

Problem Set 5

Out: May 3

Due: May 10

Reminder: you are encouraged to work in groups of two or three; however you must turn in your own write-up and note with whom you worked. You may consult the course materials and text (Papadimitriou). Please attempt all problems.

1. MINIMUM TRUTH TABLE CIRCUIT (MTTC) is the language of pairs (x, k) for which (1) $|x|$ is a power of 2, and (2) there exists a Boolean circuit of size at most k computing the function whose truth table is x . Observe that MTTC is in **NP**.
 - (a) Show that $\text{MTTC} \in \mathbf{P}$ implies $\mathbf{BPP} = \mathbf{ZPP}$.
 - (b) Show that $\mathbf{NP}^{\mathbf{BPP}} \subseteq \mathbf{ZPP}^{\mathbf{NP}}$.

Hint: for both parts you may want to refer to Shannon's theorem from Lecture 5.

2. CNFs and DNFs. Recall that a Boolean formula is said to be in *3-CNF* form if it is the conjunction of *clauses*, with each clause being the disjunction of at most 3 literals. A Boolean formula is said to be in *3-DNF* form if it is the disjunction of *terms*, with each term being the conjunction of at most 3 literals.

Describe a polynomial-time computable function that is given as input a fan-in two (\wedge, \vee, \neg) -circuit $C(x_1, x_2, \dots, x_n)$, and produces a 3-CNF Boolean formula ϕ on variables x_1, x_2, \dots, x_n and additional variables z_1, z_2, \dots, z_m for which

$$\exists z_1, z_2, \dots, z_m \phi(x_1, x_2, \dots, x_n, z_1, z_2, \dots, z_m) = 1 \Leftrightarrow C(x_1, x_2, \dots, x_n) = 1.$$

Also, describe a polynomial-time computable function that is given as input a fan-in two (\wedge, \vee, \neg) -circuit $C(x_1, x_2, \dots, x_n)$, and produces a 3-DNF Boolean formula ϕ on variables x_1, x_2, \dots, x_n and additional variables z_1, z_2, \dots, z_m for which

$$\forall z_1, z_2, \dots, z_m \phi(x_1, x_2, \dots, x_n, z_1, z_2, \dots, z_m) = 1 \Leftrightarrow C(x_1, x_2, \dots, x_n) = 1.$$

Hint: identify the z variables with the gates of C .

3. Approximate counting and sampling with an **NP** oracle. For every n, k (positive integers, with $k \leq n$), there is a multiset $\mathcal{H}_{n,k}$ of functions $h : \{0, 1\}^n \rightarrow \{0, 1\}^k$, called an "*n-wise independent hash family*". This multiset comes equipped with a probabilistic procedure that runs in time $\text{poly}(n)$ and outputs a uniformly chosen h from $\mathcal{H}_{n,k}$, in the form of a circuit for h of size $\text{poly}(n)$. These functions behave like random functions from n bits to k bits in the following sense:

Lemma 5.1 For every set $S \subseteq \{0, 1\}^n$ and every $y \in \{0, 1\}^k$:

$$\Pr_{h \in \mathcal{H}_{n,k}} \left[|\{x : x \in S \wedge h(x) = y\}| > 2 \cdot \frac{|S|}{2^k} \right] \leq 2^{-2n},$$

provided that $2^k \leq 4|S|/n^4$.

Note that for a random function h from n bits to k bits, the expected size of

$$\{x : x \in S \wedge h(x) = y\}$$

is $|S|/2^k$; the lemma says that with high probability, the same set with respect to a function h drawn uniformly from $\mathcal{H}_{n,k}$ does not exceed this expected size by more than a factor of two.

In the problems below, the input is a set $S \subset \{0, 1\}^n$ given *implicitly* by a circuit $C : \{0, 1\}^n \rightarrow \{0, 1\}$ for which $C(x) = 1$ iff $x \in S$. You can think of C as an instance of CIRCUIT SAT, and then the questions below concern the problems of estimating the number of satisfying assignment, and sampling from them, respectively.

- (a) Describe a probabilistic polynomial-time procedure, with access to an **NP** oracle, that with probability at least $7/8$ outputs an integer k for which $2^k < \frac{|S|}{n^4} \leq 2^{k+2}$. Hint: argue that deciding whether an implicitly given set has size *at least* s , for polynomially-large s , is in **NP**, and then perform an experiment for each $k = 1, 2, 3, \dots$
- (b) Describe a probabilistic polynomial-time procedure, with access to an **NP** oracle, that outputs “fail” with probability at most $7/8$ and otherwise outputs an exactly uniformly distributed element of S . Hint: suppose a notebook has L lines on every page, with an enumeration of the elements of a set S are written on a subset of the lines in the notebook. Consider selecting a random page and a random line on that page, and outputting the element written on that line, or “fail” if the line is empty. What is the probability of outputting a given element of S ? What is the probability of outputting “fail”?