Towards hitting-sets for multilinear depth-3 circuits

Nitin Saxena (IIT Kanpur, India)

(Based on joint works with Manindra Agrawal, Rohit Gurjar, Arpita Korwar, Chandan Saha)

2014

Contents

- Polynomial identity testing
- Depth-3 circuits
- The multilinear model – whitebox
- Rank concentration idea
- Concentration in set-multilinear depth-3
- Concentration in low-distance multilinear depth-3
- Concentration in invertible ROABP
- Conclusion

Polynomial identity testing

- Given an arithmetic circuit $C(x_1, ..., x_n)$ of size s, whether it is zero?
  - In $poly(s)$ many bit operations?
  - Think of field $F =$ finite field or rationals.
- Brute-force expansion is as expensive as s^s.
- Randomization gives a practical solution.
  - Evaluate $C(x_1, ..., x_n)$ at a random point in F^n.
  - (Ore 1922), (DeMillo & Lipton 1978), (Zippel 1979), (Schwartz 1980).
- This test is blackbox, i.e. one does not need to see C.
  - Whitebox PIT – where we are allowed to look inside C.
- Blackbox PIT is equivalent to designing a hitting-set $H \subset F^n$.
  - H contains a non-root of *each* nonzero $C(x_1, ..., x_n)$ of size s.

Polynomial identity testing

- 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 & Kopparty, Saraf, Shpilka 2014), …

Polynomial identity testing

- Hitting-sets relate to circuit lower bounds.
- It is conjectured that VP$\neq$VNP.
  - Or, permanent is *harder* than 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 seems more doable than proving one doesn't exist!
- Connections to *Geometric Complexity Theory* and derandomizing the *Noether's normalization lemma*. (Mulmuley 2011, 2012)

Contents

Depth-3 circuits

- The smallest, yet mysterious, circuit model is depth-3.
  - Computes a polynomial of the form $C(x_1,\ldots,x_n) = \sum_i \prod_j L_{ij}$, where L_{ij} are *linear* polynomials in $F[x_1,\ldots,x_n]$.
- First serious study by (Dvir,Shpilka 2005).
  - They gave a rank bound for identities $C=0$.
- Depth-3 is more than a mere curiousity now.
  - (Gupta, Kamath, Kayal, Saptharishi 2013) showed that PIT (resp. lower bounds) for depth-3 implies nontrivial results for general circuits.
- Depth-3 PIT is open except for restricted models.
  - Set-multilinear, bounded fanin, diagonal, etc.

Depth-3 circuits

- Let $C(x_1,\ldots,x_n) = \sum_{i\in[k]} \prod_{j\in[d]} L_{ij}$.
- C is set-multilinear if there is a *partition* P of $[n]$ s.t. the variables in L_{ij} come only from the j-th part of P.
  - (Raz, Shpilka 2004) gave a poly-time PIT for set-multilinear depth-3.
  - Uses linear algebra. Whitebox.
- C is bounded fanin if the *top fanin* k is ``small''.
  - Sequence of works (Dvir, Shpilka '05; Kayal, S. '06; Karnin, Shpilka '08; S., Seshadhri '09; Kayal, Saraf '09; S., Seshadhri '10; S., Seshadhri '11) gave a $\mathrm{poly}(nd^k)$ time hitting-set.
  - Tools in (S., Seshadhri '11) are ideal theory & Vandermonde map.
- C is diagonal if each product gate is a d-th power.
  - (S. '08) gave a poly-time PIT. Devised a *dual form*. Whitebox.

Contents

- Polynomial identity testing
- Depth-3 circuits
- The multilinear model – whitebox
- Rank concentration idea
- Concentration in set-multilinear depth-3
- Concentration in low-distance multilinear depth-3
- Concentration in invertible ROABP
- Conclusion

The multilinear model

- Let $C(x_1,\ldots,x_n) = \sum_{i\in[k]} \prod_{j\in[d]} L_{ij}$ be multilinear.
  - $\forall i$, $\exists$ partition P_i of $[n]$ s.t. the variables in L_{ij} come only from the j-th part of P_i .
  - Clearly, $d \le n$.
- Eg. the defining polynomial of any immanant is multilinear.
  - (Raz, Yehudayoff 2008) showed an *exponential* lower bound against multilinear depth-3.
  - Clever use of the *partial derivatives method*.
- No subexponential PIT is known though.
  - A good model to test new hitting-set-design ideas!
- Recent developments have focussed on restricting the partitions P_i .

