

Polynomial Identity Testing

Amir Shpilka

Technion and MSR NE

Based on joint works with:

Zeev Dvir, Zohar Karnin, Partha Mukhopadhyay,
Ran Raz, Ilya Volkovich and Amir Yehudayoff

Exam

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

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

Prove it!

Will do so later.

Goal of talk

- Survey known results
- Explain proof techniques
- Give an interesting set of `accessible' open questions

Talk outline

- Definition of the problem
- Connection to lower bounds (hardness)
- Survey of positive results
- Some proofs
- Time permitting (no real chance):
Connection to polynomial factorization

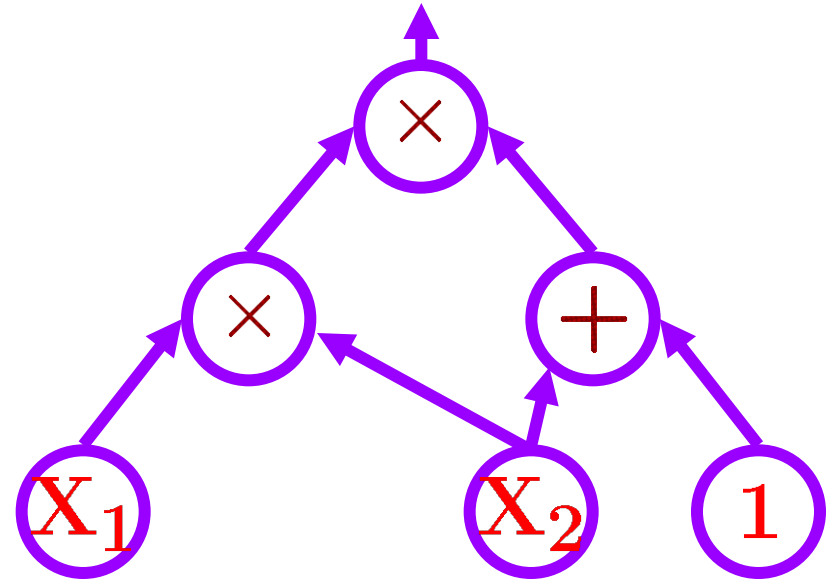
Playground: Arithmetic Circuits

Field: \mathbb{F}

Variables: X_1, \dots, X_n

Gates: $+$, \times

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



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

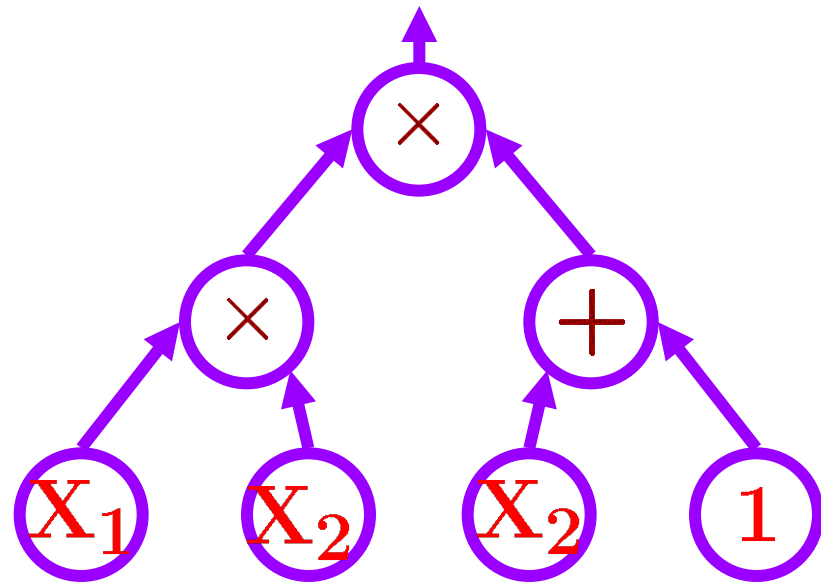
Size = number of gates/wires

Depth = length of longest input-output path

Degree = max degree of internal gates

Arithmetic Formulas

