Sparse Polynomial Factorization: Structural and Algorithmic results

Vishwas Bhargava
Rutgers

Shubhangi Saraf
Rutgers

Ilya Volkovich
University of Michigan

Sparsity

Given, $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $\forall\, i,\ deg_{x_i} f \leq d$.

- Sparsity of f (denoted by $\|f\|$) $:=$ number of monomials in f(with non-zero coeff.).
- Example, $f = x_1 + x_2^3 + x_3 x_4 + 20$ then $\|f\|$=4.

Sparsity

Given, $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $\forall\, i,\ deg_{x_i} f \leq d$.

- Sparsity of f (denoted by $\|f\|$) := number of monomials in f(with non-zero coeff.).
- Example, $f = x_1 + x_2^3 + x_3x_4 + 20$ then $\|f\|$=4.
- $\|f\|$ can be as high as $(d+1)^n$. Polynomials that contain much less monomials are considered *sparse polynomials.*

Sparsity

Given, $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $\forall\, i,\ deg_{x_i} f \leq d$.

- Sparsity of f (denoted by $\|f\|$) := number of monomials in f(with non-zero coeff.).
- Example, $f = x_1 + x_2^3 + x_3x_4 + 20$ then $\|f\|$=4.
- $\|f\|$ can be as high as $(d+1)^n$. Polynomials that contain much less monomials are considered *sparse polynomials.*
- Sparsity is natural complexity measure and was studied in [GK85, KS01, Zip79, SW05, SSS13 and ....*many more*].

Are factors of sparse polynomials sparse?

Example (von zur Gathen-Kaltofen'85)

Let

$$f(x) = \prod_{i=1}^{n} (x_i^d - 1),$$
$$g(x) = \prod_{i=1}^{n} (1 + x_i + \ldots + x_i^{d-1})$$

Are factors of sparse polynomials sparse?

Example (von zur Gathen-Kaltofen'85)

Let

$$f(x) = \prod_{i=1}^{n}(x_i^d - 1),$$
$$g(x) = \prod_{i=1}^{n}(1 + x_i + \ldots + x_i^{d-1})$$

$\|f\| = 2^n$ and $\|g\| = d^n \implies \|g\| = \|f\|^{\log d}$.

Are factors of sparse polynomials sparse?

Example (von zur Gathen-Kaltofen'85)

Let

$$f(x) = \prod_{i=1}^{n} (x_i^d - 1),$$
$$g(x) = \prod_{i=1}^{n} (1 + x_i + \ldots + x_i^{d-1})$$

$\|f\| = 2^n$ and $\|g\| = d^n \implies \|g\| = \|f\|^{\log d}$.

Conjecture [von zur Gathen-Kaltofen'85]

Whether a quasi-polynomial bound holds for the sparsity of factors of sparse polynomials?

Are factors of sparse polynomials sparse?

Example (Volkovich'15, Dvir-Oliveira'15)

Let $f \in \mathbb{F}_p[x_1, \dots x_n]$, p-prime and let $0 < d < p$.

$$f(x) = x_1^p + x_2^p + \ldots + x_n^p,$$
$$g(x) = \left(x_1 + x_2 + \ldots x_n\right)^d$$

$\|f\| = n$ and $\|g\| = \binom{n+d-1}{d} \approx n^d \implies \|g\| = \|f\|^d$.

Previous works

Are factors of sparse polynomials of low sparsity?

Previous works

Are factors of sparse polynomials of low sparsity?

- multilinear and multi-quadratic polynomials (d=1 and d=2) [SV'10, Vol'17]

Previous works

Are factors of sparse polynomials of low sparsity?

- multilinear and multi-quadratic polynomials (d=1 and d=2) [SV'10, Vol'17]
- an *attempt* by [Dvir-Oliveira'15].

Are factors of “low complexity” polynomials of low complexity?

Are factors of "low complexity" polynomials of low complexity?

Yes, in these cases.

Are factors of “low complexity” polynomials of low complexity?

Yes, in these cases.

- VP [Kaltofen’87, Kaltofen’89]

Are factors of “low complexity” polynomials of low complexity?

Yes, in these cases.

- VP [Kaltofen’87, Kaltofen’89]
- Constant depth circuits [Oliviera’15] (small individual degree)

Are factors of “low complexity” polynomials of low complexity?

Yes, in these cases.

