Blackbox Identity Testing for Depth-3 Circuits

Nitin Saxena (Hausdorff Center for Mathematics, Bonn)

Joint work with

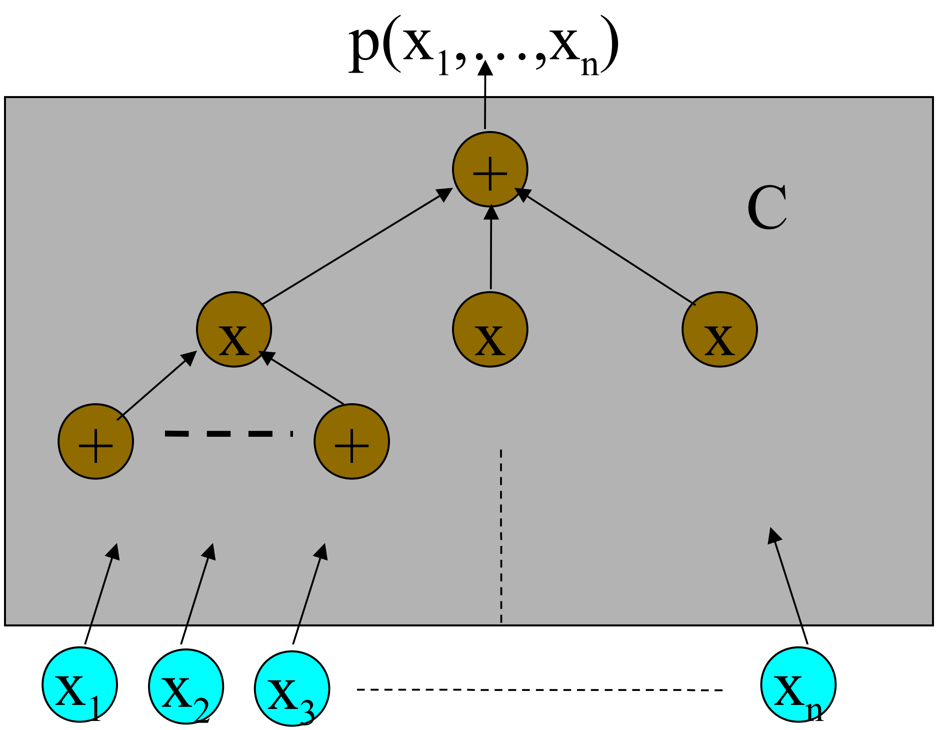
C. Seshadhri (Sandia National Laboratories, Livermore)

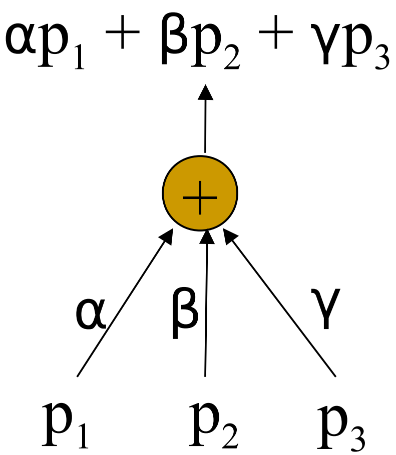
The problem of PIT

- Polynomial identity testing: given a polynomial $p(x_1,x_2,\ldots,x_n)$ over F, is it identically zero?
  - *All* coefficients of $p(x_1,\ldots,x_n)$ are zero.
  - $(x+y)^2 - x^2 - y^2 - 2xy$ is identically zero.
  - So is: $(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2)$
    $- (aA+bB+cC+dD)^2 - (aB-bA+cD-dC)^2$
    $- (aC-bD-cA+dB)^2 - (aD-dA+bC-cB)^2$
  - $x(x-1)$ is NOT identically zero over F_2.

Euler 1707- 1783

Circuits: Blackbox or not





We want algorithm whose running time is polynomial in size of the circuit.

- Non blackbox: can analyze structure of C
- Blackbox: cannot look *inside* C
  - Feed values and see what you get

A simple, randomized test

If output is 0, we guess it is identity.

Otherwise, we know it isn't.

- [Schwartz'80, Zippel'79, DeMillo Lipton'78] This is a randomized blackbox poly-time algorithm.

- (Big) open problem: Find a deterministic polynomial time algorithm.
  - We would really like a blackbox algorithm, i.e. a *hitting-set*.

Why?

- It's a natural algebraic problem!

- [Kabanets Impagliazzo'03] Derandomization implies circuit lower bounds for permanent.
- [Heintz Schnorr'80, Agrawal'05 '06] Hitting-set implies VP ≠ VNP.

- [Agrawal Kayal S '02] Primality Testing: $(x + a)^n - x^n - a = 0 \pmod{n}$.
- [Lovasz'79, Karp Upfal Wigderson'86] Bipartite matching in NC?...
- Many more (in complexity & algorithms).

