Probability and Computation: Problem sheet 6 Solutions

Question 1. *Let $G = (V, E)$ be a random graph of n vertices generated as follows: for any pair of vertices $u, v \in V$, $\{u, v\} \in E$ with probability $p \geq 0.01$. Prove that, for large enough n and with high probability, the conductance of G is greater or equal than $1/8$.*
Hint*: Use a Chernoff bound to lower bound the conductance of any fixed set $S \subset V$ (in this step pay special attention to the volume of S!). Then apply the union bound on every subset of V. You may also want to use the fact that for any two integers $1 \leq k \leq n$:*

$$\binom{n}{k} \leq \left(\frac{en}{k}\right)^k.$$

Solution: We will use the fact that

$$\Phi(G) = \min_{S \subseteq V, 1 \leq |S| \leq n/2} \left\{ \frac{|E(S, V \setminus S)|}{\min\{\mathrm{vol}(S), \mathrm{vol}(V \setminus S)\}} \right\}.$$

In order to lower bound $\Phi(G)$, fix an arbitrary set $S \subseteq V$ with $|S| \leq n/2$. Let $Y := |E(S, V \setminus S)|$. Then

$$\mathbf{E}[\,Y\,] = |S| \cdot |V \setminus S| \cdot p.$$

Also let $Z := \mathrm{vol}(S)$. Then

$$\mathbf{E}[\,Z\,] = 2 \cdot \binom{|S|}{2} \cdot p + |S| \cdot |V \setminus S| \cdot p.$$

Applying a Chernoff bound yields,

$$\mathbf{P}[\,Y \leq 1/2 \cdot \mathbf{E}[\,Y\,]\,] \geq \exp\left(-(1/2)^2/2 \cdot \mathbf{E}[\,Y\,]\right) \geq \exp\left(-p/8 \cdot |S| \cdot n)\right).$$

Similarly the version for the upper tails yields,

$$\mathbf{P}[\,Z \geq 2 \cdot \mathbf{E}[\,Z\,]\,] \geq \exp\left(-1/3 \cdot \mathbf{E}[\,Z\,]\right) \geq \exp\left(-p/3 \cdot |S| \cdot n)\right).$$

If both events $Y \geq 1/2 \cdot \mathbf{E}[\,Y\,]$ and $Z \leq 2 \cdot \mathbf{E}[\,Z\,]$ occur, then

$$\Phi(S) = \frac{|E(S, V \setminus S)|}{\min\{\mathrm{vol}(S), \mathrm{vol}(V \setminus S)\}} \geq \frac{|E(S, V \setminus S)|}{\mathrm{vol}(S)} \geq \frac{\frac{1}{2} \cdot |S| \cdot |V \setminus S| \cdot p}{4 \cdot |S| \cdot V \setminus S| \cdot p} = \frac{1}{8}.$$

where we have used the fact that $2 \cdot \binom{|S|}{2} \leq |S| \cdot |V \setminus S|$, as $|S| \leq n/2$. Now a twofold application of the Union Bound yields,

$$\begin{aligned}
\mathbf{P}[\,\Phi(G) \geq 1/8)\,] &= \mathbf{P}\left[\bigcap_{S \subseteq V, 1 \leq |S| \leq n/2} \{\Phi(S) \geq 1/8\}\right] \\
&= 1 - \mathbf{P}\left[\bigcup_{S \subseteq V, 1 \leq |S| \leq n/2} \{\Phi(S) < 1/8\}\right] \\
&= 1 - \mathbf{P}\left[\bigcup_{k=1}^{n/2} \bigcup_{S \subseteq V, |S| = k} \{\Phi(S) < 1/8\}\right] \\
&\geq 1 - \sum_{k=1}^{n/2} \mathbf{P}\left[\bigcup_{S \subseteq V, |S| = k} \{\Phi(S) < 1/8\}\right] \\
&\geq 1 - \sum_{k=1}^{n/2} \sum_{S \subseteq V, |S| = k} \mathbf{P}[\,\{\Phi(S) < 1/8\}\,].
\end{aligned}$$

