Polynomial Identity Testing

Amir Shpilka

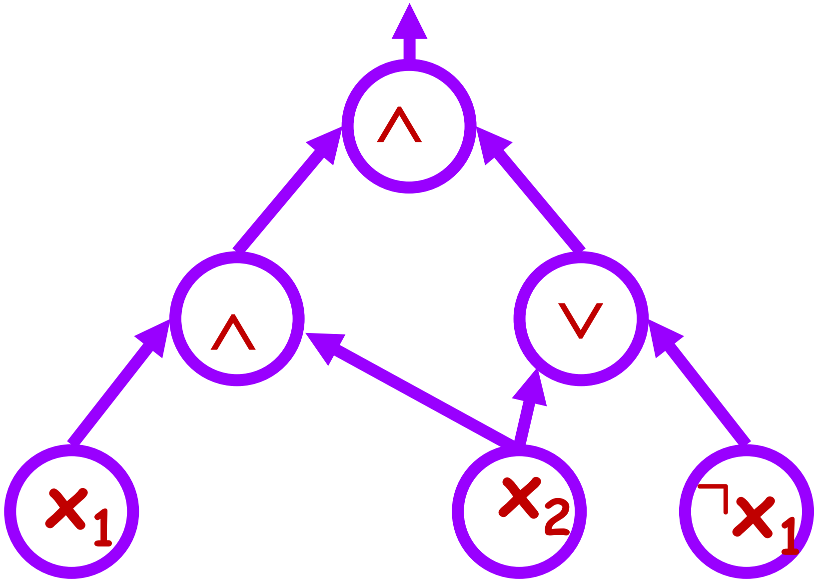
Technion

Goal of talk

- Model: Arithmetic circuits
- Problem: Polynomial Identity Testing
- Example: Depth-3 circuits
- Some open problems

Boolean Complexity

- Holy grail: $\mathbb{P}$ vs. $\mathbb{NP}$
- In a nutshell: Show that certain problems (e.g., finding the minimum distance of a binary code given by its parity check matrix) cannot be decided by small Boolean circuits



Boolean Complexity

- Holy grail: $\mathbb{P}$ vs. $\mathbb{NP}$
- In a nutshell: Show that certain problems (e.g., finding the minimum distance of a binary code given by its parity check matrix) cannot be decided by small Boolean circuits
- Problem notoriously difficult – with minuscule advance
- Natural idea: consider more structured models

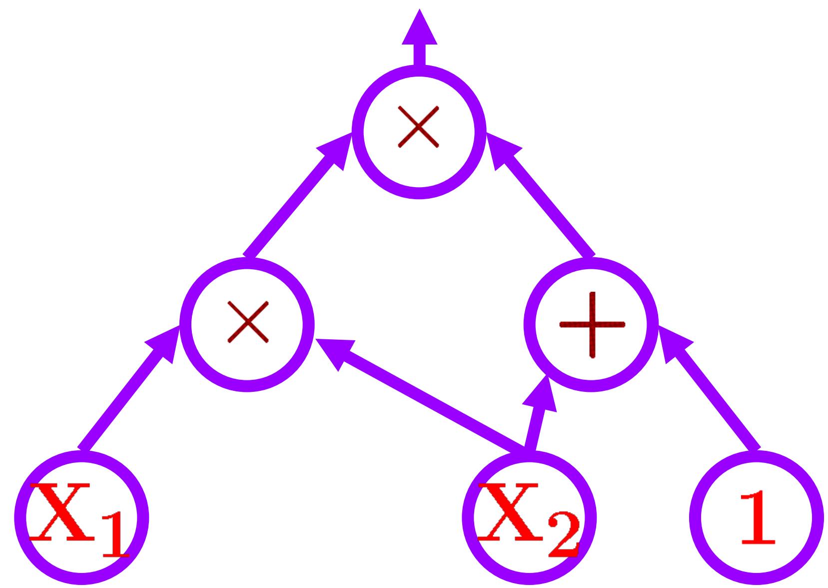
Playground: Arithmetic Circuits

Field: $\mathbb{F}$ (e.g., $\mathbb{F}_2$, $\mathbb{R}$)

Variables: $X_1,\ldots,X_n$

Gates: $+$, $\times$

Every gate in the circuit computes a polynomial in $\mathbb{F}[X_1,\ldots,X_n]$



Example: $(X_1 \cdot X_2) \cdot (X_2 + 1)$

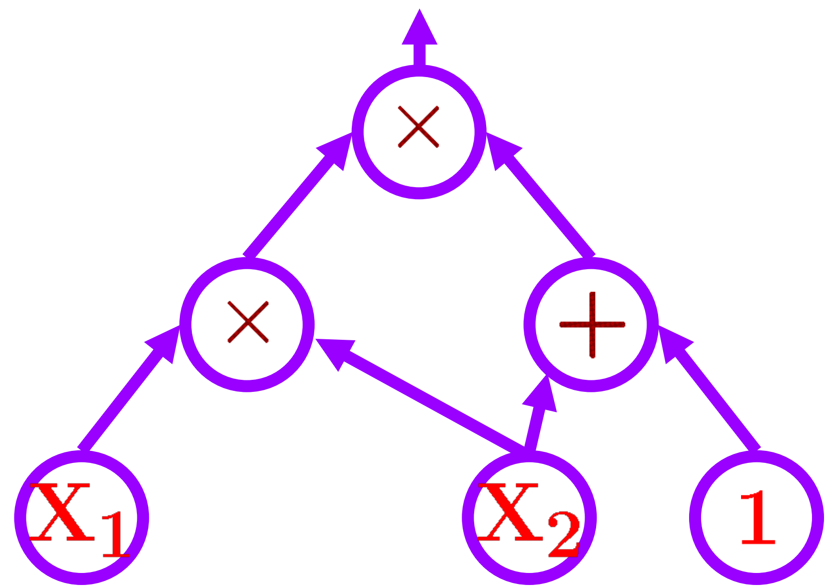
Size = number of wires

Depth = length of longest input-output path

Degree = max degree of internal gates

Playground: Arithmetic Circuits

In Example:
- ❑ Size = 6
- ❑ Depth = 2
- ❑ Degree = 3



Example: $(X_1 \cdot X_2) \cdot (X_2 + 1)$

Size = number of wires

Depth = length of longest input-output path

Degree = max degree of internal gates

Why Arithmetic Circuits?

