Space-Bounded Computation – Questions Pool

Amnon Ta-Shma and Noam Parzanchevski

November 6, 2018

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>

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

   \( k \)-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
   
   \[ \Pr_{a_1, \ldots, a_m \in \Lambda} [p(a_1, \ldots, a_m) = 0] \leq \frac{d}{|\Lambda|^t}. \]

6. (Mandatory). Give a \( \text{coRP} \) 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 $\text{NC}^0 \subseteq \text{AC}^0 \subseteq \text{NC}^1 \subseteq \cdots \subseteq \text{NC} = \text{AC} \subseteq \text{P}$

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

1. (Know). Let $X_i$ be i.i.d random variables such that $X_i \sim \text{Ber}(p)$ for some $p \in (0, 1)$ and define $X = \sum_i X_i$, then for $0 < q \leq p$:

$$\Pr[X < qn] \leq e^{-\text{KL}(q||p)n}$$

Maximal Independent Set

2. (Mandatory). In class, we derandomized the RNC algorithm for MIS using simplifying (and unjustified) assumptions. You are now asked to removed the unjustified assumptions.

Show an NC algorithm for MIS that works for the general case. I assume that as part of the construction you will use a distribution $X = X_1, \ldots, X_n$ with small support size. Write precisely:

- What properties you need from $X$,
- How you construct $X$,
- Why $X$ has the desired properties, and,
- Why these properties suffice for solving MIS in NC,

3. (Mandatory). Fix a finite field $\mathbb{F} = \mathbb{F}_q$. Show how to “naturally extend” the 2UFOHF family we’ve seen in class for larger independence. I.e.,

- Define $k$-wise independence, and,
- Show an explicit distribution over $(X_1, \ldots, X_q)$ that is $k$-wise independent, each $X_i$ is distributed over $\mathbb{F}_q$, and has support size $q^k$.

4. (Mandatory). Let $V = \{0, 1\}^m$ and $\mathcal{H} \subseteq \{ h : V \rightarrow V \}$ a two universal family of hash functions. 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 $\rho(C) = \frac{|C|}{|V|}$.

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

$$\Pr_{h \in \mathcal{H}} [ h \text{ is not } \varepsilon\text{-good for } A, B ] \leq \frac{\rho(A)\rho(B)(1 - \rho(B))}{\varepsilon^2 \cdot |V|} \leq \frac{1}{\varepsilon^2 |V|}.$$
Error Correcting Codes

5. (Mandatory). Let $C$ be a linear $[n, k, d]_q$ code.

- Show that $d = \min_{x \in C} \text{wt}(x)$ where $\text{wt}(x) = |\{i : x_i \neq 0\}|$.
- Prove the Singleton bound: $d \leq n - k + 1$.
- Recall the parity code we’ve seen in class $\text{Par} : \{0, 1\}^k \rightarrow \{0, 1\}^{k+1}$ where $\text{Par}(x) = x \oplus \bigoplus_i x_i$. Show that $\text{Par}$ is a linear code and describe its generator matrix $G \in \mathbb{F}_2^{k+1 \times k}$.

6. (Mandatory). In this exercise we will prove two simple (non-matching) upper and lower bounds on the number of codewords in the best code with distance $d$. Let $\Sigma$ be some alphabet and denote $q = |\Sigma|$. Let $d \leq n$ be integers. We also let $B_q(r) = \{x \in [q]^n \mid \text{wt}(x) \leq r\}$, the ball around zero of radius $r - 1$ in the Hamming weight distance.

- (The Gilbert-Varshamov bound, A lower bound on the number of codewords) Prove that there exists a distance $d$ code $C \subseteq \Sigma^n$ with
  \[ |C| \geq \frac{|\Sigma|^n}{|B_q(d-1)|}. \]

- (The Hamming bound) An upper bound on the number of codewords) Prove that for any distance $d$ code $C \subseteq \Sigma^n$,
  \[ |C| \leq \frac{|\Sigma|^n}{|B_q(d-1/2)|}. \]

- Use the asymptotic estimates given in class for $q = 2$ to show that for any $0 < \delta < 1/2$ there exists a code $C \subseteq \{0, 1\}^n$ with relative distance $\delta$ and relative rate $r \geq 1 - H(\delta) - o(1)$, and every code $C \subseteq \{0, 1\}^n$ with relative distance $\delta$ has relative rate $r \leq 1 - H(\delta/2) + o(1)$.

A reminder. If $C \subseteq \Sigma^n$ has distance $d$, then $C$ has relative distance $\delta = \frac{d}{n}$ and relative rate $r = \frac{\log |C|}{n \log |\Sigma|}$. You may use $|B_2(\lambda n)| \leq 2^{H(\lambda)n}$ and $\lim_{n \to \infty} \frac{\log |B_2(\lambda n)|}{n} = H(\lambda)$ for any $0 < \lambda < 1/2$. 