# Sparsity Bound of Polynomials with Bounded Individual Degree

Rishabh Kothary
**Advisor:** Prof. Nitin Saxena
rishk@iitk.ac.in

## 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.

We can see how closely sparse polynomial factorization is related to the sparsity bounds of factors. In this paper we will study sparsity bounds of multivariate polynomial in the bounded individual degree setting as Example 4.1 shows that in the unbounded setting, the factors can be exponentially large.

The central problem we study in this paper 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 $g|f \implies ||g|| \leq ||f||^{\nu(d)}$.*

# 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 $f$.

## 2.2 Polytopes

Let $S = \{u_1, .., u_m\}$ such that $u_i \in \mathbb{R}^t$, then define the convex span or convex hull of S as

$$CS(S) = \left\{ \sum_i \alpha_i u_i \mid \alpha_i \in \mathbb{R}, \alpha_i \geq 0, \sum_i \alpha_i = 1 \right\}.$$

We call a set $P \subset \mathbb{R}^n$ a convex set if for any two points $u, v \in P$ and any $0 \leq \alpha \leq 1$

$$\alpha u + (1 - \alpha) v \in P.$$

We call a convex set $P \subset \mathbb{R}^n$ a polytope if there exists a finite set $S \subset \mathbb{R}^n$ such that $P = CS(S)$. We call $v \in P$ a vertex if there is no $u, w \in P \setminus \{v\}$ such that for any $0 \leq \alpha \leq 1$

$$v = \alpha u + (1 - \alpha)w.$$

Let $V_P$ denote the vertex set of polytope $P = CS(S)$, then it is easy to see that $V_P \subset S$.

Denote $\mathbb{R}^n \setminus \{0\}$ by $\mathbb{R}^n_*$. We define an equivalence relation in $\mathbb{R}^n_*$ as $(a_1, ...a_n) \sim (b_1, ...b_n)$ iff there exists $t > 0$

$$(a_1, .., a_n) = (tb_1, .., tb_n).$$

Then the set of equivalence classes $\left(\mathbb{R}^n_* / \sim\right)$ partitions $\mathbb{R}^n_*$ and we call each equivalence class a direction. For a direction $\lambda$, we can pick a representative element from the equivalence class namely $(\lambda_1, ...\lambda_n)$. Define the function :

$$L_\lambda : \mathbb{R}^n \longrightarrow \mathbb{R}$$
$$(x_1, ..., x_n) \longrightarrow \sum_i x_i \lambda_i$$

Since a polytope is closed and bounded and the function $L_\lambda$ is continous thus for a polytope $P$ there exists a unique constant $c_\lambda \in \mathbb{R}$ such that

$$\max_{x \in P} L_\lambda(x) = c_\lambda.$$

The hyperplane

$$E_\lambda = \{x \in \mathbb{R}^n \mid L_\lambda(x) = c_\lambda\}$$

is called the supporting hyperplane of $P$ in the direction $\lambda$ and

$$P^\lambda = P \cap E_\lambda$$

is called the face of $P$ in the direction $\lambda$. Note that for all $x \in P$, $L_\lambda(x) \leq c_\lambda$, hence $E_\lambda$ is called the supporting hyperplane. Then it can be seen easily that

$$\partial P = \bigcup_\lambda P^\lambda$$

For two sets A,B we define the Minkowski sum as

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

For a polynomial $f \in \mathbb{F}[x_1, ..., x_n]$ we define the Newton polytope $P_f = CS(supp(f))$. We denote the set of vertices of $P_f$ by $V_f$.

# 3 Important Results

## 3.1 Polytopes

**Lemma 3.1.** *Let $P, R$ be polytopes, then $P+R$ is a polytope and*

$$P + R = CS(V_P + V_R).$$

*Proof.* It is trivial to see $CS(V_P + V_R) \subset P + R$. To show $P + R \subset CS(V_P + V_R)$ take any $\gamma \in P + R$, then by $\gamma = \alpha + \beta$, where $\alpha \in P$ and $\beta \in R$. Let $V_P = \{u_1, ..u_m\}$ and $V_R = w_1, ...w_n$ then

$$\alpha = \sum_i a_i u_i$$
$$\beta = \sum_j b_j w_j$$

where $a_i, b_j \geq 0$ and $\sum_i a_i = \sum_j b_j = 1$. Define $c_{i,j} = a_i b_j$ for $1 \leq i \leq m$ and $1 \leq j \leq n$ then

$$\gamma = \alpha + \beta = \sum_{i,j} c_{i,j} (u_i + v_j)$$

implying $\gamma \in CS(V_P + V_R)$ which implies $P + R \subset CS(V_P + V_R)$ and proving the lemma. □