- VP [Kaltofen’87, Kaltofen’89]
- Constant depth circuits [Oliviera’15] (small individual degree)
- VNP [DSS’18, CKS’18]
- ABP/Formulas [DSS’18, CKS’18] (quasi-polynomial blowup)

Our Result

Factor Sparsity Bound

Let $\mathbb{F}$ be an arbitrary field and let $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ be a polynomial of sparsity s and individual degrees at most d, then the sparsity of every factor of f is bounded by $s^{\mathcal{O}(d^2 \log n)}$.

Our Result

Factor Sparsity Bound

Let $\mathbb{F}$ be an arbitrary field and let $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ be a polynomial of sparsity s and individual degrees at most d, then the sparsity of every factor of f is bounded by $s^{\mathcal{O}(d^2 \log n)}$.

Remark: This is the first nontrivial bound on factor sparsity for any $d > 2$.

Our Result

Factor Sparsity Bound

Let $\mathbb{F}$ be an arbitrary field and let $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ be a polynomial of sparsity s and individual degrees at most d, then the sparsity of every factor of f is bounded by $s^{\mathcal{O}(d^2 \log n)}$.

Remark: This is the first nontrivial bound on factor sparsity for any $d > 2$.

Remark: Our bound is *field oblivious* and thus "somewhat tight".

Proof of Sparsity Bound

Suppose that $f, g, h \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ such that

$$f = g \cdot h.$$

Want to show, f is s-sparse and with bounded individual degree d, then g and h are both at most s' sparse, where $s' = s^{\mathcal{O}(d^2 \log n)}$.

Proof of Sparsity Bound

Suppose that $f, g, h \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ such that

$$f = g \cdot h.$$

Want to show, f is s-sparse and with bounded individual degree d, then g and h are both at most s' sparse, where $s' = s^{\mathcal{O}(d^2 \log n)}$.

We instead show the following slightly more general result.

Proof of Sparsity Bound

Suppose that $f, g, h \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ such that

$$f = g \cdot h.$$

Want to show, f is s-sparse and with bounded individual degree d, then g and h are both at most s' sparse, where $s' = s^{\mathcal{O}(d^2 \log n)}$.

We instead show the following slightly more general result.

Suppose that g is any polynomial of individual degree d such that $\|g\| = s$, and suppose that $f = g \cdot h$ *(with no assumptions on the degrees of f and h)*, then

$$\|f\| \geq s^{\frac{1}{\mathcal{O}(d^2 \log n)}}.$$

In particular, there is no polynomial h that one can multiply g with, so that the product $g \cdot h$ has an overwhelming cancellation of monomials.

Newton Polytopes

Let,

$$f = \sum a_{i_1 i_2 \dots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}.$$

Newton Polytopes

Let,

$$f = \sum a_{i_1 i_2 \dots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}.$$

Consider the set,

$$\mathrm{Supp}(f) = \{(i_1, i_2, \dots, i_n) \mid a_{i_1 i_2 \dots i_n} \neq 0\} \subseteq \mathbb{R}^n$$

of exponent vectors of f.

One can then associate a polytope $P_f \subseteq \mathbb{R}^n$, called the Newton polytope of f, which is the convex hull of points in $\mathrm{Supp}(f)$.

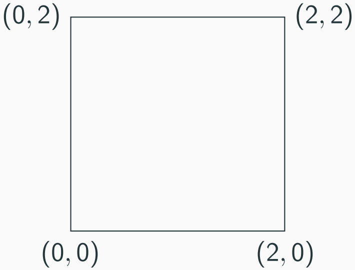
Newton Polytope: Example

Let, $f = 1 + x_1^2 + x_2^2 + x_1^2 x_2^2$

Newton Polytope: Example

Let, $f = 1 + x_1^2 + x_2^2 + x_1^2 x_2^2$

$P_f =$



Newton Polytope: Properties

Fact 1 [Ostrowski'21]

If $f = g \cdot h$, then $P_f = P_g + P_h$. ($+$ represents Minkowski sum)

Newton Polytope: Properties

Fact 1 [Ostrowski'21]

If $f = g \cdot h$, then $P_f = P_g + P_h$. ($+$ represents Minkowski sum)

Fact 2 (Folklore)

let $V(P)$ denote the set of vertices (equivalently corner points) of a polytope P, then

$$|V(A + B)| \geq \max\{|V(A)|, |V(B)|\}.$$

Newton Polytope: Properties

Fact 1 [Ostrowski'21]

If $f = g \cdot h$, then $P_f = P_g + P_h$. ($+$ represents Minkowski sum)