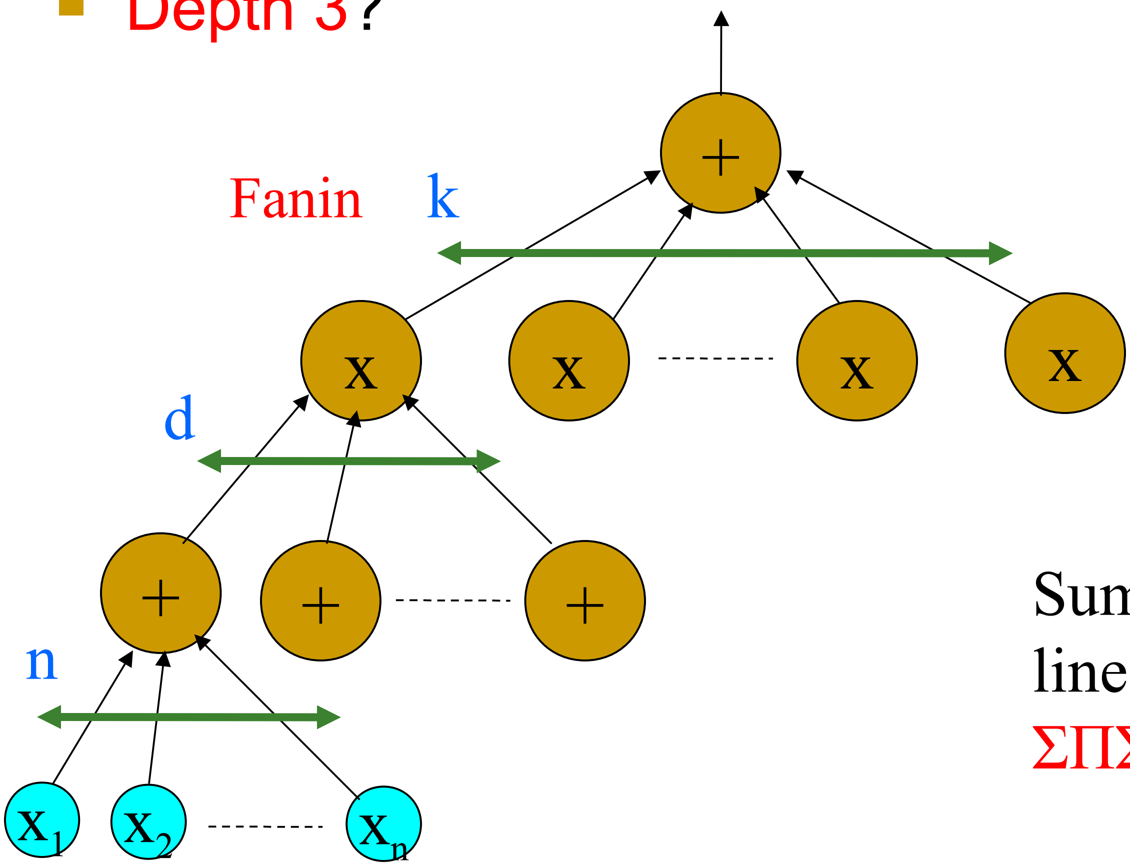
What do we do?

George Pólya 1887-1985

If you can't solve a problem, then there is an easier problem you *can* solve. Find it.

Get shallow results

- Let's restrict the depth and see what we get.
- Depth 2? Non-blackbox trivial!
  - [GK'87, BOT'88,…,KS'01, A'05] Polytime & blackbox.
- Depth 3?

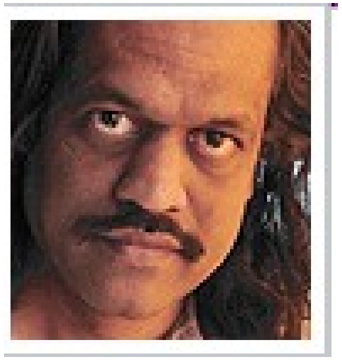


$$C \equiv \sum_{i=1}^{k} \prod_{j=1}^{d} L_{ij} = \sum_{i=1}^{k} T_i$$

Sum of k products of d linear forms in n variables: ΣΠΣ(k,d,n) circuit

Some good news

M. Agrawal



V. Vinay

- They say…
- [Agrawal Vinay'08] Chasm at Depth 4!
- If you can solve blackbox PIT for depth 4, then you've "solved" it all.

- Build the bridge from depth 3 end!

