Sparsity Bounds of Square Polynomials

Name: Rishabh Kothary
Roll No: 180608
Email: rishk@iitk.ac.in

Course: CS498
Advisor: Prof. Nitin Saxena

Contents

1 Introduction

Polynomial factorization is a central question in computer algebra having applications in areas such as cryptography [CR88], list decoding [VG99, Sud97] and derandomization [KI04]. The study of factorization of sparse polynomials was initiated by [VZGK85], where von zur Gathen and Kaltofen gave the first randomized algorithm of factorization of sparse multivariate polynomials. The runtime of this algorithm has a polynomial dependence on the sparsity of its factors.

Kopparty et al. [KSS14] showed the equivalence of the problem of derandomizing polynomial identitiy testing for general arithmetic circuits and the problem of derandomizing multivariate polynomial factoring. Then, Bhargav et al. [BSV20] derandomized multivariate polynomial factoring for the class of sparse polynomials. The runtime of their algorithm has a polynomial dependence on sparsity of the sparsity of its factors.

The central problem we want to tackle is

Problem 1.1. *Let $f, g, h \in \mathbb{F}[x_1, ..., x_n]$ such that $f = g \cdot h$, then how are $||g||$ and $||f||$ related to each other.*

Note that $||g||$ is simply the sparsity of g. Volkovich [Vol17] conjectured that

Conjecture 1.2 ([Vol17])**.** *There exists a function $\nu : \mathbb{N} \to \mathbb{N}$ such that if $f \in \mathbb{F}[x_1, .., x_n]$ is a polynomial with individual degree atmost d, then $g|f \implies ||g|| \leq ||f||^{\nu(d)}$.*

We handle an easier variant of the central problem in this report which is:

Problem 1.3. *Let $f \in \mathbb{R}[x_1, ..., x_n]$, then how is $||f^2||$ and $||f||$ related?*

To study the problem we developed a new set theoretic framework through the approach of 'positive polynomials'.

2 Definitions and Notations

2.1 Polynomials

Let $f \in \mathbb{F}[x_1, ..., x_n]$ such that

$$f(x_1, .., x_n) = \sum_{i_1, .. i_n} a_{i_1, .., i_n} x_1^{i_1} ... x_n^{i_n}$$

then define the support of f as

$$supp(f) = \{(i_1, .., i_n) | a_{i_1, .., i_n} \neq 0\}$$

and let

$$||f|| = |supp(f)|.$$

The individual degree of variable x_i in f denoted by $deg_{x_i}(f)$ is the maximum degree of variable x_i in f. The individual degree of f is defined as the maximum among all individual degrees of all variables of f.

We fix the field $\mathbb{F}$ to $\mathbb{R}$ unless stated otherwise. We define $f \in \mathbb{R}[x]$ to be a positive polynomial if

$$f(x) = \sum_i a_i x^i$$

where $a_i \geq 0$. We call $f \in \mathbb{F}[x_1, ..., x_n]$ a square polynomial iff there exists $g \in \mathbb{F}[x_1, ..., x_n]$ such that $f = g^2$.

2.2 Sets

Let A, B be two sets then we define their Minkowski Sum as as

$$A + B = \{\alpha + \beta | \alpha \in A, \beta \in B\}.$$

Denote $A + A + ... + A$ (n times) by nA. For two sets A, B we define their symmetric difference as

$$A \triangle B = (A \cup B) \setminus (A \cap B).$$

For two set $A, B \subset \mathbb{N}$ define

$$spread(A, B) = \max(A \cup B) - \min(A \cup B).$$

For $d \in \mathbb{N}$ define $[d]$ as

$$[d] = \{0, 1, ..., d\}.$$

3 Kronecker Map

A useful tool to reduce multivariate polynomials to univariate polynomials is the Kronecker map [VZGG13]. Let $f \in \mathbb{F}[x_1, ..., x_n]$ such that individual degree of $f < d$. We define the Kronecker map of degree d to be the map:

$$\begin{aligned} \Psi_d : \mathbb{F}[x_0, x_1, , ..., x_n] &\to \mathbb{F}[x] \\ f(x_0, x_1, ..., x_n) &\to f(x, x^d, ..., x^{d^n}) \end{aligned}$$

and for ease of notation denote $\Psi_d(f)$ by $\hat{f}_d$. Some important properties of the Kronecker map are :

Lemma 3.1 (Sparsity Preservation)**.** *Let $f \in \mathbb{F}[x_0, x_1, ..., x_n]$ such that individual degree of $f < d$,then $||f|| = ||\hat{f}_d||$.*

