NP-hardness of testing equivalence to sparse polynomials and to constant-support polynomials

by

Omkar Baraskar

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Computer Science

Waterloo, Ontario, Canada, 2025

© Omkar Baraskar 2025

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

This work is conducted in collaboration with Agrim Dewan, Prof. Chandan Saha and Pulkit Sinha. It is based on the publication [BDSS24], which appeared in the proceedings of ICALP'24.

I solely authored Chapter 1 and 2, section 3.1 and 3.3. The rest of the work is co-authored with Agrim Dewan and Pulkit Sinha.

Abstract

Given a list of monomials of a n-variate polynomial $f \in \mathbb{F}[\mathbf{x}]$ and an integer s, decide whether there exists an invertible transform A and a $b \in \mathbb{F}^n$ such that $f(Ax + b)$ has less than s monomials. This problem is called the Equivalence testing to sparse polynomials (ETsparse). It was studied in [GK93] over $\mathbb{Q}$, in this work, they give an exponential in n^4 time algorithm for the problem. The lack of progress in the complexity of the problem over last three decades raises a question, is ETsparse hard? In this thesis we give an affirmative answer to the question by showing that it is NP-hard over any field.

Sparse orbit complexity of a polynomial f is the smallest integer s_0 such that there exists an invertible transform A such that $f(Ax)$ has s_0 monomials. Since ETsparse is NP-hard hence computing the sparse orbit complexity is also NP-hard. We also show that approximating the sparse orbit complexity upto a factor of $s_f^{1/3-\epsilon}$ for any $\epsilon \in (0, \frac{1}{3})$ is NP-hard, where s_f is the number of monomials in f. Interestingly, this approximation result has been shown without invoking the celebrated PCP theorem.

[CGS23] study a variant of the problem which focus on shift equivalence. More precisely, given $f \in \mathrm{R}[\mathbf{x}]$ (the input has the same representation as in ETsparse) and an integer s, does there exists a $b \in \mathrm{R}^n$ such that $f(x + b)$ has less than s monomials. It is called the SETsparse problem, [CGS23] showed that SETsparse is NP-hard when R is an integral domain which is not a field; we extend their result to the case when R is a field.

Finally, we also study the problem of testing equivalence to constant-support polynomials; more precisely, given a polynomial f as before and with support σ, does there exists a invertible transform A such that $f(Ax)$ has support $\sigma - 1$. We call this problem ETsupport. We show that ETsupport is NP-hard for $\sigma \geq 5$ and over any field.

Acknowledgements

I would like to express my gratitude towards my advisors Prof. Rafael Oliveira and Prof. Eric Schost for their exceptional supervision, guidance, and flexibility, especially as my research interests evolved. Their zeal for research and the sincerity with which they carry it out has been really inspiring for me. The reading group on Complexity Theory and several A&C talks organized by Rafael have exposed me to several other avenues of research.

The Algorithms and Complexity Lab has hosted a lot of pleasant memories for me - existential discussions, group lunches and dinner, and much more. A heartfelt thank you goes to my friends and colleagues, who have been my support system throughout this journey - Prashant, Vihan, Parth, Janani, Pulkit, Ipsita, Abhiroop, Matt, Denis, Amolak, Avantika and countless others whose names I regrettably cannot mention individually.

There are not enough words to express my gratitude to my parents, Anjali and Bhalchandra. Thank you for your endless sacrifices and for being my greatest pillar of support through the toughest times. To my sister, Aditi — thank you for being my constant cheerleader and my close friend, your love and humour has always been a joyful escape from this world. I am very grateful to have you all in my life.

Dedication

I would like to dedicate this work to my late grandmother, Shakuntala, whose blessings continue to guide me, and to my maternal grandparents, Vijay and Shalini, whose love and zest for life have been a constant source of joy for me.

I would also like to dedicate this work to my parents, Anjali and Bhalchandra, and my sister, Aditi. Their unwavering support and countless sacrifices have made this journey possible.

Table of Contents

Author's Declaration ii

Statement of Contributions iii

Abstract iv

Acknowledgements v

Dedication vi

1 Introduction 1

1.1 Our Results . . . 3

1.2 Discussion on Previous Work . . . 5

2 Preliminaries 7

2.1 Definitions and notations . . . 7

2.2 Algebraic preliminaries . . . 8

2.2.1 Degree separated polynomials . . . 8

2.2.2 Bounds on the sparsity of polynomials . . . 8

2.2.3 Bound on the support of polynomials . . . 10

3 NP-hardness of ETsparse 12

3.1 Inhomogenous Case . . . 12

3.1.1 Constructing f and s . . . 13

3.1.2 The forward direction . . . 16

3.1.3 The reverse direction . . . 17

3.2 Homogenous Case . . . 19
3.3 Extension to finite characteristic fields . . . 22
3.3.1 The non-homogeneous case . . . 22
3.3.2 Setting of parameters in the non-homogeneous case . . . 25
3.3.3 The homogeneous case . . . 25
3.3.4 Setting of parameters in the homogeneous case . . . 28
3.4 Extending Theorem 1 for translations . . . 29
3.4.1 Setting of parameters . . . 35

4 NP-hardness of α-gap-ETsparse **36**
4.1 Analyzing the gap: the non-homogeneous case . . . 36
4.2 Analyzing the gap: the homogeneous case . . . 38
4.3 Extension to finite characteristic fields . . . 40
4.3.1 The non-homogeneous case . . . 40
4.3.2 The homogeneous case . . . 44
4.4 Extending Theorem 2 for translations . . . 48
4.4.1 For characteristic 0 fields . . . 48
4.4.2 For finite characteristic fields . . . 50

5 NP-hardness of ETsupport **54**
5.1 Construction of f . . . 54
5.2 The forward direction . . . 57
5.3 The reverse direction . . . 57
5.4 Choosing the degrees . . . 59

References **61**

Chapter 1

Introduction

Given a field $\mathbb{F}$, an arithmetic circuit is a directed acyclic graph. It has three types of nodes: Input gates (in-degree 0 and are labelled by field elements), sum and product gates (these gates take field elements as input and output the result of the operation on the field elements), and output gate (these gates have out-degree 0). These are algebraic analogues of boolean circuits and are a widely used model of computation to study polynomials. With algebraic circuits, the three main categories of questions studied are

- Polynomial Identity Testing (PIT): Given an algebraic circuit of a polynomial f, determine whether f is the zero polynomial.
- Circuit Lower Bounds: Give an "explicit" polynomial which requires a super-polynomial size arithmetic circuit to compute.
- Circuit Reconstruction: Given a polynomial f[1] what is the smallest size arithmetic circuit computing f?

Interested readers can look at the following surveys: [LV24], [Sap], [SY10] and [CKW11].

In this thesis, we will study the problem of Equivalence Test (ET) for two families of polynomials, namely sparse and constant-support polynomials. The motivation to study this problem originates from a natural problem one can study about polynomials called the Polynomial Equivalence (PE) problem, which we discuss in more detail below.

Polynomial Equivalence (PE) and Equivalence Testing (ET): Given two polynomials $f, g \in \mathbb{F}[\mathbf{x}]$ as a list of their monomials, decide whether there exists an invertible transform A such that $f = g(Ax)$. This problem is known as the Polynomial Equivalence (PE) problem. Equivalently, it is asking whether f can be obtained from g after a change of

[1]Here f is either given explicitly or oracle access to input-output evaluations of the polynomials

coordinates; hence PE can be seen as an algebraic analogue of the Graph Isomorphism (GI) problem. In fact, [AS05] and [Kay11] show that PE is as hard as GI. But neither do we know if it is polynomially equivalent to GI nor if it is NP-hard. Over finite field, [Sax06] and [Thi98] show that PE is in AM $\cap$ co-AM hence not NP-hard unless PH collapses. Over $\mathbb{Q}$, it is not even known if the problem is decidable.

Since not much is known about the complexity of PE, a natural variant of the problem is being studied in the literature to gain further insight. In this variant, we fix a polynomial family $\mathscr{F}$, and we ask the following question: Given f as a list of monomials, does there exist an invertible transform A such that $f(Ax)$ belongs to $\mathscr{F}$. This problem is called the Equivalence Testing (ET) for $\mathscr{F}$.

[Kay11] and [Kay12b] introduced this problem and gave randomised polynomial time equivalence test for Determinants, Permanents, Elementary and Power Symmetric polynomials over $\mathbb{C}$. Following this result randomised polynomial time algorithms were given for Iterated Matrix Multiplication (IMM) [KNST17], Read once formulas[2] [GST23] and several other polynomial classes as mentioned in more detail in section 1.2.

In the previous work on ET, no hardness result was known. A potential reason for this is as follows, most of the polynomial families for which ET was studied had the following property: When you fix the number of variables of the input f, there exists a unique polynomial $g \in \mathscr{F}$ which can be equivalent to f for example say f is n-variate then there is a unique polynomial in the Determinant family namely $\mathrm{Det}_{n\times n}$ which can be equivalent to f. Moreover, g also has a polynomial sized circuit. Now, if we assume the input to the ET algorithm is given as a circuit, then this problem reduces to PE in the case both inputs are given as circuits; this version of PE is known to be in AM $\cap$ co-AM hence not NP-hard unless PH collapses. The polynomial families which do not satisfy the above property are the Read-once formulas and t-design polynomials with t constant (a dense subclass of homogeneous depth-3 circuits); this is because there might be multiple polynomials in the family which can be equivalent to f as they are polynomial families derived from circuit classes. Hence, the natural question which arises is, what is the complexity of ET for the simplest circuit class? The simplest circuits are the depth-2 circuits, also known as the sparse polynomial.

Sparse Polynomials We say a n-variate degree d polynomial is s-sparse if it has at most s monomials. It is easy to see that the class of polynomials computed by a depth-2 arithmetic circuit with top fan-in bounded by s is precisely the set of s-sparse polynomials. Sparse polynomials have been widely studied in algebraic complexity theory in the context of identity testing, factorisation, and interpolation; interested readers can look at [Roc18]. Moreover, ET has been previously studied for sparse polynomials over $\mathbb{Q}$ in [GK93]. In this work, they give an algorithm exponential in n^4. The lack of progress on

[2]Equivalence Testing for a circuit class $\mathscr{C}$ is defined as the Equivalence test for a polynomial family $\mathscr{F}$ where $\mathscr{F}$ is the set of all polynomials computable by circuits class $\mathscr{C}$

the complexity over the last three decades gives another reason to study the problem and believe that it might be hard to solve. ET for sparse polynomials also has connections with *MCSP for depth three circuits*; a detailed exposition on this can be found in [BDSS24].

Constant-support polynomials ET is efficiently solvable for two special sparse polynomial families, namely the power symmetric polynomial $\mathsf{PSym} := x_1^d + \ldots + x_n^d$ [Kay11] and the sum-product polynomial $\mathsf{SP} := \sum_{i\in[s]} \prod_{j\in[d]} x_{i,j}$ [MS21, Kay11]. What makes ET easy for these sparse polynomials? Explanations were provided in [GST23, BDS24]: SP is a read-once formula; it is also a 1-design polynomial. PSym is a 1-design polynomial, but it is also a support-1 polynomial. It is natural to wonder about the complexity of ET for constant-support polynomials. In Theorem 3, we show that checking if a given f is in the orbit of a support-5 polynomial is NP-hard; this answers the question in the negative.

Model of Computation We will specify the model of computation we will be working with over different fields. Over finite fields and $\mathbb{Q}$ we will be working with the turing model. Over characteristic 0 fields, we will consider an arithmetic model of computation which allows to store a field element in unit space and perform an arithmetic operation in unit time.

1.1 Our Results

We now state our results formally. The ETsparse problem is defined as follows.

Problem 1.1.1 (ETsparse)**.** Given a polynomial $f \in \mathbb{F}[\mathbf{x}]$ in its sparse representation and an integer s, check if there exist an $A \in \mathrm{GL}(|\mathbf{x}|, \mathbb{F})$ and a $\mathbf{b} \in \mathbb{F}^{|\mathbf{x}|}$ such that $f(A\mathbf{x} + \mathbf{b})$ is s-sparse.

Our first result, Theorem 1, shows the NP-hardness of ETsparse over any field.

Theorem 1 (ETsparse is NP-hard)**.** *1. Let $\mathbb{F}$ be any field. There is a deterministic polynomial-time many-one reduction from* 3-SAT *to* ETsparse *over $\mathbb{F}$.*

2. Let $\mathbb{F}$ be any field. There is a deterministic polynomial-time many-one reduction from 3-SAT *to* ETsparse *over $\mathbb{F}$ where the input polynomial to the* ETsparse *problem is homogeneous.*

Here are a few remarks on theorem 1

1. Part 2 of the theorem subsumes part 1. We state parts 1 and 2 separately for two reasons: One, part 1 has simpler proof. Two, the degree parameters in the proof of part 1 have a better upper bound in comparison to that in the proof of part 2.

2. When $\mathrm{char}(\mathbb{F}) \neq 2$ then the reduction is *natural* and has the feature that a satisfying assignment can be mapped to a sparsifying invertible $A \in \{-1,0,1\}^{|\mathbf{x}|\times|\mathbf{x}|}$ and vice versa. So, ETsparse is NP-hard even when A is restricted to having only $\{-1,0,1\}$ entries.

3. The authors of [BDS24] gave a randomised polynomial-time ET algorithm for *random*[3] sparse polynomials, assuming black-box access to the input. Such average-case results for hard problems are not unusual; for example, [DF89] gave polynomial-time algorithms for average cases of NP-hard problems like Graph 3-colorability.

Problem 1.1.2 (α-gap-ETsparse)**.** Let $\alpha > 1$ be a parameter. Given a polynomial $f \in \mathbb{F}[\mathbf{x}]$ in its sparse representation and an integer s_0, output:

- YES, if there exist an $A \in \mathrm{GL}(|\mathbf{x}|, \mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^{|\mathbf{x}|}$ such that $f(A\mathbf{x}+\mathbf{b})$ is s_0-sparse.
- NO, if for all $A \in \mathrm{GL}(|\mathbf{x}|, \mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^{|\mathbf{x}|}$, $f(A\mathbf{x}+\mathbf{b})$ has sparsity at least αs_0.

Our second result, Theorem 2, shows that α-gap-ETsparse is NP-hard for $\alpha = s^{\frac{1}{3}-\epsilon}$, where s is the sparsity of the input polynomial f and $\epsilon \in (0, \frac{1}{3})$ is an arbitrary constant.

Theorem 2 ($s^{\frac{1}{3}}$-gap-ETsparse is NP-hard)**.** *Let $\epsilon \in (0, \frac{1}{3})$ be an arbitrary constant.*

1. *Let $\mathbb{F}$ be any field. There exists a deterministic polynomial-time many-one reduction from* 3-SAT *to* $s^{\frac{1}{3}-\epsilon}$-gap-ETsparse *over $\mathbb{F}$ where the input polynomial in* $s^{\frac{1}{3}-\epsilon}$-gap-ETsparse *is s-sparse.*

2. *Let $\mathbb{F}$ be any field. There exists a deterministic polynomial-time many-one reduction from* 3-SAT *to* $s^{\frac{1}{3}-\epsilon}$-gap-ETsparse *over $\mathbb{F}$ where the input polynomial in* $s^{\frac{1}{3}-\epsilon}$-gap-ETsparse *is homogeneous and s-sparse.*

Here are a few remarks on theorem 2

1. Again as in theorem 1 part 2 subsumes part 1.

2. An interesting feature of the reduction is that it does not invoke the celebrated PCP theorem. Moreover, it is the same reduction as in theorem 1, hence, the reduction is natural when $\mathrm{char}(\mathbb{F}) \neq 2$.

Definition 1.1.1 (Sparse orbit complexity of a polynomial)**.** The smallest s_0 for which f is in the orbit of an s_0-sparse polynomial is the sparse orbit complexity of f.

[3] A random s-sparse degree-d polynomial in their work was defined to be a polynomial where each monomial is formed independently of the others by selecting d variables uniformly at random from the variable set; the coefficients are allowed to be arbitrary.

Theorem 1 shows that computing the sparse complexity of a polynomial is NP-hard. As a corollary of theorem 2, we will show that approximating the sparse complexity of a polynomial is also NP-hard.

Corollary 1.1.1. Let $0 < \epsilon < \frac{1}{3}$ be an arbitrary constant.

1. Let $\mathbb{F}$ be any field. It is NP-hard to compute $s^{\frac{1}{3}-\epsilon}$ factor approximation of the sparse-orbit complexity when the input is an s-sparse polynomial over $\mathbb{F}$.

2. Let $\mathbb{F}$ be any field. It is NP-hard to compute $s^{\frac{1}{3}-\epsilon}$ factor approximation of the sparse-orbit complexity when the input is an s-sparse homogeneous polynomial over $\mathbb{F}$.

Now, we formally define the support of a polynomial.

Definition 1.1.2 (Support of a polynomial)**.** For a monomial $\mathbf{x}^{\boldsymbol{\alpha}}$, where $\boldsymbol{\alpha}$ is the exponent vector, the support of $\mathbf{x}^{\boldsymbol{\alpha}}$, $\mathrm{Supp}(\mathbf{x}^{\boldsymbol{\alpha}})$, is the number of variables with non-zero exponent. The support of a polynomial f, $\mathrm{Supp}(f)$, is the maximum support size over all the monomials of f.

Thus, a polynomial has support σ if there exists a monomial with support σ and no other monomial has support $> \sigma$. The ET problem for constant-support polynomials and a stronger version of it are defined next (henceforth, σ is assumed to be a constant).

Problem 1.1.3 (ETsupport)**.** Given a polynomial $f \in \mathbb{F}[\mathbf{x}]$ in its sparse representation and an integer σ, check if there exists an $A \in \mathrm{GL}(|\mathbf{x}|, \mathbb{F})$ such that $\mathrm{Supp}(f(A\mathbf{x})) \leq \sigma$.

Problem 1.1.4 ($(\sigma+1)$-to-σ ETsupport)**.** Given a polynomial $f \in \mathbb{F}[\mathbf{x}]$ with support $\sigma+1$ in its sparse representation, check if there exists an $A \in \mathrm{GL}(|\mathbf{x}|, \mathbb{F})$ such that $\mathrm{Supp}(f(A\mathbf{x})) \leq \sigma$.

One small difference in the definition here is that we consider invertible transformations not affine transformations, this is because translation does not change support of a polynomial. In our third result, Theorem 3, shows that ETsupport and $(\sigma+1)$-to-σ ETsupport are NP-hard.

Theorem 3 (ETsupport is NP-hard)**.** *Let $\sigma \geq 6$ be a constant and $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) = 0$ or $> \sigma+1$. There is a deterministic polynomial-time many-one reduction from* 3-SAT *to* ETsupport *over $\mathbb{F}$. In particular,* 3-SAT *reduces to* $(\sigma+1)$-to-σ ETsupport *in deterministic polynomial time.*

1.2 Discussion on Previous Work

Previous work on PE: [Sax06] shows that PE for quadratic polynomials can be solved in polynomial time given access to an integer factoring oracle. On the other hand, [AS05]

shows that Cubic form equivalence (CFE) is known to be as hard as GI. [BDS24] gave an explicit class of polynomials for which PE is polynomially equivalent to GI.

A variant of PE is the Shift Equivalence Testing problem (SET) where given two n-variate polynomials f and g, one needs to check if there exists $\mathbf{b} \in \mathbb{F}^n$ such that $f(\mathbf{x}) = g(\mathbf{x} + \mathbf{b})$. The author of [Gri97] gave a deterministic algorithm over characteristic 0 fields, a randomised algorithm over prime residue fields and a quantum algorithm over characteristic 2 fields for SET. All these algorithms have running time polynomial in the dense representation of the input, that is, for n-variate, degree-d polynomials given in the verbose representation as input, the running time is $\text{poly}(\binom{n+d}{d})$. The authors of [DdOS14] gave a randomised algorithm for SET assuming black-box access to n-variate polynomials f and g with degree bound d and circuit size bound s. Their algorithm runs in $\text{poly}(n, d, s)$ time. Another randomised polynomial-time algorithm for SET is given in [Kay12a].

Previous work on ET: As mentioned before, the study of ET was initiated in [Kay11] where efficient ET algorithms were given for the power symmetric and the elementary symmetric polynomials. Following this, efficient ET algorithms were given for several other important polynomial families and circuit classes such as the permanent [Kay12a], the determinant [Kay12a, Gro12, GGKS19], the iterated matrix multiplication (IMM) polynomial [KNST19, MNS20], the continuant polynomial [MS21], read-once formulas (ROFs) [GST23], and design polynomials [BDS24, GS19].

Chapter 2

Preliminaries

In this section, first, we will define some notation and terms which we will be using throughout the thesis. Later, we give some bounds on sparsity and support of polynomials, which will be key for the proofs.

2.1 Definitions and notations

For $n, a, b \in \mathbb{N}$, $[n]$ denotes the set $\{1, 2 \ldots, n\}$ and $[a, b]$ denotes the integers from a to b, both inclusive. A polynomial is *homogeneous* if all its monomials have the same total degree. The set of invertible linear transforms in n variables over a field $\mathbb{F}$ is denoted by $\mathrm{GL}(n, \mathbb{F})$. For a polynomial $f \in \mathbb{F}[\mathbf{x}]$, the action of a linear transform $A \in \mathbb{F}^{|\mathbf{x}| \times |\mathbf{x}|}$ on its variables is denoted by $f(A\mathbf{x})$ as well as by $A(f)$. The *sparsity* of a polynomial f, denoted as $\mathcal{S}(f)$, is the number of monomials in f with non-zero coefficients. For a polynomial f, $\mathrm{var}(f)$ denotes the set of variables that occur in at least one monomial of f. We have used the notation $f \sim g$ earlier to denote $f = g(A\mathbf{x} + \mathbf{b})$. Henceforth, we will ignore the translation vector $\mathbf{b}$ in the main body of the discussion for simplicity but mention the necessary changes in the proofs or point to appropriate sections when translations are involved. Thus, for polynomials f and g, $f \sim g$ will mean $f(\mathbf{x}) = g(A\mathbf{x})$ where $A \in \mathrm{GL}(|\mathbf{x}|, \mathbb{F})$. Similarly, the *orbit* of a polynomial f will denote the set $\{f(A\mathbf{x}), A \in \mathrm{GL}(|\mathbf{x}|, \mathbb{F})\}$. The *degree* of a monomial is its total degree, and the degree of a polynomial f is the maximum degree amongst all monomials in f. The x-degree of a monomial is the degree of the variable x in the monomial.

Definition 2.1.1 (Degree separated polynomials)**.** Polynomials f and g are *degree separated* if no monomial of f has the same degree as a monomial of g. Similarly, f and g are degree separated *with respect to a variable* x if no monomial of f has the same x-degree as a monomial of g.

The *set of degrees* of a polynomial is the set of distinct degrees of all the monomials in the polynomial. For example, the set of degrees of $f(x_1, x_2) = x_1^2 + x_1x_2 + 4x_2$ is $\{2, 1\}$.

A *linear form* is a homogeneous degree one polynomial. An *affine form* is a degree one polynomial.

2.2 Algebraic preliminaries

2.2.1 Degree separated polynomials

Observation 2.2.1. Let f and g be polynomials such that $f \sim g$. Then, f and g have the same set of degrees for the monomials. Thus, if f and g are degree separated, then $f \not\sim g$.

Proof. Under any invertible linear transform applied to the variables of f, every monomial of f maps to a linear combination of monomials of the same degree. Thus, no new degree can be added to the set of degrees of f under any invertible linear transform. As $f \sim g$, the set of degrees of f is contained in the set of degrees of g, and vice versa, implying the two sets are the same. □

Observation 2.2.2. If f and g are degree separated (or degree separated with respect to some variable), then $\mathcal{S}(f+g) = \mathcal{S}(f) + \mathcal{S}(g)$.

Proof. As f and g are degree separated (or degree separated with respect to some variable), each monomial of $f+g$ is a monomial of f or g, but not both. □

Observation 2.2.3. If f and g are degree separated, $f_1 \sim f$ and $g_1 \sim g$, then $\mathcal{S}(f_1+g_1) = \mathcal{S}(f_1) + \mathcal{S}(g_1)$.

Proof. As $f_1 \sim f$ and $g_1 \sim g$, therefore f_1 and g_1 are degree separated by Observation 2.2.1. By Observation 2.2.2, the statement holds. □

2.2.2 Bounds on the sparsity of polynomials

Observation 2.2.4 analyzes the sparsity of powers of linear forms. Observation 2.2.5 is a special case of Observation 2.2.4 and is stated separately because it is simpler and is invoked many times. Observation 2.2.6 analyzes the sparsity of powers of affine forms.

Observation 2.2.4. Let ℓ be a linear form in m variables and $d \in \mathbb{N}$. If $\text{char}(\mathbb{F}) = 0$, $\mathcal{S}(\ell^d) = \binom{d+m-1}{m-1}$, and if $\text{char}(\mathbb{F}) = p$, $\mathcal{S}(\ell^d) = \prod_{i=0}^{k} \binom{e_i+m-1}{m-1}$, where $d = \sum_{i=0}^{k} e_i p^i$, $e_i \in [0, p-1]$.

Proof. Without loss of generality, let $\ell = \sum_{i=1}^{m} c_i x_i$ where $c_i \in \mathbb{F}\backslash\{0\}$. If $\text{char}(\mathbb{F}) = 0$, then $\mathcal{S}(\ell^d) = \binom{d+m-1}{m-1}$ follows from the multinomial theorem and the fact that the number

of monomials of degree d in m variables is $\binom{d+m-1}{m-1}$. Suppose $\mathrm{char}(\mathbb{F}) = p$. Then, d is expressible as in the observation statement. It will be shown by induction on k that,

$$\mathcal{S}(\ell^d) = \prod_{i=0}^{k} \binom{e_i + m - 1}{m-1}.$$

In the base case $k = 0$, $d < p$ and, like the $\mathrm{char}(\mathbb{F}) = 0$ case, it easily follows that $\mathcal{S}(\ell^d) = \binom{d+m-1}{m-1}$. Assume the statement for all $j < k$. Suppose $d = e_k p^k + \sum_{i=0}^{k-1} e_i p^i$, where $0 < e_k < p$. Then, using the fact that $(\sum_{j=1}^{m} c_j x_j)^p = \sum_{j=1}^{m} c_j^p x_j^p$ over $\mathbb{F}$,

$$\ell^d = \Big(\sum_{j=1}^{m} c_j x_j\Big)^{\sum_{i=0}^{k} e_i p^i} = \Big(\sum_{j=1}^{m} c_j^{p^k} x_j^{p^k}\Big)^{e_k} \prod_{i=0}^{k-1} \Big(\sum_{j=1}^{m} c_j^{p^i} x_j^{p^i}\Big)^{e_i}.$$

Let $h = \prod_{i=0}^{k-1} (\sum_{j=1}^{m} c_j^{p^i} x_j^{p^i})^{e_i}$. Note,

$$\Big(\sum_{j=1}^{m} c_j^{p^k} x_j^{p^k}\Big)^{e_k} = \sum_{\alpha_1 + \cdots + \alpha_m = e_k} \binom{e_k}{\alpha_1 \ldots \alpha_m} \Big(\prod_{i=1}^{m} (c_i^{p^k} x_i^{p^k})^{\alpha_i}\Big).$$

By the inductive hypothesis, $\mathcal{S}(h) = \prod_{i=0}^{k-1} \binom{e_i+m-1}{m-1}$, while $\mathcal{S}((\sum_{j=1}^{m} c_j^{p^k} x_j^{p^k})^{e_k}) = \binom{e_k+m-1}{m-1}$, as $e_k < p$. Now,

$$\ell^d = \sum_{\alpha_1 + \cdots + \alpha_m = e_k} \binom{e_k}{\alpha_1 \ldots \alpha_m} \Big(\prod_{i=1}^{m} (c_i^{p^k} x_i^{p^k})^{\alpha_i}\Big) \cdot h.$$

The degree of $h < p^k$, while any two monomials in the above expansion are degree separated by at least p^k in at least one variable. Consequently, by Observation 2.2.2, $\mathcal{S}(\ell^d) = \prod_{i=0}^{k} \binom{e_i+m-1}{m-1}$. The above inductive argument is similar to the multinomial version of Lucas's theorem. □

Observation 2.2.5. If $\mathrm{char}(\mathbb{F}) = 0$ and ℓ be a linear form in exactly two variables, then $\mathcal{S}(\ell^d) = d + 1$. The result holds for characteristic p fields if $p > d$ or if $d = p^k - 1$ for some $k \in \mathbb{N}$. Further, if ℓ is a linear form in more than two variables and d is as before, then $\mathcal{S}(\ell^d) \geq d + 1$.