Same, except underlying graph is a tree



Bounded depth circuits

- $\Sigma\Pi$ circuits: depth-2 circuits with $+$ at the top and \times at the bottom. Size s circuits compute s -sparse polynomials.
- $\Sigma\Pi\Sigma$ circuits: depth-3 circuits with $+$ at the top, \times at the middle and $+$ at the bottom. Compute sums of products of linear functions. I.e. a sparse polynomial composed with a linear transformation.
- $\Sigma\Pi\Sigma\Pi$ circuits: depth-4 circuits. Compute sums of products of sparse polynomials.

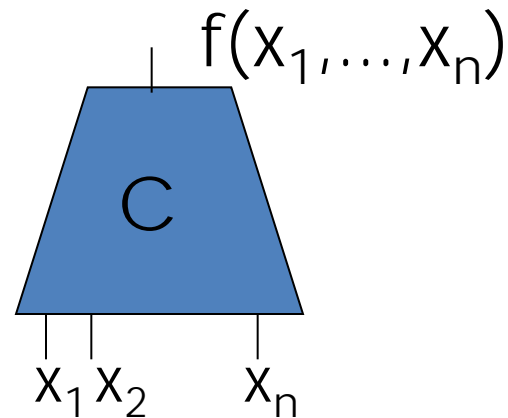
Why Arithmetic Circuits?

- 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
- Structured model (compared to Boolean circuits) \mathbf{P} vs. \mathbf{NP} may be easier

Polynomial Identity Testing

Input: Arithmetic circuit computing f

Problem: Is $f \equiv 0$?



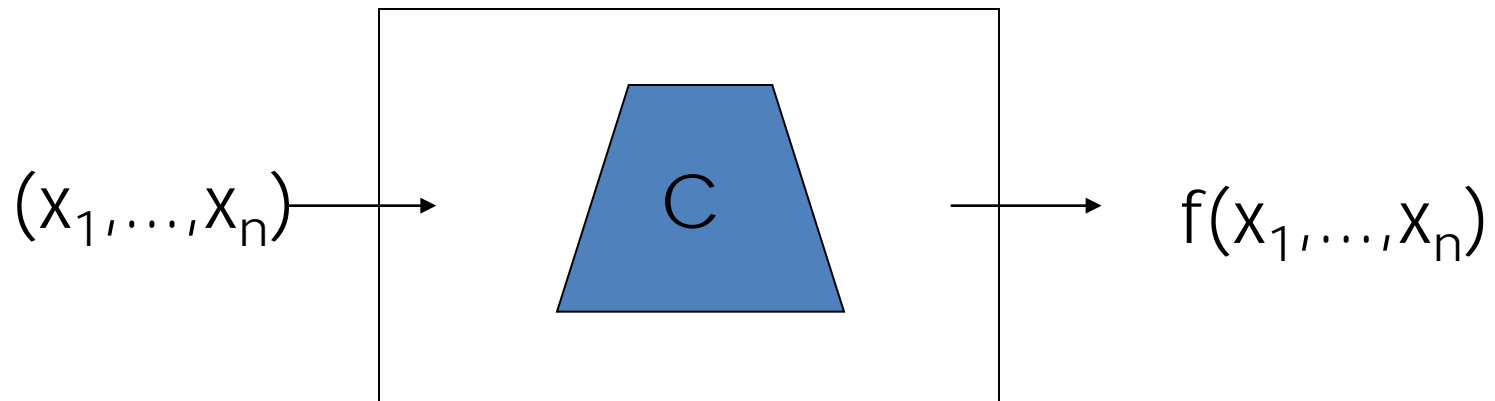
Randomized algorithm [Schwartz, Zippel, DeMillo-Lipton]: evaluate f at a random point

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

Black Box PIT \equiv Explicit Hitting Set

Input: A Black-Box circuit computing f .

Problem: Is $f=0$?



