General instructions:

1. The deadline for the exam is 12/07/18.
2. Submit your (typed) solution by mail to amnon@tau.ac.il and deandoron@mail.tau.ac.il.
3. Work must be done alone.
4. If you had to use an electronic source, state it explicitly within the relevant question.
Question 1

ZPL is the probabilistic, logspace class with zero-sided error (for every input, with probability at least half the answer is the correct one, and otherwise it is quit). Let ZPL∗ be the variant of ZPL where the machine has multiple access to the random tape.

Prove that BPL ⊆ ZPL∗.

Question 2

We want to find an explicit, polynomial-length UTS for consistently labeled undirected d-regular graphs over n vertices with $\lambda < \frac{3}{4}$. Call this family of graphs $G_n$.

Definition 1. $\sigma \in [d]^*$ is a UTS for $G_n$, if for every $G = (V, E) \in G_n$, $v \in V$, walking on $G$ from $v$ according to $\sigma$ reaches all the vertices in the graph. $\sigma$ is explicit, if there exists an algorithm running in $\text{poly}(n)$ time outputting it.

Definition 2. We say $S \subseteq [d]^*$ is good for $(G, v_0)$ ($G \in G_n$) if there exists $\sigma \in S$ such that for every vertex $v$, a walk over $G$ according to $\sigma$ starting from $v$ will visit $v_0$. We say $S$ is explicit if $|S|$ is polynomial, and there exists a poly(n) algorithm that given $i \in [|S|]$ outputs the $i$-th string in $S$.

1. Show that given an explicit $S$ that is good for $(G, v_0)$ for every $G \in G$ and $v_0$, one can construct an explicit UTS for $G$.

2. Construct a sequence of sets $S_i \subseteq [d]^*$ such that

$$S_0 = \{\varepsilon\} , \ S_{i+1} = \{utu : u \in S_i, t \in [d]\}.$$  

Fix $G = (V, E) \in G$ and $v_0$. Define

$$R_{G,v_0}^{-1}(\sigma) = \{v \in V \mid \text{The walk on } G \text{ from } v \text{ according to } \sigma \text{ visits } v_0\}.$$  

Define

$$r_i = \max_{\sigma \in S_i} |R_{G,v_0}^{-1}(\sigma)|.$$  

Prove that $r_0 = 1$ and $r_{i+1} > r_i + \delta$, where $\delta = \frac{r_i(n-r_i)}{4n}$.

Guidance:

- Choose $\sigma \in S_i$ that attains $r_i$. Show that walks according to $\sigma$ from $V \setminus R_{G,v_0}^{-1}(\sigma)$ end in exactly $n - r_i$ vertices. Denote these vertices by $B$. Show that there exist enough edges between $R_{G,v_0}^{-1}(\sigma)$ and $B$.

3. Show that $r_k = n$ for $k = O(\log n)$.

4. Conclude an explicit UTS. What is its cardinality as a function of $n$ and $d$?
Question 3

In this question we will construct PRGs fooling “almost-balanced” halfspaces. Given \(w \in \mathbb{R}^n\) and \(\theta \in \mathbb{R}\), the halfspace \(H_{w,\theta} : \{1, -1\}^n \rightarrow \{1, -1\}\) is the function \(H_{w,\theta}(x) = \text{sign}(\langle w, x \rangle - \theta)\).

**Definition 3.** We say \(G : \{0, 1\}^\ell \rightarrow \{1, -1\}^n\) \(\varepsilon\)-fools \(H_{w,\theta}\) if

\[
|\mathbb{E}[H_{w,\theta}(U_{\{1, -1\}^n})] - \mathbb{E}[H_{w,\theta}(G(U_\ell))]| \leq \varepsilon.
\]

We measure distance between real-valued distributions \(P, Q\) by the CDF distance,

\[
d(P, Q) = \|\text{CDF}(P) - \text{CDF}(Q)\|_\infty = \max_{t \in \mathbb{R}} \left| \Pr_{x \sim P}[x < t] - \Pr_{x \sim Q}[x < t] \right|.
\]

1. Fix \(w \in \mathbb{R}^n\) and \(\theta \in \mathbb{R}\). Prove that if \(G : \{0, 1\}^\ell \rightarrow \{1, -1\}^n\) is such that

\[
d(\langle w, G(U_\ell) \rangle, \langle w, U_{\{1, -1\}^n} \rangle) \leq \varepsilon
\]

then \(G\) \(2\varepsilon\)-fools \(H_{w,\theta}\).

We will assume \(\|w\| = 1\), as this can be done without loss of generality. We say a unit-norm \(w \in \mathbb{R}^n\) is \(\eta\)-balanced if \(\|w\|_\infty \leq \eta\). We say a halfspace \(H_{w,\theta}\) is \(\eta\)-balanced if \(w\) is.

Fooling monotone BPs and a first try at fooling halfspaces

Throughout, all of our BPs are read-once.

**Definition 4.** Given a \([W, T]_\Sigma\) BP \(M\) and a vertex \(v\) at layer \(i\), we let \(\text{Acc}_M(v)\) be the set of all \(z \in \Sigma^{T-i}\) such that starting from \(v\), \(M\) accepts \(z\). We say \(M\) is monotone if for every layer \(i\) there exists an ordering \(v_1, \ldots, v_w\) of the vertices in layer \(i\) such that if \(j < k\) then \(A_M(v_j) \subseteq A_M(v_k)\).

2. Prove that for any \(w \in \mathbb{R}^n\) and \(\theta \in \mathbb{R}\) there exists a monotone \([\mathbb{R}, n]_{\Sigma = \{-1, 1\}}\) BP \(M\) that solves \(H_{w,\theta}\), where you can define yourselves what a BP with an infinite state space is.

