0-1}{n-1}}$ such that for all $c \in U$, taking $(g, f_1, \dots, f_p) = \phi_c(\mathbf{f}_{(n,d_0,\dots,d_0)})$, for any $1 \leq k \leq n-p-1$, $\text{HF}_{\mathcal{J}_k(\text{jac}(g,F))}(d)$ is

$$\begin{cases} \binom{n+d-1}{n-1} - \sum_{j=0}^{\lfloor \frac{n+d-1}{d_0} \rfloor} (-1)^j \binom{n+d-d_0j-1}{n-1} \binom{(p+1)k}{j} & \text{if } d < D \\ \binom{n+d-1}{n-1} & \text{if } d \geq D \end{cases}$$

where $\mathcal{J}_k(\text{jac}(g,F))$ is the ideal generated by the first k columns of $\text{jac}(g,F)$, and D is its Hilbert regularity.

Proof. Let U be the set defined in Proposition 4.3.4 and take any $c \in U$. Then for any $1 \leq k \leq n-p-1$, the set of generators for $\mathcal{J}_k(\text{jac}(g,F))$ given by the first k columns of $\text{jac}(g,F)$ forms a semi-regular sequence. We can therefore apply Proposition 4.3.3 to obtain the Hilbert function of $\mathcal{R}_n/\mathcal{J}_k(\text{jac}(g,F))$. Since the Hilbert function of $\mathcal{R}_n$ itself is $\text{HF}_{\mathcal{R}_n}(d) = \binom{n+d-1}{n-1}$, the result follows. $\square$

CONJECTURE 4.3.6. — The set U defined in Proposition 4.3.4 is nonempty.

REMARK 4.3.7. — One possible way to prove Conjecture 4.3.6 would be to exhibit the existence of a family of explicit examples of polynomial systems parameterised by (p, n, d_0) such that, for these polynomial systems, the statement of Proposition 4.3.3 holds. This is a classical method of proof for statements similar to that of Conjecture 4.3.6, and has been used successfully even in the determinantal context (see e.g. [HSEDSV21, Sec. 8]). However, in our setting, it is not even known that semi-regularity holds for overdetermined sequences of polynomials. Indeed, this is one possible formulation of Fröberg's conjecture.

Finally, we compute the ranks of the Macaulay matrices associated to the maximal minors of a polynomial matrix from the Eagon-Northcott complex.

PROPOSITION 4.3.8. — Let A be a $p \times q$ matrix with entries homogeneous polynomials of degree d_0 in $\mathbb{k}[x_1, \dots, x_n]$, with $q \geq p$. If $\text{grade}(\mathcal{I}_p(A)) = q - p + 1$, then

$$\text{HF}_{\mathcal{I}_p(A)}(d) = \sum_{j=0}^{q-p} (-1)^j \binom{n+d-(p+j)d_0-1}{n-1} \binom{p+j-1}{p-1} \binom{q}{p+j}.$$

MAXIMAL MINORS AND CRITICAL POINTS

Proof. Since $\text{grade}(\mathcal{I}_p(A)) = q - p + 1$, by Theorem 4.1.1, the Eagon-Northcott complex is a free resolution of $\mathcal{I}_p(A)$. In order to turn the Eagon-Northcott complex into a graded resolution, we need to shift the grading on the component free modules to ensure that the boundary homomorphisms are graded.

First, the degree of the maximal minors of A is pd_0 . As such, in order to make the augmentation homomorphism ϵ of $\mathbf{EN}(A)$ graded, we need only replace $\mathcal{E}_0$ by $\mathcal{E}_0(-pd_0)$.

Now, by the description of the boundary homomorphisms in [Eis05, A2H] (see also [Eis05, Exa. A2.69]), each boundary homomorphism (except for the augmentation homomorphism) can be represented by a matrix with entries linear in the entries of A . Thus, in order to make these boundary homomorphisms graded, we need to replace $\mathcal{E}_j$ by $\mathcal{E}_j(-pd_0 - id_0)$ for each $1 \leq j \leq q - p$.

Finally, we have $\text{rank}(\mathcal{E}_0(-pd_0)) = \binom{q}{p}$ and

$$\begin{aligned} \text{rank}(\mathcal{E}_j(-d_0(p+j))) &= \text{rank}\left(\text{Sym}_j(\mathcal{R}^p)^\vee \otimes \bigwedge^{p+j}(\mathcal{R}^q)\right) \\ &= \binom{p+j-1}{p-1} \binom{q}{p+j}. \end{aligned}$$

The result then follows from Corollary 1.1.8. $\square$

PROPOSITION 4.3.9. — Let $F = (f_1, \dots, f_p) \subseteq \mathbb{k}[x_1, \dots, x_n]$ be a regular sequence of homogeneous polynomials, all of degree d_0 , and let $g \in \mathbb{k}[x_1, \dots, x_n]$ be a homogeneous polynomial of degree d_0 . Then the Hilbert function of the ideal $\mathcal{I}(g, F) = \langle F \rangle + \mathcal{I}_{p+1}(\text{jac}(g, F))$ is given by $\text{HF}_{\mathcal{R}_n/\mathcal{I}(g, F)}(d)$ which is

$$\begin{aligned} &\sum_{i=0}^p (-1)^i \binom{p}{i} \left(\binom{n+d-id_0-1}{n-1} - \right. \\ &\quad \left. \sum_{j=0}^{n-p-1} (-1)^j \binom{n+d-(p+j+i+1)d_0-1}{n-1} \binom{p+j}{p} \binom{n}{p+j+1} \right) \end{aligned}$$

Proof. By [Spa14, Lem. 2.2], the sequence F is a $\mathcal{R}_n/\mathcal{I}_{p+1}(\text{jac}(g, F))$ -regular sequence. It follows (see e.g. [Eis95, Exe. 10.13(a)]) that

$$H_{\mathcal{R}_n/\mathcal{I}(g, F)}(t) = H_{\mathcal{R}_n/\mathcal{I}_{p+1}(\text{jac}(g, F))}(t)(1 - t^{d_0})^p. \quad (4.1)$$

By Proposition 4.3.8, $\text{HF}_{\mathcal{I}_{p+1}(\text{jac}(g, F))}(d)$ equals

$$\sum_{j=0}^{n-p-1} (-1)^j \binom{n+d-(p+j+1)d_0-1}{n-1} \binom{p+j}{p} \binom{n}{p+j+1}. \quad (4.2)$$

Since the Hilbert series $H_{\mathcal{R}_n/\mathcal{I}_{p+1}(\text{jac}(g, F))}(t)$ is the generating series of the difference between the Hilbert function of $\mathcal{R}_n$ (which is simply $\text{HF}_{\mathcal{R}_n}(d) = \binom{n+d-1}{n-1}$) and this Hilbert function, the result follows by combining Eq. (4.2) with Eq. (4.1) and expanding. $\square$

We use the Hilbert functions to estimate the cost of echelonizing each of the Macaulay matrices encountered in Algorithm 5.

THEOREM 4.3.10. — Let $F = (f_1, \dots, f_p) \subseteq \mathbb{k}[x_1, \dots, x_n]$ be a regular sequence of homogeneous polynomials, all of degree d_0 , and let $g \in \mathbb{k}[x_1, \dots, x_n]$ be a homogeneous polynomial of degree d_0 . Finally, for each $1 \leq k \leq n - p - 1$, let $\mathcal{J}_k(\text{jac}(g, F))$ be the ideal of $\mathcal{R}_n$ generated by the first k columns of $\text{jac}(g, F)$. Then assuming that Conjecture 4.3.2 and Conjecture 4.3.6 are true, the number of arithmetic operations in $\mathbb{k}$ required to compute a grevlex Gröbner basis for the ideal $\mathcal{I}(g, F) = \langle F \rangle + \mathcal{I}_{p+1}(\text{jac}(g, F))$ is in

$$O \left(\sum_{d=d_0}^D \left(\binom{n+d-1}{n-1} - \text{HF}_{\mathcal{R}_n/\mathcal{I}(g,F)}(d) \right)^{\omega-2} \mathcal{R}(d) \binom{n+d-1}{n-1} \right)$$

with

$$\begin{aligned} \mathcal{R}(d) = & p \binom{n+d-d_0-1}{n-1} + \binom{n+d-(p+1)d_0-1}{n-1} \binom{n}{p+1} \\ & - \left(\sum_{k=1}^{n-p-1} \text{HF}_{\mathcal{J}_k(\text{jac}(g,F))}(d - (p+1)d_0) \binom{n-k-1}{p} \right) \end{aligned}$$

where the Hilbert function $\text{HF}_{\mathbb{k}[x_1, \dots, x_n]/\mathcal{I}(g,F)}(d)$ is given in Proposition 4.3.9, the Hilbert functions $\text{HF}_{\mathcal{J}_k(\text{jac}(g,F))}(d)$ are those given in Corollary 4.3.5, $D = (n+p)d_0 + 1$, and $2 \leq \omega \leq 3$ is a suitable exponent of matrix multiplication.

Proof. By [Spa14, Cor.2.3], the largest degree of an element of the reduced grevlex Gröbner basis of $\mathcal{I}(g, F)$ is $D = (n+p)d_0 + 1$. The output of $\text{CritGB}(F, g, D)$ is thus a grevlex Gröbner basis of $\mathcal{I}(g, F)$.

The complexity of computing Gröbner bases for systems of partial derivatives of F in Algorithm 5 is bounded by the complexity of computing a Gröbner basis of F itself, and thus the complexity of Algorithm 5 is bounded by that of its final step. MatrixF_5 only performs arithmetic operations when computing row-echelon forms for the Macaulay matrices it builds. We can therefore bound the number of arithmetic operations performed by MatrixF_5 on any given input by the cost of echelonizing the Macaulay matrices it encounters. For a given $d_0 \leq d \leq D$, the Macaulay matrix $\mathcal{M}_d(\mathcal{I}(g, F))$ is of rank $\text{HF}_{\mathcal{I}(g,F)}(d)$ and has $\# \text{Mon}_d(\mathcal{R}_n) = \binom{n+d-1}{n-1}$. The rows of $\mathcal{M}_d(\mathcal{I}(g, F))$ are indexed by a subset of

$$(\text{Mon}_{d-d_0}(\mathcal{R}_n^{\#F}) \cup \text{Mon}_{d-(p+1)d_0}(\mathcal{R}_n^{\#F_{r+1}(M)p+1\text{jac}(g,F)})) \setminus H_{d-pd_0},$$

which has cardinality precisely $\mathcal{R}(d)$ by Proposition 4.3.1. By [Sto00, Sec.2.2], an $s \times t$ matrix of rank r over $\mathbb{k}$ can be echelonized using $O(r^{\omega-2}st)$ operations, so the result follows. $\square$

4.3.2 COMPARISON WITH LAZARD'S ALGORITHM

We conclude with a comparison of the upper bound

$$\sum_{d=pd_0}^{d_0(p-1)+(d_0-1)n+1} \mathcal{R}(d)$$

from Theorem 4.3.10 on the total number of rows in all of the Macaulay matrices built by Algorithm 4 to the upper bound

$$\binom{q}{p} \binom{d_0(p-1) + (d_0-1)n + 1 + n}{n}.$$

on the number of rows in the Macaulay matrices built by Lazard's algorithm obtained in [FSS13, Theorem 20].

This comparison does not take into account the fact that in [GNS23, Algorithm 1], Macaulay matrices are computed degree-by-degree, so that reductions to zero in lower degrees can be used to eliminate reductions to zero in subsequent degrees.

This comparison also does not take into account the F_5 criterion [Fau02, Theorem 1], which allows for several more reductions to zero to be avoided. However, the complexity of F_5 has only been analysed in the case of a regular sequence, in [BFS15].

REMARK 4.3.11. — By computing a $\prec_{\text{pot}}$ -Gröbner basis for $\text{Syz}(F_p(A))$, we can estimate the number of extra reductions to zero avoided by Algorithm 4 thanks to Proposition 1.2.2 (ii). For $p = 3, q = 6, n = 4, d_0 = 3$, the ratio of the number of rows estimated by taking into account this criterion to the number of rows computed by Lazard's algorithm is 29.397, while not taking into account this criterion yields a ratio of 26.786. Similarly, for $p = 3, q = 7, n = 5, d_0 = 3$, taking into account this criterion gives a ratio of 41.006, while not taking into account this criterion gives a ratio of 34.946. This suggests that a careful complexity analysis of Algorithm 5 might provide a theoretical complexity improvement that is better than the one suggested by the graphs we give here.

p, n fixed, d_0 grows

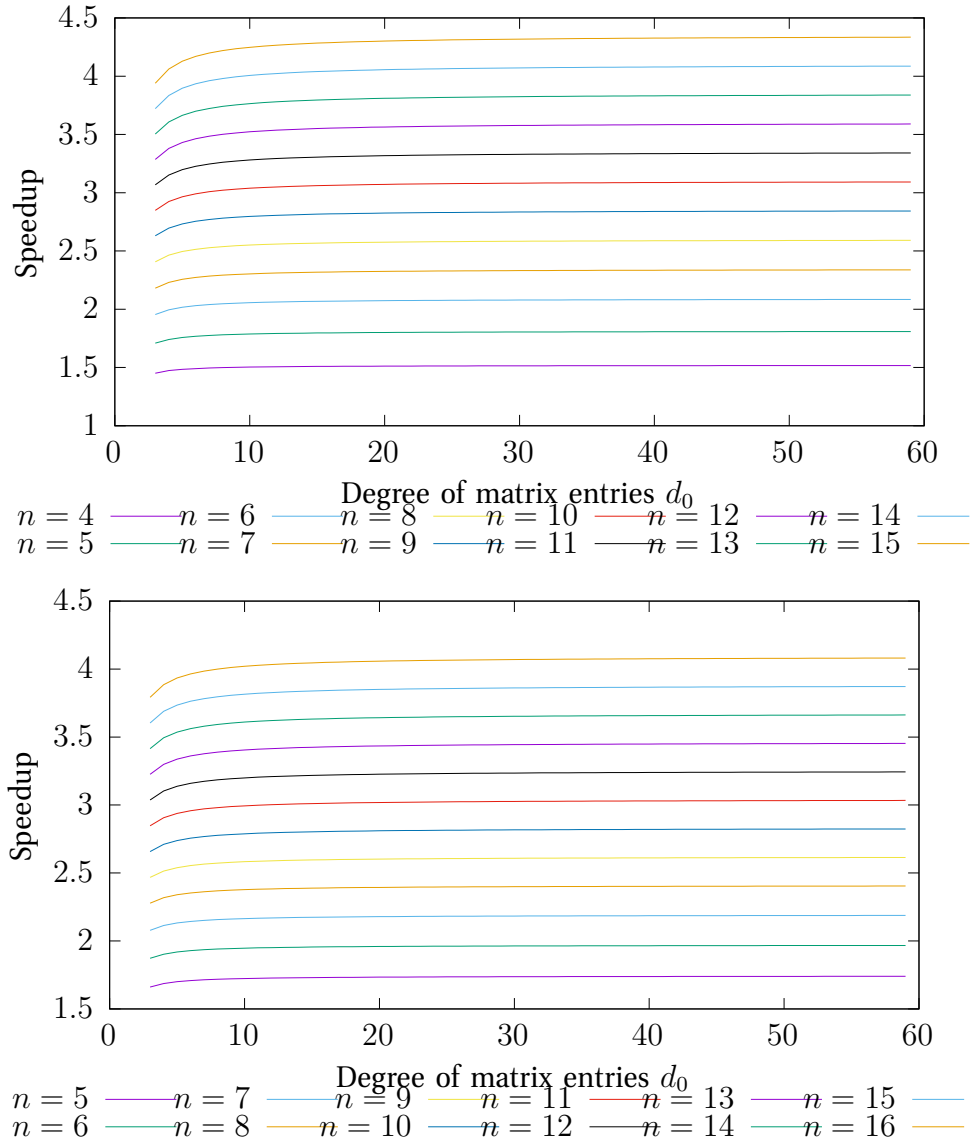
First, we fix the number of polynomials p and the number of variables n , and allow the degree d_0 to grow. We take $q = n + p - 1$, so that the ideal of maximal minors has dimension zero. Figure 4.1 shows that for a fixed p and n , the theoretical gain which we obtain appears to grow logarithmically in d_0 .

Finally, we compare Lazard's algorithm to a (nonexistent) algorithm which would compute full-rank Macaulay matrices. Fig. 4.2 shows that such an algorithm appears to also only provide a theoretical gain which grows logarithmically in d_0 .

p, d_0 fixed, n grows

Next, we fix the number of polynomials p and the degree d_0 and allow the number of variables n to grow. Again, we take $q = n + p - 1$ so that the ideal of maximal minors has dimension zero. Figure 4.3 shows that for a fixed p and d_0 , the theoretical gain which we obtain appears to grow linearly in n .

We conclude by again comparing Lazard's algorithm to a (nonexistent) algorithm which would compute full-rank Macaulay matrices. Figure 4.4 shows that such an algorithm appears to provide a theoretical gain which grows exponentially in n , demonstrating that there is still potentially much to be gained by devising new criteria which predict more reductions to zero.

Figure 4.1: Speedup of Algorithm 4. Top: $p = 3$; bottom: $p = 4$

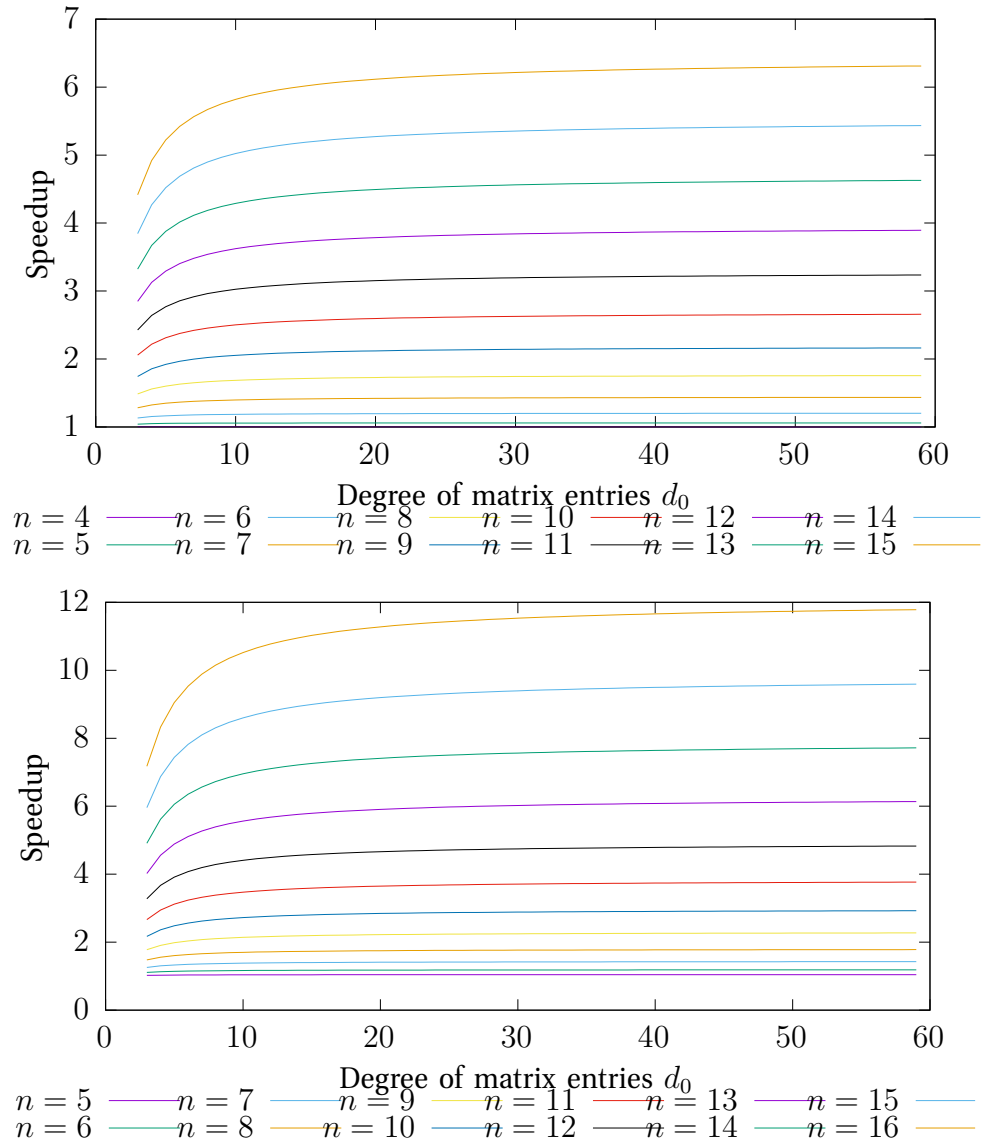
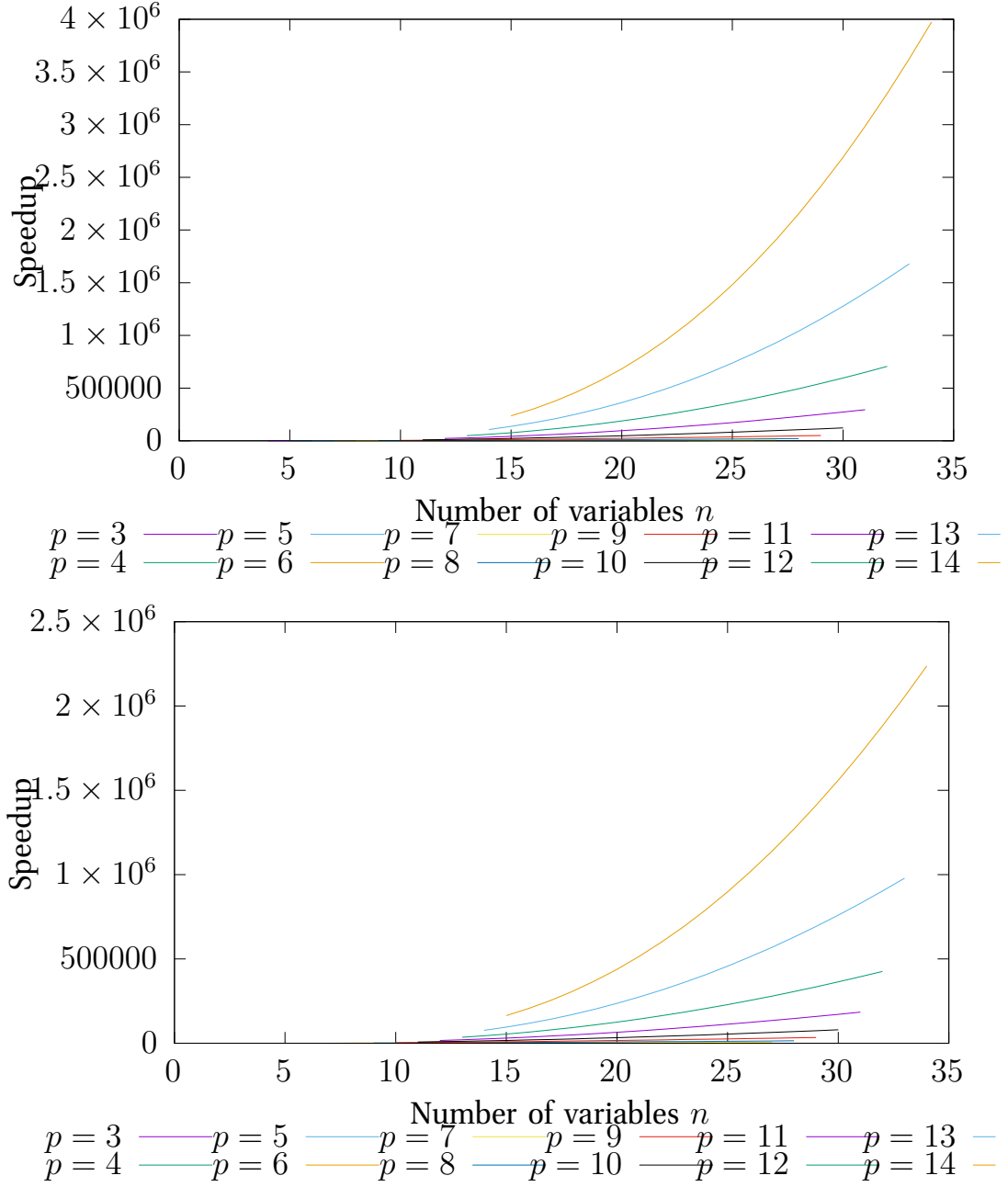


Figure 4.2: Speedup of an algorithm which computes full-rank Macaulay matrices. Top: $p = 3$; bottom: $p = 4$.

Figure 4.3: Speedup of Algorithm 4. Top: $d_0 = 3$; bottom: $d_0 = 4$.

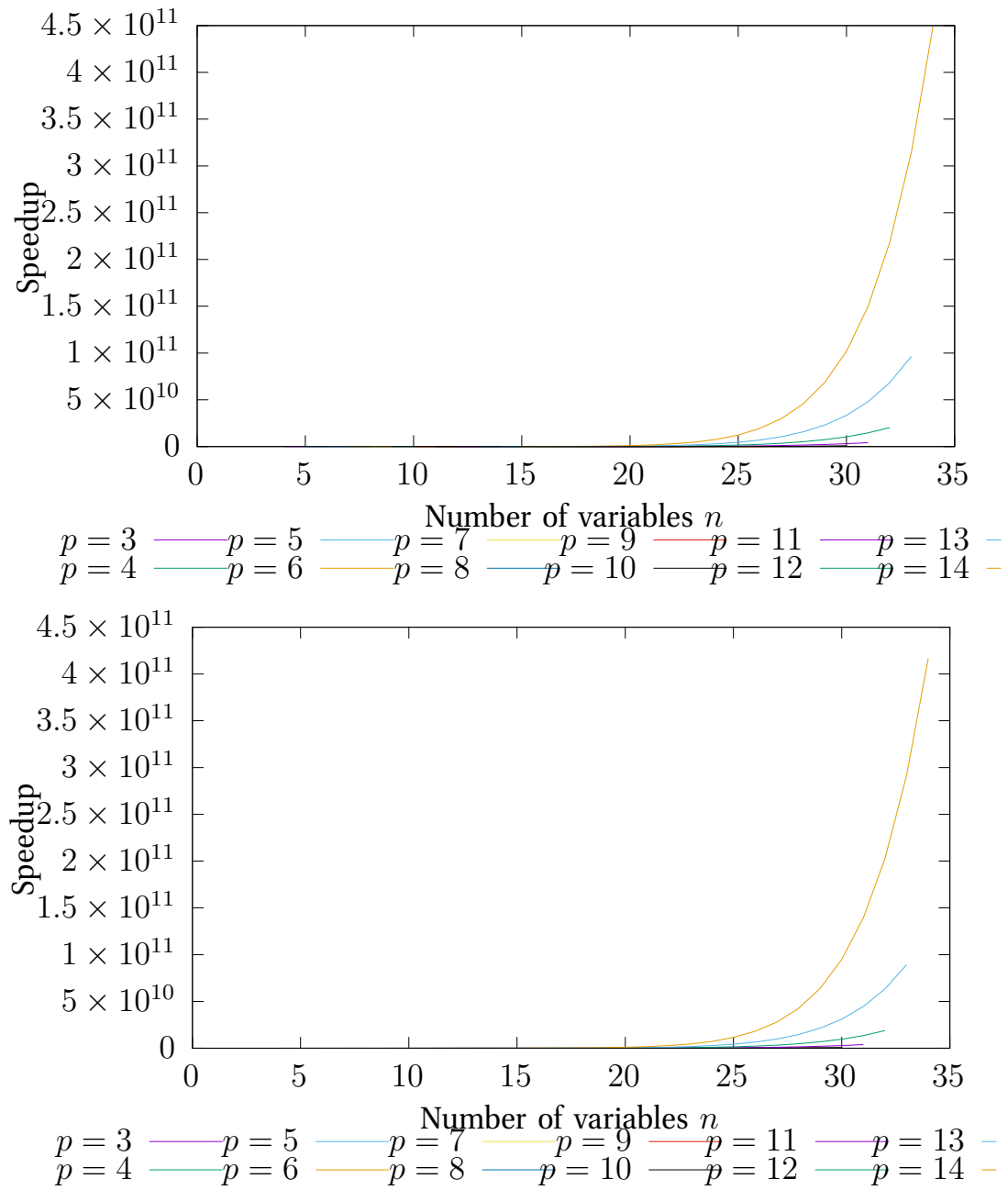


Figure 4.4: Speedup of an algorithm which computes full-rank Macaulay matrices. Top: $d_0 = 3$; bottom: $d_0 = 4$.

