The rank & file of circuits

Nitin Saxena

Department of CSE

Indian Institute of Technology Kanpur

**all pictures are works of others.

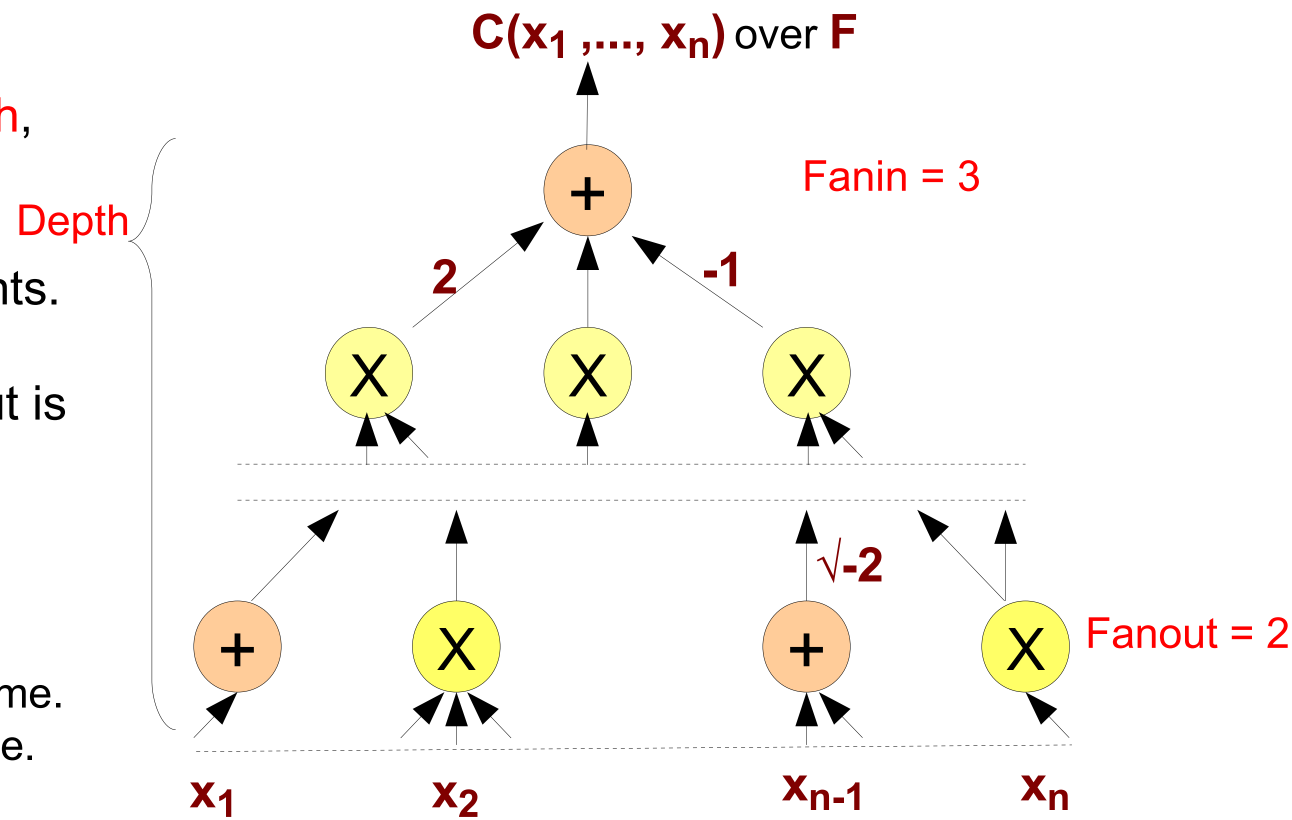
UPMC Paris, 2014

Contents

- *Arithmetic circuits*
- Hitting-set, blackbox PIT
- P≠NP wish & flip
- Rank -- Depth-3 circuits
- Rank -- Depth-4 circuits
- Rank concentration
- At the end …

Arithmetic Circuits

- Directed rooted graph, gates, wires, leaves.
- Size: wires + constants.
- Formula: when fanout is bounded by 1.
- Compare Turing Machines:
  - Size is like *sequential* time.
  - Depth is like *parallel* time.



