Some Accessible Open Problems

WACT 2016

February 12, 2016

1 Shifted Partial Derivatives

These are questions from Chandan Saha's tutorial on shifted partial derivative and variants.

1. Can one show that $\mathsf{IMM}_{w,d}$, the iterated matrix multiplication polynomial involving d matrices of width w each, cannot be computed by multilinear formulas?

   This would be sufficient to separate non-commutative ABPs and formulas. We know the answer is yes for Det_n but is it also true for IMM?

2. Can one show a super-polynomial lower bound for $\Sigma\Pi\Sigma$ circuits?

   We know strong lower bounds when the fan-in of the linear polynomials at the bottom is *slightly* smaller than n. Can this be improved? One possibility is to attack this via homogeneous depth-5 circuits (suggestion by Ankit Gupta).

3. Can we prove that Sym_d is requires super-polynomial homogeneous formulas (for d large enough)? As a first step, can we show Sym_d require homogeneous $\Sigma\Pi\Sigma\Pi$ circuits of super-polynomial size?

   The best upper-bound, for hom. $\Sigma\Pi\Sigma\Pi$ circuits we have is $2^{O(\sqrt{d})}$, and the best known unbounded depth hom. formula has size $d^{O(\log d)} \cdot \mathrm{poly}(n)$. These results are by Hrubes and Yehudayoff [HY11].

4. Are the *Nisan-Wigderson* polynomial families VNP-complete?

2 Border Complexity of Polynomials

The talks by both Ketan Mulmuley and Michael Forbes looked at the *closure* of computational classes. The following questions are from Ketan's talk.

1. Show that PIT for the closure of VP is in EXPH or even better, in PSPACE.

2. Is $\overline{\mathsf{VP}} \subset \mathsf{VNP}$?

3. Can we solve the problem of *efficient Noether Normalization* for left-right action (i.e. A, B acts on $(M_1, \cdots, M_r)$ as $(AM_1B, \ldots, AM_rB)$) in P, or in quasi-polynomial time?

The following concrete questions were posed by Michael Forbes in his talk.

Consider the class $\Sigma^s \wedge^d \Sigma$ of top fan-in s depth-3 powering circuits (or depth-3 diagonal circuits). Let $\mu(f) = \dim \partial^{<\infty}(f)$.

1. If $\mu(f)$ is small, does that imply that $f \in \overline{\Sigma^s \wedge^d \Sigma}$?
2. If $f \in \overline{\Sigma^s \wedge^d \Sigma}$, then does that imply that $f \in \Sigma^{s'} \wedge^d \Sigma$ where $s' = \mathrm{poly}(s, n, d)$ (or maybe quasi-poly)?
3. What is the order of approximation needed in the closure of diagonal? (that is, what is the largest power of ε that we need to use. Known is $\exp(O(n))$ for general circuits. Can we improve?)
4. For the monomial $x_1 \cdots, x_n$, what is the best *infinitesimal approximation* by $\Sigma \wedge \Sigma$ circuits? We know that the answer is at most 2^{n-1} and is at least $\Omega(2^n/\sqrt{n})$. Can we close the gap?

   And a more general question about hitting sets.

5. Suppose we have a hitting set $\mathcal{H}$ for a class $\mathcal{C}$ of polynomials, can we construct a hitting set for $\overline{\mathcal{C}}$ also?

3 Determinantal complexity, and Kronecker coefficients

Let $\mathrm{dc}(f)$ denote the determinantal complexity of f and let $\overline{\mathrm{dc}}(f)$ refer to the *border determinantal complexity*. The following are some concrete questions in Christian Ikenmeyer's talk.

1. What is the right answer for $\overline{\mathrm{dc}}(\mathsf{Perm}_3)$? We know the answer is at least 5 and at most 7.
2. Is computing Kronecker coefficients in #P? (Stanley's 10th problem [Sta99])
3. Is computing Plethysm coefficients in #P? (Stanley's 9th problem [Sta99])

4 Proof Complexity

One of the major questions in this field is the question of finding lower bounds for Frege or extended-Frege proofs. There were also many other question mentioned during the talks.

1. Is there an "optimal" proof system? That is, do we have a proof system for which proving lower bounds would imply $\mathsf{NP} \neq \mathsf{coNP}$?
2. What can we say about the *proof complexity* of Polynomial Identity Testing?
3. Are there more inter-connections between monotone circuit complexity, various notions of ranks, Sum-of-squares proofs etc., and are there more connections to algebraic complexity theory?