Proof. Let ℓ be a linear form in exactly 2 variables. When $\mathrm{char}(\mathbb{F}) = 0$, then by Observation 2.2.4, $\mathcal{S}(\ell^d) = \binom{d+2-1}{2-1} = d + 1$. When $\mathrm{char}(\mathbb{F}) = p$, then $\mathcal{S}(\ell^d) = \prod_{i=0}^{k-1} \binom{e_i+2-1}{2-1} = \prod_{i=0}^{k-1} (e_i + 1)$, where $d = \sum_{i=0}^{k-1} e_i p^i$. It is easy to see the observation holds when $d < p$. When $d = p^k - 1 = \sum_{i=0}^{k-1} (p-1) p^i$, then $\prod_{i=0}^{k-1} (e_i + 1) = p^k = d + 1$. Finally, when ℓ is a linear form in $m \geq 2$ variables, then the observation follows from the fact that $\binom{c+m-1}{m-1} \geq c + 1$ for any $c \in \mathbb{N}$. □

Observation 2.2.6. Let $h = \ell + c_0$, where ℓ is a linear form in at least one variable and $c_0 \in \mathbb{F} \setminus \{0\}$, then $\mathcal{S}(h^d) \geq \mathcal{S}(\ell^d) + 1$. More precisely, $\mathcal{S}(h^d) \geq d + 1$ holds if $\mathrm{char}(\mathbb{F}) = 0$ or if $\mathrm{char}(\mathbb{F}) = p$ and $p > d$ or $d = p^k - 1$ for some $k \in \mathbb{N}$.

Proof. Using the binomial theorem,

$$h^d = \ell^d + c_0^d + \sum_{i=1}^{d-1} \binom{d}{i} c_0^i \ell^{d-i}.$$

As the degree of every monomial in ℓ^{d-i} is $d-i$, all the summands in the above expansion are degree separated. From Observations 2.2.2 and 2.2.5, it holds that $\mathcal{S}(h^d) \geq \mathcal{S}(\ell^d) + 1$. More precisely, $\mathcal{S}(h^d) \geq d+1$, as $\mathcal{S}(\ell^{d-i}) \geq 1$ and $\binom{d}{i} \neq 0$ for d as in the observation statement (by Lucas's theorem). □

Claim 2.2.1 analyzes the sparsity of polynomials divisible by a power of some linear form in at least two variables and is used to prove part two of Theorems 1 and 2. Claim 2.2.2 analyzes the support of monomials under invertible linear transforms and is used to prove Theorem 3.

Claim 2.2.1. Let $\text{char}(\mathbb{F}) = 0$. If $f \in \mathbb{F}[\mathbf{x}]$ is a non-zero polynomial divisible by ℓ^d for some linear form ℓ in at least two variables, then $\mathcal{S}(f) \geq d+1$. The claim also holds for characteristic p fields, where the degree of f is less than p.

Proof. We prove this by induction on d. For the base case $d = 0$, it is easy to see that the sparsity of any non-zero polynomial is at least 1. Suppose now the result holds for all $k < d$. Let $\ell = \sum_{i=1}^n c_i x_i$ and $f = \ell^d h$. Without loss of generality, assume f is not divisible by any variable, for if it were divisible by some variable x_i, then x_i must not divide ℓ as ℓ contains at least two distinct variables and hence x_i divides h, in which case we can replace f and h by $\frac{f}{x_i}$ and $\frac{h}{x_i}$ respectively. Let x_j be a variable in ℓ with a non-zero coefficient and consider $\frac{\partial f}{\partial x_j}$. Now,

$$\mathcal{S}(f) \geq 1 + \mathcal{S}\left(\frac{\partial f}{\partial x_j}\right)$$

as the derivative map either sends monomials to distinct monomials or eliminates them, and by assumption some monomial in f is not divisible by x_j and will be eliminated. As $f = \ell^d h$,

$$\frac{\partial f}{\partial x_j} = c_j d \ell^{d-1} h + \ell^d \frac{\partial h}{\partial x_j}.$$

Clearly, ℓ^{d-1} divides $\frac{\partial f}{\partial x_j}$. By induction, $\mathcal{S}(\frac{\partial f}{\partial x_j}) \geq d$. Hence, $\mathcal{S}(f) \geq 1 + \mathcal{S}(\frac{\partial f}{\partial x_j}) \geq d+1$. □

2.2.3 Bound on the support of polynomials

Claim 2.2.2. Let $\sigma, d, n \in \mathbb{N}$, $d \geq \sigma$, $f = (x_1 \cdots x_n)^d$, and $\ell_1, \ldots, \ell_n$ be linearly independent linear forms in $x_1, \ldots, x_n$. If $|\cup_{i=1}^n \text{var}(\ell_i)| \geq \sigma$ and $g := f(\ell_1 \cdots \ell_n)$, then $\text{Supp}(g) \geq \sigma$.

The claim holds if $\mathrm{char}(\mathbb{F}) = 0$, or $\mathrm{char}(\mathbb{F}) = p$ with $p > d$, or $p > \sigma$ and $d = p^k - 1$ for some $k \in \mathbb{N}$.

Proof. The claim is first proven for $n = 1$. Thus, $g = \ell^d$ where $\ell = \sum_{i=1}^{|\mathrm{var}(\ell)|} c_i x_i$, $c_i \neq 0$, and $|\mathrm{var}(\ell)| \geq \sigma$, without loss of generality. Note that

$$\frac{\partial^\sigma g}{\partial x_1 \cdots \partial x_\sigma} = \sigma! \binom{d}{\sigma} c_1 c_2 \cdots c_\sigma \ell^{d-\sigma}.$$

Clearly, $\sigma!\binom{d}{\sigma} \neq 0$ when $\mathrm{char}(\mathbb{F}) = 0$. When $\mathrm{char}(\mathbb{F}) = p$ with $p > d$, or $p > \sigma$ and $d = p^k - 1$ for some $k \in \mathbb{N}$, this follows by Lucas's Theorem [Luc78]. So the derivative is non-zero, as $d \geq \sigma$, implying there exists a monomial of support at least σ in g.

Now, for arbitrary n, $g = (\ell_1 \cdots \ell_n)^d$, where $|\cup_{i=1}^n \mathrm{var}(\ell_i)| \geq \sigma$. Observe that

$$\frac{\partial^\sigma g}{\partial x_{i_1} \cdots \partial x_{i_\sigma}} = \sum_{\substack{j_1 + \cdots + j_n = \sigma \\ j_i \geq 0}} c_{j_1, \cdots, j_n} \cdot \frac{\partial^\sigma (\ell_1^{j_1} \cdots \ell_n^{j_n})}{\partial x_{i_1} \cdots \partial x_{i_\sigma}} \cdot (\ell_1^{d-j_1} \cdots \ell_n^{d-j_n})$$

where $c_{j_1 \cdots j_n} = \binom{d}{j_1} \cdots \binom{d}{j_n}$. Clearly, when $\mathrm{char}(\mathbb{F}) = 0$ or $> d$, $c_{j_1, \cdots, j_n} \neq 0$. When $\mathrm{char}(\mathbb{F}) = p$ and $d = p^k - 1$ for some $k \in \mathbb{N}$, then by Lucas's Theorem, all the binomial coefficients are non-zero. Hence $c_{j_1, \cdots, j_n} \neq 0$. Observe that the elements of the set $\mathscr{M} := \{\ell_1^{d-j_1} \cdots \ell_n^{d-j_n} \mid j_1 + \cdots + j_n = \sigma, \ \ j_i \geq 0\}$ are linearly independent as the ℓ_i's are linearly independent and $d \geq \sigma$. Also, $\frac{\partial^\sigma (\ell_1^{j_1} \cdots \ell_n^{j_n})}{\partial x_{i_1} \cdots \partial x_{i_\sigma}} \in \mathbb{F}$ as $j_1 + \cdots + j_n = \sigma$. It suffices to show that for some choice of $j_1, \ldots, j_n$ and $x_{i_1}, \ldots, x_{i_\sigma}$,where $i_1, \ldots, i_\sigma$ are pairwise distinct, $\frac{\partial^\sigma (\ell_1^{j_1} \cdots \ell_n^{j_n})}{\partial x_{i_1} \cdots \partial x_{i_\sigma}} \neq 0$. As elements of $\mathscr{M}$ are linearly independent and $c_{j_1 \cdots j_n} \neq 0$, this would imply $\frac{\partial^\sigma g}{\partial x_{i_1} \cdots \partial x_{i_\sigma}} \neq 0$, indicating that $\mathrm{Supp}(g) \geq \sigma$.

For every $i \geq 1$, define $S_i := \mathrm{var}(\ell_i) \setminus \cup_{j=1}^{i-1} S_j$ if $|\cup_{j=1}^{i} S_j| < \sigma$ else choose $S_i \subseteq \mathrm{var}(\ell_i) \setminus \cup_{j=1}^{i-1} S_j$ such that $|\cup_{j=1}^{i} S_j| = \sigma$; here, $\cup_{j=1}^{i-1} S_j = \emptyset$ for $i = 1$. Note that such a collection of sets always exists as $|\cup_{i=1}^{n} \mathrm{var}(\ell_i)| \geq \sigma$. Say we choose $m \leq n$ such non-empty sets. Let $j_i := |S_i|$ and $S_i := \{x_{i1}, \ldots, x_{ij_i}\}$. Hence,

$$\frac{\partial^\sigma (\ell_1^{j_1} \cdots \ell_m^{j_m})}{(\partial x_{11} \cdots \partial x_{1j_1}) \cdots (\partial x_{m1} \cdots \partial x_{mj_m})} = \prod_{i=1}^{m} \frac{\partial^{j_i} \ell_i^{j_i}}{\partial x_{i1} \cdots \partial x_{ij_i}}.$$

As $\{x_{i1}, \ldots, x_{ij_i}\} \subseteq \mathrm{var}(\ell_i)$ is not empty and $j_i \leq \sigma < p$ (in case of finite characteristic fields), by the analysis of the $n = 1$ case, $\frac{\partial^{j_i} \ell_i^{j_i}}{\partial x_{i1} \cdots \partial x_{ij_i}} \neq 0$. Hence,

$$\frac{\partial^\sigma (\ell_1^{j_1} \cdots \ell_m^{j_m})}{(\partial x_{11} \cdots \partial x_{1j_1}) \cdots (\partial x_{m1} \cdots \partial x_{mj_m})} \neq 0$$

and $\mathrm{Supp}(g) \geq \sigma$. □

Chapter 3

NP-hardness of ETsparse

In this chapter, we will prove theorem 1. In section 3.1, we prove the theorem for the inhomogenous case, to provide more clarity in the proof we introduce an additional notation after observation 3.1.1, so it is encouraged to not skip past remark 3.1.1. A similar convention is followed in section 3.3.1, here we extend the theorem for the non-homogenous case to finite characteristic fields. In section 3.2 we prove the theorem for the homogenous case. The proof provided in both the sections ignore translation for ease of understanding, later in section 3.4, we will show how to handle translations.

3.1 Inhomogenous Case

Proof Sketch. Given a $\psi \in$ 3SAT with n variables and m clauses we want a (f, s) such that ψ is satisfiable if and only if there exists some invertible A such that $\mathscr{S}(f(Ax)) < s$. Our idea is to define a $2n+1$ variate polynomial f as the sum of two sets of polynomials denoted by $\{Q_i\}_{i=1,\ldots,n}$ and $\{R_i\}_{i=1,\ldots,m}$. The polynomials $\sum_{i=1}^{n} Q_i$ and $\sum_{i=1}^{m} R_i$ are degree-separated, hence by observation 2.2.2 and 2.2.3 we can understand the sparsity of f by analyzing the sparsities of $\sum_{i=1}^{n} Q_i$ and $\sum_{i=1}^{m} R_i$ separately.

We wish to define Q_i's such that there exists a set $\mathscr{A} \subset \mathrm{GL}(2n+1, \mathbb{F})$ of size $(2n!) \cdot 2^n$, such that $\mathscr{S}(\sum_{i=1}^{n} Q_i(Ax)) \ll \mathscr{S}(\sum_{i=1}^{n} Q_i(x))$ if and only if $A \in \mathscr{A}$. One must ignore the $2n!$ factor in the size of $\mathscr{A}$ as it arises because of Permutation Matrices (since the sparsity of a polynomial does not change on permutation of its variables). Ignoring these permutation matrices, we can form a one-to-one mapping between $\mathscr{A}$ and the set of all boolean assignments that is $\{0,1\}^n$. This mapping is the first key step in the reduction, and in the next paragraph we show that with our choice of Q_i's we can get a lot of structure in the one-to-one map.

For the i-th variable in the 3SAT formula, we introduce a bi-variate polynomial $Q_i(x_i, y_i)$ as shown in section 3.1.1. This satisfies the following property: Let A be a linear transformation which maps $x_i \mapsto x_i$ and $y_i \mapsto x_i \pm y_i$ then $\mathscr{S}(Q_i(A(x_i, y_i))) \ll \mathscr{S}(Q_i(x_i, y_i))$;

moreover for any other linear map A which maps x_i, y_i to some other linear polynomials we have $\mathcal{S}(Q_i(A(x_i, y_i))) \gg \mathcal{S}(Q_i(x_i, y_i))$. We also ensure that the degrees of polynomials Q_i's are pairwise disjoint so by observation 2.2.2 and 2.2.3 the sparsity of $\sum_{i=1}^{n} Q_i$ decreases when $x_i \mapsto x_i$ and $y_i \mapsto x_i \pm y_i$ for all $i \in [n]$, for every other linear map it explodes. Hence it is easy to see that $\mathscr{A} = \prod_{i=1}^{n} \{x_i \mapsto x_i \text{ and } y_i \mapsto x_i \pm y_i\}$, here we again ignore the permutation matrices. Intuitively, we want to associate the linear transformation which maps $y_i \mapsto y_i + x_i$ with the assignment where the i-th variable is set to True, and similarly $y_i \mapsto y_i - x_i$ with the assignment where the i-th variable is set to False. Note that the boolean assignment of the i-th variable corresponding to an element of $\mathscr{A}$ solely depends on which of $A(y_i + x_i)$ or $A(y_i - x_i)$ is variable, and this is a permutation invariant decision thus we can safely ignore permutation matrices.

Note that till now we haven't discussed what the value of s should be. Trivially, we want $s < \mathcal{S}(f(x))$; otherwise, the identity transformation will be a viable sparsifying transform[1]. Secondly, we want sparsifying transforms to be a subset of $\mathscr{A}$, we ensure this by setting $s < \mathcal{S}((\sum_{i=1}^{n} Q_i)(Ax))$ for all $A \notin \mathscr{A}$ as shown in lemma 3.1.3.

We have a one-to-one correspondence between viable sparsifying transforms and $\{0,1\}^n$; we now define polynomials R_k's as shown in section 3.1.1. Every R_k satisfies the property that whenever the k-th clause is not satisfied, for every $A \in \mathscr{A}$ we have $\mathcal{S}(\sum_{i=1}^{n} Q_i(Ax) + R_k(Ax)) > s$ as shown in proposition 3.1.2. Finally we want to ensure that when there is a satisfying assignment for ψ there is a sparsifying transform, as shown in section .

3.1.1 Constructing f and s

Let ψ be a 3-CNF in variables $\mathbf{x} := \{x_1, x_2 \dots x_n\}$ and m clauses:

$$\psi = \wedge_{k=1}^{m} \vee_{j \in C_k} (x_j \oplus a_{k,j}),$$

where C_k denotes the set of indices of the variables in the k^{th} clause and $a_{k,j} \in \{0,1\}$. Let $\mathbf{y} := \{y_1, y_2 \dots y_n\}$, x_0 be a new variable and $\mathbf{z} := \{x_0\} \sqcup \mathbf{x} \sqcup \mathbf{y}$. For $d_1, d_2, d_3, d_4 \in \mathbb{N}$, consider the following polynomials:

- Corresponding to variable x_i, where $i \in [n]$, define $Q_i(\mathbf{z})$ as:

  $$Q_i(\mathbf{z}) := Q_{i,1}(\mathbf{z}) + Q_{i,2}(\mathbf{z}) + Q_{i,3}(\mathbf{z}), \text{ where}$$
  $$Q_{i,1}(\mathbf{z}) := x_0^{(3i-2)d_1} x_i^{d_2},\ Q_{i,2}(\mathbf{z}) := x_0^{(3i-1)d_1}(y_i + x_i)^{d_3} \text{ and } Q_{i,3}(\mathbf{z}) := x_0^{3id_1}(y_i - x_i)^{d_3}.$$

  Intuitively, $Q_{i,2}$ and $Q_{i,3}$ correspond to assigning 0 and 1, respectively, to x_i in ψ. $Q_{i,1}$ is used to establish a mapping between satisfying assignments and sparsifying transforms.

[1] We call A to be a sparsifying transform iff $\mathcal{S}(f(Ax)) < s$

- For the k^{th} clause, $k \in [m]$, define $R_k(\mathbf{z}) := x_0^{(3n+k)d_1} \prod_{j \in C_k} (y_j + (-1)^{a_{k,j}} x_j)^{d_4}$.

Define $s := 1 + n(3 + d_3) + m(d_4 + 1)^2$ and the polynomial f as:

$$f(\mathbf{z}) := x_0^{d_1} + \sum_{i=1}^{n} Q_i(\mathbf{z}) + \sum_{k=1}^{m} R_k(\mathbf{z}). \tag{3.1}$$

The following conditions are imposed on the d_i's:

$$d_1 \geq \max(s, d_2 + 1),\ d_2 \geq 2d_3,\ d_3 \geq m(d_4 + 1)^2 + 1, \text{ and } d_4 \geq m. \tag{3.2}$$

For characteristic 0 fields, the inequalities of (3.2) can be converted to equalities. Thus, we get

$$\begin{aligned} &d_4 = m,\ d_3 = m(m+1)^2 + 1 = O(m^3) \implies s = O(nm^3) \\ &d_2 = 2m(m+1)^2 + 2 = O(m^3),\ d_1 = 1 + n(4 + m(m+1)^2) + m(m+1)^2 = O(nm^3). \end{aligned} \tag{3.3}$$

Note, for the above choices of d_3 and d_2, $s \geq d_2 + 1$. Hence, d_1 is set to s. Under the conditions of (3.2) the following observations hold.

Observation 3.1.1. For all $i \in [n]$, $k \in [m]$, the polynomials $x_0^{d_1}$, $Q_{i,1}(\mathbf{z})$, $Q_{i,2}(\mathbf{z})$, $Q_{i,3}(\mathbf{z})$ and $R_k(\mathbf{z})$ are degree separated from one another. Also, $Q_i(\mathbf{z})$ is degree separated from other $Q_j(\mathbf{z})$'s, for $i, j \in [n]$ and $i \neq j$. Similarly, $R_k(\mathbf{z})$ is degree separated from $R_l(\mathbf{z})$ for $k, l \in [m]$ and $k \neq l$.

Proof. Let $i \in [n]$. Note that $Q_{i,1}(\mathbf{z})$ has degree $(3i-2)d_1 + d_2$, $Q_{i,2}(\mathbf{z})$ has degree $(3i-1)d_1 + d_3$ and $Q_{i,3}(\mathbf{z})$ has degree $3id_1 + d_3$. Clearly $3id_1 + d_3 > (3i-1)d_1 + d_3$. Also, $(3i-1)d_1 + d_3 > (3i-2)d_1 + d_2$ because $d_1 > d_2 > d_2 - d_3$ by the conditions in (3.2). Thus, $Q_{i,1}(\mathbf{z})$, $Q_{i,2}(\mathbf{z})$ and $Q_{i,3}(\mathbf{z})$ are degree separated and Q_i is a sum of 3 degree separated polynomials and has degree $3id_1 + d_3$.

Now, let $i \in [n]$ and $k \in [m]$. $R_k(\mathbf{z})$ is a polynomial of degree $(3n+k)d_1 + 3d_4$ while the degree of $Q_i(\mathbf{z})$ is $3id_1 + d_3$. Note that

$$(3n+k)d_1 + 3d_4 \geq (3n+1)d_1 + 3d_4 > 3nd_1 + d_3 \geq 3id_1 + d_3,$$

where the second inequality holds because $d_1 > d_3$ by the constraints in (3.2). Therefore, $R_k(\mathbf{z})$ and $Q_i(\mathbf{z})$ (hence also $Q_{i,1}$, $Q_{i,2}$ and $Q_{i,3}$) are degree separated from one another. Further, the degree of $R_k(\mathbf{z})$ and that of $Q_i(\mathbf{z})$ are greater than d_1 implying $x_0^{d_1}$ is degree separated from $R_k(\mathbf{z})$ and $Q_i(\mathbf{z})$.

Lastly, let $i, j \in [n]$ where $i < j$ without loss of generality. The highest degree of a monomial in $Q_i(\mathbf{z})$ is $3id_1 + d_3$, while the lowest degree of a monomial in $Q_j(\mathbf{z})$ is $(3j-2)d_1 + d_2$. Now,

$$(3j-2)d_1 + d_2 \geq (3i+1)d_1 + d_2 > 3id_1 + d_3$$

as $j \geq i+1$ and $d_1 > d_2 > d_3$ by the conditions in (3.2). Thus, Q_i and Q_j are degree separated. That $R_k(\mathbf{z})$ is degree separated from $R_l(\mathbf{z})$ for $k, l \in [n]$ and $k \neq l$ can be observed from the fact that the degree of $R_k(\mathbf{z})$ is $(3n+k)d_1 + 3d_4$. □

Remarks. Observation 3.1.1 shows that the $3n+m+1$ polynomials are degree separated. The choice of powers of x_0 in each one of the polynomial was made in order to obtain this degree separation. Furthermore other than providing this degree separation they do not serve any other purpose in section 3.1, hence we will replace the powers of x_0 by a $\star$ and will reference observation 3.1.1 whenever necessary.

Observation 3.1.2. The degree of f is $(3n+m)d_1 + 3d_4 = (mn)^{O(1)}$.

Proof. From the definition of f in (3.1), it follows that the degree of f is the maximum of that of $x_0^{d_1}$, Q_i and R_k , where $i \in [n]$ and $k \in [m]$. As observed in the proof of Observation 3.1.1, degree of Q_i is $3id_1 + d_3$, degree of R_k is $(3n+k)d_1 + 3d_4$ and $(3n+k)d_1 + 3d_4 > 3id_1 + d_3 > d_1$. Since $k \leq m$, therefore the highest degree is $(3n+m)d_1 + 3d_4$. So, the degree of f is $(3n+m)d_1 + 3d_4$. □

Observation 3.1.3. $\mathcal{S}(f(\mathbf{z})) = 1 + n(2d_3+3) + m(d_4+1)^3$ and $\mathrm{Supp}(f) = 7$.

Proof. By Observation 3.1.1, f is a sum of the $n+m+1$ degree separated polynomials $x_0^{d_1}$, Q_i and R_k, where $i \in [n]$ and $k \in [m]$. Applying Observation 2.2.5 (for linear forms in two variables over $\mathrm{char}(\mathbb{F}) = 0$ fields) to $Q_{i,2}$ and $Q_{i,3}$ and Observation 2.2.2 to Q_i, we get

$$\mathcal{S}(Q_i(\mathbf{z})) = \mathcal{S}(Q_{i,1}(\mathbf{z})) + \mathcal{S}(Q_{i,2}(\mathbf{z})) + \mathcal{S}(Q_{i,3}(\mathbf{z})) = 2d_3 + 3, \ \ \forall i \in [n].$$

By Observation 2.2.5 (for linear forms in two variables over $\mathrm{char}(\mathbb{F}) = 0$ fields) and the assumption that each clause in ψ has 3 distinct variables, we get that:

$$\mathcal{S}(R_k(\mathbf{z})) = \mathcal{S}(x_0^\star) \prod_{j \in C_k} \mathcal{S}((y_j + (-1)^{a_{k,j}} x_j)^{d_4}) = (d_4+1)^3 \ \ \forall k \in [m].$$

Finally, applying Observations 3.1.1 and 2.2.2 to f gives

$$\mathcal{S}(f(\mathbf{z})) = \mathcal{S}(x_0^\star) + \sum_{i=1}^{n} \mathcal{S}(Q_i(\mathbf{z})) + \sum_{k=1}^{m} \mathcal{S}(R_k(\mathbf{z})) = 1 + n(2d_3+3) + m(d_4+1)^3.$$

Thus, $\mathcal{S}(f(\mathbf{z})) > s$ but also $(mn)^{O(1)}$.

For the support of f, note that $\mathrm{Supp}(R_k) = 7$ for all $k \in [m]$ while $\mathrm{Supp}(Q_i) = 3$ for all $i \in [n]$ and $\mathrm{Supp}(x_0^{d_1}) = 1$. By Observation 3.1.1, $\mathrm{Supp}(f) = \mathrm{Supp}(R_k) = 7$. □

3.1.2 The forward direction

Proposition 3.1.1 shows how a satisfiable ψ implies the existence of an invertible A, such that $\mathcal{S}(f(A\mathbf{z})) \leq s$ by constructing A from a satisfying assignment $\mathbf{u} \in \{0,1\}^n$ of ψ.

Proposition 3.1.1. Let $\mathbf{u} = (u_1, \ldots, u_n) \in \{0,1\}^n$ be such that $\psi(\mathbf{u}) = 1$. Then $\mathcal{S}(f(A\mathbf{z})) \leq s$, where A is as:

$$A : x_0 \mapsto x_0, x_i \mapsto x_i, y_i \mapsto y_i + (-1)^{u_i} x_i, \quad \forall i \in [n]. \tag{3.4}$$

Proof. It follows from the definition of f in (3.1), Observations 3.1.1 and 2.2.3 that

$$\mathcal{S}(f(A\mathbf{z})) = \mathcal{S}(A(x_0^\star)) + \sum_{i=1}^{n} \mathcal{S}(Q_i(A\mathbf{z})) + \sum_{k=1}^{m} \mathcal{S}(R_k(A\mathbf{z})).$$

Thus, it suffices to analyze the sparsity of $A(x_0^{d_1})$, $Q_i(A\mathbf{z})$'s and $R_k(A\mathbf{z})$'s. Now, $\mathcal{S}(A(x_0^{d_1})) = 1$ as $A(x_0^{d_1}) = x_0^{d_1}$. We now analyze $\mathcal{S}(Q_i(A\mathbf{z}))$ for $i \in [n]$. If $u_i = 0$, then

$$Q_{i,1}(A\mathbf{z}) = x_0^\star x_i^{d_2},\ Q_{i,2}(A\mathbf{z}) = x_0^\star (y_i + 2x_i)^{d_3} \text{ and } Q_{i,3}(A\mathbf{z}) = x_0^\star y_i^{d_3}.$$

If $u_i = 1$, then

$$Q_{i,1}(A\mathbf{z}) = x_0^\star x_i^{d_2},\ Q_{i,2}(A\mathbf{z}) = x_0^\star y_i^{d_3} \text{ and } Q_{i,3}(A\mathbf{z}) = x_0^\star (y_i - 2x_i)^{d_3}.$$

By Observation 2.2.5 (for linear forms in two variables over characteristic 0 fields), if $u_i = 0$ then $\mathcal{S}(Q_{i,2}(A\mathbf{z})) = d_3 + 1$ and $\mathcal{S}(Q_{i,3}(A\mathbf{z})) = 1$ and, if $u_i = 1$ then $\mathcal{S}(Q_{i,2}(A\mathbf{z})) = 1$ and $\mathcal{S}(Q_{i,3}(A\mathbf{z})) = d_3 + 1$. In either case, by Observations 3.1.1 and 2.2.3,

$$\mathcal{S}(Q_i(A\mathbf{z})) = \mathcal{S}(Q_{i,1}(A\mathbf{z})) + \mathcal{S}(Q_{i,2}(A\mathbf{z})) + \mathcal{S}(Q_{i,3}(A\mathbf{z})) = d_3 + 3.$$

For the k^{th} clause, $k \in [m]$, the action of A on the corresponding polynomial R_k is:

$$R_k(A\mathbf{z}) = x_0^\star \prod_{j \in C_k} (y_j + ((-1)^{a_{k,j}} + (-1)^{u_j}) x_j)^{d_4}.$$

As the multiplicands in $R_k(A\mathbf{z})$ do not share any variables, $\mathcal{S}(R_k(A\mathbf{z}))$ is the product of the sparsity of the multiplicands. Since $\psi(\mathbf{u}) = 1$, therefore in the k^{th} clause there exists $j \in C_k$ such that $a_{k,j} \neq u_j$. For that j, $(y_j + ((-1)^{a_{k,j}} + (-1)^{u_j}) x_j)^{d_4} = y_j^{d_4}$. As at least one literal is true in every clause under $\mathbf{u}$, $\mathcal{S}(R_k(A\mathbf{z})) \leq (d_4 + 1)^2$ using Observation 2.2.5. Thus,

$$\mathcal{S}(f(A\mathbf{z})) = \mathcal{S}(A(x_0^\star)) + \sum_{i=1}^{n} \mathcal{S}(Q_i(A\mathbf{z})) + \sum_{k=1}^{m} \mathcal{S}(R_k(A\mathbf{z})) \leq 1 + n(d_3+3) + m(d_4+1)^2 = s.$$

□

3.1.3 The reverse direction

Now, we show that $(f, s) \in$ ETsparse implies $\psi \in$ 3-SAT by showing that the permuted and scaled versions of the transform of (3.4) form all the viable sparsifying invertible linear transforms. This is where the constraints on the d_i's are used. So, let $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ be such that $\mathcal{S}(f(A\mathbf{z})) \leq s$. Lemma 3.1.1 shows that $A(x_0)$ is just a variable by leveraging $d_1 \geq s$.

Lemma 3.1.1. Without loss of generality, $A(x_0) = x_0$.

