General guidelines

The questions fall into several categories:

<table>
<thead>
<tr>
<th>(Know).</th>
<th>Make sure you know how to solve. Do not submit.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Mandatory).</td>
<td>Mandatory questions.</td>
</tr>
<tr>
<td>(Bonus).</td>
<td>Bonus questions.</td>
</tr>
</tbody>
</table>

On the submission date we will collect your answers. We will then go over the questions and solve them in class. After that you have a week to write the solutions and submit to us, as long as

1. You write the solutions alone,

2. You give credit to any source (or any person) you consulted with.

You have to submit solutions to, at least, the mandatory questions. We give the same grade to solutions that were submitted before or after we solved the question in class.
$k$-wise independence

1. (Mandatory). A distribution $X = (X_1, \ldots, X_n)$ over $\Sigma^n$ is called $k$-wise independent if for every $\{i_1, \ldots, i_\ell\} \subseteq [n]$ where $\ell \leq k$ and every $\sigma \in \Sigma^\ell$ it holds that

$$\Pr[(X_{i_1}, \ldots, X_{i_\ell}) = \sigma] = \prod_{j=1}^{\ell} \Pr[X_{i_j} = \sigma_j].$$

We will almost always deal with distributions whose marginals are uniform, so we’ll in fact say that a distribution is $k$-wise independent if

$$\Pr[(X_{i_1}, \ldots, X_{i_\ell}) = \sigma] = \frac{1}{|\Sigma|^{\ell}}.$$

(a) Give an explicit distribution over 3 bits which is pairwise independent (i.e., $k = 2$-wise independent) but not uniform (or, not $k = 3$-wise independent).

(b) Let $\mathbb{F}$ be a finite field of cardinality $n$ and fix some $k < n$. Draw $(a_0, \ldots, a_{k-1}) \in \mathbb{F}^k$ uniformly and for every $i \in \mathbb{F}$, let $X_i$ be the random variable $X_i = \sum_{\ell=0}^{k-1} a_{\ell} \cdot i^\ell$.

Prove that $X = (X_1, \ldots, X_n)$, a distribution over $\mathbb{F}^n$ with support size $n^k$, is $k$-wise independent.

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

2. (Bonus). Prove that if $X = (X_1, \ldots, X_n)$ is $k$-wise independent and each $X_i$ is Boolean then $|\text{Supp}(X)| \geq B(k/2, n)$, where $B(r, n)$ is the number of words of weight at most $r$ in the $n$ dimensional Boolean cube.

Hint: Work over $\{\pm 1\}$. Map appropriate subsets of $[n]$ to real vectors and deduce linear independency.

3. (Mandatory). Let $V = \{0, 1\}^m$ and $\mathcal{H} \subseteq V \to V$ a two universal family of hash functions (see definition in Lecture 2). Fix two sets $A, B \subseteq V$. Call a hash function $h \in \mathcal{H}$ $\varepsilon$-good for $A, B$ if

$$\left| \Pr_{x \in V} [x \in A \cap h(x) \in B] - \rho(A)\rho(B) \right| \leq \varepsilon,$$

where $\rho(C) = |C|/|V|$.

Prove that for any $A, B \subseteq V$, $\varepsilon > 0$,

$$\Pr_{h \in \mathcal{H}} [h \text{ is not } \varepsilon\text{-good for } A, B] \leq \frac{\rho(A)\rho(B)(1 - \rho(B))}{\varepsilon^2 \cdot |V|} \leq \frac{1}{\varepsilon^2 |V|}.$$
4. (Mandatory). You are about to play a game where \( n \) coins are laid covered on a table and you uncover and take \( 2n/3 \) coins. You are promised that \( k < 2/3 \) 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 \( 1 - O(\frac{1}{k}) \).

**Graphs, operators and norms**

5. (Know). Prove that if \( A \in \mathbb{R}^{n \times n} \) is symmetric than it has real eigenvalues and an orthonormal basis of real eigenvectors.

6. (Mandatory). Let \( A \) be a Hermitian matrix with eigenvalues \( \lambda_n \leq \ldots \leq \lambda_1 \) and corresponding eigenvectors \( v_n, \ldots, v_1 \). Prove that \( \lambda_2 = \max_{x \perp v_1} \frac{x^* A x}{x^* x} \).

7. Let \( A \in \mathbb{C}^{n \times n} \) and define the spectral norm \( \|A\| = \max_{x \neq 0} \frac{\|Ax\|}{\|x\|} \), where \( \|x\| = \|x\|_2 = \sqrt{\sum_i |x_i|^2} \). Prove:

(a) (Know). \( \|A + B\| \leq \|A\| + \|B\| \).

(b) (Know). \( \|cA\| = |c| \cdot \|A\| \).

(c) (Know). \( \|A\| = 0 \) iff \( A = 0 \).

(d) (Know). \( \|AB\| \leq \|A\| \cdot \|B\| \).

(e) (Mandatory). \( \|A\| \geq \max_i |\lambda_i(A)| \) and if \( A \) is normal than equality is attained.

(f) (Mandatory). Given an example of a matrix \( A \) such that \( \|A\| \gg \max_i |\lambda_i(A)| \).

8. (Know). Let \( A \in \mathbb{C}^{n \times n} \) and define the induced \( \ell_\infty \) norm \( \|A\|_\infty = \max_{x \neq 0} \frac{\|Ax\|_\infty}{\|x\|_\infty} \), where \( \|x\|_\infty = \max_i |x_i| \). Prove:

(a) \( \|A\|_\infty = \max_i \|A_i\|_1 \) where \( A_i \) is the \( i \)-th row of \( A \) and \( \|x\|_1 = \sum_i |x_i| \).