Proof. To prove the equality we show a bijection between $supp(f)$ and $supp(\hat{f}_d)$. Consider the map :

$$\begin{aligned} \phi : supp(f) &\to supp(\hat{f}_d) \\ (k_0, ..., k_n) &\to \sum_{i=0}^{n} k_i d^i. \end{aligned}$$

The map is onto by the definition of Ψ_d. Suppose for $(a_0, ...a_n)$ and $(b_0, .., b_n) \in supp(f)$

$$\begin{aligned} \phi(a_0, ..., a_n) &= \phi(b_0, .., b_n) \\ (\implies) \sum_{i=0}^{n} a_i d^i &= \sum_{i=0}^{n} b_i d^i. \end{aligned}$$

Since individual degree of $f < d$, thus $a_i, b_i < d$ for $0 \leq i \leq n$. By uniqueness of d-ary expansion of a number, $a_i = b_i$ for $0 \leq i \leq n$ implying $(a_0, ..., a_n) = (b_0, ..., b_n)$ and thus proving ϕ is one-one which implies ϕ is a bijection. □

Lemma 3.2 (Factor Sparsity Preservation)**.** *Let $f, g, h \in \mathbb{F}[x_0, .., x_n]$ such that $f = g \cdot h$ and individual degree of $f < d$, then*

$$\hat{f}_d = \hat{g}_d \cdot \hat{h}_d.$$

Also $||\hat{g}_d|| = ||g||$ and $||\hat{h}_d|| = ||h||$.

Proof. Note that

$$\begin{aligned}\hat{f}_d(x) &= f(x, x^d, ..., x^{d^n}) \\ &= g(x, x^d, ..., x^{d^n}) \cdot h(x, x^d, ..., x^{d^n}) \\ &= \hat{g}_d(x) \cdot \hat{h}_d(x).\end{aligned}$$

We used the fact that evaluation map is a homomorphism. By Lemma 3.1 we have $||\hat{g}_d|| = ||g||$ and $||\hat{h}_d|| = ||h||$. □

We can use the Kronecker map to reduce problems related to sparsity in the multivariate setting to problems related to sparsity in the univariate setting.

4 Earlier Results

4.1 Bounded Degree Setting

In the bounded individual degree setting [BSV20] showed that

Theorem 4.1 ([BSV20]). *There exists an non-decreasing function $\xi(n, s, d) \leq s^{\mathcal{O}(d^2 \log n)}$ such that if $f \in \mathbb{F}[x_1, ..., x_n]$ is a polynomial of sparsity s and individual degrees at most d and if $f = g \cdot h$, for $g, h \in \mathbb{F}[x_1, ..., x_n]$, then the sparsity of g is upper bounded by $\xi(n, s, d)$.*

A corollary of the above theorem would be:

Corollary 4.2. *Let $f \in \mathbb{F}[x]$ such that $deg(f) < d$, then*

$$||f^2|| \geq ||f||^{\Omega(1/d^2)}.$$

The tightness of this bound has not been proven yet.

4.2 Unbounded Degree Setting

The problem of sparsity shrinkage when squaring a real univariate polynomial in the unbounded degree setting has been studied a little in the past ([Erd49, Rén47, Abb02, Ver49]). Erdös defined the term :

$$Q(k) = \min_{\substack{f \in \mathbb{R}[x] \\ ||f|| = k}} ||f^2||$$

which is basically the minimum possible shrinkage possible and showed that

Theorem 4.3 ([Erd49]). *There exists real constants $c_2 > 0$ and $0 < c_1 < 1$ such that*

$$Q(k) < c_2 k^{1-c_1}.$$

Verdenius found the value of constant c_1 for real complete polynomials. He defined the term

$$\hat{Q}(k) = \min_{\substack{f \in \mathbb{R}[x] \\ ||f|| = k \\ deg(f) = k-1}} ||f^2||$$

and showed that

Theorem 4.4 ([Ver49]). *There exists real constant $c_1 > 0$ such that*

$$\hat{Q}(k) < c_1 k^{0.81071...}.$$

Schinzel studied the relationship between $||f^k||$ and $||f||$ and showed that

Theorem 4.5 ([Sch87]). *Let $f \in \mathbb{F}[x]$ and $k \in \mathbb{N}$. If $char(\mathbb{F}) = 0$ or $char(\mathbb{F}) > k \cdot deg(f)$ then*

$$||f^k|| \geq k + 1 + (\log 2)^{-1} \log\left(1 + \frac{\log(||f|| - 1)}{k \log 4k - \log k}\right).$$

4.3 When is $||f^2|| < ||f||$?

Since the existence of large shrinkage has been shown it naturally raises it question whether we can give explicit examples of when it occurs.