**Lemma 3.2.** *Let $\lambda$ be any direction and P,R be two polytopes, then if*

$$E_\lambda^P = \{x \in \mathbb{R}^n \mid L_\lambda(x) = c_\lambda^P\}$$
$$E_\lambda^R = \{x \in \mathbb{R}^n \mid L_\lambda(x) = c_\lambda^R\}$$

*are the supporting hyperplanes of $P, R$ in the direction $\lambda$ respectively then*

$$E_\lambda^{P+R} = \{x \in \mathbb{R}^n \mid L_\lambda(x) = c_\lambda^P + c_\lambda^R\}$$

*is the supporting hyperplane of $P + R$ in the direction $\lambda$. Moreover*

$$(P + R)^\lambda = P^\lambda + R^\lambda$$

*Proof.* To show $E_\lambda^{P+R}$ is the supporting hyperplane of $P + R$ it is enough to show

$$\max_{\gamma \in P+R} L_\lambda(\gamma) = c_\lambda^P + c_\lambda^R$$

Note that for any $\gamma \in P + R$, there exists $\alpha \in P, \beta \in R$ such that $\gamma = \alpha + \beta$ which implies

$$\begin{aligned}
\max_{\gamma \in P+R} L_\lambda(\gamma) &= \max_{\substack{\alpha \in P \\ \beta \in R}} L_\lambda(\alpha + \beta) \\
&= \max_{\substack{\alpha \in P \\ \beta \in R}} L_\lambda(\alpha) + L_\lambda(\beta) \\
&= \max_{\alpha \in P} L_\lambda(\alpha) + \max_{\beta \in R} L_\lambda(\beta) \\
&= c_\lambda^P + c_\lambda^R.
\end{aligned}$$

To show

$$(P + R)^\lambda = P^\lambda + R^\lambda$$

note that $P^\lambda + R^\lambda \subset (P + R)^\lambda$ follows trivially. We only need to show $(P + R)^\lambda \subset P^\lambda + R^\lambda$. Suppose $(P + R)^\lambda \not\subset P^\lambda + R^\lambda$, then without loss of generality we can assume that there exists $\alpha \in P \setminus P^\lambda$, $\beta \in R$ such that $\alpha + \beta \in (P + R)^\lambda$. But then

$$\begin{aligned}
L_\lambda(\alpha + \beta) &= L_\lambda(\alpha) + L_\lambda(\beta) \\
&< c_\lambda^P + L_\lambda(\beta) \\
&\leq c_\lambda^P + c_\lambda^R
\end{aligned}$$

which is not possible by the definition of $(P + R)^\lambda$, and hence by contradiction $(P + R)^\lambda \subset P^\lambda + R^\lambda$. □

**Lemma 3.3** ([Zie12])**.** *A point $u \in P$ is a vertex iff there exists a direction $\lambda$ such that $P^\lambda = \{u\}$.*

The following corollary follows from the above lemmas :

**Corollary 3.4.** *Let $P, Q, R$ be polytopes such that $P = Q + R$ and if there exists a direction $\lambda$ such that $P^\lambda = \{u\}$ then there exists $v \in Q$ and $w \in R$ such that $Q^\lambda = \{v\}$ and $R^\lambda = \{w\}$. Moreover there doesnot exist any other pair of points $v' \in Q$ and $w' \in R$ such $u = v' + w'$.*

*Proof.* $P^\lambda = Q^\lambda + R^\lambda$ implies that $P^\lambda$ contains a translated copy of $Q^\lambda$ and $R^\lambda$. Since $Q^\lambda$ and $R^\lambda \neq \phi$ by definition, and $|P^\lambda| = 1$ this implies $|Q^\lambda| = |R^\lambda| = 1$ which implies there exists $v \in Q$ and $w \in R$ such that $Q^\lambda = \{v\}$ and $R^\lambda = \{w\}$.

