# Problem Set 1

- Due date: **23 Feb, 2026** (released on 10 Feb, 2026).
- Turn in your problem sets electronically (PDF; either LaTeXed or scanned etc.) via email. If you submit a LaTeX document, you will get an additional **5 points**.
- The points for each problem is indicated on the side. The total for this set is **65** points.
- The problem set has a fair number of questions so please do not wait until close to the deadline to start on them. Try and do one question every couple of days.
- Collaboration with other students taking this course is encouraged, but collaboration with others is not allowed. Irrespective of this, all writeups must be done individually and must include names of all collaborators (if any).
- The use of LLMs for this problem set is NOT allowed.
- Referring to sources other than the text book and class notes is STRONGLY DISCOURAGED. But if you do use an external source (eg.,other text books, lecture notes, or any material available online), ACKNOWLEDGE all your sources (including collaborators) in your writeup. This will not affect your grades. However, not acknowledging will be treated as a serious case of academic dishonesty.

---

0. **[Create homepage]** (5)

   Create a personal homepage for yourself and give the URL. (It doesn't have to be hosted on the STCS / TIFR servers. You are welcome to use Google Sites, or Github Pages, or Bitbucket Pages.)

1. **[Some closure propreties]** (3 + 2 + 3)

   For $x, y \in \{0,1\}^n$, we shall say $x \succeq y$ to mean that $y_i = 1$ implies $x_i = 1$. A function $f : \{0,1\}^n \to \{0,1\}$ is said to be *monotone* if $x \succeq y \implies f(x) \geq f(y)$.

   (a) Let $k$ be a constant. Suppose $L_1, \ldots, L_k \in \mathsf{coNP}$ and $f : \{0,1\}^k \to \{0,1\}$ is a monotone function. Define the language

   $$\tilde{L} = \left\{ x \in \{0,1\}^* \ : \ f(b_1, \ldots, b_k) = 1 \text{ where } b_i = \mathbb{1}(x \in L_i) \right\}.$$

   Show that $\tilde{L}$ is also in $\mathsf{coNP}$.

   (b) Let $k$ be a constant. Suppose $L_1, \ldots, L_k \in \mathsf{NP} \cap \mathsf{coNP}$ and $f : \{0,1\}^k \to \{0,1\}$ be *any* function. Define the language

   $$\tilde{L} = \left\{ x \in \{0,1\}^* \ : \ f(b_1, \ldots, b_k) = 1 \text{ where } b_i = \mathbb{1}(x \in L_i) \right\}.$$

   Show that $\tilde{L}$ is also in $\mathsf{NP} \cap \mathsf{coNP}$.

   (c) In your answers above, where did you use that $k$ is a constant? If you want to extend the arguments above for non-constant $k$, what additional assumptions would yield a similar conclusion?

2. **[Equations that have integer solutions]** (5 + 2)

(a) Consider the following language

$$L = \left\{ (a,b) \;:\; a,b \in \mathbb{Z}\,, \begin{array}{c}\text{there exists integers } x,y \\ \text{such that } x^2 + ay + b = 0\end{array} \right\}$$

Here, the inputs $a, b$ are provided in binary.

Prove that $L \in \mathsf{NP}$.

(b) Consider the following language

$$L' = \left\{ (a,b,c) \;:\; a,b,c \in \mathbb{Z}\,, \begin{array}{c}\text{there exists integers } x,y,z \\ \text{such that } x^3 + ay^2 + bz + c = 0\end{array} \right\}.$$

Why is it unclear if the above problem is in $\mathsf{NP}$?

3. **[Circuit size for any function]** (4 + 3 + 3)

Throughout this question, we will use 'size' to refer to the number of gates.

In this question, you will show that any function $f : \{0,1\}^n \to \{0,1\}$ is computable by a circuit of size $O(2^n/n)$.

(a) Let $k \leq n$. For any $x \in \{0,1\}^k$, define $y_a \in \{0,1\}^{2^{n-k}}$ as $(y_a)_b = f(ab)$ for all $b \in \{0,1\}^{n-k}$.

Let $g : \{0,1\}^k \to \{0,1\}^{2^{n-k}}$ be defined as $g(a) = y_a$ for all $a \in \{0,1\}^k$. Show that $g$ is computable by a circuit of size $O\left(2^k \cdot 2^{2^k} + 2^{n-k}\right)$.