The multilinear model

- Let $C(x_1,\ldots,x_n) = \sum_{i\in[k]} \prod_{j\in[d]} L_{ij}$ be set-multilinear.
  - Partitions $P_1 = P_2 = \ldots = P_k$.
- Eg. $C(x_1,\ldots,x_n) = \sum_{i\in[k]} \prod_{j\in[n]} (c_{ij}+a_{ij}\, x_j)$.
- (Raz, Shpilka 2004) poly-time PIT repeatedly uses two operations on the product-gates:
  - Brute-force expansion of the initial divisor, till the *sparsity* grows beyond k.
  - Contraction of these k divisors, using $\leq k$ fresh variables, keeping the F-linear-dependencies unchanged.
- Whitebox, as the operations require the knowledge of the coeffs.
  - (Forbes, Shpilka '12) turned this idea into a $n^{\log n}$ time-contructible hitting-set, assuming the partition known.

Contents

- Polynomial identity testing
- Depth-3 circuits
- The multilinear model – whitebox
- Rank concentration idea
- Concentration in set-multilinear depth-3
- Concentration in low-distance multilinear depth-3
- Concentration in invertible ROABP
- Conclusion

Rank concentration idea

- Let $C(x_1,\ldots,x_n) = \sum_{i\in[k]} \prod_{j\in[d]} L_{ij}$.
  - With $L_{ij} = (a_{ij,0} + a_{ij,1}x_1 + \cdots + a_{ij,n}x_n)$.
- To reduce the study to a simpler model, we consider vectors & their Hadamard product:
  - $$D(x_1,\ldots,x_n) := \begin{pmatrix} L_{11} \\ L_{21} \\ \vdots \\ L_{k1} \end{pmatrix} * \cdots * \begin{pmatrix} L_{1d} \\ L_{2d} \\ \vdots \\ L_{kd} \end{pmatrix}.$$
  - Clearly, $C(x_1,\ldots,x_n)$ is the dot-product $\mathbf{1}^T \bullet D(x_1,\ldots,x_n)$.
- Further, rewrite $D(x_1,\ldots,x_n) = \prod_{j\in[d]} (z_{j,0} + z_{j,1}x_1 + \cdots + z_{j,n}x_n)$.
  - Where, the i-th entry of $z_{j,m}$ is $(z_{j,m})_i = a_{ij,m}$ in the base field F.

Rank concentration idea

- We call $D(x_1,\ldots,x_n) = \prod_{j\in[d]} (z_{j,0}+ z_{j,1}x_1+ \cdots + z_{j,n}x_n)$ a $\prod\sum$-circuit over $H_k(F)$.
  - $H_k(F) := (F^k,+,*)$ is an algebra. (With $0/1$ as the zero/unity.)
  - An F-vector space endowed with the Hadamard product.
  - In this talk you could keep any commutative F-algebra of dimension k in mind.
- Consider the F-span $\mathrm{span}(D)$ of all coeffs of D.
  - It has dimension at most k.
  - Define $\ell := 2+\lg k$.
- We want to focus on the coeffs of low-support monomials M in D.
  - Define $|M|_0$ as the number of variables that nontrivially appear in M.
  - Consider the F-span $\mathrm{span}_\ell(D)$ of $\{\mathrm{coef}_D(M) \mid |M|_0 < \ell\}$.

Rank concentration idea

- Conjecture 0: $\mathrm{span}_\ell(D) = \mathrm{span}(D)$.
  - Since the low-support span includes at least $2k$ coeffs of D, don't we have a good shot of spanning everything?
- An easy counter-example is $D := x_1 x_2 \cdots x_n$.
  - Here, $\mathrm{span}_{n-1}(D) = \{0\}$.
- But, $D(x_1+1, x_2+1, \ldots, x_n+1)$ satisfies Conjecture 0 !
  - Merely, $\mathrm{span}_1(D) = \mathrm{span}(D)$.