Proof. If $A(x_0)$ is a linear form in at least two variables, then it follows from the definition of f in (3.1), Observation 3.1.1, Observation 2.2.5 applied on $A(x_0^{d_1})$, Observation 2.2.3, and the constraint $d_1 \geq s$ in (3.2) that $\mathcal{S}(f(A\mathbf{z})) > \mathcal{S}(A(x_0^{d_1})) \geq d_1 + 1 > s$, a contradiction. Hence, $A(x_0)$ has only one variable. By multiplying A with a permutation and a scaling matrix, we can assume without loss of generality that $A(x_0) = x_0$. This can be assumed because permutation and non-zero scaling of variables do not affect the sparsity of a polynomial. □

The proof of Lemma 3.1.2 uses $d_2 \geq 2d_3$ while that of Lemma 3.1.3 uses $d_3 \geq m(d_4 + 1)^2 + 1$.

Lemma 3.1.2. For any invertible A and $i \in [n]$:

$$\mathcal{S}(Q_i(A\mathbf{z})) = \mathcal{S}(Q_{i,1}(A\mathbf{z})) + \mathcal{S}(Q_{i,2}(A\mathbf{z})) + \mathcal{S}(Q_{i,3}(A\mathbf{z})) \geq d_3 + 3,$$

where Q_i, $Q_{i,1}$, $Q_{i,2}$ and $Q_{i,3}$ are as defined in Section 3.1.1. Equality holds if and only if under A

$$x_i \mapsto X_i \text{ and } y_i \mapsto Y_i + (-1)^{u_i} X_i$$

for some scaled variables $X_i, Y_i \in \mathbf{z}$ and $u_i \in \{0, 1\}$. Further, if $\mathcal{S}(Q_i(A\mathbf{z})) \neq d_3 + 3$, then $\mathcal{S}(Q_i(A\mathbf{z})) \geq 2d_3 + 3$.

Proof. It follows from Observations 3.1.1 and 2.2.3 that for any $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$, $\mathcal{S}(Q_i(A\mathbf{z})) = \mathcal{S}(Q_{i,1}(A\mathbf{z})) + \mathcal{S}(Q_{i,2}(A\mathbf{z})) + \mathcal{S}(Q_{i,3}(A\mathbf{z}))$, where Q_i is as described in Section 3.1.1. Now, the if direction in the lemma statement is easy to verify. For the only if direction, consider the following cases of A:

1. $\mathcal{S}(A(x_i)) \geq 2$: It follows from Observation 2.2.5 and $d_2 \geq 2d_3$ that $\mathcal{S}(Q_{i,1}(A\mathbf{z})) \geq d_2 + 1 \geq 2d_3 + 1$. Also, $\mathcal{S}(Q_{i,2}(A\mathbf{z})) \geq 1$ and $\mathcal{S}(Q_{i,3}(A\mathbf{z})) \geq 1$. Thus, $\mathcal{S}(Q_i(A\mathbf{z})) \geq d_2 + 3 \geq 2d_3 + 3$.

2. $\mathcal{S}(A(x_i)) = 1$, $\mathcal{S}(A(y_i + x_i)) \geq 2$ and $\mathcal{S}(A(y_i - x_i)) \geq 2$: It follows from Observation 2.2.5 that $\mathcal{S}(Q_{i,2}(A\mathbf{z})) \geq d_3 + 1$ and $\mathcal{S}(Q_{i,3}(A\mathbf{z})) \geq d_3 + 1$ implying $\mathcal{S}(Q_i(A\mathbf{z})) \geq 2d_3 + 3$.

3. $\mathcal{S}(A(x_i)) = 1$ with $\mathcal{S}(A(y_i + x_i)) = 1$ or $\mathcal{S}(A(y_i - x_i)) = 1$: Let $A(x_i) = X_i$ for some scaled variable $X_i \in \mathbf{z}$. Because A is invertible exactly one of $\mathcal{S}(A(y_i + x_i)) = 1$ or $\mathcal{S}(A(y_i - x_i)) = 1$ holds true. Let $\mathcal{S}(A(y_i + x_i)) = 1$, without loss of generality. Then, it must be that $A(y_i) = Y_i - X_i$ for some scaled variable $Y_i \in \mathbf{z}$. Thus, $A(y_i - x_i) = Y_i - 2X_i$. Hence, $\mathcal{S}(Q_{i,1}(A\mathbf{z})) = 1$, $\mathcal{S}(Q_{i,2}(A\mathbf{z})) = 1$ and $\mathcal{S}(Q_{i,3}(A\mathbf{z})) = d_3 + 1$ (by Observation 2.2.5) implying $\mathcal{S}(Q_i(A\mathbf{z})) = d_3 + 3$.

The first two cases show that if A is not as per the lemma statement, then $\mathcal{S}(Q_i(A\mathbf{z})) \geq 2d_3 + 3$; otherwise, $\mathcal{S}(Q_i(A\mathbf{z})) = d_3 + 3$. □

Lemma 3.1.3. Under the given A, $\mathcal{S}(Q_i(A\mathbf{z})) = d_3 + 3$ holds for all $i \in [n]$.

Proof. Suppose $\mathcal{S}(Q_j(A\mathbf{z})) \neq d_3 + 3$ for some $j \in [n]$. Then, $\mathcal{S}(Q_j(A\mathbf{z})) \geq 2d_3 + 3$ by Lemma 3.1.2. By the definition of f in (3.1), Observations 3.1.1 and 2.2.3 and the condition $d_3 \geq m(d_4 + 1)^2 + 1$, we get the following contradiction:

$$\begin{aligned}\mathcal{S}(f(A\mathbf{z})) &> \mathcal{S}(A(x_0^\star)) + \sum_{i=1, i\neq j}^{n} \mathcal{S}(Q_i(A\mathbf{z})) + \mathcal{S}(Q_j(A\mathbf{z})) \geq 1 + (n-1)(3+d_3) + (3+2d_3) \\ &= 1 + n(3+d_3) + d_3 = s - m(d_4+1)^2 + d_3 > s.\end{aligned}$$

□

Lemmas 3.1.1, 3.1.2 and 3.1.3 together show that A is a permuted scaled version of the transform of (3.4). We can assume A to be as described in (3.4) without loss of generality as permutation and non-zero scaling of variables do not affect the sparsity of a polynomial. Proposition 3.1.2 shows how a satisfying assignment can be derived from A using $d_4 \geq m$.

Proposition 3.1.2. With A as described in (3.4), $\mathbf{u} = (u_1, \ldots, u_n)$ is a satisfying assignment for ψ.

Proof. Suppose not; then there exists $k \in [m]$ such that the k^{th} clause, $\vee_{j \in C_k}(x_j \oplus a_{k,j})$, in ψ is unsatisfied. Since this clause is unsatisfied, $u_j = a_{k,j}$ for all $j \in C_k$. Thus, $R_k(A\mathbf{z}) = x_0^{(3n+k)d_1} \prod_{j \in C_k}(y_j \pm 2x_j)^{d_4}$, where R_k is as defined in Section 3.1.1, and $\mathcal{S}(R_k(A\mathbf{z})) = (d_4 + 1)^3 \geq (m+1)(d_4+1)^2$ by Observation 2.2.5, the fact that $R_k(A\mathbf{z})$ is a product of linear forms not sharing variables, and the condition $d_4 \geq m$. By the definition of f and s in Section 3.1.1, Observations 3.1.1 and 2.2.3, it holds that

$$\begin{aligned}\mathcal{S}(f(A\mathbf{z})) &\geq \mathcal{S}(A(x_0)^\star) + \sum_{i=1}^{n} \mathcal{S}(Q_i(A\mathbf{z})) + \mathcal{S}(R_k(A\mathbf{z})) \\ &\geq 1 + n(3+d_3) + m(d_4+1)^2 + (d_4+1)^2 = s + (d_4+1)^2 > s,\end{aligned}$$

a contradiction. Thus, $\mathbf{u}$ is a satisfying assignment for ψ. □

3.2 Homogenous Case

We show a modification of the construction in Section 3.1.1 which, along with arguments similar to those in Sections 3.1.2 and 3.1.3, can be used to prove Theorem 1 for homogeneous polynomials over characteristic 0 fields. Because the polynomials are homogeneous, we cannot use degree separation like in the non-homogeneous case. Instead, we introduce a new variable y_0, a new degree parameter $d_5 \in \mathbb{N}$, and redefine $Q_i(\mathbf{z})$ and $R_k(\mathbf{z})$ of Section 3.1.1 along with modified constraints on the d_i's so that:

1. Each polynomial is homogeneous with the same degree and is divisible by $x_0^{d_1}$ and $y_0^{d_2}$.
2. Each polynomial has a distinct x_0 degree.

The divisibility condition ensures that both x_0 and y_0 map to scaled variables under a sparsifying invertible linear transform (see Lemma 3.2.1 and its proof). Due to the second condition, the polynomials are degree separated with respect to x_0 (see Observation 3.2.1). This fact is used to show that, under a sparsifying invertible linear transform, the polynomials are degree separated with respect to x_0 (see Lemma 3.2.2 and its proof). Formally, let x_0, $\mathbf{x}$ and $\mathbf{y}$ be as defined in Section 3.1.1 and y_0 be a new variable. Define $\mathbf{z} := \mathbf{x} \sqcup \mathbf{y} \sqcup \{x_0\} \sqcup \{y_0\}$. Let $d_1, d_2, d_3, d_4, d_5 \in \mathbb{N}$. Consider the following polynomials:

1. For each variable x_i, $i \in [n]$, define $Q_i(\mathbf{z}) := Q_{i,1}(\mathbf{z}) + Q_{i,2}(\mathbf{z}) + Q_{i,3}(\mathbf{z})$, where

$$\begin{aligned}
Q_{i,1}(\mathbf{z}) &:= x_0^{d_1+(3i-2)(d_3+1)} y_0^{d_2+(3n+m-3i+3)(d_3+1)-d_3} x_i^{d_3}, \\
Q_{i,2}(\mathbf{z}) &:= x_0^{d_1+(3i-1)(d_3+1)} y_0^{d_2+(3n+m-3i+2)(d_3+1)-d_4} (y_i + x_i)^{d_4}, \\
Q_{i,3}(\mathbf{z}) &:= x_0^{d_1+3i(d_3+1)} y_0^{d_2+(3n+m-3i+1)(d_3+1)-d_4} (y_i - x_i)^{d_4}.
\end{aligned}$$

2. For the k^{th} clause, $k \in [m]$, define

$$R_k(\mathbf{z}) := x_0^{d_1+(3n+k)(d_3+1)} y_0^{d_2+(m-k+1)(d_3+1)-3d_5} \prod_{j \in C_k} (y_j + (-1)^{a_{k,j}} x_j)^{d_5}.$$

Define $s := 1 + n(d_4 + 3) + m(d_5 + 1)^2$ and impose the following conditions on the d_i's:

$$\begin{aligned}
&d_1 \geq d_2 + (3n + m + 1)(d_3 + 1) + 1,\ d_2 \geq \max((3n + m + 1)(d_3 + 1), s) + 1, \\
&d_3 \geq 2d_4,\ d_4 \geq m(d_5 + 1)^2 + 1,\ d_5 \geq m.
\end{aligned} \tag{3.5}$$

For characteristic 0 fields, the inequalities of (3.5) can be converted to equalities to get

$$\begin{aligned}
&d_5 = m,\ d_4 = m(d_5 + 1)^2 + 1,\ d_3 = 2d_4, \\
&d_2 = \max((3n + m + 1)(d_3 + 1), s) + 1, \\
&d_1 = d_2 + (3n + m + 1)(d_3 + 1) + 1.
\end{aligned} \tag{3.6}$$

For these choices, $s = 1 + n(d_4+3) + m(d_5+1)^2 = O(nm^3)$, while $(3n+m+1)(d_3+1) = \Theta((n+m)m^3)$. Hence,

$$d_5 = O(m),\ d_4 = O(m^3),\ d_3 = O(m^3),$$
$$d_2 = O((n+m)m^3),\ d_1 = O((n+m)m^3).$$

Using the conditions in (3.5), it is easy to verify that the individual degree of x_0 and y_0 in every polynomial defined above is at least d_1 and d_2, respectively. Define f as:

$$f(\mathbf{z}) := x_0^{d_1} y_0^{d_2+(3n+m+1)(d_3+1)} + \sum_{i=1}^{n} Q_i(\mathbf{z}) + \sum_{k=1}^{m} R_k(\mathbf{z}). \tag{3.7}$$

Clearly, f is a homogeneous polynomial of degree $d_1 + d_2 + (3n+m+1)(d_3+1)$ and is divisible by $x_0^{d_1}$ and $y_0^{d_2}$. Further, the following observations hold under the constraints of (3.5).

Observation 3.2.1. For all $i \in [n]$, $k \in [m]$, the polynomials $x_0^{d_1} y_0^{d_2+(3n+m+1)(d_3+1)}$, $Q_{i,1}(\mathbf{z})$, $Q_{i,2}(\mathbf{z})$, $Q_{i,3}(\mathbf{z})$ and $R_k(\mathbf{z})$ are degree separated with respect to x_0 from one another. Also, $Q_i(\mathbf{z})$ is degree separated with respect to x_0 from other $Q_j(\mathbf{z})$'s, for $i, j \in [n]$ and $i \neq j$. Similarly, $R_k(\mathbf{z})$ is degree separated with respect to x_0 from $R_l(\mathbf{z})$ for $k, l \in [m]$ and $k \neq l$.

Proof. The observation follows from the fact that the x_0-degree of the summands in f, as defined in (3.7), form an arithmetic progression with common difference $d_3 + 1$ and hence every polynomial in the observation statement has distinct x_0-degree. □

Observation 3.2.2. $\mathcal{S}(f(\mathbf{z})) = 1 + n(2d_4+3) + m(d_5+1)^3$ and $\mathrm{Supp}(f) = 8$.

Proof. By Observation 3.2.1, f is a sum of the $n+m+1$ polynomials $x_0^{d_1} y_0^{d_2+(3n+m+1)(d_3+1)}$, Q_i and R_k, where $i \in [n]$ and $k \in [m]$, which are degree separated with respect to x_0. Using arguments similar to the proof of Observation 3.1.3, it holds that

$$\mathcal{S}(Q_i(\mathbf{z})) = \mathcal{S}(Q_{i,1}(\mathbf{z})) + \mathcal{S}(Q_{i,2}(\mathbf{z})) + \mathcal{S}(Q_{i,3}(\mathbf{z})) = 2d_4 + 3 \ \ \forall i \in [n],$$
$$\mathcal{S}(R_k(\mathbf{z})) = \mathcal{S}(x_0^{d_1+(3n+k)(d_3+1)} y_0^{d_2+(m-k+1)(d_3+1)-3d_5}) \prod_{j \in C_k} \mathcal{S}((y_j + (-1)^{a_{k,j}} x_j)^{d_5}) = (d_5+1)^3 \ \ \forall k \in [m],$$

and

$$\mathcal{S}(f(\mathbf{z})) = \mathcal{S}(x_0^{d_1} y_0^{d_2+(3n+m+1)(d_3+1)}) + \sum_{i=1}^{n} \mathcal{S}(Q_i(\mathbf{z})) + \sum_{k=1}^{m} \mathcal{S}(R_k(\mathbf{z})) = 1 + n(2d_4+3) + m(d_5+1)^3.$$

Thus, $\mathcal{S}(f(\mathbf{z})) > s$ but also $(mn)^{O(1)}$. For the support of f, note that $\mathrm{Supp}(R_k) = 8$ for all $k \in [m]$ while $\mathrm{Supp}(Q_i) = 4$ for all $i \in [n]$ and $\mathrm{Supp}(x_0^{d_1} y_0^{d_2+(3n+m+1)(d_3+1)}) = 2$. Hence, by Observation 3.2.1, $\mathrm{Supp}(f) = \mathrm{Supp}(R_k) = 8$. □

The forward direction. Let $\mathbf{u} \in \{0,1\}^n$ be such that $\psi(\mathbf{u}) = 1$ and f, as described in (3.7), be the polynomial corresponding to ψ. Proposition 3.2.1 shows how $\mathbf{u}$ can be used to construct a sparsifying transform. The proof of Proposition 3.2.1 is very similar to that of Proposition 3.1.1.

Proposition 3.2.1. $\mathcal{S}(f(A\mathbf{z})) \leq s$ where $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ is as follows:

$$A : y_0 \mapsto y_0,\ x_0 \mapsto x_0,\ x_i \mapsto x_i,\ y_i \mapsto y_i + (-1)^{u_i} x_i \ \ i \in [n]. \tag{3.8}$$

The reverse direction. Let $\mathcal{S}(f(A\mathbf{z})) \leq s$ for some $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$. Lemma 3.2.1, the proof of which requires Claim 2.2.1, shows that $A(x_0)$ and $A(y_0)$ have only one variable each. With this established, Lemma 3.2.2 shows that the summands of $f(A\mathbf{z})$ must be degree separated with respect to x_0.

Lemma 3.2.1. Without loss of generality, $A(x_0) = x_0$ and $A(y_0) = y_0$.

Proof. Suppose one of $A(x_0)$ or $A(y_0)$ is a linear form in at least two variables. As $A(x_0)^{d_1}$ and $A(y_0)^{d_2}$ divide $f(A\mathbf{z})$, Claim 2.2.1 and the conditions of (3.5) imply $\mathcal{S}(f(A\mathbf{z})) > s$, a contradiction. So, $A(x_0)$ and $A(y_0)$ must have only one variable each. Hence, without loss of generality (i.e., after applying scaling and permutation to A), $A(x_0) = x_0$ and $A(y_0) = y_0$. □

Lemma 3.2.2. For all $i \in [n]$, $k \in [m]$, the polynomials $x_0^{d_1} y_0^{d_2+(3n+m+1)(d_3+1)}$, $Q_{i,1}(A\mathbf{z})$, $Q_{i,2}(A\mathbf{z})$, $Q_{i,3}(A\mathbf{z})$ and $R_k(A\mathbf{z})$ are degree separated from one another with respect to x_0. Also, $Q_i(A\mathbf{z})$ is degree separated with respect to x_0 from other $Q_j(A\mathbf{z})$'s, for $i, j \in [n]$ and $i \neq j$. Similarly, $R_k(A\mathbf{z})$ is degree separated with respect to x_0 from $R_l(A\mathbf{z})$ for $k, l \in [m]$ and $k \neq l$.

Proof. Note that each of the $3n + m + 1$ summand polynomials, as mentioned in the lemma statement, is of form $x_0^{d_1+t(d_3+1)} \cdot y_0^{d_2+v} \cdot h(\mathbf{z})$, where $t \in [0, 3n+m]$ and $v \in \mathbb{N}$. By the construction of f, each t corresponds to a unique summand polynomial. For $x_0^{d_1} y_0^{d_2+(3n+m+1)(d_3+1)}$ the degree of h is 0. Let $i \in [n]$. For $Q_{i,1}(A\mathbf{z})$, the degree of h is d_3 while for $Q_{i,2}(A\mathbf{z})$ and $Q_{i,3}(A\mathbf{z})$ the degree of h is d_4. Lastly, for $R_k(A\mathbf{z})$, where $k \in [m]$, the degree of h is $3d_5$. Thus, going over all the summand polynomials, the degree of h is at most the maximum of d_3, d_4 and $3d_5$. Since $d_3 > d_4$ and $d_3 > 3d_5$ by the conditions in (3.5), therefore the degree of h is at most d_3. As shown in Lemma 3.2.1, $A(x_0) = x_0$ and $A(y_0) = y_0$ while there may be monomials in $h(\mathbf{z})$ which have non-zero x_0-degree. Thus, the possible range of x_0-degree of any monomial of a summand polynomial lies in the range $[d_1 + t(d_3+1), d_1 + t(d_3+1) + d_3]$, which is clearly disjoint for distinct t. Therefore, the summand polynomials are degree separated with respect to x_0. □

$$\therefore\ \mathcal{S}(f(A\mathbf{z})) = \mathcal{S}(x_0^{d_1} y_0^{d_2+(3n+m+1)(d_3+1)}) + \sum_{i=1}^{n} \mathcal{S}(Q_i(A\mathbf{z})) + \sum_{k=1}^{m} \mathcal{S}(R_k(A\mathbf{z})),\ \text{by Lemma 3.2.2.}$$

Lemmas 3.2.3 and 3.2.4 are modified versions of Lemmas 3.1.2 and 3.1.3 respectively and have similar proofs as the original lemmas. Together, Lemmas 3.2.1, 3.2.3 and 3.2.4 show that A is a permuted scaled version of the transform of (3.8). Proposition 3.2.2 then shows how to obtain a satisfying assignment from A and can be proved similarly as Proposition 3.1.2.

Lemma 3.2.3. For any invertible A and $i \in [n]$:

$$\mathcal{S}(Q_i(A\mathbf{z})) = \mathcal{S}(Q_{i,1}(A\mathbf{z})) + \mathcal{S}(Q_{i,2}(A\mathbf{z})) + \mathcal{S}(Q_{i,3}(A\mathbf{z})) \geq d_4 + 3,$$

where Q_i, $Q_{i,1}$, $Q_{i,2}$ and $Q_{i,3}$ are as defined earlier. Equality holds if and only if under A

$$x_i \mapsto X_i \text{ and } y_i \mapsto Y_i + (-1)^{u_i} X_i$$

for some scaled variables $X_i, Y_i \in \mathbf{z}$ and $u_i \in \{0, 1\}$. Further, if $\mathcal{S}(Q_i(A\mathbf{z})) \neq d_4 + 3$, then $\mathcal{S}(Q_i(A\mathbf{z})) \geq 2d_4 + 3$.

Lemma 3.2.4. Under the given A, $\mathcal{S}(Q_i(A\mathbf{z})) = d_4 + 3$ for all $i \in [n]$.

Proposition 3.2.2. With A as described in (3.8), $\mathbf{u} = (u_1, \ldots, u_n)$ is a satisfying assignment for ψ.

3.3 Extension to finite characteristic fields

In this section, we will show how the construction of Sections 3.1.1 and 3.2, with some changes for appropriate cases, can be used to show the NP-hardness of ETsparse over finite characteristic fields for the non-homogeneous case (in the following section) and the homogeneous case (in Section 3.3.3), respectively.

3.3.1 The non-homogeneous case

We first show how the construction of Section 3.1.1 also proves the reduction over fields $\mathbb{F}$ where the characteristic is greater than 2 and then give a modified construction to prove the reduction over characteristic 2 fields. Note that the degrees are chosen in Section 3.3.2 to satisfy (3.2) in any finite characteristic field.

So, let the characteristic be p, where $p > 2$. In this case, the polynomial f and the parameter s of Section 3.1.1 remain the same with the d_i's chosen as specified in Section

3.3.2. The overall argument in both directions of the reduction is highly similar to the characteristic 0 case, with the main differences being the choice of the d_i's and that in the proofs of the observations, lemmas and propositions in Sections 3.1.1, 3.1.2 and 3.1.3 wherever Observation 2.2.5 is used, then it is invoked for the finite characteristic case. Thus, Observations 3.1.1 and 3.1.2 hold without any change while Observation 3.1.3 holds by using Observation 2.2.5 for the finite characteristic case.

The forward direction. If $\mathbf{u} \in \{0,1\}^n$ is such that $\psi(\mathbf{u}) = 1$ and f, as described in (3.1), is the polynomial corresponding to ψ, then Proposition 3.1.1 shows that for the transform A of (3.4), defined using $\mathbf{u}$, $\mathcal{S}(f(A\mathbf{z})) \leq s$ holds.

The reverse direction. If $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ is such that $\mathcal{S}(f(A\mathbf{z})) \leq s$, then the analysis of Section 3.1.3 continues to hold in this case with little changes. Thus, Lemma 3.1.1 shows that $A(x_0) = x_0$ without loss of generality. Then, Lemmas 3.1.2 and 3.1.3 analyse the sparsity of $Q_i(A\mathbf{z})$, where $i \in [n]$ and Q_i is as defined in Section 3.1.1. Together, Lemmas 3.1.1, 3.1.2 and 3.1.3 show that A is a permuted scaled version of the transform of (3.4). Finally, Proposition 3.1.2 shows that a satisfying assignment for ψ can be extracted from A.

Construction for characteristic 2 fields

Over characteristic 2 fields, the polynomial $y_i + x_i$ is the same as $y_i - x_i$. Due to this, the definition of Q_i and that of R_k in Section 3.1.1 need to be changed. Moreover, the sparsifying transform will also be slightly different. Formally, let ψ, $\mathbf{x}$, x_0, $\mathbf{y}$ and $\mathbf{z}$ be as denoted in Section 3.1.1. Let $d_1, d_2, d_3, d_4 \in \mathbb{N}$. The construction of Section 3.1.1 is modified as follows:

- For all $i \in [n]$, define $Q_i(\mathbf{z})$ as:

$$Q_i(\mathbf{z}) := Q_{i,1}(\mathbf{z}) + Q_{i,2}(\mathbf{z}) + Q_{i,3}(\mathbf{z}), \text{ where}$$
$$Q_{i,1}(\mathbf{z}) := x_0^{(3i-2)d_1} x_i^{d_2},\ Q_{i,2}(\mathbf{z}) := x_0^{(3i-1)d_1}(y_i + x_i)^{d_3} \text{ and } Q_{i,3}(\mathbf{z}) := x_0^{3id_1} y_i^{d_3}.$$

- For the k^{th} clause, $k \in [m]$, define $R_k := x_0^{(3n+k)d_1} \prod_{j \in C_k} (y_j + a_{k,j} x_j)^{d_4}$.

Define $s := 1 + n(d_3 + 3) + m(d_4 + 1)^2$ as before. Set the d_i's as specified in Section 3.3.2 with the conditions of (3.2) imposed. Define f as:

$$f(\mathbf{z}) := x_0^{d_1} + \sum_{i=1}^{n} Q_i(\mathbf{z}) + \sum_{k=1}^{m} R_k(\mathbf{z}). \tag{3.9}$$

Observations 3.1.1 and 3.1.2 hold with little change. Observation 3.3.1 analyses the sparsity and support of f.

Observation 3.3.1. $\mathcal{S}(f) \leq 1 + n(d_3+3) + m(d_4+1)^3$ and $4 \leq \text{Supp}(f) \leq 7$.

Proof. By Observation 3.1.1, f is a sum of the $n+m+1$ degree separated polynomials $x_0^{d_1}$, Q_i and R_k, where $i \in [n]$ and $k \in [m]$. Applying Observation 2.2.5 (for linear forms in two variables over finite characteristic fields) to $Q_{i,2}$ and Observation 2.2.2 to Q_i, we get

$$\mathcal{S}(Q_i(\mathbf{z})) = \mathcal{S}(Q_{i,1}(\mathbf{z})) + \mathcal{S}(Q_{i,2}(\mathbf{z})) + \mathcal{S}(Q_{i,3}(\mathbf{z})) = d_3 + 3, \ \ \forall i \in [n].$$

By Observation 2.2.5 (for linear forms in two variables over finite characteristic fields) and the assumption that each clause in ψ has 3 distinct variables, we get that:

$$\mathcal{S}(R_k(\mathbf{z})) = \mathcal{S}(x_0^*) \prod_{j \in C_k} \mathcal{S}((y_j + a_{k,j}x_j)^{d_4}) \leq (d_4+1)^3 \ \ \forall k \in [m].$$

depending on $a_{k,j} = 0$ or 1. Finally, applying Observations 3.1.1 and 2.2.2 to f gives

$$\mathcal{S}(f(\mathbf{z})) = \mathcal{S}(x_0^{d_1}) + \sum_{i=1}^{n} \mathcal{S}(Q_i(\mathbf{z})) + \sum_{k=1}^{m} \mathcal{S}(R_k(\mathbf{z})) \leq 1 + n(d_3+3) + m(d_4+1)^3.$$

For the support of f, note that $4 \leq \text{Supp}(R_k) \leq 7$ for $k \in [m]$, $\text{Supp}(Q_i) = 3$ for all $i \in [n]$ and $\text{Supp}(x_0^{d_1}) = 1$. By Observation 3.1.1, $4 \leq \text{Supp}(f) \leq 7$. □

The forward direction. Let $\mathbf{u} \in \{0,1\}^n$ be such that $\psi(\mathbf{u}) = 1$ and f, as described in (3.9), be the polynomial corresponding to ψ. Proposition 3.3.1 shows how $\mathbf{u}$ can be used to construct a sparsifying transform. The proof of Proposition 3.3.1 is very similar to that of Proposition 3.1.1.

Proposition 3.3.1. $\mathcal{S}(f(A\mathbf{z})) \leq s$ where $A \in \text{GL}(|\mathbf{z}|, \mathbb{F})$ is as follows:

$$A : x_0 \mapsto x_0, \ x_i \mapsto x_i, \ y_i \mapsto y_i + (1-u_i)x_i \ \ \forall i \in [n]. \tag{3.10}$$

The reverse direction. Let $A \in \text{GL}(|\mathbf{z}|, \mathbb{F})$ be such that $\mathcal{S}(f(A\mathbf{z})) \leq s$. The analysis of Section 3.1.3 holds with some changes. Formally, Lemma 3.1.1 holds without any change in its proof. Thus, $A(x_0) = x_0$ without loss of generality. Lemma 3.3.1 analyses $\mathcal{S}(Q_i(A\mathbf{z}))$, $i \in [n]$, and its proof is similar to that of Lemma 3.1.2.