Fact 2 (Folklore)

let $V(P)$ denote the set of vertices (equivalently corner points) of a polytope P, then

$$|V(A+B)| \geq \max\{|V(A)|, |V(B)|\}.$$

Notice,

$$\|f\| \geq |V(P_f)|$$

Newton Polytope: Properties

Fact 1 [Ostrowski'21]

If $f = g \cdot h$, then $P_f = P_g + P_h$. ($+$ represents Minkowski sum)

Fact 2 (Folklore)

let $V(P)$ denote the set of vertices (equivalently corner points) of a polytope P, then

$$|V(A + B)| \geq \max\{|V(A)|, |V(B)|\}.$$

Notice,

$$\|f\| \geq |V(P_f)| = |V(P_g + P_h)|$$

Newton Polytope: Properties

Fact 1 [Ostrowski'21]

If $f = g \cdot h$, then $P_f = P_g + P_h$. ($+$ represents Minkowski sum)

Fact 2 (Folklore)

let $V(P)$ denote the set of vertices (equivalently corner points) of a polytope P, then

$$|V(A+B)| \geq \max\{|V(A)|, |V(B)|\}.$$

Notice,

$$\|f\| \geq |V(P_f)| = |V(P_g + P_h)| \geq \max\{|V(P_g)|, |V(P_h)|\}.$$

Main Task

arbitrary nonzero polynomial

$$f = g \cdot h$$

$\|f\| \geq |V(P_g)|$

n-variate, individual degree d

Main Task

arbitrary nonzero polynomial

$$f = g \cdot h$$

$\|f\| \geq |V(P_g)|$

n-variate, individual degree d

Showing a lower bound on $|V(P_g)|$ will be the main technical core of our proof of the sparsity bound.

Main Task

$$\|f\| \geq |V(P_g)| \longrightarrow f = g \cdot h$$

arbitrary nonzero polynomial

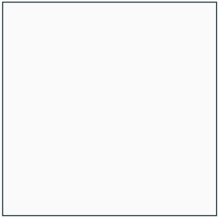
n-variate, individual degree d

Showing a lower bound on $|V(P_g)|$ will be the main technical core of our proof of the sparsity bound.

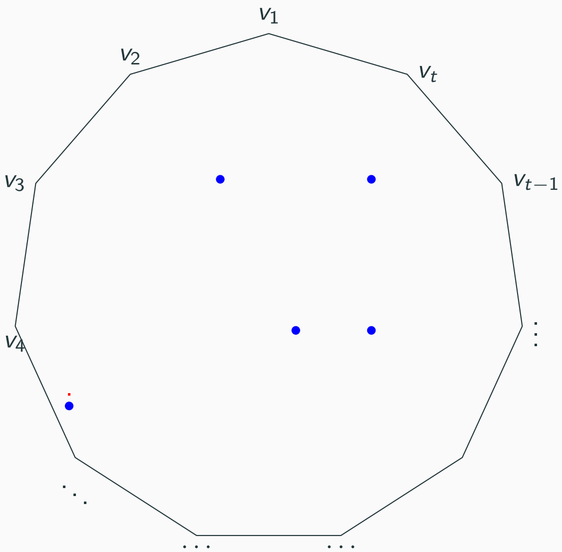
This connection between Newton polytopes and sparsity bounds was first made in [Dvir-Oliveira'14] and indeed it inspired the approach taken in this paper.

Note that in general, for an arbitrary Polytope P, there is no good bound on the number of vertices of P in terms of the number of monomials of g.

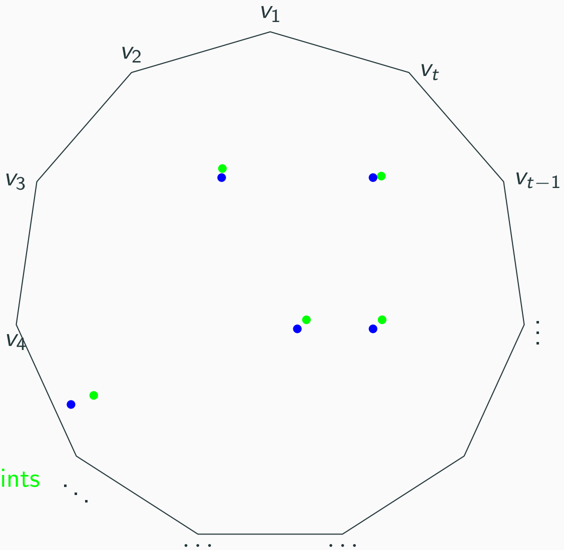
Note that in general, for an arbitrary Polytope P, there is no good bound on the number of vertices of P in terms of the number of monomials of g.