$C(\mathbf{x}+\mathbf{t})$ has an uncancelled monomial of support below ℓ, if $C(\mathbf{x})\neq 0$.

- ℓ-conc. Conjecture: After a suitable small shift D' of D, we have $\mathrm{span}_\ell(D') = \mathrm{span}(D')$.
  - We can afford at most a subexp-time shift & an $\ell = o(n)$.
  - An equivalent formulation is $D' = 0 \pmod{\mathrm{span}_\ell(D')}$.

Rank concentration idea

- Claim: A random shift makes D ℓ-concentrated for $\ell := 2 + \lg k$.
  - We need to study the *transfer* from D to D'.
- Let $D(x_1,\ldots,x_n) = \prod_{j\in[d]} (z_{j,0} + z_{j,1}x_1 + \cdots + z_{j,n}x_n)$ be a multilinear circuit over $H_k(F)$.
  - Denote the j-th factor by L_j .
- Let us apply the formal shift:
  - $D'(\mathbf{x}) := D(\mathbf{x}+\mathbf{t}) = \prod_{j\in[d]} (L_j(\mathbf{t}) + z_{j,1}x_1 + \cdots + z_{j,n}x_n)$.
- We would like to study how the F-dependencies of the coeffs of D change under the shift.
  - Let Z be the coeffs matrix $[\ \mathrm{coef}_D(S) : S \subseteq [n]\ ]$.
  - We define the null-vectors matrix $\mathcal{N}(Z) := [\ v : Zv = 0\ ]$.

Rank concentration idea

- Z has its rows resp. cols indexed by $[k]$ resp. $2^{[n]}$.
  - $\mathcal{N}(Z)$ has its rows indexed by $2^{[n]}$.

- (Agrawal, Saha, S. 2013) studied the relationship between $\mathcal{N}(Z)$ and $\mathcal{N}(Z')$.
  - (Forbes, Saptharishi, Shpilka 2014) instead took the primal approach, i.e. only focussing on Z & Z'.

- From $D(\mathbf{x}) = D'(\mathbf{x} - \mathbf{t})$ we deduce that for every coefficient
  $z_T = \sum_{T\subseteq S} z'_S \cdot (-t)_{S\setminus T}$.

- We collect such equations for all T to get the matrix equation:
  $Z = Z'\, A\, M\, A^{-1}$, where
  - $M(S,T) = 1$ if $T\subseteq S$, else $=0$.
  - A is a diagonal matrix with $A(S,S) = (-t)_S$.

$(-t)_S$ refers to the signed monomial $\prod_{i\in S}(-t_i)$.

Rank concentration idea

- We now go modulo $span_\ell(D')$ to get the truncated form:
  $Z \equiv Z'_\ell \, A_\ell \, M_\ell \, A^{-1} \pmod{span_\ell(D')}$, where
  - $[n]_{\geq \ell}$ denotes the subsets of size $\geq \ell$.
  - M_ℓ has its rows resp. cols indexed by $[n]_{\geq \ell}$ resp. $2^{[n]}$.
  - With $M_\ell(S,T) = 1$ if $T \subseteq S$, else $= 0$.
  - A_ℓ is a diagonal matrix, indexed by $[n]_{\geq \ell}$, with $A_\ell(S,S) = (-t)_S$.
  - Z'_ℓ has its rows resp. cols indexed by $[k]$ resp. $[n]_{\geq \ell}$.
- Transfer Equation: $0 \equiv Z'_\ell \, A_\ell \, M_\ell \, A^{-1} \mathcal{N}(Z) \pmod{span_\ell(D')}$.
- Source of ℓ-conc.:
  If $M_\ell \, A^{-1} \mathcal{N}(Z)$ is full rank then $0 \equiv Z'_\ell \pmod{span_\ell(D')}$.

null-vector of Z gets transformed to a null-vector of Z' (even Z'_ℓ)

- Goal: To understand the properties of the transfer matrix M_ℓ and the null-vectors $\mathcal{N}(Z)$.