- Structured model (compared to Boolean circuits) $\mathbb{P}$ vs. $\mathbb{NP}$ may be easier
- Most natural model for computing polynomials
- For many problems (e.g. Matrix Multiplication, Det) best algorithm is an arithmetic circuit
- Great algorithmic achievements:
  - Fourier Transform
  - Matrix Multiplication
  - Polynomial Factorization

Important Problems

- Design new algorithms:
  - Õ(n^2) for Matrix Multiplication?
  - Understanding $\mathbb{P}$
- Prove lower bounds:
  - Find a polynomial (e.g. Permanent) that requires super-polynomial size or super-logarithmic depth
  - **Analog of $\mathbb{P}$ vs. $\mathbb{NP}$**
- Derandomize Polynomial Identity Testing:
  - Understanding the power of randomness
  - Analog of $\mathbb{P}$ vs. $\mathbb{BPP}$

Exam(ple)

$\omega^n=1$. Is the following polynomial identically 0?

$$\prod_{i=1}^{n}\left(\omega^5\pi X+\left(\omega^5 e-\omega^i\hbar\right)Y-\omega^i\pi e Z\right)+$$
$$\prod_{i=1}^{n}\left(-e\omega^i X+\left(\pi\omega^i+\hbar\right)Y+(\pi e-\hbar\omega^i)Z\right)+$$
$$\prod_{i=1}^{n}\left((e\omega^2-\pi\omega^i)X-\left(\pi\omega^2+e\omega^i\right)Y+\hbar\omega^2 Z\right)$$

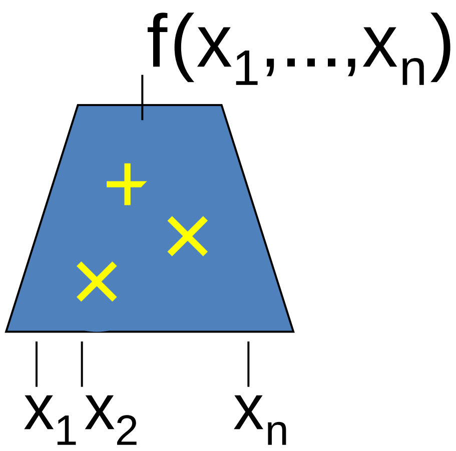
Prove it!

Will do so later.

Polynomial Identity Testing

Input: Arithmetic circuit computing f

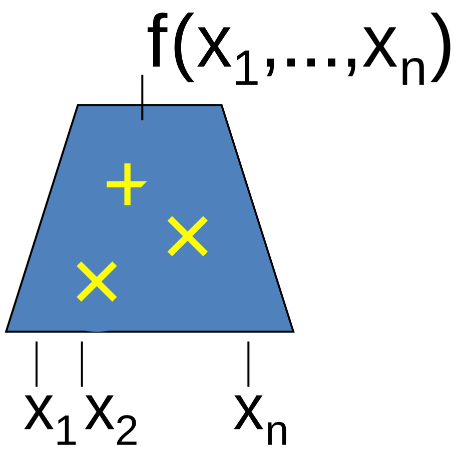
Problem: Is $f \equiv 0$?



Note: $x^2 - x$ is the zero function over $\mathbb{F}_2$ but not the zero polynomial!

Polynomial Identity Testing

Input: Arithmetic circuit computing f
Problem: Is $f \equiv 0$?



Randomized algorithm [Schwartz, Zippel, DeMillo-Lipton]: evaluate f at a random point

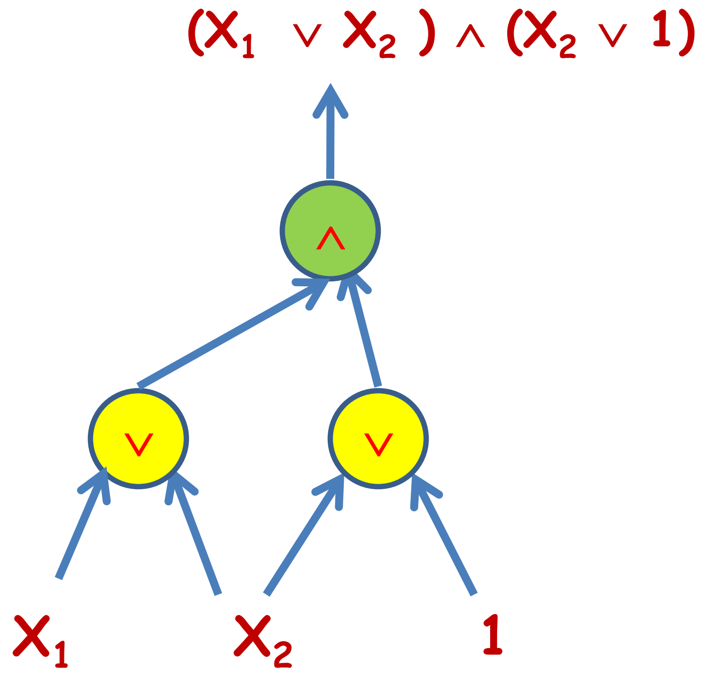
Goal: A proof. I.e., a deterministic algorithm