PART II

BIT COMPLEXITY

PRELIMINARIES

The second part of this thesis finds its mathematical foundations in (arithmetic) intersection theory. We begin, therefore, by recalling these foundations. First, in the realm of usual (algebraic) intersection theory, all of the statements which we give can be found, with proof, in [Ful98b]. For the reader who is willing to admit, without proof, some of the more technical machinery, [EH16] is perhaps a more approachable reference.

Second, in the realm of arithmetic intersection theory, we draw the basic constructions from [GS90a]. We also rely heavily on the theory developed in [BGS94] for heights of projective varieties, and on [GS90b] for the theory of characteristic classes of Hermitian vector bundles. Finally, it seems prudent, before delving into all of this theory, to acknowledge that this second part is far more technical than the first.¹

5.1 ALGEBRAIC CONSTRUCTIONS

5.1.1 THE ALGEBRAIC CHOW RING

Let X be an algebraic scheme over a field $\mathbb{k}$. For an integer $p \geq 0$, we will denote by $Z^p(X)$ (resp. $Z_p(X)$) the group of cycles of codimension (resp. dimension) p on X . Let $Y \subseteq X$ be a subvariety of X of codimension $p - 1$, with generic point y . Let $f \in k(y)^*$ be a nonzero rational function on Y . Then f gives rise to a cycle $\text{div}(f) \in Z^p(X)$ defined by

$$\text{div}(f) = \sum_{\substack{V \subseteq Y \\ \text{of codimension one}}} \text{ord}_V(f)[V].$$

Cycles of the form $\text{div}(f)$ are called *cycles rationally equivalent to zero*. We denote by $R^p(X) \subseteq Z^p(X)$ (resp. $R_p(X) \subseteq Z_p(X)$) the subgroup of cycles rationally equivalent to zero. The quotients $\text{CH}^p(X) = Z^p(X)/R^p(X)$ (resp. $\text{CH}_p(X) = Z_p(X)/R_p(X)$) are the *algebraic Chow groups* of X . We will denote by $Z^*(X) = \bigoplus_p Z^p(X)$ (resp. $Z_*(X) = \bigoplus_p Z_p(X)$) the *group of cycles graded by codimension* (resp. *dimension*).

Similarly, we denote by $R^*(X) = \bigoplus_p R^p(X)$ and $\text{CH}^*(X) = \bigoplus_p \text{CH}^p(X)$ (resp. $R_*(X) = \bigoplus_p R_p(X)$ and $\text{CH}_*(X) = \bigoplus_p \text{CH}_p(X)$) the *group of cycles rationally equivalent to zero graded by codimension* (resp. *dimension*) and the *algebraic Chow group graded by codimension* (resp. *dimension*) of X . When the choice of grading is unimportant, we will simply denote by $Z(X)$ (resp. $R(X)$, $\text{CH}(X)$) the *group of cycles* (resp. *group of cycles rationally equivalent to zero*, *algebraic Chow group*) of X .

We recall that rational equivalence has a slightly more geometric interpretation: two cycles $V, W \in Z(X)$ are rationally equivalent if and only if there exists a cycle $Z \in Z(X \times \mathbb{P}^1)$ not contained in any fibre such that $V = \pi_1(Z \cap (X \times \{0\}))$ and $W = \pi_1(Z \cap (X \times \{\infty\}))$.

¹This acknowledgement, of course, completely shields the author from any criticism arising from the perceived difficulty of the presented material.

THEOREM 5.1.1 ([Ful98c, Proposition 8.1.1, Example 8.1.1], [EH16, Theorem-Definition 1.5]). — Let X be a smooth, quasi-projective scheme. Then the group $\mathrm{CH}(X)$ carries on it an *intersection product*, under which the product of the classes of two generically transverse subvarieties $V, W \subseteq X$ is the class of their intersection:

$$[V] \cdot [W] = [V \cap W] \in \mathrm{CH}(X).$$

Note that this intersection product makes our choice of grading $\mathrm{CH}(X)$ by codimension (rather than by dimension) a well-motivated one, and, by [Ful98c, Proposition 8.3], turns $\mathrm{CH}(X)$ into a graded ring $\mathrm{CH}^*(X)$, called the *Chow ring* of X .

5.1.2 FUNCTORIALITY

Let $f : Y \rightarrow X$ be a proper map of algebraic schemes over a field $\mathbb{k}$, and $V \subseteq Y$ a subvariety. The *pushforward* of the cycle $[V]$ under f is defined to be

$$f_*[V] = \begin{cases} 0 & \text{if } \dim(f(V)) < \dim(V) \\ [\kappa(V) : \kappa(f(V))][f(V)] & \text{if } \dim(f(V)) = \dim(V) \end{cases}.$$

Extending by linearity, the pushforward becomes a map $f_* : Z_p(Y) \rightarrow Z_p(X)$. It turns out that f_* respects rational equivalence and is therefore functorial.

THEOREM 5.1.2 ([Ful98d, Theorem 1.4], [EH16, Theorem 1.20]). — Let $f : Y \rightarrow X$ be a proper map of schemes. Then the pushforward of cycles $f_* : Z_p(Y) \rightarrow Z_p(X)$ respects rational equivalence, and therefore defines a graded morphism of Chow groups $f_* : \mathrm{CH}_*(Y) \rightarrow \mathrm{CH}_*(X)$.

Now suppose that $f : Y \rightarrow X$ is a flat map of schemes over a field $\mathbb{k}$, and $V \subseteq Y$ a subvariety. The *pullback* of the cycle $[V]$ under f is defined to be $f^*[V] = [f^{-1}(V)]$. Analogously to pushforwards, f^* respects rational equivalence, and even the intersection product when it exists.

THEOREM 5.1.3 ([Ful98d, Theorem 1.7], [Ful98c, Proposition 8.3(a)], [EH16, Theorem 1.25]). — Let $f : Y \rightarrow X$ be a flat map of schemes. Then

- (i) the pullback of cycles $f^* : Z^p(X) \rightarrow Z^p(Y)$ respects rational equivalence, and therefore defines a graded morphism of Chow groups $f^* : \mathrm{CH}^*(X) \rightarrow \mathrm{CH}^*(Y)$.
- (ii) if, moreover, X and Y are smooth, quasi-projective, algebraic schemes over a field $\mathbb{k}$, then $f^* : \mathrm{CH}(X) \rightarrow \mathrm{CH}(Y)$ is a graded ring morphism, turning $\mathrm{CH}(-)$, together with f_* into a functor from the category of smooth, quasi-projective, algebraic $\mathbb{k}$ -schemes to graded rings.

Of particular importance is the relationship between the pullback and the pushforward, called the *projection formula*.

THEOREM 5.1.4 (Projection formula, [Ful98c, Proposition 8.3(c)], [EH16, Theorem 1.23(b)]). — Let $f : Y \rightarrow X$ be a proper map of smooth, quasi-projective, algebraic $\mathbb{k}$ -varieties. Then $f_* : \mathrm{CH}(Y) \rightarrow \mathrm{CH}(X)$ is a graded morphism of graded $\mathrm{CH}(X)$ -modules. In particular, for any $\alpha \in \mathrm{CH}(X)$ and $\beta \in \mathrm{CH}(Y)$,

$$f_*(f^*(\alpha) \cdot \beta) = \alpha \cdot f_*(\beta).$$

PRELIMINARIES

5.1.3 ALGEBRAIC VECTOR BUNDLES

Let X be an algebraic scheme and $\mathcal{F}$ a coherent locally free sheaf on X . Let $\mathcal{F}^\vee$ be the dual of $\mathcal{F}$ and $\text{Sym}(\mathcal{F}^\vee)$ the symmetric algebra of $\mathcal{F}^\vee$. The X -scheme $F = \underline{\text{Spec}}_X(\text{Sym}(\mathcal{F}^\vee))$ is the *algebraic vector bundle* associated to $\mathcal{F}$. It has a natural geometric interpretation. Let $p \in X$ be a point, with residue field $\kappa(p)$. Let $\pi : F \rightarrow X$ be the structure map, and $g : \text{Spec}(\kappa(p)) \rightarrow X$ the canonical map. Then

$$\begin{aligned} \pi^{-1}\{p\} &= F \times_X \text{Spec}(\kappa(p)) \\ &= \underline{\text{Spec}}_{\text{Spec}(\kappa(p))}(g^* \text{Sym}(\mathcal{F}^\vee)) \\ &= \underline{\text{Spec}}_{\text{Spec}(\kappa(p))}(g^{-1} \text{Sym}(\mathcal{F}^\vee) \otimes_{g^{-1}\mathcal{O}_X} \mathcal{O}_{\text{Spec}(\kappa(p))}) \\ &= \underline{\text{Spec}}_{\text{Spec}(\kappa(p))}(\text{Sym}(\mathcal{F}^\vee)_p \otimes_{\mathcal{O}_{X,p}} \kappa(p)) \\ &= \underline{\text{Spec}}_{\text{Spec}(\kappa(p))}(\text{Sym}(\mathcal{F}_p^\vee \otimes_{\mathcal{O}_{X,p}} \kappa(p))) \end{aligned}$$

Now $\mathcal{F}_p^\vee \otimes_{\mathcal{O}_{X,p}} \kappa(p)$ is a vector space over $\kappa(p)$ of dimension equal to the rank of $\mathcal{F}_p$ as a free $\mathcal{O}_{X,p}$ -module. If this rank is r , we can then conclude that

$$\pi^{-1}\{p\} = \underline{\text{Spec}}_{\text{Spec}(\kappa(p))}(\kappa(p)[t_1, \dots, t_r]) = \mathbb{A}_{\kappa(p)}^r.$$

Since F is the scheme-theoretic union of the fibres of π , this construction allows us to realise any point of F as a pair (p, t) where $p \in X$ and $t \in \mathbb{A}_{\kappa(p)}^r$.

PROPOSITION 5.1.5 ([Ful98b, B.3.3]). — Let $\pi : Y \rightarrow X$ be an X -scheme and suppose that there exists an open cover $\{U_i\}$ of X , isomorphisms of U -schemes $\varphi_i : Y \times_X U_i \rightarrow \mathbb{A}^r \times_X U_i$, and, for any pair i, j , automorphisms $g_{i,j} : U_i \cap U_j \rightarrow \text{GL}_{r,X}$ such that $(\varphi_i \circ \varphi_j^{-1})|_{U_i \cap U_j} = g_{i,j}$. Then there exists a coherent, locally free sheaf $\mathcal{F}$ of rank r on X such that $Y = \underline{\text{Spec}}_X(\text{Sym}(\mathcal{F}^\vee))$.

A *section* of F is a map of schemes $s : X \rightarrow F$ such that $\pi \circ s = \text{id}_F$. Note in particular that if s is a section of F , then $s(x) \in \pi^{-1}\{x\}$. The sections of $\mathcal{F}$ over an open set $U \subseteq X$ correspond to sections of $\pi|_U : \pi^{-1}(U) \rightarrow U$.

Motivating the terminology here is the fact that sections of F are exactly global sections of $\mathcal{F}$ as a sheaf. In one direction, a global section $s \in \mathcal{F}(X)$ defines the section $x \mapsto s_x \otimes 1$ of F . In the other direction, the universal property of the relative spectrum shows that sections $s : X \rightarrow F$ correspond to $\mathcal{O}_X$ -algebra maps $\text{Sym}(\mathcal{F}^\vee) \rightarrow \mathcal{O}_X$. Each such map restricts to a map $\mathcal{F}^\vee \rightarrow \mathcal{O}_X$, which in turn dualises to a global section of $\mathcal{F}$. Indeed, given an X -scheme $Y \rightarrow X$ satisfying the hypotheses of Proposition 5.1.5, the corresponding sheaf $\mathcal{F}$ given by Proposition 5.1.5 is called the *sheaf of sections* of Y .

EXAMPLE 5.1.6. — Let $\mathbb{k}$ be an algebraically closed field and let $X = \text{Spec}(\mathbb{k}[t]) = \mathbb{A}_{\mathbb{k}}^1$. Let $\mathcal{F} = \mathcal{O}_X$. Consider the global section $t \in \mathcal{F}(X) = \mathbb{k}[t]$. For any closed point $x \in X$, the residue field $\kappa(x) \cong \mathbb{k}$ and $t_x = x \in \mathbb{A}_{\mathbb{k}}^1 = F_x$. At the generic point $\eta \in X$, we have $t_\eta = t \in \mathbb{A}_{\mathbb{k}(t)}^1 = F_\eta$.

The zero section $0 \in \mathcal{F}(X)$ corresponds to a section $0 : X \rightarrow F$. Let $s : X \rightarrow F$ be any section of F . Consider the pushout diagram

$$\begin{array}{ccc} Z(s) & \longrightarrow & X \\ \downarrow & & \downarrow 0 \\ X & \xrightarrow{s} & F \end{array}$$

The fibre product $Z(s) = X \times_{s,F,0} X$ is called the *zero subscheme* of the section X . Note that if we denote by $Z \subset F$ the image of X , then $Z(s) = s^{-1}(Z)$.

EXAMPLE 5.1.7. — Consider again the global section $t \in \mathcal{F}(X)$. The zero subscheme of t is the subscheme of X consisting of those points $x \in X$ such that $t_x = 0$. In other words, $Z(t) = \{0\}$ as a set.

Consider now the global section $t^2 \in \mathcal{F}(X)$. As a set, the zero scheme of t^2 is the same as that of t . Note, however, that as a scheme, $Z(t^2)$ is non-reduced. Indeed, it is the scheme corresponding to the ideal $(t^2) \subseteq \mathbb{k}[t]$.

PROPOSITION 5.1.8. — Let $\mathcal{F}$ be a coherent, locally free sheaf of rank r on a scheme X . Let F be its associated vector bundle. Let $s : \mathcal{O}_X \rightarrow \mathcal{F}$ be a global section of $\mathcal{F}$. Then $Z(s)$ is the closed subscheme of X defined by the quasicohherent ideal sheaf $\text{im}(\mathcal{F}^\vee \xrightarrow{s^\vee} \mathcal{O}_X)$.

Proof. Let $\{U_i\}$ be an affine open cover of X . Refining our cover if necessary, we may assume that $\mathcal{F}$ is trivial over each U_i . The $\mathcal{O}_X$ -module map defined by s is given, over some U_i , by $1 \mapsto s|_{U_i}$. For each i , let $U_i = \text{Spec } A_i$ and choose an A_i -basis $e_1^{(i)}, \dots, e_r^{(i)}$ for each free A_i -module $\mathcal{F}|_{U_i}$. Write, for each i , $s|_{U_i} = f_1^{(i)}e_1^{(i)} + \dots + f_r^{(i)}e_r^{(i)}$ for some $f_1^{(i)}, \dots, f_r^{(i)} \in A_i$. Then the dual of s defines an $\mathcal{O}_X$ -module map $\mathcal{F}^\vee \rightarrow \mathcal{O}_X$ which is given, over some U_i , by $e_j^{(i)} \mapsto f_j^{(i)}$.

Over a U_i , the image of $s^\vee$ is then the ideal $(f_1^{(i)}, \dots, f_r^{(i)})$ in A_i .

The construction of relative Spec allows us to cover F by the collection of affine open subschemes $\{\pi^{-1}(U_i) = \text{Spec}(\mathcal{F}(U_i)[t_1, \dots, t_r])\}$. Subsequently, the zero subscheme $Z(s) = X \times_{0,F,s} X$ can be covered by $\{U_i \times_{0,\pi^{-1}(U_i),s} U_i\}$. But, for each i ,

$$\begin{aligned} U_i \times_{0,\pi^{-1}(U_i),s} U_i &= \text{Spec}(A_i \otimes_{s^\#, A_i[t_1, \dots, t_r], 0^\#} A_i) \\ &= \text{Spec} \left(\frac{A_i[t_1, \dots, t_r]}{(t_1 - f_1^{(i)}, \dots, t_r - f_r^{(i)})} \otimes_{A_i[t_1, \dots, t_r]} \frac{A_i[t_1, \dots, t_r]}{(t_1, \dots, t_r)} \right) \\ &= \text{Spec}(A_i / (f_1^{(i)}, \dots, f_r^{(i)})). \end{aligned}$$

The ideal sheaf defining $Z(s)$ therefore agrees with the ideal sheaf $\text{im}(\mathcal{F}^\vee \xrightarrow{s^\vee} \mathcal{O}_X)$ on each U_i , so we are done. $\square$

We will call a section $s \in \mathcal{F}(X)$ (equivalently $s : X \rightarrow F$) a *regular section* if $Z(s)$ has pure codimension r .

EXAMPLE 5.1.9. — Consider the sheaf $\mathcal{F} = \mathcal{O}_X \oplus \mathcal{O}_X$, with $X = \text{Spec}(\mathbb{k}[x, y, z])$. Then (xy, x) is a global section of $\mathcal{F}$. The zero scheme of (xy, x) is simply $\text{Spec} \left(\frac{\mathbb{k}[x, y, z]}{(xy, x)} \right)$ which has codimension one in X . Thus, (xy, x) is not a regular section of $\mathcal{F}$. Note that (xy, x) is not a regular sequence. In general, if $\mathcal{F}$ is locally free of rank r , then a section $s \in \mathcal{F}(X)$ is regular if and only if for each $U \subseteq X$, the r -tuple of regular functions on U defining $s|_U$ is a regular sequence.

5.1.4 GRASSMANN BUNDLES

Let X be a smooth scheme. A *projective bundle* on X is an X -scheme $\pi : Y \rightarrow X$ such that there exists an open cover $\{U_i\}$ of X , isomorphisms $\varphi_i : Y \times_X U_i \rightarrow \mathbb{P}^r \times_X U_i$, and, for any

PRELIMINARIES

pair i, j , automorphisms $g_{i,j} : U_i \cap U_j \rightarrow \mathrm{PGL}_{r+1,X}$ such that $(\varphi_i \circ \varphi_j^{-1})|_{U_i \cap U_j} = g_{i,j}$. The following fact, for which we do not furnish a proof, allows us to view projective bundles as fibrewise projectivisations of vector bundles:

PROPOSITION 5.1.10. — Let $\pi : Y \rightarrow X$ be a projective bundle. Then there exists a coherent, locally free sheaf $\mathcal{F}$ on X such that for all $p \in X$, $\pi^{-1}\{p\} = \mathbb{P}(\mathcal{F}_p \otimes_{\mathcal{O}_{X,p}} \kappa(p))$. Conversely, for any coherent locally free sheaf $\mathcal{F}$ on X , there exists a projective bundle $\pi : \mathbb{P}(\mathcal{F}) \rightarrow X$ such that for all $p \in X$, $\pi^{-1}\{p\} = \mathbb{P}(\mathcal{F}_p \otimes_{\mathcal{O}_{X,p}} \kappa(p))$.

According to Proposition 5.1.10, we may view points of a projective bundle $\mathbb{P}(\mathcal{F})$ as pairs (p, ℓ) , where $p \in X$ and $\ell \subseteq \mathcal{F}_p \otimes_{\mathcal{O}_{X,p}} \kappa(p)$ is a one-dimensional subspace of the fibre above p of the bundle corresponding to $\mathcal{F}$. Accordingly, $\mathbb{P}(\mathcal{F})$ carries on it a bundle whose fibre over a point (p, ℓ) is simply ℓ . The sheaf on $\mathbb{P}(\mathcal{F})$ associated to this bundle is $\mathcal{O}_{\mathbb{P}(\mathcal{F})}(-1)$, and so there is an injection $\mathcal{O}_{\mathbb{P}(\mathcal{F})}(-1) \hookrightarrow \pi^*\mathcal{F}$. If $\mathcal{Q}$ is the cokernel of this map, we then have an exact sequence

$$0 \rightarrow \mathcal{O}_{\mathbb{P}(\mathcal{F})}(-1) \hookrightarrow \pi^*\mathcal{F} \rightarrow \mathcal{Q} \rightarrow 0.$$

This sequence is called the *tautological exact sequence* on $\mathbb{P}(\mathcal{F})$. The bundle $\mathcal{O}_{\mathbb{P}(\mathcal{F})}(-1)$ (resp. $\mathcal{Q}$) is called the *tautological subbundle* (resp. *tautological quotient bundle*) on $\mathbb{P}(\mathcal{F})$.

The interpretation in Proposition 5.1.10 of projective fibre bundles as fibrewise projectivisations of vector bundles has a natural generalisation.

PROPOSITION 5.1.11. — Let $\mathcal{F}$ be a coherent, locally free sheaf of rank r on an algebraic scheme X . For any $k \in \mathbb{Z}_{>0}$, the functor which associates to an X -scheme T the set of locally free submodules of $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_T$ of rank k is representable by an X -scheme $\mathbb{G}(k, \mathcal{F}) \rightarrow X$.

The scheme $\mathbb{G}(k, \mathcal{F})$ from Proposition 5.1.11 is called a *Grassmann bundle*. Taking $T = \{p\}$ for a point $p \in X$ shows that $\mathbb{G}(k, \mathcal{F})$ can be viewed as pairs (p, V) with $p \in X$ and $V \subseteq \mathcal{F}_p^\vee \otimes_{\mathcal{O}_{X,p}} \kappa(p)$ a k -dimensional subspace of the fibre of $\mathcal{F}$ above p . As in the projective case (when $k = 1$), the Grassmann bundle $\mathbb{G}(k, \mathcal{F})$ carries on it a vector bundle whose fibre over a point (p, V) is simply V , called the *tautological rank- k subbundle*. Denoting by $\mathcal{S}$ the sheaf associated to this bundle, there is an injection $\mathcal{S} \hookrightarrow \pi^*\mathcal{F}$ which is just fibrewise inclusion. Taking $\mathcal{Q}$ to be the cokernel of this injection – called the *tautological quotient bundle* – yields the tautological exact sequence on $\mathbb{G}(k, \mathcal{F})$

$$0 \rightarrow \mathcal{S} \hookrightarrow \pi^*\mathcal{F} \rightarrow \mathcal{Q} \rightarrow 0.$$

5.1.5 ALGEBRAIC CHERN CLASSES

Let $\mathcal{F}$ be a coherent, locally free sheaf of rank r on a smooth projective scheme X . Let $s \in \Gamma(\mathbb{P}(\mathcal{F}), \mathcal{O}_{\mathbb{P}(\mathcal{F})}(1))$ be an arbitrary regular section. Then the zero subscheme $Z(s)$ has pure codimension one in $\mathbb{P}(\mathcal{F})$, so corresponds to a Weil divisor $\mathrm{div}(s)$. Let t be any other regular section of $\mathcal{O}_{\mathbb{P}(\mathcal{F})}(1)$. Then $\mathrm{div}(t) - \mathrm{div}(s) = \mathrm{div}(\frac{t}{s})$ is the divisor of a rational function on $\mathbb{P}(\mathcal{F})$, and thus $[\mathrm{div}(s)] = [\mathrm{div}(t)]$ in $\mathrm{CH}^1(\mathbb{P}(\mathcal{F}))$. This class is called the *hyperplane class* of $\mathbb{P}(\mathcal{F})$.

PROPOSITION 5.1.12 ([EH16, Theorem 5.9], [Ful98e, Remark 3.2.4]). — Let $\mathcal{F}$ be a coherent, locally free sheaf of rank r on a smooth algebraic scheme X , and let $\pi : \mathbb{P}(\mathcal{F}) \rightarrow X$ be the canonical

projection. Let $\xi \in \mathrm{CH}^1(\mathbb{P}(\mathcal{F}))$ be the hyperplane class. Then for any class $x \in \mathrm{CH}^p(\mathbb{P}(\mathcal{F}))$ there exist $(\alpha_1, \dots, \alpha_r) \in \bigoplus_{i=1}^r \mathrm{CH}^{p-r+i}(X)$ such that

$$x = \sum_{i=1}^r (-1)^{i-1} \pi^*(\alpha_i) \xi^{r-i}.$$

In particular, there exist $(\alpha_1, \dots, \alpha_r) \in \bigoplus_{i=1}^r \mathrm{CH}^i(X)$ such that

$$\xi^r = \sum_{i=1}^r (-1)^{i-1} \pi^*(\alpha_i) \xi^{r-i}.$$

The coefficient α_i is called the i^{th} Chern class of $\mathcal{F}$ and is denoted by $c_i(\mathcal{F})$. We will additionally take $c_0(\mathcal{F}) = 1$. The sum

$$c(\mathcal{F}) = \sum_{i=0}^r c_i(\mathcal{F}) \in \mathrm{CH}^*(X)$$

is called the *total Chern class* of $\mathcal{F}$. It behaves well with respect to exact sequences.