Lemma 3.3.1. For any invertible A and $i \in [n]$:

$$\mathcal{S}(Q_i(A\mathbf{z})) = \mathcal{S}(Q_{i,1}(A\mathbf{z})) + \mathcal{S}(Q_{i,2}(A\mathbf{z})) + \mathcal{S}(Q_{i,3}(A\mathbf{z})) \geq d_3 + 3,$$

where Q_i, $Q_{i,1}$, $Q_{i,2}$ and $Q_{i,3}$ are as defined in this subsection. Equality holds if and only if under A

$$x_i \mapsto X_i \text{ and } y_i \mapsto Y_i + (1-u_i)X_i$$

for some scaled $X_i, Y_i \in \mathbf{z}$ and $u_i \in \{0,1\}$. Further, if $\mathcal{S}(Q_i(A\mathbf{z})) \neq d_3+3$, then $\mathcal{S}(Q_i(A\mathbf{z})) \geq 2d_3+3$.

Lemma 3.1.3 also holds with the same proof as before. Lemmas 3.1.1, 3.3.1 and 3.1.3 together show that A is a permuted scaled version of the transform described in (3.10). Proposition 3.3.2 then holds and can be proven similarly to Proposition 3.1.2.

Proposition 3.3.2. With A as described in (3.10), $\mathbf{u} = (u_1, \ldots, u_n)$ is a satisfying assignment for ψ.

3.3.2 Setting of parameters in the non-homogeneous case

Let the characteristic be $p > 0$. If $p > d_1$, where the value of d_1 is as set in (3.3) for characteristic 0 fields, then the d_i's are chosen to be the same as in (3.3). Otherwise, p must be $O(nm^3)$. When $p = O(nm^3)$, we choose d_1, d_2, d_3 and d_4, to be of form $p^j - 1$, $j \in \mathbb{N}$, while satisfying the inequalities of (3.2) along with $d_1 > d_2 > d_3 > d_4$. This is done so that Observation 2.2.5 can be used for characteristic p fields with $p = O(nm^3)$. It is possible to choose d_i's in this way because, for any $k \in \mathbb{N}$, there is exactly one number of form $p^j - 1$, $j \in \mathbb{N}$, in $[k, pk]$. The bounds on d_1, d_2, d_3 and d_4 are as follows:

$$d_4 \leq pm,\ d_3 \leq pm(d_4+1)^2 + p = O(p^3m^3) \implies s = O(nm^3p^3),$$
$$d_2 = pd_3 + (p-1) = O(p^4m^3),\ d_1 = \max(r, pd_2 + p - 1)$$

where $r \in [s, ps]$ is of form $p^j - 1$, $j \in \mathbb{N}$. Thus, $r \leq ps = O(nm^3p^4)$, while $pd_2 + p - 1 = O(p^5m^3)$. As $p = O(nm^3)$,

$$d_1 = O(n^5m^{18}),\ d_2 = O(n^4m^{15}),\ d_3 = O(n^3m^{12}),\ d_4 = O(nm^4) \text{ and } s = O(n^4m^{12}).$$

3.3.3 The homogeneous case

Like in the non-homogeneous case, we first show how the construction of Section 3.2 can be used to prove the reduction over fields where the characteristic is greater than 2 and then give a modification of this construction to prove the reduction over characteristic 2 fields. Note that the degrees are chosen in Section 3.3.4 to satisfy (3.5) in any finite characteristic field.

So, let the characteristic be p, where $p > 2$. We consider the polynomial f and parameter s as defined in Section 3.2. Note that the degree of f is $d_1 + d_2 + (3n + m + 1)(d_3 + 1)$. We choose d_i's in Section 3.3.4 such that d_3, d_4 and d_5 are of form $p^k - 1$ for some $k \in \mathbb{N}$, while d_1 and d_2 are of form $p^l(p^t - 1)$, for some $t, l \in \mathbb{N}$. For this choice of the d_i's, Observations 3.2.1 and 3.2.2 continue to hold for f. While the forward direction is proved similarly to the characteristic 0 case, the reverse direction requires some change. More precisely, Lemma 3.2.1, which was proven earlier using Claim 2.2.1, requires a different proof. This is because Claim 2.2.1 holds for fields with characteristic 0 or p, with p being "large enough". If $p > d_1 + d_2 + (3n + m + 1)(d_3 + 1)$ for d_i's as chosen in (3.6), then Claim 2.2.1

holds and so does Lemma 3.2.1 along with the rest of the argument in the reverse direction of Section 3.2. Thus, we consider the case when $p \leq d_1 + d_2 + (3n+m+1)(d_3+1) = O((n+m)m^3)$ and prove Lemma 3.2.1 by a different argument. Then, the rest of the argument in the reverse direction of Section 3.2 continues to hold in the same way as before.

The forward direction. Let $\mathbf{u} \in \{0,1\}^n$ be such that $\psi(\mathbf{u}) = 1$ and f, as described in Section 3.2, be the polynomial corresponding to ψ. Proposition 3.2.1, with the same proof as before, shows how $\mathbf{u}$ can be used to construct a sparsifying transform.

The reverse direction. Let $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ such that $\mathcal{S}(f(A\mathbf{z})) \leq s$. We prove Lemma 3.2.1, which shows that $A(x_0)$ and $A(y_0)$ have only one variable each, by showing that for an appropriate choice of d_1 and d_2 (see Section 3.3.4), and the characteristic being finite, the following holds

$$\mathcal{S}(f(A\mathbf{z})) = \mathcal{S}(A(x_0^{d_1}))\mathcal{S}(A(y_0^{d_2}))\mathcal{S}(g(A\mathbf{z})).$$

Here $g(\mathbf{z})$ is a polynomial of degree $(3n+m+1)(d_3+1)$. Using Observation 2.2.4 and the choice of d_i's, $A(x_0)$ and $A(y_0)$ are shown to be single variables. With Lemma 3.2.1 proven, Lemma 3.2.2, with the same proof as before, shows that all the summands in $f(A\mathbf{z})$ are degree separated from one another with respect to x_0. From Lemmas 3.2.1 and 3.2.2, it follows that

$$\mathcal{S}(f(A\mathbf{z})) = \mathcal{S}(x_0^{d_1} y_0^{d_2+(3n+m+1)(d_3+1)}) + \sum_{i=1}^{n} \mathcal{S}(Q_i(A\mathbf{z})) + \sum_{k=1}^{m} \mathcal{S}(R_k(A\mathbf{z})).$$

Then, Lemmas 3.2.3 and 3.2.4 hold just as in the characteristic 0 case because d_3, d_4 and d_5 are of form $p^k - 1$. Together, Lemmas 3.2.1, 3.2.3 and 3.2.4 show that A is a permuted scaled version of the transform of (3.8). Proposition 3.2.2 shows how to derive a satisfying assignment for ψ from A.

Construction for characteristic 2 fields

Similar to the non-homogeneous case, we modify the construction of Section 3.2 to make the reduction work over characteristic 2 fields. Consider the following polynomials:

- For all $i \in [n]$, define $Q_i(\mathbf{z}) := Q_{i,1}(\mathbf{z}) + Q_{i,2}(\mathbf{z}) + Q_{i,3}(\mathbf{z})$ as:

$$\begin{aligned}
Q_{i,1}(\mathbf{z}) &:= x_0^{d_1+(3i-2)(d_3+1)} y_0^{d_2+(3n+m-3i+3)(d_3+1)-d_3} x_i^{d_3}, \\
Q_{i,2}(\mathbf{z}) &:= x_0^{d_1+(3i-1)(d_3+1)} y_0^{d_2+(3n+m-3i+2)(d_3+1)-d_4} (y_i + x_i)^{d_4}, \\
Q_{i,3}(\mathbf{z}) &:= x_0^{d_1+3i(d_3+1)} y_0^{d_2+(3n+m-3i+1)(d_3+1)-d_4} y_i^{d_4}.
\end{aligned}$$

- For the k^{th} clause, $k \in [m]$, define

$$R_k(\mathbf{z}) := x_0^{d_1+(3n+k)(d_3+1)} y_0^{d_2+(m-k+1)(d_3+1)-3d_5} \prod_{j \in C_k} (y_j + a_{k,j} x_j)^{d_5}.$$

Define $s := 1 + n(d_4+3) + m(d_5+1)^2$ as before. Set the d_i's as specified in Section 3.3.4 to satisfy the conditions in (3.5). Define f as:

$$f(\mathbf{z}) := x_0^{d_1} y_0^{d_2+(3n+m+1)(d_3+1)} + \sum_{i=1}^{n} Q_i(\mathbf{z}) + \sum_{k=1}^{m} R_k(\mathbf{z}). \tag{3.11}$$

Observation 3.2.1 holds with little change. Observation 3.3.2 analyses $\mathcal{S}(f)$ and $\text{Supp}(f)$.

Observation 3.3.2. $\mathcal{S}(f) \leq 1 + n(d_4+3) + m(d_5+1)^3$ and $5 \leq \text{Supp}(f) \leq 8$.

Proof. By Observation 3.2.1, f is a sum of the $n+m+1$ polynomials $x_0^{d_1} y_0^{d_2+(3n+m+1)(d_3+1)}$, Q_i and R_k, where $i \in [n]$ and $k \in [m]$, which are degree separated with respect to x_0. Applying Observation 2.2.5 (for linear forms in two variables over finite characteristic fields) to $Q_{i,2}$ and Observation 2.2.2 to Q_i, we get

$$\mathcal{S}(Q_i(\mathbf{z})) = \mathcal{S}(Q_{i,1}(\mathbf{z})) + \mathcal{S}(Q_{i,2}(\mathbf{z})) + \mathcal{S}(Q_{i,3}(\mathbf{z})) = d_4 + 3, \ \ \forall i \in [n].$$

By Observation 2.2.5 (for linear forms in two variables over finite characteristic fields) and the assumption that each clause in ψ has 3 distinct variables, we get that:

$$\mathcal{S}(R_k(\mathbf{z})) = \mathcal{S}(x_0^{d_1+(3n+k)(d_3+1)}) \mathcal{S}(y_0^{d_2+(m-k+1)(d_3+1)-3d_5}) \prod_{j \in C_k} \mathcal{S}((y_j + a_{k,j} x_j)^{d_5}) \leq (d_5+1)^3 \ \forall k \in [m].$$

depending on whether $a_{k,j}$ is 0 or 1. Finally, applying Observations 3.2.1 and 2.2.2 to f gives

$$\mathcal{S}(f(\mathbf{z})) = \mathcal{S}(x_0^{d_1} y_0^{d_2+(3n+m+1)(d_3+1)}) + \sum_{i=1}^{n} \mathcal{S}(Q_i(\mathbf{z})) + \sum_{k=1}^{m} \mathcal{S}(R_k(\mathbf{z})) \leq 1 + n(d_4+3) + m(d_5+1)^3.$$

For the support of f, note that $5 \leq \text{Supp}(R_k) \leq 8$ for $k \in [m]$, $\text{Supp}(Q_i) = 4$ for all $i \in [n]$ and $\text{Supp}(x_0^{d_1} y_0^{d_2+(3n+m+1)(d_3+1)}) = 2$. By Observation 3.2.1, $5 \leq \text{Supp}(f) \leq 8$.

□

The forward direction. Let $\mathbf{u} \in \{0,1\}^n$ be such that $\psi(\mathbf{u}) = 1$ and f, as described in (3.11), be the polynomial corresponding to ψ. Proposition 3.3.3 shows how $\mathbf{u}$ can be used to construct a sparsifying transform. The proof of Proposition 3.3.3 is similar to that of Proposition 3.2.1.

Proposition 3.3.3. $\mathcal{S}(f(A\mathbf{z})) \leq s$ where $A \in \text{GL}(|\mathbf{z}|, \mathbb{F})$ is as follows:

$$A : x_0 \mapsto x_0, \ y_0 \mapsto y_0, \ x_i \mapsto x_i, \ y_i \mapsto y_i + (1-u_i)x_i \ \ \forall i \in [n]. \tag{3.12}$$

The reverse direction. Let $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ be such that $\mathcal{S}(f(A\mathbf{z})) \leq s$. Lemmas 3.2.1 and 3.2.2 hold with little change in the arguments presented in the finite characteristic case. Thus, $A(x_0) = x_0$ and $A(y_0) = y_0$ without loss of generality. Lemma 3.3.2 analyses $\mathcal{S}(Q_i(A\mathbf{z}))$, $i \in [n]$, and its proof is similar to that of Lemma 3.2.3.

Lemma 3.3.2. For any invertible A and $i \in [n]$:

$$\mathcal{S}(Q_i(A\mathbf{z})) = \mathcal{S}(Q_{i,1}(A\mathbf{z})) + \mathcal{S}(Q_{i,2}(A\mathbf{z})) + \mathcal{S}(Q_{i,3}(A\mathbf{z})) \geq d_4 + 3,$$

where Q_i, $Q_{i,1}$, $Q_{i,2}$ and $Q_{i,3}$ are as defined in this subsection. Equality holds if and only if under A

$$x_i \mapsto X_i \text{ and } y_i \mapsto Y_i + (1 - u_i)X_i$$

for some scaled $X_i, Y_i \in \mathbf{z}$ and $u_i \in \{0, 1\}$. Further, if $\mathcal{S}(Q_i(A\mathbf{z})) \neq d_4 + 3$, then $\mathcal{S}(Q_i(A\mathbf{z})) \geq 2d_4 + 3$.

Lemma 3.2.4 also holds with the same proof as before. Lemmas 3.2.1, 3.3.2 and 3.2.4 together show that A is a permuted scaled version of the transform described in (3.12). Proposition 3.3.4 then holds and can be proven similarly to Proposition 3.2.2.

Proposition 3.3.4. With A as described in (3.12), $\mathbf{u} = (u_1, \ldots, u_n)$ is a satisfying assignment for ψ.

3.3.4 Setting of parameters in the homogeneous case

Let the characteristic be $p > 0$. If $p > d_1 + d_2 + (3n + m + 1)(d_3 + 1)$, where d_1, d_2 and d_3 are as chosen in (3.6) for the characteristic 0 case, then the same setting of d_i's holds. Otherwise, $p = O((n + m)m^3)$. Similar to the non-homogeneous case, we choose d_3, d_4 and d_5 so that $d_3 > d_4 > d_5$ and they are of form $p^k - 1$, $k \in \mathbb{N}$. We have the following bounds:

$$\begin{aligned}
&d_5 \leq pm \implies d_5 = O(pm) = O((n + m)m^4),\\
&d_4 \leq pm(d_5 + 1)^2 + p \implies d_4 = O(p^3m^3) = O((n + m)^3m^{12}),\\
&\therefore s = O(p^3nm^3) = O((n + m)^3nm^{12}),\\
&d_3 = pd_4 + p - 1 \implies d_3 = O(p^4m^3) = O((n + m)^4m^{15}).
\end{aligned} \tag{3.13}$$

This choice of d_3, d_4 and d_5 ensures they are $(mn)^{O(1)}$, satisfy (3.5) and that Observation 2.2.5 can be used for characteristic p fields with $p = O((n + m)m^3)$. Now, let $k_1 := \lfloor \log_p(s) \rfloor + 1, k_2 := \lfloor \log_p((3n + m + 1)(d_3 + 1)) \rfloor + 1$, then set

$$d_2 = \sum_{i=k_2}^{k_1+k_2-1} (p - 1)p^i = p^{k_1+k_2} - p^{k_2}. \tag{3.14}$$

For this choice, $d_2 > s$ and $d_2 > (3n+m+1)(d_3+1)$. Lastly, let $k_3 := \lfloor \log_p(d_2 + (3n+m+1)(d_3+1)) \rfloor + 1$, then set

$$d_1 = \sum_{i=k_3}^{k_3+k_1-1} (p-1)p^i = p^{k_1+k_3} - p^{k_3} > d_2 + (3n+m+1)(d_3+1). \tag{3.15}$$

For this choice of d_1 and d_2 it holds that,

$$d_2 = O(p^2 s(3n+m+1)(d_3+1)) = O(p^9 nm^6(n+m)) = O((n+m)^{10}nm^{33})$$
$$d_1 = O(p^2 s(d_2 + (3n+m+1)(d_3+1))) = O(p^{14}n^2m^9(n+m)) = O((n+m)^{15}n^2m^{51}).$$

3.4 Extending Theorem 1 for translations

In this section, we modify the construction of Section 3.1.1 to prove part 1 of Theorem 1 while considering translations. The idea is to choose the degree parameters for the polynomial f such that if $f(A\mathbf{z}+\mathbf{b})$ is s-sparse, where $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^{|\mathbf{z}|}$, then $\mathbf{b}$ must be $\mathbf{0}$ (the all 0s vector in $\mathbb{F}^{|\mathbf{z}|}$) and A must be as described in (3.4). We first show the reduction over any field of characteristic not equal to 2 and give a separate construction for characteristic 2 fields.

Formally, let ψ, $\mathbf{x}, x_0, \mathbf{y}$ and $\mathbf{z}$ be as denoted in Section 3.1.1. For $\mathbf{b} \in \mathbb{F}^{|\mathbf{z}|}$, $\mathbf{b}_{|w}$ denotes the component of $\mathbf{b}$ corresponding to the variable $w \in \mathbf{z}$. Let $d_1, d_2, d_3, d_4 \in \mathbb{N}$. Consider the following polynomials:

- Corresponding to x_i, where $i \in [n]$, define $Q_i(\mathbf{z})$ as:

$$Q_i(\mathbf{z}) := Q_{i,1}(\mathbf{z}) + Q_{i,2}(\mathbf{z}) + Q_{i,3}(\mathbf{z}),\ Q_{i,1}(\mathbf{z}) := x_0^{(3i-2)(d_2+1)} x_i^{d_2},$$
$$Q_{i,2}(\mathbf{z}) := x_0^{(3i-1)(d_2+1)}(y_i + x_i)^{d_3} \text{ and } Q_{i,3}(\mathbf{z}) := x_0^{3i(d_2+1)}(y_i - x_i)^{d_3}.$$

- For the k^{th} clause, $k \in [m]$, define $R_k(\mathbf{z}) := x_0^{k(3d_4+1)} \prod_{j \in C_k}(y_j + (-1)^{a_{k,j}} x_j)^{d_4}$.

Define $s := 1 + n(d_3+3) + m(d_4+1)^2$. Impose the following conditions on the d_i's:

$$d_1 \geq 6n(d_2+1) + 2d_3 + 2,\ d_2 \geq 2d_3,\ d_3 \geq m(d_4+1)^2 + 1,\ d_4 \geq m. \tag{3.16}$$

Finally, define $f(\mathbf{z})$ as:

$$f(\mathbf{z}) := x_0^{d_1} + \sum_{i=1}^{n} Q_i(\mathbf{z}) + \sum_{k=1}^{m} R_k(\mathbf{z}). \tag{3.17}$$

The d_i's are chosen in Section 3.4.1 such that they are $(mn)^{O(1)}$ and also satisfy the inequalities of (3.16) over any field. Observations 3.4.1, 3.4.2 and 3.4.3 hold under the conditions of (3.16).

Observation 3.4.1. For all $i \in [n]$, $k \in [m]$, the polynomials $x_0^{d_1}$, $Q_{i,1}(\mathbf{z})$, $Q_{i,2}(\mathbf{z})$, $Q_{i,3}(\mathbf{z})$ and $R_k(\mathbf{z})$ are degree separated from one another. Also, $Q_i(\mathbf{z})$ is degree separated from other $Q_j(\mathbf{z})$'s, for $i, j \in [n]$ and $i \neq j$. Similarly, $R_k(\mathbf{z})$ is degree separated from $R_l(\mathbf{z})$ for $k, l \in [m]$ and $k \neq l$.

Proof. Let $i \in [n]$. Note that $Q_{i,1}(\mathbf{z})$ has degree $(3i-2)(d_2+1)+d_2$, $Q_{i,2}(\mathbf{z})$ has degree $(3i-1)(d_2+1)+d_3$ and $Q_{i,3}(\mathbf{z})$ has degree $3i(d_2+1)+d_3$. Clearly,

$$3i(d_2+1)+d_3 > (3i-1)(d_2+1)+d_3 > (3i-2)(d_2+1)+d_2.$$

Thus, $Q_{i,1}(\mathbf{z})$, $Q_{i,2}(\mathbf{z})$ and $Q_{i,3}(\mathbf{z})$ are degree separated and $Q_i(\mathbf{z})$ is a sum of three degree separated polynomials and has degree $3i(d_2+1)+d_3$.

Now, let $i \in [n]$ and $k \in [m]$. The lowest degree of any monomial of $Q_i(\mathbf{z})$ is $(3i-2)(d_2+1)+d_2 > 2d_2$, while the degree of any monomial of $R_k(\mathbf{z})$ is $k(3d_4+1)+3d_4 \leq m(3d_4+1)+3d_4$. As $d_2 \geq 2d_3$ and $d_3 > m(d_4+1)^2$ from (3.16), therefore

$$2d_2 \geq 4d_3 > 4m(d_4+1)^2 > m(3d_4+1)+3d_4$$

Thus $Q_i(\mathbf{z})$ is degree separated from $R_k(\mathbf{z})$.

Lastly, let $i, j \in [n]$ where $i < j$ without loss of generality. The highest degree of any monomial of $Q_i(\mathbf{z})$ is $3i(d_2+1)+d_3$ while the lowest degree of any monomial of $Q_j(\mathbf{z})$ is $(3j-2)(d_2+1)+d_2$. Note that

$$(3j-2)(d_2+1)+d_2 \geq (3i+1)(d_2+1)+d_2 > 3i(d_2+1)+d_3$$

because $j \geq i+1$ and $d_2 > d_3$ from (3.16). Therefore $Q_i(\mathbf{z})$ and $Q_j(\mathbf{z})$ are degree separated. That $R_k(\mathbf{z})$ is degree separated from $R_l(\mathbf{z})$ for $k, l \in [m]$ and $k \neq l$ can be observed from the fact that the degree of $R_k(\mathbf{z})$ is $k(3d_4+1)+3d_4$. Clearly, $x_0^{d_1}$ is degree separated from the rest of the polynomials because $d_1 \geq 6n(d_2+1)+2d_3+2$ while the highest degree polynomial among $Q_i(\mathbf{z})$'s and $R_k(\mathbf{z})$'s is $Q_n(\mathbf{z})$ of degree $3n(d_2+1)+d_3$. □

Observation 3.4.2. The degree of f is $d_1 = (mn)^{O(1)}$ with $\frac{d_1}{2} > s$.

Proof. By the definition of f in (3.17) and Observation 3.4.1, the degree of f is the maximum degree among $x_0^{d_1}$, Q_i's and R_k's, where $i \in [n]$ and $k \in [m]$. The degree of Q_i is $3i(d_2+1)+d_3$ and that of R_k is $k(3d_4+1)+3d_4$ with $3i(d_2+1)+d_3 > k(3d_4+1)+3d_4$. Further, $d_1 \geq 6nd_2+6n+2d_3+2$. Hence the degree of f is d_1. Finally, it holds by (3.16) that $\frac{d_1}{2} > 3nd_2 > 3nd_3 > s$. □

Observation 3.4.3. $\mathcal{S}(f(\mathbf{z})) = 1+n(2d_3+3)+m(d_4+1)^3$ and $\mathrm{Supp}(f) = 7$.

The proof of Observation 3.4.3 is similar to that of Observation 3.1.3 and uses Observations 3.4.1, 2.2.2 and 2.2.5.

The forward direction. If $\mathbf{u} \in \{0,1\}^n$ is such that $\psi(\mathbf{u}) = 1$ and f, as described in (3.17), is the polynomial corresponding to ψ, then Proposition 3.1.1, with some small changes to its statement and proof, shows that for $\mathbf{b} = \mathbf{0}$ and the transform A as described in (3.4), $\mathcal{S}(f(A\mathbf{z})) \leq s$ holds.

The reverse direction. We leverage the constraints in (3.16) to show that if $\mathcal{S}(f(A\mathbf{z} + \mathbf{b})) \leq s$ for some $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^{|\mathbf{z}|}$, then A is as described in (3.4) and $\mathbf{b} = \mathbf{0}$. Lemma 3.4.1 shows that $A(x_0) = x_0$, without loss of generality, and $\mathbf{b}_{|x_0} = 0$. Then, Lemma 3.4.2 shows that the summands of $f(A\mathbf{z} + \mathbf{b})$ are degree separated with respect to x_0.

Lemma 3.4.1. *$A(x_0) = x_0$, without loss of generality, and $\mathbf{b}_{|x_0} = 0$.*

Proof. Let $\ell_0 = A(x_0)$ and $b_0 = \mathbf{b}_{|x_0}$. If $b_0 = 0$ and ℓ_0 is a linear form in at least two variables, then by the choice of d_1 and Observation 2.2.5, $\mathcal{S}((\ell_0 + b_0)^{d_1}) \geq d_1 + 1 > s$. If $b_0 \neq 0$, then by the binomial theorem

$$(\ell_0 + b_0)^{d_1} = \sum_{i=0}^{d_1} \binom{d_1}{i} b_0^i \ell_0^{d_1 - i}.$$

The summands in the above expansion are degree separated and $\binom{d_1}{i} \neq 0$ for all $i \in [0, d_1]$ because of the choice of d_1 (and Lucas's Theorem if the characteristic is finite). Thus, $(\ell_0 + b_0)^{d_1}$ contains at least one monomial of degree i, for all $i \in [0, d_1]$. Since $\frac{d_1}{2} > 3n(d_2+1) + d_3 > s$ and the maximum degree of any polynomial among the Q_i's and R_k's, with $i \in [n]$ and $k \in [m]$, is $3n(d_2+1) + d_3$, therefore at least $s+1$ monomials in $(\ell_0 + b_0)^{d_1}$ are degree separated from $Q_i(A\mathbf{z} + \mathbf{b})$'s and $R_k(A\mathbf{z} + \mathbf{b})$'s. Hence $\mathcal{S}(f(A\mathbf{z} + \mathbf{b})) > s$, a contradiction. Thus, $\mathbf{b}_{|x_0} = b_0$ must be 0 and $A(x_0) = \ell_0$ must have only one variable, which can be assumed to be x_0 without loss of generality, as permutation and non-zero scaling of variables does not affect the sparsity. □

Lemma 3.4.2. *For all $i \in [n]$, $k \in [m]$, $x_0^{d_1}$, $Q_{i,1}(A\mathbf{z} + \mathbf{b})$, $Q_{i,2}(A\mathbf{z} + \mathbf{b})$, $Q_{i,3}(A\mathbf{z} + \mathbf{b})$ and $R_j(A\mathbf{z} + \mathbf{b})$ are degree separated from one another with respect to x_0. Also, $Q_i(A\mathbf{z} + \mathbf{b})$ is degree separated with respect to x_0 from other $Q_j(A\mathbf{z} + \mathbf{b})$'s, for $i, j \in [n]$ and $i \neq j$. Similarly, $R_k(A\mathbf{z} + \mathbf{b})$ is degree separated with respect to x_0 from $R_l(A\mathbf{z} + \mathbf{b})$ for $k, l \in [m]$ and $k \neq l$.*

Proof. Let $i \in [n]$. For $Q_{i,1}(A\mathbf{z} + \mathbf{b})$, $Q_{i,2}(A\mathbf{z} + \mathbf{b})$ and $Q_{i,3}(A\mathbf{z} + \mathbf{b})$, the respective range of x_0-degree of a monomial of respective polynomials is $[(3i-2)(d_2+1), (3i-2)(d_2+1) + d_2]$, $[(3i-1)(d_2+1), (3i-1)(d_2+1) + d_3]$ and $[3i(d_2+1), 3i(d_2+1) + d_3]$. As $d_2 > d_3$, it can be observed that these ranges are disjoint, implying $Q_{i,1}(A\mathbf{z} + \mathbf{b})$, $Q_{i,2}(A\mathbf{z} + \mathbf{b})$ and $Q_{i,3}(A\mathbf{z} + \mathbf{b})$ are degree separated from one another with respect to x_0.

Let $i, j \in [n]$ and $i < j$ without loss of generality. For $Q_i(A\mathbf{z}+\mathbf{b})$ and $Q_j(A\mathbf{z}+\mathbf{b})$, the respective range of x_0-degree of a monomial of respective polynomials is $[(3i-2)(d_2+1), 3i(d_2+1)+d_3]$ and $[(3j-2)(d_2+1), 3j(d_2+1)+d_3]$. As $d_2 > d_3$ and $j \geq i+1$, therefore $(3j-2)(d_2+1) > 3i(d_2+1)+d_3$. Hence, $Q_i(A\mathbf{z}+\mathbf{b})$ is degree separated from $Q_j(A\mathbf{z}+\mathbf{b})$ with respect to x_0.

Now, let $k, l \in [m]$ and $k < l$ without loss of generality. For $R_k(A\mathbf{z}+\mathbf{b})$ and $R_l(A\mathbf{z}+\mathbf{b})$, the respective range of x_0-degree of a monomial of respective polynomials is $[k(3d_4+1), k(3d_4+1)+3d_4]$ and $[l(3d_4+1), l(3d_4+1)+3d_4]$. As $l \geq k+1$, therefore $l(3d_4+1) > k(3d_4+1)+3d_4$. Hence, $R_k(A\mathbf{z}+\mathbf{b})$ is degree separated from $R_l(A\mathbf{z}+\mathbf{b})$ with respect to x_0.