[Rén47] gave the following example :

Example 4.6. *For the following polynomial*

$$P(x) = (4x^4 + 4x^3 - 2x^2 + 2x + 1) \cdot (-84x^{24} + 28x^{20} - 10x^{16} + 4x^{12} - 2x^8 + 2x^4 + 1)$$

$||P|| = 29$ *and* $||P^2|| = 28$ *which essentially proves* $Q(29) \leq 28$.

Moreover, [Abb02] showed that for $f(x) \in \mathbb{R}[x]$ such that $deg(f) \leq 11$, then $||f^2|| \geq ||f||$. This result is tight as for the polynomials:

$$P_\alpha(x) = (1 + 2x - 2x^2 + 4x^3 - 10x^4 + 50x^5 + 125x^6) \cdot (1 + \alpha x^6)$$

where $\alpha \in \{-110, -253, -55/2, 15625\}$, $||P_\alpha^2|| < ||P_\alpha||$.

5 Main Conjecture

Considering the best known sparsity shrinkage results known we conjectured :

Conjecture 5.1. *Let* $f \in \mathbb{R}[x]$ *then* $||f^2|| \geq \Omega\left(||f||^{1/2}\right)$.

We are working in the unbounded degree setting now and thus it is difficult to use the Newton Polytope approach introduced in [BSV20] to find a good bound. Due to [Abb02], it is difficult to construct simple counterexamples to the above problem as for polynomial f of degree less than 11, $||f^2|| > ||f||$. To study the Conjecture 5.1 we introduced the approach of positive polynomials.

The following conjecture seems to be a much more generalized version of the earlier conjecture :

Conjecture 5.2. *If* $f \in \mathbb{R}[x_1, ..., x_n]$ *then* $||f^2|| \geq \Omega\left(||f||^{1/2}\right)$.

But we can show that :

Lemma 5.3. *Conjecture 5.1 is true iff Conjecture 5.2 is true.*

Proof. If Conjecture 5.2 is true then Conjecture 5.1 is true as Conjecture 5.1 is a special case of Conjecture 5.2.

Suppose Conjecture 5.1 is true and let $f \in \mathbb{R}[x_1, .., x_n]$ with individual degree of $f \leq d$, then by Conjecture 5.1 we have

$$||\hat{f}_d^2|| \geq \Omega\left(||\hat{f}_d||^{1/2}\right).$$

By Lemma 3.1 and Lemma 3.2 we have

$$||\hat{f}_d^2|| = ||f^2|| \qquad ||\hat{f}_d|| = ||f||$$

which implies

$$||f^2|| \geq \Omega\left(||f||^{1/2}\right)$$

□

We thus will focus our attention on the Conjecture 5.1 throughout this report. We are working in the unbounded degree setting and thus it is difficult to use the Newton Polytope approach introduced in [BSV20] to find a good bound. Due to [Abb02], it is difficult to construct simple counterexamples to the above problem as for polynomial f of degree less than 11, $||f^2|| > ||f||$. To study the Conjecture 5.1 we introduced the approach of positive polynomials.

6 Positive Polynomials

The key property of positive polynomials which we will exploit is :

Lemma 6.1. *Let f, g be positive polynomials then fg is a positive polynomial and*

$$supp(fg) = supp(f) + supp(g)$$

Proof. If f, g are positive polynomials then fg is a positive polynomial by definition of polynomial multiplication. If

$$f = \sum_i f_i x^i \qquad g = \sum_j g_j x^j$$

then their product is

$$fg = \sum_i \sum_j f_i g_j x^{i+j}.$$

If $k \in supp(fg)$ then there exists $i \in supp(f)$ and $j \in supp(g)$ such that $i + j = k$ which implies $supp(fg) \subset supp(f) + supp(g)$.

