

Final

Out: May 24

Due: 4pm May 31

This is the final exam. You may consult any of the course materials and the text (Papadimitriou), but not any other source or person. There are 4 problems on two pages. Please attempt all problems, and write clear, concise solutions. Good luck!

Instructions for turning in the exam: Please bring your exam to Diane Goodfellow in Jorgensen 266 any time before the deadline.

1. Define \mathbf{L}_i to be the class of languages decidable by a deterministic Turing Machine using at most $O(\log^i n)$ space, and \mathbf{NL}_i to be the class of languages decidable by a non-deterministic Turing Machine using at most $O(\log^i n)$ space. The classes \mathbf{L}_1 and \mathbf{NL}_1 should be familiar – they are just deterministic logspace and nondeterministic logspace, respectively.
 - (a) Show that for all i , $\mathbf{NC}_i \subseteq \mathbf{L}_i$.
 - (b) Show that for all i , \mathbf{NL}_i has $O(\log^{2i} n)$ depth, fan-in 2, Boolean circuits. Your circuits do not need to be uniform.
 - (c) It is tempting to try to show that for all i , $\mathbf{NL}_i \subseteq \mathbf{NC}_{2i}$ (since this holds for $i = 1$). Show that this would solve a major open problem. Try to give the strongest implication you can, i.e., if the containment implies A , and A implies B , you should pick A .
2. Recall the problem VC-DIMENSION from Problem Set 6, which you showed to be Σ_3^P -complete. Here we use the shorthand $VC(C)$ to mean “the VC dimension of the collection of subsets succinctly defined by circuit C .”

In this problem you will show that VC-DIMENSION can be *approximated* within a factor 2 in the class \mathbf{AM} . The precise meaning of this statement is as follows: given mutual input (C, k) , Arthur and Merlin engage in a constant-round interactive protocol. If $VC(C) \geq k$, then Merlin has a strategy that causes Arthur to accept with probability 1; if $VC(C) < k/2$ then Arthur rejects with probability at least $1/2$ no matter what Merlin does. The behavior of the protocol when $k/2 \leq VC(C) < k$ is not specified.

Your task is to describe an Arthur-Merlin protocol meeting the above requirements. You may use the following lemma:

Lemma 1 *Let $\mathcal{S} = \{S_1, S_2, \dots, S_m\}$ be a collection of subsets of a finite universe U . If for some subset $X \subseteq U$ we have:*

$$\Pr_{X' \subseteq X} [\exists S_i \in \mathcal{S} \text{ for which } S_i \cap X = X'] \geq 1/2,$$

then there exists a subset $X'' \subseteq X$ with $|X''| \geq |X|/2$ that is shattered by \mathcal{S} . (The probability is taken over X' chosen uniformly from among all subsets of X .)

3. Recall the definition of the class $\mathbf{S}_2^{\mathbf{P}}$ from problem 2 on Problem Set 6. Parts (a) – (c) of that problem show that $\mathbf{S}_2^{\mathbf{P}}$ lies between $\mathbf{P}^{\mathbf{NP}}$ and $(\Sigma_2^{\mathbf{P}} \cap \Pi_2^{\mathbf{P}})$. In this problem you will improve the upper bound by showing that $\mathbf{S}_2^{\mathbf{P}} \subseteq \mathbf{ZPP}^{\mathbf{NP}}$.

- (a) Let M be an $N \times N$ matrix with 0/1 entries, and let S be a subset of $[N]$ (the integers from 1 to N). Consider choosing a random multiset I by sampling m elements uniformly from S , with replacement. Show that

$$\Pr \left[\exists j \text{ such that } \left(\Pr_{i \in S} [M(i, j) = 0] \leq 1/2 \text{ and } \forall i \in I M(i, j) = 0 \right) \right] \leq N2^{-m}.$$

Hint: Fix a j for which $\Pr_{i \in S} [M(i, j) = 0] \leq 1/2$. For that j , what is

$$\Pr[\forall i \in I M(i, j) = 0]?$$

- (b) Consider the following procedure, whose input is an $N \times N$ matrix M with 0/1 entries:

Step 0: set $S_0 = [N]$; set $\ell = 0$

Step 1: sample I_ℓ of size $m = 2 \log N$ from S_ℓ as in part (a)

Step 2: select $j_\ell \in [N]$ for which $\forall i \in I_\ell M(i, j_\ell) = 0$; if such a j_ℓ doesn't exist, halt

Step 3: set $S_{\ell+1} = \{i : M(i, j_k) = 1 \text{ for all } k = 0, 1, \dots, \ell\}$

Step 4: if $|S_{\ell+1}| = 0$, then halt; otherwise increment ℓ and go to Step 1

Argue that with probability at least $3/4$, the procedure halts after at most $\log N$ steps.

Hint: how large is $S_{\ell+1}$ compared to S_ℓ (with high probability)?

- (c) Fix a language $L \in \mathbf{S}_2^{\mathbf{P}}$. Use part (b) to give a randomized, polynomial-time procedure to decide L , with access to an \mathbf{NP} oracle. The procedure should output “fail” with probability at most $1/2$, and otherwise correctly declare either “ $x \in L$ ” or “ $x \notin L$ ”. Conclude that $\mathbf{S}_2^{\mathbf{P}} \subseteq \mathbf{ZPP}^{\mathbf{NP}}$.

Hint: use the result from problem 3(b) on Problem Set 5 to implement the sampling step. Recall the “matrix” interpretation of $\mathbf{S}_2^{\mathbf{P}}$ in which $x \in L$ implies an all-ones row and $x \notin L$ implies an all-zeros column.

4. Prove that if $\mathbf{PSPACE} \subseteq \mathbf{P}/\text{poly}$, then $\mathbf{PSPACE} = \mathbf{MA}$. You may use the following fact: in the proof that $\mathbf{IP} = \mathbf{PSPACE}$, the function describing what message the (honest) prover should send in each round (as a function of the mutual input and the messages seen so far) is computable in polynomial space.