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

S,Z,DM-L: \exists small Hitting Set (not explicit)

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!

Polynomial Identity Testing

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

Hardness: PIT \equiv lower bounds

[Kabanets-Impagliazzo]:

- $2^{\Omega(n)}$ lower bound for Permanent \Rightarrow PIT in $n^{\text{polylog}(n)}$ time
- PIT $\in P \Rightarrow$ super-polynomial lower bounds:
Boolean for NEXP or arithmetic for Permanent

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

[Heintz-Schnorr, Agrawal]: Polynomial time Black-Box PIT \Rightarrow Exponential lower bounds for arithmetic 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 $\text{poly}(s)$

(i.e. $\text{poly}(s)$ size hitting set)

\Rightarrow exp. lower bounds for arithmetic circuits:

Given $\mathcal{H}=\{p_i\}$, find non-zero $\log(|\mathcal{H}|)+1$ -
variate polynomial f such that $f(p_i)=0$ for all i .

$\Rightarrow f$ does not have size s circuits

Gives lower bounds for f in **PSPACE**

Conjecture [Agrawal]:

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

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.

Proof: 1. Depth reduction a-la $P=NC^2$ [Valiant-Skyum-Berkowitz-Rackoff] 2. Break the circuit in the middle and interpolate each part using $\Sigma\Pi$ 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. [Agrawal-Vinay] \Rightarrow exponential lower bounds for general circuits. Now use [K-I].

Polynomial Identity Testing

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

Deterministic algorithms for PIT

- $\Sigma\Pi$ circuits (a.k.a., sparse polys) [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,Arvind-Mukhopadhyay,Karnin-S,Kayal-Saraf,Saxena-Seshadri]
 - Black-Box in time $n^{O(k)}$ *
- Sum of k Read-once formulas [S-Volkovich]
 - Black-Box in $n^{O(\log(n) + k)}$
 - White-Box in time $n^{O(k)}$
- Multilinear $\Sigma\Pi\Sigma\Pi(k)$ [Karnin-Mukhopadhyay-S-Volkovich, Saraf-Volkovich]
 - Black-Box in time $n^{\text{poly}(k)}$

Why study restricted models

- [Agrawal-Vinay] PIT for $\Sigma\Pi\Sigma\Pi$ circuits implies PIT for general depth.
- Gaining insight into more general questions:
 - Intuitively: lower bounds imply PIT
 - Multilinear formulas: super polynomial bounds [Raz,Raz-Yehudayoff] but no PIT algorithms
 - Not even for Depth-3 multilinear formulas!
 - Read-k, depth-3,4 multilinear formulas
 - relaxations of the more general problem
- Interesting results: Structural theorems for $\Sigma\Pi\Sigma(k)$ and $\Sigma\Pi\Sigma\Pi(k)$ circuits.

Polynomial Identity Testing

- ✓ Definition of the problem
- ✓ Connection to lower bounds (hardness)
- ✓ Survey of positive results
- Some proofs:
 - Depth-3 circuits
 - Depth-4 circuits
- Connection to polynomial factorization

Proofs – tailored for the model

Proofs usually use ‘weakness’ inherent in model

- **Depth 2**: few monomials. Substituting y^{a_i} to x_i we can control ‘collapses’ of different monomials.
- **Non Commutative formulas**: Polynomial has few linearly independent partial derivatives [Nisan]. Keep track of a basis for derivatives to do PIT.
- **$\Sigma\Pi\Sigma(k)$** : setting a linear function to zero reduces top fan-in. If $k=2$ then multiplication gates must be the same. Calls for induction.
- **Multilinear $\Sigma\Pi\Sigma\Pi(k)$** : in some sense ‘combination’ of sparse polynomials and multilinear $\Sigma\Pi\Sigma(k)$.
- **Read-Once-Formulas**: subformulas of root contain $\frac{1}{2}$ of variables.