Analogy with SAT

Input: Boolean circuit

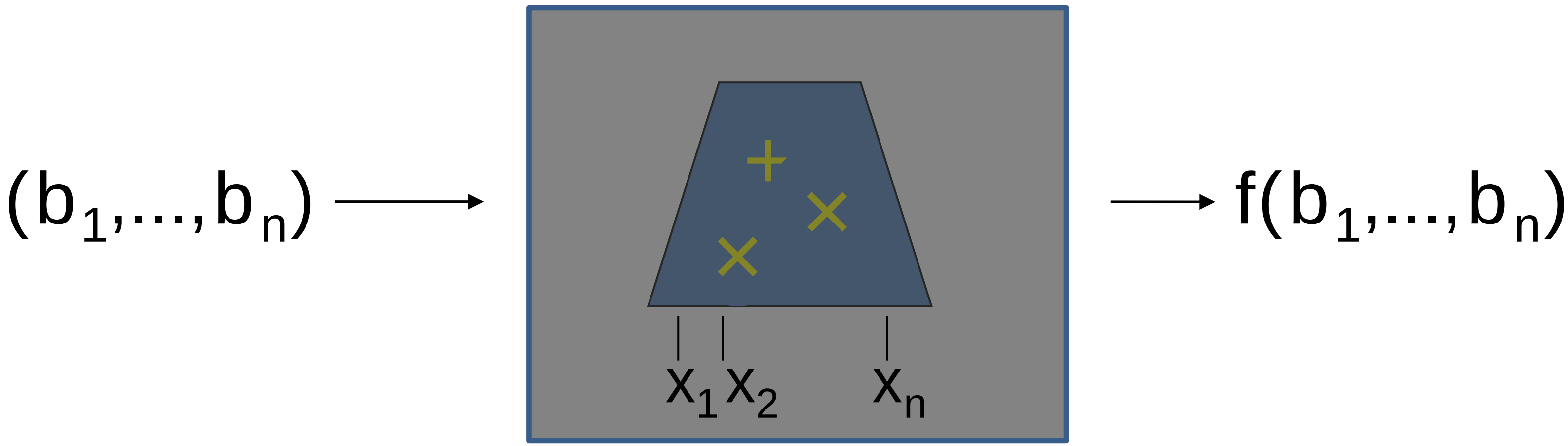
Decide: is C = 0?

Note: SAT does not have
randomized algorithms



Black Box PIT ≡ Explicit Hitting Set

Input: A Black-Box circuit computing f.



Problem: Is $f \equiv 0$?

S,Z,DM-L: Evaluate at a random point

Goal: deterministic algorithm (a.k.a. Hitting Set):

find *explicit* set **H**: **if $f \neq 0$, $\exists a \in H$ with $f(a) \neq 0$**

Motivation

- Natural and fundamental problem
- Strong connection to circuit lower bounds
- Algorithmic importance:
  - Primality testing [Agrawal-Kayal-Saxena]
  - Parallel algorithms for finding matching [Karp-Upfal-Wigderson, Mulmuley-Vazirani-Vazirani]
- May help you solve exams!

Talk Overview

- ✓ Definition of the problem
- Connection to lower bounds (hardness)
- Survey of positive results
- Some proofs
- Open problems

Hardness: PIT $\equiv$ lower bounds

[Heintz-Schnorr,Agrawal]:

Polynomial time Black-Box PIT $\Rightarrow$
Exponential lower bounds for arith. Circuits

[Kabanets-Impagliazzo]:

- Exponential lower bound for Permanent $\Rightarrow$
  Black-Box PIT in $n^{\mathrm{polylog}(n)}$ time
- Polynomial time White-Box PIT $\Rightarrow$
  (roughly) super-polynomial lower bounds.

[Dvir-S-Yehudayoff]: (almost) same as K-I for bounded depth circuits

Lesson: Derandomizing PIT essentially equivalent to proving lower bounds for arithmetic circuits

Black-Box PIT $\Rightarrow$ Lower Bounds

[Heintz-Schnorr,Agrawal]:

BB PIT for size s circuits in time poly(s)
(i.e. poly(s) size hitting set)
$\Rightarrow$ exp. lower bounds for arithmetic circuits.

Proof: Given $\mathcal{H}=\{p_i\}$, find non-zero polynomial f in $\log(|\mathcal{H}|)$ variables, such that $f(p_i)=0$ for all i.

$\Rightarrow$ f does not have size s circuits ■

Gives lower bounds for f in EXP (PSPACE)

Conjecture [Agrawal]:

$\mathcal{H}=\{(y_1,\ldots, y_n) : y_i=y^{k^i \bmod r}, k,r < s^{20}\}$ is a hitting set for size s circuits

A short digression

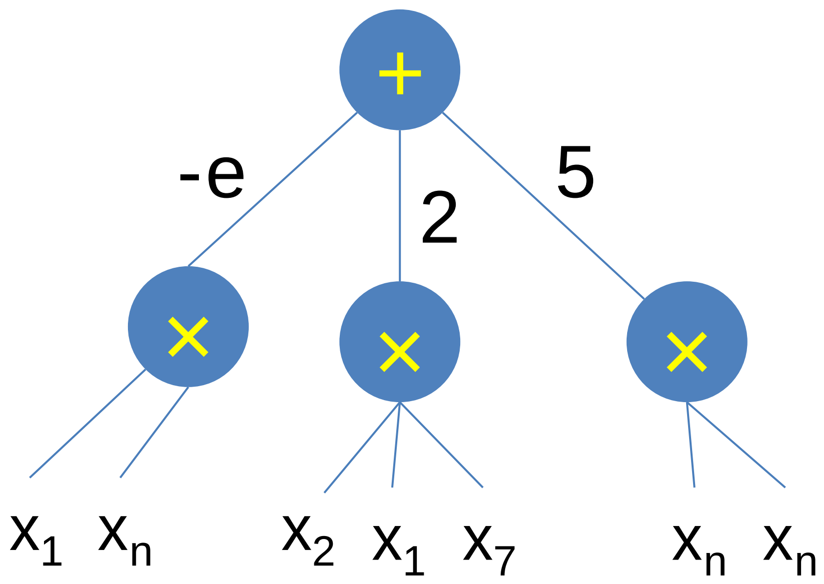
Bounded Depth Circuits

Bounded depth circuits: $\Sigma\Pi$

- $\Sigma\Pi$ circuits: depth-2 circuits with + at the top and × at the bottom. Size s circuits compute s-sparse polynomials.