THEOREM 5.1.13 (Whitney sum formula, [Ful98e, Theorem 3.2(e)]). — Let $0 \rightarrow \mathcal{F}' \rightarrow \mathcal{F} \rightarrow \mathcal{F}'' \rightarrow 0$ be an exact sequence of coherent, locally free sheaves on a smooth projective scheme X . Then

$$c(\mathcal{F}) = c(\mathcal{F}')c(\mathcal{F}'') \in \mathrm{CH}^*(X).$$

EXAMPLE 5.1.14. — Let $X = \mathrm{Spec} \mathbb{k}$, for $\mathbb{k}$ a field. Since X has dimension zero, $\mathrm{CH}^0(X) = \mathbb{Z}$ and $\mathrm{CH}^i(X) = 0$ for all $i > 0$. Let $\mathcal{F} = \mathcal{O}_X^{\oplus r}$. Then Proposition 5.1.12 shows that we can decompose

$$\mathrm{CH}_0(\mathbb{P}(\mathcal{F})) = \mathrm{CH}^{r-1}(\mathbb{P}(\mathcal{F})) = \bigoplus_{i=1}^r \mathrm{CH}^{i-1}(X) = \mathrm{CH}^0(X) = \mathbb{Z}.$$

In this case, $\mathbb{P}(\mathcal{F}) = \mathbb{P}_{\mathbb{k}}^{r-1}$, and the computation $\mathrm{CH}_0(\mathbb{P}_{\mathbb{k}}^{r-1}) = \mathbb{Z}$ admits a particularly intuitive explanation – any two zero-dimensional varieties with the same number of points (counted with multiplicity) are rationally equivalent.

5.2 ARITHMETIC CONSTRUCTIONS

5.2.1 FORMS AND CURRENTS

For an integer $n \geq 1$, denote by $C_c^\infty(\mathbb{C}^n)$ the vector space over $\mathbb{C}$ of smooth, compactly supported, complex valued functions on $\mathbb{C}^n$. For each integer $p \geq 1$, the space $C_c^\infty(\mathbb{C}^n)$ carries on it the C^p topology. A sequence $(\phi_k)_k$ of smooth functions, the support of each of which is contained in a compact set $K \subseteq \mathbb{C}^n$, converges to 0 in the C^p topology if for any tuple $(\alpha_1, \dots, \alpha_n)$ of nonnegative integers with $\alpha_1 + \dots + \alpha_n \leq p$, the sequence $\frac{\partial^{\alpha_1 + \dots + \alpha_n}}{\partial x_1^{\alpha_1} \dots \partial x_n^{\alpha_n}} \phi(x)$ converges uniformly to 0 for any $x \in K$. The sequence $(\phi_k)_k$ converges to 0 in the C^∞ topology on $C_c^\infty(\mathbb{C}^n)$ if the support of each ϕ_k is contained in a compact set K , and if it does so in the C^p topology for each $p \geq 1$.

PRELIMINARIES

For an integer $k \geq 0$, we denote by $A^k(\mathbb{C}^n)$ the space of differential k -forms on $\mathbb{C}^n$. This space admits a decomposition

$$A^k(\mathbb{C}^n) = \bigoplus_{p+q=k} A^{p,q}(X)$$

where $A^{p,q}(\mathbb{C}^n)$ is the vector space over $\mathbb{C}$ of differential forms of type (p, q) on $\mathbb{C}^n$. The space $A^{p,q}(\mathbb{C}^n)$ is spanned by

$$\{\phi dz_I \wedge d\bar{z}_J : |I|=p, |J|=q\}.$$

The C^∞ topology on $C_c^\infty(\mathbb{C}^n)$ induces a topology on the space $A_c^{p,q}(\mathbb{C}^n) \subseteq A^{p,q}(\mathbb{C}^n)$ of compactly supported differential forms of type (p, q) . A linear functional on $A_c^{p,q}(\mathbb{C}^n)$ which is continuous for this topology is called a *current of type (p, q)* . We denote by $\mathcal{D}_{p,q}(\mathbb{C}^n)$ the space of all currents of type (p, q) on $\mathbb{C}^n$, and let

$$\mathcal{D}_k(\mathbb{C}^n) = \bigoplus_{p+q=k} \mathcal{D}_{p,q}(\mathbb{C}^n).$$

Let X be a complex manifold of (complex) dimension n . Extending the definition of differential forms on $\mathbb{C}^n$ by working on coordinate charts, we define $A_c^{p,q}(X)$ to be the topological vector space of compactly supported differential forms on X . Similarly, we denote by $\mathcal{D}_{p,q}(X)$ the space of currents of type (p, q) on X .

Of particular importance are the *currents of integration*. Let $i : Y \hookrightarrow X$ be an analytic subspace of dimension k , and let $\text{Sing}(Y)$ be the closed subspace of singular points of Y . The map

$$\delta_Y : \alpha \mapsto \int_{Y \setminus \text{Sing}(Y)} i^* \alpha$$

defines a current $\delta_Y \in \mathcal{D}_{k,k}(X)$. This definition extends by linearity to define currents of integration along analytic cycles on X .

For integers $p \leq r$ and $q \leq s$, the wedge product on differential forms induces a map

$$\mathcal{D}_{p,q}(X) \otimes A_c^{r,s}(X) \rightarrow \mathcal{D}_{p-r,q-s}(X)$$

defined by $T \otimes \alpha \mapsto (\beta \mapsto T(\alpha \wedge \beta))$. We will denote by $T \wedge \alpha \in \mathcal{D}_{p-r,q-s}(X)$ the image of $T \otimes \alpha$ under this map.

Specialising this construction to the case where $T = \delta_X \in \mathcal{D}_{n,n}(X)$ is the current of integration on X itself, we obtain a map

$$[\cdot] : A_c^{r,s}(X) \rightarrow \mathcal{D}_{n-r,n-s}(X)$$

which sends a differential form α to the current $[\alpha] = \delta_X \wedge \alpha$. Note that if α is a locally L^1 form on X , then the current $\delta_X \wedge \alpha$ is well-defined, even if α is not compactly supported. For such forms, we will also denote by $[\alpha]$ the current $\delta_X \wedge \alpha$. For ease of exposition (actually there are much better reasons to do this), we let $\mathcal{D}^{r,s}(X) = \mathcal{D}_{n-r,n-s}(X)$.

As usual, we denote by $\partial : A_c^{*,*}(X) \rightarrow A_c^{*+1,*}(X)$ (resp. $\bar{\partial} : A_c^{*,*}(X) \rightarrow A_c^{*,*+1}(X)$) the holomorphic (resp. antiholomorphic) derivative. The map ∂ (resp. $\bar{\partial}$) dualises to a map $\mathcal{D}^{*,*}(X) \rightarrow \mathcal{D}^{*+1,*}(X)$ (resp. $\mathcal{D}^{*,*}(X) \rightarrow \mathcal{D}^{*,*+1}(X)$), which, abusing notation, we denote by ∂ (resp. $\bar{\partial}$). On both forms and currents, we let $d = \partial + \bar{\partial}$ and $d^c = \frac{i}{4\pi}(\bar{\partial} - \partial)$.

Finally, let

$$\begin{aligned}\tilde{A}_c^{p,q}(X) &= A_c^{p,q}(X)/(\partial A_c^{p-1,q}(X) + \bar{\partial} A_c^{p,q-1}(X)) \\ \tilde{\mathcal{D}}^{p,q}(X) &= \mathcal{D}^{p,q}(X)/(\partial \mathcal{D}^{p-1,q}(X) + \bar{\partial} \mathcal{D}^{p,q-1}(X))\end{aligned}$$

Since the map ∂^2 (resp. $\bar{\partial}^2, d^2, (d^c)^2$) is zero, the map on these quotients induced by ∂ (resp. $\bar{\partial}, d, d^c$) is well-defined and will also be denoted by ∂ (resp. $\bar{\partial}, d, d^c$).

5.2.2 THE ARITHMETIC CHOW RING

Let X be a regular scheme, flat and quasi-projective over $\text{Spec } \mathbb{Z}$, with regular generic fibre $X_{\mathbb{Q}}$. The scheme X is a particular kind of *arithmetic variety*, as in [BGS94, 2.1]. Following the notation therein, we will denote by $F_{\infty} : X(\mathbb{C}) \rightarrow X(\mathbb{C})$ the complex conjugation involution, and by

$$\begin{aligned}A^{p,p}(X_{\mathbb{R}}) &= \{\alpha \in A^{p,p}(X(\mathbb{C})) : F_{\infty}^*(\alpha) = (-1)^p \alpha\} \\ \mathcal{D}^{p,p}(X_{\mathbb{R}}) &= \{\alpha \in \mathcal{D}^{p,p}(X(\mathbb{C})) : F_{\infty}^*(\alpha) = (-1)^p \alpha\}.\end{aligned}$$

We will also denote by $\tilde{A}^{p,p}(X_{\mathbb{R}})$ (resp. $\tilde{\mathcal{D}}^{p,p}(X_{\mathbb{R}})$) the image of $A^{p,p}(X_{\mathbb{R}})$ (resp. $\mathcal{D}^{p,p}(X_{\mathbb{R}})$) in $\tilde{A}^{p,p}(X(\mathbb{C}))$ (resp. $\tilde{\mathcal{D}}^{p,p}(X(\mathbb{C}))$).

For any cycle $Z \in Z^p(X)$, the complex points $Z(\mathbb{C})$ of Z form an analytic cycle on $X(\mathbb{C})$, and therefore we can, abusing notation, define $\delta_Z \in \mathcal{D}^{p,p}(X_{\mathbb{R}})$ to be the current of integration along $Z(\mathbb{C})$. A *Green current* for Z is then a current $g \in \mathcal{D}^{p-1,p-1}(X_{\mathbb{R}})$ such that $dd^c g + \delta_Z$ is smooth. An *arithmetic cycle* is a pair (Z, g) where $Z \in Z^p(X)$ and g is a Green current for Z . In order to define arithmetic cycles rationally equivalent to zero in a way which is compatible with the construction of the algebraic Chow group of X , we must find Green currents for algebraic cycles rationally equivalent to zero.

Let f be a holomorphic function on $X(\mathbb{C})$. Let $Y = \text{div}(f)$ be the analytic hypersurface associated to f . The function $-\log|f|^2$ is locally L^1 on X , and so defines a current $[-\log|f|^2] \in \mathcal{D}_{n,n}(X)$. Moreover, $dd^c[-\log|f|^2] = -\frac{i}{\pi} \partial \bar{\partial} [\log|f|]$. The Poincaré-Lelong formula (see [GH94b, pg. 388]) therefore immediately implies that $[-\log|f|^2]$ is a Green current for Y . It follows that for any subvariety $Y \subseteq X$ of codimension $p-1$ with generic point y , and any $f \in k(y)^*$, the pair $(\text{div}(f), [-\log|f|^2])$ is a well-defined analytic cycle on X . We define $\hat{R}^p(X) \subseteq \hat{Z}^p(X)$ to be the subgroup of arithmetic cycles generated by those of the form $(0, \partial u + \bar{\partial} v)$ and $(\text{div}(f), [-\log|f|^2])$. Finally,

$$\widehat{\text{CH}}^p(X) = \hat{Z}^p(X) / \hat{R}^p(X)$$

are the *arithmetic Chow groups* of X . There are several group morphisms relating $\widehat{\text{CH}}(X)$, $\text{CH}(X)$, and $A^{p,p}(X_{\mathbb{R}})$ (see [GS90a, 3.3.4]):

$$\begin{aligned}z : \widehat{\text{CH}}^p(X) &\rightarrow \text{CH}^p(X) & \omega : \widehat{\text{CH}}(X) &\rightarrow A^{p,p}(X_{\mathbb{R}}) \\ [(Z, g)] &\mapsto [Z] & [(Z, g)] &\mapsto dd^c g + \delta_Z\end{aligned}$$

$$\begin{aligned}a : \tilde{A}^{p-1,p-1}(X_{\mathbb{R}}) &\rightarrow \widehat{\text{CH}}(X) \\ [\eta] &\mapsto [(0, \eta)]\end{aligned}$$

As in the algebraic setting, arithmetic Chow groups admit pushforwards and pullbacks.

PRELIMINARIES

THEOREM 5.2.1 ([GS90a, Theorem 3.6.1]). — Let X and Y be regular schemes, flat and quasi-projective over $\text{Spec } \mathbb{Z}$, with regular generic fibres and let $f : Y \rightarrow X$ be a morphism between them. Suppose that the map $Y_{\mathbb{Q}} \rightarrow X_{\mathbb{Q}}$ induced by f on generic fibres is smooth. Then

- (i) If f is flat, then for any $p \geq 0$, there is a group homomorphism

$$f^* : \widehat{\text{CH}}^p(X) \rightarrow \widehat{\text{CH}}^p(Y).$$

- (ii) If f is proper and X and Y are equidimensional, then for any $p \geq 0$, there is a group homomorphism

$$f_* : \widehat{\text{CH}}_p(Y) \rightarrow \widehat{\text{CH}}_p(X).$$

Provided X is smooth over $\text{Spec } \mathbb{Z}$, arithmetic Chow groups also carry an intersection product.

THEOREM 5.2.2 ([GS90a, Theorem 4.2.3], [GS90a, Theorem 4.5.1]). — Let X be a scheme which is smooth and quasi-projective over $\text{Spec } \mathbb{Z}$. Then for any $p, q \geq 0$, there is a pairing

$$\widehat{\text{CH}}^p(X) \otimes \widehat{\text{CH}}^q(X) \rightarrow \widehat{\text{CH}}^{p+q}(X)$$

equipped with which $\widehat{\text{CH}}^*(X) = \bigoplus_{i=0}^{\dim X} \widehat{\text{CH}}^i(X)$ is a commutative, associative, graded ring.

The ring $\widehat{\text{CH}}^*(X)$ is called the *arithmetic Chow ring* of X . The construction of the arithmetic Chow ring is functorial in the following sense.

THEOREM 5.2.3 (Projection formula, [GS90a, Theorem 4.5.1], [GS90a, Theorem 4.4.3(7)]). — Let X and Y be schemes which are smooth and quasi-projective over $\text{Spec } \mathbb{Z}$. Let $f : Y \rightarrow X$ be a flat morphism. Suppose that the map $Y_{\mathbb{Q}} \rightarrow X_{\mathbb{Q}}$ induced by f on generic fibres is smooth. Then

- (i) There is a ring homomorphism

$$f^* : \widehat{\text{CH}}^*(X) \rightarrow \widehat{\text{CH}}^*(Y)$$

which agrees with the pullback map on the level of arithmetic Chow groups.

- (ii) If f is projective, $\alpha \in \widehat{\text{CH}}^p(X)$, and $\beta \in \widehat{\text{CH}}^q(Y)$ for any $p, q \geq 0$, then

$$f_*(\alpha \cdot f^*\beta) = f_*(\alpha) \cdot \beta.$$

5.2.3 ARITHMETIC CHERN CLASSES

Let X be a regular scheme, flat and quasi-projective over $\text{Spec } \mathbb{Z}$, with regular generic fibre. Let $\mathcal{F}$ be a coherent, locally free sheaf on X , and let $\mathcal{F}_{\mathbb{C}}$ be the corresponding holomorphic vector bundle on $X(\mathbb{C})$. If h is a C^∞ Hermitian scalar product on $\mathcal{F}_{\mathbb{C}}$ invariant under F_∞ , then $\overline{\mathcal{F}} = (\mathcal{F}, h)$ is called an *Hermitian vector bundle*. Hermitian vector bundles admit characteristic classes lying in arithmetic Chow groups. In particular, there is an *arithmetic Chern class*

$$\widehat{c}_p(\overline{\mathcal{F}}) \in \widehat{\text{CH}}^p(X).$$

A construction of these classes can be found in [GS90b, Section 4]. For any $p \geq 0$,

$$z(\widehat{c}_p(\overline{\mathcal{F}})) = c_p(\mathcal{F}) \in \text{CH}^p(X) \quad \text{and} \quad \omega(\widehat{c}_p(\overline{\mathcal{F}})) = c_p(\overline{\mathcal{F}}) \in A^{p,p}(X_{\mathbb{R}}).$$

Arithmetic Chern classes fail to be multiplicative on exact sequences in general, and this failure is measured by the *Bott-Chern secondary characteristic class*.

THEOREM 5.2.4 ([GS90b, Theorem 1.2.2]). — Let X be a scheme which is smooth and quasi-projective over $\operatorname{Spec} \mathbb{Z}$. Let $\overline{\mathcal{F}} : 0 \rightarrow \overline{\mathcal{F}}' \rightarrow \overline{\mathcal{F}} \rightarrow \overline{\mathcal{F}}'' \rightarrow 0$ be an exact sequence of Hermitian vector bundles on X . Then for any $p \geq 0$, the equality

$$\widehat{c}_p(\overline{\mathcal{F}}) = \sum_{r+s=p} \widehat{c}_r(\overline{\mathcal{F}}') \widehat{c}_s(\overline{\mathcal{F}}'') - a(\widetilde{c}_p(\overline{\mathcal{F}}))$$

holds in $\widehat{\operatorname{CH}}^p(X)$, where $\widetilde{c}_p(\overline{\mathcal{F}}) \in \widetilde{A}^{p-1,p-1}(X_{\mathbb{R}})$ is the *Bott-Chern secondary characteristic class* of the exact sequence $\overline{\mathcal{F}}$.

The sum

$$\widehat{c}(\overline{\mathcal{F}}) = \sum_{p \geq 0} \widehat{c}_p(\overline{\mathcal{F}}) \in \widehat{\operatorname{CH}}^*(X)$$

is called the *total arithmetic Chern class* of $\overline{\mathcal{F}}$. Similarly, in the setting of Theorem 5.2.4, the sum

$$\widetilde{c}(\overline{\mathcal{F}}) = \sum_{p \geq 0} \widetilde{c}_p(\overline{\mathcal{F}}) \in \widetilde{A}^{*,*}(X_{\mathbb{R}})$$

is called the *total Bott-Chern secondary characteristic class* of $\overline{\mathcal{F}}$.

As one might hope, the construction of both arithmetic Chern classes and of Bott-Chern classes is functorial.

THEOREM 5.2.5 ([GS90b, Theorem 4.1]). — Let X and Y be schemes which are smooth and quasi-projective over $\operatorname{Spec} \mathbb{Z}$. Let $f : Y \rightarrow X$ be a flat morphism, and suppose that the map $Y_{\mathbb{Q}} \rightarrow X_{\mathbb{Q}}$ induced by f on generic fibres is smooth. Then

- (i) For any Hermitian vector bundle $\overline{\mathcal{F}}$ on X , the equality $f^*\widehat{c}(\overline{\mathcal{F}}) = \widehat{c}(f^*\overline{\mathcal{F}})$ holds in $\operatorname{CH}^*(Y)$.
- (ii) For any exact sequence $\overline{\mathcal{F}} : 0 \rightarrow \overline{\mathcal{F}}' \rightarrow \overline{\mathcal{F}} \rightarrow \overline{\mathcal{F}}'' \rightarrow 0$ of Hermitian vector bundles on X , the equality $f^*\widetilde{c}(\overline{\mathcal{F}}) = \widetilde{c}(f^*\overline{\mathcal{F}})$ holds in $\widetilde{A}^{*,*}(Y_{\mathbb{R}})$.

5.2.4 DEGREE MAPS

Let $S = \operatorname{Spec} \mathbb{Z}$. First, we have $\widehat{\operatorname{CH}}^0(S) = \operatorname{CH}^0(S) = \mathbb{Z}$, and we will call the isomorphism

$$\deg_{\mathbb{Q}} : \widehat{\operatorname{CH}}^0(S) \xrightarrow{\cong} \mathbb{Z}$$

the *degree map*.

The only other nontrivial Chow group of S is $\widehat{\operatorname{CH}}^1(S)$, since S has dimension one. Codimension one cycles on S are formal sums over the closed points of S , and $\mathcal{D}^{0,0}(S_{\mathbb{R}}) = \mathbb{R}$, so

$$\widehat{Z}^1(S) = \left\{ \left(\sum_{p \text{ prime}} n_p(p), \lambda \right) : \lambda \in \mathbb{R}, n_p = 0 \text{ for all but finitely many } p \right\}.$$

On the other hand, the only codimension 0 subvariety of S is S itself, so

$$\widehat{R}^1(S) = \{(\operatorname{div}(f), -2 \log|f|) : f \in \mathbb{Q}^*\}.$$

PRELIMINARIES

The kernel of the surjective map

$$\widehat{Z}^1(S) \rightarrow \mathbb{R}$$

$$\left(\sum_{p \text{ prime}} n_p(p), \lambda \right) \mapsto \sum_{p \text{ prime}} n_p \log p + \frac{\lambda}{2}$$

is precisely $\widehat{R}^1(S)$, yielding an isomorphism

$$\widehat{\deg} : \widehat{\text{CH}}^1(S) \xrightarrow{\cong} \mathbb{R}$$

called the *arithmetic degree map*.

As in [BGS94, 2.1.3], the arithmetic degree of an Hermitian vector bundle $\overline{\mathcal{E}}$ on S is the arithmetic degree of its first arithmetic Chern class:

$$\widehat{\deg}(\overline{\mathcal{E}}) = \widehat{\deg}(\widehat{c}_1(\overline{\mathcal{E}})).$$

5.2.5 THE CYCLE PAIRING

Let $\pi : X \rightarrow S$ be an equidimensional scheme which is smooth and projective over $S = \text{Spec } \mathbb{Z}$. Let $Y \in Z_p(X)$ be a cycle of dimension p on X , and let $x \in \widehat{\text{CH}}^q(X)$. We will define a class $(x | Y) \in \widehat{\text{CH}}^{q-p+1}(X)$. There are a few equivalent definitions of this pairing, all of which can be found in [BGS94, Section 2.3.1]. We will reproduce just one of these definitions here.

First, if $p \notin \{q, q+1\}$, let $(x | Y) = 0$.

Next, if $p = q+1$, let $(x | Y)$ be the intersection number of $z(x)$ and $[Y]$ on the generic fibre of X . That is, choose an arithmetic cycle (Z, g) representing x , and let

$$(x | Y) = [Z] \cdot [Y] \in \widehat{\text{CH}}^0(S) = \text{CH}^0(S) = \mathbb{Z}$$

where $[Z]$ (resp. $[Y]$) is the class of Z in $\text{CH}_p(X)$ (resp. $\text{CH}^q(X)$).

Finally, if $p = q$, then choose a green current g_Y for Y , let $y \in \widehat{\text{CH}}_p(X)$ be the class of the pair (Y, g_Y) , and let

$$(x | Y) = \pi_*(x \cdot y - a(\omega(x)g_Y)) \in \widehat{\text{CH}}^1(S) = \mathbb{R}.$$

THEOREM 5.2.6 ([BGS94, Proposition 2.3.1]). — Let X be an equidimensional scheme which is smooth and projective over $S = \text{Spec } \mathbb{Z}$. Then $x \otimes Y \mapsto (x | Y)$ defines a biadditive pairing

$$\widehat{\text{CH}}^q(X) \otimes Z_p(X) \rightarrow \widehat{\text{CH}}^{q-p+1}(S).$$

Moreover, if X' is an equidimensional scheme which is smooth and projective over S and $f : X' \rightarrow X$ is a morphism, then

(i) For any $x' \in \widehat{\text{CH}}^q(X')$ and $Y \in Z_p(X)$,

$$(f^*(x') | Y) = (x' | f_*(Y)) \in \widehat{\text{CH}}^*(S).$$

(ii) If $f : X \rightarrow X'$ is flat, and the map $X_{\mathbb{Q}} \rightarrow X'_{\mathbb{Q}}$ induced by f on generic fibres is smooth with constant relative dimension, then for any $x \in \widehat{\text{CH}}^q(X)$ and $Y \in Z_p(X)$,

$$(x | f^*(Y)) = (f_*(x) | Y) \in \widehat{\text{CH}}^*(S).$$

5.2.6 HEIGHTS

Let $\mathbb{k}$ be an arbitrary field, let $N \in \mathbb{Z}_{>0}$, and let $Z \in Z_p(\mathbb{P}_{\mathbb{k}}^N)$ be a p -dimensional cycle. Since $\mathbb{P}_{\mathbb{k}}^N$ is smooth and projective, its Chow group carries an intersection product. Accordingly,

$$c_1 \left(\mathcal{O}_{\mathbb{P}_{\mathbb{k}}^N}(1) \right)^p \cdot [Z] \in \text{CH}_0(\mathbb{P}_{\mathbb{k}}^N) = \mathbb{Z}.$$

This integer is called the *degree* of Z . It can be thought of as the number of points of intersection that Z has with p generic hyperplanes. Indeed, multiplying $c_1(\mathcal{O}_{\mathbb{P}_{\mathbb{k}}^N}(1))$ by $[Z]$ corresponds to intersecting Z with a generic hyperplane. This will cut the dimension of Z down by one. Iterating this process $p = \dim(Z)$ times yields a zero-dimensional variety, and the number of points of this variety is the degree of Z .

Now let $S = \text{Spec } \mathbb{Z}$ and $\mathcal{E} = \mathcal{O}_S^{\oplus N+1}$. Then $\mathbb{P}(\mathcal{E}) = \mathbb{P}_{\mathbb{Z}}^N$ is a smooth, projective scheme over S . The pair $(\overline{\mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)}, h_{\text{FS}})$ is an Hermitian vector bundle on $\mathbb{P}(\mathcal{E})$, where h_{FS} is the Fubini-Study Kähler metric (see [GH94a, pg. 31]). Since

$$z \left(\widehat{c}_1 \left(\overline{\mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)} \right) \right) = c_1(\mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)),$$

we can rephrase the discussion of degrees in the language of arithmetic pairings and degree maps on $\mathbb{P}(\mathcal{E})$. Indeed, for any cycle $Z \in Z_{p+1}(\mathbb{P}(\mathcal{E}))$ with generic fibre $Z_{\mathbb{Q}} \in Z_p(\mathbb{P}_{\mathbb{Q}}^N)$,

$$\deg_{\mathbb{Q}} \left(\widehat{c}_1 \left(\overline{\mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)} \right)^p \mid Z \right) = c_1 \left(\mathcal{O}_{\mathbb{P}_{\mathbb{Q}}^N}(1) \right)^p \cdot [Z_{\mathbb{Q}}] = \deg(Z_{\mathbb{Q}})$$

It is natural then, to consider also

$$h_{\overline{\mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)}}(Z) = \widehat{\deg} \left(\widehat{c}_1 \left(\overline{\mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)} \right)^{p+1} \mid Z \right) \in \widehat{\text{CH}}^1(S) = \mathbb{R}.$$

The real number $h_{\overline{\mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)}}(Z)$ is called the *Faltings height* of the cycle Z . Of particular importance to us will be the Faltings height of $\mathbb{P}_{\mathbb{Z}}^N$ itself. For any $p \geq 1$, let

$$\mathcal{H}_p = \sum_{m=1}^p \frac{1}{m}$$

be the p^{th} *Harmonic number*, and let

$$\sigma_p = \frac{1}{2} \sum_{k=1}^p \mathcal{H}_k = \frac{p+1}{2} \mathcal{H}_p - \frac{p}{2}$$

be the p^{th} *Stoll number*.