4. Can we find *simple* polynomials $f_1, \ldots, f_k$ such that $1 \in \langle f_1, \ldots, f_k \rangle$ but any certificate requires super-polynomial circuit size? Note that it may be possible that the certificates could have exponentially large degree but it is not clear we have a proof of this even assuming $\mathsf{VP} \neq \mathsf{VNP}$.

5. Suppose you have $f \in \langle f_1, \ldots, f_k \rangle$ and suppose we know that there is a low-degree solution to $f = \sum g_i f_i$. Can we find a certificate of low-degree efficiently?

6. As a related question, can we do Strassen's division elimination in $\mathrm{poly}(s, \log d)$ instead of $s \cdot \mathrm{poly}(d)$?

7. Can we find an f that vanishes on $\{0,1\}^n$ so that any certificate for $f \in \langle x_i^2 - x_i \,:\, i \in [n] \rangle$ requires super-polynomial size? If the answer is no, then $\mathsf{coNP} \subseteq \mathsf{NP}^{\mathrm{PIT}}$ which is unlikely. But the answer to this question is unknown even assuming $\mathsf{VP} \neq \mathsf{VNP}$.

5 Pseudorandomness for bounded memory

1. Can we prove an $2^{\Omega(n)}$ lower bound for AC^0 depth-3? Parity certainly won't work as we have an upper bound of $2^{\sqrt{n}}$ for parity. One approach is to construct optimal PRGs for DNFs.

   A candidate function for this seems to be the support of an ε-biased distribution with some noise added to it.

2. Can one construct a truly optimal hashing (seed-length $O(\log n)$ instead of $\tilde{O}(\log n)$) for the m-balls-to-m-bins problem?

3. Do we have algebraic analogues of Combinatorial Shapes or Fourier Shapes? There are some analogues of the *gradually increasing paradigm* in the some hitting sets for roABPs, but are there more?

   The following concrete question is from Nitin Saxena's talk:

4. Construct a weight assignment Φ of the form $x_i \mapsto t^{w_i}$ with the following property:

   > For every t^d in the range of Φ, let $\Phi^{-1}(t^d)$ denote the set of n-variate monomials that Φ maps to t^d. Then, there must be a set $S_d \subset [n]$ such that if $T = \left\{\prod_{i \in S} x_i^{e_i} \,:\, \mathbf{x}^{\mathbf{e}} \in \Phi^{-1}(t^d)\right\}$ (the restriction of $\Phi^{-1}(t^d)$ to the variables in S) then $|\Phi(T)| > w$.

   If we can find an explicit such map Φ, then turns out that would yield a polynomial sized hitting set for width w commutative roABPs.

6 Polynomial factorization

1. Dvir, Shpilka and Yehudayoff [DSY09] show that given a polynomial $f(\mathbf{x}, y)$ that is computable by a size s circuit of depth d with $\deg_y(f) = r$, then all its roots (factors of the form $(y - g(\mathbf{x}))$) have circuits of $\mathrm{poly}(s, n^r)$ size and depth $d + O(1)$. Can the exponential dependence in r be removed in this case?

2. Can we show that factors of sparse polynomials can be computed by restricted circuits? Say $\Sigma\Pi\Sigma\Pi$ circuits of polynomial sized?

3. Can we derandomize polynomial factorization for restricted classes for which we have PIT/hitting sets?

4. If $P(x_1, \cdots, x_n)$ is a circuit of polynomial size (but $\deg(P)$ could be exponential), can we show that every factor of degree $\mathrm{poly}(n)$ can be computed by small circuits?

5. Suppose we have a PIT for the class VP (say without any constants on wires), is it possible to get PIT for even polynomial sized circuits (of possibly super-polynomial degree)?

7 Determinant and matrix multiplication

Consider the two tasks of computing the determinant of a matrix (with say real entries), and the task of multiplying two matrices. Do these two tasks have the same complexity?

The computational model in mind is a straight-line program where you are allowed to divide, and branch on zero-tests. In this model, are the above two tasks of the same complexity? The best such program known for the determinant seems to be $n^{\omega+1}$, where ω is the exponent of matrix multiplication. Can we say more?

8 Non-commutative identity testing

There were quite a few open problems suggested in the Ankit Garg and K V Subrahmanyam's talks on non-commutative rational identity testing.

1. The algorithm of [GGOW15] was largely analytic rather than algebraic. Are there other analytic polynomial identity tests for other classes?

2. Can we get an coRP algorithm for PIT for non-commutative circuits of possibly exponential degree?

   Conjecture. If $p \neq 0$ is a polynomial computed by a non-commutative circuit of size s (possibly of very large degree), then there exists matrices $B_1, \cdots, B_n$ of dimension $\mathrm{poly}(s)$ such that $p(B_1, \cdots, B_n) \neq 0$.