Lastly, let $i \in [n]$ and $k \in [m]$. The highest x_0-degree of a monomial in $R_k(A\mathbf{z}+\mathbf{b})$ is $k(3d_4+1)+3d_4 \leq m(3d_4+1)+3d_4$, while the lowest x_0-degree of any monomial in $Q_i(A\mathbf{z}+\mathbf{b})$ is $(3i-2)(d_2+1) > d_2$. Now,

$$d_2 \geq 2d_3 > 2m(d_4+1)^2 > m(3d_4+1)+3d_4$$

where the inequalities follow from the conditions in (3.16). Therefore $Q_i(A\mathbf{z}+\mathbf{b})$ is degree separated from $R_k(A\mathbf{z}+\mathbf{b})$'s with respect to x_0. Clearly, $x_0^{d_1}$ is degree separated with respect to x_0 from $Q_i(A\mathbf{z}+\mathbf{b})$ and $R_k(A\mathbf{z}+\mathbf{b})$ because $d_1 > 3n(d_2+1)+d_3$, the highest x_0-degree of any monomial among the $Q_i(A\mathbf{z}+\mathbf{b})'s$ and $R_k(A\mathbf{z}+\mathbf{b})$'s. □

$$\therefore \mathcal{S}(f(A\mathbf{z}+\mathbf{b})) = \mathcal{S}(x_0^{d_1}) + \sum_{i=1}^{n} \mathcal{S}(Q_i(A\mathbf{z}+\mathbf{b})) + \sum_{k=1}^{m} \mathcal{S}(R_k(A\mathbf{z}+\mathbf{b})) \text{ by Lemma 3.4.2.}$$

Lemma 3.4.3 analyses the sparsity of $Q_i(A\mathbf{z}+\mathbf{b})$. The proof of Lemma 3.4.3 is similar to that of Lemma 3.1.2 and uses Observations 2.2.5 and 2.2.6.

Lemma 3.4.3. For any invertible A, $\mathbf{b} \in \mathbb{F}^{|\mathbf{z}|}$ and $i \in [n]$:

$$\mathcal{S}(Q_i(A\mathbf{z}+\mathbf{b})) = \mathcal{S}(Q_{i,1}(A\mathbf{z}+\mathbf{b})) + \mathcal{S}(Q_{i,2}(A\mathbf{z}+\mathbf{b})) + \mathcal{S}(Q_{i,3}(A\mathbf{z}+\mathbf{b})) \geq d_3+3,$$

where Q_i, $Q_{i,1}$, $Q_{i,2}$ and $Q_{i,3}$ are as defined in this section. Equality holds if and only if $\mathbf{b}_{|x_i} = 0, \mathbf{b}_{|y_i} = 0$ and under A

$$x_i \mapsto X_i \text{ and } y_i \mapsto Y_i + (-1)^{u_i} X_i$$

for some scaled $X_i, Y_i \in \mathbf{z}$ and $u_i \in \{0,1\}$. Further, if $\mathcal{S}(Q_i(A\mathbf{z}+\mathbf{b})) \neq d_3+3$, then $\mathcal{S}(Q_i(A\mathbf{z}+\mathbf{b})) \geq 2d_3+3$.

Proof. From Lemma 3.4.2 and Observation 2.2.2, it follows that $\mathcal{S}(Q_i(A\mathbf{z}+\mathbf{b})) = \mathcal{S}(Q_{i,1}(A\mathbf{z}+\mathbf{b})) + \mathcal{S}(Q_{i,2}(A\mathbf{z}+\mathbf{b})) + \mathcal{S}(Q_{i,3}(A\mathbf{z}+\mathbf{b}))$. The if direction of the lemma statement is easy to verify. For the only if direction consider the following cases of A and $\mathbf{b}$:

1. $\mathcal{S}(A(x_i) + \mathbf{b}_{|x_i}) \geq 2$: If $\mathbf{b}_{|x_i} = 0$ then $\mathcal{S}(A(x_i)) \geq 2$ and by Observation 2.2.5, $\mathcal{S}(Q_{i,1}(A\mathbf{z} + \mathbf{b})) \geq d_2 + 1$. If $\mathbf{b}_{|x_i} \neq 0$ then by the choice of d_2 and Observation 2.2.6, $\mathcal{S}(Q_{i,1}(A\mathbf{z} + \mathbf{b})) \geq d_2 + 1$. Also, $\mathcal{S}(Q_{i,2}(A\mathbf{z} + \mathbf{b})) \geq 1$ and $\mathcal{S}(Q_{i,3}(A\mathbf{z} + \mathbf{b})) \geq 1$. Hence, $\mathcal{S}(Q_i(A\mathbf{z} + \mathbf{b})) \geq d_2 + 3 \geq 2d_3 + 3$ as $d_2 \geq 2d_3$. For the remaining cases, we consider $\mathcal{S}(A(x_i) + \mathbf{b}_{|x_i}) = 1$, meaning $A(x_i) = X_i$ for some scaled variable $X_i \in \mathbf{z}$ and $\mathbf{b}_{|x_i} = 0$.

2. $\mathcal{S}(A(x_i) + \mathbf{b}_{|x_i}) = 1$, $\mathcal{S}(A(y_i + x_i) + \mathbf{b}_{|y_i} + \mathbf{b}_{|x_i}) \geq 2$ and $\mathcal{S}(A(y_i - x_i) + \mathbf{b}_{|y_i} - \mathbf{b}_{|x_i}) \geq 2$: Like in the previous case, it can be shown using Observation 2.2.5 (if $\mathbf{b}_{|y_i} = 0$) or Observation 2.2.6 (if $\mathbf{b}_{|y_i} \neq 0$) that $\mathcal{S}(Q_{i,2}(A\mathbf{z} + \mathbf{b})) \geq d_3 + 1$ and $\mathcal{S}(Q_{i,3}(A\mathbf{z} + \mathbf{b})) \geq d_3 + 1$ implying $\mathcal{S}(Q_i(A\mathbf{z} + \mathbf{b})) \geq 2d_3 + 3$.

3. $\mathcal{S}(A(x_i) + \mathbf{b}_{|x_i}) = 1$ with $\mathcal{S}(A(y_i + x_i) + \mathbf{b}_{|y_i} + \mathbf{b}_{|x_i}) = 1$ or $\mathcal{S}(A(y_i - x_i) + \mathbf{b}_{|y_i} - \mathbf{b}_{|x_i}) = 1$: Because A is invertible, $\mathcal{S}(A(y_i - x_i)) \geq 1$ and $\mathcal{S}(A(y_i + x_i)) \geq 1$. Further, since $\mathbf{b}_{|x_i} = 0$, therefore $\mathbf{b}_{|y_i}$ must be 0. This observation and the invertibility of A imply that exactly one of $\mathcal{S}(A(y_i + x_i)) = 1$ or $\mathcal{S}(A(y_i - x_i)) = 1$ holds. Without loss of generality, let $\mathcal{S}(A(y_i + x_i)) = 1$, which implies $A(y_i) = Y_i - X_i$ for some scaled variable $Y_i \in \mathbf{z}$. Then $A(y_i - x_i) = Y_i - 2X_i$. Hence, $\mathcal{S}(Q_{i,1}(A\mathbf{z} + \mathbf{b})) = 1$, $\mathcal{S}(Q_{i,2}(A\mathbf{z} + \mathbf{b})) = 1$ and $\mathcal{S}(Q_{i,3}(A\mathbf{z} + \mathbf{b})) = d_3 + 1$ (by Observation 2.2.5) implying $\mathcal{S}(Q_i(A\mathbf{z} + \mathbf{b})) = d_3 + 3$.

The first two cases show that if A and $\mathbf{b}$ are not as per the lemma statement, then $\mathcal{S}(Q_i(A\mathbf{z} + \mathbf{b})) \geq 2d_3 + 3$; otherwise, $\mathcal{S}(Q_i(A\mathbf{z} + \mathbf{b})) = d_3 + 3$. □

Lemma 3.1.3 holds with some change to its statement and can be proved using Lemmas 3.4.2 and 3.4.3, and Observation 2.2.2. Lemmas 3.4.1, 3.4.3 and 3.1.3 together show that A is a permuted scaled version of the transform of (3.4) and that $\mathbf{b} = \mathbf{0}$. Then, Proposition 3.1.2 shows how a satisfying assignment for ψ can be recovered from A.

Construction for characteristic 2 fields

Since over characteristic 2 fields $y_i + x_i$ and $y_i - x_i$ are the same polynomials, we need to modify the previous construction. Moreover, the sparsifying transform will also be slightly different. Formally, let ψ, $\mathbf{x}$, x_0, $\mathbf{y}$ and $\mathbf{z}$ be as denoted in Section 3.1.1. Let d_1, d_2, d_3, $d_4 \in \mathbb{N}$. Consider the following polynomials:

- Corresponding to x_i, where $i \in [n]$, define $Q_i(\mathbf{z})$ as:

$$Q_i(\mathbf{z}) := Q_{i,1}(\mathbf{z}) + Q_{i,2}(\mathbf{z}) + Q_{i,3}(\mathbf{z}),\ Q_{i,1}(\mathbf{z}) := x_0^{(3i-2)(d_2+1)} x_i^{d_2},$$
$$Q_{i,2}(\mathbf{z}) := x_0^{(3i-1)(d_2+1)} (y_i + x_i)^{d_3} \text{ and } Q_{i,3}(\mathbf{z}) := x_0^{3i(d_2+1)} y_i^{d_3}.$$

- For the k^{th} clause, $k \in [m]$, define $R_k(\mathbf{z}) := x_0^{k(3d_4+1)} \prod_{j \in C_k} (y_j + a_{k,j} x_j)^{d_4}$.

Define $s := 1 + n(d_3 + 3) + m(d_4 + 1)^2$. Choose d_i's as specified in Section 3.4.1 so that they are $(mn)^{O(1)}$ and satisfy the conditions of (3.16). Finally, define $f(\mathbf{z})$ as:

$$f(\mathbf{z}) := x_0^{d_1} + \sum_{i=1}^{n} Q_i(\mathbf{z}) + \sum_{k=1}^{m} R_k(\mathbf{z}). \tag{3.18}$$

Observations 3.4.1, 3.4.2 hold with little change. Observation 3.4.4 analyses the sparsity and support of f and has a proof similar to that of Observations 3.4.3 and Observation 3.3.1.

Observation 3.4.4. $\mathcal{S}(f(\mathbf{z})) \leq 1 + n(d_3 + 3) + m(d_4 + 1)^3$ and $4 \leq \text{Supp}(f) \leq 7$.

Remarks. Like in Section 3.3.3, the sparsity of the polynomial output by the reduction over characteristic 2 fields depends on the number of variables which are complemented within a clause. Hence, for the same number of variables n and the same number of clauses m, the output polynomial corresponding to two different ψ's may have different sparsity. Thus, the reduction is not natural over characteristic 2 fields.

The forward direction. Let $\mathbf{u} \in \{0,1\}^n$ be such that $\psi(\mathbf{u}) = 1$ and f, as described in (3.18), be the polynomial corresponding to ψ. Proposition 3.3.1 shows how $\mathbf{u}$ can be used to construct a sparsifying transform A with $\mathbf{b} = \mathbf{0}$.

The reverse direction. Let $A \in \text{GL}(|\mathbf{z}|, \mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^{|\mathbf{z}|}$ be such that $\mathcal{S}(f(A\mathbf{z} + \mathbf{b})) \leq s$. The analysis of the reverse direction in the previous section holds with some changes. Formally, Lemma 3.4.1 holds without any change in its proof while Lemma 3.4.2 holds with some change in its statement and proof. Thus, $A(x_0) = x_0$ without loss of generality. Lemma 3.4.4 analyses $\mathcal{S}(Q_i(A\mathbf{z} + \mathbf{b}))$, where $i \in [n]$, and its proof is similar to that of Lemma 3.4.3.

Lemma 3.4.4. For any $A \in \text{GL}(|\mathbf{z}|, \mathbb{F}^{|\mathbf{z}|})$, $\mathbf{b} \in \mathbb{F}^{|\mathbf{z}|}$ and $i \in [n]$:

$$\mathcal{S}(Q_i(A\mathbf{z} + \mathbf{b})) = \mathcal{S}(Q_{i,1}(A\mathbf{z} + \mathbf{b})) + \mathcal{S}(Q_{i,2}(A\mathbf{z} + \mathbf{b})) + \mathcal{S}(Q_{i,3}(A\mathbf{z} + \mathbf{b})) \geq d_3 + 3,$$

where Q_i, $Q_{i,1}$, $Q_{i,2}$ and $Q_{i,3}$ are as defined in this section. Equality holds if and only if $\mathbf{b}_{|x_i} = 0, \mathbf{b}_{|y_i} = 0$ and under A

$$x_i \mapsto X_i \text{ and } y_i \mapsto Y_i + (1 - u_i)X_i$$

for some scaled $X_i, Y_i \in \mathbf{z}$ and $u_i \in \{0,1\}$. Further, if $\mathcal{S}(Q_i(A\mathbf{z} + \mathbf{b})) \neq d_3 + 3$, then $\mathcal{S}(Q_i(A\mathbf{z} + \mathbf{b})) \geq 2d_3 + 3$.

Lemma 3.1.3 holds with the same proof (for translations) as before. Lemmas 3.4.1, 3.4.4 and 3.1.3 together show that A is a permuted scaled version of the transform of (3.10) and that $\mathbf{b} = \mathbf{0}$. Then, Proposition 3.3.2 shows how a satisfying assignment for ψ can be recovered from A.

3.4.1 Setting of parameters

For characteristic 0 fields. In this case, the inequalities in (3.16) can be converted to equalities. Thus

$$d_4 = m,\ d_3 = m(m+1)^2 + 1 = O(m^3) \implies s = O(nm^3),$$
$$d_2 = 2m(m+1)^2 + 2 = O(m^3),\ d_1 = 6nd_2 + 6n + 2d_3 + 2 = O(nm^3).$$

For finite characteristic fields. Let the characteristic be $p > 0$. If $p > d_1$, where the value of d_1 is as in the characteristic 0 fields case, then the d_i's are set as per the characteristic 0 fields case. Otherwise $p = O(nm^3)$. In such a case, we choose the $d_1 > d_2 > d_3 > d_4$ to be of form $p^k - 1$, for some $k \in \mathbb{N}$, so that the conditions in (3.16) are satisfied and Observation 2.2.5 can be used over characteristic p fields. The lemmas and the observations in the previous section hold for this choice of the d_i's. Now, the following bounds hold on the d_i's:

$$d_4 \leq pm,\ d_3 \leq pm(d_4+1)^2 + p = O(p^3m^3) \implies s = O(nm^3p^3),$$
$$d_2 = pd_3 + (p-1) = O(p^4m^3),\ d_1 \leq p(6nd_2 + 6n + 2d_3 + 2) = O(nm^3p^5).$$

As $p = O(nm^3)$, therefore

$$d_1 = O(n^6m^{18}),\ d_2 = O(n^4m^{15}),\ d_3 = O(n^3m^{12}),\ d_4 = O(nm^4) \text{ and } s = O(n^4m^{12}).$$

Chapter 4

NP-hardness of α-gap-ETsparse

In this section, we prove Theorem 2. We first prove parts 1 and 2 of Theorem 2 over characteristic 0 fields without considering translations in Sections 4.1 and 4.2, respectively. Section 4.3 extends both parts to finite characteristic fields.

Proof sketch. For a 3-CNF ψ, we carefully analyze the sparsity of the corresponding polynomial f as defined in Section 3, for the non-homogeneous and the homogeneous case. For unsatisfiable ψ's, we do a slightly deeper analysis on $\mathcal{S}(f(A\mathbf{z}))$, for all $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$, to show a lower bound. For satisfiable ψ's, $\mathcal{S}(f(A\mathbf{z}))$ has already been upper bounded for an appropriate $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$. The degree parameters are also chosen differently so that the gap between the lower bound and the upper bound is significant. Comparing the sparsities for satisfiable and unsatisfiable ψ's proves Theorem 2. Note that throughout this section, we assume $\epsilon \in (0, 1/3)$ to be an arbitrary constant.

4.1 Analyzing the gap: the non-homogeneous case

For a 3-CNF ψ, consider the polynomial f as defined in (3.1). Choose the d_i's to satisfy the following while also being $(mn)^{O(1)}$:

$$d_4 \geq \max(4mn, (mn)^{O(1/\epsilon)}),\ d_3 = m(d_4+1)^2 + 1,\ d_2 = d_3^2 + 1,\ d_1 = d_2 + 1. \tag{4.1}$$

Note under these constraints, the conditions in (3.2) are also satisfied. Let $s := \mathcal{S}(f)$. Then, $s = 1 + n(2d_3 + 3) + m(d_4+1)^3$ by Observation 3.1.3. For $\psi \in \overline{\text{3-SAT}}$, Lemma 4.1.1 shows lower bounds on $\mathcal{S}(f(A\mathbf{z}))$ for all $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$. In the lemma, Item 1 is essentially Lemma 3.1.1, Items 2 and 3 are a slightly deeper analysis of that in Lemmas 3.1.2 and 3.1.3, and Item 4 is the analysis in Proposition 3.1.2. Thus, Lemma 4.1.1 encapsulates the analysis of Section 3.1.3. For $\psi \in$ 3-SAT, by Proposition 3.1.1, there exists $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ such that $\mathcal{S}(f(A\mathbf{z})) \leq s_0$, where $s_0 = 1 + n(d_3+3) + m(d_4+1)^2$. Proposition 4.1.1 shows

α-gap-ETsparse is NP-hard by comparing the sparsity for satisfiable and unsatisfiable ψ's, and uses Lemma 4.1.1 and the conditions in (4.1).

Lemma 4.1.1. Let $\psi \in \overline{\text{3-SAT}}$, f be as defined in (3.1) corresponding to ψ and $A \in \text{GL}(|\mathbf{z}|, \mathbb{F})$.

1. If $A(x_0)$ is a linear form in at least 2 variables, $\mathcal{S}(f(A\mathbf{z})) \geq d_1 + 1$.
2. If A is not as in item 1 and $A(x_j)$ is a linear form in at least 2 variables for some $j \in [n]$, then $\mathcal{S}(f(A\mathbf{z})) \geq d_2 + 1$.
3. If A is not as in items 1 and 2 and for some $j \in [n]$, $A(y_j + x_j)$ or $A(y_j - x_j)$ is a linear form in at least 3 variables, then $\mathcal{S}(f(A\mathbf{z})) \geq \frac{d_3^2+3d_3+2}{2}$.
4. If A is not of the form described in the previous three items, then $\mathcal{S}(f(A\mathbf{z})) \geq (d_4+1)^3$.

Proof. By Observations 3.1.1, 2.2.3 and the definition of f as in (3.1), it follows that:

$$\mathcal{S}(f(A\mathbf{z})) = \mathcal{S}(A(x_0^{d_1})) + \sum_{i=1}^{n} \mathcal{S}(Q_i(A\mathbf{z})) + \sum_{k=1}^{m} \mathcal{S}(R_k(A\mathbf{z})).$$

We now analyse $\mathcal{S}(f(A\mathbf{z}))$ under the transforms listed in the lemma statement. The list covers all possible types of transforms.

1. By Observation 2.2.5, $\mathcal{S}(f(A\mathbf{z})) \geq \mathcal{S}(A(x_0^{d_1})) \geq d_1 + 1$ follows.
2. In this case, $A(x_0) = x_0$ without loss of generality, as permutation and non-zero scaling of variables do not influence the sparsity of the polynomial. By Observation 2.2.5, it follows that $\mathcal{S}(f(A\mathbf{z})) \geq \mathcal{S}(Q_{j,1}(A\mathbf{z})) \geq d_2 + 1$.
3. In this case, $A(x_i)$, where $i \in [0, n]$ is some scaled variable in $\mathbf{z}$. Without loss of generality, let $A(y_j + x_j)$ be a linear form in at least 3 variables. By Observation 2.2.4, $\mathcal{S}(Q_{j,2}(A\mathbf{z})) \geq \binom{d_3+2}{2}$ holds. Therefore,
$$\mathcal{S}(f(A\mathbf{z})) \geq \mathcal{S}(Q_j(A\mathbf{z})) \geq \mathcal{S}(Q_{j,2}(A\mathbf{z})) \geq \binom{d_3+2}{2} = \frac{d_3^2+3d_3+2}{2}.$$
4. In this case, $A(x_i) = X_i$, where $i \in [0, n]$ and $X_i \in \mathbf{z}$ is some scaled variable. Also, $A(y_i + x_i)$ and $A(y_i - x_i)$ are linear forms in at most two variables for all $i \in [n]$. Thus, $A(y_i) = Y_i + c_i X_i$, where $c_i \in \mathbb{F}$ and $Y_i \in \mathbf{z}$ is some scaled variable. As A is invertible, the Y_i's and X_i's are distinct variables. Hence,
$$\mathcal{S}(R_k(A\mathbf{z})) = \mathcal{S}(X_0^{(3n+k)d_1}) \prod_{j \in C_k} \mathcal{S}((Y_j + (c_j + (-1)^{a_{k,j}})X_j)^{d_4}).$$
Since ψ is unsatisfiable, for any such A, there exists $k \in [m]$ such that $\mathcal{S}(R_k(A\mathbf{z})) \geq (d_4+1)^3$ (by Observation 2.2.5). Therefore, $\mathcal{S}(f(A\mathbf{z})) \geq \mathcal{S}(R_k(A\mathbf{z})) \geq (d_4+1)^3$.

□

Proposition 4.1.1. Let $\mathrm{char}(\mathbb{F}) = 0$. If the input in α-gap-ETsparse is an s-sparse polynomial, then α-gap-ETsparse is NP-hard for $\alpha = s^{1/3-\epsilon}$.

Proof. If $\psi \in$ 3-SAT, then $\mathcal{S}(f(A\mathbf{z})) \leq s_0$ where A is as described in (3.4). If $\psi \in \overline{\text{3-SAT}}$, then it follows from Lemma 4.1.1 that for any $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$:

$$\mathcal{S}(f(A\mathbf{z})) \geq \min\left(d_1+1, d_2+1, \frac{d_3^2+3d_3+2}{2}, (d_4+1)^3\right).$$

The constraints imposed in (4.1) ensure that $(d_4+1)^3$ is the minimum. As $d_3 = m(d_4+1)^2+1$, therefore $s_0 = 1+n(d_3+3)+m(d_4+1)^2 \leq 3nd_3 = 3mn(d_4+1)^2+3n \leq 4mn(d_4+1)^2$. Thus, the gap in the sparsities of the YES instances and the NO instances is

$$\frac{(d_4+1)^3}{s_0} \geq \frac{(d_4+1)^3}{4mn(d_4+1)^2} = \frac{d_4+1}{4mn}.$$

Also, as $d_4 \geq 4mn$, $\mathcal{S}(f) = s \leq 2m(d_4+1)^3 \implies d_4+1 \geq (\frac{s}{2m})^{1/3}$. Then, the gap is

$$\frac{(d_4+1)^3}{s_0} \geq \frac{d_4+1}{4mn} \geq \frac{s^{1/3}}{2^{1/3}4m^{4/3}n}.$$

Finally, note that $s \geq d_4^3$. Thus, for $d_4^{3\epsilon} \geq (mn)^{O(1)}$ large enough,

$$s^\epsilon \geq d_4^{3\epsilon} \geq 2^{1/3}4m^{4/3}n \implies \frac{s^{1/3}}{2^{1/3}4m^{4/3}n} \geq s^{1/3-\epsilon}.$$

Hence, the gap is at least $s^{1/3-\epsilon}$. Therefore, 3-SAT reduces to α-gap-ETsparse for $\alpha = s^{1/3-\epsilon}$. □

4.2 Analyzing the gap: the homogeneous case

Consider the polynomial f as defined in (3.7) for ψ. Choose the d_i's to satisfy the following constraints while also being $(mn)^{O(1)}$.

$$\begin{aligned} &d_5 \geq \max((4mn, (mn)^{O(1/\epsilon)}),\ d_4 = m(d_5+1)^2+1,\ d_3 = d_4^2+1, \\ &d_2 = \max((3n+m+1)(d_3+1), s)+1, \\ &d_1 = d_2+(3n+m+1)(d_3+1)+1. \end{aligned} \tag{4.2}$$

Under these constraints, the conditions in (3.5) are also satisfied. Let $s := \mathcal{S}(f)$. Then, $s = 1+n(2d_4+3)+m(d_5+1)^3$ by Observation 3.2.2. For $\psi \in \overline{\text{3-SAT}}$, Lemma 4.2.1, proved using Claim 2.2.1, shows lower bounds on $\mathcal{S}(f(A\mathbf{z}))$, for all $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$. In

the lemma, Items 1 and 2 are essentially Lemma 3.2.1, Items 3 and 4 are a deeper analysis of that in Lemmas 3.2.3 and 3.2.4, and Item 5 is the analysis in Proposition 3.2.2. For $\psi \in$ 3-SAT, by Proposition 3.2.1, there exists $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ such that $\mathcal{S}(f(A\mathbf{z})) \leq s_0$, where $s_0 = 1 + n(d_4 + 3) + m(d_5 + 1)^2$. Proposition 4.2.1 proves α-gap-ETsparse is NP-hard using Lemma 4.2.1 and the conditions in (4.2).

Lemma 4.2.1. Let $\psi \in \overline{\text{3-SAT}}$, $f(\mathbf{z})$ be the polynomial as defined in (3.7) corresponding to ψ and $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$.

1. If $A(x_0)$ is a linear form in at least 2 variables, $\mathcal{S}(f(A\mathbf{z})) \geq d_1 + 1$.
2. If A is not as in item 1 and $A(y_0)$ is a linear form in at least 2 variables, $\mathcal{S}(f(A\mathbf{z})) \geq d_2 + 1$.
3. If A is not as in items 1 and 2, and $A(x_j)$ is a linear form in at least 2 variables for some $j \in [n]$, then $\mathcal{S}(f(A\mathbf{z})) \geq d_3 + 1$.
4. If A is not as in items 1, 2 and 3, and for some $j \in [n]$, $A(y_j + x_j)$ or $A(y_j - x_j)$ is a linear form in at least 3 variables, then $\mathcal{S}(f(A\mathbf{z})) \geq \frac{d_4^2+3d_4+2}{2}$.
5. If A is not of the form described in the previous four items, then $\mathcal{S}(f(A\mathbf{z})) \geq (d_5 + 1)^3$.

Proof. Like in the proof of Lemma 4.1.1, we analyse $\mathcal{S}(f(A\mathbf{z}))$ with A as listed in the lemma statement. Suppose $A(x_0)$ is a linear form in at least 2 variables. Since $x_0^{d_1}$ divides f, it follows from Claim 2.2.1 that $\mathcal{S}(f(A\mathbf{z})) \geq d_1 + 1$. Similarly, if $A(x_0)$ is a variable while $A(y_0)$ is a linear form in at least 2 variables, then since $y_0^{d_2}$ divides f, $\mathcal{S}(f(A\mathbf{z})) \geq d_2 + 1$ holds by Claim 2.2.1. For the remaining cases, $A(x_0) = x_0$ and $A(y_0) = y_0$ without loss of generality. It then follows from Lemma 3.2.2 that

$$\mathcal{S}(f(A\mathbf{z})) = \mathcal{S}(A(x_0^{d_1} y_0^{d_2+(3n+m+1)(d_3+1)})) + \sum_{i=1}^{n} \mathcal{S}(Q_i(A\mathbf{z})) + \sum_{k=1}^{m} \mathcal{S}(R_k(A\mathbf{z})).$$

The last three cases then can be proved the same way as the last three cases of Lemma 4.1.1 in the non-homogeneous case. □

Proposition 4.2.1. Let $\mathrm{char}(\mathbb{F}) = 0$. If the input in α-gap-ETsparse is an s-sparse homogeneous polynomial, then α-gap-ETsparse is NP-hard for $\alpha = s^{1/3-\epsilon}$.

Proof. If $\psi \in$ 3-SAT, then $\mathcal{S}(f(A\mathbf{z})) \leq s_0$ where A is as described in (3.8). If $\psi \in \overline{\text{3-SAT}}$, then it follows from Lemma 4.2.1 that for any $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$:

$$\mathcal{S}(f(A\mathbf{z})) \geq \min\left(d_1 + 1, d_2 + 1, d_3 + 1, \frac{d_4^2 + 3d_4 + 2}{2}, (d_5 + 1)^3\right).$$

The constraints imposed in (4.2) ensure that $(d_5+1)^3$ is the minimum. As $d_4 = m(d_5+1)^2+1$, therefore $s_0 = 1+n(d_4+3)+m(d_5+1)^2 \leq 3nd_5 = 3mn(d_5+1)^2+3n \leq 4mn(d_5+1)^2$. Thus, the gap in the sparsities of the YES instances and the NO instances is

$$\frac{(d_5+1)^3}{s_0} \geq \frac{(d_5+1)^3}{4mn(d_5+1)^2} = \frac{d_5+1}{4mn}.$$

Also, as $d_5 \geq 4mn$, $\mathcal{S}(f) = s \leq 2m(d_5+1)^3 \implies d_5+1 \geq (\frac{s}{2m})^{1/3}$. Then, the gap is

$$\frac{(d_5+1)^3}{s_0} \geq \frac{d_5+1}{4mn} \geq \frac{s^{1/3}}{2^{1/3}4m^{4/3}n}.$$

Finally, note that $s \geq d_5^3$. Thus, for $d_5^{3\epsilon} \geq (mn)^{O(1)}$ large enough,

$$s^\epsilon \geq d_5^{3\epsilon} \geq 2^{1/3}4m^{4/3}n \implies \frac{s^{1/3}}{2^{1/3}4m^{4/3}n} \geq s^{1/3-\epsilon}.$$

Hence, the gap is at least $s^{1/3-\epsilon}$. Therefore, 3-SAT reduces to α-gap-ETsparse for $\alpha = s^{1/3-\epsilon}$. □

4.3 Extension to finite characteristic fields

In this section, we will show how the construction of Sections 3.1.1 and 3.2, with some changes for appropriate cases, can be used to show the NP-hardness of α-gap-ETsparse over finite characteristic fields for the non-homogeneous case (in the following section) and homogeneous case (in Section 4.3.2), respectively.