Example:

$(-e)x_1 \cdot x_n + 2x_1 \cdot x_2 \cdot x_7 + 5(x_n)^2$

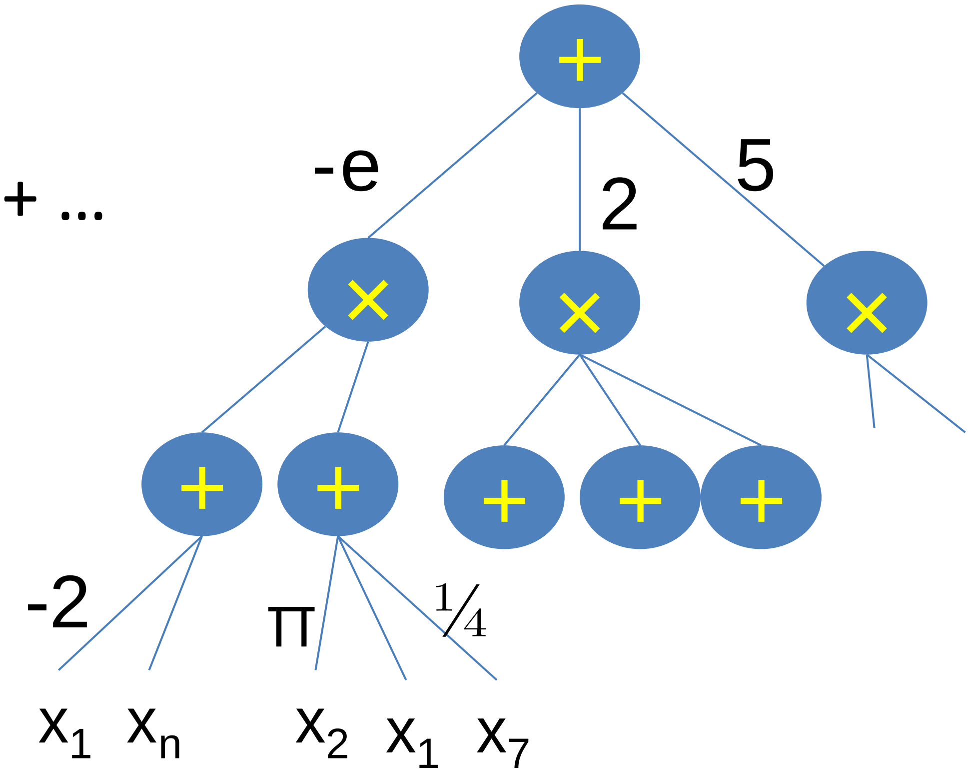


Bounded depth circuits: $\Sigma\Pi\Sigma$

- $\Sigma\Pi\Sigma$ circuits: + at the top, × at the middle and + at the bottom: computes sums of products of linear functions.

Example:

$(-e)\cdot(-2x_1+x_n)\cdot(x_1+\pi x_2+¼x_7) + \ldots$



Bounded depth circuits: $\Sigma\Pi\Sigma$

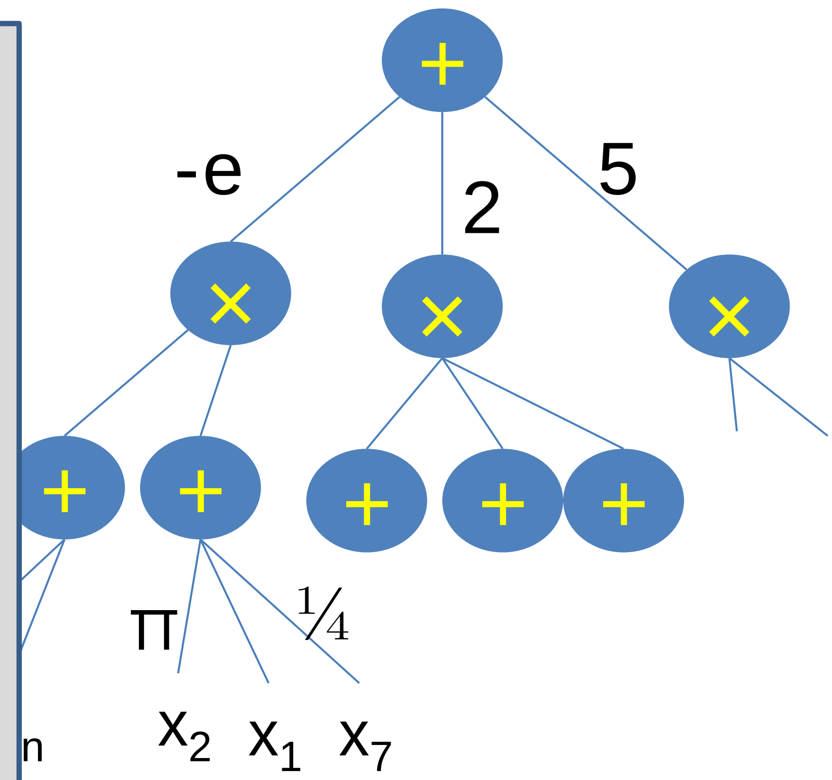
- $\Sigma\Pi\Sigma$ circuits: + at the top, × at the middle and + at the bottom: computes sums of products of linear functions.

Another Exam(ple):

$$\prod_{i=1}^{n}\left(\omega^{5}\pi X+\left(\omega^{5}e-\omega^{i}\hbar\right)Y-\omega^{i}\pi e Z\right)+$$

