CS748 - ARITHMETIC CIRCUIT COMPLEXITY
NITIN SAXENA

ASSIGNMENT 4

POINTS: 40

DATE GIVEN: 06-APR-2019 DUE: 18-APR-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: *[15 points]* Read about the complexity class #P/poly. #P is the class of boolean functions F such that there is a non-deterministic poly-time Turing machine M: for every binary input x, $F(x) =$ number of accepting paths in $M(x)$.

If we allow M to also take poly($|x|$)-bits of an 'advice' string, then F is said to be in #P/poly.

Consider a polynomial, in $\mathbb{Z}[\mathbf{x}]$,

$$f(x_1, \ldots, x_n) =: \sum_{\mathbf{e}\in\mathbb{N}^n} f_{\mathbf{e}}\mathbf{x}^{\mathbf{e}}, \qquad f_{\mathbf{e}} \in \{0, 1\}\,.$$

Show that, if the function $F : \mathbf{e} \mapsto f_{\mathbf{e}}$ is in #P/poly, then $f \in$ VNP.

Question 2: *[6 points]* Show that the Nisan-Wigderson polynomial is in VNP.

Question 3: *[8 points]* For a finite field $\mathbb{F}$, PIT is the question of testing whether a circuit C, given in $\mathbb{F}[\mathbf{x}]$, is *identically* zero. We saw that PIT is in BPP.

What can you say about the problem to test: Whether $C(\mathbf{a}) = 0$, $\forall \mathbf{a} \in \mathbb{F}^n$?

Question 4: *[11 points]* Consider a circuit family: circuit $C \in \mathbb{F}_q[\mathbf{x}]$ of size s. For this family, show the *existence* of a hitting-set generator with degree $d(s) =$poly(s). Try for the best possible $d(s)$.

Question 5: *[0 points]* Show that, in a homogeneous linear system of equations, there is always a nonzero solution if the number of variables exceeds the number of constraints.

Question 6: *[0 points]* Show that for a circuit of size resp. degree $\leq s$, the factors have size poly(s).

Question 7: *[0 points]* Complete the analysis of randomized PIT algorithm in the case of rational field $\mathbb{Q}$. In particular, the part where we go modulo a *random* prime.

Question 8: *[0 points]* Show that $\mathrm{IMM}_{n,d}$ has homogeneous depth-4 complexity $(nd)^{\Theta(\sqrt{d})}$.

□□□