Space-Bounded Computation – Questions Pool

Amnon Ta-Shma and Dean Doron

June 10, 2018

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.

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.

HW 1

Out: 6.3.2018
Due: 19.3.2018

k-wise independence

1. (Mandatory). A distribution $X = (X_1, \ldots, X_n)$ over Σ^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 $X_i = \langle a, i \rangle \bmod 2$.
   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 $|\mathsf{Supp}(X)| \geq B(k/2, n)$, 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 $h \in \mathcal{H}$ *ε-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 $A, B \subseteq V$, $\varepsilon > 0$,

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

4. (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 $1 - O(\frac{1}{k})$.

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 $\lambda_2 = \max_{x : x \perp v_1} \frac{x^\dagger A x}{x^\dagger x}$.

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). $\|AB\| \leq \|A\| \, \|B\|$.

   (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 ℓ_∞ 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) $\|AB\|_\infty \leq \|A\|_\infty \, \|B\|_\infty$.

   (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 ω 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 Λ For $f : \Lambda \to \Lambda'$, $f(A)$ (corr. $f(B)$) denotes the distribution over Λ' 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 $A \in \mathbb{C}^{n_1,m_1}$ and $B \in \mathbb{C}^{n_2,m_2}$ 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 AC^0.

   (b) Addition of n integers (n-bits each) is in NC^1.

   (c) Multiplication of two integers represented in binary is in 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 $\mathsf{NC}^1 \subseteq \mathsf{L} \subseteq \mathsf{NL} \subseteq \mathsf{AC}^1$ and that $\mathsf{BPL} \subseteq \mathsf{NC}^2$.

6. (Bonus). We define arithmetic 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 SAC^1.

   (b) Prove that computing the characteristic polynomial of an arbitrary matrix is in arithmetic SAC^1, and also in (Boolean) 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 $\bar{\lambda} \leq 3/4$ is connected or not .

In both questions do not use the fact that USTCONN $\in \mathsf{L}$.

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 USTCONN $\in \mathsf{L}$).

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) $\alpha(G) \leq \frac{\bar{\lambda}(G)}{1+\bar{\lambda}(G)} N$.

   (b) $\chi(G) \geq \frac{1+\bar{\lambda}(G)}{\bar{\lambda}(G)}$.

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:

$$|\Gamma(A)| \;\geq\; |A| \cdot \frac{1}{\rho(A) + (1 - \rho(A))\bar{\lambda}(G)^2}.$$

    Assume G is Ramanujan. Conclude that there exists some constant $\alpha > 0$ such that all sets $A \subseteq V$ of density at most α (and this is still constant density) the vertex expansion $|\Gamma(A)|/|A|$ is at least $D/4$.

HW 3

Out: 24.4.2018
Due: 22.5.2018

Dry part

1. (Mandatory). Let Γ be a finite group and let $S \subseteq \Gamma$. Consider the corresponding Cayley graph $G = Cay(\Gamma, S)$.
   (a) Prove that G is consistently labeled.
   (b) Let H be a consistently labeled regular graph over $|S|$ vertices. Prove that $G Ⓢ H$ is a Cayley graph.
2. (Mandatory). The explicit family of expanders we constructed in class using the zig-zag product was sparse. The following construction amends that. Let H be a $[D^8, D, 1/8]$-graph, $G_1 = H^2$ and
$$G_t = (G_{\lceil t/2 \rceil} \otimes G_{\lfloor t/2 \rfloor})^2 Ⓩ H.$$
   - Prove that the family is well-defined, fully explicit, regular, has degree D^2 and second eigenvalue of at most $1/2$.
   - Prove the space complexity of computing Rot_{G_t} is $O(\log |V(G_t)|)$ space, where $V(G_t)$ is the set of vertices of G_t.

Wet part

In this part we ask you to *implement* the space-efficient undirected connectivity algorithm that is based on derandomized squaring.

1. Implement **Rozenman and Vadhan's algorithm** for USTCONN. Given a graph over N vertices and two vertices s and t, checks whether s is connected to t (via the derandomized-squaring product).
2. Implement a logspace algorithm that given N and D, outputs a polynomial-length universal *exploration* sequence for undirected D-regular graphs over N vertices. Use the derandomized-squaring construction.
3. Modify the algorithm to work with directed out-regular graphs.
4. Please generate interesting undirected, and directed regular graphs and upload them to the shared directory. Test your algorithms on them. Please measure your space and time complexity, and upload it to the appropriate table.

Guidelines:

- You need a family of constant degree expanders. You can use the Gabber-Galil construction from, e.g., `https://people.eecs.berkeley.edu/~luca/cs366/lecture13.pdf`. You can also come up with your own favorite family of expanders.

- Your algorithm, besides solving the connectivity algorithm, should write the series of edge labels to a file. The output of UES algorithms should also be written to a file, and they will be compared among the class.
- The input graphs for the algorithm should be in a standard format stated below.
- You are welcome to choose your favorite programming language. However, it should be platform-oblivious (and specifically runnable on a university PC and on a Mac).
- The code should be readable and documented. Try to practice good design principles.
- Each algorithm should be supplied with a suitable readme file.
- Trace the amount of memory your algorithm uses (on top of the input of course) and show how it grows with the input size.
- We also announce a competition. Above all, we are after low space. Please supply two undirected graphs for the final competition (and keep them a secret from the rest of the group).
- Your algorithm should also be adopted to work with *directed out-regular graphs*. In your documentation, please attach some running examples, and we will also give some canonical ones.
- In due time, we will refer you to a shared repository to upload your work.