Rank concentration idea

- Lemma 1 (Agrawal, Gurjar, Korwar, S. 2013): Any nontrivial combination of the rows of M_l has at least 2^l nonzero entries.
  - Assume $l \leq n$. Apply induction on n.
- Lemma 2: The column-space of $\mathcal{N}(Z)$ is generated by the columns of sparsity at most $(k+1)$.
  - Simply because any $(k+1)$ columns of Z are F-dependent.
- These two lemmas can be used to analyze the *formal* (or *random*) shift.
  - Using a monomial ordering on $\mathbf{t}$, order the cols of Z.
  - Let B be the least basis of Z. Note that $|B| \leq k$.
  - Every column $v \notin B$, of Z, depends on B.
  - Focus on these ``good'' null-vectors $G(Z) \subseteq \mathcal{N}(Z)$.
  - They are 2^n-k many and F-linearly independent.

Rank concentration idea

- The amount of good null-vectors is $|G(Z)| \geq 2^n\text{-}k \geq |[n]_{\geq \ell}|$.
  - Let us pick $|G(Z)| = |[n]_{\geq \ell}|$.
  - What is the determinant of $M_\ell\ A^{-1}\ G(Z)$?

M_ℓ is $[n]_{\geq \ell} \times 2^n$. $G(Z)$ is $2^n \times [n]_{\geq \ell}$.

- By considering the leading $\mathbf{t}$-monomial of this determinant and Lemma 1, we deduce its nonzeroness.
- Thm: Under a formal shift, D gets $(2+\lg k)$-concentrated over $F(\mathbf{t})$.
- $\Rightarrow$ For a suitably large F, a random efficient shift works as well!
- We didn't use the $\prod\sum$ structure of D, at all, in this proof.
- Key: To *efficiently derandomize* this shift, we need to somehow use the special structure of D.

Rank concentration idea

- We could work towards the conc.-conjecture by studying simpler models.
- Diagonal model: $D(x_1,\ldots,x_n) = (1 + z_1x_1 + \cdots + z_nx_n)^d \in H_k(F)[\mathbf{x}]$.
- Theorem: D is already ɭ-concentrated!
- *Proof:* Order the coefficients $z_S{}^e$ wrt to deg-lex $(x_1 < \ldots < x_n)$.
  - Let B be the least basis of the coefficients. Note that $|B| \leq k$.
  - Consider a monomial $z_S{}^e$ in B. Pick a submonomial $z_{S'}{}^{e'}$.
  - Suppose $z_{S'}{}^{e'}$ is not in B.
  - Then, $z_{S'}{}^{e'}$ is F-dependent on some *smaller* monomials in B.
  - Implying, $z_S{}^e$ is F-dependent on some *smaller* monomials in B. A ↯ .
  - Thus, B is closed under submonomials! $\square$

Contents

- Polynomial identity testing
- Depth-3 circuits
- The multilinear model – whitebox
- Rank concentration idea
- Concentration in set-multilinear depth-3
- Concentration in low-distance multilinear depth-3
- Concentration in invertible ROABP
- Conclusion

Concentration in set-multilr depth-3

- Let $C(x_1,\ldots,x_n) = \sum_{i\in[k]} \prod_{j\in[d]} L_{ij}$ be set-multilinear.
  - Each product gate respects the partition P. (P has *parts*.)
  - Corresponding $D(\mathbf{x}) = \prod_{p\in P} \left(z_{p,0} + \sum_{i\in p} z_{p,i}\, x_i \right) \in H_k(F)[\mathbf{x}]$.

- We want to design an efficient map φ s.t. the shift $\varphi(\mathbf{t})$ makes D ℓ-concentrated, for $\ell := 2+\lg k$.

- Theorem (Agrawal, Saha, S. 2013): D can be made ℓ-concentrated in time $n^{O(\ell)}$.
  - The idea of the proof – *Tiny factors* of D!
  - Define for a subset of parts S, $D_S(\mathbf{x}) := \prod_{p\in S} \left(z_{p,0} + \sum_{i\in p} z_{p,i}\, x_i \right)$.