(b) \( \|cA\|_\infty = |c| \cdot \|A\|_\infty \).

(c) \( \|A\|_\infty = 0 \) iff \( A = 0 \).

(d) \( \|AB\|_\infty \leq \|A\|_\infty \cdot \|B\|_\infty \).

(e) If \( A \) is the transition matrix of an undirected graph then \( \|A\|_\infty = 1 \).

9. (Know). Let \( A \) be the transition matrix of the undirected \( n \)-cycle.

(a) Prove that \( \{\chi_k\}_{k=0}^{n-1} \) is an eigenvector basis of \( A \), where \( \chi_k(i) = \omega^{ki} \) and \( \omega \) is a primitive \( n \)-th root of unity.

(b) Find a real orthonormal basis for \( A \).
HW 2

Out: 20.3.2018
Due: 17.4.2018

1. (Mandatory). Let $A, B$ be two distributions taking values in $\Lambda$. For $f: \Lambda \rightarrow \Lambda'$, $f(A)$ (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 $f$.

2. For $A \in \mathbb{C}^{n_1 \times m_1}$ and $B \in \mathbb{C}^{n_2 \times m_2}$ we define the tensor product $A \otimes B \in \mathbb{C}^{n_1 n_2 \times m_1 m_2}$ so that $(A \otimes B)[(i_1, i_2), (j_1, j_2)] = A[i_1, j_1] \cdot B[i_2, j_2]$.
   
   (a) (Know). Prove: $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$.
   (b) (Know). Prove: $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$ whenever the dimensions fit.
   (c) (Know). Prove that the tensor product of two projections is a projection.
   (d) (Know). Prove that the tensor product of two unitary matrices is unitary.
   (e) (Mandatory). Suppose that $A \in \mathbb{C}^{n \times n}$ and $B \in \mathbb{C}^{m \times m}$ with eigenvalues $\lambda_1, \ldots, \lambda_n$ and $\mu_1, \ldots, \mu_m$ respectively. Prove that the eigenvalues of $A \otimes B$ are $\{\lambda_i \mu_j\}_{i \in [n], j \in [m]}$.

Basic problems and classes

3. (Mandatory). Shortly outline a proof of each of the following:
   
   (a) Addition of two integers represented in binary is in $\text{AC}^0$.
   (b) Addition of $n$ integers ($n$-bits each) is in $\text{NC}^1$.
   (c) Multiplication of two integers represented in binary is in $\text{NC}^1$.

4. (Know). The parity function over $n$ bits is simply $x_1 \oplus \ldots \oplus x_n$. Show a depth-three Boolean circuit computing Parity with $O(\sqrt{n} 2^{\sqrt{n}})$ gates of unbounded fan-in. NOT gates are allowed only at the input level and are not counted in the depth complexity.

5. (Mandatory). Prove that $\text{NC}^1 \subseteq L \subseteq \text{NL} \subseteq \text{AC}^1$ and that $\text{BPL} \subseteq \text{NC}^2$.

6. (Bonus). We define arithmetic $\text{SAC}^1$ as uniform, polynomial-size arithmetic circuits with $O(\log n)$ depth over unbounded fan in $+$ and bounded fan-in $\times$.
   
   (a) Prove that computing the product of $n$ matrices of dimension $n \times n$ is in arithmetic $\text{SAC}^1$.
   (b) Prove that computing the characteristic polynomial of an arbitrary matrix is in arithmetic $\text{SAC}^1$, and also in (Boolean) $\text{NC}^2$.

Connectivity and expanders

7. (Mandatory). Give a deterministic logspace algorithm that
   
   • checks whether a given undirected graph is a connected tree or not,
   • checks whether a $D = 3$ regular graph with $\lambda \leq 3/4$ is connected or not.
In both questions do not use the fact that \( \text{USTCONN} \in L \).

8. (Mandatory). We say that a directed graph is Eulerian if every vertex has the same indegree as outdegree.

(a) Prove that in an Eulerian graph each strongly connected component is isolated.
(b) Give a logspace reduction from the problem of connectivity in directed Eulerian graphs to connectivity in undirected graphs (without using the fact that \( \text{USTCONN} \in L \)).

9. (Mandatory). Let \( G \) be a \( D \)-regular undirected graph over \( N \) vertices. Let \( \alpha(G) \) denote the size of the largest independent set of \( G \) and let \( \chi(G) \) denote the chromatic number of \( G \).
   Prove:
   (a) \( \alpha(G) \leq \frac{\lambda(G)}{1+\lambda(G)} N \).
   (b) \( \chi(G) \geq \frac{1+\lambda(G)}{\lambda(G)} \).

10. (Mandatory).

Let \( G = (V,E) \) be a \( D \)-regular undirected graph over \( N \) vertices. For \( A \subseteq V \) we denote \( \Gamma(A) = \{ w \in V : \exists v \in A : (v,w) \in E \} \).
   Prove:
   \[ |\Gamma(A)| \geq |A| \cdot \frac{1}{\rho(A) + (1 - \rho(A))\lambda(G)^2}. \]
   Assume \( G \) is Ramanujan. Conclude that there exists some constant \( \alpha > 0 \) such that all sets \( A \subseteq V \) of density at most \( \alpha \) (and this is still constant density) the vertex expansion \( |\Gamma(A)|/|A| \) is at least \( D/4 \).