Challenges In and Around Sparse Polynomial Factorization

Amir Shpilka

Tel Aviv University

WACT 2025

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Disclaimer

- (Biased) selection of results and open questions
- Focused on factorization and complexity of factors
- Both univariate and multivariate polynomials
  (different notions of sparsity)
- Restricted domains: $\mathbb{Z}$ for Univariate, $\mathbb{C}$ for multivariate
  (many results relevant for other domains as well)
- No proofs, just (many) sketches
- Many open problems

Overview

Sparse Polynomials

Sparse Polynomials

- Polynomials with few monomials (compared to dimension of space)
  $\|f\|_0$ denotes number of monomials in f

Two very different settings:

- Univariate: $f \in \mathbb{Z}[x]$, $\deg(f) = \exp(n)$, $\|f\|_0 = \mathrm{poly}(n)$
  - Example: $f(x) = x^{2^n} - 1$
- Multivariate: n-variate $f \in \mathbb{C}[\mathbf{x}]$, $\deg(f) = \mathrm{poly}(n)$, $\|f\|_0 = \mathrm{poly}(n)$
  - Example: $f(\mathbf{x}) = \prod_{i=1}^{n} x_i + \prod_{i=n+1}^{2n} x_i$
  - In General: Polynomial computed by poly-size $\Sigma\Pi$ circuits

Motivation

- Practical importance: used by computer algebra systems and libraries (Maple, Mathematica, Sage, and Singular)
- Simple model for studying basic questions
- Many open problems

Key Problems

- Decision Problems:
  - Divisibility testing: does g divide f?
  - Factors: does f have a low degree factor?
- Algorithmic:
  - Find irreducible factors of f
  - Find a sparse/low-degree factor of f
- Complexity of factors:
  - Sparsity of factors
  - ℓ_∞ norm of factors
- Related Problems:
  - Behavior of complexity measures under products

Divisibility Testing

Divisibility Testing

Task:

- Given sparse polynomials g, f, decide whether g divides f?

Different complexity for Univariate and Multivariate

- Univariate: No known algorithms; hardness result for similar problems
  Can't use simple division: co-factor may have $\|f/g\|_0 = \exp(n)$

$$x^{2^n} - 1 = (x-1) \cdot \left(1 + x + \ldots + x^{2^n - 1}\right)$$

- Multivariate: Kaltofen's factoring algorithm [Kal89] + randomize polynomial identity testing (PIT). No deterministic algorithm.

Divisibility Testing:

Univariate Polynomials

Related NP Hardness Results

Theorem ([Pla77, Pla84])

The following are NP-hard problems:

- *Do sparse $f_1, \ldots, f_n$ have a common zero?*
- *Determine whether $x^N - 1$ does not divide $\prod_n f_i$ for sparse f_i*
- *Does a sparse f have a zero on the complex unit circle?*

Proof sketch - Reduction from 3SAT:

- Let $N = q_1 \cdots q_n$ product of first n primes.
- Assignment are roots of unity ω: $x_j(\omega) = \text{True iff } \omega^{N/q_j} = 1$
- Clauses $C_1, \ldots, C_m$ encoded as sparse polynomials with small coefficients such that: $f_i(w) = 0$ iff $w \models C_i$
- A common root to all polynomials is a satisfying assignment □

Positive Results (over $\mathbb{Z}$)

Theorem ([GKO92])

Sparse polynomials divisibility testing in coNP (assuming ERH)

Proof sketch:

- By ERH: if $g \nmid f$ then, $\exists$ prime $p = \exp(n)$, $\alpha \in \mathbb{F}_p$, $m < \|g\|_0$ such that $(x-\alpha)^m \mid g$ but $(x-\alpha)^m \nmid f$ □

Theorem ([Len99])

Can compute all irreducible degree-d factors in time poly(n, d)

Proof sketch:

- If $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ and α not a root of unity, then $\|\tilde{\alpha}\| = \Omega_d(1)$
- If $f(\tilde{\alpha}) = 0$ then, $f = f_{low} + x^r \cdot f_{high}$ where $f_{low}(\tilde{\alpha}), f_{high}(\tilde{\alpha}) = 0$ □

Open Problems

Challenge of [DC09]:

Either

- Find a class of problems for which divisibility testing is coNP-complete; or
- find a polynomial-time algorithm for divisibility testing; or,
- find a polynomial-time algorithm for divisibility testing of cyclotomic-free polynomials

Open:

- Prove hardness results not using cyclotomic polynomials

Divisibility Testing:

Multivariate Polynomials

Algorithms for Divisibility Testing

Randomized algorithm:

- Run [Kal89] randomized factorization algorithm
- Check if g is one of the factors using PIT for sparse polynomials

Theorem (Deterministic low degree divisibility testing [For15])

Quasi-poly time divisibility testing algorithm when $\deg(g) = O(1)$

Proof sketch:

- If $h = f/g$ and $g(0) = 1$, then $h = \mathrm{H}_{\leq \deg h}[f \cdot \sum_i (1-g)^i]$
- Multiplying by g, reduces to PIT of $f - \sum m_i \cdot g^{e_i}$, for monomials m_i
- By considering shifted partial derivatives, for an appropriate translation of $\mathbf{x}$, polynomial has a low-support monomial □

Open Problems

- Sub-exp* := faster than PIT for bounded-depth circuits [LST24]
- Sub-exp* time deterministic divisibility testing for sparse g, f
  - If $\deg(g) = O(1)$ then quasi-poly algorithm [For15]
- Polynomial time deterministic divisibility testing of sparse by quadratic
  - For $\deg(g) = 1$ can test using the PIT of [RS05]
  - If $\deg_i(f) \leq d$ and $\deg(g) = 2$ then can test divisibility in time $\text{poly}(\|f\|_0, n^d)$ using PIT for sparse polynomials a-la [For15]
- Sub-exp* time deterministic irreducibility testing of sparse polynomials
  - Even with bounded-individual degrees ≥ 3 ([Vol17] solved the case of ind-deg $= 2$)

Complexity of Factors:

Univariate Polynomials

Factors of Sparse Univariate polynomials

Examples:

- $x^N - 1 = (x-1)\cdot(1 + x + x^2 + \ldots + x^{N-1})$
- $x^N - 1$ has exponentially hard factors (counting arguments)
- $\Phi_N \mid x^N - 1$, Nth-cyclotomic polynomial. For infinitely many N:

$$\log \|\Phi_N\|_\infty \geq N^{\Omega(1/\log\log N)}$$

Take away:

- Factors may have exponential many monomials (unavoidable)
- Factors may have exponential complexity
- ℓ_∞ norm of factors doubly exponentially large

Question:

- Complexity of factors for cyclotomic-free f ?
- If g is sparse, can we obtain better upper bound on $\|f/g\|_\infty$?

Height of the Cofactor Polynomial

Theorem (Gel'fond's Lemma[Gel60])

$$\|f/g\|_\infty \leq 2^{\deg f} \|f\|_\infty$$

Theorem (Mignotte's Bound [Mig74])

$$\|f/g\|_1 \leq 2^{\deg f/g} \|f\|_2$$

Bound is tight up to basis of exponent (but examples not sparse)

Theorem ([NS24])

$$\|f/g\|_2 \leq \|f\|_1 \cdot (\deg f)^{O(\|g\|_0)}$$

Open problem:

- Prove tight bound for sparse polynomials

Norm of Cofactors

Theorem ([NS24])

$$\|f/g\|_2 \le \|f\|_1 \cdot (\deg f)^{O(\|g\|_0)}$$

Proof sketch:

- Fourier: $\exists \deg(f) < p$-th root of unity θ s.t. $\|f/g\|_2 \le \|f\|_1 / |g(\theta)|$
- Claim: $\exists$ small $B(g) \subset \mathbb{D}$ such that $\forall \alpha \in \mathbb{D}$ far from B, $g(\alpha)$ "large"
- Density of primes: $\exists p \approx \deg f$ whose primitive roots far from $B(g)$ $\square$
- Pf. by induction: Base case $\|g\|_0 = 2$: holds for α far from roots of g
- Induction step: set $B(g) := Z(\mathrm{Re}(g')) \cup Z(\mathrm{Im}(g')) \cup B(g')$
- Signs of $R(g')$ and $\mathrm{Im}(g')$ fixed within intervals in $\mathbb{D} \setminus B(g)$
- As $\|g'\|_0 = \|g\|_0 - 1$, by induction: $g'(\alpha)$ large for α far from $B(g')$
- Simple calculus: $g(\alpha)$ large for α far from $B(g)$ $\square$

Complexity of Factors:

Multivariate Polynomials

Sparsity of Factors of Sparse Polynomials

Example [vzGK85]:

$$\prod_{i=1}^{n}(x_i^n - 1) = \left(\prod_{i=1}^{n}(x_i - 1)\right) \cdot \left(\prod_{i=1}^{n}(1 + x_i + x^2 + \ldots + x_i^{n-1})\right)$$

LHS has sparsity $s = 2^n$, RHS has sparsity $n^n = s^{\log s}$

Open Problems:

- Can the sparsity of a factor exceed $s^{O(\log s)}$?
- What is the sparsity of f/g when $\deg(g) = 2$?
- Bounded depth circuit complexity of factors?