- Lemma 3: $D'(\mathbf{x}) := D(\mathbf{x}+\mathbf{t})$ is ℓ-concentrated, if $\forall S\subseteq P, |S|=\ell$, $D'_S(\mathbf{x})$ is ℓ-concentrated.

Concentration in set-multilr depth-3

- Let us prove the Theorem using Lemma 3.
  - For an $S \subseteq P$, $|S| = \ell$, we make $D'_S(\mathbf{x})$ ℓ-concentrated by following the formal shift proof.
  - It only requires the $\mathbf{t}$-monomials appearing in $D'_S(\mathbf{x})$ to be distinct.
  - Since, these are monomials of degree bounded by ℓ, we can easily design a morphism φ in time $n^{O(\ell)}$, that keeps them all distinct. □

- Pf Lemma 3: It will be convenient to work with a normalized $D'(\mathbf{x})$:
  - $E(\mathbf{x}) := \prod_{p \in P} (1 + \sum_{i \in p} z'_{p,i}\, x_i) \in H_k(F(\mathbf{t}))[\mathbf{x}]$.
  - Clearly, $D'(\mathbf{x})$ is ℓ-conc. iff $E(\mathbf{x})$ is ℓ-conc.
  - Suppose $\forall S \subseteq P$, $|S| = \ell$, $E_S(\mathbf{x})$ is ℓ-conc.
  - $\Rightarrow \prod_{p \in S} z'_{p,\, i(p)}$ is F-dependent on the ($<\ell$)-support coeffs. of $E_S(\mathbf{x})$.
  - $\Rightarrow z'_{q,i} \bullet \prod_{p \in S} z'_{p,\, i(p)}$ is F-dep. on ($<\ell+1$)-support coeffs. of $E_{S \cup \{q\}}(\mathbf{x})$. □

Contents

- Polynomial identity testing
- Depth-3 circuits
- The multilinear model – whitebox
- Rank concentration idea
- Concentration in set-multilinear depth-3
- Concentration in low-distance multilinear depth-3
- Concentration in invertible ROABP
- Conclusion

Concentration in low-distance multilr depth-3

- Can rank-conc. idea deal with multilinear models where *no* subexp-time PIT algorithms are known?
  - Eg. When there are two *different* underlying partitions?
- Let $D(\mathbf{x}) = \prod_{j\in[d]} (z_{j,0} + z_{j,1}x_1 + \cdots + z_{j,n}x_n)$ be a multilinear $\prod\sum$ circuit over $H_k(F)$.
  - Each of the top k_1 rows respect a partition P_1 and the rest of the $k_2 = k-k_1$ rows respect a partition P_2 .
  - Product gates of the former resp. latter kind we call P_1-type resp. P_2-type.
  - The monomials x_S that can possibly appear in a P_1-type product we collect as $\chi P_1 := \{ S\subseteq[n] \mid \text{elements of } S \text{ come from distinct parts of } P_1\}$.
  - Similarly, define χP_2 – the P_2-type monomials.

Concentration in low-distance multilr depth-3

- We could now divide our study of $D(\mathbf{x})$ into three monomial-cases, based on where a monomial lives:

- Case I – $S \in \chi P_1 \setminus \chi P_2$:
  - Such an S contains $i \neq j$ which belong to the same part of P_2 .
  - $\Rightarrow$ If we take the partial derivative of D wrt x_i & x_j then:
  - $\partial_{i,j} D(\mathbf{x})$ is zeroed out in the bottom k_2 part,
  - thus, $\partial_{i,j} D(\mathbf{x})$ is set-multilinear wrt P_1 .
  - Within Case-I monomials we have $(2+\ell)$-concentration. □

- Case II – $S \in \chi P_2 \setminus \chi P_1$: Similar as above. □

- Case III – $S \in \chi P_1 \cap \chi P_2$: Need new ideas to design the map φ.
  - No *tiny factors* of D available!