- Studies computation more *algebraically* than Turing machines.

Arithmetic Circuits

- $C(x_1, \ldots, x_n)$ usually has *exponentially* many monomials.
  - Due to the *multiplication* gates.
  - For size s, there can be s^s monomials.
- The degree can also be exponential.
  - Due to repeated-squaring in a *circuit*.
  - Eg. $x\hat{}(2^s)$
  - Not possible in a *formula*.
- Conversely, (Valiant, Skyum, Berkowitz & Racko 1983) showed that a circuit of degree d can be *shrunk* to depth $\log d$.
- Our interest is in *log*-depth circuits.
  - *constant*-depth *formulas* are hard enough!

Contents

Hitting-set, Blackbox PIT

- Polynomial Identity Testing (PIT) is the problem of testing whether a given circuit $C(x_1, \ldots, x_n)$, over F, is *zero*.

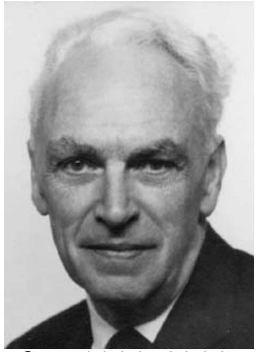
- We know several identities …
  - $(x+y)(x-y) - x^2 + y^2 = 0.$
  - Euler's four-square: $(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2) - (aA+bB+cC+dD)^2 - (aB-bA+cD-dC)^2 - (aC-bD-cA+dB)^2 - (aD-dA+bC-cB)^2 = 0.$

Euler 1707-1783

- PIT: Is there a test better than brute-force?
  - Brute-force is *exponential* as a circuit can have so many monomials.

- Randomization gives a simple answer.
  - Evaluate $C(x_1, \ldots, x_n)$ at a random point in F^n.
  - (Ore 1922), (DeMillo & Lipton 1978), (Zippel 1979), (Schwartz 1980).

- PIT has a randomized polynomial time algorithm.



Ore 1899-1968

Hitting-set, Blackbox PIT

- The randomized algorithm needs only a *degree* bound, in turn, only a circuit-size bound.
  - No need to look inside the circuit.
  - Blackbox PIT: Don't *see* the circuit, only evaluation allowed.
- Per size bound, we ask for an *efficient* hitting-set.
  - A *small* subset $H \subset F^n$ that contains a non-root of *each* nonzero $C(x_1, \ldots, x_n)$.
- For size bound s, the hitting-set has to be $\Omega(s)$ in size.
- Potentially, circuit $C(x)$ can have $\Omega(s^s)$ roots.
  - Still we believe a hitting-set of size poly(s) is constructible!

Hitting-set, Blackbox PIT

- Question of interest: Design hitting-sets for circuits.
- Appears in numerous guises in computation:
- Complexity results
  - Interactive protocol (Babai,Lund,Fortnow,Karloff,Nisan,Shamir 1990), PCP theorem (Arora,Safra,Lund,Motwani,Sudan,Szegedy 1998), …
- Algorithms
  - Graph matching in parallel, matrix completion (Lovász 1979), equivalence of branching programs (Blum, et al 1980), interpolation (Clausen, et al 1991), primality (Agrawal,Kayal,S. 2002), learning (Klivans, Shpilka 2006), polynomial solvability (Kopparty, Yekhanin 2008), factoring (Shpilka, Volkovich 2010), …

Contents

- Arithmetic circuits
- Hitting-set, blackbox PIT
- *P≠NP wish & flip*
- Rank -- Depth-3 circuits
- Rank -- Depth-4 circuits
- Rank concentration
- At the end …

P≠NP Wish & Flip

- Almost *everyone* wishes P≠NP (*few* venture a proof!).
  - Is there a problem whose solutions are *easy* to certify, but *hard* to discover?