Complexity of Factors

Known results:

- [Kal89] proved factors have small algebraic circuits
- Moreover, if $\deg_i(f) = O(1)$ (or $\deg(g) = \log^a n$), then depth $= 5$ (or depth $= 2 + a$) [DSY10, Oli16, CKS19]
- If $\deg_i(f) \leq d$ then factors $s^{O(d^2 \log n)}$ sparse factors (and deterministic factorization) [BSV20]
  - If also symmetric then $(sn)^{\mathrm{poly}(d)}$ time [BS22]
- Deterministic quasi-poly (sub-exp) algorithm computing a list of polynomials (circuits with ÷) that contains all bounded degree (all) factors (and some "junk") [KRS24, DST24], [KRSV24]

Note:

- Sub-exp bound on sparsity of factors only when $\deg_i(f) = O(1)$

Bounded individual degrees

Theorem ([BSV20])

If $\deg_i(f) \le d$ *then factors are* $s^{O(d^2 \log n)}$ *sparse*

Proof sketch:

- If $f = gh$ then $\text{Newton}(f) = \text{Newton}(g) + \text{Newton}(h)$ (Newton polytope = convex hull of exponent vectors)
- $\|f\|_0$ small $\Rightarrow$ Newton(f) has few vertices, hence also Newton(g)
- $\deg_i(g) = O(1) \Rightarrow$ bound on ℓ_∞ of integral points in Newton(g)
- Claim: This implies that Newton(g) has few integral points □
- Proof: by Chernoff, sampling $O(d^2 \log n)$ vertices from convex combination, gives unique approximation to each inner integral point
- Count number of possible approximations □

Bounded Degree Factors

Theorem ([KRS24, DST24])

Can compute all $O(1)$-degree factors in quasi-polynomial time

Proof sketch (of [DST24]):

- Effective Hilbert Irreducibility: $\exists \varphi(\boldsymbol{s}, \boldsymbol{t})$, $\deg(\varphi) = d^5$, such that $\varphi(\boldsymbol{\alpha}, \boldsymbol{\beta}) \neq 0 \Rightarrow g(z, u \cdot \boldsymbol{\alpha} + \boldsymbol{\beta})$ is irreducible, for every $\deg(g) = d$ irreducible factor of f
- Find small number of weight functions $\{\boldsymbol{\omega}^{(i)} \in \mathbb{N}^n\}$ such that
  - $\{(y^{\boldsymbol{\omega}^{(i)}}, y^{\boldsymbol{\omega}^{(j)}})\}$ hitting set for φ
  - degree d factor g reconstructible from $g(z, u \cdot y^{\boldsymbol{\omega}_i} + y^{\boldsymbol{\omega}_j})$
  - different degree d factors remain coprime under substitution
- Factor $f(z, u \cdot y^{\boldsymbol{\omega}_i} + y^{\boldsymbol{\omega}_j})$
- Reconstruct degree d factors and verify using PIT □

Beck to the Example

Question: can we improve the example:

$$\prod_{i=1}^{n}(x_i^n - 1) = \left(\prod_{i=1}^{n}(x_i - 1)\right) \cdot \left(\prod_{i=1}^{n}(1 + x_i + x^2 + \ldots + x_i^{n-1})\right)$$

Theorem ([BS17] (unpublished, M.Sc. thesis))

$f = (\prod_{i=1}^{k} \ell_i) \cdot g$, ℓ_i *linear with* $\|\ell_i\|_0 \geq 2 \Rightarrow r := \dim(\{\ell_i\}) = \tilde{O}(\log \|f\|_0)$

$\Rightarrow$ *No significantly better example with many independent linear factors*

Proof sketch.

- If $\exists$ set of variables $|J| = \tilde{O}(\log r)$ such that $f|_{J \leftarrow 0} = 0$, then, setting $|J| - 1$ of them to zero we get $\|f\|_0 \to \|f\|_0 / |J|$ and $r \to r - |J|$
- Otherwise, set variables to zero (carefully) with probability $\approx 1/\log r$ w.h.p. rank remains large, monomial support drops dimension of partial derivatives $\Rightarrow \|f\|_0 = \exp(O(r))$ □

Obstacles for Higher Degrees

Proof relied on partial derivative method: $\dim\left(\partial\left(\prod_{i=1}^{n} x_i\right)\right) = 2^n$

Questions:

1. Assume $g_1, \ldots, g_n$ algebraically independent polynomials does $\dim\left(\partial\left(\prod_{i=1}^{n} g_i\right)\right) = \exp(n)$?
2. How small can $\dim(\partial(g_1 \cdot g_2))$ be compared to $\dim(\partial(g_1)) + \dim(\partial(g_2))$?
3. Assume $g_1, \ldots, g_n$ algebraically independent polynomials does $\prod_{i=1}^{n} g_i$ contain a monomial with $\Omega(n)$ many variables?
4. If g_1 has a monomial with t different variables, how small can the maximal support of a monomial in $g_1 \cdot g_2$ be?
    - Example: $(x^2 + xy + y^2)(x - y) = x^3 - y^3$

More Problems

Questions

U: Bound sparsity of non-cyclotomic factors of univariate sparse polys

U: Lower bound $\|f^2\|_0$ in terms of $\|f\|_0$ [SZ09, CD91]:

$$\forall.\ \Omega(\log \|f\|_0) \leq \|f^2\|_0 \leq \exists.\ (\|f\|_0)^{12/13}$$

M: Find all sparse factors of a sparse f in deterministic subexp* time
* Faster than PIT for bounded depth circuits

- Find bounded ind-deg sparse factors in quasi-poly time [DST24]
- Find a multilinear factors of a sparse polynomial in deterministic polynomial time [Vol15]

M: Polynomial time factorization of $f = \prod_{i=1}^{m} g_i^{e_i}$ for sparse g_i
Open even if $m = 2$ or if g_i are of bounded degree [DST24]

M: What is the bounded depth complexity of factors? $\deg_i(f) = O(1)$, or small degree factors $\Rightarrow$ depth is $= O(1)$ [D**S**Y10, Oli16, CKS19]

References I

- T. Binkovich and A. Shpilka, *The rank of linear factors of sparse polynomials*, 2017.
- P. Bisht and N. Saxena, *Derandomization via symmetric polytopes: Poly-time factorization of certain sparse polynomials*, 2022
- V. Bhargava, S. Saraf, and I. Volkovich, *Deterministic factorization of sparse polynomials with bounded individual degree*, 2020
- C. Chou, M. Kumar, and N. Solomon, *Closure results for polynomial factorization*, 2019
- D. Coppersmith and J, Davenport, *Polynomials whose powers are sparse* 1991
- J. Davenport and J. Carette, *The sparsity challenges*, 2009

References II

- P. Dutta, A. Sinhababu, and T. Thierauf, *Derandomizing multivariate polynomial factoring for low degree factors*, 2024
- Z. Dvir, A. Shpilka, and A. Yehudayoff, *Hardness-randomness tradeoffs for bounded depth arithmetic circuits*, 2009
- M. A. Forbes, *Deterministic divisibility testing via shifted partial derivatives*, 2015
- J. v. z. Gathen and E. L. Kaltofen, *Factoring Sparse Multivariate Polynomials*, 1985
- A. O. Gel'fond, *Transcendental and algebraic numbers*, 1960
- D. Y. Grigoriev, M. Karpinski, and A. M. Odlyzko, *Existence of short proofs for nondivisibility of sparse polynomials under the extended Riemann hypothesis*, 1992

References III

- E. Kaltofen, *Factorization of polynomials given by straight-line programs*, 1989.
- M. Kumar, V. Ramanathan, and R. Saptharishi, *Deterministic algorithms for low degree factors of constant depth circuits*, 2024
- M. Kumar, V. Ramanathan, R. Saptharishi, and B. Volk, *Towards deterministic algorithms for constant-depth factors of constant-depth circuits*, 2024.
- H. W. Lenstra, *Finding small degree factors of lacunary polynomials*, 1999.
- N. Limaye and S. Srinivasan and S. Tavenas, *Superpolynomial lower bounds against low-depth algebraic circuits*, 2024
- M. Mignotte, *An inequality about factors of polynomials*, 1974

References IV

- I. Nahshon and A. Shpilka, *New bounds on quotient polynomials with applications to exact division and divisibility testing of sparse polynomials*, 2024
- R. Oliveira, *Factors of low individual degree polynomials*, 2016
- D. A. Plaisted, *Sparse complex polynomials and polynomial reducibility*, 1977
- ———, *New NP-hard and NP-complete polynomial and integer divisibility problems*, 1984
- R. Raz and A. Shpilka, *Deterministic polynomial identity testing in non-commutative models*, 2005
- A. Schinzel and U. Zannier, *On the number of terms of a power of a polynomial*, 2009

References V

- I. Volkovich, *Deterministically factoring sparse polynomials into multilinear factors and sums of univariate polynomials*, 2015
- ______, *On some computations on sparse polynomials*, 2017