How do depth 3 identities look like

- Over Q

$$(x+z)(y+z) - xy - z(x+y+z) = 0$$

$$x_1x_2x_3(2y + x_1 + x_2 + x_3) - (y+x_1)(y+x_2)(y+x_3)(y+x_1+x_2+x_3)$$
$$+y(y+x_1+x_2)(y+x_2+x_3)(y+x_1+x_3) = 0$$

- [Kayal S '06] Over F_2

$$\prod_{\sum_i b_i \equiv 1} (b_1 x_1 + \dots + b_n x_n) + \prod_{\sum_i b_i \equiv 1} (x_0 + b_1 x_1 + \dots + b_n x_n)$$
$$+ \prod_{\sum_i b_i \equiv 0} (x_0 + b_1 x_1 + \dots + b_n x_n) = 0.$$

- ΣΠΣ(3,d,n) identities could carry substantial structure!

The past…

- A $\Sigma\Pi\Sigma(k,d,n)$ circuit:

- [Dvir Shpilka'05] Non-blackbox $n.2^{(\log d)^k}$ algorithm.
- [Kayal S '06] Non-blackbox nd^k algorithm.

The past... [redacted]

A Tale of four Methods

- [DS'05 + Karnin Shpilka'08] Blackbox, $n.2^{(\log d)^k}$ time.
- [S Seshadhri'09] $n.d^{(k^3 \log d)}$ time.
- [Kayal Saraf '09] $n.d^{(k^k)}$ time *over* Q.
- [S Seshadhri'10] $n.d^{(k^2)}$ time *over* Q.
  - $n.d^{(k^2 \log d)}$ time, any field.

- [Us '11] Blackbox, nd^k time, any field.
  - This *exactly* matches the non-blackbox test!

What we did

- We show that for $\Sigma\Pi\Sigma(k,d,n)$ PIT, it is enough to focus on $\Sigma\Pi\Sigma(k,d,k)$ circuits.

- Formally, we design a linear homomorphism Ψ from $F[x_1,...,x_n]$ to $F[y_1,...,y_k]$ in *poly(kdn)* time such that :

  for any $\Sigma\Pi\Sigma(k,d,n)$ circuit C, C=0 iff Ψ(C)=0.

  - Ψ maps x_i to $a_{i,1}y_1+...+a_{i,k}y_k$ for some constants $a_{i,j} \in F$.
  - Trivially, C=0 implies Ψ(C)=0.

- This converts an n-variate question into a k-variate one, *without even looking at C* !

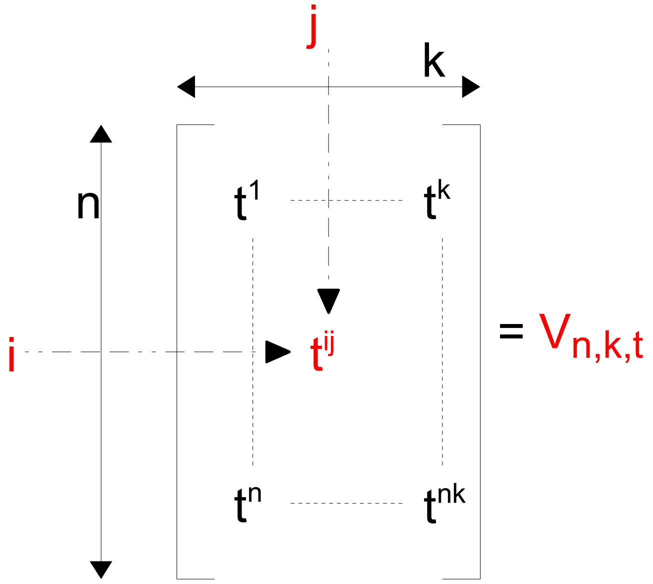
k-variate is easy

- We have: a k-variate circuit $C':=\Psi(C)$ of degree d.
- A consequence of Schwartz-Zippel, a kind of Combinatorial Nullstellensatz [Alon'99]:

Theorem: Let polynomial $f(y_1,\ldots,y_k)$ be of degree at most d in each variable. Let $S\subseteq F$ of size d+1. Then, $f(s_1,\ldots,s_k)=0$ for all $(s_1,\ldots,s_k)\in S^k$ iff $f(y_1,\ldots,y_k)=0$.

- Using this theorem we see that S^k is a hitting-set for C'.
- Thus, $\Psi^{-1}(S^k)$ is a $(d+1)^k$ sized hitting-set for $\Sigma\Pi\Sigma(k,d,n)$ circuits!

What is this Ψ ?



- Vandermonde matrix $V_{n,k,t}$ is in $F(t)^{n \times k}$.
- Think of $k \le n$.
- Classical fact: $V_{n,k,t}$ has rank k.
- [Gabizon Raz'05] showed a stronger property and built an *extractor for affine sources*.
- Theorem [GR'05]: If a matrix A in $F^{k \times n}$ has *full* rank, then $A.V_{n,k,t}$ is an *invertible* matrix over F(t).
  - Thus, $\det(A.V_{n,k,t})$ is a *nonzero* polynomial of *degree* at most nk^2.
  - *Proof:* Do row operations on A and consider the leading term in t.
- We define $\Psi_t : x_i \rightarrow t^{i.1}y_1+\ldots+t^{i.k}y_k$, for all $i=1,\ldots,n$.