PROPOSITION 5.2.7 ([BGS94, Lemma 3.3.1]). — The Faltings height of $\mathbb{P}_{\mathbb{Z}}^N$ is

$$h_{\overline{\mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)}}(\mathbb{P}_{\mathbb{Z}}^N) = \sigma_N.$$

Let $\overline{\mathcal{Q}}$ be the tautological quotient bundle on $\mathbb{P}(\mathcal{E})$, equipped with the quotient Hermitian metric induced by the trivial metric on $\pi^*\mathcal{E}$ itself, where $\pi : \mathbb{P}(\mathcal{E}) \rightarrow S$ is the structure morphism for the bundle $\mathbb{P}(\mathcal{E})$. Note that the tautological subbundle $\mathcal{O}_{\mathbb{P}(\mathcal{E})}(-1)$ also carries

PRELIMINARIES

a metric induced by the trivial metric on $\pi^*\mathcal{E}$, and the dual of this metric is precisely the Fubini-Study metric on $\mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)$. For any cycle $Z \in Z_{p+1}(\mathbb{P}(\mathcal{E}))$, we define the *projective height* of Z to be

$$h^{\bar{\mathcal{E}}}(Z) = \widehat{\deg}(\widehat{c}_{p+1}(\bar{\mathcal{Q}}) \mid Z) \in \widehat{\mathrm{CH}}^1(S) = \mathbb{R}.$$

When the bundle $\bar{\mathcal{E}}$ over which we are working is clear from context, we will simply write $h(Z)$ in place of $h^{\bar{\mathcal{E}}}(Z)$.

We will need one final notion of height attached to products of projective spaces. Let $\bar{\mathcal{E}}_1, \dots, \bar{\mathcal{E}}_f$ be Hermitian vector bundles on S , and let, for each $1 \leq i \leq f$, $\bar{\mathcal{Q}}_i$ be the tautological quotient bundle on $\mathbb{P}(\mathcal{E}_i)$, equipped with the quotient Hermitian metric induced by that on $\mathcal{E}_i$. For each $1 \leq i \leq f$, let $N_i = \mathrm{rank}(\mathcal{E}_i) - 1$ be the relative dimension of $\mathbb{P}(\mathcal{E}_i)$ over S . For a divisor D on the product $\prod_{i=1}^f \mathbb{P}(\mathcal{E}_i)$, we will take

$$h(D) = \widehat{\deg}\left(\prod_{i=1}^f \widehat{c}(\bar{\mathcal{Q}}_i) \mid D\right) \in \widehat{\mathrm{CH}}^1(S) = \mathbb{R}$$

and

$$\deg_i(D) = \deg_{\mathbb{Q}}\left(c_{N_i-1}(\mathcal{Q}_i) \prod_{j \neq i} c_{N_j}(\mathcal{Q}_j) \mid D\right) \in \mathbb{Z}.$$

Of particular importance to us will be the case where D is the divisor of a rational section. In this case, the height $h(D)$ has a (relatively) simple expression in terms of the Mahler measure of the section itself.

LEMMA 5.2.8 ([BGS94, Lemma 4.3.4]). — Let $\bar{\mathcal{E}}_1, \dots, \bar{\mathcal{E}}_f$ be Hermitian vector bundles on S , and let, for each $1 \leq i \leq f$, $\bar{\mathcal{L}}_i$ be the pullback of the tautological hermitian subbundle on $\mathbb{P}(\mathcal{E}_i)$ to the product $\prod_{i=1}^f \mathbb{P}(\mathcal{E}_i)$. Let $\mu_i = c_1(\bar{\mathcal{L}}_i)$ and let $N_i = \mathrm{rank}(\mathcal{E}_i) - 1$ be the relative dimension of $\mathbb{P}(\mathcal{E}_i)$ over S . For any f -tuple of integers $(\delta_1, \dots, \delta_f)$ and any nonzero rational section s of $\bigotimes_{i=1}^f \mathcal{L}_i^{\otimes \delta_i}$,

$$h(\mathrm{div}(s)) = \int_{(\prod_{i=1}^f \mathbb{P}(\mathcal{E}_i))(\mathbb{C})} \log|s| \prod_{i=1}^f \mu_i^{N_i} + \frac{1}{2} \sum_{i=1}^f \delta_i \mathcal{H}_{N_i}.$$

5.2.7 ARITHMETIC SCHUBERT CALCULUS

Let $S = \mathrm{Spec} \mathbb{Z}$ and $\mathcal{E} = \mathcal{O}_S^{\oplus N+1}$. Let $\bar{\mathcal{E}}$ be the Hermitian bundle obtained by equipping $\mathcal{E}$ with its trivial Hermitian metric. For any integer $1 \leq k \leq N+1$, the scheme $\mathbb{G}(k, \mathcal{E})$ is smooth and projective over $\mathrm{Spec} \mathbb{Z}$, so by Theorem 5.2.2, the arithmetic Chow groups $\widehat{\mathrm{CH}}(\mathbb{G}(k, \mathcal{E}))$ carry an intersection product. A presentation of the arithmetic Chow ring of $\mathbb{G}(k, \mathcal{E})$ was first given in [Mai95]. A different one was given later in [Tam99]. We recall here the presentation given in [Mai95] which we will need in order to effectively compute heights of certain cycles on $\mathbb{G}(k, \mathcal{E})$.

For integers $0 < p \leq n$, a *p-partition* is a sequence of integers $\lambda = (\lambda_1, \dots, \lambda_p)$ such that $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_p \geq 0$. The *weight* of a p -partition λ is $|\lambda| = \lambda_1 + \dots + \lambda_p$, and its *length* is the maximum index i such that $\lambda_i \neq 0$. Following [Mai95, 5.2], we partition the set of p -partitions into two disjoint subsets. First, the *p-partitions of n* are those p -partitions such that $\lambda_1 \leq n - p$. The collection of all p -partitions of n will be denoted $\mathcal{P}(p, n)$. Its complement, the set of p -partitions such that $\lambda_1 > n - p$, will be denoted by $\mathcal{C}(p, n)$.

Let $\mathcal{E}_\bullet : 0 \subsetneq \mathcal{E}_1 \subsetneq \cdots \subsetneq \mathcal{E}_{N+1} = \mathcal{E}$ be a complete flag of subbundles of $\mathcal{E}$, and let, for each $1 \leq i \leq N+1$, π_i be the structure map for the bundle $\mathcal{E}_i$. To a partition $\lambda \in \mathcal{P}(k, N+1)$ is associated a *Schubert cycle* (relative to $\mathcal{E}_\bullet$)

$$\Sigma_\lambda = \{(\mathfrak{p}, \Lambda) : \dim(\pi_{N+1-k+i-\lambda_i}^{-1}(\mathfrak{p}) \cap \Lambda) \geq i\} \in Z^{|\lambda|}(\mathbb{G}(k, \mathcal{E})).$$

By Kleiman's transversality theorem (see [Kle74, Corollary 8] and [EH16, Theorem 1.7]), since two different complete flags are GL_n -conjugate, the class $[\Sigma_\lambda] \in \mathrm{CH}^{|\lambda|}(\mathbb{G}(k, \mathcal{E}))$ depends only on the partition λ and not on the chosen flag. We will need two easy facts about Schubert cycles.

LEMMA 5.2.9. — Let $S = \mathrm{Spec} \mathbb{Z}$, $\mathcal{E}$ a bundle of rank $N+1$ on S , and $\mathcal{E}_\bullet : 0 \subsetneq \mathcal{E}_1 \subsetneq \cdots \subsetneq \mathcal{E}_{N+1} = \mathcal{E}$ a complete flag of subbundles of $\mathcal{E}$, with structure maps π_i . Then for any $1 \leq k \leq N+1$ and any Schubert cycle Z of dimension k on $\mathbb{G}(k, \mathcal{E})$, there exists $1 \leq r \leq N+1$ such that, as cycles on $\mathbb{P}(\mathcal{E}^\vee)$

$$\{(\mathfrak{p}, \ell) \in \mathbb{P}(\mathcal{E}^\vee) : \text{there exists } (\mathfrak{p}, \Lambda) \in Z \text{ such that } \ell|_\Lambda = 0\} = \mathbb{P}((\mathcal{E}/\mathcal{E}_r)^\vee).$$

Proof. Let λ be the partition corresponding to Z . Let r be the largest index i such that $\lambda_i = N+1-k$. Such r exists, since Z has dimension k . We are left to prove that if the hyperplane in $\pi_{N+1}^{-1}(\mathfrak{p})$ corresponding to some $(\mathfrak{p}, \ell) \in \mathbb{P}(\mathcal{E}^\vee)$ contains the entire fibre $\pi_r^{-1}(\mathfrak{p})$, then it must contain some $\Lambda \in \mathbb{G}(k, \pi_{N+1}^{-1}(\mathfrak{p}))$ such that $(\mathfrak{p}, \Lambda) \in Z$.

Working fibrewise, it suffices to treat $\mathcal{E}$ as a vector space of dimension $N+1$ over some field. Let H be a hyperplane in $\mathcal{E}$ containing $\mathcal{E}_r$. For each $1 \leq i \leq k$, let $a_i = N+1-k+i-\lambda_i$ and let $W_i = H \cap \mathcal{E}_{a_i}$. We will show that $\dim(W_i) \geq i$ for all $1 \leq i \leq k$. This is immediate for $1 \leq i \leq r$, since H contains $\mathcal{E}_r$. For $r+1 \leq i \leq k$, $a_i > i$, so $\dim(W_i) \geq a_i - 1 \geq i$, and we are done. $\square$

Now let $c_1, c_2, \dots$ and $s_1, s_2, \dots$ be sequences of formal variables such that

$$(1 + c_1 t + c_2 t^2 + \cdots)(1 - s_1 t + s_2 t^2 - \cdots) = 1.$$

To a p -partition λ is associated a *Schur polynomial*²

$$\Delta_\lambda(c_1, \dots, c_p) = \det \begin{pmatrix} c_{\lambda_1} & c_{\lambda_1+1} & \cdots & c_{\lambda_1+p-1} \\ c_{\lambda_2-1} & c_{\lambda_2} & \cdots & c_{\lambda_2+p-2} \\ \vdots & \vdots & \ddots & \vdots \\ c_{\lambda_p-p+1} & c_{\lambda_p-p+2} & \cdots & c_{\lambda_p} \end{pmatrix} \in \mathbb{Z}[x_1, \dots, x_p]$$

The product of Schur polynomials associated to two p -partitions λ and μ admits a decomposition

$$\Delta_\lambda(x_1, \dots, x_p) \Delta_\mu(x_1, \dots, x_p) = \sum_{\nu} N_{\lambda, \mu}^{\nu} \Delta_{\nu}(x_1, \dots, x_p)$$

where $N_{\lambda, \mu}^{\nu} \in \mathbb{Z}$ are the *Littlewood-Richardson coefficients*. It turns out that classes of Schubert cycles agree with Schur polynomials in Chern classes of the tautological quotient bundle $\mathcal{Q}$ on $\mathbb{G}(k, \mathcal{E})$. For $\lambda \in \mathcal{P}(k, N+1)$,

$$\Delta_\lambda(c_1(\mathcal{Q}), \dots, c_{N-k+1}(\mathcal{Q})) = [\Sigma_\lambda] \in \mathrm{CH}^{|\lambda|}(\mathbb{G}(k, \mathcal{E})).$$

²Traditionally, the variables c_i are elementary symmetric polynomials and the variables s_i are the complete homogeneous symmetric polynomials, and the definition we give of Schur polynomials here is the second Jacobi-Trudi identity.

PRELIMINARIES

We will therefore use the shorthand notation $c_\lambda(\mathcal{Q}) = \Delta_\lambda(c_1(\mathcal{Q}), \dots, c_{N+1-k}(\mathcal{Q}))$.

We turn now to the arithmetic Schubert calculus of [Mai95]. Let

$$\overline{\mathcal{E}} : 0 \rightarrow \overline{\mathcal{S}} \rightarrow \pi^* \overline{\mathcal{E}} \rightarrow \overline{\mathcal{Q}} \rightarrow 0$$

be the tautological exact sequence on $\mathbb{G}(k, \mathcal{E})$, where all metrics are induced by that on $\mathcal{E}$. By Theorem 5.2.4, we can write

$$\widehat{c}(\overline{\mathcal{Q}}) \widehat{c}(\overline{\mathcal{S}}) = 1 + a(\widetilde{c}(\overline{\mathcal{E}})).$$

Following the notation of [Mai95, 5.2], we write

$$\widehat{c}(\overline{\mathcal{Q}} - \overline{\mathcal{E}}) = \widehat{c}(\overline{\mathcal{Q}}) (1 - a(\widetilde{c}(\overline{\mathcal{E}})))$$

so that $\widehat{c}(\overline{\mathcal{Q}} - \overline{\mathcal{E}}) \widehat{c}(\overline{\mathcal{S}}) = 1$. Crucially, unlike $\widehat{c}_p(\overline{\mathcal{Q}})$ the arithmetic class $\widehat{c}_p(\overline{\mathcal{Q}} - \overline{\mathcal{E}})$ does not necessarily vanish for $p > N - k + 1$. Similarly, defining

$$\widehat{c}_\lambda(\overline{\mathcal{Q}} - \overline{\mathcal{E}}) = \Delta_\lambda(\widehat{c}_1(\overline{\mathcal{Q}} - \overline{\mathcal{E}}), \dots),$$

it follows that $\widehat{c}_\lambda(\overline{\mathcal{Q}} - \overline{\mathcal{E}})$ does not necessarily vanish for $\lambda \in \mathcal{C}(k, N + 1)$. Note, however, that for $\lambda \in \mathcal{C}(k, N + 1)$ (which, in particular, includes $i > N - k + 1$), $z(\widehat{c}(\overline{\mathcal{Q}} - \overline{\mathcal{E}})) = 0$. For p -partitions α, β, λ such that $|\lambda| = |\alpha| + |\beta| - 1$, the *arithmetic Littlewood-Richardson* coefficient is defined, in [Mai95, 5.2], by

$$\widetilde{N}_{\alpha, \beta}^\lambda = \sum_{\substack{\mu \in \mathcal{C}(p, n) \\ |\mu| = |\alpha| + |\beta|}} N_{\alpha, \beta}^\mu \sum_{\substack{r+s+t+1=\mu_1+j \\ r, s, t, j \geq 0 \\ l(\mu)-1 \geq j}} (-1)^{r+j+1} r \mathcal{H}_{r+s} N_{\lambda, \gamma(r, s, t, \mu, j)}^{\delta(r, s, t, \mu)}$$

where

$$\begin{aligned} \delta(r, s, t, \mu) &= (\mu_2 + s + t + 1, \mu_2 + t + 1, (\mu_2 + 1)^r, \mu_2, \mu_3, \dots, \mu_p) \\ \gamma(r, s, t, \mu, j) &= (\mu_2 + t + 1, \mu_2 + 1, (\mu_2)^r, (1)^j). \end{aligned}$$

Here, for integers $u, j \geq 0$, $(u)^j$ is the partition

$$\underbrace{(u, \dots, u)}_j.$$

Finally, we can give the presentation of the arithmetic Chow ring of $\mathbb{G}(k, \mathcal{E})$.

THEOREM 5.2.10 ([Mai95, Théorème 5.2.1]). — For any integer $0 \leq p \leq k(N - k + 1) + 1$ and any $x \in \widehat{\text{CH}}^p(\mathbb{G}(k, \mathcal{E}))$, there exist $k_\lambda \in \mathbb{Z}$ and $f_\lambda \in \mathbb{R}$ such that

$$x = \sum_{\substack{\lambda \in \mathcal{P}(k, N+1) \\ |\lambda|=p}} k_\lambda \widehat{c}_\lambda(\overline{\mathcal{Q}} - \overline{\mathcal{E}}) + \sum_{\substack{\lambda \in \mathcal{P}(k, N+1) \\ |\lambda|=p-1}} a(f_\lambda c_\lambda(\overline{\mathcal{Q}})).$$

Moreover, for any $\lambda, \mu \in \mathcal{P}(k, N + 1)$,

$$\begin{aligned} \widehat{c}_\lambda(\overline{\mathcal{Q}} - \overline{\mathcal{E}}) \cdot \widehat{c}_\mu(\overline{\mathcal{Q}} - \overline{\mathcal{E}}) &= \sum_{\substack{\nu \in \mathcal{P}(k, N+1) \\ |\nu|=|\lambda|+|\mu|}} N_{\lambda, \mu}^\nu \widehat{c}_\nu(\overline{\mathcal{Q}} - \overline{\mathcal{E}}) + \sum_{\substack{\nu \in \mathcal{P}(k, N+1) \\ |\nu|=|\lambda|+|\mu|-1}} a(\widetilde{N}_{\lambda, \mu}^\nu c_\nu(\overline{\mathcal{Q}})), \\ \widehat{c}_\lambda(\overline{\mathcal{Q}} - \overline{\mathcal{E}}) \cdot a(c_\mu(\overline{\mathcal{Q}})) &= \sum_{\substack{\nu \in \mathcal{P}(k, N+1) \\ |\nu|=|\lambda|+|\mu|}} a(N_{\lambda, \mu}^\nu c_\nu(\overline{\mathcal{Q}})), \\ a(c_\lambda(\overline{\mathcal{Q}})) \cdot a(c_\mu(\overline{\mathcal{Q}})) &= 0. \end{aligned}$$

HEIGHTS OF DETERMINANTAL VARIETIES

Our construction of the determinantal resultant is naturally motivated by an intuitive description of its geometry. We begin by giving a short summary of the construction of the determinantal resultant of [Bus04], specialised to our context. Next, using a slightly different perspective, we develop a new incidence correspondence which defines the same resultant, but to which many of the results of [BGS94] can be more readily adapted. Using this new incidence correspondence, we define an object which we call the *determinantal Chow divisor* and give formulas for both its Faltings height and its multidegree. This study culminates in bit size bounds for rational points on determinantal varieties, and mercifully, the end of this thesis.

6.1 THE DETERMINANTAL RESULTANT

6.1.1 BUSÉ'S CONSTRUCTION

Let $S = \operatorname{Spec} \mathbb{Z}$, $\mathcal{E} = \mathcal{O}_S^{\oplus N+1}$ and $X = \mathbb{P}(\mathcal{E}) = \mathbb{P}_{\mathbb{Z}}^N$. Let $e, f, r \in \mathbb{Z}_{>0}$ with $r \leq \min\{e, f\}$, and $d_1, \dots, d_f \in \mathbb{Z}_{>0}$. Put

$$\mathcal{H} = \operatorname{Hom} \left(\mathcal{O}_X^{\oplus e}, \bigoplus_{i=1}^f \mathcal{O}_X(d_i) \right)$$

and let $Y = \mathbb{P}(\mathcal{H})$. For any field $\mathbb{k}$, a point $\phi \in Y(\mathbb{k})$ is represented by an $f \times e$ matrix of homogeneous polynomials in $N + 1$ variables with coefficients in $\mathbb{k}$, the i^{th} row of which consists of polynomials of degree d_i . It follows that

$$Y(\mathbb{k}) \cong \prod_{i=1}^f \mathbb{P}_{\mathbb{k}}^{e \binom{N+d_i}{d_i} - 1}.$$

We endow $Y(\mathbb{k})$ with multihomogeneous coordinates given by the coefficients of the polynomials in the matrices representing its points.

The scheme $X \times_S Y$ contains an incidence correspondence W whose $\mathbb{k}$ -points are pairs (x, ϕ) such that $\operatorname{rank}(\tilde{\phi}(\tilde{x})) \leq r$ for any representatives $\tilde{\phi} \in \mathcal{H}(\mathbb{k})$ and $\tilde{x} \in \mathbb{A}_{\mathbb{k}}^{N+1}$ of ϕ and x respectively.

Consider the diagram

$$\begin{array}{ccc} & W & \\ \pi_1 \swarrow & & \searrow \pi_2 \\ X & & Y \end{array}$$

Since π_1 is flat and π_2 is proper, the cycle $\pi_{2*}\pi_1^*[X]$ in Y is well-defined. According to [Bus04, Theorem 1], when $N = (e - r)(f - r) - 1$, the cycle $\pi_{2*}\pi_1^*[X]$ is supported on a single irreducible hypersurface ∇ in Y , called the *resultant variety*. It is therefore the divisor of a multihomogeneous polynomial with integer coefficients which vanishes precisely on the locus of points in Y which are represented by morphisms in $\mathcal{H}$ which have a nonempty r^{th} degeneracy

HEIGHTS OF DETERMINANTAL VARIETIES

locus. In [Bus04], this polynomial is called the *determinantal resultant*¹. We will denote this polynomial by $\text{Res}_{e,f,r,(d_1,\dots,d_f)}$.

REMARK 6.1.1. — The determinantal resultant of [Bus04] is defined in a far more general context. The projective space X is replaced by an arbitrary irreducible projective variety X and the bundles $\bigoplus_{i=1}^f \mathcal{O}_X(d_i)$ and $\mathcal{O}_X^{\oplus e}$ are replaced by arbitrary vector bundles of ranks f and e respectively. In this setting, [Bus04, Theorem I] establishes sufficient conditions on X and the chosen bundles for the determinantal resultant to be irreducible of codimension one.

6.1.2 A DIFFERENT PERSPECTIVE

Let $S, X, \mathcal{E}, e, f, r$, and $d_1, \dots, d_f$ be as in Section 6.1.1. Let $\mathcal{E}^\vee$ be the dual bundle of $\mathcal{E}$ and for each $1 \leq i \leq f$, let

$$\mathbb{P}_i = \mathbb{P}((\text{Sym}^{d_i} \mathcal{E}^\vee)^\vee) \quad \text{and} \quad \check{\mathbb{P}}_i = \mathbb{P}((\text{Sym}^{d_i} \mathcal{E}^\vee)^{\oplus e})$$

and let

$$\mathbb{G}_i = \mathbb{G}(e - r, \mathcal{O}_S^{\oplus e} \otimes_{\mathcal{O}_S} (\text{Sym}^{d_i} \mathcal{E}^\vee)^\vee).$$

The scheme $\mathbb{G}_i \times_S \check{\mathbb{P}}_i$ contains an incidence correspondence $\mathcal{W}_i$ defined fibrewise by pairs of $(e - r)$ -planes and one-dimensional subspaces of functionals annihilating them.

Let $\Gamma = \mathcal{W}_1 \times_S \cdots \times_S \mathcal{W}_f$ and

$$p : \Gamma \rightarrow \prod_{i=1}^f \mathbb{G}_i$$

and

$$q : \Gamma \rightarrow \prod_{i=1}^f \check{\mathbb{P}}_i$$

be the projection maps.

For each $1 \leq i \leq f$, let

$$s_i : \mathbb{P}_i \times_S \mathbb{G}(e - r, \mathcal{O}_S^{\oplus e}) \rightarrow \mathbb{G}_i$$

be the Segre embedding and,

$$\nu_i : X \rightarrow \mathbb{P}((\text{Sym}^{d_i} \mathcal{E}^\vee)^\vee) = \mathbb{P}_i.$$

be the Veronese embedding of degree d_i . Let $\nu : X \rightarrow \prod_{i=1}^f \mathbb{P}_i$ be the product of the ν_i , and $s = s_1 \times_S \cdots \times_S s_f$ the product of the s_i .

Consider the diagram

$$\begin{array}{ccccc} & & \Gamma & & \\ & \swarrow p & & \searrow q & \\ X \times_S \mathbb{G}(e - r, \mathcal{O}_S^{\oplus e}) & \xrightarrow{\nu \times id} & \prod_{i=1}^f \mathbb{P}_i \times_S \mathbb{G}(e - r, \mathcal{O}_S^{\oplus e}) & \xrightarrow{s} & \prod_{i=1}^f \mathbb{G}_i & \quad \prod_{i=1}^f \check{\mathbb{P}}_i \end{array}$$

¹Of course, this resultant is defined only up to multiplication by an element of $\mathbb{Z}$. However, we can always choose a generator for the (principal) ideal defining ∇ whose coefficients are pairwise coprime.

Since s and ν are closed immersions, they are proper. Thus, we can consider, for any cycle $Z \in Z(X)$, the cycle $q_* p^* s_* (\nu \times id)_* (Z \times_S \mathbb{G}(e - r, \mathcal{O}_S^{\oplus e}))$ in $\prod_{i=1}^f \tilde{\mathbb{P}}_i$.

For $Z \in Z_{(f-r)(e-r)}(X)$, we denote

$$\text{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(Z) = q_* p^* s_* (\nu \times id)_* (Z \times_S \mathbb{G}(e - r, \mathcal{O}_S^{\oplus e})).$$

THEOREM 6.1.2. — Suppose $Z \in Z_{(f-r)(e-r)}(X)$ is flat and irreducible. Then there is an equality

$$\text{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(Z) = \pi_{2*} \pi_1^*(Z)$$

of cycles in Y .

This theorem essentially follows from a diagram chase. We defer this argument to after Section 6.1.3, where we perform such a diagram chase for some specific parameters. Note that Theorem 6.1.2 implies, in particular, that if $N = (f - r)(e - r) - 1$, then

$$\text{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(X) = \text{div}(\text{Res}_{e,f,r,(d_1,\dots,d_f)}).$$

PROPOSITION 6.1.3. — Suppose $Z \in Z_{(f-r)(e-r)}(X)$ is flat and irreducible. Then the support of the cycle $\text{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(Z)$ is an irreducible hypersurface in Y .

Proof. For each $1 \leq i \leq f$, let $\mathcal{F}_i = \mathcal{O}_S^{\oplus e} \otimes_{\mathcal{O}_S} (\text{Sym}^{d_i} \mathcal{E}^\vee)^\vee$, so that $\tilde{\mathbb{P}}_i = \mathbb{P}(\mathcal{F}_i^\vee)$. Then W_i , as a fibre bundle on $\tilde{\mathbb{P}}_i$, is isomorphic to $\mathbb{G}(e - r, \mathcal{Q}_{\mathcal{F}_i^\vee}^\vee)$.

Indeed, the fibre of $\mathcal{W}_i$ over a point (p, ℓ) of $\tilde{\mathbb{P}}_i$ is the subscheme of $\mathbb{G}_i$ consisting of those pairs (p, V) such that $V \subseteq (\mathcal{F}_i)_p \otimes_{\mathcal{O}_{X,p}} \kappa(p)$ contains the hyperplane ℓ .

On the other hand, the fibre over (p, ℓ) of $\mathbb{G}(e - r, \mathcal{Q}_{\mathcal{F}_i^\vee}^\vee)$ consists of those pairs (p, W) where

$$W \subseteq \left(\frac{((\mathcal{F}_i)_p \otimes_{\mathcal{O}_{X,p}} \kappa(p))^\vee}{\ell} \right)^\vee$$

is an $(e - r)$ -dimensional subspace.

Each map $\mathcal{W}_i \rightarrow \tilde{\mathbb{P}}_i$ is therefore flat with irreducible fibres, so the scheme Γ is itself irreducible and has rank $(e - r) \left(\sum_{i=1}^f \left(e \binom{N+d_i}{d_i} - e + r - 1 \right) \right)$ as a bundle on $\tilde{\mathbb{P}}_i$. The dimension of $\mathbb{G}_i$ is $(e - r) \left(e \binom{N+d_i}{d_i} - e + r \right) + 1$, so we are done. $\square$

PROPOSITION 6.1.4. — Suppose $Z \in Z_{(f-r)(e-r)}(X)$ is flat and irreducible. Then the cycle $\text{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(Z)$ is irreducible.