The input's format The input file that represents a graph is very simple – either as an adjacency matrix (A) or as a list of edges (L). For example, the following two "files" represent the same graph. In the (L) format, the edges can come in any order.

```
A
0 1 0 1
0 1 1 0
0 0 0 0
0 1 0 0

L
1,2
1,4
2,2
2,3
4,2
```

HW 4

Out: 15.5.2018
Due: 29.5.2018

1. (Choose either this question or question 2) Prove that there *exists* a UTS for undirected, non-bipartite, labeled, d-regular graphs over n vertices of length $\text{poly}(n)$.

2. (Choose either this question or question 1) Prove that for every n, k and $\varepsilon > 0$ there *exists* $E\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ which is a (k,ε) extractor, for $d \leq \log(n-k) + 2\log\frac{1}{\varepsilon} + O(1)$ and $m \leq k + d - 2\log\frac{1}{\varepsilon} - O(1)$.

3. Let G be a directed graph over n vertices and let A be its transition matrix.

   (a) (Mandatory). Prove that if A is doubly-stochastic[1] then $\|A\| = 1$.

   (b) (Bonus). Prove that if $\|A\| = 1$ then A is doubly stochastic.

   (c) (Mandatory). Suppose G is D-out-regular and has maximal in-degree Δ. Prove that $\|A\| \leq \sqrt{\Delta/D}$.

   (d) (Mandatory). Suppose G is D-regular (i.e., the in-degree and out-degree of every vertex is D), connected and has a self-loop on every vertex. Prove that there exists a constant c such that $\lambda_2(A) = \max_{v:\|v\|=1, v\perp\vec{1}} \|Av\| \leq 1 - n^{-c}$.

4. (Mandatory). Let G be an (N, D, λ_1) directed, regular graph and H be a (D, d, λ_2) graph. Define $G\textcircled{S}H$, prove it is well defined, directed regular graph, and that,

$$\lambda(G\textcircled{S}H) \;\leq\; 1 - (1-\lambda_1)(1-\lambda_2^2).$$

5. (Mandatory).

   (a) Given a D-regular graph G, let $G' = G\textcircled{R}C_D$ where $\textcircled{R}$ is the replacement product and C_D is the cycle. Give a fully explicit locally-invertible labelling for G'.

   (b) (Mandatory). Use the result above to give a logspace algorithm that on input 1^{N+D} outputs a UES for D-regular graphs over N vertices.

   Hint: We already constructed UTS for 3-regular locally-invertible graphs. Show a transformation $\sigma : \{0,1,2\}^\star \to \{0,\ldots,D-1\}^\star$ that transforms a UTS for G' into a UES for G.

6. (Mandatory).

   (a) Let G be an undirected D-regular graph over N vertices. Prove that every labeling of G induces a consistent labelling of the line graph $L(G)$.

   (b) Use the result above to give a logspace algorithm that on input 1^{N+D} outputs a UES for D-regular graphs over N vertices.

[1] A matrix is doubly-stochastic if it has non-negative entries and the sum of each row and each column is 1.

HW 5

Out: 29.5.2018
Due: 12.6.2018

1. (Mandatory). Let X and Y be random variables, where Y is distributed over $\{0,1\}^s$. Prove that for every $\varepsilon > 0$,

$$\Pr_{y \sim Y}\left[H_\infty(X \mid Y = y) < H_\infty(X) - s - \log(1/\varepsilon)\right] \;<\; \varepsilon.$$

2. (Mandatory). Prove there exists a UTS for undirected, arbitrarily labeled, graphs, over n vertices of size $n^{O(\log n)}$ computable in space $O(\log^2 n)$.

3. (Mandatory). In this question we assume the existence of an (s,ε) extractor $E\colon \{0,1\}^{10s} \times \{0,1\}^t \to \{0,1\}^s$ for $\varepsilon \geq 2^{-s}$ with seed-length $t = O(\log s + \log(1/\varepsilon))$. We furthermore assume E is explicit and runs in space linear in its input length (such explicit extractors are indeed known).

   (a) Prove that $G\colon \{0,1\}^{10s+\ell t} \to \{0,1\}^{10s+\ell s}$ defined by

$$G(x; y_1, \ldots, y_\ell) \;=\; x \circ E(x,y_1) \circ E(x,y_2) \circ \ldots \circ E(x,y_\ell)$$

   is an $O(\ell\varepsilon)$-PRG against $[2^s, 10s+\ell s]_{\{0,1\}}$ BPs.

   (b) Prove that any language solvable by a BPL machine using at most $\frac{\log^2 n}{\log\log n}$ random bits, already belongs to L.

   (c) Prove that any language solvable by a BPL machine using at most $\mathrm{poly}(\log n)$ random bits, already belongs to L.

4. (Bonus). Define the $ExactHalf_n$ function as follows. n is a fixed even integer. The input to the problem is a sequence $e_{i,j}$ for $1 \leq i < j \leq n$ with $e_{i,j} \in \{0,1\}$. The input defined an undirected graph $G = (V = [n], E)$ with $(i,j) \in E$ iff $e_{i,j} = 1$. The function is 1 on the input iff the graph G has a clique of size $n/2$ and *no other edge*.

   Prove that every $[W, \binom{n}{2}]_{\{0,1\}}$ read-once BP that accepts $ExactHalf_n$ must have $W = 2^{\Omega(n)}$.