4.3.1 The non-homogeneous case

Let the characteristic be p, where $p > 2$. If $p > d_1$, where d_1 is as chosen in Section 4.1, then the argument of that section holds. Hence, it is assumed that $p \leq d_1 = (mn)^{O(1)}$. Consider the polynomial f defined in (3.1). Let $\epsilon \in (0, 1/3)$ be an arbitrary constant. Choose the d_i's to be of form $p^k - 1$ for some $k \in \mathbb{N}$ to satisfy the following inequalities, along with those of (3.2):

$$d_4 \geq \max(3pmn, (mn)^{O(1/\epsilon)}),\ d_3 > m(d_4+1)^2,\ d_2 > (d_3+1)^2,\ d_1 > d_2. \tag{4.3}$$

Note that we can get $d_3 = O(pm(d_4+1)^2)$, $d_2 = O(p(d_3+1)^2)$ and $d_1 = O(pd_2)$. Let $s := \mathcal{S}(f)$. Then, $s = 1+n(2d_3+3)+m(d_4+1)^3$ by Observation 3.1.3. For $\psi \in \overline{\text{3-SAT}}$, Lemma 4.3.1 shows lower bounds on $\mathcal{S}(f(A\mathbf{z}))$ for all $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$. Like Lemma 4.1.1, Lemma 4.3.1 is a slightly deeper analysis of that in the reverse direction of Section 3.3.1. For $\psi \in$ 3-SAT, by Proposition 3.1.1 there exists $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ such that $\mathcal{S}(f(A\mathbf{z})) \leq s_0$, where $s_0 = 1+n(d_3+3)+m(d_4+1)^2$. Proposition 4.3.1 shows the NP-hardness of α-gap-ETsparse using Lemma 4.3.1 and the inequalities in (4.3).

Lemma 4.3.1. Let $\psi \in \overline{\text{3-SAT}}$, f, as defined in (3.1), be the polynomial corresponding to ψ and $A \in \text{GL}(|\mathbf{z}|, \mathbb{F})$.

1. If $A(x_0)$ is a linear form in at least 2 variables, $\mathcal{S}(f(A\mathbf{z})) \geq d_1 + 1$.
2. If A is not as in item 1 and for some $j \in [n]$, $A(x_j)$ is a linear form in at least 2 variables, then $\mathcal{S}(f(A\mathbf{z})) \geq d_2 + 1$.
3. If A is not as in item 1 and 2 and for some $j \in [n]$, $A(y_j + x_j)$ or $A(y_j - x_j)$ is a linear form in at least 3 variables, $\mathcal{S}(f(A\mathbf{z})) \geq (d_3 + 1)^{1.63}$.
4. If A is not of the form described in the previous three cases, then $\mathcal{S}(f(A\mathbf{z})) \geq (d_4 + 1)^3$.

Proof. By Observations 3.1.1, 2.2.3 and the definition of f as in (3.1), it follows that:

$$\mathcal{S}(f(A\mathbf{z})) = \mathcal{S}(A(x_0^{d_1})) + \sum_{i=1}^{n} \mathcal{S}(Q_i(A\mathbf{z})) + \sum_{k=1}^{m} \mathcal{S}(R_k(A\mathbf{z})).$$

We now analyse $\mathcal{S}(f(A\mathbf{z}))$ with A as listed in the lemma statement. The analysis for the first, second and fourth cases is similar to that of the respective cases in the proof of Lemma 4.1.1. In the third case, without loss of generality, let $A(y_j + x_j)$, for some $j \in [n]$, be a linear form in at least 3 variables. By Observation 2.2.4 and the fact that $d_3 = p^k - 1 = \sum_{i=0}^{k-1}(p-1)p^i$ for some $k \in \mathbb{N}$,

$$\mathcal{S}(A((y_j + x_j)^{d_3})) \geq \prod_{i=0}^{k-1} \binom{p-1+3-1}{3-1} = \left(\frac{p(p+1)}{2}\right)^k = (d_3+1)\left(\frac{p+1}{2}\right)^k = (d_3+1)^{1+\log_p(\frac{p+1}{2})}$$

Note, $\log_p(\frac{p+1}{2})$ is an increasing function for $p \geq 3$. Hence, $\log_p(\frac{p+1}{2}) \geq \log_3(4/2) \geq 0.63$. Therefore,

$$\mathcal{S}(f(A\mathbf{z})) \geq \mathcal{S}(Q_{j,2}(A\mathbf{z})) \geq (d_3+1)^{1.63}.$$

Similarly, if $A(y_j - x_j)$ is a linear form in at least 3 variables, then $\mathcal{S}(f(A\mathbf{z})) \geq \mathcal{S}(Q_{j,3}(A\mathbf{z})) \geq (d_3+1)^{1.63}$. □

Proposition 4.3.1. Let $\text{char}(\mathbb{F}) = p > 2$. If the input in α-gap-ETsparse is an s-sparse polynomial, then α-gap-ETsparse is NP-hard for $\alpha = s^{1/3-\epsilon}$.

Proof. The proof is similar to that of Proposition 4.1.1. If ψ is satisfiable, then $\mathcal{S}(f(A\mathbf{z})) \leq s_0$ where A is as described in (3.4) and $s_0 = 1 + n(d_3+3) + m(d_4+1)^2$. For unsatisfiable ψ, it follows from Lemma 4.3.1 that for any $A \in \text{GL}(|\mathbf{z}|, \mathbb{F})$:

$$\mathcal{S}(f(A\mathbf{z})) \geq \min(d_1+1, d_2+1, (d_3+1)^{1.63}, (d_4+1)^3).$$

As $d_3 > m(d_4+1)^2$, therefore $s_0 = 1 + n(d_3+3) + m(d_4+1)^2 \leq 3nd_3 \leq 3pmn(d_4+1)^2$. The conditions imposed in (4.3) ensure that $d_1 + 1 > d_2 + 1 > (d_3+1)^{1+\log_p((p+1)/2)} > (d_4+1)^3 > s_0$. Thus, the gap in the sparsities of the YES instances and NO instances is

$$\frac{(d_4+1)^3}{s_0} \geq \frac{(d_4+1)^3}{3pmn(d_4+1)^2} = \frac{d_4+1}{3pmn}.$$

Also, note as $d_4 \geq 3pmn$, therefore $s \leq 2m(d_4+1)^3 \implies d_4+1 \geq (\frac{s}{2m})^{1/3}$. Then, the gap is

$$\frac{(d_4+1)^3}{s_0} \geq \frac{d_4+1}{3pmn} \geq \frac{s^{1/3}}{p2^{1/3}3m^{4/3}n}.$$

Finally, note that $s \geq d_4^3$. Thus, for $d_4^{3\epsilon} \geq (mn)^{O(1)}$ large enough,

$$s^\epsilon \geq d_4^{3\epsilon} \geq p2^{1/3}3m^{4/3}n \implies \frac{s^{1/3}}{p2^{1/3}3m^{4/3}n} \geq s^{1/3-\epsilon}.$$

Hence, the gap is at least $s^{1/3-\epsilon}$. Therefore, 3-SAT reduces to α-gap-ETsparse for $\alpha = s^{1/3-\epsilon}$. □

Analysis over characteristic 2 fields

In this case, we consider the construction of Section 3.3.1. For a 3-CNF ψ, let f be the corresponding polynomial as defined in (3.9). Let $s := \mathcal{S}(f)$. Over characteristic 2 fields, the value of s depends on the number of variables complemented in a clause. To show the hardness of α-gap-ETsparse, we require $s \geq d_4^3$ (see the proof of Proposition 4.3.2). This can be achieved if there exists a clause with all variables complemented. Hence, we assume, without loss of generality, that there is such a clause in ψ.[1] The d_i's are chosen in the same way as in Section 4.3.1 to satisfy (4.3) with p set to 2. In particular, they satisfy the following inequalities.

$$d_4 \geq \max(6mn, (mn)^{O(1/\epsilon)}),\ d_3 > m(d_4+1)^2,\ d_2 > (d_3+1)^2,\ d_1 > d_2. \tag{4.4}$$

By Observation 3.3.1 and the assumption on ψ, it holds that

$$1 + n(d_3+3) + (d_4+1)^3 \leq s \leq 1 + n(d_3+3) + m(d_4+1)^3.$$

For $\psi \in \overline{\text{3-SAT}}$, Lemma 4.3.2 shows lower bounds on $\mathcal{S}(f(A\mathbf{z}))$ where $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$. For $\psi \in$ 3-SAT, by Proposition 3.3.1 there exists $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ such that $\mathcal{S}(f(A\mathbf{z})) \leq s_0$, where $s_0 = 1 + n(d_3+3) + m(d_4+1)^2$. Proposition 4.3.2 shows the NP-hardness of α-gap-ETsparse using Lemma 4.3.2 and the inequalities in (4.4).

[1] To have some clause, say the first one, contain only complemented variables, every uncomplemented variable x in the clause can be replaced by $\neg x$ followed by complementing each occurrence of x in the remaining clauses.

Lemma 4.3.2. Let $\psi \in \overline{\text{3-SAT}}$, f, as defined in (3.9), be the polynomial corresponding to ψ and $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$.

1. If $A(x_0)$ is a linear form in at least 2 variables, $\mathcal{S}(f(A\mathbf{z})) \geq d_1 + 1$.
2. If A is not as in item 1 and for some $j \in [n]$, $A(x_j)$ is a linear form in at least 2 variables, then $\mathcal{S}(f(A\mathbf{z})) \geq d_2 + 1$.
3. If A is not as in item 1 and 2 and for some $j \in [n]$, $A(y_j + x_j)$ or $A(y_j)$ is a linear form in at least 3 variables, $\mathcal{S}(f(A\mathbf{z})) \geq (d_3 + 1)^{1.58}$.
4. If A is not of the form described in the previous three cases, then $\mathcal{S}(f(A\mathbf{z})) \geq (d_4 + 1)^3$.

Proof. The proof of this lemma is very similar to that of Lemma 4.3.1. In particular, the analysis for the first, second and fourth cases is similar to that of the respective cases in the proof of Lemma 4.3.1. So, we consider the third case. Without loss of generality, let $A(y_j + x_j)$ be a linear form in at least 3 variables for some $j \in [n]$. Then, by Observation 2.2.4 and the fact that $d_3 = 2^k - 1 = \sum_{i=0}^{k-1} 2^i$ for some $k \in \mathbb{N}$,

$$\mathcal{S}(A((y_j + x_j)^{d_3})) \geq \prod_{i=0}^{k-1} \binom{1+3-1}{3-1} = 3^k = (d_3+1)^{\log_2 3} \geq (d_3+1)^{1.58}.$$

Therefore

$$\mathcal{S}(f(A\mathbf{z})) \geq \mathcal{S}(Q_{j,2}(A\mathbf{z})) \geq (d_3+1)^{1.58}.$$

Similarly, if $A(y_j)$ is a linear form in at least 3 variables, then $\mathcal{S}(f(A\mathbf{z})) \geq \mathcal{S}(Q_{j,3}(A\mathbf{z})) \geq (d_3+1)^{1.58}$.

□

Proposition 4.3.2. Let $\mathrm{char}(\mathbb{F}) = 2$. If the input in α-gap-ETsparse is an s-sparse polynomial, then α-gap-ETsparse is NP-hard for $\alpha = s^{1/3-\epsilon}$.

Proof. The proof is similar to that of Proposition 4.3.1. If ψ is satisfiable, then $\mathcal{S}(f(A\mathbf{z})) \leq s_0$ where A is as described in (3.4) and $s_0 = 1 + n(d_3+3) + m(d_4+1)^2$. For unsatisfiable ψ, it follows from Lemma 4.3.1 that for any $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$:

$$\mathcal{S}(f(A\mathbf{z})) \geq \min(d_1+1, d_2+1, (d_3+1)^{1.58}, (d_4+1)^3).$$

As $d_3 > m(d_4+1)^2$, therefore $s_0 = 1 + n(d_3+3) + m(d_4+1)^2 \leq 3nd_3 \leq 6mn(d_4+1)^2$. The conditions imposed in (4.4) ensure that $d_1 + 1 > d_2 + 1 > (d_3+1)^{1.58} > (d_4+1)^3 > s_0$. Consequently, the gap in the sparsities of the YES instances and NO instances is

$$\frac{(d_4+1)^3}{s_0} \geq \frac{(d_4+1)^3}{6mn(d_4+1)^2} = \frac{d_4+1}{6mn}.$$

Also, note as $d_4 \geq 6mn$, therefore $s \leq 2m(d_4+1)^3 \implies d_4+1 \geq (\frac{s}{2m})^{1/3}$. Then, the gap is

$$\frac{(d_4+1)^3}{s_0} \geq \frac{d_4+1}{6mn} \geq \frac{s^{1/3}}{2^{4/3}3m^{4/3}n}.$$

Finally, note that $s \geq d_4^3$. Thus, for $d_4^{3\epsilon} \geq (mn)^{O(1)}$ large enough,

$$s^\epsilon \geq d_4^{3\epsilon} \geq 2^{4/3}3m^{4/3}n \implies \frac{s^{1/3}}{2^{4/3}3m^{4/3}n} \geq s^{1/3-\epsilon}.$$

Hence, the gap is at least $s^{1/3-\epsilon}$. Therefore, 3-SAT reduces to α-gap-ETsparse for $\alpha = s^{1/3-\epsilon}$. □

4.3.2 The homogeneous case

Let the characteristic be p, where $p > 2$. If $p > d_1$, where d_1 is as chosen in Section 4.2, then the argument of that section holds. Hence, assume $p \leq d_1 = O((mn)^{O(1)})$. Consider the polynomial f defined in (3.7). Choose d_3, d_4 and d_5 to be of form $p^k - 1$ for some $k \in \mathbb{N}$ while also satisfying:

$$d_5 \geq \max(3pmn, (mn)^{O(1/\epsilon)}),\ d_4 > m(d_5+1)^2,\ d_3 > (d_4+1)^2. \tag{4.5}$$

Thus, $d_4 = O(pm(d_5+1)^2)$ and $d_3 = O(p(d_4+1)^2)$. Now, let $k_1 := \lfloor \log_p(d_3+2) \rfloor + 1, k_2 := \lfloor \log_p((3n+m+1)(d_3+1)) \rfloor + 1$, then set

$$d_2 := \sum_{i=k_2}^{k_1+k_2-1} (p-1)p^i = p^{k_1+k_2} - p^{k_2}. \tag{4.6}$$

Lastly, let $k_3 := \lfloor \log_p(d_2 + (3n+m+1)(d_3+1)) \rfloor + 1$, then set

$$d_1 := \sum_{i=k_3}^{k_3+k_1-1} (p-1)p^i = p^{k_1+k_3} - p^{k_3}. \tag{4.7}$$

For this choice of the d_i's, the conditions in (3.5) are satisfied. Let $s := \mathcal{S}(f)$. By Observation 3.2.2, $s = 1 + n(2d_4+3) + m(d_5+1)^3$. For $\psi \in \overline{\text{3-SAT}}$, Lemma 4.3.3 shows lower bounds on $\mathcal{S}(f(A\mathbf{z}))$ for all $A \in \text{GL}(|\mathbf{z}|, \mathbb{F})$. Like Lemma 4.2.1, Lemma 4.3.3 is a slightly deeper analysis of that in the reverse direction of Section 3.3.3 For $\psi \in$ 3-SAT, by Proposition 3.2.1 there exists $A \in \text{GL}(|\mathbf{z}|, \mathbb{F})$ such that $\mathcal{S}(f(A\mathbf{z})) \leq s_0$, where $s_0 = 1 + n(d_4+3) + m(d_5+1)^2$. Proposition 4.3.3 shows the NP-hardness of α-gap-ETsparse using Lemma 4.3.3 and the setting of the d_i's in this section.

Lemma 4.3.3. Let $\psi \in \overline{\text{3-SAT}}$, f, as defined in (3.7), be the polynomial corresponding to ψ and $A \in \text{GL}(|\mathbf{z}|, \mathbb{F})$.

1. If $A(x_0)$ or $A(y_0)$ is a linear form in at least 2 variables, $\mathcal{S}(f(A\mathbf{z})) \geq d_3 + 2$.
2. If A is not as in item 1 and $A(x_j)$ is a linear form in at least 2 variables for some $j \in [n]$, then $\mathcal{S}(f(A\mathbf{z})) \geq d_3 + 1$.
3. If A is not as in items 1 and 2 and for some $j \in [n]$, $A(y_j + x_j)$ or $A(y_j - x_j)$ is a linear form in at least 3 variables, $\mathcal{S}(f(A\mathbf{z})) \geq (d_4 + 1)^{1.63}$.
4. If A is not of the form described in the previous three cases, then $\mathcal{S}(f(A\mathbf{z})) \geq (d_5 + 1)^3$.

Proof. Suppose $A(x_0)$ is a linear form in at least two variables. Applying the argument in the proof of Lemma 3.2.2 for the finite characteristic case (refer Section **??**) shows that

$$\mathcal{S}(f(A\mathbf{z})) \geq \mathcal{S}(A(x_0)^{d_1}) \geq p^{k_1+1} \geq d_3 + 2.$$

Similarly, if $A(x_0)$ is a variable and $A(y_0)$ is a linear form in at least two variables, the same argument shows that

$$\mathcal{S}(f(A\mathbf{z})) \geq \mathcal{S}(A(y_0)^{d_2}) \geq p^{k_1+1} \geq d_3 + 2.$$

For the remaining cases, $A(x_0) = x_0$ and $A(y_0) = y_0$ without loss of generality. It then follows from Lemma 3.2.2 that

$$\mathcal{S}(f(A\mathbf{z})) = \mathcal{S}(A(x_0^{d_1} y_0^{d_2+(3n+m+1)(d_3+1)})) + \sum_{i=1}^{n} \mathcal{S}(Q_i(A\mathbf{z})) + \sum_{k=1}^{m} \mathcal{S}(R_k(A\mathbf{z})).$$

The last three cases can then be proved in the same way as the last three cases of Lemma 4.3.1.

□

Proposition 4.3.3. Let $\mathrm{char}(\mathbb{F}) = p > 2$. If the input in α-gap-ETsparse is an s-sparse homogeneous polynomial, then α-gap-ETsparse is NP-hard for $\alpha = s^{1/3-\epsilon}$.

Proof. The proof is similar to that of Proposition 4.2.1. If $\psi \in$ 3-SAT, then $\mathcal{S}(f(A\mathbf{z})) \leq s_0$ where A is as described in (3.8). If $\psi \in \overline{\text{3-SAT}}$, then it follows from Lemma 4.3.1 that for any $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$:

$$\mathcal{S}(f(A\mathbf{z})) \geq \min\left(d_3 + 2, d_3 + 1, (d_4 + 1)^{1.63}, (d_5 + 1)^3\right).$$

The constraints imposed in (4.1) ensure that $(d_5 + 1)^3$ is the minimum. As $d_4 > m(d_5 + 1)^2$, therefore $s_0 = 1 + n(d_4 + 3) + m(d_5 + 1)^2 < 3nd_4 \leq 3pmn(d_5 + 1)^2$. Thus, the gap in the sparsities of the YES instances and the NO instances is

$$\frac{(d_5+1)^3}{s_0} \geq \frac{(d_5+1)^3}{3pmn(d_5+1)^2} = \frac{d_5+1}{3pmn}.$$

Also, as $d_5 \geq 3pmn$, $\mathcal{S}(f) = s \leq 2m(d_5+1)^3 \implies d_5 + 1 \geq (\frac{s}{2m})^{1/3}$. Then, the gap is

$$\frac{(d_5+1)^3}{s_0} \geq \frac{d_5+1}{3pmn} \geq \frac{s^{1/3}}{p2^{1/3}3m^{4/3}n}.$$

Finally, note that $s \geq d_5^3$. Thus, for $d_5^{3\epsilon} \geq (mn)^{O(1)}$ large enough,

$$s^\epsilon \geq d_5^{3\epsilon} \geq p2^{1/3}3m^{4/3}n \implies \frac{s^{1/3}}{p2^{1/3}3m^{4/3}n} \geq s^{1/3-\epsilon}.$$

Hence, the gap is at least $s^{1/3-\epsilon}$. Therefore, 3-SAT reduces to α-gap-ETsparse for $\alpha = s^{1/3-\epsilon}$. □

Analysis over characteristic 2 fields

For characteristic 2 fields, consider the polynomial f as defined in (3.11). Let $s := \mathcal{S}(f)$. Like in the characteristic 2 construction for the non-homogeneous case, the value of s depends on the number of variables complemented within a clause. To show the NP-hardness of α-gap-ETsparse, $s \geq d_5^3$ is required (see the proof of Proposition 4.3.4), which can be achieved if there is at least one clause where all variables are complemented. Therefore, we assume that such a clause exists (see footnote 1). Set the d_i's as specified in the beginning of Section 4.3.2 with $p = 2$. For this setting of the d_i's, the constraints in (3.5) are satisfied. By Observation 3.3.2 and the assumption on ψ, it holds that

$$1 + n(d_4+3) + (d_5+1)^3 \leq s \leq 1 + n(d_4+3) + m(d_5+1)^3.$$

For $\psi \in \overline{\text{3-SAT}}$, Lemma 4.3.4 shows lower bounds on $\mathcal{S}(f(A\mathbf{z}))$ for all $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$. For $\psi \in$ 3-SAT, by Proposition 3.3.3 there exists $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ such that $\mathcal{S}(f(A\mathbf{z})) \leq s_0$, where $s_0 = 1 + n(d_4+3) + m(d_5+1)^2$. Proposition 4.3.4 shows the NP-hardness of α-gap-ETsparse using Lemma 4.3.4 and the setting of the d_i's in this section.

Lemma 4.3.4. Let $\psi \in \overline{\text{3-SAT}}$, f, as defined in (3.11), be the polynomial corresponding to ψ and $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$.

1. If $A(x_0)$ or $A(y_0)$ is a linear form in at least 2 variables, $\mathcal{S}(f(A\mathbf{z})) \geq d_3 + 2$.
2. If A is not as in item 1 and $A(x_j)$ is a linear form in at least 2 variables for some $j \in [n]$, then $\mathcal{S}(f(A\mathbf{z})) \geq d_3 + 1$.
3. If A is not as in items 1 and 2 and for some $j \in [n]$, $A(y_j + x_j)$ or $A(y_j - x_j)$ is a linear form in at least 3 variables, $\mathcal{S}(f(A\mathbf{z})) \geq (d_4+1)^{1.58}$.
4. If A is not of the form described in the previous three cases, then $\mathcal{S}(f(A\mathbf{z})) \geq (d_5 + 1)^3$.

Proof. Suppose $A(x_0)$ is a linear form in at least two variables. Applying the argument in the proof of Lemma 3.2.2 for the finite characteristic case (refer Section **??**) shows that

$$\mathcal{S}(f(A\mathbf{z})) \geq \mathcal{S}(A(x_0)^{d_1}) \geq 2^{k_1+1} \geq d_3 + 2.$$

Similarly, if $A(x_0)$ is a variable and $A(y_0)$ is a linear form in at least two variables, the same argument shows that

$$\mathcal{S}(f(A\mathbf{z})) \geq \mathcal{S}(A(y_0)^{d_2}) \geq 2^{k_1+1} \geq d_3 + 2.$$

For the remaining cases, $A(x_0) = x_0$ and $A(y_0) = y_0$ without loss of generality. It then follows from Lemma 3.2.2 that

$$\mathcal{S}(f(A\mathbf{z})) = \mathcal{S}(A(x_0^{d_1} y_0^{d_2+(3n+m+1)(d_3+1)})) + \sum_{i=1}^{n} \mathcal{S}(Q_i(A\mathbf{z})) + \sum_{k=1}^{m} \mathcal{S}(R_k(A\mathbf{z})).$$

The last three cases can then be proved in the same way as the last three cases of Lemma 4.3.2. □

Proposition 4.3.4. Let $\mathrm{char}(\mathbb{F}) = 2$. If the input in α-gap-ETsparse is an s-sparse homogeneous polynomial, then α-gap-ETsparse is NP-hard for $\alpha = s^{1/3-\epsilon}$.

Proof. The proof is similar to that of Proposition 4.3.3. If $\psi \in$ 3-SAT, then $\mathcal{S}(f(A\mathbf{z})) \leq s_0$ where A is as described in (3.12). If $\psi \in \overline{\text{3-SAT}}$, then it follows from Lemma 4.3.1 that for any $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$:

$$\mathcal{S}(f(A\mathbf{z})) \geq \min\left(d_3 + 2, d_3 + 1, (d_4+1)^{1.58}, (d_5+1)^3\right).$$

The constraints imposed in (4.1) ensure that $(d_5+1)^3$ is the minimum. As $d_4 > m(d_5+1)^2$, therefore $s_0 = 1 + n(d_4+3) + m(d_5+1)^2 < 3nd_4 \leq 6mn(d_5+1)^2$. Thus, the gap in the sparsities of the YES instances and the NO instances is

$$\frac{(d_5+1)^3}{s_0} \geq \frac{(d_5+1)^3}{6mn(d_5+1)^2} = \frac{d_5+1}{6mn}.$$

Also, as $d_5 \geq 6mn$, $s \leq 2m(d_5+1)^3 \implies d_5 + 1 \geq (\frac{s}{2m})^{1/3}$. Then, the gap is

$$\frac{(d_5+1)^3}{s_0} \geq \frac{d_5+1}{6mn} \geq \frac{s^{1/3}}{2^{4/3}3m^{4/3}n}.$$

Finally, note that $s \geq d_5^3$. Thus, for $d_5^{3\epsilon} \geq (mn)^{O(1)}$ large enough,

$$s^\epsilon \geq d_5^{3\epsilon} \geq 2^{4/3}3m^{4/3}n \implies \frac{s^{1/3}}{2^{4/3}3m^{4/3}n} \geq s^{1/3-\epsilon}.$$

Hence, the gap is at least $s^{1/3-\epsilon}$. Therefore, 3-SAT reduces to α-gap-ETsparse for $\alpha = s^{1/3-\epsilon}$. □

4.4 Extending Theorem 2 for translations

In this section, we prove part 1 of Theorem 2 over all fields while considering translations. The proof involves a careful analysis of the sparsity of f as defined corresponding to a 3-CNF ψ. We split the proof into two cases: over characteristic 0 fields and finite characteristic fields. The reason for the split is that in the analysis, we consider the sparsity of powers of affine forms $h = \ell + c$, where $\mathcal{S}(h) \geq 3$. The sparsity of such affine forms depends on the underlying field, as shown in the following analysis using Observation 2.2.4 and the binomial theorem. Note that we take $\epsilon \in (0, 1/3)$ to be an arbitrary constant throughout this section.

4.4.1 For characteristic 0 fields

Consider the polynomial f as defined in (3.17) for a 3-CNF ψ and choose the d_i's to be $(mn)^{O(1)}$ and also satisfy the following conditions:

$$d_4 \geq \max(4mn, (mn)^{O(1/\epsilon)}),\ d_3 = m(d_4+1)^2 + 1,\ d_2 = d_3^2 + 1,\ d_1 = 6nd_2 + 6n + 2d_3 + 2. \tag{4.8}$$

Note that the constraints in (3.16) are also satisfied under (4.8). Let $s := \mathcal{S}(f)$. By Observation 3.4.3, $s = 1 + n(2d_3 + 3) + m(d_4+1)^3$. From Section 3.4, it follows that for satisfiable ψ's, there exists $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$, $\mathbf{b} = \mathbf{0}$ such that $\mathcal{S}(f(A\mathbf{z})) \leq s_0$, where $s_0 = 1 + n(d_3+3) + m(d_4+1)^2$. For unsatisfiable ψ's, Lemma 4.4.1 gives lower bounds on $\mathcal{S}(f(A\mathbf{z}+\mathbf{b}))$, where $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^{|\mathbf{z}|}$, and encapsulates the argument of the reverse direction of the reduction in Section 3.4 with a slightly deeper analysis. Comparing the sparsities for satisfiable and unsatisfiable ψ's proves part 1 of Theorem 2 for translations. Proposition 4.4.1 shows α-gap-ETsparse is NP-hard using Lemma 4.4.1 and the conditions in (4.8).

Lemma 4.4.1. Let $\psi \in \overline{\text{3-SAT}}$, f, as defined in (3.17), be the polynomial corresponding to ψ, $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^{|\mathbf{z}|}$.

1. If $A(x_0) + \mathbf{b}_{|x_0}$ is a non-trivial affine form, then $\mathcal{S}(f(A\mathbf{z}+\mathbf{b})) \geq \frac{d_1}{2}$.[2]
2. If A and $\mathbf{b}$ are not as in item 1 and for some $j \in [n]$, $A(x_j) + \mathbf{b}_{|x_j}$ is a non-trivial affine form, then $\mathcal{S}(f(A\mathbf{z}+\mathbf{b})) \geq d_2 + 1$.
3. If A and $\mathbf{b}$ are not as in items 1 and 2 and for some $j \in [n]$, $\mathcal{S}(A(y_j + x_j) + \mathbf{b}_{|y_j}) \geq 3$ or $\mathcal{S}(A(y_j - x_j) + \mathbf{b}_{|y_j}) \geq 3$, then $\mathcal{S}(f(A\mathbf{z}+\mathbf{b})) \geq \frac{(d_3+1)(d_3+2)}{2}$.

