Algebraic Circuit Complexity

Problem Set 3

Due date: November 12^{th}, 2017

Instructions

- The problem set has **6 questions** with a total score of **100 points**.
- You are expected to work independently.
- Solutions are expected as a LaTeX document.
- The deadline is 12th November 2017. You can also submit answers to some (or all) of the questions **any time after the deadline** (a little before the course ends, of course; they need to be graded) for **half the credit**.

  This is to encourage you to solve all the question in these problem sets, even if it is past the deadline.

Questions

Question 1. (10 points) *Let $f(\mathbf{x}) \in \mathbb{Q}[\mathbf{x}]$ is an n-variate degree d polynomial. Suppose you are told that* $\dim \{\partial^{=*}(f)\} \leq r$ *(the dimension of partial derivatives of* all *orders). Prove that for any partition $\mathbf{x} = \mathbf{y} \sqcup \mathbf{z}$, the partial derivative matrix with respect to this partition has rank at most* $\text{poly}(n, d, r)$.

What can you say about the converse?

Question 2. (10 points) *Suppose you are given two sparse n-variate polynomials $f(\mathbf{x})$ and $g(\mathbf{x})$ and you are promised the individual degree of f and g with respect to each variable is at most 42. Construct a* deterministic *polynomial time algorithm to check if f and g have a non-trivial gcd.*

Question 3. (10 points) *Say we have an* algebraic formula *(possibly non-homogeneous) of size s computing a homogeneous n-variate degree d polynomial $f(\mathbf{x})$. Show that $f(\mathbf{x})$ can also be computed by a* homogeneous algebraic formula *of size at most*

$$\operatorname{poly}\left(s, \binom{d + \log s}{d}\right).$$

Conclude that the polynomial $\mathrm{ESYM}_d(\mathbf{x})$ for $d = O(\log n)$ has a polynomial-sized homogeneous algebraic formula *computing it.*

Prior to this result, it was conjectured that ESYM_d cannot have polynomial-sized homogeneous formulas for any non-constant d.

Question 4. (10 points) *Suppose you are given a blackbox that computes an n-variate degree $\leq d$ polynomial $f(x_1, \ldots, x_n) \in \mathbb{Q}[\mathbf{x}]$. You are told that this polynomial has at most s monomials.*

Using just $\operatorname{poly}(s, d, n)$ evaluations, reconstruct the polynomial $f(x_1, \ldots, x_n)$ (i.e. figure out each non-zero monomial of f and its coefficient).

Question 5. (20 points) *In class, we looked briefly at Kayal's lower bound for $\Sigma \bigwedge \Sigma\Pi^{[t]}$ circuits computing a monomial $x_1 \ldots x_n$. For this, we worked with the dimension of shifted partial derivatives,*

$$\Gamma_{k,\ell}(f) := \dim \left\{ \mathbf{x}^{=\ell} \partial^{=k}(f) \right\}$$

and proved in class that for any k, ℓ we have:

$$\Gamma_{k,\ell}(Q^d) \leq \binom{n + \ell + (t-1)k}{n} \quad , \quad \text{if } \deg(Q) = t,$$

$$\Gamma_{k,\ell}(x_1^{e_1} \ldots x_n^{e_n}) \geq \binom{n}{k}\binom{n - k + \ell}{n - k} \quad , \quad \text{if } e_1, \ldots, e_n \geq 1.$$

1. **(10 points)** *Prove that if $\ell = tn$, there we can choose $k = \epsilon n/t$ for suitably small constant $\epsilon > 0$ such that*

   $$\frac{\binom{n}{k}\binom{n-k+\ell}{n-k}}{\binom{n+\ell+(t-1)k}{n}} = 2^{\Omega(n/t)}.$$

   You might want to use the fact that $(n-b)^{a+b} \leq \frac{(n+a)!}{(n-b)!} \leq (n+a)^{a+b}$ for any $a, b \geq 0$.

2. **(10 points)** *Formally prove that if $0 \neq f = Q_1^d + \cdots + Q_s^d$ with $\deg Q_i = t$ for all i, then there must be some non-zero monomial of f of support-size at most $O(t \log s)$.*

Question 6. (40 points) *In this problem, we'll extend the previous problem from $\Sigma \bigwedge \Sigma\Pi^{[t]}$ circuits to circuits of the form*

$$C = \sum_{i=1}^{s} m_i \cdot Q_i^d$$

where each m_i is a monomial, and $\deg(Q_i) = t$. These are also referred to as $\Sigma m \bigwedge \Sigma\Pi^{[t]}$ circuits.

For any $i \in [n]$, define the operator $\Delta_i : \mathbb{F}[\mathbf{x}] \to \mathbb{F}[\mathbf{x}]$ as $\Delta_i(f) = x_i \cdot \frac{\partial f}{\partial x_i}$. We shall use $\Delta^{=k}$ to refer to the span of k-th order operators using these Δ_i's. That is,

$$\Delta^{=k}(f) = \operatorname{span}\left\{\Delta_{i_1} \circ \cdots \circ \Delta_{i_k}(f) \ : \ i_1, \ldots, i_k \in [n]\right\}.$$

For parameters k, ℓ, define $\tilde{\Gamma}_{k,\ell}(f) = \dim\left\{\mathbf{x}^{=\ell}\Delta^{=k}(f)\right\}$.

Some of these expressions are slightly different from the previous problem as $\Delta^{=k}$ also accounts for a degree k monomial, but this should not drastically change any calculations.

1. **(15 points)** *Suppose Q is a homogeneous polynomial of degree t, and m is an arbitrary monomial. Show that for any $d \geq 0$,*

$$\tilde{\Gamma}_{k,\ell}(m \cdot Q^d) \leq \binom{n + \ell + kt}{n}.$$

   Also show that if $f = (x_1 + 1)^{e_1} \cdots (x_n + 1)^{e_n}$ where $e_1, \ldots, e_n \geq 1$, then

$$\tilde{\Gamma}_{k,\ell}(f) \geq \binom{n}{k}\binom{n - k + \ell}{n - k}.$$

2. **(5 points)** *Construct an explicit hitting set of size $\operatorname{poly}(n, d, s)^{O(t \log s)}$ for the class of $\Sigma m \bigwedge \Sigma\Pi^{[t]}$ circuits.*

3. **(20 points)** *Show that the task of checking if a given degree t polynomial $Q(\mathbf{x})$ divides a given sparse polynomial $f(\mathbf{x})$ reduces to PIT of circuits as above.*

   Formally, suppose you are given a polynomial $f(\mathbf{x})$ that has at most s monomials, and a polynomial $Q(\mathbf{x})$ that has degree at most t. Construct a circuit C of the form $\Sigma m \bigwedge \Sigma\Pi^{[t]}$, in polynomial time, such that $C \equiv 0$ if and only if Q divides f.

   (Hint: Strassen)