Valiant 1949-

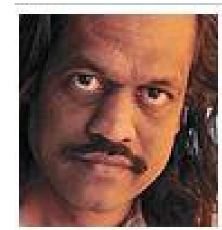
- How about counting the #certificates?
  - VP≠VNP?
  - Or, permanent vs. determinant?
- "proving permanent hardness" flips to "designing hitting-sets".
  - *Almost,* (Heintz,Schnorr 1980), (Kabanets,Impagliazzo 2004), (Agrawal 2005 2006), (Dvir,Shpilka,Yehudayoff 2009), (Koiran 2011) ...
- Designing an efficient algorithm is less intimidating than proving one doesn't exist!

P≠NP Wish & Flip

- Moreover, (Agrawal,Vinay 2008) showed: It suffices to consider depth-4 circuits.
  - $C(x_1,\ldots,x_n) = \sum_i \prod_j f_{ij}$, where f_{ij} are *explicitly* given polynomials in the variables $x_1,\ldots,x_n$.

f_{ij} are linear

Agrawal 1966-



Vinay 196?-

- (Gupta,Kamath,Kayal,Saptharishi 2013) showed: It suffices to consider depth-3 circuits.

- A reasonable plan, then, is –
  - Short term: Study depth-3 *well enough*; design a hitting-set.
  - Long term: VP≠VNP.

Contents

- Arithmetic circuits
- Hitting-set, Blackbox PIT
- P≠NP wish & flip
- *Rank -- Depth-3 circuits*
- Rank -- Depth-4 circuits
- Rank concentration
- At the end …

Rank -- Depth-3 Circuits

- Consider a depth-3 circuit C:
  - $C(x_1,\ldots,x_n) = \sum_{i\in[k]} \prod_{j\in[d]} f_{ij}$, where f_{ij} are *linear* polynomials in $F[x_1,\ldots,x_n]$.
- The rank of C is $rk(C) := rk_F\{f_{ij} \mid i\in[k], j\in[d]\}$.
  - (Dvir,Shpilka 2005) showed the *first* rank bound r when $C=0$.
  - (Karnin,Shpilka 2008) gave a hitting-set in time $nd^{r(k,d)}$.
  - (S.,Seshadhri 2009) showed $r(k,d) < k^3 \log d$.
  - (Kayal,Saraf 2009) showed $r(k,d) < k^k$ over Q.
  - (S.,Seshadhri 2010) improved to k^2 over Q (& $k^2 \log d$ any field).
- (S.,Seshadhri 2011) gave a nd^k time hitting-set over any field.
  - *Indirect* use of rank.

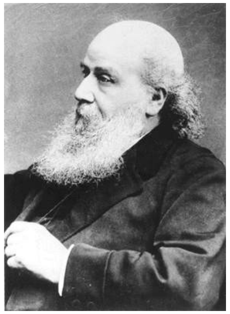
Rank -- Depth-3 Circuits

- Ingredients of the proofs are –

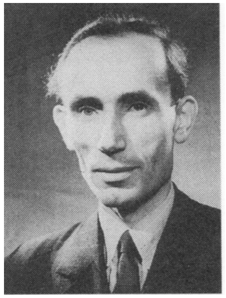
- Found *higher* Sylvester-Gallai theorems (over any field).
  - If any two points in $S \subset R^n$ have a *collinear* third point, then S is a *line*!
  - Generalized both to hyperplanes & to other fields.

- Found ideal Chinese remaindering.
  - If *coprime* f & g divide h, then fg divides h.
  - Generalized to *ideals* generated by *products* of *linear* forms.

- We show that a depth-3 identity contains a k-dimensional Sylvester-Gallai configuration.