[2] an affine form $\ell + c$, where ℓ is a linear form and c is a constant, is non-trivial if ℓ is a linear form in at least two variables or $c \neq 0$ or both.

4. If A and $\mathbf{b}$ are not of the form described in the previous three cases, then $\mathbf{b} = \mathbf{0}$ and $\mathcal{S}(f(A\mathbf{z})) \geq (d_4+1)^3$.

Proof. 1. The proof of this case follows from the argument in the proof of Lemma 3.4.1. Henceforth, we assume $A(x_0) = x_0$ and $\mathbf{b}_{|x_0} = 0$. Then, by Lemma 3.4.2, it follows that

$$\mathcal{S}(f(A\mathbf{z}+\mathbf{b})) = \mathcal{S}(x_0^{d_1}) + \sum_{i=1}^{n} \mathcal{S}(Q_i(A\mathbf{z}+\mathbf{b})) + \sum_{k=1}^{m} \mathcal{S}(R_k(A\mathbf{z}+\mathbf{b})).$$

2. By Lemma 3.4.2 and Observation 2.2.6 (applied to $Q_{i,1}(A\mathbf{z}+\mathbf{b})$) it follows that

$$\mathcal{S}(f(A\mathbf{z}+\mathbf{b})) \geq \mathcal{S}(Q_{i,1}(A\mathbf{z}+\mathbf{b})) \geq d_2+1.$$

3. In this case, for $i \in [0,n]$, $A(x_i)$ is some scaled variable in $\mathbf{z}$ and $\mathbf{b}_{|x_i} = 0$. If $\mathbf{b}_{|y_j} = 0$, then this case is the same as the third case of Lemma 4.1.1. Otherwise, let $A(y_j + x_j) + \mathbf{b}_{|y_j} = \ell_j + b_j$, where ℓ_j is a linear form in at least two variables. Then, using the binomial theorem and Observations 2.2.2 and 2.2.4, it follows that

$$\mathcal{S}((\ell_j+b_j)^{d_3}) = \mathcal{S}\Big(\sum_{i=0}^{d_3}\binom{d_3}{i} b_j^{d_3-i}\ell_j^i\Big) = \sum_{i=0}^{d_3}\mathcal{S}\Big(\binom{d_3}{i} b_j^{d_3-i}\ell_j^i\Big) \geq \sum_{i=0}^{d_3}(i+1) = \frac{(d_3+1)(d_3+2)}{2}.$$

Thus,

$$\mathcal{S}(f(A\mathbf{z}+\mathbf{b})) \geq \mathcal{S}(Q_{i,2}(A\mathbf{z}+\mathbf{b})) \geq \frac{(d_3+1)(d_3+2)}{2}.$$

Similarly, if $\mathcal{S}(A(y_j - x_j) + \mathbf{b}_{|y_j}) \geq 3$, then $\mathcal{S}(f(A\mathbf{z}+\mathbf{b})) \geq \frac{(d_3+1)(d_3+2)}{2}$.

4. In this case, for $i \in [0,n]$, $A(x_i) = X_i$ and $\mathbf{b}_{|x_i} = 0$. For $i \in [n]$, $\mathcal{S}(A(y_i + x_i) + \mathbf{b}_{|y_i}) \leq 2$ and $\mathcal{S}(A(y_i - x_i) + \mathbf{b}_{|y_i}) \leq 2$. As A is invertible, $\mathcal{S}(A(y_i + x_i)) \geq 1$ and $\mathcal{S}(A(y_i - x_i)) \geq 1$. If $\mathcal{S}(A(y_i + x_i)) \geq 2$ or $\mathcal{S}(A(y_i - x_i)) \geq 2$, then $\mathbf{b}_{|y_i}$ must be 0. Further, as A is invertible and $A(x_i) = X_i$, therefore if $\mathcal{S}(A(y_i + x_i)) = 1$, then $\mathcal{S}(A(y_i - x_i)) \geq 2$ and vice versa also holds, which again implies $\mathbf{b}_{|y_i} = 0$. Thus, for all $i \in [n]$, $\mathbf{b}_{|y_i} = 0$ implying $\mathbf{b} = \mathbf{0}$. This case can then be proved in the same way as the last case of Lemma 4.1.1.

□

Proposition 4.4.1. Let $\mathrm{char}(\mathbb{F}) = 0$. If the input in α-gap-ETsparse is an s-sparse polynomial, then α-gap-ETsparse is NP-hard for $\alpha = s^{1/3-\epsilon}$.

Proof. The proof is similar to that of Proposition 4.1.1. If $\psi \in$ 3-SAT, then $\mathcal{S}(f(A\mathbf{z})) \leq s_0$ where A is as described in (3.4) and $s_0 = 1 + n(d_3+3) + m(d_4+1)^2$. If $\psi \in \overline{\text{3-SAT}}$, it follows from Lemma 4.4.1 that for any $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^{|\mathbf{z}|}$:

$$\mathcal{S}(f(A\mathbf{z}+\mathbf{b})) \geq \min\Big(\frac{d_1}{2}, d_2+1, \frac{d_3^2+3d_3+2}{2}, (d_4+1)^3\Big).$$

The conditions imposed in (4.1) ensure that $(d_4+1)^3 > s_0$ and $(d_4+1)^3$ is the minimum. As $d_3 = m(d_4+1)^2+1$, therefore $s_0 = 1+n(d_3+3)+m(d_4+1)^2 \leq 3nd_3 \leq 4mn(d_4+1)^2$. Consequently, the gap in the sparsities of the YES instances and NO instances is

$$\frac{(d_4+1)^3}{s_0} \geq \frac{(d_4+1)^3}{4mn(d_4+1)^2} = \frac{d_4+1}{4mn}.$$

Also, note that as $d_4 \geq 4mn$, therefore $s \leq 2m(d_4+1)^3 \implies d_4+1 \geq (\frac{s}{2m})^{1/3}$. Then, the gap is

$$\frac{(d_4+1)^3}{s_0} \geq \frac{d_4+1}{4mn} \geq \frac{s^{1/3}}{2^{1/3}4m^{4/3}n}.$$

Finally, note that $s \geq d_4^3$. Thus, for $d_4^{3\epsilon} \geq (mn)^{O(1)}$ large enough,

$$s^\epsilon \geq d_4^{3\epsilon} \geq 2^{1/3}4m^{4/3}n \implies \frac{s^{1/3}}{2^{1/3}4m^{4/3}n} \geq s^{1/3-\epsilon}.$$

Hence, the gap is at least $s^{1/3-\epsilon}$. Therefore, 3-SAT reduces to α-gap-ETsparse for $\alpha = s^{1/3-\epsilon}$.

□

4.4.2 For finite characteristic fields

Let the characteristic be p, where $p > 2$. If $p > d_1$, where d_1 is as chosen in Section 4.4.1, then the argument of that section holds. Hence, it is assumed that $p \leq d_1 = (mn)^{O(1)}$. We again consider the polynomial f as defined in (3.17) and impose the following constraints on the d_i's.

$$d_4 \geq \max(3pmn, (mn)^{O(1/\epsilon)}),\ d_3 > m(d_4+1)^2,\ d_2 > (d_3+1)^2,\ d_1 > 6nd_2+6n+2d_3+2. \tag{4.9}$$

Note, we can get $d_3 = O(pm(d_4+1)^2)$, $d_2 = O(p(d_3+1)^2)$ and $d_1 = O(p(6nd_2+6n+2d_3+2))$. The conditions of (3.16) are also satisfied under (4.9). From Section 3.4, it follows that for satisfiable ψ's, there exists $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$, $\mathbf{b} = \mathbf{0}$ such that $\mathcal{S}(f(A\mathbf{z})) \leq s_0$, where $s_0 = 1+n(d_3+3)+m(d_4+1)^2$. For unsatisfiable ψ's, Lemma 4.4.2 gives lower bounds on $\mathcal{S}(f(A\mathbf{z}+\mathbf{b}))$, where $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^{|\mathbf{z}|}$. Proposition 4.4.2 shows α-gap-ETsparse is NP-hard using Lemma 4.4.2 and the constraints in (4.9).

Lemma 4.4.2. Let $\psi \in \overline{\text{3-SAT}}$, $f(\mathbf{z})$ be as defined in (3.17) corresponding to ψ, $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^{|\mathbf{z}|}$.

1. If $A(x_0) + \mathbf{b}_{|x_0}$ is a non-trivial affine form, then $\mathcal{S}(f(A\mathbf{z}+\mathbf{b})) \geq \frac{d_1}{2}$.
2. If A and $\mathbf{b}$ are not as in item 1 and for some $j \in [n]$, $A(x_j) + \mathbf{b}_{|x_j}$ is a non-trivial affine form, then $\mathcal{S}(f(A\mathbf{z}+\mathbf{b})) \geq d_2+1$.

3. If A and $\mathbf{b}$ are not as in items 1 and 2 and for some $j \in [n]$, $\mathcal{S}(A(y_j + x_j) + \mathbf{b}_{|y_j}) \geq 3$ or $\mathcal{S}(A(y_j - x_j) + \mathbf{b}_{|y_j}) \geq 3$, then $\mathcal{S}(f(A\mathbf{z} + \mathbf{b})) \geq (d_3 + 1)^{1.63}$.

4. If A and $\mathbf{b}$ are not of the form described in the previous three cases, then $\mathbf{b} = \mathbf{0}$ and $\mathcal{S}(f(A\mathbf{z})) \geq (d_4 + 1)^3$.

Proof. The first, second and fourth cases can be proved similarly to those of Lemma 4.4.1. Hence, we consider the third case. Then, for $i \in [0, n]$, $A(x_i)$ is some scaled variable in $\mathbf{z}$ and $\mathbf{b}_{|x_i} = 0$. If $\mathbf{b}_{|y_j} = 0$, then this case is the same as the third case of Lemma 4.3.1. If $\mathbf{b}_{|y_j} \neq 0$, then, without loss of generality, $A(y_j + x_j) + \mathbf{b}_{|y_j} = \ell_j + b_j$, with ℓ_j a linear form in at least two variables. Using the binomial theorem, the fact that $d_3 = p^k - 1 = \sum_{i=0}^{k-1}(p-1)p^i$, Lucas's theorem and Observations 2.2.2 and 2.2.4 gives

$$\mathcal{S}((\ell_j + b_j)^{d_3}) = \mathcal{S}\left(\sum_{i=0}^{d_3}\binom{d_3}{i} b_j^{d_3-i}\ell_j^i\right) = \sum_{i=0}^{d_3}\mathcal{S}\left(\binom{d_3}{i} b_j^{d_3-i}\ell_j^i\right)$$

$$\geq \sum_{i=0}^{d_3}\prod_{l=0}^{k-1}\binom{e_{i,l}+2-1}{2-1} = \sum_{i=0}^{d_3}\prod_{l=0}^{k-1}(e_{i,l}+1)$$

where $i = \sum_{l=0}^{k-1} e_{i,l}p^l$ with $e_{i,l} \in [0, p-1]$ ($e_{i,l}$ represents the l^{th} "digit" in the base-p expansion of i). Note that for $i = rp$, where $r \in [0, p^{k-1} - 1]$, the value of $e_{t,l}$, where $l \geq 1$ and $t \in [i, i + p - 1]$, is the same for all t while $e_{t,0} = t - i$. Therefore, for such i's, the following holds

$$\sum_{t=i}^{i+p-1}\prod_{l=0}^{k-1}(e_{t,l}+1) = \left(\prod_{l=1}^{k-1}(e_{rp,l}+1)\right)\cdot\sum_{t=rp}^{rp+p-1}(t - rp + 1) = \frac{p(p+1)}{2}\prod_{l=1}^{k-1}(e_{rp,l}+1).$$

Using the above observation and the fact that $d_3 = p^k - 1$,

$$\sum_{i=0}^{d_3}\prod_{l=0}^{k-1}(e_{i,l}+1) = \sum_{r=0}^{p^{k-1}-1}\sum_{t=0}^{p-1}\prod_{l=0}^{k-1}(e_{rp+t,l}+1) = \frac{p(p+1)}{2}\sum_{r=0}^{p^{k-1}-1}\prod_{l=1}^{k-1}(e_{rp,l}+1).$$

By repeating the same argument, we get

$$\sum_{i=0}^{d_3}\prod_{l=0}^{k-1}(e_{i,l}+1) = \left(\frac{p(p+1)}{2}\right)^k = (d_3+1)^{1+\log_p((p+1)/2)}.$$

Now, $\log_p((p+1)/2)$ is an increasing function for $p \geq 3$. Thus, $\log_p((p+1)/2) \geq \log_3((3+1)/2) \geq 0.63$. We can then conclude that

$$\mathcal{S}(f(A\mathbf{z})) \geq \mathcal{S}(Q_{j,2}(A\mathbf{z} + \mathbf{b})) \geq (d_3+1)^{1.63}.$$

Similarly, if $\mathcal{S}(A(y_j - x_j) + \mathbf{b}_{|y_j}) \geq 3$, then $\mathcal{S}(f(A\mathbf{z} + \mathbf{b})) \geq \mathcal{S}(Q_{j,3}(A\mathbf{z} + \mathbf{b})) \geq (d_3 + 1)^{1.63}$. □

Proposition 4.4.2. Let $\text{char}(\mathbb{F}) = p > 2$. If the input in α-gap-ETsparse is an s-sparse polynomial, then α-gap-ETsparse is NP-hard for $\alpha = s^{1/3-\epsilon}$.

Proof. The proof is similar to that of Proposition 4.4.1. For the polynomial f defined in (3.17), $s := \mathcal{S}(f) = 1 + n(2d_3 + 3) + m(d_4 + 1)^3$. If $\psi \in$ 3-SAT, then $\mathcal{S}(f(A\mathbf{z})) \leq s_0$ where A is as described in (3.4) and $s_0 = 1 + n(d_3 + 3) + m(d_4 + 1)^2$. If $\psi \in \overline{\text{3-SAT}}$, it follows from Lemma 4.4.1 that for any $A \in \text{GL}(|\mathbf{z}|, \mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^{|\mathbf{z}|}$:

$$\mathcal{S}(f(A\mathbf{z} + \mathbf{b})) \geq \min\left(\frac{d_1}{2}, d_2 + 1, (d_3 + 1)^{1.63}, (d_4 + 1)^3\right).$$

The conditions imposed in (4.9) ensure that $(d_4 + 1)^3 > s_0$ and $(d_4 + 1)^3$ is the minimum. As $d_3 > m(d_4 + 1)^2$, therefore $s_0 = 1 + n(d_3 + 3) + m(d_4 + 1)^2 \leq 3nd_3 \leq 3pmn(d_4 + 1)^2$. Consequently, the gap in the sparsities of the YES instances and NO instances is

$$\frac{(d_4 + 1)^3}{s_0} \geq \frac{(d_4 + 1)^3}{3pmn(d_4 + 1)^2} = \frac{d_4 + 1}{3pmn}.$$

Also, note that as $d_4 \geq 3pmn$, therefore $s \leq 2m(d_4 + 1)^3 \implies d_4 + 1 \geq (\frac{s}{2m})^{1/3}$. Then, the gap is

$$\frac{(d_4 + 1)^3}{s_0} \geq \frac{d_4 + 1}{3pmn} \geq \frac{s^{1/3}}{p2^{1/3}3m^{4/3}n}.$$

Finally, note that $s \geq d_4^3$. Thus, for $d_4^{3\epsilon} \geq (mn)^{O(1)}$ large enough,

$$s^\epsilon \geq d_4^{3\epsilon} \geq p2^{1/3}3m^{4/3}n \implies \frac{s^{1/3}}{p2^{1/3}3m^{4/3}n} \geq s^{1/3-\epsilon}.$$

Hence, the gap is at least $s^{1/3-\epsilon}$. Therefore, 3-SAT reduces to α-gap-ETsparse for $\alpha = s^{1/3-\epsilon}$. □

For characteristic 2 fields

Let the characteristic be 2. Consider the polynomial as defined in (3.18). Let $s := \mathcal{S}(f)$. Now, s depends on the number of variables complemented in a clause. To prove the hardness of α-gap-ETsparse, $s \geq d_4^3$ is required (see the proof of Proposition 4.4.3), and this can be achieved if there is at least one clause where all the variables are complemented. Thus, assume, without loss of generality, that such a clause exists (see footnote 1). Choose the d_i's to satisfy (4.9) with p set to 2. By Observation 3.4.4 and the assumption on ψ, it holds that

$$1 + n(d_3 + 3) + (d_4 + 1)^3 \leq s \leq 1 + n(d_3 + 3) + m(d_4 + 1)^3.$$

For $\psi \in \overline{\text{3-SAT}}$, Lemma 4.4.3, which can be proved in the same way as Lemma 4.4.2, shows lower bounds on $\mathcal{S}(f(A\mathbf{z} + \mathbf{b}))$ where $A \in \text{GL}(|\mathbf{z}|, \mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^{|\mathbf{z}|}$. For $\psi \in$ 3-SAT,

by Proposition 3.3.1 there exists $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ such that $\mathcal{S}(f(A\mathbf{z})) \leq s_0$, where $s_0 = 1 + n(d_3+3) + m(d_4+1)^2$. Proposition 4.4.3 shows the NP-hardness of α-gap-ETsparse using Lemma 4.4.3 and the inequalities in (4.9).

Lemma 4.4.3. Let $\psi \in \overline{\text{3-SAT}}$, $f(\mathbf{z})$ be as defined in (3.18) corresponding to ψ, $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^{|\mathbf{z}|}$.

1. If $A(x_0) + \mathbf{b}_{|x_0}$ is a non-trivial affine form, then $\mathcal{S}(f(A\mathbf{z}+\mathbf{b})) \geq \frac{d_1}{2}$.
2. If A and $\mathbf{b}$ are not as in item 1 and for some $j \in [n]$, $A(x_j) + \mathbf{b}_{|x_j}$ is a non-trivial affine form, then $\mathcal{S}(f(A\mathbf{z}+\mathbf{b})) \geq d_2 + 1$.
3. If A and $\mathbf{b}$ are not as in items 1 and 2 and for some $j \in [n]$, $\mathcal{S}(A(y_j + x_j) + \mathbf{b}_{|y_j}) \geq 3$ or $\mathcal{S}(A(y_j) + \mathbf{b}_{|y_j}) \geq 3$, then $\mathcal{S}(f(A\mathbf{z}+\mathbf{b})) \geq (d_3+1)^{1.58}$.
4. If A and $\mathbf{b}$ are not of the form described in the previous three cases, then $\mathbf{b} = \mathbf{0}$ and $\mathcal{S}(f(A\mathbf{z})) \geq (d_4+1)^3$.

Proposition 4.4.3. Let $\mathrm{char}(\mathbb{F}) = 2$. If the input in α-gap-ETsparse is an s-sparse polynomial, then α-gap-ETsparse is NP-hard for $\alpha = s^{1/3-\epsilon}$.

Proof. The proof is similar to that of Proposition 4.4.2. If $\psi \in$ 3-SAT, then $\mathcal{S}(f(A\mathbf{z})) \leq s_0$ where A is as described in (3.4) and $s_0 = 1 + n(d_3+3) + m(d_4+1)^2$. If $\psi \in \overline{\text{3-SAT}}$, it follows from Lemma 4.4.3 that for any $A \in \mathrm{GL}(|\mathbf{z}|, \mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^{|\mathbf{z}|}$:

$$\mathcal{S}(f(A\mathbf{z}+\mathbf{b})) \geq \min\left(\frac{d_1}{2}, d_2+1, (d_3+1)^{1.58}, (d_4+1)^3\right).$$

The conditions imposed in (4.9) ensure that $(d_4+1)^3 > s_0$ and $(d_4+1)^3$ is the minimum. As $d_3 > m(d_4+1)^2$, therefore $s_0 = 1 + n(d_3+3) + m(d_4+1)^2 \leq 3nd_3 \leq 6mn(d_4+1)^2$. Consequently, the gap in the sparsities of the YES instances and NO instances is

$$\frac{(d_4+1)^3}{s_0} \geq \frac{(d_4+1)^3}{6mn(d_4+1)^2} = \frac{d_4+1}{6mn}.$$

Also, note that as $d_4 \geq 6mn$, therefore $s \leq 2m(d_4+1)^3 \implies d_4 + 1 \geq (\frac{s}{2m})^{1/3}$. Then, the gap is

$$\frac{(d_4+1)^3}{s_0} \geq \frac{d_4+1}{6mn} \geq \frac{s^{1/3}}{2^{4/3}3m^{4/3}n}.$$

Finally, note that $s \geq d_4^3$. Thus, for $d_4^{3\epsilon} \geq (mn)^{O(1)}$ large enough,

$$s^\epsilon \geq d_4^{3\epsilon} \geq 2^{4/3}3m^{4/3}n \implies \frac{s^{1/3}}{2^{4/3}3m^{4/3}n} \geq s^{1/3-\epsilon}.$$

Hence, the gap is at least $s^{1/3-\epsilon}$. Therefore, 3-SAT reduces to α-gap-ETsparse for $\alpha = s^{1/3-\epsilon}$. □

Chapter 5

NP-hardness of ETsupport

In this section, we prove Theorem 3.

Proof sketch. The proof strategy is similar to that outlined in section 3.1; here, instead of the sparsity, we are working with the support of the polynomial. We map ψ, a 3-CNF, to a polynomial f, which is the sum of polynomials which are degree separated or degree separated with respect to some variable. At least one polynomial in f is of support $\sigma+1$ and the rest of support σ (where σ is a constant). As the summands are degree separated or degree separated with respect to some variable, $\mathrm{Supp}(f) = \sigma+1$ and for any invertible linear transform A, $\mathrm{Supp}(A(f))$ is equal to the maximum support size among the transformed summands. Claim 2.2.2 is used to show that $\psi \in$ 3-SAT iff there exists an invertible linear transform A, such that $\mathrm{Supp}(A(f)) \leq \sigma$. Thus, the reduction also holds for $(\sigma+1)$-to-σ ETsupport. For characteristic p fields, we assume $p > \sigma+1$ so that Claim 2.2.2 holds.

5.1 Construction of f

Let $\sigma \geq 5$ be an even integer constant and ψ be as denoted in Section 3.1.1. For odd σ, we describe the changes in the construction/argument at the appropriate points. As σ is a constant, let $n \geq \sigma+4$. The proofs of Lemmas 5.3.1 and 5.3.2 use $n \geq \sigma+4$. To ensure $\mathrm{Supp}(f) = \sigma+1$, we assume that all the variables in the first clause are complemented (see footnote 1) and that no clause is repeated. Let $\mathbf{x} := \{x_1, \ldots, x_n\}$, $\mathbf{y} := \{y_1, \ldots, y_n\}$ and $\mathbf{z} := \{z_1, \ldots, z_{\sigma-5}\}$ and $\mathbf{w} := \mathbf{x} \sqcup \mathbf{y} \sqcup \mathbf{z}$. Note that when $\sigma = 5$, $\mathbf{z}$ is an empty set and hence we do not consider the $\mathbf{z}$ variables in such a case. By $(w_1 \cdots w_l)^\star$, where $w_i \in \mathbf{w}$ and $l, \star \in \mathbb{N}$, we denote a power of $w_1 \cdots w_l$. Consider the polynomials:

- First, introduce $\binom{n+\sigma-5}{\sigma}$ many monomials defined by the set

$$P := \{(w_1 \cdots w_\sigma)^\star \mid w_1, \ldots, w_\sigma \in \mathbf{z} \sqcup \mathbf{x} \text{ and are pairwise distinct}\}.$$

- Then, introduce $\binom{n}{\frac{\sigma}{2}}$ many monomials defined by the set

$$Q := \{((x_{i_1} y_{i_1}) \cdots (x_{i_{\frac{\sigma}{2}}} y_{i_{\frac{\sigma}{2}}}))^\star \mid i_1, \ldots, i_{\frac{\sigma}{2}} \in [n] \text{ and are pairwise distinct}\}.$$

  Note: For odd σ, the monomials are of form $((x_{i_1} y_{i_1}) \cdots (x_{i_{\frac{\sigma-1}{2}}} y_{i_{\frac{\sigma-1}{2}}}) x_{i_{\frac{\sigma+1}{2}}})^\star$. Thus $|Q| = \binom{n}{\frac{\sigma+1}{2}} \frac{\sigma+1}{2}$.

- Let $R := \{R_k(\mathbf{w}) \mid k \in [m]\}$, where $R_k(\mathbf{w})$ is defined corresponding to the k^{th} clause as:

$$R_k(\mathbf{w}) := (\prod_{j \in C_k} (y_j - a_{k,j} x_j)^{2+a_{k,j}})(z_1 \cdots z_{\sigma-5}).$$

Define $f(\mathbf{w}) := \sum_{g \in P} g(\mathbf{w}) + \sum_{h \in Q} h(\mathbf{w}) + \sum_{k=1}^{m} R_k(\mathbf{w})$. The powers, denoted by $\star$, must be such that the following hold:

1. All the polynomials in $P \sqcup Q$ are degree separated from one another and from the R_k's, with the powers being at least $\sigma + 1$.
2. Over characteristic p fields, where $p > 0$, all the powers are less than p or are of the form $p^k - 1$ for some $k \in \mathbb{N}$.

In Section 5.4, we choose the powers to satisfy the above conditions over any field. The following observations hold by the definition of the polynomials and the above conditions.

Observation 5.1.1. For $k \in [m]$, the degree of R_k is at most $\sigma + 4$ and $\text{Supp}(R_k(\mathbf{w})) \leq \sigma + 1$ with equality in both cases when $a_{k,j} = 1$ for all $j \in C_k$. For $k, l \in [m]$ with $l \neq k$, any monomial of R_k is degree separated from every monomial of R_l with respect to some variable in $\mathbf{x} \sqcup \mathbf{y}$.

Proof. Note that $R_k(\mathbf{w})$ is a product of variable disjoint polynomials. Hence, the degree of R_k is $\sigma - 5 + \sum_{j \in C_k} (2 + a_{k,j})$ where

$$\sigma + 1 \leq \sigma - 5 + \sum_{j \in C_k} (2 + a_{k,j}) \leq \sigma + 4$$

and the upper bound is achieved if $a_{k,j} = 1$ for all $j \in C_k$. Similarly, it can be seen that the variable disjointness property along with the fact that the characteristic of the underlying field is not equal to 2 or 3 implies

$$\sigma - 2 \leq \text{Supp}(R_k(\mathbf{w})) \leq \sigma + 1$$

where the upper bound is achieved if $a_{k,j} = 1$ for all $j \in C_k$. Now for $k, l \in [m]$, where $k \neq l$, there are two possibilities for the clauses C_k and C_l:

1. C_k and C_l contain the same set of $\mathbf{x}$ variables in which case there exists a j such that $a_{k,j} \neq a_{l,j}$. Assume without loss of generality that $a_{k,j} = 1$, therefore $a_{l,j} = 0$. From this and the definition of R_k and R_l, it can be seen that

$$R_k(\mathbf{w}) = (y_j - x_j)^3 \tilde{R}_k \cdot (z_1 z_2 \dots z_{\sigma-5}),\ R_l(\mathbf{w}) = y_j^2 \tilde{R}_l \cdot (z_1 z_2 \dots z_{\sigma-5})$$

where $\tilde{R}_k$ and $\tilde{R}_l$ are polynomials which do not contain a variable from $\mathbf{z} \sqcup \{x_j, y_j\}$. Thus, the monomials of R_k are degree separated from those of R_l with respect to x_j or y_j.

2. Otherwise C_k and C_l differ in at least one variable. This again implies that there exists a variable y_j such that the monomials of R_k have non-zero y_j-degree or non-zero x_j-degree while the monomials of R_l have zero y_j-degree and zero x_j-degree.

Note that the above argument also holds, with some modification, if all the R_k's are of the form

$$R_k(\mathbf{w}) = (\prod_{j \in C_k} (y_j - c_j x_j)^{2+a_{k,j}})(z_1 z_2 \dots z_{\sigma-5}), \quad c_j \in \mathbb{F}.$$

□

Observation 5.1.2. $\mathcal{S}(f(\mathbf{w})) = O(n^\sigma + m)$ and $\text{Supp}(f(\mathbf{w})) = \sigma + 1$.