Suppose there exists $v' \in Q$ and $w' \in R$ such that $u = v' + w'$, then

$$\begin{aligned} u &= \left(\frac{v+w}{2}\right) + \left(\frac{v'+w'}{2}\right) \\ &= \left(\frac{v+w'}{2}\right) + \left(\frac{v'+w}{2}\right). \end{aligned}$$

Since $v + w', v' + w \in Q + R = P$ and $u$ is a vertex by Lemma 3.3, thus

$$v + w' = v' + w = u = v + w = v' + w'$$

implying $v = v'$ and $w = w'$. □

Corollary 3.4 effectively says that if $P = Q + R$, then every vertex of $P$ can be written as the unique sum of a vertex of $Q$ and of a vertex of $R$.

**Lemma 3.5** ([Sch00]). *Let $P, Q, R$ be polytopes such that $P = Q + R$, then*

$$|V_P| \geq max\{|V_Q|, |V_R|\}$$

*Proof.* We first show that $|V_P| \geq |V_Q|$ by showing that for any $v \in V_Q$, there exists $w \in V_R$ such that $u = v + w \in V_P$. Polytopes have finite number of distinct faces, thus for a vertex $v \in V_Q$ there are infinite choices of directions $\lambda$ such that $Q^\lambda = \{v\}$. Thus we choose a $\lambda$ such that $|R^\lambda| = 1$ implying there exists $w \in V_R$ such that $R^\lambda = \{w\}$. Since $P^\lambda = Q^\lambda + R^\lambda$, thus $u = v + w \in V_P$. Thus implying $|V_P| \geq |V_Q|$.

Using a similar argument for $V_R$ we can show $|V_P| \geq |V_R|$, thus implying

$$|V_P| \geq max\{|V_Q|, |V_R|\}.$$

□

## 3.2 Polynomials and Polytopes

The following theorem tells about a key structural property of newton polytope of a multivariate polynomials :

**Theorem 3.6** ([Ost21],[Ost75],[Gao01]). *Let $f, g, h \in \mathbb{F}[x_1, ..., x_n]$ such that $f = g \cdot h$, then*

$$P_f = P_g + P_h$$

*where $P_f, P_g, P_h$ are the Newton polytopes of $f, g, h$ respectively.*

*Proof.* Since $supp(f) \subset supp(g) + supp(h)$, thus $P_f \subset P_g + P_h$. By Corollary 3.4, for every vertex $u$ of $P_g + P_h$, there exists pair of vertices $v \in V_g$ and $w \in V_h$ such that $u = v + w$. Hence in the multiplication of $g, h$ due to the uniqueness of the pair, the monomial corresponding to $u$ survives and hence $u \in supp(f)$. This implies that $P_g + P_h \subset P_f$ which implies $P_f = P_g + P_h$. □

## 3.3 Convex Geometry

The famous Caratheodory's theorem in Convex geometry is:

**Lemma 3.7** ([Zie12]). *If $\mu \in \mathbb{R}^n$ lies in the convex hull of a set $U$ then $\mu$ can be written as the convex combination of at most $n + 1$ points of $U$.*

We will be needing a slight modification of this fundamental result which is

**Theorem 3.8** ([Bar15]). *Given a set of vectors $U = \{u_1, .., u_m\} \subset \mathbb{R}^n$ with $||u_i||_\infty \leq 1$ and $\epsilon > 0$. For every $\mu \in CS(U)$ there exists an $\mathcal{O}\left(\frac{\log n}{\epsilon^2}\right)$ uniform vector $\mu' \in CS(U)$ such that $||\mu - \mu'|| \leq \epsilon$*

*Proof.* Since $\mu \in CS(U)$ thus

$$\mu = \sum_{i=1}^{m} a_i u_i$$

where $\sum_{i=1}^{m} a_i = 1$. Define the following probability distribution on the set $U$ where $Pr[u_i] = a_i$ for $1 \leq i \leq m$. If we take $t = \left(\frac{\log n}{\epsilon^2}\right)$ iid samples from this distribution call it $\{v_1, ..., v_t\}$ and let

$$\mu' = \frac{1}{t} \sum_{i=1}^{t} v_i$$

Let $\mu'_j, \mu_j$ be the $j^{th}$ co-ordinate of $\mu'$ and $\mu$ respectively, then the claim is that

$$Pr\left[|\mu_j - \mu'_j| \geq \epsilon\right] < \frac{1}{n}.$$

The claim follows from the Chernoff-Hoeffding inequality applied to t independent samples $Y_1, ...Y_t$ of the random variable $Y$, where $Pr[Y = (u_i)_j] = a_i$ for $1 \leq i \leq m$. Thus by union bound

$$Pr\left[||\mu - \mu'||_\infty > \epsilon\right] < 1$$

which implies that with positive probability there exists $||\mu - \mu'||_\infty < \epsilon$, thus proving the existence of a suitable uniform vector as demanded in the theorem. □