Proof. Note that Proposition 6.1.3 shows that the support of this cycle is an irreducible subscheme of $\prod_{i=1}^f \tilde{\mathbb{P}}_i$, so we only need to prove that the map $p^{-1}(s((\nu \times id)(X \times_S \mathbb{G}(e - r, \mathcal{O}_S^{\oplus e})))) \xrightarrow{q} \prod_{i=1}^f \tilde{\mathbb{P}}_i$ is generically injective.

The proof of [BGS94, Lemma 4.3.1] goes through verbatim, with the scheme $\mathbb{P}_i$ replaced by $\mathbb{G}_i$. See also [Bus04, Theorem 1] for an alternative proof of this fact. $\square$

REMARK 6.1.5. — Suppose $e = 1, r = 0$ and take $N = f - 1$. According to Proposition 6.1.4, the cycle $\text{Ch}_{1,f,0,(d_1,\dots,d_f)}^{\det}(\mathbb{P}^N)$ is a principal divisor. Indeed, it is simply the divisor of the usual multivariate (Macaulay) resultant of f homogeneous polynomials of degrees $d_1, \dots, d_f$ in f variables. If we further specialise to $f = 2$, we recover $\text{Ch}_{1,2,0,(d_1,d_2)}^{\det}(\mathbb{P}^1)$ as the Sylvester resultant of two homogeneous polynomials of degrees d_1, d_2 in two variables.

Note that the Grassmann bundle $\mathbb{G}(1, \mathcal{O}_S)$ is simply S itself, in the diagram defining $\text{Ch}_{1,f,0,(d_1,\dots,d_f)}^{\det}(Z)$, the product $Z \times_S \mathbb{G}(1, \mathcal{O}_S) = Z$, the product $\mathbb{P}_i \times_S \mathbb{G}(1, \mathcal{O}_S) = \mathbb{P}_i$, and the Segre embedding s is simply the identity map. It follows that for any N , if $Z \in Z_f(\mathbb{P}^N)^2$, the cycle $\text{Ch}_{1,f,0,(d_1,\dots,d_f)}^{\det}(Z)$ is simply the generalised Chow divisor of Z (see [BGS94, Section 4.3]). In particular, $\text{Ch}_{1,f,0,(1,\dots,1)}^{\det}(Z)$ is the divisor of the usual Chow form of Z (see [CvdW37]).

For arbitrary parameters $e, f, r, (d_1, \dots, d_f)$, it would be nice to have a geometric description of the divisor $\text{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(Z)$.

6.1.3 AN EXAMPLE

Let $f = 4, e = 3, r = 1$. Let $d_1 = d_2 = d_3 = 1$ and $d_4 = 2$. According to Proposition 6.1.4, if we take $N = 5$, the resultant $\text{Res}_{3,4,1,(1,1,1,2)} = \text{Ch}_{3,4,1,(1,1,1,2)}^{\det}(\mathbb{P}^5)$ will be an irreducible hypersurface in $\check{\mathbb{P}}^{17} \times \check{\mathbb{P}}^{17} \times \check{\mathbb{P}}^{17} \times \check{\mathbb{P}}^{3\binom{7}{2}-1}$. Give $\mathbb{P}^5$ homogeneous coordinates $X_0, \dots, X_5$. Endow the first (resp. second, third) copy of $\check{\mathbb{P}}^{17}$ with homogeneous coordinates $\mathbf{a}_{X_0}^{(1)}, \dots, \mathbf{a}_{X_5}^{(1)}, \mathbf{a}_{X_0}^{(2)}, \dots, \mathbf{a}_{X_5}^{(2)}, \mathbf{a}_{X_0}^{(3)}, \dots, \mathbf{a}_{X_5}^{(3)}$ (resp. $\mathbf{b}_{X_0}^{(1)}, \dots, \mathbf{b}_{X_5}^{(3)}, \mathbf{c}_{X_0}^{(1)}, \dots, \mathbf{c}_{X_5}^{(3)}$). Similarly, give $\mathbb{P}^{3\binom{7}{2}-1}$ homogeneous coordinates $\mathbf{u}_{\tau}^{(i)}$ where τ ranges over all monomials of degree 2 in $X_0, \dots, X_5$ and $1 \leq i \leq 3$. Consider the matrix

$$\begin{pmatrix} \mathbf{a}_{X_0}^{(1)}X_0 + \dots + \mathbf{a}_{X_5}^{(1)}X_5 & \mathbf{a}_{X_0}^{(2)}X_0 + \dots + \mathbf{a}_{X_5}^{(2)}X_5 & \mathbf{a}_{X_0}^{(3)}X_0 + \dots + \mathbf{a}_{X_5}^{(3)}X_5 \\ \mathbf{b}_{X_0}^{(1)}X_0 + \dots + \mathbf{b}_{X_5}^{(1)}X_5 & \mathbf{b}_{X_0}^{(2)}X_0 + \dots + \mathbf{b}_{X_5}^{(2)}X_5 & \mathbf{b}_{X_0}^{(3)}X_0 + \dots + \mathbf{b}_{X_5}^{(3)}X_5 \\ \mathbf{c}_{X_0}^{(1)}X_0 + \dots + \mathbf{c}_{X_5}^{(1)}X_5 & \mathbf{c}_{X_0}^{(2)}X_0 + \dots + \mathbf{c}_{X_5}^{(2)}X_5 & \mathbf{c}_{X_0}^{(3)}X_0 + \dots + \mathbf{c}_{X_5}^{(3)}X_5 \\ \mathbf{u}_{X_0^2}^{(1)}X_0^2 + \dots + \mathbf{u}_{X_5^2}^{(1)}X_5^2 & \mathbf{u}_{X_0^2}^{(2)}X_0^2 + \dots + \mathbf{u}_{X_5^2}^{(2)}X_5^2 & \mathbf{u}_{X_0^2}^{(3)}X_0^2 + \dots + \mathbf{u}_{X_5^2}^{(3)}X_5^2 \end{pmatrix}. \quad (6.1)$$

For a field $\mathbb{k}$, choosing a $\mathbb{k}$ -point of $\check{\mathbb{P}}^{17} \times \check{\mathbb{P}}^{17} \times \check{\mathbb{P}}^{17} \times \check{\mathbb{P}}^{3\binom{7}{2}-1}$ is the same as choosing a specialisation of the coefficients of (6.1) in $\mathbb{k}$. For a general such choice, the quotient of $\mathbb{k}[X_0, X_1, X_2, X_3, X_4, X_5]$ by the ideal of 2×2 minors of the corresponding matrix has Krull dimension zero by [BV88, Proposition 1.1], so its projective variety is empty (see also [FSS13, Theorem 10]).

The cycle $\text{Ch}_{3,4,1,(1,1,1,2)}^{\det}(\mathbb{P}^5) \times_{\mathbb{Z}} \text{Spec } \mathbb{k}$ is the divisor of a polynomial in $\mathbf{a}_{\tau}^{(i)}, \mathbf{b}_{\tau}^{(i)}, \mathbf{c}_{\tau}^{(i)}, \mathbf{u}_{\tau}^{(i)}$, homogeneous with respect to each block of variables, which vanishes precisely on those choices of coefficients such that the projective variety defined by the 2×2 minors of the corresponding matrix of polynomials over $\mathbb{k}$ is nonempty.

To see this, we chase through the diagram defining the determinantal resultant. In what follows, we will denote by $\mathbb{G}(k, n)$ the Grassmann bundle $\mathbb{G}(k, \mathcal{O}_S^{\oplus n})$. A $\mathbb{k}$ -point of $\mathbb{G}(k, n)$ can be represented by a $k \times n$ matrix of full rank k , whose rows generate the corresponding k -dimensional subspace of $\mathbb{k}^n$.

First, we have

$$id \times_S id \times_S id \times_S \nu_2 : \mathbb{P}^5 \times_S \mathbb{G}(2, 3) \rightarrow (\mathbb{P}^5 \times_S \mathbb{G}(2, 3))^{\times_{S^3}} \times_S (\mathbb{P}^{\binom{7}{2}-1} \times_S \mathbb{G}(2, 3)).$$

²Recall that we work over $\text{Spec } \mathbb{Z}$, which has dimension one, so the generic fibre $Z_{\mathbb{Q}}$ will have dimension $f - 1$. In particular, $\mathbb{P}_{\mathbb{Z}}^N$ has dimension $N + 1$.

A $\mathbb{k}$ -point of $\mathbb{P}^5 \times_S \mathbb{G}(2, 3)$ is simply a pair $([v_0 : v_1 : v_2 : v_3 : v_4 : v_5], W)$ where $[v_0 : \dots : v_5] \in \mathbb{P}_{\mathbb{k}}^5$ and

$$W = \begin{pmatrix} w_{11} & w_{12} & w_{13} \\ w_{21} & w_{22} & w_{23} \end{pmatrix}.$$

is a full rank 2×3 matrix with entries in $\mathbb{k}$. The image of such a point under this map is a 4-tuple whose first three coordinates are just the point $([v_0 : \dots : v_5], W)$ again, and whose last coordinate is $([v_0^2 : v_0 v_1 : \dots : v_5^2], W)$.

The Segre embedding

$$s_1 = s_2 = s_3 : \mathbb{P}^5 \times_S \mathbb{G}(2, 3) \rightarrow \mathbb{G}(2, 18).$$

sends the point $([v_0 : \dots : v_5], W)$ to the 2-plane represented by the 2×18 matrix

$$W' = \begin{pmatrix} v_0 w_{11} & v_1 w_{11} & \dots & v_5 w_{11} & \dots & v_0 w_{13} & \dots & v_5 w_{13} \\ v_0 w_{21} & v_1 w_{21} & \dots & v_5 w_{21} & \dots & v_0 w_{23} & \dots & v_5 w_{23} \end{pmatrix}. \quad (6.2)$$

Without loss of generality, let us suppose that the maximal minor of W defined by its first two columns does not vanish, and that $v_0 \neq 0$. Then the determinant of the submatrix of (6.2) defined by the columns $(v_0 w_{11} \ v_0 w_{21})^T$ and $(v_0 w_{12} \ v_0 w_{22})^T$ does not vanish, so (6.2) does indeed represent a point of $\mathbb{G}(2, 18)$.

Similarly, the Segre embedding

$$s_4 : \mathbb{P}^{\binom{7}{2}-1} \times_S \mathbb{G}(2, 3) \rightarrow \mathbb{G}\left(2, 3 \binom{7}{2}\right)$$

restricted to the image of ν_2 sends the point $([v_0^2 : v_0 v_1 : \dots : v_5^2], W)$ to the 2-plane represented by

$$W'' = \begin{pmatrix} v_0^2 w_{11} & v_0 v_1 w_{11} & \dots & v_5^2 w_{11} & \dots & v_0^2 w_{13} & \dots & v_5^2 w_{13} \\ v_0^2 w_{21} & v_0 v_1 w_{21} & \dots & v_5^2 w_{21} & \dots & v_0^2 w_{23} & \dots & v_5^2 w_{23} \end{pmatrix}$$

which indeed represents a point of $\mathbb{G}\left(2, 3 \binom{7}{2}\right)$ by the same argument as for $s_1 = s_2 = s_3$.

Consider a point $w \in (\check{\mathbb{P}}_{\mathbb{k}}^{17})^3 \times \check{\mathbb{P}}_{\mathbb{k}}^{3 \binom{7}{2}-1}$

$$w = \left(\left[a_{X_0}^{(1)} : \dots : a_{X_5}^{(3)} \right], \left[b_{X_0}^{(1)} : \dots : b_{X_5}^{(3)} \right], \left[c_{X_0}^{(1)} : \dots : c_{X_5}^{(3)} \right], \left[u_{X_0^2}^{(1)} : \dots : u_{X_5^2}^{(3)} \right] \right).$$

The pair $\left(W', \left[a_{X_0}^{(1)} : \dots : a_{X_5}^{(3)} \right] \right)$ belongs to the incidence correspondence $\mathcal{W}_1$ if and only if both

$$a_{X_0}^{(1)} v_0 w_{11} + \dots + a_{X_5}^{(1)} v_5 w_{11} + a_{X_0}^{(2)} v_0 w_{12} + \dots + a_{X_5}^{(2)} v_5 w_{12} + a_{X_0}^{(3)} v_0 w_{13} + \dots + a_{X_5}^{(3)} v_5 w_{13} = 0$$

and

$$a_{X_0}^{(1)} v_0 w_{21} + \dots + a_{X_5}^{(1)} v_5 w_{21} + a_{X_0}^{(2)} v_0 w_{22} + \dots + a_{X_5}^{(2)} v_5 w_{22} + a_{X_0}^{(3)} v_0 w_{23} + \dots + a_{X_5}^{(3)} v_5 w_{23} = 0.$$

Analogous statements hold for $\left(W', \left[b_{X_0}^{(1)} : \dots : b_{X_5}^{(3)} \right] \right)$ and $\left(W', \left[c_{X_0}^{(1)} : \dots : c_{X_5}^{(3)} \right] \right)$.

Similarly, $\left(W'', \left[u_{X_0^2}^{(1)} : \dots : u_{X_5^2}^{(3)} \right] \right) \in \mathcal{W}_4$ if and only if

$$u_{X_0^2}^{(1)} v_0^2 w_{11} + \dots + u_{X_5^2}^{(1)} v_5^2 w_{11} = 0$$

and

$$u_{X_0^2}^{(1)} v_0^2 w_{21} + \cdots + u_{X_5^2}^{(5)} v_5^2 w_{23} = 0.$$

It follows that $(W', W', W', W'', w) \in \Gamma$ if and only if W^T is in the right kernel of the matrix (6.1) specialised at the point w , then evaluated at $[v_0 : \cdots : v_5]$. But of course, if this is the case, then this matrix has a right kernel of dimension at least 2, and therefore its rank cannot exceed 1.

6.1.4 THE PROOF OF THEOREM 6.1.2

By [Bus04, Theorem 1], the cycle $\pi_{2*}\pi_1^*(Z)$ is $[\nabla]$, where ∇ is an irreducible hypersurface in $\prod_{i=1}^f \check{\mathbb{P}}_i$. On the other hand, Proposition 6.1.4 combined with Proposition 6.1.3 shows that the cycle $\text{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(Z)$ is $[\nabla']$, where ∇' is the principal Weil divisor associated to some multihomogeneous polynomial on $\prod_{i=1}^f \check{\mathbb{P}}_i$. It suffices, therefore, to prove that for a point $y \in \prod_{i=1}^f \check{\mathbb{P}}_i$, the intersection $q^{-1}(y) \cap p^{-1}(s((\nu \times id)(Z \times_S \mathbb{G}(e-r, \mathcal{O}_S^{\oplus e}))))$ is nonempty if and only if the intersection $\pi_2^{-1}(y) \cap \pi_1^{-1}(Z)$ is.

First, by the discussion in Section 5.1.4 and [GD60, Proposition 3.4.7], a point of $Z \times_S \mathbb{G}(e-r, \mathcal{O}_S^{\oplus e})$ can be represented by a tuple $(\ell, \Lambda, \mathbf{p})$, where $\mathbf{p} \in S$, $\ell \subseteq \kappa(\mathbf{p})^{N+1}$ is a one-dimensional subspace, and $\Lambda \subseteq \kappa(\mathbf{p})^e$ is an $(e-r)$ -dimensional subspace. Subsequently,

$$s(\nu \times id)((\ell, \Lambda, \mathbf{p})) = \left(\prod_{i=1}^f \ell^{\otimes d_i} \otimes \Lambda, \mathbf{p} \right).$$

As a sanity check, note that $\ell^{\otimes d_i} \otimes \Lambda$ is indeed an $(e-r)$ -dimensional subspace of $\kappa(\mathbf{p})^e \otimes \text{Sym}^{d_i}(\kappa(\mathbf{p})^{N+1}) \cong \kappa(\mathbf{p})^{e(N+d_i)}$.

Again, by the discussion in Section 5.1.4 and [GD60, Proposition 3.4.7], we can represent y as a tuple $(U_1, \dots, U_f, \mathbf{p})$, where $U_i \subseteq \text{Sym}^{d_i}(\kappa(\mathbf{p})^{N+1})^{\oplus e}$ is a codimension one linear subspace. By definition of the incidence correspondence Γ , a tuple

$$\left(\prod_{i=1}^f \ell^{\otimes d_i} \otimes \Lambda, (U_1, \dots, U_f), \mathbf{p} \right) \in q^{-1}(y) \cap p^{-1}(s((\nu \times id)(Z \times_S \mathbb{G}(e-r, \mathcal{O}_S^{\oplus e}))))$$

if and only if $\ell^{\otimes d_i} \otimes \Lambda \subseteq U_i$ for each $1 \leq i \leq f$.

Turning our attention to the incidence correspondence W , the point y can be represented by a pair $([\phi], \mathbf{p})$, where $[\phi] \in \mathbb{P}\left(\text{Hom}\left(\kappa(\mathbf{p})^e, \bigoplus_{i=1}^f \text{Sym}^{d_i}(\kappa(\mathbf{p})^{N+1})\right)\right)$ is the class of a linear map $\phi \in \text{Hom}\left(\kappa(\mathbf{p})^e, \bigoplus_{i=1}^f \text{Sym}^{d_i}(\kappa(\mathbf{p})^{N+1})\right)$. By tensor-hom adjunction,

$$\text{Hom}\left(\kappa(\mathbf{p})^e, \bigoplus_{i=1}^f \text{Sym}^{d_i}(\kappa(\mathbf{p})^{N+1})\right) \cong \bigoplus_{i=1}^f \left(\text{Sym}^{d_i}(\kappa(\mathbf{p})^{N+1})^{\oplus e}\right)^\vee.$$

This isomorphism amounts to choosing bases and representing ϕ as a matrix M_ϕ .

Under the induced isomorphism on projective spaces, the point $[\phi]$ gets sent to the tuple $(U_1, \dots, U_f)$ where U_i is the codimension one linear subspace of $\text{Sym}^{d_i}(\kappa(\mathbf{p})^{N+1})^{\oplus e}$ spanned by the i^{th} row of M_ϕ .

The tuple

$$([\phi], \ell, \mathbf{p}) \in \pi_2^{-1}(y) \cap \pi_1^{-1}(Z)$$

if and only if $\text{rank}(\phi(x)) \leq r$, where x is any point in $\mathbb{A}_{\kappa(\mathfrak{p})}^{N+1}$ representing $\ell \in \mathbb{P}_{\kappa(\mathfrak{p})}^N$. Now $\text{rank}(\phi(x)) \leq r$ if and only if $\dim \ker(\phi(x)) \geq e - r$, which in turn happens if and only if there is an $(e - r)$ -dimensional subspace $\Lambda \subseteq \kappa(\mathfrak{p})^e$ contained in the kernel of $\phi(x)$. Applying the tensor-hom adjunction isomorphism once more, we see that $\text{rank}(\phi(x)) \leq r$ if and only if $\ell^{\otimes d_i} \otimes \Lambda \subseteq U_i$ for each $1 \leq i \leq f$.

6.1.5 THE DETERMINANTAL u -RESULTANT

In this section, we will work over an arbitrary field $\mathbb{k}$. Let $e, f, r, d_1, \dots, d_f \in \mathbb{Z}_{>0}$ with $0 \leq r \leq \min\{e, f\}$. Let $N = (f - r)(e - r)$ and give $\mathbb{P}_{\mathbb{k}}^N$ homogeneous coordinates $[X_0 : \dots : X_N]$. For each $0 \leq j \leq N$, let $\mathbb{k}_j(u) = \text{Frac}(\mathbb{k}[u_0, \dots, u_{j-1}, u_{j+1}, \dots, u_N])$, and $F_j = u_0 X_0 + \dots + u_{j-1} X_{j-1} + X_j + u_{j+1} X_{j+1} + \dots + u_N X_N$.

A morphism $\phi \in \text{Hom}\left(\mathcal{O}_{\mathbb{P}_{\mathbb{k}}^N}^{\oplus e}, \bigoplus_{i=1}^f \mathcal{O}_{\mathbb{P}_{\mathbb{k}}^N}(d_i)\right)$ can be represented by an $f \times e$ matrix, the i, j entry of which is a homogeneous polynomial of degree d_i in $X_0, \dots, X_N$ with coefficients in $\mathbb{k}$. For each such morphism, we define, for each $1 \leq j \leq N$, $\phi^{(j)} \in \text{Hom}\left(\mathcal{O}_{\mathbb{P}_{\mathbb{k}_j(u)}^N}^{\oplus e}, \bigoplus_{i=1}^f \mathcal{O}_{\mathbb{P}_{\mathbb{k}_j(u)}^N}(d_i)\right)$ coordinatewise by

$$\phi_{\ell, k}^{(j)} = \phi_{\ell, k}(X_0, \dots, X_{j-1}, -F_j(X_0, \dots, X_{j-1}, 0, X_{j+1}, \dots, X_N), X_{j+1}, \dots, X_N)$$

for each $1 \leq \ell \leq f$ and $1 \leq k \leq e$.

THEOREM 6.1.6. — Let $\phi \in \text{Hom}\left(\mathcal{O}_{\mathbb{P}_{\mathbb{k}}^N}^{\oplus e}, \bigoplus_{i=1}^f \mathcal{O}_{\mathbb{P}_{\mathbb{k}}^N}(d_i)\right)$ and suppose that for any $0 \leq j \leq N$, the degeneracy locus $M_r(\phi^{(j)})$ is reduced and of dimension zero. Then for each $0 \leq j \leq N$, there exists a nonzero constant C_j such that

$$\text{Res}_{e, f, r, (d_1, \dots, d_f)}(\phi^{(j)}) = C_j \prod_{p \in M_r(\phi) \cap D_+(X_j)} F_j(p).$$

Proof. For ease of exposition, for each $0 \leq j \leq N$, let

$$\mathbb{P}^{(j)} = \text{Proj}(\mathbb{k}[u_0, \dots, u_{j-1}, u_{j+1}, \dots, u_N]).$$

By Theorem 6.1.2,

$$V(\text{Res}_{e, f, r, (d_1, \dots, d_f)}(\phi^{(j)})) = \{v \in \mathbb{P}^{(j)} : M_r(\phi^{(j)}(v)) \neq \emptyset\}.$$

On the other hand,

$$V\left(\prod_{p \in M_r(\phi) \cap D_+(X_j)} F_j(p)\right) = \bigcup_{p \in M_r(\phi) \cap D_+(X_j)} V(F_j(p)).$$

Since

$$V(F_j(p)) = \{v \in \mathbb{P}^{(j)} : v_0 p_0 + \dots + v_{j-1} p_{j-1} + v_{j+1} p_{j+1} + \dots + v_N p_N = -p_j\}$$

we can write this latter union as

$$\begin{aligned} \bigcup_{p \in M_r(\phi) \cap D_+(X_j)} V(F_j(p)) &= \left\{v \in \mathbb{P}^{(j)} : \begin{array}{l} \exists p \in M_r(\phi) \cap D_+(X_j), \\ v_0 p_0 + \dots + v_N p_N = -p_j \end{array}\right\} \\ &= \{v \in \mathbb{P}^{(j)} : M_r(\phi^{(j)}(v)) \neq \emptyset\}. \end{aligned}$$

As $M_r(\phi)$ is reduced, we are done. $\square$

HEIGHTS OF DETERMINANTAL VARIETIES

REMARK 6.1.7. — As in the case of the standard u -resultant, the determinantal u -resultant which we define here can be used to solve zero-dimensional determinantal polynomial systems. This requires the explicit computation of a polynomial defining the determinantal resultant, or at least a way to evaluate such a polynomial. It would be interesting and worthwhile to ascertain if such a polynomial or black box could be extracted from our construction of the determinantal resultant in Section 6.1.2, as is done in [Bus04].

As an immediate corollary of Theorem 6.1.6, we can compute a polynomial defining the Chow divisor of a zero-dimensional determinantal variety.

COROLLARY 6.1.8. — Let $\phi \in \text{Hom} \left(\mathcal{O}_{\mathbb{P}_{\mathbb{k}}^N}^{\oplus e}, \bigoplus_{i=1}^f \mathcal{O}_{\mathbb{P}_{\mathbb{k}}^N}(d_i) \right)$ and suppose that the degeneracy locus $M_r(\phi)$ is reduced and of dimension zero. Suppose, moreover, that $M_r(\phi) \subseteq D_+(X_j)$ for some $0 \leq j \leq N$. Then, as cycles on $\tilde{\mathbb{P}}_{\mathbb{k}}^N$,

$$\text{Ch}_{(1, \dots, 1)}(M_r(\phi)) = \text{div} \left(\text{Res}_{e, f, r, (d_1, \dots, d_f)}(\phi^{(j)}) \right).$$

6.2 PRINCIPAL DETERMINANTAL RESULTANTS

Of particular interest in the context of polynomial optimisation is the case when $r = \min\{e, f\} - 1$. The corresponding resultant $\text{Res}_{e, f, r, (d_1, \dots, d_f)}$ is called, in [Bus04], the *principal determinantal resultant*. In this section, we give explicit degree and height formulæ for principal determinantal resultants in the case that $e \leq f$. Throughout this section, we will suppose that $e \leq f$ and $r = e - 1$.

6.2.1 PULLING BACK THE QUOTIENT BUNDLE

The key computation that enables us to compute degrees and heights is the pullback of the tautological quotient bundle on some $\tilde{\mathbb{P}}_i$ through the incidence correspondence $\mathcal{W}_i$.

Under our assumptions on the parameters e, f , and r , we have $e - r = 1$, and the Grassmannian $\mathbb{G}(e - r, \mathcal{O}_S^{\oplus e})$ is simply $\mathbb{P}^{e-1}$. In this situation, the incidence correspondence Γ is simply that of points on lines, and we can appeal to [BGS94, Proposition 4.3.3].

PROPOSITION 6.2.1 ([BGS94, Proposition 4.3.3]). — Let $S = \text{Spec } \mathbb{Z}$ and $\bar{\mathcal{E}}$ an Hermitian vector bundle on S of rank $N + 1$. Let $\bar{\mathcal{E}}^\vee$ be the dual bundle of $\bar{\mathcal{E}}$, and $\mathcal{W} \subseteq \mathbb{P}(\mathcal{E}) \times_S \mathbb{P}(\mathcal{E}^\vee)$ the incidence correspondence of points on lines. Let $\overline{\mathcal{Q}}_{\mathbb{P}(\mathcal{E}^\vee)}$ be the tautological Hermitian quotient bundle on $\mathbb{P}(\mathcal{E}^\vee)$, and $\overline{\mathcal{O}}_{\mathbb{P}(\mathcal{E})}(1)$ tautological Hermitian hyperplane bundle on $\mathbb{P}(\mathcal{E})$. Then, in $\widehat{\text{CH}}^*(\mathbb{P}(\mathcal{E}))_{\mathbb{Q}}$,

$$\mathcal{W}^* \left(\widehat{c} \left(\overline{\mathcal{Q}}_{\mathbb{P}(\mathcal{E}^\vee)} \right) \right) = \widehat{c} \left(\overline{\mathcal{O}}_{\mathbb{P}(\mathcal{E})}(1) \right).$$

We reproduce here the proof of this proposition from [BGS94, Proposition 4.3.3], adding some relevant details where necessary.