Concentration in low-distance multilr depth-3

- Let us make a ``simplification'': Assume that $P_1 \leq P_2$ is a refinement.
  - I.e. Every part in P_2 is a *union* of parts in P_1 .
  - Eg. $\{ \{1\}, \{2\}, \{3\}, \{4\} \} \leq \{ \{1, 2\}, \{3, 4\} \}$.
- Lemma 4: If $P_1 \leq P_2$ then $\chi P_1 \cap \chi P_2 = \chi P_2$.

The parts in the top are the subsets of those that appear in S.

- This inspires a ``tiny'' factor $D_S(\mathbf{x}) := \prod_{p \in S} (z_{p,0} + \sum_{i \in [n]} z_{p,i} x_i)$ for every $S \subseteq P_2$, $|S| = \ell$.
  - Though its lower P_2-part is degree ℓ , the upper P_1-part can be *arbitrary*.
- Say, we work with the normalized shift $D'(\mathbf{x})$ and the factors D'_S .
  - So, the *sole* P_1-monomials in $D'_S(\mathbf{x})$ are already handled in Case-I.
  - The remaining monomials in D'_S are few – $n^{O(\ell)}$ many.
  - This provides ℓ-concentration in Case-III as well! □

Concentration in low-distance multilr depth-3

- We could get more mileage from this approach by relaxing the $P_1 \le P_2$ condition to low-distance δ.
  - For every part $p \in P_2$ there is $p \in N \subseteq P_2$, $|N| \le \delta$, s.t. the union of S is a *union* of some parts in P_1. (N is a neighborhood.)
  - Eg. a refinement case $P_1 \le P_2$ has distance one.
  - Eg. $\{ \{1,2\}, \{3,4\}, \{5,6\} \}$ and $\{ \{1,4\}, \{3,6\}, \{5,2\} \}$ have distance three.

- The previous proof extends in this case as well.
  - Pick `tiny' factors $D_S(\mathbf{x}) := \prod_{p \in S} (z_{p,0} + \sum_{i \in [n]} z_{p,i} x_i)$ for every $S \subseteq P_2$, $|S| \le \delta\ell$, where S contains ℓ parts & their neighborhoods.
  - We get $(2+\ell)$-concentration in D'_S. Cost of φ grows as $n^{O(\delta\ell)}$.

Concentration in low-distance multilr depth-3

- The proof extends to arbitrary many partitions of low-distance.
  - The proof divides the monomials into phases depending on which partitions could possibly produce them.
  - We could prove $(1+\delta+\ell)$-concentration, with the cost of the morphism φ being $n^{O(\delta\ell)}$.
- Another extension is to the model of sum-of-set-multilinear depth-3.
- Theorem (Agrawal, Gurjar, Korwar, S. 2013):
  Whitebox PIT for a sum of c set-multilinear depth-3 circuits can be done in $n^{O(n^{1-\epsilon}\log k)}$ time, where $\epsilon := 1/2^{c-1}$.
  - First *subexponential* PIT for this class.

Contents

- Polynomial identity testing
- Depth-3 circuits
- The multilinear model – whitebox
- Rank concentration idea
- Concentration in set-multilinear depth-3
- Concentration in low-distance multilinear depth-3
- Concentration in invertible ROABP
- Conclusion

Concentration in invertible ROABP

- Width-w ABP is a matrix product $D(x_1, \ldots, x_n) = \prod_{i\in[d]} D_i(\mathbf{x})$.
  - Where, $D_i(\mathbf{x})$ is a $w \times w$ matrix with entries as *linear* polynomials from $F[\mathbf{x}]$.
  - We say that a polynomial $f \in F[\mathbf{x}]$ is computable by an ABP, if it appears as the (1,1)-th entry of an ABP D.

- (Ben-Or, Cleve '92) showed that any *poly-sized* formula can be reduced to an efficient width-3 ABP.
  - It has an additional property of invertibility, i.e. each D_i is an *invertible* formal matrix.

- (Saha, Saptharishi, S. '09) showed that depth-3 PIT reduces to that of invertible width-2 ABP.

