CS748 - ARITHMETIC CIRCUIT COMPLEXITY
NITIN SAXENA

ASSIGNMENT 1

POINTS: 50

DATE GIVEN: 17-JAN-2019 DUE: 31-JAN-2019

Rules:
- You are strongly encouraged to work *independently*. That is the best way to understand & master the subject.
- Write the solutions on your own and honorably *acknowledge* the sources if any. `http://cse.iitk.ac.in/pages/AntiCheatingPolicy.html`
- Submit your solutions, before time, to your TA. Preferably, give the TA a printed copy of your LaTeXed or Word processed solution sheet.
- Clearly express the fundamental *idea* of your proof/ algorithm before going into the other proof details. The distribution of partial marks is according to the proof steps.
- There will be a penalty if you write unnecessary or unrelated details in your solution. Also, do not repeat the proofs done in the class.
- Problems marked '0 points' are for practice.

Question 1: *[6 points]* Consider the class of polynomial families with circuit complexity $O(1)$. Show that it has *uncomputable* problems.

Question 2: *[6 points]* Let $\mathbb{F}_p$ be a finite field. Show that the question of existence of a zero of a system of *quadratic equations* is NP-complete.

Question 3: *[10 points]* For $n, d \in \mathbb{N}$, show that there exists a d-degree n-variate polynomial f, over the finite field $\mathbb{F}_2$, such that any circuit computing f has size $\Omega\left(\sqrt{\binom{n+d}{d}}\right)$.

(*Hint:* There is a counting argument.)

Question 4: *[13 points]* Show a homogenization theorem for ABPs: Prove that if f has an ABP of size s then there is a $O(sd)$-size ABP to compute the degree d homogeneous part of f.

Question 5: *[11+4 points]* Show that the zeros of a polynomial are "few": For a finite subset $S \subseteq \mathbb{F}$, and a degree d polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ show that

$$\mathrm{Pr}_{\alpha \in S^n}\left[f(\alpha) = 0\right] \leq \frac{d}{|S|}.$$

What can you say when the polynomial f is over a commutative ring R that is *not* a field?

Question 6: *[0 point]* Show that a size s formula can only compute a polynomial of degree $O(s)$.

What can you say for circuits?

Question 7: *[0 point]* Show that VP=VNP implies P/poly = NP/poly.

What do you do when the circuits use large integers as constants?

Question 8: *[0 point]* Show that, over rationals, the ring generated by symmetric polynomials is equal to the ring generated by the power-sums $p_i = \sum_{j \in [n]} x_j^i$.

Question 9: *[0 point]* Is the ABP model same as formulas (up to poly-size blowup)?

□□□