Sylvester 1814-1897

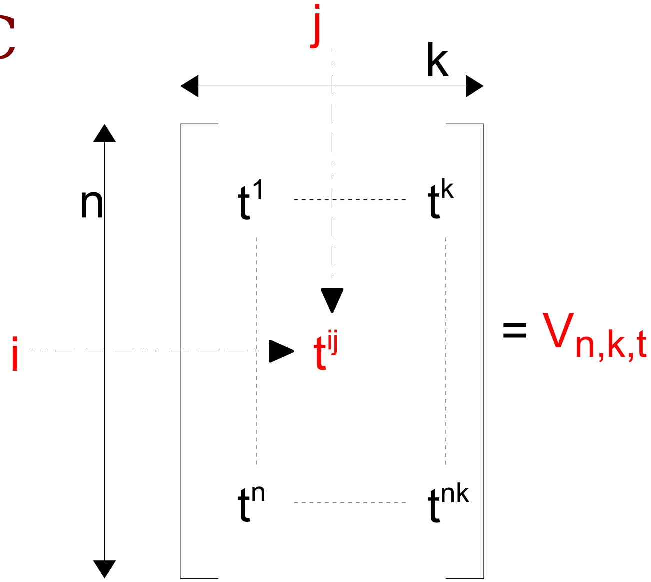


Gallai 1912-1992

Rank -- Depth-3 Circuits

Vandermonde 1735-1796

- Finally, Vandermonde matrix is employed.
- We define $\Psi_t : x_i \to t^{i.1}y_1+\ldots+t^{i.k}y_k$, for all $i=1,\ldots,n$.
- We show that Ψ_t reduces the variables of C from n to k, and preserves non-zeroness!
- This yields a nd^k time hitting-set.



Contents

- Arithmetic circuits
- Hitting-set, Blackbox PIT
- P≠NP wish & flip
- Rank -- Depth-3 circuits
- *Rank -- Depth-4 circuits*
- Rank concentration
- At the end …

Rank -- Depth-4 Circuits

- Consider a depth-4 circuit C:
  - $C(x_1,\ldots,x_n) = \sum_{i\in[k]} \prod_{j\in[d]} f_{ij}$, where f_{ij} are *sparse* polynomials in $F[x_1,\ldots,x_n]$.

- The rank of C is $rk(C) := trdeg_F\{f_{ij} \mid i\in[k], j\in[d]\}$.
  - The transcendence degree is the maximum number of algebraically independent polynomials.
  - $\{g_1,\ldots,g_m\}$ are called algebraically independent if there is no non-zero polynomial $A \in F[y_1,\ldots,y_m]$ such that $A(g_1,\ldots,g_m)=0$.
  - Eg, $trdeg_F\{x_1, x_2, x_1^3+x_2^2\} = 2$ ...
  - … with annihilating polynomial $A := (y_1^3+y_2^2-y_3)$.

- This generalizes the notion of linear independence to higher degree.

Rank -- Depth-4 Circuits

- (Beecken,Mittmann,S. 2011) showed: For rank bound r, there is a hitting-set in time $|C|^r$.

- Ingredients of the proof are –

- **Theorem** (Jacobi 1841; Beecken,Mittmann,S. 2011): If $ch(F)=0$ or $>d^r$, then $rk\, J_x(g_1,\ldots,g_m) = trdeg\{g_1,\ldots,g_m\}$.
  - Jacobian $J_x(g_1,\ldots,g_m)$ is the $m \times n$ matrix $(\partial_j g_i)_{i,j}$.

Jacobi 1804-1851

- A *Vandermonde-based* map reduces the variables from n to r.
  - Preserves $rk(C)$: By studying the map's action on the Jacobian.
  - Preserves $C\neq 0$: By Krull's Hauptidealsatz.

- $rk(C)$ is like the minimum number of variables needed to describe the 'essence' of C.

Krull 1899-1971

Rank -- Depth-4 Circuits

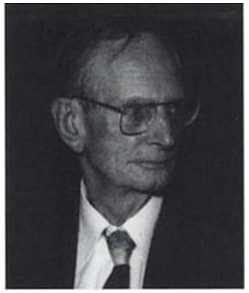
- (Agrawal,Saha,Saptharishi,S. 2012) used Jacobian to explain all known *poly-time* hitting-sets, and more ...
  - Hitting-sets for new models, eg *constant*-depth *constant*-read *multilinear* formulas, were found.
  - Permanent lower bounds for *certain* depth-4 circuits.

- These methods use Jacobian as a tool,
  - without actually proving a rank bound for depth-4 identities.

