General guidelines

The questions fall into several categories:

(Know). Make sure you know how to solve. Do not submit.
(Mandatory). Mandatory questions.
(Bonus). Bonus questions.

Put your answers in the dropbox folder. You have to

1. write the solutions yourself,
2. give credit to any source (or any person) you consulted with.

You have to submit solutions to, at least, the mandatory questions.
Unique Perfect Matching

1. (Mandatory). Finish the proof of the probabilistic algorithm we’ve seen in class: show how to find a Unique Perfect Matching using the Isolation Lemma

   \textit{k-wise independence}

2. (Mandatory). Draw \( a \in \{0, 1\}^{\log n} \) uniformly and for every \( 0 \neq i \in \{0, 1\}^{\log n} \) let \( X_i \) be the random variable \( X_i = \langle a, i \rangle \mod 2 \).

   Prove that \( X = (X_1, \ldots, X_{n-1}) \) is a distribution over \( \mathbb{F}_2^{n-1} \) with support size \( n \) and is pairwise independent.

3. (Mandatory). You are about to play a game where \( n \) coins are laid covered on a table and you uncover and take \( \frac{2n}{3} \) coins. You are promised that \( k < \frac{n}{3} \) of the coins are pure gold and the rest copper. The catch is that you first have to announce your strategy (be it deterministic or probabilistic) and only then an adversary places the coins on the table. Show that:
   
   (a) If you use a deterministic strategy, you can guarantee no gold coin.
   
   (b) If you use \( n \) random coins you can almost certainly get \( \Omega(k) \) gold coins. What is the failure probability?
   
   (c) If you use \( O(\log n) \) random coins, you can guarantee \( \Omega(k) \) gold coins with probability at least \( 1 - O\left(\frac{1}{k}\right) \).

4. (Know). Let \( A, B \) be two distributions taking values in \( \Lambda \) For \( f : \Lambda \to \Lambda' \), \( f(A) \) (corr. \( f(B) \)) denotes the distribution over \( \Lambda' \) obtained by picking \( a \sim A \) and outputting \( f(a) \). Prove that \( \|f(A) - f(B)\|_1 \leq \|A - B\|_1 \) for every function \( f \).

PIT

5. (Mandatory). Prove the Schwartz-Zippel lemma.

   If \( p : \mathbb{F}^m \to \mathbb{F} \) is a non-zero polynomial of total degree \( d \) over a field \( \mathbb{F} \) and \( \Lambda \subseteq \mathbb{F} \), then \( \Pr_{a_1, \ldots, a_m \in \Lambda}[p(a_1, \ldots, a_m) = 0] \leq \frac{d}{|\Lambda|} \).

6. (Mandatory). Give a \textbf{coRP} algorithm for Polynomial Identity Testing (PIT). In the proof work over the finite field \( \mathbb{Z}_p \) for an appropriately random prime \( p \), and prove its correctness

Boolean and Arithmetic Circuits

7. (Mandatory). Prove that almost all function \( f : \{0, 1\}^n \to \{0, 1\} \) require circuits of size \( \geq \frac{2^n}{10n} \), i.e.

\[
\Pr_f \left[ s(f) \geq \frac{2^n}{10n} \right] \xrightarrow{n \to \infty} 1
\]
8. (Mandatory). Give an algorithm for addition of two integers represented in binary in $\text{AC}^0$

9. (Know). Prove that $\text{NC}^0 \subseteq \text{AC}^0 \subseteq \text{NC}^1 \subseteq \cdots \subseteq \text{NC} = \text{AC} \subseteq P$

10. (Bonus). Prove that $\text{NC}^k \subseteq \text{Space}(O(\log^k n))$. Note the cost of pointers.