Proof. Consider the diagram

$$\begin{array}{ccccc}
 & & \mathbb{P}(\mathcal{E}) \times_S \mathbb{P}(\mathcal{E}^\vee) & & \\
 & \swarrow p & \downarrow \pi & \searrow q & \\
 \mathbb{P}(\mathcal{E}) & & S & & \mathbb{P}(\mathcal{E}^\vee) \\
 & \searrow \alpha & & \swarrow \beta & \\
 & & & &
 \end{array}$$

The bundle $\mathbb{P}(\mathcal{E})$ carries on it a tautological exact sequence

$$0 \rightarrow \mathcal{O}_{\mathbb{P}(\mathcal{E})}(-1) \rightarrow \alpha^* \mathcal{E} \rightarrow \mathcal{Q}_{\mathbb{P}(\mathcal{E})} \rightarrow 0$$

which dualises to

$$0 \rightarrow \mathcal{Q}_{\mathbb{P}(\mathcal{E})}^\vee \rightarrow \alpha^* \mathcal{E}^\vee \rightarrow \mathcal{O}_{\mathbb{P}(\mathcal{E})}(1) \rightarrow 0. \quad (6.3)$$

On the other hand, the bundle $\mathbb{P}(\mathcal{E}^\vee)$ carries on it a tautological exact sequence

$$0 \rightarrow \mathcal{O}_{\mathbb{P}(\mathcal{E}^\vee)}(-1) \rightarrow \beta^* \mathcal{E}^\vee \rightarrow \mathcal{Q}_{\mathbb{P}(\mathcal{E}^\vee)} \rightarrow 0. \quad (6.4)$$

Pulling (6.3) back by p , (6.4) back by q , and identifying the middle terms yields

$$\begin{array}{ccccc}
 p^* \mathcal{Q}_{\mathbb{P}(\mathcal{E})}^\vee & \longrightarrow & \pi^* \mathcal{E}^\vee & \longrightarrow & p^* \mathcal{O}_{\mathbb{P}(\mathcal{E})}(1) \\
 & & \parallel & & \\
 q^* \mathcal{O}_{\mathbb{P}(\mathcal{E}^\vee)}(-1) & \longrightarrow & \pi^* \mathcal{E}^\vee & \longrightarrow & q^* \mathcal{Q}_{\mathbb{P}(\mathcal{E}^\vee)}
 \end{array} \quad (6.5)$$

The vanishing locus³ of the composite map $q^* \mathcal{O}_{\mathbb{P}(\mathcal{E}^\vee)}(-1) \rightarrow p^* \mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)$ is precisely $\mathcal{W}$. This can be seen by computing fibrewise. By the discussion in Section 5.1.4 and [GD60, Proposition 3.4.7], a point of $\mathbb{P}(\mathcal{E}) \times_S \mathbb{P}(\mathcal{E}^\vee)$ can be represented by a tuple $(\mathfrak{p}, \ell, U)$, where $\mathfrak{p} \in S$, and $\ell \subseteq \mathcal{E}_{\mathfrak{p}} \otimes_{\mathcal{O}_{S, \mathfrak{p}}} \kappa(\mathfrak{p})$ and $U \subseteq \mathcal{E}_{\mathfrak{p}}^\vee \otimes_{\mathcal{O}_{S, \mathfrak{p}}} \kappa(\mathfrak{p})$ are one-dimensional subspaces. The point $(\mathfrak{p}, \ell, U)$ lies in $\mathcal{W}$ if and only if $\phi(x) = 0$ for any $\phi \in U$ and $x \in \ell$.

We can identify the fibre $(q^* \mathcal{O}_{\mathbb{P}(\mathcal{E}^\vee)}(-1))_{(\mathfrak{p}, \ell, U)}$ with U itself, and the fibre $(p^* \mathcal{O}_{\mathbb{P}(\mathcal{E})}(1))_{(\mathfrak{p}, \ell, U)}$ with $\ell^\vee$. The map $q^* \mathcal{O}_{\mathbb{P}(\mathcal{E}^\vee)}(-1) \rightarrow \pi^* \mathcal{E}^\vee$ is fibrewise inclusion, and the map $\pi^* \mathcal{E}^\vee \rightarrow p^* \mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)$ is fibrewise restriction, so the composite map

$$U \hookrightarrow \mathcal{E}_{\mathfrak{p}}^\vee \otimes_{\mathcal{O}_{S, \mathfrak{p}}} \kappa(\mathfrak{p}) \twoheadrightarrow \ell^\vee$$

sends a point $\phi \in U$ to the restriction $\phi|_\ell$, and is therefore identically zero if and only if $(\mathfrak{p}, \ell, U) \in \mathcal{W}$.

This shows that, restricted to $\mathcal{W}$, the sequence

$$q^* \mathcal{O}_{\mathbb{P}(\mathcal{E}^\vee)}(1) \rightarrow \pi^* \mathcal{E}^\vee \rightarrow p^* \mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)$$

³The composite map $q^* \mathcal{O}_{\mathbb{P}(\mathcal{E}^\vee)}(-1) \rightarrow p^* \mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)$ can be understood as a section of the Hom bundle $\text{Hom}(q^* \mathcal{O}_{\mathbb{P}(\mathcal{E}^\vee)}(-1), p^* \mathcal{O}_{\mathbb{P}(\mathcal{E})}(1))$, and we refer to the zero subscheme of this section as the vanishing locus of the map.

is a complex. By exactness of the rows of (6.5), the homology of this complex is

$$\begin{aligned} H &= \frac{\ker(\pi^* \mathcal{E}^\vee \rightarrow p^* \mathcal{O}_{\mathbb{P}(\mathcal{E})}(1))}{\operatorname{im}(q^* \mathcal{O}_{\mathbb{P}(\mathcal{E}^\vee)}(-1) \rightarrow \pi^* \mathcal{E}^\vee)} \\ &= \frac{\operatorname{im}(p^* \mathcal{Q}_{\mathbb{P}(\mathcal{E})}^\vee \rightarrow \pi^* \mathcal{E}^\vee)}{\operatorname{im}(q^* \mathcal{O}_{\mathbb{P}(\mathcal{E}^\vee)}(-1) \rightarrow \pi^* \mathcal{E}^\vee)} \\ &= \operatorname{coker}(q^* \mathcal{O}_{\mathbb{P}(\mathcal{E}^\vee)}(-1) \rightarrow p^* \mathcal{Q}_{\mathbb{P}(\mathcal{E})}^\vee). \end{aligned}$$

Here, the map $q^* \mathcal{O}_{\mathbb{P}(\mathcal{E}^\vee)}(-1) \rightarrow p^* \mathcal{Q}_{\mathbb{P}(\mathcal{E})}^\vee$ is defined, fibrewise over $(\mathfrak{p}, \ell, U) \in \mathcal{W}$, by sending $\phi \in U$ to the residue class $\bar{\phi} \in \left(\frac{\mathcal{E}_{\mathfrak{p}}^\vee \otimes_{\mathcal{O}_{S, \mathfrak{p}}} \kappa(\mathfrak{p})}{\ell} \right)^\vee$, which is well-defined since $\phi|_\ell = 0$.

Similarly, there is a map $q^* \mathcal{Q}_{\mathbb{P}(\mathcal{E}^\vee)} \rightarrow p^* \mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)$ defined fibrewise over $(\mathfrak{p}, \ell, U) \in \mathcal{W}$ by sending $\bar{\psi} \in \frac{\mathcal{E}_{\mathfrak{p}}^\vee \otimes_{\mathcal{O}_{S, \mathfrak{p}}} \kappa(\mathfrak{p})}{U}$ to $\psi|_\ell \in \ell^\vee$ where ψ is any lift of $\bar{\psi}$ to $\mathcal{E}_{\mathfrak{p}}^\vee \otimes_{\mathcal{O}_{S, \mathfrak{p}}} \kappa(\mathfrak{p})$. This map is independent of the choice of lift of $\bar{\psi}$ since any functional in U annihilates ℓ . We can identify H with $\ker(q^* \mathcal{Q}_{\mathbb{P}(\mathcal{E}^\vee)} \rightarrow p^* \mathcal{O}_{\mathbb{P}(\mathcal{E})}(1))$, yielding an exact sequence

$$\mathcal{E} : 0 \rightarrow H \rightarrow q^* \mathcal{Q}_{\mathbb{P}(\mathcal{E}^\vee)} \rightarrow p^* \mathcal{O}_{\mathbb{P}(\mathcal{E})}(1) \rightarrow 0.$$

Equipping all bundles with the Hermitian metric induced by that on $\bar{\mathcal{E}}$ and applying Theorem 5.2.4, we see that

$$\widehat{c}(q^* \bar{\mathcal{Q}}_{\mathbb{P}(\mathcal{E}^\vee)}) = \widehat{c}(\bar{H}) \widehat{c}\left(\overline{p^* \mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)}\right) - a(\widetilde{c}(\mathcal{E}))$$

where $\widetilde{c}(\mathcal{E})$ is the Bott-Chern secondary characteristic class of $\mathcal{E}$. By definition, $\mathcal{W}^* \mathcal{Q}_{\mathbb{P}(\mathcal{E}^\vee)} = p_{|\mathcal{W}}^* q^* \mathcal{Q}_{\mathbb{P}(\mathcal{E}^\vee)}$. Functoriality of the arithmetic Chern class (see Theorem 5.2.5) and the projection formula (see Theorem 5.1.4) shows that

$$\mathcal{W}^* (\widehat{c}(\bar{\mathcal{Q}}_{\mathbb{P}(\mathcal{E}^\vee)})) = (p_{|\mathcal{W}}^* \widehat{c}(\bar{H})) \widehat{c}\left(\overline{\mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)}\right) - p_{|\mathcal{W}}^* a(\widetilde{c}(\mathcal{E})).$$

Exactness of $\mathcal{E}$ allows us to compute $\operatorname{rank}(H) = N - 1$. On the other hand, as can be checked on fibres, $p_{|\mathcal{W}} : \mathcal{W} \rightarrow \mathbb{P}(\mathcal{E})$ is isomorphic, as a fibre bundle on $\mathbb{P}(\mathcal{E})$, to $\mathbb{P}(\mathcal{Q}_{\mathbb{P}(\mathcal{E})}^\vee) \rightarrow \mathbb{P}(\mathcal{E})$. This forces

$$p_{|\mathcal{W}}^* \widehat{c}(\bar{H}) \in \widehat{\operatorname{CH}}^0(\mathbb{P}(\mathcal{E})) = \operatorname{CH}^0(\mathbb{P}(\mathcal{E})) = \mathbb{Z},$$

so we can compute $p_{|\mathcal{W}}^* \widehat{c}(\bar{H}) = p_{|\mathcal{W}}^* c(H)$ on the generic fibre. Over $\mathbb{P}(\mathcal{E})$, the bundle $p_{|\mathcal{W}} : H \rightarrow \mathbb{P}(\mathcal{E})$ is isomorphic to the tautological quotient bundle on $\mathbb{P}\left(\mathcal{Q}_{\mathbb{P}(\mathcal{E})}^\vee\right) \rightarrow \mathbb{P}(\mathcal{E})$, so the Whitney sum formula applied to the tautological exact sequence on $\mathbb{P}\left(\mathcal{Q}_{\mathbb{P}(\mathcal{E})}^\vee\right)$ allows us to write

$$c(H) = c(p^* \mathcal{Q}_{\mathbb{P}(\mathcal{E})}^\vee) (1 + \zeta + \zeta^2 + \cdots)$$

and the projection formula yields

$$p_{|\mathcal{W}}^* c(H) = c_0(\mathcal{Q}_{\mathbb{P}(\mathcal{E})}^\vee) = 1.$$

It remains to show that $p_{|\mathcal{W}}^* a(\widetilde{c}(\mathcal{E})) = 0$.

The pushforward $p_{|\mathcal{W}}^* \widetilde{c}(\mathcal{E})$ is concentrated in codimension zero, so is a smooth function on $\mathbb{P}(\mathcal{E})(\mathbb{C})$, which is invariant under the action of the unitary group $U(\bar{\mathcal{E}}_{\mathbb{C}})$. This forces

$p_{|\mathcal{W}*}a(\tilde{c}(\mathcal{E})) = a(\lambda)$ to be some real constant $\lambda \in \mathbb{R}$. Now let $\overline{\mathcal{L}}$ be a line subbundle of $\mathcal{E}$, equipped with its induced metric, and let $Z = \mathbb{P}(\mathcal{L}) \in Z_1(\mathbb{P}(\mathcal{E}))$. Using Theorem 5.2.6 (see also [BGS94, Lemma 4.2.1],

$$\begin{aligned} (\widehat{c}(\overline{\mathcal{Q}}_{\mathbb{P}(\mathcal{E}^\vee)}) | \mathcal{W}_*(Z)) &= (\mathcal{W}^*(\widehat{c}(\overline{\mathcal{Q}}_{\mathbb{P}(\mathcal{E}^\vee)})) | Z) \\ &= \left(\widehat{c}(\overline{\mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)}) | Z \right) - (p_{|\mathcal{W}*}a(\tilde{c}(\mathcal{E}^\vee)) | Z) \\ &= \left(\widehat{c}(\overline{\mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)}) | Z \right) - (\alpha^*a(\lambda) | Z) \\ &= \widehat{c}_1(\overline{\mathcal{L}}) - a(\lambda). \end{aligned}$$

Taking arithmetic degrees⁴, we see that

$$h^{\overline{\mathcal{E}^\vee}}(\mathcal{W}_*(Z)) = \widehat{\deg}(\overline{\mathcal{L}^\vee}) - \frac{\lambda}{2}.$$

Notice, on the other hand, that $\mathcal{W}_*(Z)$ consists of those points of $\mathbb{P}(\mathcal{E}^\vee)$ corresponding, fibrewise, to hyperplanes meeting the fibres of $\mathcal{L}$ nontrivially. Thus, $\mathcal{W}_*(Z) = \mathbb{P}((\mathcal{E}/\mathcal{L})^\vee)$, so by [BGS94, Proposition 4.1.2 (ii)],

$$h^{\overline{\mathcal{E}^\vee}}(\mathcal{W}_*(Z)) = \widehat{\deg}(\overline{\mathcal{E}^\vee}) - \widehat{\deg}((\overline{\mathcal{E}/\mathcal{L}})^\vee) = \widehat{\deg}(\overline{\mathcal{L}^\vee})$$

forcing $\lambda = 0$. □

6.2.2 CONSEQUENCES

Heights and degrees of some kinds of principal determinantal resultants follow readily from Theorem 6.1.2 and Proposition 6.2.1. We begin with degrees. Let $\text{esym}_k(X_1, \dots, X_n)$ be the k^{th} elementary symmetric polynomial in n variables, and, for each $1 \leq i \leq n$, let

$$\text{esym}_k^{(i)}(X_1, \dots, X_n) = \text{esym}_k(X_1, \dots, X_{i-1}, 0, X_{i+1}, \dots, X_n).$$

PROPOSITION 6.2.2. — Let $S = \text{Spec } \mathbb{Z}$, $N \in \mathbb{Z}_{\geq 0}$, and $\mathcal{E} = \mathcal{O}_S^{\oplus N+1}$. Let $e, f, d_1, \dots, d_f \in \mathbb{Z}_{\geq 0}$ with $1 \leq e \leq f$, and $Z \in Z_{f-e+1}(\mathbb{P}(\mathcal{E}))$. Then

$$\deg_i \left(\text{Ch}_{e,f,e-1,(d_1,\dots,d_f)}^{\det}(Z) \right) = \text{esym}_{f-e}^{(i)}(d_1, \dots, d_f) \deg_{\mathbb{Q}}(Z).$$

Proof. For each $1 \leq j \leq f$, let $N_j = \text{rank}(\check{\mathbb{P}}_j) = e \binom{N+d_j}{d_j} - 1$, and let $\mathcal{Q}_j$ be the tautological quotient bundle on $\check{\mathbb{P}}_j$. Let

$$\alpha = c_{N_i-1}(\mathcal{Q}_i) \prod_{j \neq i} c_{N_j}(\mathcal{Q}_j).$$

⁴Up until this point in the proof, our proof is exactly the same as that of [BGS94, Proposition 4.3.3]. The only tweak we make is to compute projective heights, so that we can work in $\widehat{\text{CH}}^1(S) \cong \mathbb{R}$ rather than $\widehat{\text{CH}}^1(\mathbb{P}(\mathcal{E}))$. We do this here so that the proof of the generalisation obtained by replacing $\mathbb{P}(\mathcal{E})$ by a Grassmann bundle reduces verbatim to the projective case.

Then by definition (see Section 5.2.6)

$$\deg_i \left(\text{Ch}_{e,f,e-1,(d_1,\dots,d_f)}^{\det}(Z) \right) = \deg_{\mathbb{Q}} \left(\alpha \mid \text{Ch}_{e,f,e-1,(d_1,\dots,d_f)}^{\det}(Z) \right).$$

Let $\mathcal{L}_j = \mathcal{O}_{\mathbb{P}((\text{Sym}^{d_j}(\mathcal{E}^\vee))^{\oplus e})}(1)$ be the hyperplane bundle on $\mathbb{G}_i = \mathbb{P}((\text{Sym}^{d_j}(\mathcal{E}^\vee))^{\oplus e})$. Then by Proposition 6.2.1, for each $1 \leq j \leq f$, we have

$$\mathcal{W}_j^* c_{N_j}(\mathcal{Q}_j) = c_1(\mathcal{L}_j) \quad \text{and} \quad \mathcal{W}_i^* c_{N_{i-1}}(\mathcal{Q}_i) = c_0(\mathcal{L}_i) = 1.$$

Let $\mathcal{Z} = Z \times_S \mathbb{P}(\mathcal{O}_S^{\oplus e})$. Let $\pi_1 : \mathbb{P}_j \times_S \mathbb{P}(\mathcal{O}_S^{\oplus e}) \rightarrow \mathbb{P}_j$ (resp. π_2) is projection onto the first (resp. second) factor. For each $1 \leq j \leq f$, let $\mathcal{M}_j = s_j^* \mathcal{L}_j$ be the pullback of $\mathcal{L}_j$ under the Segre embedding. We can then write

$$\mathcal{M}_j = s_j^* \mathcal{L}_j = \mathcal{M}_j^{(1)} \otimes \mathcal{M}_j^{(2)}$$

where

$$\mathcal{M}_j^{(1)} = \pi_1^* \mathcal{O}_{\mathbb{P}_j}(1) \quad \text{and} \quad \mathcal{M}_j^{(2)} = \pi_2^* \mathcal{O}_{\mathbb{P}(\mathcal{O}_S^{\oplus e})}(1).$$

Repeated application of Theorem 5.2.6 (see also [BGS94, Lemma 4.2.1] yields

$$\begin{aligned} \deg_{\mathbb{Q}} \left(\alpha \mid \text{Ch}_{e,f,e-1,(d_1,\dots,d_f)}^{\det}(Z) \right) &= \deg_{\mathbb{Q}} \left(\Gamma^*(\alpha) \mid s_*(\nu \times id)_*(\mathcal{Z}) \right) \\ &= \deg_{\mathbb{Q}} \left(\prod_{j \neq i} c_1(\mathcal{L}_j) \mid s_*(\nu \times id)_*(\mathcal{Z}) \right) \\ &= \deg_{\mathbb{Q}} \left(s^* \left(\prod_{j \neq i} c_1(\mathcal{L}_j) \right) \mid (\nu \times id)_*(\mathcal{Z}) \right) \\ &= \deg_{\mathbb{Q}} \left(\prod_{j \neq i} c_1(\mathcal{M}_j) \mid (\nu \times id)_*(\mathcal{Z}) \right) \\ &= \deg_{\mathbb{Q}} \left(\prod_{j \neq i} \left(c_1(\mathcal{M}_j^{(1)}) + c_1(\mathcal{M}_j^{(2)}) \right) \mid (\nu \times id)_*(\mathcal{Z}) \right) \\ &= \deg_{\mathbb{Q}} \left((\nu \times id)^* \prod_{j \neq i} \left(c_1(\mathcal{M}_j^{(1)}) + c_1(\mathcal{M}_j^{(2)}) \right) \mid \mathcal{Z} \right) \\ &= \deg_{\mathbb{Q}} \left(\prod_{j \neq i} \left(d_j c_1(\mathcal{M}_j^{(1)}) + c_1(\mathcal{M}_j^{(2)}) \right) \mid \mathcal{Z} \right) \end{aligned}$$

Since Z has dimension $f - e + 1$, its generic fibre $Z_{\mathbb{Q}}$ has dimension $f - e$, and the only term of this final product which survives is

$$\text{esym}_{f-e}^{(i)}(d_1, \dots, d_f) \deg_{\mathbb{Q}}(c_1(\mathcal{O}_X(1))^{f-e} \mid Z).$$

as desired. □

PROPOSITION 6.2.3. — Let $S = \operatorname{Spec} \mathbb{Z}$, $N \in \mathbb{Z}_{\geq 0}$, and $\mathcal{E} = \mathcal{O}_S^{\oplus N+1}$. Let $\bar{\mathcal{E}}$ be $\mathcal{E}$ equipped with its trivial Hermitian metric. Let $e, f, d_1, \dots, d_f \in \mathbb{Z}_{\geq 0}$ with $1 \leq e \leq f$, and $Z \in Z_{f-e+1}(\mathbb{P}(\mathcal{E}))$. Then

$$h(\operatorname{Ch}_{e,f,e-1,(d_1,\dots,d_f)}^{\det}(Z)) = \operatorname{esym}_{f-e+1}(d_1, \dots, d_f) h_{\overline{\mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)}}(Z) \\ + \operatorname{esym}_{f-e}(d_1, \dots, d_f) \deg(Z) \sigma_{e-1}.$$

Proof. For each $1 \leq i \leq f$, let $\bar{\mathcal{Q}}_i$ be the tautological quotient bundle on $\check{\mathbb{P}}_i$, equipped with the Hermitian metric induced by that on $\mathcal{E}$. By definition (see Section 5.2.6),

$$h\left(\operatorname{Ch}_{e,f,e-1,(d_1,\dots,d_f)}^{\det}(Z)\right) = \widehat{\deg}\left(\prod_{i=1}^f \widehat{c}(\bar{\mathcal{Q}}_i) \mid \operatorname{Ch}_{e,f,e-1,(d_1,\dots,d_f)}^{\det}(Z)\right).$$

As in the proof of Proposition 6.2.2, for each $1 \leq i \leq f$, let $\bar{\mathcal{L}}_i = \overline{\mathcal{O}_{\mathbb{P}((\operatorname{Sym}^{d_i}(\mathcal{E}^\vee))^{\oplus e})}(1)}}$, equipped with the Hermitian metric induced by that on $\mathcal{E}$. Then, by Proposition 6.2.1, for each $1 \leq i \leq f$, $\mathcal{W}_i^* \widehat{c}(\bar{\mathcal{Q}}_i) = \widehat{c}(\bar{\mathcal{L}}_i)$. Let $\mathcal{Z} = Z \times_S \mathbb{P}(\mathcal{O}_S^{\oplus e})$. Once again, let $\pi_1 : \mathbb{P}_i \times_S \mathbb{P}(\mathcal{O}_S^{\oplus e}) \rightarrow \mathbb{P}_i$ (resp. π_2) be projection onto the first (resp. second) factor. For each $1 \leq i \leq f$, let $\bar{\mathcal{M}}_i = s_i^* \bar{\mathcal{L}}_i$ be the pullback of $\bar{\mathcal{L}}_i$ under the Segre embedding, equipped with the pulled back Hermitian metric, so that

$$\bar{\mathcal{M}}_i = s_i^* \bar{\mathcal{L}}_i = \bar{\mathcal{M}}_i^{(1)} \otimes \bar{\mathcal{M}}_i^{(2)}$$

where

$$\bar{\mathcal{M}}_i^{(1)} = \pi_1^* \overline{\mathcal{O}_{\mathbb{P}_i}(1)} \quad \text{and} \quad \bar{\mathcal{M}}_i^{(2)} = \pi_2^* \overline{\mathcal{O}_{\mathbb{P}(\mathcal{O}_S^{\oplus e})}(1)}.$$

By Theorem 5.2.6 (see also [BGS94, Lemma 4.2.1]),

$$\begin{aligned} \widehat{\deg}\left(\prod_{i=1}^f \widehat{c}(\bar{\mathcal{Q}}_i) \mid \operatorname{Ch}_{e,f,e-1,(d_1,\dots,d_f)}^{\det}(Z)\right) \\ &= \widehat{\deg}\left(\prod_{i=1}^f \mathcal{W}_i^* \widehat{c}(\bar{\mathcal{Q}}_i) \mid s_*(\nu \times id)_*(\mathcal{Z})\right) \\ &= \widehat{\deg}\left(\prod_{i=1}^f \widehat{c}(\bar{\mathcal{L}}_i) \mid s_*(\nu \times id)_*(\mathcal{Z})\right) \\ &= \widehat{\deg}\left(s^*\left(\prod_{i=1}^f \widehat{c}(\bar{\mathcal{L}}_i)\right) \mid (\nu \times id)_*(\mathcal{Z})\right) \\ &= \widehat{\deg}\left(\prod_{i=1}^f \widehat{c}(\bar{\mathcal{M}}_i) \mid (\nu \times id)_*(\mathcal{Z})\right) \\ &= \widehat{\deg}\left(\prod_{i=1}^f \left(\widehat{c}_1(\bar{\mathcal{M}}_i^{(1)}) + \widehat{c}_1(\bar{\mathcal{M}}_i^{(2)})\right) \mid (\nu \times id)_*(\mathcal{Z})\right) \\ &= \widehat{\deg}\left((\nu \times id)^*\left(\prod_{i=1}^f \left(\widehat{c}_1(\bar{\mathcal{M}}_i^{(1)}) + \widehat{c}_1(\bar{\mathcal{M}}_i^{(2)})\right)\right) \mid \mathcal{Z}\right) \\ &= \widehat{\deg}\left(\prod_{i=1}^f \left(\widehat{c}_1(\bar{\mathcal{M}}_i^{(1)}) + \widehat{c}_1(\bar{\mathcal{M}}_i^{(2)})\right) \mid \mathcal{Z}\right) \end{aligned}$$

$$= \widehat{\deg} \left(\prod_{i=1}^f \left(d_i \widehat{c}_1 \left(\overline{\mathcal{M}}_i^{(1)} \right) + \widehat{c}_1 \left(\overline{\mathcal{M}}_i^{(2)} \right) \right) \mid \mathcal{Z} \right)$$