# 4 General Sparsity Bounds

Let $f, g, h \in \mathbb{F}[x_1, ., ..x_n]$ such that $f = gh$, then in this section we find a bound of $||g||$ in terms of $||f||$. We first state the best known examples of largest blowups in sparsity of in the factor.

## 4.1 Examples of largest blowups

The biggest blowup in characteristic zero field known is the following

**Example 4.1** ([VZGK85]). *Let $f \in \mathbb{F}[x_1, ...x_n]$ where $\mathbb{F}$ is characteristic zero field of bounded individual degree $d$, such that*

$$f = \prod_{i=1}^{n} (x_i^d - 1)$$

*then the following polynomial $g \in \mathbb{F}[x_1, ...x_n]$ is a factor of $f$ :*

$$g = \prod_{i=1}^{n} \left(1 + x_i + ... + x_i^{d-1}\right)$$

*and note that $||f|| = 2^n$ and $||g|| = d^n = ||f||^{\log d}$.*

The biggest blowup in the characteristic $p$ case known is

**Example 4.2** ([BSV20]). *Let $p$ be a prime and let $0 < d < p$. Define $f \in \mathbb{F}_p[x_1, ..x_n]$ as*

$$f = x_1^p + ... + x_n^p = (x_1 + ... + x_n)^p$$

*then the polynomial $g \in \mathbb{F}_p[x_1, ..., x_n]$ defined as*

$$g = (x_1 + ... + x_n)^d$$

*is a factor of $f$. Note that $||f|| = n$ and $||g|| = \binom{n+d-1}{d} \approx n^d = ||f||^d$.*

Both the examples are in agreement with Conjecture 1.2.

## 4.2 Finding General Sparsity Bound

To find the general sparsity bound we first approximate the number of internal points of a polytope in terms of the size of its vertex set with the following lemma

**Lemma 4.3** ([BSV20]). *Let $E \subset \{0, 1, ..., d\}^n$ and $t = |V(CS(E))|$. Then there exists an absolute constant $C$ such that $t^{Cd^2 \log n} \geq |E|$.*

*Proof.* Define the set $E_d$ as

$$E_d = \left\{ \frac{u}{d} \mid u \in E \right\}$$

and, let $U_d = V(CS(E_d))$ and $U = V(CS(E))$ then clearly $U_d \subset E_d$ and $|U_d| = |U| = t$. For any two distinct vectors $u, v \in E_d$

$$||u - v||_\infty \geq \frac{1}{d}$$

Set $\epsilon = \frac{1}{3d}$ and applying Theorem 3.8 on the set $U_d$ we can find $\mathcal{O}(\frac{\log n}{\epsilon^2}) = \mathcal{O}(d^2 \log n)$ uniform vectors $u', v'$ such that

$$||u - u'||_\infty \leq \frac{1}{3d} \qquad ||v - v'||_\infty \leq \frac{1}{3d}.$$

By applying triangle inequality we get

$$\begin{aligned} ||u' - v'||_\infty &\geq ||u - v||_\infty - ||u - u'||_\infty - ||v - v'||_\infty \\ &\geq \frac{1}{d} - \frac{1}{3d} - \frac{1}{3d} \\ &\geq \frac{1}{3d} \end{aligned}$$

which implies that $u' \neq v'$. Hence we have shown the existence of $|E_d| = |E|$ distinct $\mathcal{O}(d^2 \log n)$ vectors. Note that the number of $\mathcal{O}(d^2 \log n)$ vectors of the set $U_d$ are $|U_d|^{\mathcal{O}(d^2 \log n)} \leq t^{Cd^2 \log n}$ for some constant $C$. Hence we have

$$t^{Cd^2 \log n} \geq |E|.$$

□

We have the tools to prove the general sparsity bound which is stated int the following theorem:

**Theorem 4.4** ([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 $\xi(n, s, d)$.*

*Proof.* Let $P_f, P_g, P_h$ be the newton polytopes of $f, g, h$respectively and let $V_f, V_g, V_h$ be the vertices of $P_f, P_g, P_h$. Then applying Lemma 4.3 on $E = supp(g)$, we get:

$$||g|| \leq |V_g|^{Cd^2 \log n}$$

for some constant C. By Theorem 3.6 and Lemma 3.5 we get $|V_f| \geq |V_g|$, hence we have

$$||g|| \leq |V_g|^{Cd^2 \log n} \leq |V_f|^{Cd^2 \log n} \leq ||f||^{Cd^2 \log n}$$

and the theorem follows. □

However the sparsity bound achieved is not in agrrement with Conjecture 1.2.