Solution to Exam

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

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

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

$$\prod_{i=1}^n (A - \omega^i B) + \prod_{i=1}^n (B - \omega^i C) + \prod_{i=1}^n (C - \omega^i A) =$$
$$(A^n - B^n) + (B^n - C^n) + (C^n - A^n) = 0$$

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

Depth 3 identities

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

Depth 3 identities

- $C = M_1 + \dots + M_k$ $M_i = \prod_{j=1 \dots d_i} L_{i,j}$
- **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 $\dim(C) \leq \text{Rank}(k,d) = (\log(d))^k$
- **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 $n^{O(k)}$ algorithm by [**Kayal-Saxena**].

Black-Box PIT

- **Black-Box Algorithm** [Karnin S]:
Intuitively, if we project the inputs to a `low` dimensional space in a way that does not collapse the dimension below $\text{Rank}(k,d)$ then the identity should not become zero.
- **Theorem** [Gabizon Raz]: \exists "small" explicit set of D -dimensional subspaces V_1, \dots, V_m such that \forall space of linear functions \mathcal{L} :
 $\dim(\mathcal{L} |_{V_i}) = \min(\dim(\mathcal{L}), D)$ for most i

In other words: the linear functions in \mathcal{L} remain as independent as possible on V_i

Black-Box PIT

- **Corollary:** $\forall i, C \upharpoonright v_i$ has low "rank" $\Rightarrow C$ has low "rank"

If C has high rank then by Gabizon-Raz, for some i , $C \upharpoonright v_i$ has high rank.

Black-Box PIT

- **Corollary:** $\forall i, C \upharpoonright_{v_i}$ has low "rank" $\Rightarrow C$ has low "rank"
- **Corollary:** if $\forall i, C \upharpoonright_{v_i} \equiv 0$ then C has structure (i.e. C is sum of circuits of low "rank")

If C is not a sum of low rank circuits then for some i , $C \upharpoonright_{v_i}$ is not a sum of low rank circuits. This contradicts the structural theorem.

Black-Box PIT

- **Corollary:** $\forall i, C|_{V_i}$ has low "rank" $\Rightarrow C$ has low "rank"
- **Corollary:** if $\forall i, C|_{V_i} \equiv 0$ then C has structure (i.e. C is sum of circuits of low "rank")
- **Theorem:** if $\forall i, C|_{V_i} \equiv 0$ then $C \equiv 0$.

C is sum of low rank subcircuits \Rightarrow
 $\exists V_i$ s.t. rank of subcircuits remain the same.
 $C|_{V_i}$ is zero \Rightarrow each subcircuit vanishes on V_i .
 \Rightarrow subcircuits compute the zero polynomial.

Black-Box PIT

- Corollary: $\forall V_i \subseteq V$, if C has low "rank" $\Rightarrow C|_{V_i} \equiv 0$
- Corollary: If C' has the same rank as C , then C' and $C|_{V_i}$ are isomorphic. Hence, $C'|_{V_i} \equiv 0 \Leftrightarrow C \equiv 0$
- Theorem: C is sum of low rank subcircuits \Rightarrow

$\exists V_i$ s.t. rank of subcircuits remain the same.
 $C|_{V_i}$ is zero \Rightarrow each subcircuit vanishes on V_i .
 \Rightarrow subcircuits compute the zero polynomial.