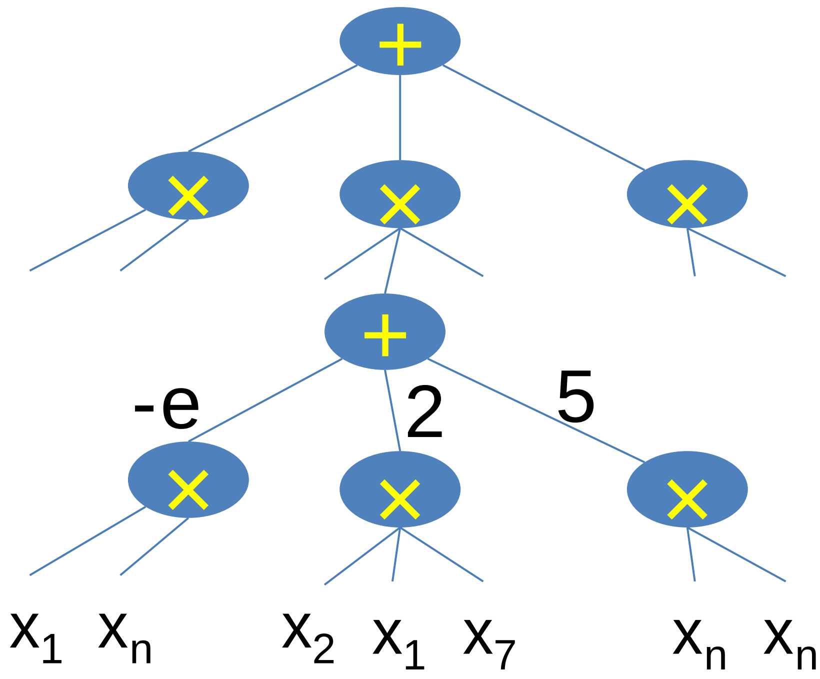
$$\prod_{i=1}^{n}\left(-e\omega^{i}X+\left(\pi\omega^{i}+\hbar\right)Y+(\pi e-\hbar\omega^{i})Z\right)+$$

$$\prod_{i=1}^{n}\left((e\omega^{2}-\pi\omega^{i})X-\left(\pi\omega^{2}+e\omega^{i}\right)Y+\hbar\omega^{2}Z\right)$$



Bounded depth circuits: $\Sigma\Pi\Sigma\Pi$

- $\Sigma\Pi\Sigma\Pi$ circuits: depth-4 circuits with + at the top, then ×, then + and another × at the bottom. Compute sums of products of sparse polynomials.



Back to Hardness-Randomness

Importance of $\Sigma\Pi\Sigma\Pi$ circuits

[Agrawal-Vinay,Raz]: Exponential lower bounds for $\Sigma\Pi\Sigma\Pi$ circuits imply exponential lower bounds for general circuits.

Cor [Agrawal-Vinay]: Polynomial time PIT of $\Sigma\Pi\Sigma\Pi$ circuits gives quasi-polynomial time PIT for general circuits.

Proof: By [Heintz-Schnorr,Agrawal] polynomial time PIT $\Rightarrow$ exponential lower bounds for $\Sigma\Pi\Sigma\Pi$ circuits. By [Agrawal-Vinay, Raz] $\Rightarrow$ exponential lower bounds for general circuits. Now use [Kabanets-Impagliazzo].

Importance of $\Sigma\Pi\Sigma\Pi$ circuits

[Agrawal-Vinay,Raz]: Exponential lower bounds for $\Sigma\Pi\Sigma\Pi$ circuits imply exponential lower bounds for general circuits.

Cor [Agrawal-Vinay]: Polynomial time PIT of $\Sigma\Pi\Sigma\Pi$ circuits gives quasi-polynomial time PIT for general circuits.

Lesson: Understanding small depth (i.e. depth 4) circuits is as important as the general case!

Talk Overview

- ✓ Definition of the problem
- ✓ Connection to lower bounds (hardness)
- Survey of positive results
- Some proofs
- Open problems

Deterministic algorithms for PIT

- $\Sigma\Pi$ circuits [BenOr-Tiwari, Grigoriev-Karpinski, Klivans-Spielman,…]
  - Black-Box in polynomial time
- Non-commutative formulas [Raz-S]
  - White-Box in polynomial time
- $\Sigma\Pi\Sigma(k)$ circuits [Dvir-S,Kayal-Saxena,Karnin-S,Kayal-Saraf,Saxena-Seshadri]
  - Black-Box in time $n^{O(k)}$
- Mult. $\Sigma\Pi\Sigma\Pi(k)$ [Karnin-Mukhopadhyay-S-Volkovich,Saraf-Volkovich]
  - Black-Box in time $n^{poly(k)}$
- Read-k multilinear formulas [S-Volkovich,Anderson-van Melkebeek-Volkovich]
  - White-Box in time $n^{k^{O(k)}}$
  - Black-Box in $n^{O(\log(n)+k^{O(k)})}$

Talk Overview

- ✓ Definition of the problem
- ✓ Connection to lower bounds (hardness)
- ✓ Survey of positive results
- Some proofs:
  - Depth-3 circuits
- Open problems

Solution to Exam ($\Sigma\Pi\Sigma$ circuit)

$\omega^n=1$. Is the following polynomial identically 0?

$$\prod_{i=1}^{n}\left(\omega^5\pi X+\left(\omega^5 e-\omega^i\hbar\right)Y-\omega^i\pi eZ\right)+$$
$$\prod_{i=1}^{n}\left(-e\omega^i X+\left(\pi\omega^i+\hbar\right)Y+(\pi e-\hbar\omega^i)Z\right)+$$
$$\prod_{i=1}^{n}\left((e\omega^2-\pi\omega^i)X-\left(\pi\omega^2+e\omega^i\right)Y+\hbar\omega^2 Z\right)$$

Prove it!

Will do so ~~later~~ now

Idea: change of basis

- $A = \pi \cdot X + e \cdot Y$
- $B = \hbar \cdot X + \pi \cdot e \cdot Z$
- $C = e \cdot X - \pi \cdot Y + \hbar \cdot Z$
- Identity becomes

$$\prod_{i=1}^{n}\left(A-\omega^{i}B\right)+\prod_{i=1}^{n}\left(B-\omega^{i}C\right)+\prod_{i=1}^{n}\left(C-\omega^{i}A\right)=$$

$$\left(A^{n}-B^{n}\right)+\left(B^{n}-C^{n}\right)+\left(C^{n}-A^{n}\right)=0$$

- But surely, this is not the general case. Right?

Depth 3 identities

- What is the structure of a zero circuit?
- If $M_1 + \ldots + M_k = 0$ then
  - Multiplying by a common factor:
    $\Pi x_i \cdot M_1 + \ldots + \Pi x_i \cdot M_k = 0$
  - Adding two identities:
    $(M_1 + \ldots + M_k) + (T_1 + \ldots + T_{k'}) = 0$
- How do the most basic identities look like?
- Basic: cannot be `broken’ to pieces (minimal) and no common linear factors (simple).