Note that in general, for an arbitrary Polytope P, there is no good bound on the number of vertices of P in terms of the number of monomials of g.



• lattice points



• ϵ close to lattice points

• lattice points

Approx. Carathéodory's Theorem

Theorem (Barman'15)

Given a set of vectors $V = \{v_1, v_2, \ldots, v_t\} \subseteq \mathbb{R}^n$ *with* $\max_{v \in U} \|u\|_\infty \leq d$, *and* $\epsilon > 0$. *For every* $\mu \in CS(U)$ *there exists an* $\mathcal{O}\left(\frac{d^2 \log n}{\epsilon^2}\right)$ *uniform vector* $\mu' \in CS(U)$ *such that* $\|\mu - \mu'\|_\infty \leq \epsilon$.

Approx. Carathéodory's Theorem

Theorem (Barman'15)

Given a set of vectors $V = \{v_1, v_2, \ldots, v_t\} \subseteq \mathbb{R}^n$ with $\max_{v \in U} \|u\|_\infty \leq d$, and $\epsilon > 0$. For every $\mu \in CS(U)$ there exists an $\mathcal{O}\left(\frac{d^2 \log n}{\epsilon^2}\right)$ uniform vector $\mu' \in CS(U)$ such that $\|\mu - \mu'\|_\infty \leq \epsilon$.

- uniform combination of $(v_1, v_2, \ldots, v_k) := \frac{\sum_i v_i}{k}$

Approx. Carathéodory's Theorem

Theorem (Barman'15)

Given a set of vectors $V = \{v_1, v_2, \ldots, v_t\} \subseteq \mathbb{R}^n$ *with* $\max_{v \in U} \|u\|_\infty \leq d$, *and* $\epsilon > 0$. *For every* $\mu \in CS(U)$ *there exists an* $\mathcal{O}\left(\frac{d^2 \log n}{\epsilon^2}\right)$ *uniform vector* $\mu' \in CS(U)$ *such that* $\|\mu - \mu'\|_\infty \leq \epsilon$.

- uniform combination of $(v_1, v_2, \ldots, v_k) := \frac{\sum_i v_i}{k}$
- each lattice point can be "associated" by atleast one $\mathcal{O}\left(d^2 \log n\right)$-uniform vector.

Theorem (Barman'15)

Given a set of vectors $V = \{v_1, v_2, \ldots, v_t\} \subseteq \mathbb{R}^n$ with $\max_{v \in U} \|u\|_\infty \leq d$, and $\epsilon > 0$. For every $\mu \in CS(U)$ there exists an $\mathcal{O}\left(\frac{d^2 \log n}{\epsilon^2}\right)$ uniform vector $\mu' \in CS(U)$ such that $\|\mu - \mu'\|_\infty \leq \epsilon$.

- uniform combination of $(v_1, v_2, \ldots, v_k) := \frac{\sum_i v_i}{k}$
- each lattice point can be "associated" by atleast one $\mathcal{O}\left(d^2 \log n\right)$-uniform vector.
- $\#\left(d^2 \log n\right)$-uniform vectors $\approx t^{\left(d^2 \log n\right)}$

This proves our Sparsity Bound. $\square$

Deterministic Factoring Algorithm

Polynomial factorization

Given, $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$

- Either give a factorization

$$f = \prod g_i$$

- Or Output f is irreducible.

Polynomial factorization

Given, $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$

- Either give a factorization

$$f = \prod g_i$$

- Or Output f is irreducible.

Applications: list decoding [Sud97, GS99], derandomization [KI04] and cryptography [CR88].

Representing a Polynomial

- **White-box Arithmetic Circuit**
- **Black-box Arithmetic Circuit**

A brief history on Polynomial factorization

- **White-box Arithmetic Circuit** [Kaltofen'87, Kaltofen'89]
- **Black-box Arithmetic Circuit** [Kaltofen-Trager'90]

A brief history on Polynomial factorization

- **White-box Arithmetic Circuit** [Kaltofen'87, Kaltofen'89]
- **Black-box Arithmetic Circuit** [Kaltofen-Trager'90]

All of them are Randomized Algorithms

A natural *Algorithmic question*, Can we derandomize this?

Equivalence of PIT and Polynomial factorization

Polynomial Identity Testing(PIT)

Given $f \in \mathcal{C}$, determine whether $f \equiv 0$.

Equivalence of PIT and Polynomial factorization

Polynomial Identity Testing(PIT)

Given $f \in \mathcal{C}$, determine whether $f \equiv 0$.

