Faster hitting-sets for certain ROABP

Nitin Saxena (IIT Kanpur, India)

(Based on joint works with Rohit, Rishabh, Arpita)

2016, τ, Tel-Aviv

Contents

- Polynomial identity testing
- ABP
- ROABP ideas
- Deg-insensitive, width-sensitive idea
- Commutative ROABP
- Conjectures for poly-time
- Conclusion

Polynomial identity testing

- Given an arithmetic circuit $C(x_1, \ldots, x_n)$ of size s, whether it is zero?
  - In $\mathrm{poly}(s)$ 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 $C(x_1, \ldots, x_n)$ 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 $C(x_1, \ldots, x_n)$ 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, 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), independence tests,….

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 leads to awesome tools!
- Connections to *Geometric Complexity Theory* and derandomizing the *Noether's normalization lemma*. (Mulmuley 2011, 2012)

Contents

Arithmetic branching program (ABP)

- ABP are special circuits.
  - More suited to *low* degree polynomial computation.

- Definition: Suppose $f(\mathbf{x})$ is the $(1,1)$-th entry in the iterated matrix product $A_1(\mathbf{x})\ldots A_D(\mathbf{x})$, where A_i are $w \times w$ matrices with entries in $\mathbf{x}\cup F$.
  - $f(\mathbf{x})$ is said to have an ABP of width-w and depth-D.

- ABP is as strong as *symbolic determinant* (Mahajan,Vinay '97) .
  - Width-3 is as strong as *formulas* (Ben-Or,Cleve '92) .
  - Width-2 PIT captures *depth-3 circuit* PIT (Saha,Saptharishi,S.'09) .
  - Depth-3 circuit *chasm* (Gupta,Kamath,Kayal,Saptharishi '13) .

Read-once oblivious ABP (ROABP)

- Definition (ROABP): $f(\mathbf{x})$ is the $(1,1)$-th entry in the matrix product $A_1(x_{\pi(1)})\ldots A_n(x_{\pi(\mathbf{n})})$, where A_i is a $w \times w$ matrix with entries in $F[x_{\pi(i)}]$ of degree at most d.
  - In blackbox model, π may be unknown.
  - *Set-multilinear* and *diagonal* depth-3 models reduce to ROABP.

- Let $C(x_1,\ldots,x_n) = \sum_{i\in[k]} \prod_{j\in[d]} L_{ij}$ be a depth-3 circuit.

- 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'04) gave a poly-time whitebox PIT.

- 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

ROABP ideas

- ROABP is a fertile model to study.
  - (Raz,Shpilka'04) gave a poly-time *whitebox* PIT.
  - (Forbes,Shpilka'12;'13; Agrawal,Saha,S.'13; Forbes,Saptharishi, Shpilka'14) progress towards *quasipoly-time* hitting-set.
- (Agrawal,Gurjar,Korwar,S.'15) gave a $(\mathrm{wnd})^{O(\lg n)}$ time hitting-set for width-w, deg-d ROABP.
  - **Idea**: design a *monomial ordering* φ that isolates a least basis in the coeffs of $A_1(x_{\pi(1)})\ldots A_n(x_{\pi(\mathbf{n})}) =: D(\mathbf{x})$.
  - It's constructed *recursively*; a pair of variables at a time.
  - Then: $D(\mathbf{x}+ \varphi(\mathbf{x}))$ has $(\lg w)$-support rank concentration.
- Nonzeroness of ROABP can be *pushed* to $O(\lg w)$-support.

ROABP ideas

- ROABP is a building block for greater models.
- (Gurjar,Korwar,S.,Thierauf'15) gave a $(wnd)^{\lg(wnd).\, 2^k}$ time hitting-set for sum of k ROABPs.
  - The proof achieves ($2^k.\lg(wnd)$)-support rank concentration as well.
  - Puts *whitebox* PIT in $(wnd)^{O(2^k)}$ time!
  - **Idea:** testing equality of two ROABPs reduces to several ROABP zero tests.
- (Oliveira,Shpilka,Volk'15) gave a $(kn)^{\tilde{O}(n^{(2/3)})}$ time hitting-set for multilinear depth-3.
  - **Idea:** Consider various *projections* of the circuit that look like ROABP.

Contents

- Polynomial identity testing
- ABP
- ROABP ideas
- Deg-insensitive, width-sensitive idea
- Commutative ROABP
- Conjectures for poly-time
- Conclusion

Deg-insensitive, width-sensitive map

- This new idea emerges from a bivariate ROABP.
  - $f = R.A_1(x_1).A_2(x_2).C$, where R resp. C is a *row* resp. a *column*, and A_1, A_2 are $w \times w$ matrices.
  - Thus, $f = \sum_{r \in [w]} g_r(x_1).h_r(x_2)$ in terms of polynomials.
- (Nisan'91) The coeff.matrix $M(f) := (\, \mathrm{coeff}(x_1^{\,i} x_2^{\,j})(f)\,)_{i,j}$ has rank at most w .
- Theorem: Our map $\varphi : (x_1 , x_2) \mapsto (t^w , t^w + t^{w-1})$ keeps f nonzero, assuming *zero*/large characteristic.
- *Proof:* Monomial $x_1^{\,i} x_2^{\,j}$ is mapped to $t^{w(i+j)} (1+ t^{-1})^j$.