Depth 3 identities

- $C = M_1 + \ldots + M_k$ $\quad M_i = \Pi_{j=1\ldots d_i} L_{i,j}$
- Rank: dimension of space spanned by $\{L_{i,j}\}$
- In the exam: Rank=3
- Turns out: this is (almost) the general case!
- Theorem [Dvir S]: If $C \equiv 0$ is a basic identity then $\dim(C) \leq \mathrm{Rank}(k,d) = (\log(d))^k$
- White-Box Algorithm: find partition to sub-circuits of low dimension (after removal of g.c.d.) and brute force verify that they vanish.
- Improved $\mathbf{n}^{O(k)}$ algorithm by [Kayal-Saxena].
- Black-Box: Similar ideas…

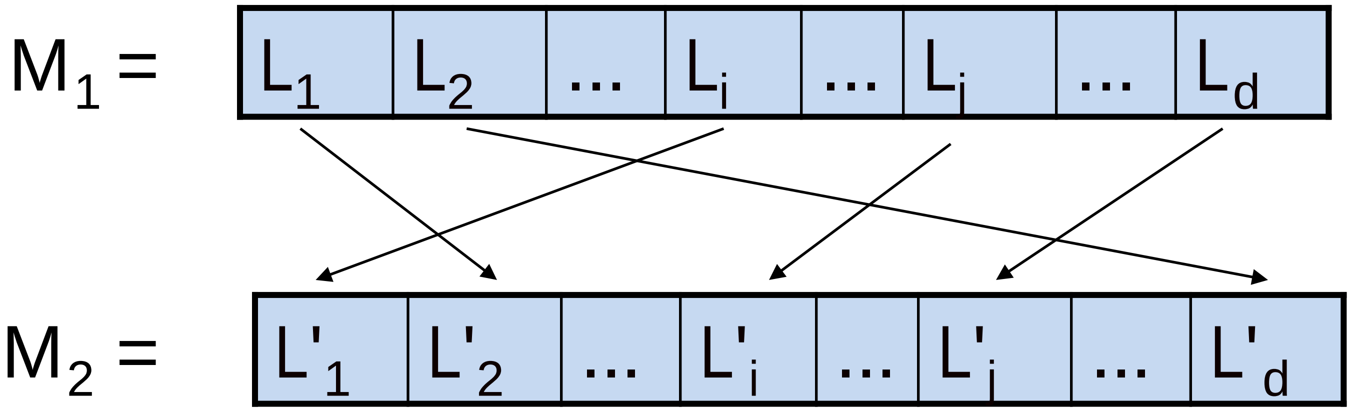
Depth 3 identities

- Lesson 1: depth 3 identities are very structured!
- Lesson 2: Rank is an important invariant to study.
- Improvements [Kayal-Saraf,Saxena-Seshadri]:
  - finite $\mathbb{F}$, $k \cdot \log(d) < \mathrm{Rank}(k,d) < k^3 \cdot \log(d)$
  - over $\mathbb{Q}$, $k < \mathrm{Rank}(k,d) < k^2 \cdot \log(k)$
- Improves [Dvir-S] + [Karnin-S] (plug and play)
- [Saxena-Seshadri] BB-PIT in time $n^{O(k)}$

Open problem: remove k from the exponent!

Bounding the rank

Basic observation: Consider $C = M_1 + M_2$



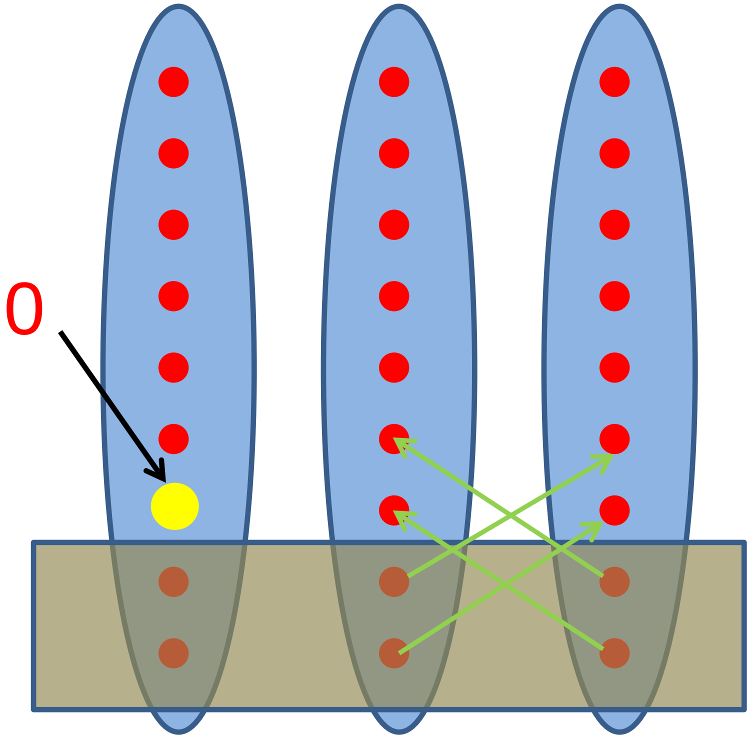
Fact: linear functions are irreducible polynomial.

Corollary: $C \equiv 0$ then M_1, M_2 have same factors.