3. Can we find hitting sets for the problem SINGULAR? Formally, is there a set of $\mathrm{poly}(n)$ tuples of matrices $\{(B_{i1}, \cdots, B_{im})\}_i$ such that for every $(A_1, \cdots, A_m)$ that do not have a shrunk subspace we have

   $$\mathsf{Det}(B_{i1} \otimes A_1 + \cdots B_{im} \otimes A_m) \neq 0$$

   for some i? This would capture many other problems such as bipartite matching, identity testing for non-commutative ABPs etc.

4. What about *syntactic proofs* for rational expressions? Can we prove upper/lower bounds for the degrees of intermediate expressions involved in resolving rational expressions syntactically?

9 Towards PIT for depth-4 circuits with bounded top and bottom fan-in

Ankit Gupta's talk gave a very concrete open problem solving which would get is closer to obtaining a polynomial identity test for depth-4 circuits with bounded top and bottom fan-in.

> **Conjecture.** Let $Q_1, \ldots, Q_m \in \mathbb{C}[x_1, \cdots, x_n]$ be homogeneous polynomials of degree at most r such that for every $i \neq j$, there is a $k \neq i, j$ such that $\mathbb{V}(Q_i, Q_j) \subseteq \mathbb{V}(Q_k)$. Then, $\mathrm{trdeg}_{\mathbb{C}} \{Q_1, \ldots, Q_m\} \leq c_r$, where c_r is a function only of r.

This can be thought of a version of Sylvester-Gallai theorem for varieties. There are many other similar conjectures in the paper [Gup14].

10 PIT and lower bounds for read-k ABPs

Ben Lee Volk's talk presented some natural questions about read-k oblivious ABPs.

1. The algorithm presented degrades quite badly with k. Can we construct a faster PIT? Even for the two-pass varying order case would be very interesting.

2. Can we get a black-box PIT where the order of variables is unknown?

3. Can we get a hierarchy theory for read-k oblivious ABPs? That is, can we show that there is a polynomial computed by read-$(k + 1)$ oblivious ABPs that require exponential sized read-k oblivous ABPs to compute it? Right now the proof separates read-k from read-$k^{O(k)}$ oblivious ABPs. Can this be made tighter?

4. What about the non-oblivious case? Open even for $k = 1$.

5. Are there connections between these hitting sets and techniques to boolean pseudorandomness?

11 Functional Lower Bounds

Ramprasad's talk presented a modest step towards trying to lift arithmetic circuit lower bounds to boolean complexity. A natural open problem there is to remove the individual degree bound required for the Taylor expansion. One concrete question was to prove functional lower bounds for the class of *sums of powers of quadratics* without an individual degree restriction. Formally, it would be great if one could prove a statement of the form:

> There exists a n-variate degree d polynomial F such that any circuit $C = \sum_{i=1}^{s} q_i^{d/2}$, where each q_i is a quadratic, that agrees with f on $\{0,1\}^n$ must satisfy $s = \exp(\Omega(n))$.

This is the simplest example where we do not know how to remove the individual degree restriction on the polynomial computed by C.

References

[DSY09] Zeev Dvir, Amir Shpilka, and Amir Yehudayoff. Hardness-randomness tradeoffs for bounded depth arithmetic circuits. *SIAM J. Comput.*, 39(4):1279–1293, 2009. Preliminary version in the *40th Annual ACM Symposium on Theory of Computing (STOC 2008)*. Pre-print available at `eccc:TR07-121`.

[GGOW15] Ankit Garg, Leonid Gurvits, Rafael Oliveira, and Avi Wigderson. A deterministic polynomial time algorithm for non-commutative rational identity testing. *CoRR*, abs/1511.03730, 2015.

[Gup14] Ankit Gupta. Algebraic geometric techniques for depth-4 PIT & sylvester-gallai conjectures for varieties. *Electronic Colloquium on Computational Complexity (ECCC)*, 21:130, 2014. Pre-print available at `eccc:TR14-130`.

[HY11] Pavel Hrubeš and Amir Yehudayoff. Homogeneous formulas and symmetric polynomials. *Computational Complexity*, 20(3):559–578, 2011. Pre-print available at `arXiv:0907.2621`.

[Sta99] Richard P. Stanley. Positivity problems and conjectures in algebraic combinatorics. In *in Mathematics: Frontiers and Perspectives*, pages 295–319. American Mathematical Society, 1999.