Black-Box PIT

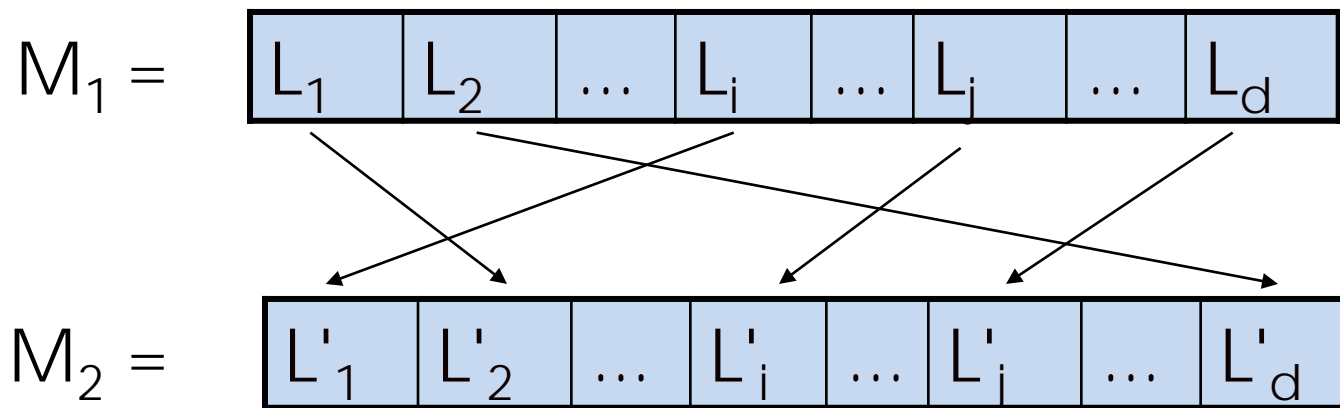
- **Corollary:** $\forall i, C|_{V_i}$ has low "rank" $\Rightarrow C$ has low "rank"
- **Corollary:** if $\forall i, C|_{V_i} \equiv 0$ then C has structure (i.e. C is sum of circuits of low "rank")
- **Theorem:** if $\forall i, C|_{V_i} \equiv 0$ then $C \equiv 0$.
- **Algorithm:** For every i , brute force compute $C|_{V_i}$
- **Time:** $\text{poly}(n) \cdot d^{\dim(V_i)} = d^{O(\text{Rank}(k,d))}$

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} , $k \cdot \log(d) < \text{Rank}(k,d) < k^3 \cdot \log(d)$
 - over \mathbb{Q} , $k < \text{Rank}(k,d) < k^2 \cdot \log(k)$
- Improves [Dvir-S] + [Karnin-S] (plug and play)
- **NEW:** [Saxena-Seshadri] BB-PIT in time $n^{O(k)}$

Bounding the rank

Basic observation: Consider $C = M_1 + M_2$



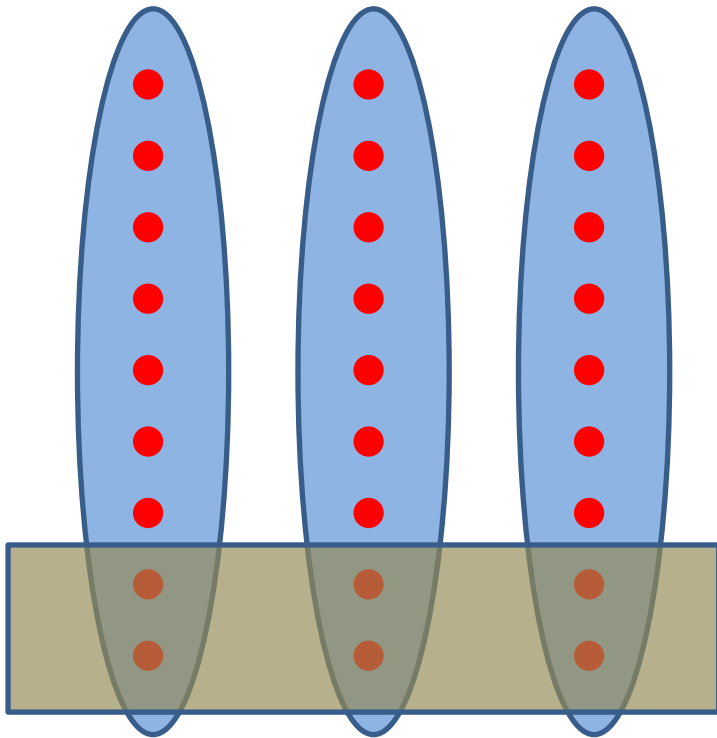
Fact: linear functions are irreducible polynomial.