(b) Use the above, and an appropriate Lookup function to show that $f$ can be computed by a circuit of size $O\left(2^k \cdot 2^{2^k} + 2^{n-k}\right)$.

(c) Choose an appropriate value of $k$ so that the above bound is $O(2^n/n)$.

4. **[Block-respecting TMs]** (10)

Hat-tip: This problem is from Ryan O'Donnell's complexity course

Let $B : \mathbb{N} \to \mathbb{N}$ be a "reasonable" function (increasing, time-constructible, yada yada). A deterministic Turing machine $M$ is said to be *B-block-respecting* if it has the following property:

> Consider a length $n$ input $x$. The tape(s) of the Turing machine are split into contiguous blocks of length $B(n)$ each. Each head of the Turing Machine crosses a block-boundary only at time-steps that are integer multiples of $B(n)$.
> (That is, within each block of $B(n)$ time steps, each head operates only within a particular block.)

Given a deterministic Turing machine $M$ that runs in time $T(n)$, and a "reasonable" function $B : \mathbb{N} \to \mathbb{N}$, construct a deterministic $B$-block-respecting Turing machine $M'$ for the same language while ensuring that the running time of $M'$ is $O(T(n))$.

| | siht | hasi | ftni | htro | orpe |
|---|---|---|---|---|---|
| this | isah | intf | orth | epro | blem |
| hasi | ftni | htro | orpe | melb | |

[Hint: Suppose the machine $M$ uses $k$ tapes, you could perhaps make use of the above picture and use $3k$ tapes.]

5. **[Non-deterministic UTM simulations]** (10)

   Assume that $T : \mathbb{N} \to \mathbb{N}$ is a time-constructible function. Consider the following task — you are given a source code of a non-deterministic machine $M$ deciding a language $L$ running in time $T : \mathbb{N} \to \mathbb{N}$ but $M$ uses 81234 tapes. Show that there is a different machine $M'$ deciding the same language $L$ with just 2 tapes with the running time $T' : \mathbb{N} \to \mathbb{N}$ of $M'$ satisfying $T'(n) = O(T(n))$.

   In words, show that we can perform tape-reduction with just a constant overhead if we have the power of non-determinism.

   [Hint: In the machine $M'$, use one of the tapes to 'interleave' the 81234 tapes of $M$ and use the second tape to write down a guess for what the heads of $M'$ do in the $T$ steps.]

6. **[Improving the time-hierarchy theorem]** (15)

   For this problem, you may assume that any 'reasonable-looking' function is time-constructible. And whenever you see functions like $n^2 \log^{3/4}(n)$, assume that there is an implicit ceiling to make sure this is an integer etc. (Basically don't worry about technicalities!)

   In class we proved that the deterministic time hierarchy theorem that stated the following:

   > Suppose $t_1, t_2 : \mathbb{N} \to \mathbb{N}$ are non-decreasing time-constructible functions with $t_1(n), t_2(n) \geq n$. If we have $t_1(n) \log t_1(n) = o(t_2(n))$, then we have $\mathsf{DTIME}(t_1) \subsetneq \mathsf{DTIME}(t_2)$.

   (a) Let $t_1, t_2, f : \mathbb{N} \to \mathbb{N}$ be time-constructible non-decreasing functions that satisfy $t_1(n), t_2(n), f(n) \geq n$. Show that $\mathsf{DTIME}(t_1(n)) = \mathsf{DTIME}(t_2(n))$ implies

   $$\mathsf{DTIME}(t_1(f(n))) = \mathsf{DTIME}(t_2(f(n))).$$

   [Hint: Padding.]

   (b) Show that $\mathsf{DTIME}(n^2) \subsetneq \mathsf{DTIME}(n^2 \log^{3/4}(n))$.

   [Hint: You may have to use the above part multiple times.]

   (c) Extend this to show that for any rational number $a, \varepsilon$ satisfying $a > 1$ and $0 < \varepsilon < 1$, we have

   $$\mathsf{DTIME}(n^a) \subsetneq \mathsf{DTIME}(n^a (\log n)^{\varepsilon}).$$