Rank -- Depth-4 Circuits

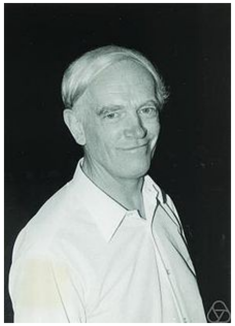
- Jacobian is not known to work for *small* $ch(F) =: p > 0$.
  - Issue: $\partial x^p = px^{p-1} = 0$.

- (Scheiblechner,Mittmann,S. 2012) used the de Rham-Witt complex to devise a Witt-Jacobian criterion.
  - A p-adic lift of the polynomials is employed.
  - This subtlety is studied in p-adic cohomology theory.



De Rham 1903-1990

- Byproduct: This gives the first improvement on algebraic-independence testing (over small characteristic).
  - PSPACE upper bound improved to $NP^{\#P}$.



Witt 1911-1991

Contents

- Arithmetic circuits
- Hitting-set, Blackbox PIT
- P≠NP wish & flip
- Rank -- Depth-3 circuits
- Rank -- Depth-4 circuits
- *Rank concentration*
- At the end …

Rank Concentration


Hadamard 1865-1963

- Consider a depth-4 circuit C:
  - $C(x_1,\ldots,x_n) = \sum_{i\in[k]} \prod_{j\in[d]} f_{ij}$, where f_{ij} are *sparse* polynomials in $F[x_1,\ldots,x_n]$.
- Let $H_k(F)$ be a Hadamard algebra.
  - It is the ring $(F^k,+,*)$,
  - where, $*$ is the coordinate-wise product.
- Rewrite C as $\mathbf{1}^T.\{\ f_1(x_1,\ldots,x_n) * \ldots * f_d(x_1,\ldots,x_n)\ \}$,
  - where, $f_j(x_1,\ldots,x_n) \in H_k(F)[x_1,\ldots,x_n]$ are again *sparse*.
  - Define $D := f_1(x_1,\ldots,x_n)*\ldots*f_d(x_1,\ldots,x_n) \in H_k(F)[x_1,\ldots,x_n]$.
- Study the *rank* of the *coefficients* in D ...

Rank Concentration

- Let $l := \log k$. Focus on the l-support monomials M_l of D.
  - Monomials $x_1^{e1} \ldots x_n^{en}$, with nonzero e's less than l.
  - Their coefficients, in D, are F^k vectors. What's their rank?
  - Eg. when $D := x_1 * \ldots * x_{l+1}$ it is zero.

- Conjecture: $\exists$ *efficient shift* after which – Coefficients of M_l in D have the same rank as *all* the coefficients in D.
  - Rank concentration in low support!

- Thus, it suffices to consider only *low support evaluations*.
  - $\forall\ S \subseteq [n]$ of size l, keep x_S free and set the rest to zero.
  - Yields a hitting-set in time $n^l = n^{\log k}$. Quasi-polynomial time!

Rank Concentration

- (Agrawal,Saha,S. 2013) proved low support rank concentration for several interesting circuits.
  - *Set-multilinear depth-3* circuits (Nisan,Wigderson 1996; Raz,Shpilka 2005). No sub-exponential hitting-set was known.
  - $C(x_1,\ldots,x_n) = \sum_{i\in[k]} \prod_{j\in[d]} f_{ij}(X_j)$, where X_j 's are disjoint variables.

- Proof ingredient: Specialized *matrix tools* to study *shifted* circuits over Hadamard algebras.

- (Forbes,Saptharishi,Shpilka 2014; Agrawal,Gurjar,Korwar,S 2014; Gurjar,Korwar,S, Thierauf 2014) have expanded rank concentration to many models.

- Quasi-poly-time hitting-set for sum of constantly many ROABPs.

At the end …

- We saw a number of natural notions of circuit rank.
  - We are yet to see the last word!
- Rank concentration conjecture for depth-3 looks hopeful.
- Need to improve the notion to get a poly-time hitting-set.
- That should push us over the VP≠VNP cliff!