# 5 Possible approaches to improve the sparsity bound

## 5.1 Improving the estimate of integer points?

We call a polytope $P \subset \mathbb{R}^n$ symmetric if for every $u \in P$ and permutation $\sigma \in S_n$, $\sigma \circ u \in P$. A better estimate of integer points has been shown :

**Lemma 5.1** ([BS22]). *Let $V \subset \{0, 1, ..., d\}^n$ be the vertices of a symmetric polytope $P$. Then, $|P \cap \mathbb{Z}^n| \leq |V|^{\mathcal{O}(d^2 \log d)}$.*

We define a polynomial $f \in \mathbb{F}[x_1, ..., x_n]$ to be symmetric if the newton polytope $P_f$ is symmetric. Then the following theorem gives a better sparsity bound when $f$ is symmetric.

**Theorem 5.2** ([BS22]). *Let $f \in \mathbb{F}[x_1, ...x_n]$ be a symmetric polynomial with constant individual degree $d$, over any field $\mathbb{F}$. Then, every factor of $f$ has its sparsity bounded by $s^{\mathcal{O}(d^2 \log d)}$.*

However, for a general polynomial we cant lose the $\log n$ factor in Lemma 4.3 factor due to the following lemma:

**Lemma 5.3** ([BSV20]). *There is a set $E \subset \{-1, 0, 1\}$ such that $|V(CS(E))| = n$ and $|E| = n^{\Omega(\log n)}$.*

*Proof.* Let $n = 2^m$ for some positive integer, define the $n \times n$ Hadamard matrix $H$ as $H_{i,j} = (-1)^{\langle i,j \rangle}$, where $i, j$ are in their binary representation and $\langle i, j \rangle$ is the dot-product. We can assume $i, j \in \mathbb{F}_2^m$.

Let $S \subset \mathbb{F}_2^m$ be any subspace of the vector space $\mathbb{F}_2^m$ over the field $\mathbb{F}_2$. Define the characteristic vector $u_S$ of size $n \times 1$ as, $u_i = 1$ if $i \in S$, else $u_i = 0$. Then the claim is that

$$\frac{1}{|S|} H \cdot u_S \subset \{0, 1\}^n.$$

Define the set $S^\perp = \{b \in \mathbb{F}_2^m \mid \langle b, a \rangle = 0, \forall a \in S\}$. For any $b \in \mathbb{F}_2^m$

$$(H \cdot u_S)_b = \sum_{a \in S} (-1)^{\langle a,b \rangle}.$$

Thus for $b \in S^\perp$, $(H \cdot u_S)_b = |S|$. If $b \notin S^\perp$, then there exists $c \in S$ such that $\langle b, c \rangle = 1$ implying that for all $a \in S$, $(-1)^{\langle a,b \rangle} = -(-1)^{\langle a+c,b \rangle}$ which implies $(H \cdot u_S)_b = 0$. Hence we have proved

$$\frac{1}{|S|} H \cdot u_S \subset \{0, 1\}^n.$$

Let $V \subset \{-1, +1\}^n$ be the set of column vectors of $H$. The number of subspaces of $\mathbb{F}_2^m = n^{\Omega(\log n)}$, and since $S^\perp$ is uniquely characterizes a subspace $S$, we have shown that the uniform convex combinations of elements of $V$ has atleast $n^{\Omega(\log n)} \in \{0, 1\}^n$. Hence completing the proof. □

[Aga22] further studies the polytope in the proof of Lemma 5.3. Firstly note that we can simply translate the entire polytope by an integer distance in each axis given in the proof of Lemma 5.3 so that $V \subset \{0, 2\}^n$ as it wont change the combinatorial properties. [Aga22] defines the polynomial $g_H \in \mathbb{F}[x_1, ..., x_n]$ such that $V_{g_H} = V$ as given in the proof of Lemma 5.3 and calls it the Hadamard polynomial. They prove the following lemma :

**Lemma 5.4.** *Let $f = g_H \cdot h$, where $g_H$ is the Hadamard polynomial, and $h$ is some polynomial in $\mathbb{F}[x_1, ..., x_n]$ such that $||h|| \leq \frac{||g_H||}{2}$, then*

$$||f|| \geq ||g_H||.$$

Thus Conjecture 1.2 still holds strong in a sense.