Corollary: $\exists$ matching $i \rightarrow \pi(i)$ s.t. $L_i \sim L'_{\pi(i)}$

Bounding the rank

- Claim: Rank(3,d) = O(log(d))

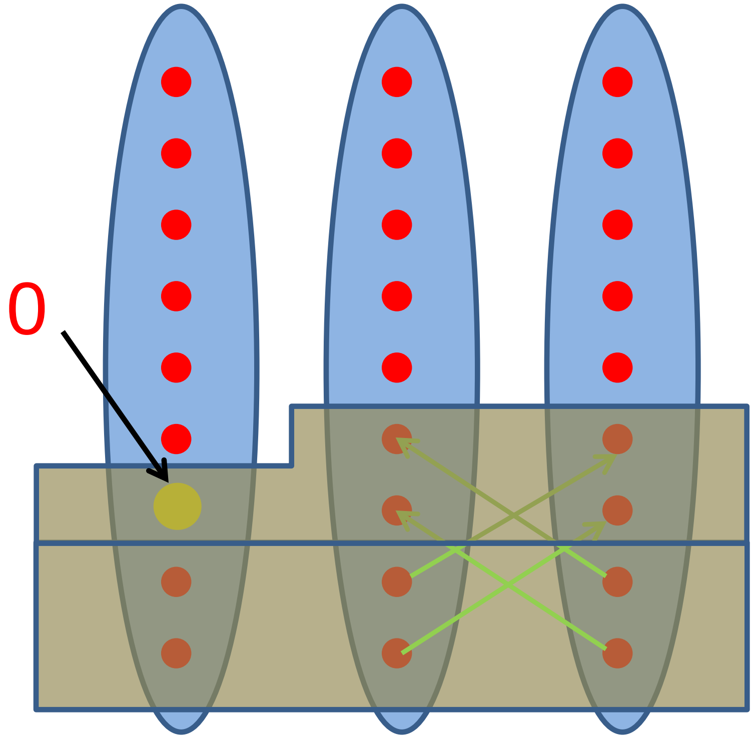


Sketch: cover all linear functions in log(d) steps, where at m'th step:

- dim of cover is O(m)
- $\Omega(2^m)$ functions in span

Bounding the rank

- Claim: Rank(3,d) = O(log(d))



Sketch: cover all linear functions in log(d) steps, where at m'th step:

- dim of cover is O(m)
- $\Omega(2^m)$ functions in span

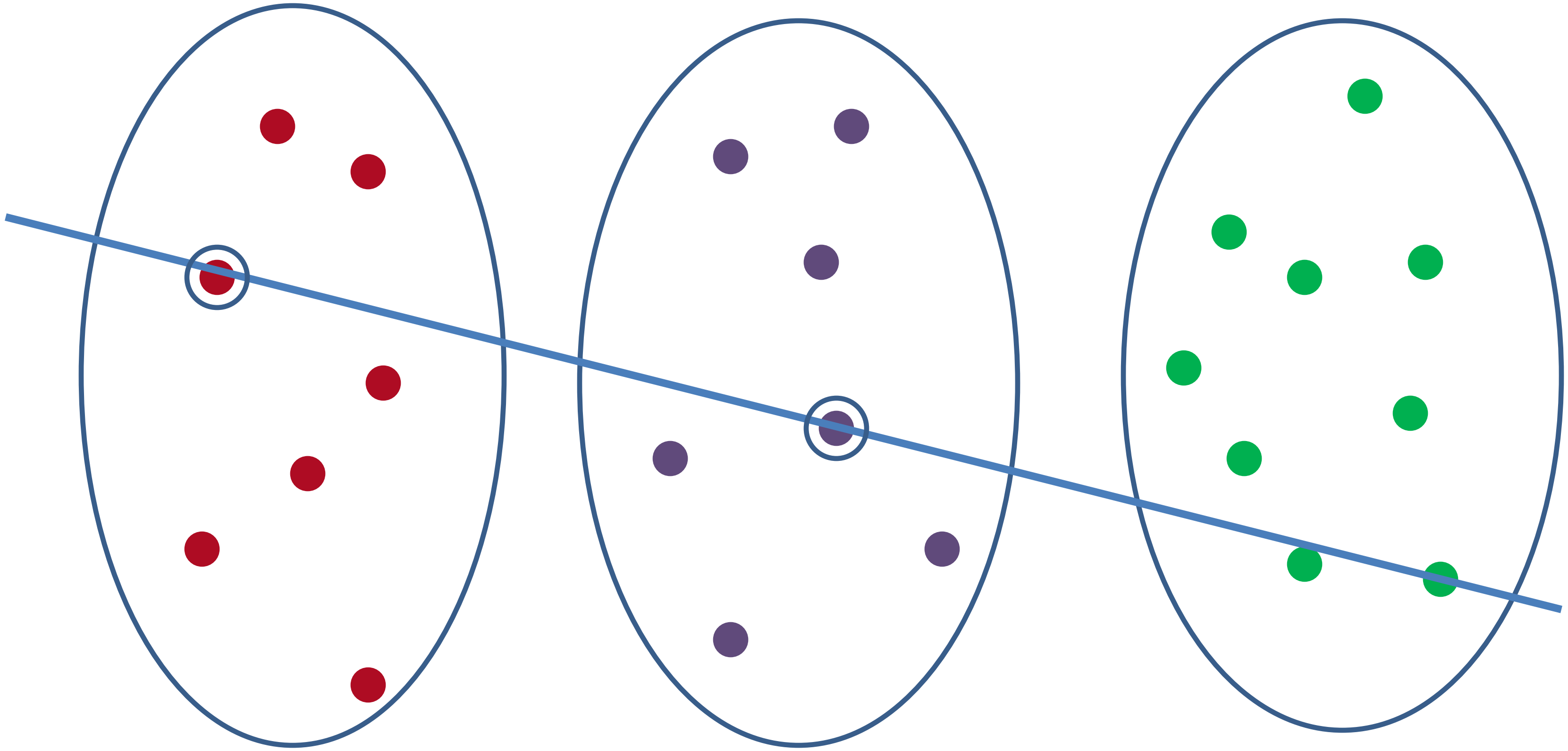
"Geometric interpretation of $M_1+M_2+M_3 = 0$"

- Lets map Linear forms to points in $\mathbb{R}^n$
- The map

$$a_1 x_1 + a_2 x_2 + \ldots + a_n x_n \mapsto (1, \frac{a_2}{a_1}, \ldots, \frac{a_n}{a_1})$$