KSS'14

Derandomizing PIT for VP $\iff$ Derandomizing Polynomial factorization for VP.

Equivalence of PIT and Polynomial factorization

Polynomial Identity Testing(PIT)

Given $f \in \mathcal{C}$, determine whether $f \equiv 0$.

KSS'14

Derandomizing PIT for VP $\iff$ Derandomizing Polynomial factorization for VP.

What about models we already knew PIT about? In particular, Sparse polynomials [Klivans-Spielman'01].

Vague overview of [KSS'14]

All mentioned [von zur Gathen-Kaltofen'85, Kaltofen'87, Kaltofen'89, Kaltofen-Trager'90] need randomness at multiple stages.

Randomized Factoring Algorithm:-

1. Step 1 requires randomness r_1
2. Step 2 requires randomness r_2
3. Step 3 requires randomness r_3

Vague overview of [KSS'14]

All mentioned [von zur Gathen-Kaltofen'85, Kaltofen'87, Kaltofen'89, Kaltofen-Trager'90] need randomness at multiple stages.

[KSS'14] Factoring Algorithm:-

1. Step 1 requires ~~randomness r_1~~ PIT for polynomial $p_1(x)$
2. Step 2 requires ~~randomness r_2~~ PIT for polynomial $p_2(x)$
3. Step 3 requires ~~randomness r_3~~ PIT for polynomial $p_3(x)$

Our Results

Main Theorem

There exists a deterministic algorithm that given a polynomial $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ of sparsity s and individual degrees at most d, computes the complete factorization of f, using $s^{\mathcal{O}(d^7 \log n)} \cdot \mathrm{poly}(d, |\mathbb{F}|)$ field operations.

Our Results

Main Theorem

There exists a deterministic algorithm that given a polynomial $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ of sparsity s and individual degrees at most d, computes the complete factorization of f, using $s^{\mathcal{O}(d^7 \log n)} \cdot \mathrm{poly}(d, |\mathbb{F}|)$ field operations.

Remark: If one could improve the sparsity bound from *quasi-polynomial* to *polynomial* then this will directly improve the run time of our deterministic factoring algorithm.

Factoring

Generic Factoring Algorithm

- Preprocessing
- Hilbert Irreducibility Theorem
- GCD (Solving System of Equations)

Factoring

Generic Factoring Algorithm

- Preprocessing
- Hilbert Irreducibility Theorem
- GCD (Solving System of Equations)

Our Approach

- Preprocessing
- "Brute force" for Hilbert Irreducibility
- Reconstructing the factors
- Test the factorization.

- For simplicity (and WLOG.),

$$f = x_1^d + f' \qquad\qquad \text{(f is monic in } x_1\text{)}$$

. (where highest degree of f' in x_1 is less than d)

- For simplicity (and WLOG.),

$$f = x_1^d + f' \qquad \text{(f is monic in } x_1\text{)}$$

. (where highest degree of f' in x_1 is less than d)

- Notice, factorization of f looks like

$$f = (x_1^{e_1} + g_1) \cdots (x_1^{e_k} + g_k)$$

- Consequently, f has at most d factors (total).

Projection to few variables

Randomized World

$$
\begin{array}{l}
f = g_1 g_2 \cdots g_5 \in \mathbb{F}[x_1, x_2, \ldots, x_n] \\
\quad \Big\downarrow \text{Hilbert Irrreducibility} \\
\quad \tilde{f} = \tilde{g_1} \tilde{g_2} \cdots \tilde{g_5} \in \mathbb{F}[x_1, y]
\end{array}
$$

Projection to few variables

Randomized World

$$f = g_1 g_2 \cdots g_5 \in \mathbb{F}[x_1, x_2, \ldots, x_n]$$

$$\Big\downarrow \text{Hilbert Irrreducibility}$$

$$\tilde{f} = \tilde{g_1}\tilde{g_2} \cdots \tilde{g_5} \in \mathbb{F}[x_1, y]$$

Deterministic World

$$f = g_1 g_2 \cdots g_5 \in \mathbb{F}[x_1, x_2, \ldots, x_n]$$

$$\Big\downarrow ??$$

$$\tilde{f} = \tilde{g_1}\tilde{g_2} \cdots \tilde{g_{20}} \in \mathbb{F}[x_1, y]$$

Projection to few variables

Randomized World

$$f = g_1 g_2 \cdots g_5 \in \mathbb{F}[x_1, x_2, \ldots, x_n]$$

$$\Big\downarrow \text{Hilbert Irrreducibility}$$

$$\tilde{f} = \tilde{g_1}\tilde{g_2} \cdots \tilde{g_5} \in \mathbb{F}[x_1, y]$$

Deterministic World

$$f = g_1 g_2 \cdots g_5 \in \mathbb{F}[x_1, x_2, \ldots, x_n]$$

$$\Big\downarrow ??$$

$$\tilde{f} = \tilde{g_1}\tilde{g_2} \cdots \tilde{g_{20}} \in \mathbb{F}[x_1, y]$$

Brute force the factorization "pattern"!!