From the above, we conclude (by applying a Union bound once more!)

$$\begin{aligned}\mathbf{P}[\,\{\Phi(S) < 1/8\}\,] &\le \exp\left(-p/8 \cdot |S| \cdot n\right)\right) + \exp\left(-p/3 \cdot |S| \cdot n\right)\right) \\ &\le 2 \cdot \exp\left(-p/8 \cdot |S| \cdot n\right)\right).\end{aligned}$$

Hence,

$$\begin{aligned}\mathbf{P}[\,\Phi(G) \ge 1/8\,] &\ge 1 - \sum_{k=1}^{n/2} \sum_{S \subseteq V, |S|=k} 2 \cdot \exp\left(-p/8 \cdot k \cdot n\right) \\ &\ge 1 - \sum_{k=1}^{n/2} \binom{n}{k} \cdot 2 \cdot \exp\left(-p/8 \cdot k \cdot n\right) \\ &\ge 1 - 2\sum_{k=1}^{n/2} \left(\frac{en}{k}\right)^k \exp\left(-p/8 \cdot k \cdot n\right) \\ &\ge 1 - 2\sum_{k=1}^{n/2} \exp\left(-\ln(en) \cdot k\right) \cdot \exp\left(-p/8 \cdot k \cdot n\right) \\ &\ge 1 - 2\sum_{k=1}^{n/2} \exp\left(-p/16 \cdot k \cdot n\right) \\ &\ge 1 - 2 \cdot (n/2) \cdot \exp(-\Omega(n)) \ge 1 - o(1).\end{aligned}$$

Question 2. *(cf. Slide 12 of Lecture 13/14 on Sublinear Algorithms).*

1. *Prove that for any triple of pairwise different indices i, j, k, the random variables $\{\sigma_{i,j}, \sigma_{j,k}\}$ may not necessarily be independent.*
2. *Can you find a concrete example (i.e., specify n, p, i, j and k) in which these random variables are independent?*

Solution:

1. For example, pick $n = 2$, $r = 3$, $p_1 = 2/3$ and $p_2 = 1/3$. Then,

   $$\mathbf{P}[\,\sigma_{1,2} = 1\,] = \mathbf{P}[\,\sigma_{2,3} = 1\,] = \|p\|_2^2 = 4/9 + 1/9 = 5/9.$$

   But on the other hand, since $\{\sigma_{1,2} = 1\} \cap \{\sigma_{2,3} = 1\}$ is equivalent to saying that all the first three samples must be identical,

   $$\mathbf{P}[\,\{\sigma_{1,2} = 1\} \cap \{\sigma_{2,3} = 1\}\,] = p_1^3 + p_2^3 = (2/3)^3 + (1/3)^3 = 8/27 + 1/27 = 9/27 = 1/3.$$

   Since $(5/9)^2 < 1/3$, the claim follows.

2. Let $n \ge 2$ and $p = (1/n, \ldots, 1/n)$. Then,

   $$\mathbf{P}[\,\sigma_{1,2} = 1\,] = \mathbf{P}[\,\sigma_{2,3} = 1\,] = 1/n.$$

   But also

   $$\mathbf{P}[\,\{\sigma_{1,2} = 1\} \cap \{\sigma_{2,3} = 1\}\,] = \sum_{n=1}^{n} (1/n)^3 = (1/n)^2,$$

   which establishes the independence.