The scheme $\mathbb{P}(\mathcal{O}_S^{\oplus e})$ has dimension e , and Z has dimension $f - e + 1$, so

$$\begin{aligned} & \left(\prod_{i=1}^f \left(d_i \widehat{c}_1 \left(\overline{\mathcal{M}}_i^{(1)} \right) + \widehat{c}_1 \left(\overline{\mathcal{M}}_i^{(2)} \right) \right) \mid \mathcal{Z} \right) \\ &= \left(\text{esym}_{f-e}(d_1, \dots, d_f) \widehat{c}_1 \left(\overline{\mathcal{M}}_i^{(1)} \right)^{f-e} \widehat{c}_1 \left(\overline{\mathcal{M}}_i^{(2)} \right)^e \mid \mathcal{Z} \right) \\ &+ \left(\text{esym}_{f-e+1}(d_1, \dots, d_f) \widehat{c}_1 \left(\overline{\mathcal{M}}_i^{(1)} \right)^{f-e+1} \widehat{c}_1 \left(\overline{\mathcal{M}}_i^{(2)} \right)^{e-1} \mid \mathcal{Z} \right) \end{aligned}$$

and the result follows from Proposition 5.2.7. $\square$

COROLLARY 6.2.4. — Let $e, f, d_1, \dots, d_f \in \mathbb{Z}_{\geq 0}$ with $1 \leq e \leq f$. Then

$$\deg_i \left(\text{div} \left(\text{Res}_{e,f,e-1,(d_1,\dots,d_f)} \right) \right) = \text{esym}_{f-e}^{(i)}(d_1, \dots, d_f)$$

and

$$h \left(\text{div} \left(\text{Res}_{e,f,e-1,(d_1,\dots,d_f)} \right) \right) = \text{esym}_{f-e+1}(d_1, \dots, d_f) \sigma_{f-e} + \text{esym}_{f-e}(d_1, \dots, d_f) \sigma_{e-1}.$$

Proof. By Theorem 6.1.2,

$$\text{Ch}_{e,f,e-1,(d_1,\dots,d_f)}^{\det} \left(\mathbb{P}^{f-e+1} \right) = \text{div} \left(\text{Res}_{e,f,e-1,(d_1,\dots,d_f)} \right)$$

and the equalities follow from Proposition 6.2.2 and Proposition 6.2.3, together with Proposition 5.2.7. $\square$

COROLLARY 6.2.5. — Let $e, f, d_1, \dots, d_f \in \mathbb{Z}_{\geq 0}$ with $1 \leq e \leq f$ and let $\mathcal{E} = \mathcal{O}_S^{\oplus f-e+1}$. For each $1 \leq i \leq f$, let $\check{\mathbb{P}}_i = \mathbb{P} \left(\left(\text{Sym}^{d_i} \mathcal{E}^\vee \right)^{\oplus e} \right)$, $N_i = \text{rank}(\check{\mathbb{P}}_i) = e \binom{f-e+d_i}{d_i} - 1$, $\pi_i : \prod_{i=1}^f \check{\mathbb{P}}_i \rightarrow \check{\mathbb{P}}_i$ the projection onto the i^{th} factor, and $\mu_i = c_1 \left(\pi_i^* \overline{\mathcal{O}_{\check{\mathbb{P}}_i}}(1) \right)$. Then

$$\begin{aligned} \int_{\left(\prod_{i=1}^f \check{\mathbb{P}}_i \right)(\mathbb{C})} \log \left\| \text{Res}_{e,f,e-1,(d_1,\dots,d_f)} \right\| \cdot \prod_{i=1}^f \mu_i^{N_i} &= \text{esym}_{f-e+1}(d_1, \dots, d_f) \sigma_{f-e} \\ &+ \text{esym}_{f-e}(d_1, \dots, d_f) \sigma_{e-1} \\ &- \frac{1}{2} \sum_{i=1}^f \text{esym}_{f-e}^{(i)}(d_1, \dots, d_f) \mathcal{H}_{N_i}. \end{aligned}$$

Proof. Apply Lemma 5.2.8, using Theorem 6.1.2 and Corollary 6.2.4. $\square$

6.2.3 AN EXAMPLE

Consider the case $e = 3, f = 4, r = 2, d_1 = d_2 = d_3 = d_4 = 1$. The corresponding resultant $\text{Res}_{3,4,2,(1,1,1,1)}$ is indeed a principal determinantal resultant, associated to the maximal minors of a 3×4 matrix of linear forms. By Corollary 6.2.4, we can immediately see that for any $1 \leq i \leq 4$, the degree of $\text{Res}_{3,4,2,(1,1,1,1)}$ in the block of variables corresponding to the i^{th} column is

$$\text{esym}_1^{(i)}(1, 1, 1, 1) = 3.$$

The total degree of $\text{Res}_{3,4,2,(1,1,1,1)}$ is therefore 12.

Again by Corollary 6.2.4, we can compute the (normalised projective) height of $\text{Res}_{3,4,2,(1,1,1,1)}$ as

$$h(\text{div}(\text{Res}_{3,4,2,(1,1,1,1)})) = \text{esym}_2(1, 1, 1, 1)\sigma_1 + \text{esym}_1(1, 1, 1, 1)\sigma_2 = \frac{1}{2}\binom{4}{2} + \frac{5}{4}\binom{4}{1} = 8$$

and, via Corollary 6.2.5, its Mahler measure as $-\frac{57}{10}$.

6.3 HIGHER CORANK CONDITIONS

We return to the general setting of the construction in Section 6.1.1, where $e, f, r \in \mathbb{Z}_{>0}$, with $r \leq \min\{e, f\}$, and $d_1, \dots, d_f \in \mathbb{Z}_{\geq 0}$. In this section, we will show that both degrees and heights of determinantal resultants can be extracted from our construction in Section 6.1.2.

6.3.1 PULLING BACK THE QUOTIENT BUNDLE

As in the principal case in order to compute degrees and heights, we must understand the pullback of the tautological quotient bundle on $\check{\mathbb{P}}_i$ through $\mathcal{W}_i$. The following theorem directly generalises Proposition 6.2.1.

THEOREM 6.3.1. — Let $S = \text{Spec } \mathbb{Z}$ and $\bar{\mathcal{E}}$ an Hermitian vector bundle on S of rank $N + 1$. Let $k \in \mathbb{Z}_{>0}$ with $k \leq N + 1$. Let $\bar{\mathcal{E}}^\vee$ be the dual bundle of $\bar{\mathcal{E}}$, and $\mathcal{W} \subseteq \mathbb{G}(k, \mathcal{E}) \times_S \mathbb{P}(\mathcal{E}^\vee)$ the incidence correspondence of k -planes contained in hyperplanes. Let $\bar{\mathcal{Q}}_{\mathbb{P}(\mathcal{E}^\vee)}$ be the tautological Hermitian quotient bundle on $\mathbb{P}(\mathcal{E}^\vee)$, and $\bar{\mathcal{S}}_{\mathbb{G}(k, \mathcal{E})}$ the tautological Hermitian rank- k subbundle on $\mathbb{G}(k, \mathcal{E})$. Then, in $\widehat{\text{CH}}^*(\mathbb{G}(k, \mathcal{E}))_{\mathbb{Q}}$,

$$\mathcal{W}^*(\widehat{c}(\bar{\mathcal{Q}}_{\mathbb{P}(\mathcal{E}^\vee)})) = \widehat{c}(\bar{\mathcal{S}}_{\mathbb{G}(k, \mathcal{E})}^\vee).$$

Proof. Replacing $\mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)$ with $\mathcal{S}_{\mathbb{G}(k, \mathcal{E})}^\vee$ in the proof of Proposition 6.2.1 yields an exact sequence of vector bundles

$$\mathcal{E} : 0 \rightarrow H \rightarrow q^*\mathcal{Q}_{\mathbb{P}(\mathcal{E}^\vee)} \rightarrow p^*\mathcal{S}_{\mathbb{G}(k, \mathcal{E})}^\vee \rightarrow 0$$

on $\mathcal{W}$. Giving all bundles Hermitian metrics induced by that on $\mathcal{E}$, we once again see that

$$\mathcal{W}^*\widehat{c}(\bar{\mathcal{Q}}_{\mathbb{P}(\mathcal{E}^\vee)}) = \widehat{c}(\bar{\mathcal{S}}_{\mathbb{G}(k, \mathcal{E})}^\vee) - p_{|\mathcal{W}*}a(\widehat{c}(\bar{\mathcal{E}})).$$

As in Proposition 6.2.1, we are left to show that $p_{|\mathcal{W}*}a(\widehat{c}(\bar{\mathcal{E}})) = 0$ in $\widehat{\text{CH}}^k(\mathbb{G}(k, \mathcal{E}))$.

By Theorem 5.2.10, we can write

$$p_{|\mathcal{W}^*} a(\tilde{c}(\overline{\mathcal{E}})) = \sum_{\substack{\lambda \in \mathcal{P}(k, N+1) \\ |\lambda| = k-1}} a(f_\lambda c_\lambda(\overline{\mathcal{Q}}))$$

for some $f_\lambda \in \mathbb{R}$.

Fix a complete flag of subbundles $\mathcal{E}_\bullet : 0 \subsetneq \mathcal{E}_1 \subsetneq \cdots \subsetneq \mathcal{E}_{N+1} = \mathcal{E}$. For each $\lambda \in \mathcal{P}(k, N+1)$ with $|\lambda| = k-1$, let $\lambda^\vee$ be the dual partition of λ , defined by

$$\lambda_i^\vee = (N+1-k) - \lambda_{k+1-i}.$$

$\Sigma_{\lambda^\vee} \in Z_k(\mathbb{G}(k, \mathcal{E}))$ be the Schubert cycle corresponding to $\lambda^\vee$ with respect to $\mathcal{E}_\bullet$. From Lemma 5.2.9, we see that there exists some $1 \leq r \leq N+1$ such that $\mathcal{W}_*(\Sigma_{\lambda^\vee}) = \mathbb{P}((\mathcal{E}/\mathcal{E}_r)^\vee)$. Using Theorem 5.2.6 (see also [BGS94, Lemma 4.2.1]), we have

$$\begin{aligned} h^{\overline{\mathcal{E}^\vee}}(\mathcal{W}_*(\Sigma_{\lambda^\vee})) &= \widehat{\deg}(\widehat{c}(\overline{\mathcal{Q}}_{\mathbb{P}(\mathcal{E}^\vee)} | \mathcal{W}_*(\Sigma_{\lambda^\vee})) \\ &= \widehat{\deg}(\mathcal{W}^*(\widehat{c}(\overline{\mathcal{Q}}_{\mathbb{P}(\mathcal{E}^\vee)})) | \Sigma_{\lambda^\vee}) \\ &= \widehat{\deg}(\widehat{c}(\overline{\mathcal{S}}_{\mathbb{G}(k, \mathcal{E})}) - p_{|\mathcal{W}^*} a(\tilde{c}(\overline{\mathcal{E}})) | \Sigma_{\lambda^\vee}) \\ &= \widehat{\deg}(\mathcal{E}_r^\vee) - \frac{f_\lambda}{2}. \end{aligned}$$

On the other hand, by [BGS94, Proposition 4.1.2(ii)],

$$h^{\overline{\mathcal{E}^\vee}}(\mathcal{W}_*(\Sigma_{\lambda^\vee})) = \widehat{\deg}((\mathcal{E}/\mathcal{E}_r)^\vee) = \widehat{\deg}(\mathcal{E}_r^\vee)$$

forcing each f_λ to vanish. □

6.3.2 CONSEQUENCES

Theorem 6.3.1 directly generalises Proposition 6.2.1. It allows for the computation of degrees and heights of determinantal resultants associated to arbitrary parameters $e, f, r, (d_1, \dots, d_f)$.

PROPOSITION 6.3.2. — Let $S = \operatorname{Spec} \mathbb{Z}$, $N \in \mathbb{Z}_{\geq 0}$, and $\mathcal{E} = \mathcal{O}_S^{\oplus N+1}$. Let $e, f, r, d_1, \dots, d_f \in \mathbb{Z}_{\geq 0}$ with $r \leq \min\{e, f\}$, and $Z \in Z_{(f-r)(e-r)}(\mathbb{P}(\mathcal{E}))$. Then

$$\deg_i \left(\operatorname{Ch}_{e, f, r, (d_1, \dots, d_f)}^{\det}(Z) \right) = \deg(Z) \left(\sum_{\substack{0 \leq k_1, \dots, k_f \leq e-r \\ k_i \leq e-r-1 \\ \sum_u k_u = (f-r)(e-r)-1}} \mathcal{N}_{k_1, \dots, k_f}^{(i)} (k_i + 1) d_i^{k_i} \prod_{j \neq i} d_j^{k_j} \right).$$

where

$$\mathcal{N}_{k_1, \dots, k_f}^{(i)} = \int_{\mathbb{G}(e-r, \mathcal{O}_S^{\oplus e})_{\mathbb{Q}}} c_{e-r-k_i-1}(\mathcal{S}^\vee) \prod_{j \neq i} c_{e-r-k_j}(\mathcal{S}^\vee).$$

Proof. As in the proof of Proposition 6.2.2, for each $1 \leq j \leq f$, let $N_j = \operatorname{rank}(\check{\mathbb{P}}_j) = e \binom{N+d_j}{d_j} - 1$, and let $\mathcal{Q}_j$ be the tautological quotient bundle on $\check{\mathbb{P}}_j$. Let

$$\alpha = c_{N_i-1}(\mathcal{Q}_i) \prod_{j \neq i} c_{N_j}(\mathcal{Q}_j).$$

Then by definition (see Section 5.2.6)

$$\deg_i(\mathrm{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(Z)) = \deg_{\mathbb{Q}}\left(\alpha \mid \mathrm{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(Z)\right).$$

For each $1 \leq j \leq f$, let $\mathcal{S}_{\mathbb{G}_j}^{\vee}$ be the dual to the tautological rank- $(e-r)$ subbundle on $\mathbb{G}_j$. By Theorem 6.3.1, we have

$$\mathcal{W}_j^* c_{N_j}(\mathcal{Q}_j) = c_{e-r}(\mathcal{S}_{\mathbb{G}_j}^{\vee}) \quad \text{and} \quad \mathcal{W}_i^* c_{N_i-1}(\mathcal{Q}_i) = c_{e-r-1}(\mathcal{S}_{\mathbb{G}_i}^{\vee}).$$

Let $\mathcal{Z} = Z \times_S \mathbb{G}(e-r, \mathcal{O}_S^{\oplus e})$. Let $\pi_1 : \mathbb{P}_j \times_S \mathbb{G}(e-r, \mathcal{O}_S^{\oplus e}) \rightarrow \mathbb{P}_j$ (resp. π_2) be projection onto the first (resp. second) factor, and let $\mathcal{S}$ be the tautological rank- $(e-r)$ subbundle on $\mathbb{G}(e-r, \mathcal{O}_S^{\oplus e})$. For each $1 \leq j \leq f$, let $\mathcal{M}_j = s_j^* \mathcal{S}_{\mathbb{G}_j}^{\vee}$ be the pullback of the bundle $\mathcal{S}_{\mathbb{G}_j}^{\vee}$ under the Segre embedding. We can then write

$$\mathcal{M}_j = s_j^* \mathcal{S}_{\mathbb{G}_j}^{\vee} = \pi_1^* \mathcal{O}_{\mathbb{P}_j}(1) \otimes \pi_2^* \mathcal{S}^{\vee}.$$

By Theorem 5.2.6 (see also [BGS94, Lemma 4.2.1], we have

$$\begin{aligned} & \deg_{\mathbb{Q}}\left(\alpha \mid \mathrm{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(Z)\right) \\ &= \deg_{\mathbb{Q}}(\Gamma^*(\alpha) \mid s_*(\nu \times id)_*(\mathcal{Z})) \\ &= \deg_{\mathbb{Q}}\left(c_{e-r-1}(\mathcal{S}_{\mathbb{G}_i}^{\vee}) \prod_{j \neq i} c_{e-r}(\mathcal{S}_{\mathbb{G}_j}^{\vee}) \mid s_*(\nu \times id)_*(\mathcal{Z})\right) \\ &= \deg_{\mathbb{Q}}\left(s^*\left(c_{e-r-1}(\mathcal{S}_{\mathbb{G}_i}^{\vee}) \prod_{j \neq i} c_{e-r}(\mathcal{S}_{\mathbb{G}_j}^{\vee})\right) \mid (\nu \times id)_*(\mathcal{Z})\right) \\ &= \deg_{\mathbb{Q}}\left(c_{e-r-1}(\mathcal{M}_i) \prod_{j \neq i} c_{e-r}(\mathcal{M}_j) \mid (\nu \times id)_*(\mathcal{Z})\right) \\ &= \deg_{\mathbb{Q}}\left((\nu \times id)^*\left(c_{e-r-1}(\mathcal{M}_i) \prod_{j \neq i} c_{e-r}(\mathcal{M}_j)\right) \mid \mathcal{Z}\right) \\ &= \deg_{\mathbb{Q}}\left(c_{e-r-1}(\pi_1^* \mathcal{O}_{\mathbb{P}(\mathcal{E})}(d_i) \otimes \pi_2^* \mathcal{S}^{\vee}) \prod_{j \neq i} c_{e-r}(\pi_1^* \mathcal{O}_{\mathbb{P}(\mathcal{E})}(d_j) \otimes \pi_2^* \mathcal{S}^{\vee}) \mid \mathcal{Z}\right) \end{aligned}$$

By [Ful98e, Remark 3.2.3(b)],

$$c_{e-r-1}(\pi_1^* \mathcal{O}_{\mathbb{P}(\mathcal{E})}(d_i) \otimes \pi_2^* \mathcal{S}^{\vee}) = \sum_{k=0}^{e-r-1} (k+1) c_1(\pi_1^* \mathcal{O}_{\mathbb{P}(\mathcal{E})}(d_i))^k c_{e-r-k-1}(\pi_2^* \mathcal{S}^{\vee})$$

and

$$c_{e-r}(\pi_1^* \mathcal{O}_{\mathbb{P}(\mathcal{E})}(d_j) \otimes \pi_2^* \mathcal{S}^{\vee}) = \sum_{k=0}^{e-r} c_1(\pi_1^* \mathcal{O}_{\mathbb{P}(\mathcal{E})}(d_j))^k c_{e-r-k}(\pi_2^* \mathcal{S}^{\vee}).$$

Since $Z_{\mathbb{Q}}$ has dimension $(f-r)(e-r)-1$ and $\mathbb{G}(e-r, \mathcal{O}_S^{\oplus e})_{\mathbb{Q}}$ has dimension $r(e-r)$, the only terms of the product which survive are

$$\deg(Z_{\mathbb{Q}}) \left(\sum_{\substack{0 \leq k_1, \dots, k_f \leq e-r \\ k_i \leq e-r-1 \\ \sum_u k_u = (f-r)(e-r)-1}} \left((k_i+1) d_i^{k_i} \prod_{j \neq i} d_j^{k_j} \int_{\mathbb{G}(e-r, \mathcal{O}_S^{\oplus e})_{\mathbb{Q}}} c_{e-r-k_i-1}(\mathcal{S}^{\vee}) \prod_{j \neq i} c_{e-r-k_j}(\mathcal{S}^{\vee}) \right) \right).$$

□

PROPOSITION 6.3.3. — Let $S = \operatorname{Spec} \mathbb{Z}$, $N \in \mathbb{Z}_{\geq 0}$, and $\mathcal{E} = \mathcal{O}_S^{\oplus N+1}$. Let $e, f, r, d_1, \dots, d_f \in \mathbb{Z}_{\geq 0}$ with $r \leq \min\{e, f\}$, and $Z \in Z_{(f-r)(e-r)}(\mathbb{P}(\mathcal{E}))$. Then

$$\begin{aligned} h\left(\operatorname{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(Z)\right) &= \deg(Z_{\mathbb{Q}}) \sum_{\substack{0 \leq k_1, \dots, k_f \leq e-r \\ k_1 + \dots + k_f = (f-r)(e-r)-1}} \prod_{i=1}^f d_i^{k_i} \widehat{\deg}(\widehat{\tau}_{k_1, \dots, k_f} \mid \mathbb{G}(e-r, \mathcal{O}_S^{\oplus e})) \\ &\quad + h_{\overline{\mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)}}(Z) \sum_{\substack{0 \leq k_1, \dots, k_f \leq e-r \\ k_1 + \dots + k_f = (f-r)(e-r)}} \prod_{i=1}^f d_i^{k_i} \int_{\mathbb{G}(e-r, \mathcal{O}_S^{\oplus e})_{\mathbb{Q}}} \tau_{k_1, \dots, k_f} \end{aligned}$$

where

$$\tau_{k_1, \dots, k_f} = \prod_{i=1}^f c_{e-r-k_i}(\mathcal{S}^{\vee}) \quad \text{and} \quad \widehat{\tau}_{k_1, \dots, k_f} = \prod_{i=1}^f \widehat{c}_{e-r-k_i}(\overline{\mathcal{S}^{\vee}}).$$

Proof. Let $\overline{\mathcal{Q}}_i$ be the tautological Hermitian quotient bundle on $\check{\mathbb{P}}_i$. We have

$$h\left(\operatorname{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(Z)\right) = \widehat{\deg}\left(\prod_{i=1}^f \widehat{c}(\overline{\mathcal{Q}}_i) \mid \operatorname{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(Z)\right).$$

Let $\mathcal{Z} = Z \times_S \mathbb{G}(e-r, \mathcal{O}_S^{\oplus e})$. Applying Theorem 6.3.1 and Theorem 5.2.6 (see also [BGS94, Lemma 4.2.1] repeatedly (as in the proof of Proposition 6.2.3), we see that

$$h\left(\operatorname{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(Z)\right) = \widehat{\deg}\left(\prod_{i=1}^f \widehat{c}_{e-r}\left(\pi_1^* \overline{\mathcal{O}_{\mathbb{P}(\mathcal{E})}(d_i)} \otimes \pi_2^* \mathcal{S}^{\vee}\right) \mid \mathcal{Z}\right). \quad (6.6)$$

By [GS90b, Theorem 4.1(III)], we can write

$$\widehat{c}_{e-r}\left(\pi_1^* \overline{\mathcal{O}_{\mathbb{P}(\mathcal{E})}(d_i)} \otimes \pi_2^* \mathcal{S}^{\vee}\right) = \sum_{k=0}^{e-r} \widehat{c}_1\left(\pi_1^* \overline{\mathcal{O}_{\mathbb{P}(\mathcal{E})}(d_i)}\right)^k \widehat{c}_{e-r-k}\left(\pi_2^* \mathcal{S}^{\vee}\right)$$

from which it follows that

$$\begin{aligned} &h\left(\operatorname{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(Z)\right) \\ &= \deg(Z) \sum_{\substack{0 \leq k_1, \dots, k_f \leq e-r \\ k_1 + \dots + k_f = (f-r)(e-r)-1}} d_i^{k_i} \widehat{\deg}\left(\prod_{i=1}^f \widehat{c}_{e-r-k_i}\left(\pi_2^* \mathcal{S}^{\vee}\right) \mid \mathbb{G}(e-r, \mathcal{O}_S^{\oplus e})\right). \end{aligned}$$

Since Z has dimension $(f-r)(e-r)$ and $\mathbb{G}(e-r, \mathcal{O}_S^{\oplus e})$ has dimension $r(e-r) + 1$, we can decompose (6.6) as

$$\begin{aligned} &\widehat{\deg}\left(\prod_{i=1}^f \widehat{c}_{e-r}\left(\pi_1^* \overline{\mathcal{O}_{\mathbb{P}(\mathcal{E})}(d_i)} \otimes \pi_2^* \mathcal{S}^{\vee}\right) \mid \mathcal{Z}\right) \\ &= \sum_{\substack{0 \leq k_1, \dots, k_f \leq e-r \\ k_1 + \dots + k_f = (f-r)(e-r)-1}} \deg_{\mathbb{Q}}(\alpha_{k_1, \dots, k_f} \mid Z) \widehat{\deg}(\beta_{k_1, \dots, k_f} \mid \mathbb{G}(e-r, \mathcal{O}_S^{\oplus e})) \\ &\quad + \sum_{\substack{0 \leq k_1, \dots, k_f \leq e-r \\ k_1 + \dots + k_f = (f-r)(e-r)}} \widehat{\deg}(\alpha_{k_1, \dots, k_f} \mid Z) \deg_{\mathbb{Q}}(\beta_{k_1, \dots, k_f} \mid \mathbb{G}(e-r, \mathcal{O}_S^{\oplus e})) \end{aligned}$$

where, for any $0 \leq k_1, \dots, k_f \leq e - r$,

$$\alpha_{k_1, \dots, k_f} = \prod_{i=1}^f \widehat{c}_1 \left(\overline{\mathcal{O}_{\mathbb{P}(\mathcal{E})}(d_i)} \right)^{k_i} = \widehat{c}_1 \left(\overline{\mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)} \right)^{\sum_{i=1}^f k_i} \prod_{i=1}^f d_i^{k_i}$$

and

$$\beta_{k_1, \dots, k_f} = \prod_{i=1}^f \widehat{c}_{e-r-k_i} \left(\overline{\mathcal{S}^\vee} \right).$$

If $k_1 + \dots + k_f = (f - r)(e - r) - 1$, then

$$\deg_{\mathbb{Q}}(\alpha_{k_1, \dots, k_f} \mid Z) = \deg(Z_{\mathbb{Q}}) \prod_{i=1}^f d_i^{k_i}.$$

On the other hand, if $k_1 + \dots + k_f = (f - r)(e - r)$, then

$$\widehat{\deg}(\alpha_{k_1, \dots, k_f} \mid Z) = h_{\overline{\mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)}}(Z) \prod_{i=1}^f d_i^{k_i}$$

and we are done. □

REMARK 6.3.4. — The number $\mathcal{N}_{k_1, \dots, k_f}^{(i)}$ appearing in Proposition 6.3.2 and the degree of $\tau_{k_1, \dots, k_f}$ appearing in Proposition 6.3.3 can both be computed recursively using the iterated Pieri rule (see [Ful98a, Proposition 14.6.1]). More specifically, for any integer $0 \leq k \leq e - r$, the Chern class $c_{e-r-k}(\mathcal{S}^\vee)$ represents the Schubert cycle corresponding to the partition $(1)^{e-r-k}$. According to the Pieri rule, multiplying this Schubert class by $c_{e-r-\ell}(\mathcal{S}^\vee)$ for some integer $0 \leq \ell \leq e - r$ yields a sum over Schubert classes indexed by those (valid) Young diagrams obtained by adding a total of $e - r - \ell$ boxes to the Young diagram corresponding to $(1)^{e-r-k}$, with at most one box added to each row.