Projection to few variables

Randomized World

$$f = g_1 g_2 \cdots g_5 \in \mathbb{F}[x_1, x_2, \ldots, x_n]$$

$$\Big\downarrow \text{Hilbert Irrreducibility}$$

$$\tilde{f} = \tilde{g_1}\tilde{g_2} \cdots \tilde{g_5} \in \mathbb{F}[x_1, y]$$

Deterministic World

$$f = g_1 g_2 \cdots g_5 \in \mathbb{F}[x_1, x_2, \ldots, x_n]$$

$$\Big\downarrow ??$$

$$\tilde{f} = \tilde{g_1}\tilde{g_2} \cdots \tilde{g_{20}} \in \mathbb{F}[x_1, y]$$

Brute force the factorization "pattern"!!

Q. How do we know which "pattern" is correct?

Projection to few variables

Randomized World

$$f = g_1 g_2 \cdots g_5 \in \mathbb{F}[x_1, x_2, \ldots, x_n]$$

$$\Big\downarrow \text{Hilbert Irrreducibility}$$

$$\tilde{f} = \tilde{g_1}\tilde{g_2} \cdots \tilde{g_5} \in \mathbb{F}[x_1, y]$$

Deterministic World

$$f = g_1 g_2 \cdots g_5 \in \mathbb{F}[x_1, x_2, \ldots, x_n]$$

$$\Big\downarrow ??$$

$$\tilde{f} = \tilde{g_1}\tilde{g_2} \cdots \tilde{g_{20}} \in \mathbb{F}[x_1, y]$$

Brute force the factorization "pattern"!!

Q. How do we know which "pattern" is correct?

A. We don't need to! We can test our factorization.

Black-box trick [Kaltofen-Trager'90]

How can one evaluate the factors?
Suppose you want to evaluate your factor at $(\alpha, \bar{\beta})$. Notice,

$$h(x, t) := f(x, \bar{b} + (\bar{\beta} - \bar{b})t)$$

Factorize $h(x, t)$ and substitute $x = \alpha, t = 1$.

Lemma (Klivans-Spielman'01)

Given an oracle access to an s-sparse polynomial $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ of degree d, we can deterministically reconstruct f in $\mathrm{poly}(n, s, d, \log|\mathbb{F}|)$ time.

Lemma (Klivans-Spielman'01)

Given an oracle access to an s-sparse polynomial $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ *of degree* d*, we can deterministically reconstruct* f *in* $\mathrm{poly}(n, s, d, \log|\mathbb{F}|)$ *time.*

Remaining steps:-

- Reconstruct the factors.
- Test the factorization.

This concludes our factoring algorithm.

Summary

Theorem (Sparsity Bound)

Let $\mathbb{F}$ be an arbitrary field and let $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ be a polynomial of sparsity s and individual degrees at most d, then the sparsity of every factor of f is bounded by $s^{\mathcal{O}(d^2 \log n)}$.

Summary

Theorem (Sparsity Bound)

Let $\mathbb{F}$ be an arbitrary field and let $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ be a polynomial of sparsity s and individual degrees at most d, then the sparsity of every factor of f is bounded by $s^{\mathcal{O}(d^2 \log n)}$.

Theorem (Deterministic factoring Algorithm)

Given a polynomial $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ of sparsity s and individual degrees at most d, we can computes the factorization of f, using $s^{\mathcal{O}(d^7 \log n)} \cdot \mathrm{poly}(d, |\mathbb{F}|)$ field operations deterministically.

Open Problems

1. Improving the sparsity bound?

Open Problems

1. Improving the sparsity bound? making it field specific?

Open Problems

1. Improving the sparsity bound? making it field specific?
2. Factoring Algorithm without the individual degree bound?

Open Problems

1. Improving the sparsity bound? making it field specific?
2. Factoring Algorithm without the individual degree bound?
3. Are ROABPs with bounded individual degree closed under factoring?

Thank you.