Proof. By Condition 1 in Section 5.1, Observations 5.1.1 and 2.2.2, it holds that,

$$\mathcal{S}(f(\mathbf{w})) = \sum_{g(\mathbf{w}) \in P} \mathcal{S}(g(\mathbf{w})) + \sum_{h(\mathbf{w}) \in Q} \mathcal{S}(h(\mathbf{w})) + \sum_{k=1}^{m} \mathcal{S}(R_k(\mathbf{w})).$$

As $g(\mathbf{w}) \in P$ and $h(\mathbf{w}) \in Q$ are monomials, thus $\mathcal{S}(g(\mathbf{w})) = 1$ and $\mathcal{S}(h(\mathbf{w})) = 1$. For $k \in [m]$,

$$\mathcal{S}(R_k(\mathbf{w})) = (\prod_{j \in C_k} \mathcal{S}(y_j - a_{k,j} x_j)^{2+a_{k,j}}) \cdot \mathcal{S}(z_1 z_2 \dots z_{\sigma-5}) \leq 64$$

because all the polynomials in the product are variable disjoint and $a_{k,j}$ can be non-zero for all $j \in C_k$. Lastly, as $|P| = \binom{n+\sigma-5}{\sigma}$ and $|Q| = \binom{n}{\sigma/2}$ (for odd σ, $|Q| = \binom{n}{\frac{\sigma+1}{2}}\frac{\sigma+1}{2}$), hence

$$\mathcal{S}(f) \leq \binom{n+\sigma-5}{\sigma} + \binom{n}{\sigma/2} + 64m.$$

Thus, $\mathcal{S}(f) = O(n^\sigma + m)$. Now, $\text{Supp}(g(\mathbf{w})) = \sigma$ and $\text{Supp}(h(\mathbf{w})) = \sigma$, where $g(\mathbf{w}) \in P$ and $h(\mathbf{w}) \in Q$. By Observation 5.1.1, $\text{Supp}(R_k(\mathbf{w})) \leq \sigma + 1$, for $k \in [m]$. In particular, $\text{Supp}(R_1) = \sigma + 1$. By Condition 1 in Section 5.1 and Observation 5.1.1, it holds that $\text{Supp}(f(\mathbf{w})) = \text{Supp}(R_1(\mathbf{w})) = \sigma + 1$. □

Observation 5.1.3. For any $A \in \text{GL}(|\mathbf{w}|, \mathbb{F})$, it holds that

$$\text{Supp}(f(A\mathbf{w})) = \max\left(\max_{g \in P, h \in Q} (\text{Supp}(g(A\mathbf{w})), \text{Supp}(h(A\mathbf{w}))), \text{Supp}\left(\sum_{k=1}^{m} R_k(A\mathbf{w})\right)\right).$$

Proof. This observation follows easily from Condition 1 in Section 5.1. □

5.2 The forward direction

Proposition 5.2.1 shows how a satisfying assignment for ψ implies the existence of an invertible A, such that $\mathrm{Supp}(f(A\mathbf{w})) = \sigma$, by constructing A from the satisfying assignment.

Proposition 5.2.1. Let $\psi \in$ 3-SAT with $(u_1, \ldots, u_n) \in \{0,1\}^n$ a satisfying assignment. Then, $\mathrm{Supp}(f(A\mathbf{w})) = \sigma$, where the transform A is defined as

$$A : z_j \mapsto z_j,\ x_i \mapsto x_i,\ y_i \mapsto y_i + (1-u_i)x_i \ \ i \in [n], j \in [\sigma - 5]. \tag{5.1}$$

Proof. As Condition 1 and Observation 5.1.3 are satisfied, it suffices to analyse the action of A on individual polynomials of $P \sqcup Q$ and then analyse $\mathrm{Supp}(\sum_{k=1}^{m} R_k(A\mathbf{w}))$. Clearly, for $g(\mathbf{w}) \in P$, $g(A\mathbf{w}) = g(\mathbf{w})$. Let $h(\mathbf{w}) \in Q$. Then $h(\mathbf{w})$ is of form $((x_{t_1}y_{t_1}) \cdots (x_{t_{\frac{\sigma}{2}}}y_{t_{\frac{\sigma}{2}}}))^\star$, $t_j \in [n]$, and A acts on h as:

$$A : ((x_{t_1}y_{t_1}) \cdots (x_{t_{\frac{\sigma}{2}}}y_{t_{\frac{\sigma}{2}}}))^\star \mapsto ((x_{t_1})(y_{t_1} + (1-u_{t_1})x_{t_1}) \cdots (x_{t_{\frac{\sigma}{2}}})(y_{t_{\frac{\sigma}{2}}} + (1-u_{t_{\frac{\sigma}{2}}})x_{t_{\frac{\sigma}{2}}}))^\star.$$

Note $|\cup_{t=1}^{\sigma} \mathrm{var}(\ell_t)| = \sigma$, where $\ell_t = A(w)$ and $w \in \mathrm{var}(h(\mathbf{w}))$. Thus, $\mathrm{Supp}(h(A\mathbf{w})) \leq \sigma$. When σ is odd, a similar argument holds for the modified construction of Q. For $k \in [m]$, A acts on $R_k(\mathbf{w})$ as:

$$A : (\prod_{j \in C_k} (y_j - a_{k,j}x_j)^{2+a_{k,j}}) \cdot (z_1 \cdots z_{\sigma-5}) \mapsto (\prod_{j \in C_k} (y_j + (1 - a_{k,j} - u_j)x_j)^{2+a_{k,j}} \cdot (z_1 \cdots z_{\sigma-5}).$$

If $a_{k,j} \neq u_j$, then $a_{k,j} = 1 - u_j$. Since ψ is satisfiable, therefore for all $k \in [m]$, $a_{k,j} \neq u_j$ for some $j \in C_k$. Hence, $\mathrm{Supp}(R_k(A\mathbf{w})) \leq (\sigma - 5) + 5 = \sigma$ for all $k \in [m]$. This implies $\mathrm{Supp}(\sum_{k=1}^{m} R_k(A\mathbf{w})) \leq \sigma$. Thus, $\mathrm{Supp}(f(A\mathbf{w})) = \sigma$. □

5.3 The reverse direction

Now, we show that if $\mathrm{Supp}(f(A\mathbf{w})) \leq \sigma$ for $A \in \mathrm{GL}(|\mathbf{w}|, \mathbb{F})$, then a satisfying assignment can be recovered for ψ. Lemmas 5.3.1 and 5.3.2, proved using Claim 2.2.2, together show that A is as:

$$A : z_j \mapsto z_j,\ x_i \mapsto x_i,\ y_i \mapsto y_i + c_i x_i \ \ c_i \in \mathbb{F},\ j \in [\sigma - 5], i \in [n]$$

without loss of generality.[1] Proposition 5.3.1 derives a satisfying assignment for ψ from A.

[1] as permutation and non-zero scaling of variables do not affect the support.

Lemma 5.3.1. If $\text{Supp}(f(A\mathbf{w})) \leq \sigma$, then $\forall w \in \mathbf{z} \sqcup \mathbf{x}$, $A(w) = W$, for scaled variable $W \in \mathbf{w}$.

Proof. Let $g(\mathbf{w}) = (w_1 \cdots w_\sigma)^\star \in P$, where $w_j \in \mathbf{z} \sqcup \mathbf{x}$ and $\star$ represents an integer power which is at least $\sigma + 1$. Now, $g(A\mathbf{w}) = (\ell_1 \cdots \ell_\sigma)^\star$, where the ℓ_j's, with $j \in [\sigma]$, are linearly independent linear forms. If $|\cup_{j=1}^{\sigma} \text{var}(\ell_j)| \geq \sigma + 1$, then by Claim 2.2.2, $\text{Supp}(g(A\mathbf{w})) \geq \sigma + 1$ a contradiction. Thus, $|\cup_{j=1}^{\sigma} \text{var}(\ell_j)| \leq \sigma$. The linear independence of these σ many linear forms implies $|\cup_{j=1}^{\sigma} \text{var}(\ell_j)| \geq \sigma$. Combining these inequalities gives $|\cup_{j=1}^{\sigma} \text{var}(\ell_j)| = \sigma$. Thus, there exist variables $W_1, \ldots, W_\sigma \in \mathbf{w}$ such that $\langle \{\ell_1, \ldots, \ell_\sigma\} \rangle = \langle \{W_1, \ldots, W_\sigma\} \rangle$, where $\langle S \rangle$ denotes the vector space spanned by the elements of a set S of polynomials. In particular, $\langle \{\ell_1, \ldots, \ell_\sigma\} \rangle = \langle \text{var}(g(A\mathbf{w})) \rangle$.

Consider the variable $x_1 \in \mathbf{x} \sqcup \mathbf{z}$ and let $A(x_1) = \ell_1$. Now, P can be seen as a collection of σ sized subsets of $\mathbf{z} \sqcup \mathbf{x}$. Since $n + \sigma - 6 \geq 2(\sigma - 1)$ (as implied by $n \geq \sigma + 4$), there exist, without loss of generality, $g_1(\mathbf{w})$ and $g_2(\mathbf{w}) \in P$, such that $\text{var}(g_1(\mathbf{w})) \cap \text{var}(g_2(\mathbf{w})) = \{x_1\}$. Note that $\langle \text{var}(g_1(\mathbf{w})) \rangle \cap \langle \text{var}(g_2(\mathbf{w})) \rangle = \langle \text{var}(g_1(\mathbf{w})) \cap \text{var}(g_2(\mathbf{w})) \rangle$. Thus,

$$\dim \langle \text{var}(g_1(\mathbf{w})) \rangle \cap \langle \text{var}(g_2(\mathbf{w})) \rangle = \dim \langle \text{var}(g_1(\mathbf{w})) \cap \text{var}(g_2(\mathbf{w})) \rangle = 1.$$

The invertibility of A and the argument of the first paragraph imply there exist σ-size sets $B_1, B_2 \subseteq \mathbf{w}$, with $B_1 = \text{var}(g_1(A\mathbf{w}))$ and $B_2 = \text{var}(g_2(A\mathbf{w}))$, such that $\langle \text{var}(g_1(\mathbf{w})) \rangle$ and $\langle B_1 \rangle$ are isomorphic and so are $\langle \text{var}(g_2(\mathbf{w})) \rangle$ and $\langle B_2 \rangle$. Similarly, under A, $\langle \text{var}(g_1(\mathbf{w})) \rangle \cap \langle \text{var}(g_2(\mathbf{w})) \rangle$ is isomorphic to $\langle B_1 \rangle \cap \langle B_2 \rangle$. Thus, $\dim \langle B_1 \rangle \cap \langle B_2 \rangle = 1$. From the first paragraph, it is also evident that $\ell_1 \in \langle B_1 \rangle \cap \langle B_2 \rangle = \langle B_1 \cap B_2 \rangle$, where the equality follows as B_1 and B_2 are sets of variables. This implies $A(x_1) = \ell_1 = W_1$, where W_1 is some scaled variable in $\mathbf{w}$. □

Lemma 5.3.2. If $\text{Supp}(f(A\mathbf{w})) \leq \sigma$, then $A(x_i) = X_i$ and $A(y_i) = Y_i + c_i X_i$, for scaled variables $Y_i, X_i \in \mathbf{w}$ and $c_i \in \mathbb{F}$.

Proof. The proof is similar to that of Lemma 5.3.1. As $\text{Supp}(f(A\mathbf{w})) \leq \sigma$, Lemma 5.3.1 holds. Thus, for all $w \in \mathbf{x} \sqcup \mathbf{z}$, $A(w) = W$ for some scaled variable $W \in \mathbf{w}$. In particular, $A(x_i) = X_i$ where $i \in [n]$ and $X_i \in \mathbf{w}$ is some scaled variable. Let $A(y_i) = \ell_i$, where ℓ_i contains at least one variable other than those in $\text{var}(A(w))$, for any $w \in \mathbf{x} \sqcup \mathbf{z}$. Without loss of generality, consider $h(\mathbf{w}) = ((x_1 y_1) \cdots (x_{\frac{\sigma}{2}} y_{\frac{\sigma}{2}}))^\star \in Q$, where $\star$ represents an integer power which is at least $\sigma + 1$. Now, $h(A\mathbf{w}) = ((X_1 \ell_1) \cdots (X_{\frac{\sigma}{2}} \ell_{\frac{\sigma}{2}}))^\star$, where $X_1 \ldots X_{\frac{\sigma}{2}}, \ell_1, \ldots \ell_{\frac{\sigma}{2}}$ are linearly independent linear forms. If $|\text{var}(\ell_1) \cup \cdots \cup \text{var}(\ell_{\frac{\sigma}{2}}) \cup \{X_1, \ldots, X_{\frac{\sigma}{2}}\}| \geq \sigma + 1$, then by Claim 2.2.2, $\text{Supp}(h(A\mathbf{w})) \geq \sigma + 1$, a contradiction. Thus, $|\text{var}(\ell_1) \cup \cdots \cup \text{var}(\ell_{\frac{\sigma}{2}}) \cup \{X_1, \ldots, X_{\frac{\sigma}{2}}\}| \leq \sigma$. The linear independence of these σ many linear forms implies $|\text{var}(\ell_1) \cup \cdots \cup \text{var}(\ell_{\frac{\sigma}{2}}) \cup \{X_1, \ldots, X_{\frac{\sigma}{2}}\}| \geq \sigma$. These inequalities imply $|\text{var}(\ell_1) \cup \cdots \cup \text{var}(\ell_{\frac{\sigma}{2}}) \cup \{X_1, \ldots, X_{\frac{\sigma}{2}}\}| = \sigma$. Hence there exists variable set $B = \{X_1, \ldots, X_{\frac{\sigma}{2}}\} \sqcup \{Y_1, \ldots, Y_{\frac{\sigma}{2}}\}$ such that $\langle B \rangle = \langle \{\ell_1, \ldots, \ell_{\frac{\sigma}{2}}\} \sqcup \{X_1, \ldots, X_{\frac{\sigma}{2}}\} \rangle$. In particular, $\langle \{\ell_1, \ldots, \ell_{\frac{\sigma}{2}}\} \sqcup \{X_1, \ldots, X_{\frac{\sigma}{2}}\} \rangle = \langle \text{var}(h(A\mathbf{w})) \rangle$.

Consider the variable $x_1 \in \mathbf{x}$. As $n-1 \geq \sigma-2$ (as implied by $n \geq \sigma+4$), then for $x_1 \in \mathbf{x}$ and $y_1 \in \mathbf{y}$, there exist, $h_1(\mathbf{w}), h_2(\mathbf{w}) \in Q$ such that $\text{var}(h_1(\mathbf{w})) \cap \text{var}(h_2(\mathbf{w})) = \{x_1, y_1\}$. Note that $\langle \text{var}(h_1(\mathbf{w}))\rangle \cap \langle \text{var}(h_2(\mathbf{w}))\rangle = \langle \text{var}(h_1(\mathbf{w})) \cap \text{var}(h_2(\mathbf{w}))\rangle$. Thus,

$$\dim\langle \text{var}(h_1(\mathbf{w}))\rangle \cap \langle \text{var}(h_2(\mathbf{w}))\rangle = \dim\langle \text{var}(h_1(\mathbf{w})) \cap \text{var}(h_2(\mathbf{w}))\rangle = 2.$$

The invertibility of A and the argument of the first paragraph imply that there exist σ-size sets $B_1, B_2 \subseteq \mathbf{w}$, with $B_1 = \text{var}(h_1(A\mathbf{w}))$ and $B_2 = \text{var}(h_2(A\mathbf{w}))$, such that $\langle \text{var}(h_1(\mathbf{w}))\rangle$ and $\langle B_1\rangle$ are isomorphic, and so are $\langle \text{var}(h_2(\mathbf{w}))\rangle$ and $\langle B_2\rangle$. Similarly under A, $\langle \text{var}(h_1(\mathbf{w}))\rangle \cap \langle \text{var}(h_2(\mathbf{w}))\rangle$ is isomorphic to $\langle B_1\rangle \cap \langle B_2\rangle$. Therefore, $\dim\langle B_1\rangle \cap \langle B_2\rangle = 2$. As $A(x_1) = X_1$, and $A(y_1) \in \langle B_1\rangle \cap \langle B_2\rangle$ (by the argument in the first paragraph), therefore $A(y_1) = Y_1 + c_1 X_1$, where $Y_1 \in \mathbf{w}$ is some scaled variable and $c_1 \in \mathbb{F}$. □

Note: For odd σ, the proof holds with some modification. First, $h(\mathbf{w}) \in Q$ is now of form $((x_1y_1)\cdots(x_{\frac{\sigma-1}{2}}y_{\frac{\sigma-1}{2}})x_{\frac{\sigma+1}{2}})^\star$. The argument in the first paragraph then shows that for $h(A\mathbf{w}) = ((X_1\ell_1)\cdots(X_{\frac{\sigma-1}{2}}\ell_{\frac{\sigma-1}{2}})X_{\frac{\sigma+1}{2}})^\star$, there exists a σ-size set $B \subseteq \mathbf{w}$, such that $B = \{X_1, \ldots, X_{\frac{\sigma+1}{2}}\} \sqcup \{Y_1, \ldots, Y_{\frac{\sigma-1}{2}}\}$ and $\langle B\rangle = \langle\{\ell_1, \ldots, \ell_{\frac{\sigma-1}{2}}\} \sqcup \{X_1, \ldots, X_{\frac{\sigma+1}{2}}\}\rangle$. Secondly, for a variable $x_1 \in \mathbf{x}$, the existence of $h_1(\mathbf{w}), h_2(\mathbf{w}) \in Q$ such that $\text{var}(h_1(\mathbf{w})) \cap \text{var}(h_2(\mathbf{w})) = \{x_1, y_1\}$ is implied by $n-1 \geq \sigma-1$ (which itself is implied by $n \geq \sigma+4$). With these changes, the remainder of the argument continues to hold.

Proposition 5.3.1. A satisfying assignment $\mathbf{u}$ for ψ can be extracted from A.

Proof. The action of A on R_k, where $k \in [m]$, is:

$$\Big(\prod_{j\in C_k}(y_j - a_{k,j}x_j)^{2+a_{k,j}}\Big)\cdot(z_1\cdots z_{\sigma-5}) \mapsto \Big(\prod_{j\in C_k}(y_j + (c_j - a_{k,j})x_j)^{2+a_{k,j}}\Big)\cdot(z_1\cdots z_{\sigma-5}).$$

An argument similar to the proof of Observation 5.1.1 shows that for any $k, l \in [m]$ with $k \neq l$, any monomial of $R_k(A\mathbf{w})$ is degree separated from every monomial of $R_l(A\mathbf{w})$ with respect to some variable in $\mathbf{x} \sqcup \mathbf{y}$. This implies $\text{Supp}(\sum_{k=1}^m R_k(A\mathbf{w})) = \max_{k\in[m]}(\text{Supp}(R_k(A\mathbf{w}))$. Since $\text{Supp}(f(A\mathbf{w})) \leq \sigma$, therefore $\text{Supp}(R_k(A\mathbf{w})) \leq \sigma$ for all $k \in [m]$. Using the fact that the characteristic of the field is not equal to 2 or 3 and the action of A of $R_k(\mathbf{w})$, it can be seen that $\text{Supp}(R_k(A\mathbf{w})) \leq \sigma$ iff for some $j \in C_k$, $c_j = a_{k,j}$. Hence, for each $R_k(\mathbf{w})$, there exists $j \in C_k$ such that $c_j \in \{0,1\}$. Construct $\mathbf{u} \in \{0,1\}^n$ by setting $u_j := 1 - c_j$, for appropriate $j \in C_k$ and the remaining u_i's to arbitrary values in $\{0,1\}$. From the definition of $\mathbf{u}$, it follows that for the k^{th} clause, there exists $j \in C_k$ such that $u_j \neq a_{k,j}$. As k is arbitrary, all clauses are satisfied. □

5.4 Choosing the degrees

In this section, we set the powers $\star$, as denoted in Section 5.1, for all polynomials in P, Q and R such that Conditions 1 and 2, specified in that section, are satisfied over any field.

We specify the choice of $\star$ separately for characteristic 0 fields and finite characteristic fields. Let $N := \binom{n+\sigma-5}{\sigma} + \binom{n}{\sigma/2}$, $i \in [N]$ and $k \in [m]$. For odd σ, $N := \binom{n+\sigma-5}{\sigma} + \binom{n}{\frac{\sigma+1}{2}}\frac{\sigma+1}{2}$.

Over characteristic 0 fields. For the polynomials in $P \sqcup Q$, arbitrarily order them and choose the powers to be of form $\sigma + i$. For this choice of the powers, every polynomial in $P \sqcup Q$ has corresponding degree $\sigma(\sigma + i)$ and is clearly degree separated from the other polynomials in $P \sqcup Q$. By Observation 5.1.1, the degree of R_k is at most $\sigma + 4$. As $i \geq 1$ and $\sigma > 2$ it can be easily observed that

$$\sigma(\sigma + i) \geq \sigma(\sigma + 1) > \sigma + 4.$$

Thus, for this choice of the powers, Condition 1 is satisfied over characteristic 0 fields. The degree of f then is $\sigma(\sigma + N) = O(n^\sigma)$.

Over finite characteristic fields. Let the characteristic be $p > 0$. We assume $p > \sigma + 1$ to ensure Claim 2.2.2 holds. If $p > \sigma + N$, the powers can be chosen just like in the characteristic 0 case. Otherwise if $\sigma + 1 < p \leq \sigma + N$, then we choose the powers to be of form $p^t - 1$, where $t \in \mathbb{N}$, from the following N disjoint intervals:

$$[\sigma + 1, p(\sigma + 1)],\ [p(\sigma + 1) + 1, p^2(\sigma + 1) + p],\ [p^2(\sigma + 1) + p + 1, p^3(\sigma + 1) + p^2 + p], \cdots$$

Order the N polynomials in $P \sqcup Q$ arbitrarily and assign powers in each polynomial from the above N intervals. Then, the degree of a polynomial in $P \sqcup Q$ lies in the range

$$[\sigma(p^{i-1}(\sigma + 1) + \sum_{l=0}^{i-2} p^l), \sigma(p^i(\sigma + 1) + \sum_{l=1}^{i-1} p^l)].$$

For distinct i this range is disjoint implying the polynomials in $P \sqcup Q$ are degree separated. By Observation 5.1.1, the degree of R_k is at most $\sigma + 4$. Now, we show that the polynomials of $P \sqcup Q$ are degree separated from the R_k's by showing that the lower bound on the degree of any polynomial in $P \sqcup Q$ is greater than the degree of any R_k. As $i \geq 1$, $\sigma > 2$ and $p > 1$, it follows that

$$\sigma(p^{i-1}(\sigma + 1) + \sum_{l=0}^{i-2} p^l) \geq \sigma(\sigma + 1) > \sigma + 4.$$

Thus, for this choice of powers, Conditions 1 and 2 are satisfied. For $p > \sigma + N$, the degree of f is $\sigma(\sigma + N) = O(n^\sigma)$ and for $\sigma + 1 < p \leq \sigma + N$, the degree of f is

$$O(\sigma(p^N(\sigma + 1) + \sum_{l=1}^{N-1} p^l)) = O(p^N) = O((\sigma + N)^N) = O((\sigma + n^\sigma)^{n^\sigma}).$$

Note that the degree of f can be represented in $n^{O(1)}$ many bits as σ is a constant. Hence, as remarked just after Theorem 3, we assume that over finite characteristic fields, the exponent vectors corresponding to the monomials of the input polynomials are given in binary.

References

[AS05] Manindra Agrawal and Nitin Saxena. Automorphisms of Finite Rings and Applications to Complexity of Problems. In *23rd Annual Symposium on Theoretical Aspects of Computer Science, STACS 2005*, pages 1–17, 2005.

[BDS24] Omkar Baraskar, Agrim Dewan, and Chandan Saha. Testing Equivalence to Design Polynomials. In Olaf Beyersdorff, Mamadou Moustapha Kanté, Orna Kupferman, and Daniel Lokshtanov, editors, *41st International Symposium on Theoretical Aspects of Computer Science, STACS 2024, March 12-14, 2024, Clermont-Ferrand, France*, volume 289 of *LIPIcs*, pages 9:1–9:22. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024.

[BDSS24] Omkar Baraskar, Agrim Dewan, Chandan Saha, and Pulkit Sinha. Np-hardness of testing equivalence to sparse polynomials and to constant-support polynomials. *arXiv preprint arXiv:2410.12251*, 2024.

[CGS23] Suryajith Chillara, Coral Grichener, and Amir Shpilka. On hardness of testing equivalence to sparse polynomials under shifts. In Petra Berenbrink, Patricia Bouyer, Anuj Dawar, and Mamadou Moustapha Kanté, editors, *40th International Symposium on Theoretical Aspects of Computer Science, STACS 2023, March 7-9, 2023, Hamburg, Germany*, volume 254 of *LIPIcs*, pages 22:1–22:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023.

[CKW11] Xi Chen, Neeraj Kayal, and Avi Wigderson. Partial Derivatives in Arithmetic Complexity and Beyond. *Foundations and Trends in Theoretical Computer Science*, 6(1-2):1–138, 2011.

[DdOS14] Zeev Dvir, Rafael Mendes de Oliveira, and Amir Shpilka. Testing Equivalence of Polynomials under Shifts. In *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part I*, volume 8572 of *Lecture Notes in Computer Science*, pages 417–428. Springer, 2014.

[DF89] M.E Dyer and A.M Frieze. The solution of some random np-hard problems in polynomial expected time. *Journal of Algorithms*, 10(4):451–489, 1989.

[GGKS19] Ankit Garg, Nikhil Gupta, Neeraj Kayal, and Chandan Saha. Determinant equivalence test over finite fields and over Q. In *46th International Colloquium on Automata, Languages, and Programming, ICALP 2019, July 9-12, 2019, Greece*, volume 132 of *LIPIcs*, pages 62:1–62:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

[GK93] Dima Grigoriev and Marek Karpinski. A Zero-Test and an Interpolation Algorithm for the Shifted Sparse Polynominals. In Gérard D. Cohen, Teo Mora, and Oscar Moreno, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 10th International Symposium, AAECC-10, San Juan de Puerto Rico, Puerto Rico, May 10-14, 1993, Proceedings*, volume 673 of *Lecture Notes in Computer Science*, pages 162–169. Springer, 1993.

[Gri97] Dima Grigoriev. Testing shift-equivalence of polynomials by deterministic, probabilistic and quantum machines. *Theor. Comput. Sci.*, 180(1-2):217–228, 1997.

[Gro12] Joshua A. Grochow. *Symmetry and equivalence relations in classical and geometric complexity theory*. PhD thesis, University of Chicago, Chicago, IL, 2012.

[GS19] Nikhil Gupta and Chandan Saha. On the symmetries of and equivalence test for design polynomials. In *44th International Symposium on Mathematical Foundations of Computer Science, MFCS 2019, August 26-30, 2019, Aachen, Germany*, volume 138 of *LIPIcs*, pages 53:1–53:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

[GST23] Nikhil Gupta, Chandan Saha, and Bhargav Thankey. Equivalence Test for Read-Once Arithmetic Formulas. In Nikhil Bansal and Viswanath Nagarajan, editors, *Proceedings of the 2023 ACM-SIAM Symposium on Discrete Algorithms, SODA 2023, Florence, Italy, January 22-25, 2023*, pages 4205–4272. SIAM, 2023.

[Kay11] Neeraj Kayal. Efficient algorithms for some special cases of the polynomial equivalence problem. In Dana Randall, editor, *Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2011, San Francisco, California, USA, January 23-25, 2011*, pages 1409–1421. SIAM, 2011.

[Kay12a] Neeraj Kayal. Affine projections of polynomials: extended abstract. In *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 643–662, 2012.

[Kay12b] Neeraj Kayal. An exponential lower bound for the sum of powers of bounded degree polynomials. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:81, 2012.

[KNST17] Neeraj Kayal, Vineet Nair, Chandan Saha, and Sébastien Tavenas. Reconstruction of Full Rank Algebraic Branching Programs. In *32nd Computational Complexity Conference, CCC 2017, July 6-9, 2017, Riga, Latvia*, pages 21:1–21:61, 2017.

[KNST19] Neeraj Kayal, Vineet Nair, Chandan Saha, and Sébastien Tavenas. Reconstruction of Full Rank Algebraic Branching Programs. *ACM Trans. Comput. Theory*, 11(1):2:1–2:56, 2019. Conference version appeared in the proceedings of CCC 2017.

[Luc78] Edouard Lucas. Théorie des fonctions numériques simplement périodiques. *American Journal of Mathematics*, 1(2):184–196, 1878.

[LV24] Ben Lee Volk. Sigact news complexity theory column 121. *SIGACT News*, 55(2):53–88, June 2024.

[MNS20] Janaky Murthy, Vineet Nair, and Chandan Saha. Randomized Polynomial-Time Equivalence Between Determinant and Trace-IMM Equivalence Tests. In *45th International Symposium on Mathematical Foundations of Computer Science, MFCS 2020, August 24-28, 2020, Prague, Czech Republic*, volume 170 of *LIPIcs*, pages 72:1–72:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

[MS21] Dori Medini and Amir Shpilka. Hitting sets and reconstruction for dense orbits in VP_e and $\Sigma\Pi\Sigma$ circuits. In *36th Computational Complexity Conference, CCC 2021, July 20-23, 2021, Toronto, Ontario, Canada (Virtual Conference)*, volume 200 of *LIPIcs*, pages 19:1–19:27. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

[Roc18] Daniel S. Roche. What Can (and Can't) we Do with Sparse Polynomials? In Manuel Kauers, Alexey Ovchinnikov, and Éric Schost, editors, *Proceedings of the 2018 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2018, New York, NY, USA, July 16-19, 2018*, pages 25–30. ACM, 2018.

[Sap] Ramprasad Saptharishi. A survey of lower bounds in arithmetic circuit complexity. https://github.com/dasarpmar/lowerbounds-survey/releases/tag/v9.0.3.

[Sax06] Nitin Saxena. *Morphisms of rings and applications to complexity*. PhD thesis, Indian Institute of Technology, Kanpur, 2006.

[SY10] Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: a survey of recent results and open questions. https://www.cs.tau.ac.il/~shpilka/publications/SY10.pdf, 2010.

[Thi98] Thomas Thierauf. The Isomorphism Problem for Read-Once Branching Programs and Arithmetic Circuits. *Chicago J. Theor. Comput. Sci.*, 1998, 1998.