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

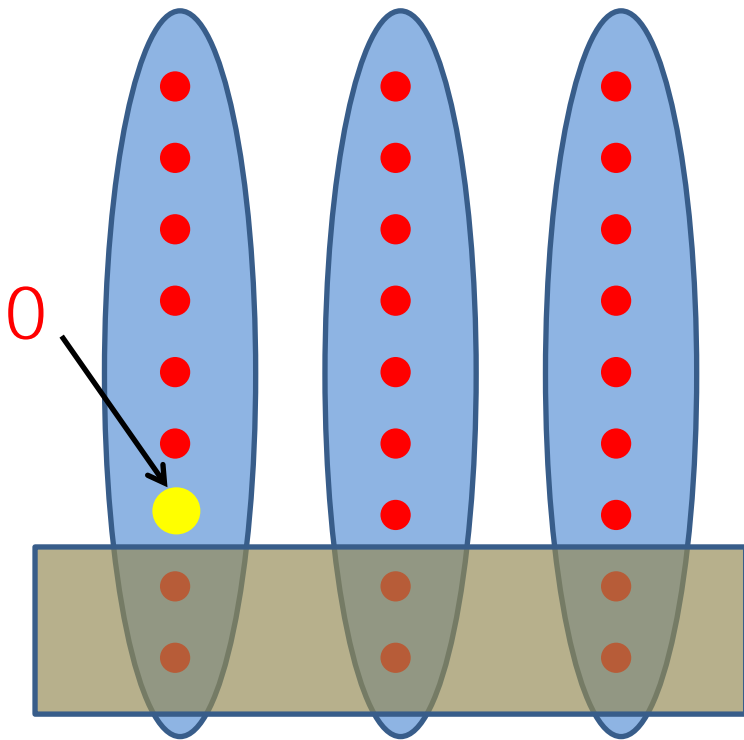
- Claim: $\text{Rank}(3,d) = O(\log(d))$



- 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

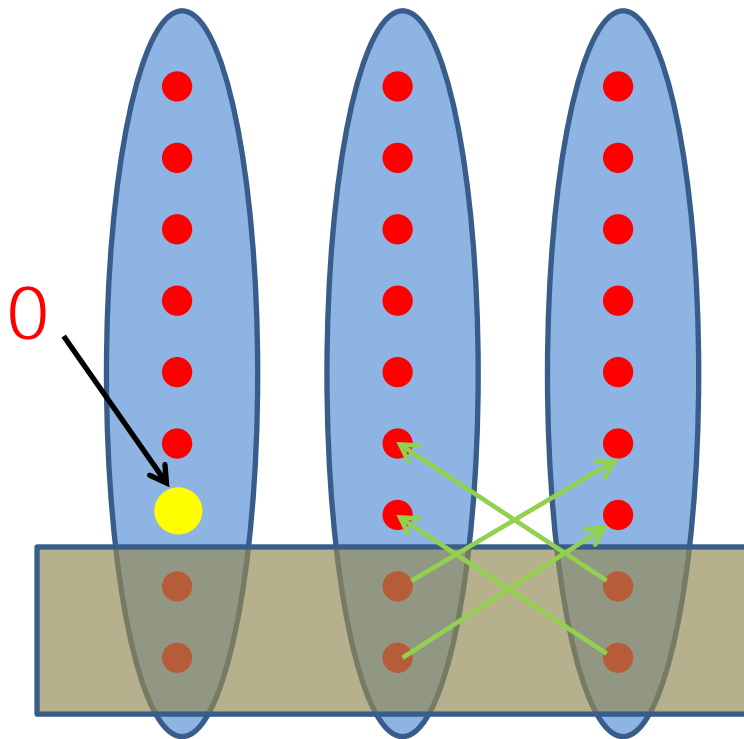
- Claim: $\text{Rank}(3,d) = O(\log(d))$