6.3.3 AN EXAMPLE

Let us consider the case $f = 3, e = 4, r = 2, d_1 = d_2 = d_3 = 1$. We will compute both the (multi)degree and height of the determinantal resultant $\text{Res}_{4,3,2,(1,1,1)}$ associated to these parameters. Note first that this is actually a principal determinantal resultant. In fact, it is precisely the resultant whose multidegrees and height we computed in Section 6.2.3. The polynomials $\text{Res}_{4,3,2,(1,1,1)}$ and $\text{Res}_{3,4,2,(1,1,1,1)}$ are the same, though they are homogenised differently – one with respect to the coefficients of the rows of the corresponding indeterminate matrix and the other with respect to the coefficients of the columns. Proposition 6.2.2 shows immediately that the total degree of $\text{Res}_{3,4,2,(1,1,1,1)}$ is simply

$$\sum_{i=1}^4 \text{esym}_1^{(i)}(1, 1, 1) = 12.$$

It follows that $\deg_i(\text{Res}_{4,3,2,(1,1,1)}) = 4$ for each $1 \leq i \leq 3$. Let us verify this for $i = 1$ (and hence, for all $1 \leq i \leq 3$) using Proposition 6.3.2

We must consider tuples $0 \leq k_1, k_2, k_3 \leq 2$ such that $k_1 \leq 1$ and $k_1 + k_2 + k_3 = 1$. The only such tuples are $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$. We have

$$\mathcal{N}_{1,0,0}^{(1)} = \int_{\mathbb{G}(2, \mathcal{O}_S^{\oplus 4})_{\mathbb{Q}}} c_2(\mathcal{S}^\vee)^2$$

and

$$\mathcal{N}_{0,1,0}^{(1)} = \mathcal{N}_{0,0,1}^{(1)} = \int_{\mathbb{G}(2, \mathcal{O}_S^{\oplus 4})_{\mathbb{Q}}} c_1(\mathcal{S}^\vee)^2 c_2(\mathcal{S}^\vee).$$

The Pieri rule (see [Ful98a, Proposition 14.6.1]) shows us that⁵

$$c_1(\mathcal{S}^\vee)^2 c_2(\mathcal{S}^\vee) = c_2(\mathcal{S}^\vee)^2 = [\Sigma_{(2,2)}]$$

which is simply the class of a point in $\mathbb{G}(2, \mathcal{O}_S^{\oplus 4})_{\mathbb{Q}}$. Thus,

$$\mathcal{N}_{1,0,0}^{(1)} = \mathcal{N}_{0,1,0}^{(1)} = \mathcal{N}_{0,0,1}^{(1)} = 1 \quad (6.7)$$

and Proposition 6.3.2 correctly recovers $\deg_i(\text{Res}_{4,3,2,(1,1,1)}) = 4$ for all $1 \leq i \leq 3$.

According to Proposition 6.3.3, we must consider tuples $0 \leq k_1, k_2, k_3 \leq 2$ such that $k_1 + k_2 + k_3 = 1$ or $k_1 + k_2 + k_3 = 2$. Note first that both τ_{k_1, k_2, k_3} and $\widehat{\tau}_{k_1, k_2, k_3}$ are invariant under permutation of k_1, k_2, k_3 . We can therefore write

$$h(\text{div}(\text{Res}_{4,2,2,(1,1,1)})) = 3\widehat{\deg}(\widehat{\tau}_{1,0,0} \mid \mathbb{G}(2, \mathcal{O}_S^{\oplus 4})) + 3\sigma_1 \int_{\mathbb{G}(2, \mathcal{O}_S^{\oplus 4})_{\mathbb{Q}}} (\tau_{2,0,0} + \tau_{1,1,0}). \quad (6.8)$$

We have $\widehat{\tau}_{1,0,0} = \widehat{c}_1(\overline{\mathcal{S}}^\vee) \widehat{c}_2(\overline{\mathcal{S}}^\vee)^2$. As in Section 5.2.7, let $\pi : \mathbb{G}(2, \mathcal{O}_S^{\oplus 4}) \rightarrow S$ be the structure map of the Grassmann bundle, and let

$$\overline{\mathcal{E}} : 0 \rightarrow \overline{\mathcal{S}} \rightarrow \pi^* \overline{\mathcal{O}}_S^{\oplus 4} \rightarrow \overline{\mathcal{Q}} \rightarrow 0$$

be the tautological exact sequence of Hermitian vector bundles on $\mathbb{G}(2, \mathcal{O}_S^{\oplus 4})$. In the notation of Section 5.2.7,

$$\widehat{c}_1(\overline{\mathcal{S}}^\vee) = -\widehat{c}_1(\overline{\mathcal{S}}) = \widehat{c}_1(\overline{\mathcal{Q}} - \overline{\mathcal{E}}) = \widehat{c}_1(\overline{\mathcal{Q}})$$

and

$$\widehat{c}_2(\overline{\mathcal{S}}^\vee) = \widehat{c}_2(\overline{\mathcal{S}}) = \widehat{c}_1(\overline{\mathcal{Q}})^2 - \widehat{c}_2(\overline{\mathcal{Q}} - \overline{\mathcal{E}}).$$

We are left, then, to compute

$$\begin{aligned} \widehat{\deg}(\widehat{\tau}_{1,0,0} \mid \mathbb{G}(2, \mathcal{O}_S^{\oplus 4})) &= \widehat{\deg}(\widehat{c}_1(\overline{\mathcal{Q}})^5 \mid \mathbb{G}(2, \mathcal{O}_S^{\oplus 4})) \\ &\quad - 2\widehat{\deg}(\widehat{c}_1(\overline{\mathcal{Q}})^3 \widehat{c}_2(\overline{\mathcal{Q}} - \overline{\mathcal{E}}) \mid \mathbb{G}(2, \mathcal{O}_S^{\oplus 4})) \\ &\quad + \widehat{\deg}(\widehat{c}_1(\overline{\mathcal{Q}}) \widehat{c}_2(\overline{\mathcal{Q}} - \overline{\mathcal{E}})^2 \mid \mathbb{G}(2, \mathcal{O}_S^{\oplus 4})). \end{aligned} \quad (6.9)$$

⁵It may seem from this equality that $c_1(\mathcal{S}^\vee)^2 = c_2(\mathcal{S}^\vee)$. This is, of course, not true. There are two ways to add one box to the Young diagram corresponding to the partition (1) , yielding $c_1(\mathcal{S}^\vee)^2 = c_2(\mathcal{S}^\vee) + [\Sigma_{(1,1)}]$.

First, since $\overline{\mathcal{Q}}$ is the pullback of the hyperplane bundle (with its Fubini-Study metric) under the Plücker embedding of $\mathbb{G}(2, \mathcal{O}_S^{\oplus 4})$ into $\mathbb{P}_{\mathbb{Z}}^5$, the arithmetic degree $\widehat{\deg}(\widehat{c_1}(\overline{\mathcal{Q}})^5 \mid \mathbb{G}(2, \mathcal{O}_S^{\oplus 4}))$ is simply the Faltings height of the Grassmannian $\mathbb{G}(2, \mathcal{O}_S^{\oplus 4})$ in its Plücker embedding, which according to [Mai95, Theorem 6.0.6] (see also [Mai95, Section 7], [Tam99, Theorem 2], and [Tam99, Corollary 1]), we know to be

$$h_{\overline{\mathcal{O}_{\mathbb{P}_{\mathbb{Z}}^5}(1)}}(\mathbb{G}(2, \mathcal{O}_S^{\oplus 4})) = \frac{43}{6} = \frac{43}{3} \widehat{\deg}(a(c_{2,2}(\overline{\mathcal{Q}})) \mid \mathbb{G}(2, \mathcal{O}_S^{\oplus 4})). \quad (6.10)$$

Next, we compute $\widehat{c_1}(\overline{\mathcal{Q}}) \widehat{c_2}(\overline{\mathcal{Q}} - \overline{\mathcal{E}})$. Applying the arithmetic Pieri rule (see Theorem 5.2.10 and [Mai95, Corollary 5.2.2]) with $\lambda = 1$ and $m = 2$, we get

$$\widehat{c_1}(\overline{\mathcal{Q}}) \widehat{c_2}(\overline{\mathcal{Q}} - \overline{\mathcal{E}}) = \widehat{c_{2,1}}(\overline{\mathcal{Q}} - \overline{\mathcal{E}}) - \frac{1}{2} a(c_{1,1}(\overline{\mathcal{Q}})) + \frac{5}{2} a(c_2(\overline{\mathcal{Q}})). \quad (6.11)$$

Applying once more the arithmetic Pieri rule with $\lambda = (2, 1)$ and $m = 2$ gives

$$\widehat{c_{2,1}}(\overline{\mathcal{Q}} - \overline{\mathcal{E}}) \widehat{c_2}(\overline{\mathcal{Q}} - \overline{\mathcal{E}}) = a\left(\widetilde{N}_{(2,1),2}^{(2,2)} c_{2,2}(\overline{\mathcal{Q}})\right) = \frac{17}{6} a(c_{2,2}(\overline{\mathcal{Q}})). \quad (6.12)$$

Using Theorem 5.2.10,

$$\widehat{c_2}(\overline{\mathcal{Q}} - \overline{\mathcal{E}}) a(c_{1,1}(\overline{\mathcal{Q}})) = a\left(N_{2,(1,1)}^{(2,2)} c_{2,2}(\overline{\mathcal{Q}})\right) = 0 \quad (6.13)$$

and

$$\widehat{c_2}(\overline{\mathcal{Q}} - \overline{\mathcal{E}}) a(c_2(\overline{\mathcal{Q}})) = a\left(N_{2,2}^{(2,2)} c_{2,2}(\overline{\mathcal{Q}})\right) = a(c_{2,2}(\overline{\mathcal{Q}})). \quad (6.14)$$

Putting (6.11) to (6.14) together,

$$\widehat{c_1}(\overline{\mathcal{Q}}) \widehat{c_2}(\overline{\mathcal{Q}} - \overline{\mathcal{E}})^2 = \frac{16}{3} a(c_{2,2}(\overline{\mathcal{Q}})). \quad (6.15)$$

An analogous computation shows that

$$\widehat{c_1}(\overline{\mathcal{Q}})^3 \widehat{c_2}(\overline{\mathcal{Q}} - \overline{\mathcal{E}}) = \frac{49}{6} a(c_{2,2}(\overline{\mathcal{Q}})). \quad (6.16)$$

Substituting (6.10), (6.15) and (6.16) into (6.9) gives

$$3 \widehat{\deg}(\widehat{\tau}_{1,0,0} \mid \mathbb{G}(2, \mathcal{O}_S^{\oplus 4})) = 10 \widehat{\deg}(a(c_{2,2}(\overline{\mathcal{Q}})) \mid \mathbb{G}(2, \mathcal{O}_S^{\oplus 4})) = 5.$$

On the other hand, using (6.7),

$$\int_{\mathbb{G}(2, \mathcal{O}_S^{\oplus 4})_{\mathbb{Q}}} (\tau_{2,0,0} + \tau_{1,1,0}) = \int_{\mathbb{G}(2, \mathcal{O}_S^{\oplus 4})_{\mathbb{Q}}} \left(c_2(\mathcal{S}^{\vee})^2 + c_1(\mathcal{S}^{\vee})^2 c_2(\mathcal{S}^{\vee}) \right) = 2$$

so 6.3.3 shows that

$$h(\operatorname{div}(\operatorname{Res}_{4,3,2,(1,1,1)})) = 8.$$

Notice that Proposition 6.2.3 also gives

$$h(\operatorname{div}(\operatorname{Res}_{3,4,2,(1,1,1)})) = \binom{4}{2} \sigma_1 + \binom{4}{1} \sigma_2 = 8$$

as it should.

HEIGHTS OF DETERMINANTAL VARIETIES

6.3.4 HEIGHTS OF DETERMINANTAL VARIETIES

We conclude by combining our construction of the u -resultant with height bounds for the determinantal resultants to bound heights of determinantal varieties. Applying [KPS01, 1.2] and [KPS01, Lemma 1.1] immediately yields a bound on the bit sizes of the coefficients of the determinantal resultant.

LEMMA 6.3.5. — Let $e, f, r, d_1, \dots, d_f \in \mathbb{Z}_{>0}$ with $0 \leq r \leq \min\{e, f\}$, and let $N = (f - r)(e - r) - 1$. Let

$$m(\text{Res}_{e,f,r,(d_1,\dots,d_f)}) = \int_{(\prod_{i=1}^f \mathbb{P}_i)(\mathbb{C})} \log \|\text{Res}_{e,f,r,(d_1,\dots,d_f)}\| \cdot \prod_{i=1}^f \mu_i^{N_i}$$

be the Mahler measure of the determinantal resultant. Let $\mathcal{A} \subseteq \mathbb{Z}$ be the collection of coefficients of $\text{Res}_{e,f,r,(d_1,\dots,d_f)}$. Then

$$\begin{aligned} \log \max_{a \in \mathcal{A}} \{|a|\} &\geq m(\text{Res}_{e,f,r,(d_1,\dots,d_f)}) - \sum_{i=1}^f \mathcal{H}_{N_i} \deg_i \left(\text{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(\mathbb{P}_{\mathbb{Z}}^N) \right) \\ \log \max_{a \in \mathcal{A}} \{|a|\} &\leq m(\text{Res}_{e,f,r,(d_1,\dots,d_f)}) + \frac{3}{2} \sum_{i=1}^f \mathcal{H}_{N_i} \deg_i \left(\text{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(\mathbb{P}_{\mathbb{Z}}^N) \right). \end{aligned}$$

Bit size bounds of rational points on zero-dimensional determinantal varieties then follow immediately from Corollary 6.1.8, using [KPS01, Lemma 1.2(c)].

THEOREM 6.3.6. — Let $e, f, r, d_1, \dots, d_f \in \mathbb{Z}_{>0}$ with $0 \leq r \leq \min\{e, f\}$ and let $N = (f - r)(e - r) - 1$. Give $\mathbb{P}_{\mathbb{Q}}^N$ homogeneous coordinates $[X_0 : \dots : X_N]$. Let $\phi \in \text{Hom} \left(\mathcal{O}_{\mathbb{P}_{\mathbb{Q}}^N}^{\oplus e}, \bigoplus_{i=1}^f \mathcal{O}_{\mathbb{P}_{\mathbb{Q}}^N}(d_i) \right)$. Suppose that $M_r(\phi)$ is reduced and of dimension zero. Let τ be the maximum of the bit sizes of the coefficients of the entries of ϕ . Then for any $0 \leq j \leq N$,

$$\begin{aligned} \max_{p \in M_r(\phi)_{\mathbb{Q}} \cap D_+(X_j)} \{\log |p|\} &\leq m(\text{Res}_{e,f,r,(d_1,\dots,d_f)}) + \frac{3}{2} \sum_{i=1}^f \mathcal{H}_{N_i} \deg_i \left(\text{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(\mathbb{P}_{\mathbb{Z}}^N) \right) \\ &\quad + \sum_{i=1}^f \deg_i \left(\text{Ch}_{e,f,r,(d_1,\dots,d_f)}^{\det}(\mathbb{P}_{\mathbb{Z}}^N) \right) \left(\tau + \log \left(2 + \sum_{i=1}^f N_i \right) + d \log(N + 1) \right). \end{aligned}$$

BIBLIOGRAPHY

- [ABRW96] M.-E. Alonso, E. Becker, M. F. Roy, and T. Wörmann. Zeros, multiplicities, and idempotents for zero-dimensional systems. In Laureano González-Vega and Tomás Recio, editors, *Algorithms in Algebraic Geometry and Applications*, pages 1–15, Basel, 1996. Birkhäuser Basel.
- [BES21] Jérémy Berthomieu, Christian Eder, and Mohab Safey El Din. msolve: A Library for Solving Polynomial Systems. In *2021 International Symposium on Symbolic and Algebraic Computation*, 46th International Symposium on Symbolic and Algebraic Computation, pages 51–58, Saint Petersburg, Russia, July 2021. ACM.
- [BFS15] M. Bardet, J.-C. Faugère, and B. Salvy. On the complexity of the F5 Gröbner basis algorithm. *J. Symbolic Comput.*, 70:49–70, 2015.
- [BGS94] Jean-Benoît Bost, Henri Gillet, and Christophe Soulé. Heights of projective varieties and positive green forms. *Journal of the American Mathematical Society*, 7:903–1027, 1994.
- [BM93] Dave Bayer and David Mumford. What can be computed in algebraic geometry?, 1993.
- [BNS22] J. Berthomieu, V. Neiger, and M. Safey El Din. Faster change of order algorithm for Gröbner bases under shape and stability assumptions. In *Proceedings of ISSAC'2022*, 2022.
- [BSHW13] Daniel J. Bates, Andrew J. Sommese, Jonathan D. Hauenstein, and Charles W. Wampler. *Numerically Solving Polynomial Systems with Bertini*. Society for Industrial and Applied Mathematics, Philadelphia, PA, 2013.
- [BT18] Paul Breiding and Sascha Timme. Homotopycontinuation.jl: A package for homotopy continuation in Julia. In James H. Davenport, Manuel Kauers, George Labahn, and Josef Urban, editors, *Mathematical Software – ICMS 2018*, pages 458–465, Cham, 2018. Springer International Publishing.
- [Buc65] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, University of Innsbruck, 1965.
- [Bus04] Laurent Busé. Resultants of determinantal varieties. *Journal of Pure and Applied Algebra*, 193(1):71–97, 2004.
- [BV88] W. Bruns and U. Vetter. *Determinantal Rings*. Springer Berlin Heidelberg, 1988.
- [CLO05] D. A. Cox, J. Little, and D. O’Shea. *Using Algebraic Geometry*. Springer, 2005.
- [CLO15] D. A. Cox, J. Little, and D. O’Shea. *Ideals, Varieties, and Algorithms*. Springer, 2015.

BIBLIOGRAPHY

- [CvdW37] W.-L. Chow and B. L. van der Waerden. Zur algebraischen geometrie. IX. *Mathematische Annalen*, 113(1):692–704, Dec 1937.
- [Dee96] Todd Deery. Rev-lex segment ideals and minimal Betti numbers. In *The Curves Seminar at Queen's*, volume 10, pages 193–219, 1996.
- [DGP04] Jean-Guillaume Dumas, Pascal Giorgi, and Clément Pernet. FFPACK: Finite Field Linear Algebra Package. In *Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, ISSAC '04, page 119–126, New York, NY, USA, 2004. Association for Computing Machinery.
- [Dub90] Thomas W. Dubé. The structure of polynomial ideals and Gröbner bases. *SIAM Journal on Computing*, 19(4):750–773, 1990.
- [EF16] C. Eder and J.-C. Faugère. A survey on signature-based algorithms for computing Gröbner basis computations. *J. Symbolic Comput.*, pages 1–75, 2016.
- [EH16] David Eisenbud and Joe Harris. *3264 and All That: A Second Course in Algebraic Geometry*. Cambridge University Press, 2016.
- [Eis95] D. Eisenbud. *Commutative Algebra: with a View Toward Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1995.
- [Eis05] D. Eisenbud. *The geometry of syzygies: A second course in commutative algebra and algebraic geometry*, volume 229. Springer, 2005.
- [EN62] J. A. Eagon and D. G. Northcott. Ideals defined by matrices and a certain complex associated with them. *Proc. of the Royal Society of London*, 269(1337):188–204, 1962.
- [Fal83] Gerd Faltings. Endlichkeitssätze für abelsche varietäten über zahlkörpern. *Inventiones mathematicae*, 73(3):349–366, Oct 1983.
- [Fau99] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F4). *J. Pure Appl. Algebra*, 139(1):61–88, 1999.
- [Fau02] J.-C. Faugère. A new efficient algorithm for computing gröbner bases without reduction to zero (F5). In *Proceedings ISSAC 2002*, pages 75–83. ACM, 2002.
- [FM17] J.-C. Faugère and C. Mou. Sparse FGLM algorithms. *J. Symbolic Comput.*, 80(3):538–569, 2017.
- [Frö85] R. Fröberg. An inequality for Hilbert series of graded algebras. *Mathematica Sandinavica*, 56:117–144, Dec. 1985.
- [FSS13] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. On the complexity of the generalized MinRank problem. *J. Symbolic Comput.*, 55:30–58, 2013.
- [Ful98a] William Fulton. *Degeneracy Loci and Grassmannians*, pages 242–279. Springer New York, New York, NY, 1998.
- [Ful98b] William Fulton. *Intersection Theory*. Springer, New York, NY, 2 edition, June 1998.

- [Ful98c] William Fulton. *Intersections on Non-singular Varieties*, pages 130–152. Springer New York, New York, NY, 1998.
- [Ful98d] William Fulton. *Rational Equivalence*, pages 6–27. Springer New York, New York, NY, 1998.
- [Ful98e] William Fulton. *Vector Bundles and Chern Classes*, pages 47–69. Springer New York, New York, NY, 1998.
- [GD60] A. Grothendieck and J. Dieudonné. Éléments de géométrie algébrique. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 4(1):5–214, Jan 1960.
- [GH94a] Phillip Griffiths and Joseph Harris. *Foundational Material*, chapter 0, pages 1–127. In *Wiley Classics Library* [GH94c], August 1994.
- [GH94b] Phillip Griffiths and Joseph Harris. *Further Techniques*, chapter 3, pages 364–468. In *Wiley Classics Library* [GH94c], August 1994.
- [GH94c] Phillip Griffiths and Joseph Harris. *Principles of Algebraic Geometry*. Wiley Classics Library. John Wiley & Sons, Nashville, TN, August 1994.
- [GN72] T. H. Gulliksen and O. G. Negård. Un complexe résolvant pour certains idéaux déterminantiels. *C. R. Acad. Sci. Paris*, 274:16–18, 1972.
- [GNS23] S. Gopalakrishnan, V. Neiger, and M. Safey El Din. Refined F5 algorithms for ideals of minors of square matrices. In *Proceedings of ISSAC' 2023*, page 270–279, 2023.
- [GNS24] Sriram Gopalakrishnan, Vincent Neiger, and Mohab Safey El Din. Optimized Gröbner basis algorithms for maximal determinantal ideals and critical point computations. In *Proceedings of the 2024 International Symposium on Symbolic and Algebraic Computation*, ISSAC '24, page 400–409, New York, NY, USA, 2024. Association for Computing Machinery.
- [Gop25] Sriram Gopalakrishnan. On the arithmetic complexity of computing Gröbner bases of comaximal determinantal ideals. *Journal of Algebra*, 668:233–264, 2025.
- [Gro19] The FFLAS-FFPACK Group. *FFLAS-FFPACK: Finite Field Linear Algebra Sub-routines / Package*, v2.4.1 edition, 2019. <http://github.com/linbox-team/fflas-ffpack>.
- [GS90a] Henri Gillet and Christophe Soulé. Arithmetic intersection theory. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 72(1):94–174, Dec 1990.
- [GS90b] Henri Gillet and Christophe Soule. Characteristic classes for algebraic vector bundles with Hermitian metric, I. *Annals of Mathematics*, 131(1):163–203, 1990.
- [HMM⁺13a] Tadahito Harima, Toshiaki Maeno, Hideaki Morita, Yasuhide Numata, Akihito Wachi, and Junzo Watanabe. *k-Lefschetz Properties*, pages 171–188. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.
- [HMM⁺13b] Tadahito Harima, Toshiaki Maeno, Hideaki Morita, Yasuhide Numata, Akihito Wachi, and Junzo Watanabe. *Lefschetz Properties*, pages 97–140. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

BIBLIOGRAPHY

- [HSEDSV21] J. D. Hauenstein, M. Safey El Din, É. Schost, and T. X. Vu. Solving determinantal systems using homotopy techniques. *J. Symbolic Comput.*, 104:754–804, 2021.
- [JPS13] C.-P. Jeannerod, C. Pernet, and A. Storjohann. Rank-profile revealing Gaussian elimination and the CUP matrix decomposition. *J. Symbolic Comput.*, 56:46–68, 2013.
- [Kle74] Steven L. Kleiman. The transversality of a general translate. *Compositio Mathematica*, 28(3):287–297, 1974.
- [Kni95] Philip A. Knight. Fast rectangular matrix multiplication and QR decomposition. *Linear Algebra and its Applications*, 221:69–81, 1995.
- [KPS01] Teresa Krick, Luis Miguel Pardo, and Martín Sombra. Sharp estimates for the arithmetic Nullstellensatz. *Duke Mathematical Journal*, 109(3):521 – 598, 2001.
- [Kur89] K. Kurano. The first syzygies of determinantal ideals. *J. Algebra*, 124(2):414–436, 1989.
- [Laz83] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Proceedings EUROSAM 83*, pages 146–156. Springer, 1983.
- [Mai95] Vincent Maillot. Un calcul de Schubert arithmétique. *Duke Mathematical Journal*, 80(1):195 – 221, 1995.
- [Mat87] H. Matsumura. *Commutative Ring Theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1987.
- [MGH⁺05] Michael B. Monagan, Keith O. Geddes, K. Michael Heal, George Labahn, Stefan M. Vorkoetter, James McCarron, and Paul DeMarco. *Maple 10 Programming Guide*. Maplesoft, Waterloo ON, Canada, 2005.
- [ML95] Saunders Mac Lane. *Tensor and Torsion Products*, pages 138–172. Springer Berlin Heidelberg, Berlin, Heidelberg, 1995.
- [MM82] Ernst W Mayr and Albert R Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. *Advances in Mathematics*, 46(3):305–329, 1982.
- [MMR03] J. Migliore and R. M. Miró-Roig. Ideals of general forms and the ubiquity of the weak Lefschetz property. *Journal of Pure and Applied Algebra*, 182(1):79–107, 2003.
- [Nic17] L. Nicklasson. On the Hilbert series of ideals generated by generic forms. *Communications in Algebra*, 45(8):3390–3395, 2017.
- [Par10] Keith Pardue. Generic sequences of polynomials. *Journal of Algebra*, 324(4):579–590, 2010.
- [Rou99] Fabrice Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Applicable Algebra in Engineering, Communications and Computing*, 9(5):433 – 461, 1999.
- [Spa14] P.-J. Spaenlehauer. On the complexity of computing critical points with Gröbner bases. *SIAM J. Optim.*, 24(3):1382–1401, 2014.

- [Sto00] A. Storjohann. *Algorithms for Matrix Canonical Forms*. PhD thesis, Swiss Federal Institute of Technology – ETH, 2000.
- [SVW05] Andrew J. Sommese, Jan Verschelde, and Charles W. Wampler. *Introduction to numerical algebraic geometry*, pages 301–337. Springer Berlin Heidelberg, Berlin, Heidelberg, 2005.
- [Tam99] Harry Tamvakis. Schubert calculus on the arithmetic Grassmannian. *Duke Mathematical Journal*, 98(3):421 – 443, 1999.
- [The22] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.8.beta6)*, 2022. <https://www.sagemath.org>.
- [Ver99] Jan Verschelde. Algorithm 795: PHCpack: a general-purpose solver for polynomial systems by homotopy continuation. *ACM Trans. Math. Softw.*, 25(2):251–276, June 1999.
- [Yap91] Chee K. Yap. A new lower bound construction for commutative Thue systems with applications. *Journal of Symbolic Computation*, 12(1):1–27, 1991.