Final Exam

Time: 150+15 mins Total Scores: 115

Question 1.(20 points). Decide if the following statements are TRUE(T) or FALSE(F) or UNKNOWN(U). You don't need to prove your answers.

(a) The class of non-regular languages is closed under the operation of complementation.

(b) The intersection of a regular language and a context-free language must be regular.

(c) The class of non-context-free languages is closed under intersection.

(d) Let $L = \{a^m b^n \mid m \neq n^2 + 1\}$. L is a regular language.

(e) There exists a language A such that both A and $\overline{A}$ are not Turing-recognizable.

(f) If A and B are two Turing-recognizable languages, then $A \backslash B = A \cap \overline{B}$ is also Turing-recognizable.

(g) If $\mathbf{NP} = \mathbf{coNP}$, then $\mathbf{BPP} \subseteq \mathbf{NP}$.

(h) The language no-PATH $= \{(G, s, t) \mid$ there is no path from s to t in $G\}$, is in $\mathbf{NL}$.

(i) In our proof for TQBF $\in$ $\mathbf{IP}$, the sumcheck protocol we designed has acceptance probability 1 for the completeness part.

(j) The XOR of $(\log n)^{\log \log n}$ bits is computable by $\mathbf{AC}^0$ circuits of size $\texttt{poly}(n)$.

◀

Solution. TFFFT FTTTF. ◁

Question 2.(15 points). Let $X = \{\langle M, w\rangle \mid M$ is a single tape TM that never modifies the portion of the tape that contains the input $w\}$

(a) (8 points) Is X decidable by any Turing Machines? Prove your answer.

(b) (7 points) Is there a (non-uniform) circuit family that can compute X? Prove your answer.

◀

Question 3.(15 points). 本题与 22 年第 3 题基本相同，将其中 a uniform $\mathbf{AC}^0$ family 改为 a non-uniform $\mathbf{AC}^0$ family. ◀

Question 4.(12 points). There are two creatures both claiming to be oracles for the Independent Set decision problem. Given any undirected graph and an integer k, each of them will give a yes/no answer (i.e., where there is a independent set of size $\geq k$) in constant time. Furthermore, they always give the same answer for the same instance. However, there is only one true oracle and the other is an impostor.

Suppose you have a large undirected graph on which the two creatures give different answers. Is it possible to expose the liar within time polynomial in the size of the graph? Explain your answer. ◀

Solution. Possible. Use the reduction from decision to search problem. ◁

Question 5.(15 points). Two groups in PKU are building teams for the next competition. Each team is comprised of n students and 1 professor. k topic areas of CS are included in this competition. For each topic areas, a student is either an expert or not.

It is guranteed that Team1 led by Prof1 will win if it includes at least one student expert from each of the k topic areas(irrespective of what Team2 does). Otherwise, team2 will win.

There are $2n$ students and the professors do their selection as follows. First, students are arbitarily organized into an ordered sequence of pairs $P_1, P_2, \cdots, P_n$. Prof1 starts by picking one student from P_1 (with the other student in P_1 going to Prof2), then Prof2 picks one student from P_2 (with the other student in P_2 going to Prof1), and so on, until all students are assigned to some team.

Consider the language `SPC` defined as follows:

$$\texttt{SPC} = \{\langle P_1, P_2, \cdots, P_n, k\rangle \mid \text{Team1 has a winning strategy for the ordered sequence of student pairs } P_1, P_2, \cdots, P_n\}$$

Here each P_i includes a student pair (a, b) and their expert areas, i.e.

$$P_i = \{(a_1, a_2), \{\text{expert areas of } a_1\}, \{\text{expert areas of } a_2\}\}$$

(a) (5 points) Is `SPC` in **PSPACE**? Prove your answer.

(b) (10 points) Is `SPC` **PSPACE**-complete? Prove your answer.

Notice: The definition of TQBF is as the following:

$$\text{TQBF} = \{\langle\psi\rangle \mid \psi \text{ is a true quantified boolean formula of the form } \exists x_1 \forall x_2 \exists x_3 \forall x_4 \cdots Q_n x_n\ \phi(x_1, x_2, \cdots, x_n) \text{ where } \phi \text{ is a boolean formula.}\}$$

◀

Question 6.(18 points).

(a) (4 points) Is it true that **BPL** $\subseteq$ (non-uniform)**AC**? Prove your answer.

(b) (4 points) Is it true that **BPL** $\subseteq$ (non-uniform)$\mathbf{AC}^1$? Prove your answer.

◀

Question 7.(20 points). Define MA to be a subset of **IP**, such that we can only allow the prover to send one message z first and the verifier can then verify use some randomness y. Specifically, the definition is as the following.

A language L is in MA if there exists a polynomial-time deterministic TM M and polynomial p, q such that for every input string x of length n,

- (completeness) if $x \in L \implies \exists z \in \{0,1\}^q$ $s.t.$ $\Pr_{y \in_R \{0,1\}^p}[M(x,y,z) = 1] \geq 2/3$;
- (soundness) if $x \notin L \implies \forall z \in \{0,1\}^q$ $s.t.$ $\Pr_{y \in_R \{0,1\}^p}[M(x,y,z) = 0] \geq 2/3$.

(a) (10 points) Is it true that MA $\subseteq$ AM[2]? Prove your answer.

(b) (10 points) If we change the completeness of MA to have success probability 1 instead of 2/3(i.e. perfect completeness), then does this change the definition of MA? Prove you answer.

注: 原本的第 7 题与 22 年第 7 题相同, 一位同学在考前向助教询问过这道题, 故临时更换题目. ◄