- 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

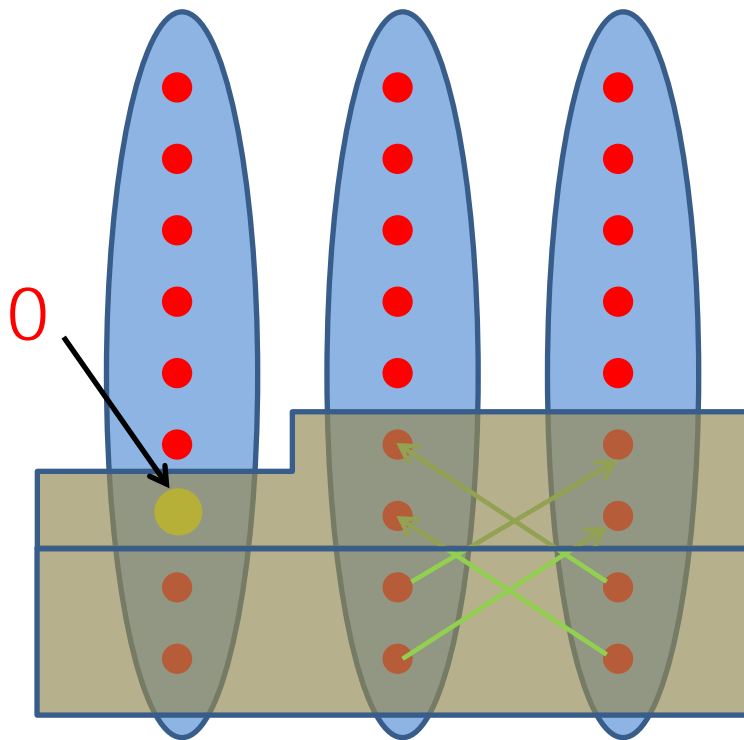
- Claim: $\text{Rank}(3,d) = O(\log(d))$



- 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: $\text{Rank}(3,d) = O(\log(d))$



- 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

Polynomial Identity Testing

- ✓ Definition of the problem
- ✓ Connection to lower bounds (hardness)
- ✓ Survey of positive results
- ✓ Some proofs:
 - ✓ Depth-3 circuits
 - ✓ Depth-4 circuits
- Connection to polynomial factorization

PIT and Factoring

f is composed if $f(X) = g(X |_S) \cdot h(X |_T)$ where S and T are disjoint

[S-Volkovich]: PIT is equivalent to factoring to decomposable factors.

\Leftarrow : $f \equiv 0$ iff $f+y \cdot z$ has two decomposable factors.

\Rightarrow : **Claim**: If we have a PIT for all circuits of the form $C_1 + C_2 \cdot C_3$, where $C_i \in M$ then given $C \in M$ we can deterministically output all decomposable factors of C .

PIT and factoring

- Deterministic decomposable factoring is equivalent to lower bounds:
 - Deterministic factoring implies **NEXP** does not have small arithmetic circuits
 - Lower bounds imply Deterministic decomposable factoring
- PIT \equiv factoring of multilinear polynomials
- Deterministic decomposable factoring for depth-2, $\Sigma\Pi\Sigma(k)$, sum of read-once...
- **Open problem**: is PIT equivalent to general factorization?

Summary of talk

- ✓ Definition of the problem
- ✓ Connection to lower bounds (hardness)
- ✓ Survey of positive results
- ✓ Some proofs:
 - ✓ Depth-3 circuits
 - ✓ Depth-4 circuits
- ✓ Connection to polynomial factorization

Some `accessible' open problems

1. Give a Black-Box PIT algorithm for non-commutative formulas
2. Solve PIT for depth-3 circuits
3. Solve PIT for multilinear depth-3 circuits
4. Black-Box PIT for set-multilinear depth-3 circuits ([degree \$d\$ tensors](#))
5. Polynomial time BB-PIT for read- k ROFs
6. PIT for depth-4 with restricted fan-in
7. Is PIT equivalent to general factorization?

Thank You!