Question 3. *(cf. Slide 13 of Lecture 13/14 on Sublinear Algorithms). Demonstrate that it is not possible to construct any randomised algorithm for testing uniformity that has a one-sided error.*

1. *Specifically prove that for any number $r \geq 1$, there is no randomised algorithm which takes at most r samples and satisfies the following two properties:*
   (a) *If $p = u$, then the algorithm always accepts.*
   (b) *If p is ϵ-far from u, then the algorithm rejects with probability > 0.*
2. *Using the same argument, proceed to prove that there is also no randomised algorithm that takes at most r samples and satisfies the following two properties:*
   (a) *If $p = u$, then the algorithm accepts with probability > 0.*
   (b) *If p is ϵ-far from u, then the algorithm always rejects.*

Solution:

1. Let $u = (1/n, \ldots, 1/n)$ be the uniform distribution. Further, let q be any distribution which is ϵ-far from u. Note that for any specific set of samples $(x_1, x_2, \ldots, x_r) \in \{1, \ldots, n\}^r$, the algorithm has to return ACCEPT, as it always returns ACCEPT if $p = u$. However this implies that if $p = q$, the algorithm will never REJECT.
2. We use the same u and q as in the previous part, but here we require additionally that $q_j > 0$ for any $1 \leq j \leq n$. Let $(x_1, x_2, \ldots, x_r) \in \{1, \ldots, n\}^r$ be any set of samples for which the algorithm returns ACCEPT (this set of samples must exist by condition (a)). Since $q_j > 0$ for any $1 \leq j \leq n$, it is possible for the algorithm to obtain the same samples if the input distribution is q, but then this would imply that the algorithm would not always return REJECT if the input is ϵ-far from u.

Question 4. *(easy) What is the time complexity for applying the Random Projection Method to a set of P input vectors?*

Solution: We first need to construct the random $M \times N$-matrix, which takes $O(MN)$ time. Then we need to multiply the random matrix to each of the P input vectors, each of which takes $O(MN)$ time, amounting to a total time of $O(MNP)$.

Question 5. *Demonstrate that it is essential for the Random Projection Method to choose the linear function f randomly. Specifically, prove that for any linear function $f : \mathbb{R}^N \to \mathbb{R}^M$ there are two vectors $x_1, x_2 \in \mathbb{R}^N$, $x_1 \neq x_2$, such that $f(x_1) = f(x_2)$.*
Hint: *Your proof should at some point exploit that $N > M$.*

Solution: As in the description of the Random Projection Method, the linear function $f : \mathbb{R}^N \to \mathbb{R}^M$ applied to any vector $w \in \mathbb{R}^N$ is the same as the matrix-vector product

$$f(w) = R \cdot w,$$

where R is a $M \times N$ matrix. Or written more explicitly,

$$f \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ \vdots \\ w_N \end{pmatrix} = \begin{pmatrix} \vdots & \vdots & & \vdots \\ r_1 & r_2 & \cdots & r_N \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \end{pmatrix} \cdot \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ \vdots \\ w_N \end{pmatrix},$$

where $\{r_1, r_2, \ldots, r_N\}$ is a set of M-dimensional vectors. Since $N > M$ and the fact that N is the largest number of linearly independent vectors, it follows that the set of vectors $\{r_1, r_2, \ldots, r_N\}$ is not linearly independent. Thus there are coefficients $\alpha_1, \alpha_2, \ldots, \alpha_N$, not all being equal to zero, such that

$$\sum_{j=1}^{N} \alpha_j \cdot r_j = \vec{0}.$$

Thus for every entry $1 \leq i \leq M$,

$$\sum_{i=1}^{N} \alpha_j \cdot r_{i,j} = \sum_{i=1}^{N} r_{i,j} \cdot \alpha_j = 0.$$

This implies that

$$f \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \vdots \\ \alpha_N \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Based on this finding, it is straightforward to pick two vectors $x_1 \in \mathbb{R}^N$ and $x_2 \in \mathbb{R}^N$ such that $x_1 \neq x_2$ but $f(x_1) = f(x_2)$. Let $x_1 \in \mathbb{R}^n$ be arbitrary and $x_2 = x_1 + \alpha$. Then, thanks to the linearity of f,

$$f(x_2) = f(x_1 + \alpha) = f(x_1) + f(\alpha) = f(x_1).$$