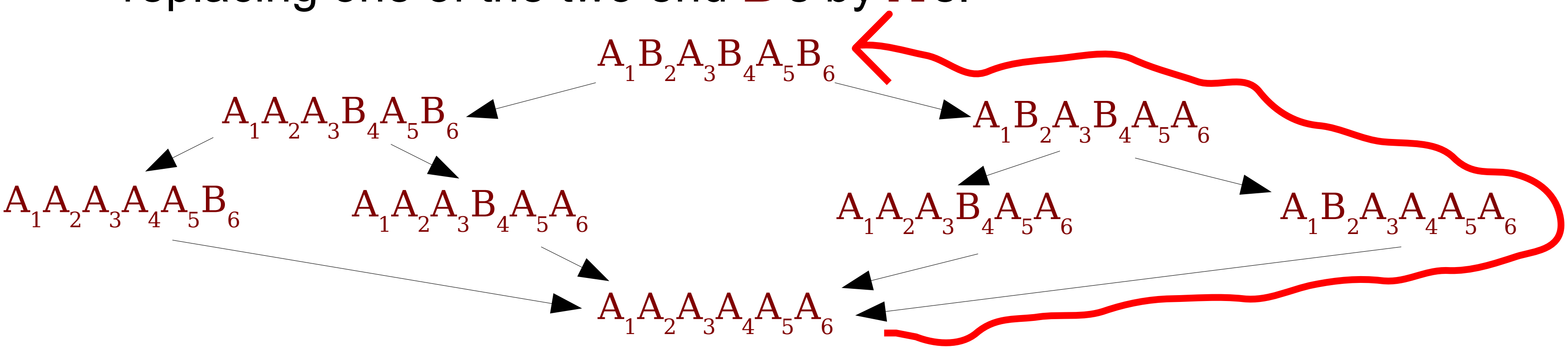
- Since $w \times w$ matrices over $F[\mathbf{x}]$ form an F-vector space, we can talk about the ℓ-concentration of the ABP D. Say, for $\ell := 1 + w^2$.

Concentration in invertible ROABP

- The analogue of set-multilinear here is called read-once ABP (ROABP) $D(\mathbf{x}) = \prod_{i\in[d]} D_i(\mathbf{x})$.
  - ∃ partition P of $[n]$ s.t. the variables in D_i come from the i-th part of P.
  - Clearly, $d \le n$.
- Theorem (Agrawal, Gurjar, Korwar, S. 2013): An invertible width-w ROABP can be made ℓ-concentrated in $poly(nw)$ time.
  - *Poly*-time hitting-set for constant w.
- *Proof sketch:* We show this for the instructive case where the D_i's are univariate.
  - i.e. $D(\mathbf{x}) = \prod_{i\in[n]} (A_i + B_i x_i)$.
  - Where, A_i and B_i are $w \times w$ matrices over F.
  - Wlog we assume that A_i is *invertible*.
  - Easy to achieve via a *shift*.

Concentration in invertible ROABP

- We will show that D is already ℓ-concentrated !
- Consider a typical coeff. in D. Say, $M := A_1B_2A_3B_4A_5B_6$.
  - It is the coeff. of $x_2x_4x_6$ in D.
- We define a partial ordering on the submonomials of M, by replacing one of the two end B's by A's.



Claim: An F-dependency within descendants lifts all the way to the root.

Contents

- Polynomial identity testing
- Depth-3 circuits
- The multilinear model – whitebox
- Rank concentration idea
- Concentration in set-multilinear depth-3
- Concentration in low-distance multilinear depth-3
- Concentration in invertible ROABP
- Conclusion

At the end …

- Rank concentration, after a shift, puts to good use the combinatorial structure of the multilinear depth-3 model.
  - It studies this via matrix equations.
  - The transfer matrix acts on the null-space of the coefficients.
  - The transfer matrix is *strongly* full-rank for any polynomial.

- The null-space was rich enough in various models – set-multilinear depth-3, low-distance multilinear, sum-of-set-multilinears, etc.

- OPEN: Can we further exploit the null-space of the coefficients of a *multilinear* $\prod\sum$-circuit over $H_k(F)$ to design an efficient shift?

Thank you!