**Definition 5.** Given a \([W, T]_\Sigma\) BP \(M\), we say that the BPs \(M_{\text{down}}\) and \(M_{\text{up}}\) \(\varepsilon\)-sandwich \(M\) if:

- For every \(z \in \Sigma^T\), \(M_{\text{down}}(z) \leq M(z) \leq M_{\text{up}}(z)\).
- \(\Pr[M_{\text{up}}(U) = 1] - \Pr[M_{\text{down}}(U) = 1] \leq \varepsilon\).

3. Prove that for any monotone \([W, T]_\Sigma\) BP \(M\) there exists \(M_{\text{down}}\) and \(M_{\text{up}}\) that \(\varepsilon\)-sandwich \(M\) with width \(\frac{2T}{\varepsilon}\) (note that it is independent of the original width \(W\)).

4. Prove that if \(G : \{0, 1\}^\ell \rightarrow (\Sigma)^T\) \(\delta\)-fools monotone \([\frac{2T}{\varepsilon}, T]_\Sigma\) BPs then it also \((\varepsilon + \delta)\)-fools monotone \([W, T]_\Sigma\) BPs for arbitrary \(W\).

5. Prove that if \(G : \{0, 1\}^\ell \rightarrow (\Sigma)^T\) \(\delta\)-fools monotone \([\frac{2T}{\varepsilon}, T]_\Sigma\) BPs then

\[
d(\langle w, G(U_\ell) \rangle, \langle w, U_{\{1, -1\}^n} \rangle) \leq O(\varepsilon + \delta).
\]

and conclude that there exists an explicit PRG that \(\varepsilon\)-fools any halfspace on \(n\) variables with seed-length \(O(\log^2 \frac{n}{\varepsilon})\).
A second try at fooling balanced halfspaces

In this section you may use the following theorem, which is a corollary of the Berry-Esseen theorem.

**Theorem 6.** Let $Y_1, \ldots, Y_t$ be independent random variables with $\mathbb{E}[Y_i] = 0$, and denote $\sum_i \mathbb{E}[Y_i^2] = \sigma^2$ and $\sum_i \mathbb{E}[Y_i^4] = \rho$. Let $S_n = \frac{1}{t} \sum_i Y_i$. Then,

$$d(S_n, \mathcal{N}(0, 1)) \leq \frac{\sqrt{\rho}}{\sigma^2},$$

where $\mathcal{N}(0, 1)$ is the normal distribution with mean 0 and variance 1.

To define the construction, given $n$ and $\eta$ we set $t = \frac{1}{n^2}$ and require the following ingredients:

- A 2-UFOHF $\mathcal{H} \subseteq \{ h: [n] \to [t] \}$, such that $\forall i \in [t], |h^{-1}(i)| = \{ x \in [n] \mid h(x) = i \} = \frac{n}{t}$.
- A 4-UFOHF $\mathcal{F} \subseteq \{ f: \{ \frac{n}{t} \} \to \{1, -1\} \}$, i.e., if we let $Y_i$ be the random variable with value $f(i)$ where $f$ is uniform over $F$, then for every distinct $i_1, i_2, i_3, i_4 \in \{ \frac{n}{t} \}$, $(Y_{i_1}, Y_{i_2}, Y_{i_3}, Y_{i_4}) = U_{\{1, -1\}^4}$. For $f \in F$ we let $\text{string}(f) \in \{-1, 1\}^n$ be the string that at location $i$ has value $f(i)$.

For $x \in \Sigma^n$ and $S \subseteq [n]$, we let $x|_S$ denote the substring of $x$ keeping only locations indexed by $S$ (so $x|_S \in \Sigma^{|S|}$). Define $G: \mathcal{H} \times \mathcal{F}^t \to \{1, -1\}^n$ by

$$G(h; f_1, \ldots, f_t) = x,$$

where $x|_{h^{-1}(i)} = \text{string}(f_i)$ for every $i \in [t]$.

6. Show the construction can be efficiently implemented with seed length $O(\frac{\log n}{n^2})$.

7. Prove that when $w$ is $\eta$-balanced, $\langle w, U_{\{1, -1\}^n} \rangle$ is $\eta$-close to $\mathcal{N}(0, 1)$ in the CDF distance.

8. Fix $h \in \mathcal{H}$ and let the probability space be choosing $f_1, \ldots, f_t \in_R \mathcal{F}$. Prove that $\langle w, G(U) \rangle$ is $\zeta_h$-close to $\mathcal{N}(0, 1)$ in the CDF distance, where $\zeta_h = O\left(\frac{\sum_{i=1}^{t} \left(\sum_{j \in h^{-1}(i)} |w_j|^2\right)^2}{\sigma^2} \right)$.

9. A typical $h \in \mathcal{H}$ spreads its weights almost evenly among the buckets. Prove if $w$ is $\eta$-balanced, then $\mathbb{E}_{h \in \mathcal{H}}[\zeta_h] = O(\eta)$.

10. Conclude that $G \varepsilon = O(\eta)$ fools halfspaces on $n$ variables with $\eta$-balanced $w$-s.

A third try at fooling balanced halfspaces

11. Derandomize the selection of $f_1, \ldots, f_t$ to achieve a shorter seed-length, using ideas similar to what we did above. Conclude that there exists an explicit PRG that $O(\eta)$-fools halfspace on $n$ variables having $\eta$-balanced $w$-s with seed-length $O(\log n + \log^2 \frac{1}{\eta})$.

We remark that in the paper they also remove the balance requirement, and achieve error $\varepsilon$ with seed length $O(\log n + \log^2(\frac{1}{\varepsilon}))$, and even that was improved in a later paper to $O(\log \frac{n}{\varepsilon})$. 

4
Question 4

To be given soon.