Let $i \in supp(f)$ and $j \in supp(g)$ then $i + j \in supp(fg)$ as no cancellation takes place in the multiplication of two positive polynomials thus $supp(f) + supp(g) \subset supp(fg)$ which implies $supp(fg) = supp(f) + supp(g)$. □

For any $f \in \mathbb{R}[x]$ such that

$$f = \sum_i f_i x^i$$

define polynomials $f_+, f_- \in \mathbb{R}[x]$ as

$$f_+ = \sum_{i:f_i>0} f_i x^i$$
$$f_- = -\sum_{j:f_j<0} f_j x^j$$

then $supp(f_+) \cap supp(f_-) = \phi$ and

$$f = f_+ - f_-.$$

Thus

$$f^2 = f_+^2 + f_-^2 - 2f_+f_-.$$

Then by Lemma 6.1 we have :

$$supp(f_+^2) = 2supp(f_+)$$
$$supp(f_-^2) = 2supp(f_-)$$
$$supp(f_+f_-) = supp(f_+) + supp(f_-).$$

We can establish the following lemma :

Lemma 6.2. *Let $f \in \mathbb{R}[x]$ then*

$$\left(supp(f_+^2 + f_-^2)\right) \triangle (supp(f_+f_-)) \subset supp\left(f^2\right)$$

Proof. Suppose $i \in \left(supp(f_+^2 + f_-^2)\right) \triangle (supp(f_+f_-))$ then i belongs in exactly one of the sets $supp(f_+^2 + f_-^2)$ or $supp(f_+f_-)$. Note that $f_+^2 + f_-^2$ and f_+f_- are both positive polynomials and a term of $f_+^2 + f_-^2$ can be cancelled by a term of f_+f_-. Thus cancellation of a term can happen only when

$$i \in (2supp(f_+) \cup 2supp(f_-)) \cap (supp(f_+) + supp(f_-))$$

which is not the case thus $i \in supp(f^2)$. □

The corollary of Lemma 6.2 is the following :

Corollary 6.3. *Let $f \in \mathbb{R}[x]$, then*

$$||f^2|| \geq |(2supp(f_+) \cup 2supp(f_-)) \triangle (supp(f_+) + supp(f_-))|$$

Proof. Since f_+^2 and f_-^2 are positive polynomials thus $supp(f_+^2 + f_-^2) = (2supp(f_+) \cup 2supp(f_-))$. Now applying Lemma 6.2 we get the desired result. □

6.1 A Much Stronger Conjecture

We make a much stronger conjecture than Conjecture 5.1 which if true would prove Conjecture 5.1. The Conjecture is the following:

Conjecture 6.4. *Let $A, B \subset \mathbb{N}$ such that $A \cap B = \phi$, then*

$$|(2A \cup 2B) \triangle (A + B)| \geq \Omega\left((|A| + |B|)^{1/2}\right)$$

We can prove the following reduction :

Theorem 6.5. *If Conjecture 6.4 is true then Conjecture 5.1 is true.*

Proof. For $f \in \mathbb{R}[x]$, set $A = supp(f_+)$ and $B = supp(f_-)$, then $||f|| = |A| + |B|$ and

$$||f^2|| \geq |(2A \cup 2B) \triangle (A + B)| \geq \Omega\left((|A| + |B|)^{1/2}\right) = \Omega\left(||f||^{1/2}\right)$$

and we are done. □

7 Simulation Study

We tried to gain insight into Conjecture 6.4 by simulating random disjoint subsets A, B and estimating the quantity $|(2A \cup 2B) \triangle (A + B)|$. We first describe the simulation model and then infer some results.

7.1 Simulation Model

We first fix $d, r_1, r_2 \in \mathbb{N}$ such that $r_1 + r_2 < d$. We simulate random subsets $A, B \subset [d]$ such that $A \cap B = \phi$ and $|A| = r_1$, $|B| = r_2$. We then compute the quantities $2A, 2B, 2A \cup 2B, A + B, (2A \cup 2B) \cap (A + B)$ and $(2A \cup 2B) \triangle (A + B)$ and estimate their size. To simplify notation we denote $(2A \cup 2B)$ by C and $(A + B)$ by D.

7.2 Simulation Results

When we set $|A| = |B| = d/2$ we simulated the following result.

d	$\|2A\|$	$\|2B\|$	$\|C\|$	$\|D\|$	$\|C \cap D\|$	$\|C \triangle D\|$
100	191	183	197	194	192	7
1000	1985	1992	1996	1994	1991	8
10000	19986	19987	19999	19990	19990	9
20000	39995	39989	39998	39994	39993	6
30000	59991	59991	59996	59993	59990	9

7.3 Interpretation of Results

Note that $2A, 2B, C, D \subset [2d]$ irrespective of $|A|, |B|$ and when $|A| = |B| = d/2$, we notice that $2A, 2B, C, D$ approximately span the entire set $2d$ due to which $C \cap D$ is very large leading to a small $|C \triangle D|$. We also note that $|C \triangle D|$ does not depend on the size of $|A|$ and $|B|$ essentially disproving Conjecture 6.4.