Deg-insensitive, width-sensitive map

- Let $k=i+j$ be the *largest* diagonal that contributes in $M(f)$.
  - There can be at most $\mathrm{rk}\ M(f) \leq w$ such monomials in f .
- Then, $f'(t) := f(t^w , t^w + t^{w-1})$ has *leading* contributions from the images $t^{wk} (1+ t^{-1})^j$.
- The *lower* contributions are, at best, from $t^{w(k-1)} (1+ t^{-1})^j$.
- Thus, the monomials $t^{wk} ,t^{wk-1} , \ldots , t^{wk-w+1}$ could only come from the images of the leading monomials.
- Consider the $t^{> -w}$ part of the distinct "polynomials" $(1+ t^{-1})^{j\_a}$ $, a\in[w]$.
  - Prove the "binomial vectors" linearly independent. $\square$

Deg-insensitive, width-sensitive map

- $\varphi : (x_1 , x_2) \mapsto (t^w , t^w + t^{w-1})$ being *deg-insensitive* is what helps in extending it to more variables.
  - Shall recurse on n, halving the variables.
- $f_0 = R.\underbrace{A_1(x_1).A_2(x_2)}\ldots\underbrace{A_{n-1}(x_{n-1}).A_n(x_n)}.C$ be width-w ROABP.
- We'll map the i-th pair to t_i using φ to get:

  $$f_1 = R.\ B_1(t_1)\ \ldots.\ B_{n/2}(t_{n/2}).\ C\ .$$

- Individual degree grows w times. Width unchanged.
- After $(\lg n)$ iterations, we get a *univariate* of degree grown $w^{\lg n} = n^{\lg w}$ times. $\square$

Deg-insensitive, width-sensitive map

- Theorem (Gurjar,Korwar,S.'15): There's a poly(d, $n^{\lg w}$) time hitting-set for width-w, deg-d ROABP (known order, char=0).
- In this constant-width model, poly-sized hitting-sets were *not* known before.

Contents

Commutative ROABP

- Definition: $f = R.A_1(x_1) \ldots . A_n(x_n).C$ is called a width-w commutative ROABP if the matrix product commutes.
  - So, every variable order works.
  - (S.'08) reduced diagonal depth-3 circuit to commutative ROABP.

- Let $\ell := O(\lg w)$. (AGKS'15) can be applied to get a *monomial ordering* φ that isolates a least basis in any sub-ABP $A'_{i1}(x_{i1})\ldots A'_{i\ell}(x_{i\ell}) =: D_\ell$, in $(wd)^{O(\lg \ell)}$ time, such that
  - $D_\ell(\mathbf{x}+ \varphi(\mathbf{x}))$ has ℓ-support rank concentration.

- Applying this idea on all the sub-ABP's of $A_1(x_1) \ldots . A_n(x_n)$ yields a *shift* f', of f , that's ℓ-concentrated.
  - Use commutativity.

Commutative ROABP

- We can use the transformation from (Forbes,Saptharishi, Shpilka'14) on f' to get $O(\ell^2)$-variate *commutative* ROABP f''.
- Applying (AGKS'15) on f'' yields:
- Theorem (Gurjar,Korwar,S.'15): There's a $(wdn)^{O(\lg \lg w)}$ time hitting-set for width-w, deg-d commutative ROABP. □
- This extends the (FSS'14) result of diagonal circuits to all commutative ROABPs.
  - Much better than ROABP.

Contents

- Polynomial identity testing
- ABP
- ROABP ideas
- Deg-insensitive, width-sensitive idea
- Commutative ROABP
- Conjectures for poly-time
- Conclusion

Conjectured poly-time hitting-sets for ROABP

- How could we improve the commutative ROABP hitting-set from $(wdn)^{O(\lg \lg w)}$ to *really* poly-time ?
  - Find a *non-recursive* argument ?

- Let $f = R.A_1(x_1) \dots A_n(x_n).C$ be a width-w commutative ROABP .
  - Assume that the underlying rank is also w .

- **Idea** [(m,w)-implicit hash]: Find a *monomial ordering* φ s.t. for any weight k and *large* ($>m$) subset $M \subseteq \varphi^{-1}(t^k)$:
  - There exists $S \subseteq [n]$ with the restriction M_S having a large image .
  - i.e. $|\ \varphi(M_S)\ | > w$.

Restrict $x_1^{e1} \dots x_n^{en}$ to $\Pi_{i \in S} x_i^{ei}$

Conjectured poly-time hitting-sets for ROABP

- **Conjecture:** There exists (*efficient*) (m,w)-implicit hash φ , with weight-bound $+ m = \text{poly}(wdn)$.
  - Φ maps ind.deg=d, n-var. monomials to t-monomials.

- Theorem (Vaid,S.'15): Conjecture => poly-time hitting-set for commutative ROABP.
  - Extendible to general ROABPs.
  - (Vaid'15) has made partial progress towards Conjecture.

- *Pf sketch:* Consider the *largest* monomials M in f wrt the ordering φ .
  - Let $S\subseteq[n]$ be a subset with $|\ \varphi(M_S)\ | > w$.
  - Since *coeff-matrix* of f wrt $S \times [n]\setminus S$ has rank at most w, we can deduce that $|M| \leq m$. □

Contents

- Polynomial identity testing
- ABP
- ROABP ideas
- Deg-insensitive, width-sensitive idea
- Commutative ROABP
- Conjectures for poly-time
- Conclusion

At the end …

- Solved the case of constant-width ROABP (for char=0).
  - Can such deg-insensitive maps be designed in other cases?
- Gave hitting-sets for commutative ROABP, just shy of poly-time.
- Design efficient (m,w)-implicit hash maps ?

Thank you!