### 5.2 When $supp(f) = V_f$ ?

If $f = g \cdot h$, where $f, g, h \in \mathbb{F}[x_1, ..., x_n]$, we can study the case when $supp(f) = V_f$ to find more structural properties about $supp(g)$. We conjectured

**Conjecture 5.5.** *Let $f, g, h \in \mathbb{F}[x_1, .., x_n]$, such that $f = g \cdot h$. If $supp(f) = V_f$, then $supp(g) = V_g$.*

The conjecture is not true as if we take $f = x^d - 1$, then $supp(f) = \{0, n\}$ and $V_f = \{0, n\} = supp(f)$. But $g = 1 + x + ... + x^{d-1}$ is a factor of $f$ such that $supp(g) = \{0, 1, .., d-1\}$ and $V_g = \{0, d-1\} \neq supp(g)$.

In the one-dimensional case it was not clear if $supp(g) \subset \partial P_g$, so we conjetured

**Conjecture 5.6.** *Let $f, g, h \in \mathbb{F}[x_1, ..., x_n]$ such that $f = g \cdot h$. If $supp(f) = V_f$, then $supp(g) \subset \partial P_g$.*

The conjecture is not true as if we take $f = (x^d - 1)(y^d - 1)$, then $supp(f) = \{(0, 0), (0, d), (d, d), (d, 0)\}$ and $V_f = \{(0, 0), (0, d), (d, d), (d, 0)\} = supp(f)$. But $g = (1 + x + ... + x^{d-1})(1 + y + .. + y^{d-1})$ is a factor of $f$ such that $supp(g) = \{(i, j) \in \mathbb{Z}^2 \mid 0 \leq i, j \leq d-1\}$ and $\partial P_g = \{(i, 0) \in \mathbb{R}^2 \mid 0 \leq i \leq d-1\} \cup \{(0, j) \in \mathbb{R}^2 \mid 0 \leq j \leq d-1\}$. Thus clearly $supp(g) \not\subset \partial P_g$, in fact $supp(g) = P_g \cap \mathbb{Z}^2$.

## 6 Conclusion and Future Scope

We studied the problem of bounding the sparsity of the factor of a multivariate polynomial and its connection to convex geometry. All of our current approaches didn't give us a way to improve the known results. We hope to study a simpler version of this problem, namely when $f$ is a perfect square and find new approaches to tackle this problem in the future. Indecomposability of polytopes [Gao01] is also an interesting property that can provide key insights to this problem.

## 7 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.

## 8 References

[Aga22] Sanyam Agarwal. *Factorization of sparse polynomials of bounded individual degree.* PhD thesis, Chennai Mathematical Institute, 2022.

[Bar15] Siddharth Barman. Approximating nash equilibria and dense bipartite subgraphs via an approximate version of caratheodory's theorem. In *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*, pages 361–369, 2015.

[BS22] Pranav Bisht and Nitin Saxena. Derandomization via symmetric polytopes: Poly-time factorization of certain sparse polynomials. 2022.

[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.

[Gao01] Shuhong Gao. Absolute irreducibility of polynomials via newton polytopes. *Journal of Algebra*, 237(2):501–520, 2001.

[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.

[Ost21] A Ostrowski. U on the meaning of the theory of convex polyhedra for the formal algebra. *Annual Reports German Math. Association*, 20:98–99, 1921.

[Ost75] Alexander M Ostrowski. On multiplication and factorization of polynomials, i. lexicographic orderings and extreme aggregates of terms. *aequationes mathematicae*, 13(3):201–228, 1975.

[Sch00] Andrzej Schinzel. *Polynomials with special regard to reducibility*, volume 77. Cambridge University Press, 2000.

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

[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.

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

[Zie12] Günter M Ziegler. *Lectures on polytopes*, volume 152. Springer Science & Business Media, 2012.