COMP 531 - Fall 2022 - Assignment 3

Due: Nov 11, 11:59pm

- In solving these questions you may only consult the lecture notes, and the Sipser book, but you need to provide citations in that case.
- Each student must find and write their own solution. Copying solutions from any source, completely or partially, allowing others to copy your work, will not be tolerated, and will be reported to the disciplinary office. You are allowed to discuss the problems with each other without revealing your solution to each other.
- You must submit your solutions as **one readable pdf file** to mycourses.
- Your grade will be based on the mathematical correctness of your solution as well as the quality of your presentation.

---

1. Prove that with $\text{Maj}, \vee, \wedge, \neg$ gates (arbitrary fan-in), there is a polynomial size, $O(1)$ depth circuit that computes Parity.
2. A function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ naturally corresponds to a bipartite graph on 2×2^n vertices. More formally there are two parts each with 2^n elements labeled with $\{0,1\}^n$, and there is an edge between x from part I and y from part II, if and only if $f(x,y) = 1$. This graph is called k-Ramsey if there do not exist $A, B \subseteq \{0,1\}^n$ with $|A| = |B| = k$, and $b \in \{0,1\}$, with $f(x,y) = b$ for all $x \in A, y \in B$.
    (a) Prove that with probability at least $\frac{1}{2}$ a random function defines a $O(n)$-Ramsey graph. More precisely, show that there is a universal constant $c > 0$ (does not depend on n) such that a random function is cn-Ramsey with probability at least $1/2$.
    (b) Show that if f has an AC circuit of size s, and depth d, then it is not $2^{\Omega(n/\log^d(s))}$-Ramsey.

3. Follow the Razborov-Smolensky proof strategy to show that Parity and Maj do not have polynomial size $\mathrm{AC}^0[\mathrm{mod}\ 3]$ circuits. These are circuits similar to AC^0 but additionally "mod 3" gates with arbitrary fan-in are allowed. The "mod 3" gates output 0 if and only if the number of 1's on the input wires is divisible by 3.

   Hint: Try to work in the field $\mathbb{F}_p$ (p is a prime) for an appropriate value of p. Recall that $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ along with operations addition and multiplication mod$p$ forms a field. Recall that for every $a \in \mathbb{F}_p$ we have $a^p = a$.)

4. Give a Boolean $A_{m \times m}$, let $\mathrm{Cov}(A)$ denote the smallest number of all-1 submatrices of A that cover all 1-entries of A. Let $\mathrm{Cov}_{\&}(A)$ be the smallest number t such that A can be written as an entry-wise $\wedge$ of t Boolean matrices $A_1, \dots, A_t$ such that $\mathrm{Cov}(A_i) \leq t$ for all i.

   Let G be a bipartite $m \times m$ graph with $m = 2^n$. We can represent G with two different functions:

   Binary: Identify the vertices of G with vectors in $\{0,1\}^n$, and represent G with the function

   $$f_G : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

   defined by $f_G(x, y) = 1$ iff x and y are adjacent in G. Here, f_G corresponds to the so-called bi-adjacency matrix of G.

   Unary: Let $e_1, \dots, e_m$ be the standard basis vectors in $\{0,1\}^m$. Define

   $$g_G : \{e_1, \dots, e_m\} \times \{e_1, \dots, e_m\} \to \{0,1\}$$

   where $g_G(e_i, e_j) = 1$ iff i and j are adjacent in G. We consider g_G as a function on $2m$ variables $(u_1, \dots, u_m) \in \{0,1\}^m$ and $(v_1, \dots, v_m) \in \{0,1\}^m$.

   (a) Let C be an AC circuit (with input variables $x_1, \dots, x_n, y_1, \dots, y_n$) computing f_G. Prove that one can replace each input *literal* by an OR of variables $u_1, \dots, u_m$ and $v_1, \dots, v_m$ so that the resulting *monotone* circuit computes g_G.

   (b) Let $\mathrm{cnf}(G)$ denote the minimum number of clauses in a monotone CNF representing g_G. Prove that

   $$\mathrm{cnf}(G) = \mathrm{Cov}(1 - f_G).$$

   Note that $1 - f_G = f_{\overline{G}}$.

(c) Use the previous parts to obtain a lower bound on the size of the smallest CNF (not necessarily monotone) that represents f_G where G is the (bipartite) complement of a perfect matching.

(d) Show that Boolean $m \times m$ matrices A with $\mathrm{Cov}_{\&}(A) \geq m^{\Omega(1)}$ exist.

(e) Suppose that we can find an explicit Boolean matrix $A_{m \times m}$ with $\mathrm{Cov}_{\&}(A) \geq m^{\Omega(1)}$. How would we use part (a) and the matrix A to obtain a strong explicit lower bound against depth 3 AC circuits?