7.4 Making Conjecture 6.4 More Precise

Observe that $|A| + |B| \leq spread(A, B)$ and $|2A| \leq \mathcal{O}\left(|A|^2\right)$. If we set $|A|, |B| \leq spread(A, B)^{1/k}$, for some fixed large number then we can ensure that $|C \cap D|$ is not too large which might make the current set theoretic framework still usable.

Conjecture 7.1. *Let $A, B \subset \mathbb{N}$ such that $A \cap B = \phi$, and $|A|, |B| \leq spread(A, B)^{1/k}$, for some fixed large number then*

$$|(2A \cup 2B) \triangle (A + B)| \geq \Omega\left((|A| + |B|)^{1/2}\right)$$

We can then make the following corollary :

Conjecture 7.2. *If Conjecture 7.1 is true then Conjecture 5.1 is true.*

Proof. For $f \in \mathbb{R}[x]$ and $t \in \mathbb{N}$ and define :

$$f_t(x) = f(x^t).$$

Then it is easy to see that $||f_t^2|| = ||f^2||$ and $||f_t|| = ||f||$ for all $t \in \mathbb{N}$. Let $A_t = supp(f_{t+})$ and $B_t = supp(f_{t-})$. If we take an arbitrarily large t, we can $spread(A_t, B_t) >> |A_t|, |B_t|$ since $|A_t| = |A_1|$ and $|B_t| = |B_1|$. Thus by conjecture 7.1 we have,

$$||f^2|| \geq \Omega\left(||f||^{1/2}\right).$$

□

8 Conclusion and Future Scope

We have thus developed a set-theoretic framework to study the relationship between $||f^2||$ and $||f||$. In the future, we hope to make Conjecture 7.1 more precise and prove Conjecture 5.1. We also hope to generalize our set theoretic framework to study factor sparsity of arbitrary polynomials rather than just square-roots.

9 Acknowledgement

I would like to thank Prof. Nitin Saxena for the regular discussions and his key insights into the problem which motivated me to work harder on the problem.

10 References

[Abb02] John Abbott. Sparse squares of polynomials. *Mathematics of computation*, 71(237):407–413, 2002.

[BSV20] Vishwas Bhargava, Shubhangi Saraf, and Ilya Volkovich. Deterministic factorization of sparse polynomials with bounded individual degree. *Journal of the ACM (JACM)*, 67(2):1–28, 2020.

[CR88] Benny Chor and Ronald L Rivest. A knapsack-type public key cryptosystem based on arithmetic in finite fields. *IEEE Transactions on Information Theory*, 34(5):901–909, 1988.

[Erd49] P Erdös. On the number of terms of the square of a polynomial. *Nieuw Arch. Wiskunde (2)*, 23:63–65, 1949.

[KI04] Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *computational complexity*, 13(1):1–46, 2004.

[KSS14] Swastik Kopparty, Shubhangi Saraf, and Amir Shpilka. Equivalence of polynomial identity testing and deterministic multivariate polynomial factorization. In *2014 IEEE 29th Conference on Computational Complexity (CCC)*, pages 169–180. IEEE, 2014.

[Rén47] Alfréd Rényi. On the minimal number of terms of the square of a polynomial. *Hungarica Acta Math*, 1:30–34, 1947.

[Sch87] Andrzej Schinzel. On the number of terms of a power of a polynomial. *Acta Arithmetica*, 1(49):55–70, 1987.

[Sud97] Madhu Sudan. Decoding of reed solomon codes beyond the error-correction bound. *Journal of complexity*, 13(1):180–193, 1997.

[Ver49] W Verdenius. On the number of terms of the square and the cube of polynomials. *Indag. Math*, 11:459–465, 1949.

[VG99] Madhu Sudan Venkatesan Guruswami. Improved decoding of reed-solomon and algebraic-geometry codes. 1999.

[Vol17] Ilya Volkovich. On some computations on sparse polynomials. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2017)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2017.

[VZGG13] Joachim Von Zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge university press, 2013.

[VZGK85] Joachim Von Zur Gathen and Erich Kaltofen. Factoring sparse multivariate polynomials. *Journal of Computer and System Sciences*, 31(2):265–287, 1985.