- Say $L_1 \rightarrow P_1$ $L_2 \rightarrow P_2$ $L_3 \rightarrow P_3$
  - If $L_3 = \alpha L_1 + \beta L_2$ then
    P_3 lies on the line through P_1 and P_2

$M_1+M_2+M_3 = 0 \rightarrow$ colored points

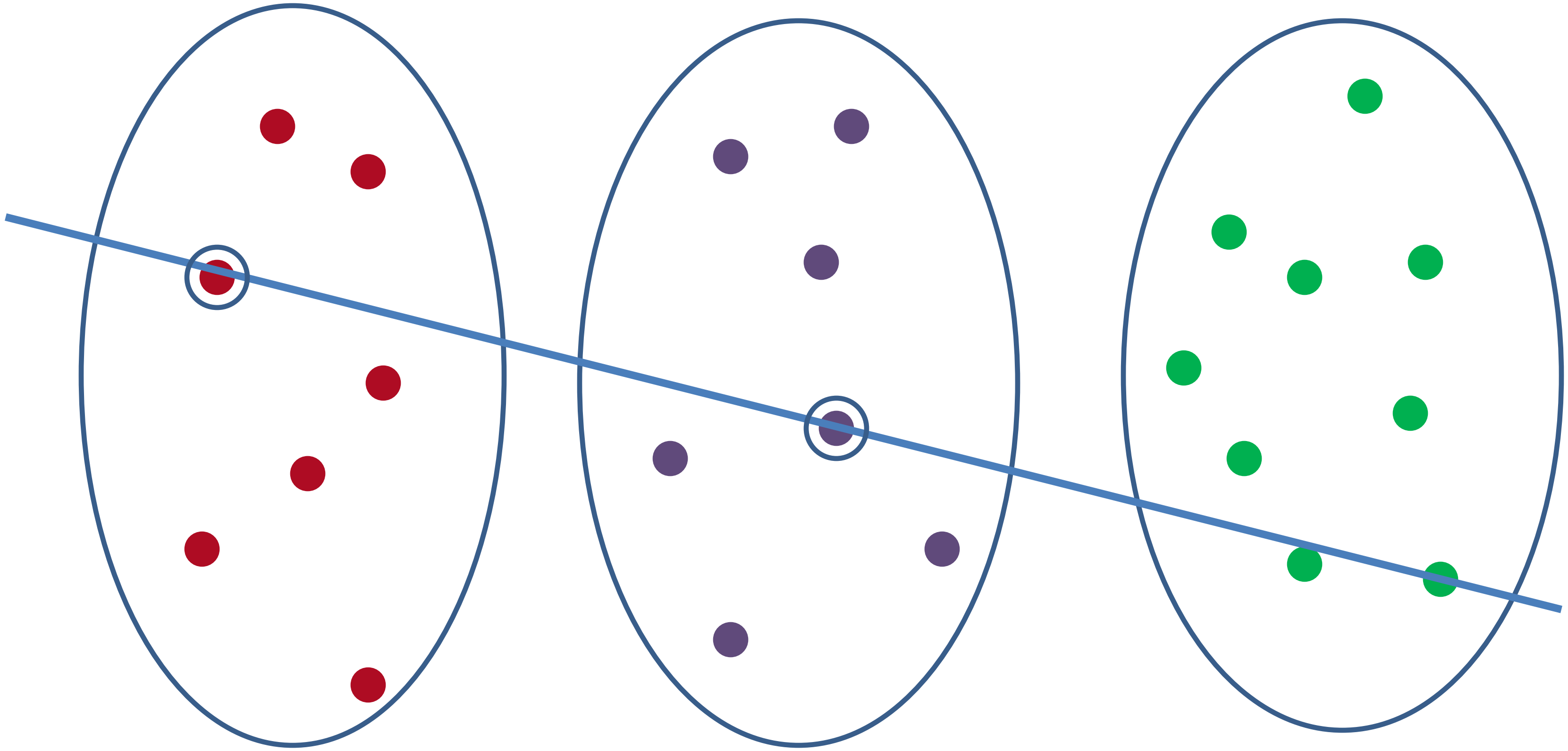


Linear forms of M_1

Linear forms of M_2

Linear forms of M_3

$M_1+M_2+M_3 = 0 \rightarrow$ colored points



Question: **If every line containing points of two colors also includes the third, must the points sit in low-dimensional space?**

The Sylvester-Gallai Theorem

- **Sylvester-Gallai Theorem**:

  Given a finite set of points S in the plane.

  – ∃ line L intersecting exactly two points of S

  – or all points in S are collinear

Not good enough!
L may contain only red points

Edelstein-Kelly Theorem

- **[Edelstein-Kelly 66]:** Let P be a set of points with the following properties:
  - Every point is assigned one of three colors – either Red or Blue or Green
  - The points span a space of ≤ 4 dimensions
  - Then there exists a line containing points of exactly 2 distinct colors from P
- Theorem: Rank(3,d) ≤ 4 over $\mathbb{R}$
- For Rank(k,d) generalizations for higher dimensions are used

Summary of depth-3

- Depth-3 important subcase before the general case of $\Sigma\Pi\Sigma\Pi$ circuits
- Demonstrated structure in depth-3 identities that led to beautiful mathematics
  - High dimensional colored versions of Sylvester-Gallai theorem
  - Extensions to finite fields
- Didn't see it but
  - Problem related to low-rank-recovery in signal processing
  - Reconstruction of depth-3 circuits

Talk Overview

- ✓ Definition of the problem
- ✓ Connection to lower bounds (hardness)
- ✓ Survey of positive results
- ✓ Some proofs:
  - ✓ Depth-3 circuits
- Open problems

Open problems

- Improve PIT of depth-3 circuits
  - e.g. to $f(k)\cdot poly(n)$
- Give PIT algorithm to $\Sigma\Pi\Sigma\Pi(k)$ circuits
  - Even $n^{f(k)}$ white-box algorithm will be great
  - Related to open problems on factorization of sparse polynomials
- PIT for tensors
  - Special case of depth-3 circuits
  - Related to Low-Rank-Recovery in signal processing
- Use PIT to reconstruct arithmetic circuits

Thank You!