Ψ_t preserves rank!

- Note $\Psi_t : x_i \rightarrow t^{i.1}y_1+\ldots+t^{i.k}y_k$ maps $F[x_1,\ldots,x_n]$ to $F(t)[y_1,\ldots,y_k]$.
- By [Gabizon Raz'05] theorem, Ψ_t preserves the rank of any k linear forms in $F[x_1,\ldots,x_n]$.
  - Think of a linear form $a_1x_1+\ldots+a_nx_n$ as the vector $(a_1,\ldots,a_n)$.
  - Ψ_t transforms it to $(a_1,\ldots,a_n).V_{n,k,t}$.
  - $rk_F\{L_1,\ldots,L_k\} = rk_{F(t)}\{ \Psi_t(L_1),\ldots,\Psi_t(L_k) \}$, for all linear forms L_i.
- Thus, Ψ_t preserves rank k subspaces.
- The key fact to prove now is:

  For any $\Sigma\Pi\Sigma(k,d,n)$ circuit C, $C\neq 0$ implies $\Psi_t(C)\neq 0$.

Certificate for C≠0

- Is there an easy *explanation* why C≠0 ?
  - One that can hopefully be preserved by Ψ_t ?
- YES! [S Seshadhri'10] showed that there is a low-rank ideal, modulo which C≠0.

Theorem [SS'10]: Let $C=T_1+\ldots+T_k\neq 0$. Then there is an $i<k$ and sub-products $f_1|T_1,\ldots,f_i|T_i$ such that:

- $C \equiv \alpha.T_{i+1} \neq 0 \pmod{f_1,\ldots,f_i}$, and
- Rank of the linear forms involved in $f_1,\ldots,f_i$ is at most i.

- If we could show $\Psi_t(T_{i+1}) \neq 0 \pmod{\Psi_t(f_1),\ldots,\Psi_t(f_i)}$ then $\Psi_t(C)\neq 0$, and we are done!

Existence of the ideal certificate

- We sketch the proof of [S Seshadri'10] by an example.
- Consider the circuit C (with products T_1, T_2 and T_3),

$$C := x_1^2 x_3 x_4 - x_2(x_2+2x_1)(x_3-x_1)(x_4+x_2-x_1) + (x_2+x_1)^2(x_3+4x_1)(x_4+x_2)$$

- We now build an ideal that certifies $C \neq 0$.
  1) Pick f_1 s.t. f_1 involves rank 1 and $T_2+T_3 \neq 0 \pmod{f_1}$.
     Say, $f_1 := x_1^2$.
  2) Pick f_2 s.t. $\{f_1,f_2\}$ involve rank ≤ 2 and $T_3 \neq 0 \pmod{f_1,f_2}$.
     Say, $f_2 := (x_3-x_1)$.

➡ $C \equiv T_3 \neq 0 \pmod{x_1^2,\ x_3-x_1}$. Yaay!!

- Warning: The ideal $(x_1^2,\ x_2(x_2+2x_1))$ does NOT work.

Ψ_t is moral: It maintains ideals!

- We have: $T_{i+1} \notin (f_1,\ldots,f_i)$, certifying $C \neq 0$.
- We want: $\Psi_t(T_{i+1}) \notin (\Psi_t(f_1),\ldots,\Psi_t(f_i))$.
- Let S be the span of the linear forms involved in $f_1,\ldots,f_i$.
  - Rank of S is at most $i<k$.
- Cute Fact 1: Any linear form $L|T_{i+1}$ and $\notin S$ is a non-zerodivisor modulo the ideal.
  - Thus, $T_{i+1}/L \notin (f_1,\ldots,f_i)$.
- After removing all such L we have $T'_{i+1} \notin (f_1,\ldots,f_i)$.
- Fact 2: Ψ_t is an isomorphism on algebras $F[L,S]$ ($\forall L$ above).
- Thus, $\Psi_t(T_{i+1}) \notin (\Psi_t(f_1),\ldots,\Psi_t(f_i))$. DONE!

At the end…

- We efficiently reduce $\Sigma\Pi\Sigma(k,d,n)$ PIT to $\Sigma\Pi\Sigma(k,d,k)$ PIT.
  - Via an elegant homomorphism.
  - Explains everything when k is small!

- What about large k?
  - Beat the exponential dependence on k?

- What about depth 4, bounded top fanin circuits?
  - Study the action of Ψ_t on them.
  - Nice behavior expected for $\Sigma\Pi\Sigma\Pi_\delta(k,d,n)$ with bounded δ,k.

Thank you!