

Due on November 24
In class, at the beginning of the lecture

The work you submit must be your own. You may discuss problems with each other; however, you should prepare written solutions alone. In particular, you should not leave with any written notes from such discussions. The style and clarity of your answers will be an important factor in the grade.

There are 4 questions, 25% each. Questions and solutions 2,3,4 are due to Greg Herman.

1. What we call the Gandalf-Frodo protocol, usually goes by the name of **Arthur-Merlin** protocol.

For part (a), on input $\langle f(x_1, \dots, x_n) \rangle$, Gandalf is trying to convince Frodo that there is a smaller arithmetical formula g computing the same polynomial as f . So Gandalf sends g to Frodo, and the degree of the polynomial computed by g is at most the size of g , which is at most the size of f . Suppose the size of f was s , then Frodo picks n integers at random from $\{1, \dots, 4sn\}$, and check whether $f(r_1, \dots, r_n) - g(r_1, \dots, r_n) = 0$. If the answer is no, Frodo “rejects”, and otherwise accepts.

If f is indeed optimal, then for any g of smaller size, $f - g \neq 0$, and the probability that Frodo does not discover this is $\leq \frac{1}{4}$: by the Schwartz-Zippel lemma, if $f - g$ is not the zero polynomial, then the probability that for a random $r_1, \dots, r_n \in \{1, \dots, 4sn\}$ $f - g = 0$ is at most $\frac{n \cdot s \cdot (4sn)^{n-1}}{(4sn)^n} = \frac{1}{4}$. If f is not optimal, then Gandalf provides a smaller g computing the same polynomial as f , and $f - g \equiv 0$, so Frodo always answers “yes”, and the probability of error in this case is $0 \leq \frac{1}{4}$.

Part (b) of this question is basically a restatement of the proof of $\mathbf{BPP} \subseteq \Sigma_2^P$ which was shown in class: first use amplification to bring the error down to 2^{-n} . Then use the idea of “translations.”

2. Fix λ and set $\epsilon = \frac{1-\lambda^2}{1+\lambda^2}$ (it is clear that $\epsilon > 0$ whenever $\lambda < 1$). Now take an (n, d, λ) -expander $G = ([n], E)$ with a subset of vertices $S \subset [n]$ and let T be the “neighbourhood” of S :

$$T = \{i \in [n] \mid \exists j \in S, \{i, j\} \in E\}$$

Denote $k = |S|$ and $m = |T|$. Pick x to be a uniform probability distribution on S :

$$x_i = \begin{cases} \frac{1}{k} & \text{if } i \in S \\ 0 & \text{otherwise} \end{cases}$$

The components of x parallel and orthogonal to the uniform distribution (denoted by x^{\parallel}

and x^\perp , respectively) satisfy

$$\begin{aligned} x_i^\parallel &= \frac{1}{n} \\ x_i^\perp &= \begin{cases} \frac{1}{k} - \frac{1}{n} & \text{if } i \in S \\ -\frac{1}{n} & \text{otherwise} \end{cases} \\ \|x^\perp\| &= \sqrt{k \left(\frac{1}{k} - \frac{1}{n} \right)^2 + (n-k) \frac{1}{n^2}} = \sqrt{\frac{n-k}{nk}} \end{aligned}$$

If we let A be the G 's normalized adjacency matrix, then taking a random step on G starting with distribution x will give us the distribution $y = Ax$. As vertices reachable in that step are precisely those from T , we will have $y_j = 0$ whenever $j \notin T$. Now we have

$$y = Ax = A(x^\parallel + x^\perp) = Ax^\parallel + Ax^\perp = x^\parallel + Ax^\perp,$$

and therefore $(Ax^\perp)_j = -\frac{1}{n}$ whenever $j \notin T$. From the fact that Ax^\perp is orthogonal to the uniform distribution (note that by definition x^\perp is orthogonal to the uniform distribution $\mathbf{1} = (1, 1, \dots, 1)$, and hence $\langle x^\perp, \mathbf{1} \rangle = 0$, and $\langle Ax^\perp, \mathbf{1} \rangle = (Ax^\perp)^T \mathbf{1} = (x^\perp)^T (A^T \mathbf{1}) = (x^\perp)^T (A\mathbf{1}) = (x^\perp)^T \mathbf{1} = \langle x^\perp, \mathbf{1} \rangle = 0$, and so it follows that Ax^\perp and $\mathbf{1}$ are orthogonal) we know that $\sum_{j \in [n]} (Ax^\perp)_j = 0$, and thus

$$\sum_{j \in T} (Ax^\perp)_j = - \sum_{j \notin T} (Ax^\perp)_j = -(n-m) \left(-\frac{1}{n}\right) = \frac{n-m}{n}.$$

By the inequality between the quadratic and arithmetic averages

$$\begin{aligned} \sum_{j \in T} (Ax^\perp)_j^2 &\geq \frac{1}{m} \left(\sum_{j \in T} (Ax^\perp)_j \right)^2 \\ &= \frac{(n-m)^2}{mn^2}, \end{aligned}$$

from which we can calculate

$$\begin{aligned} \|Ax^\perp\| &= \sqrt{\sum_{j \in [n]} (Ax^\perp)_j^2} \\ &= \sqrt{\sum_{j \in T} (Ax^\perp)_j^2 + \sum_{j \notin T} (Ax^\perp)_j^2} \\ &\geq \sqrt{\frac{n-m}{nm}}. \end{aligned}$$

Now, as all but the first eigenvalue of A have absolute values bounded by λ , we know that

$$\begin{aligned}
\lambda \|x^\perp\| &\geq \|Ax^\perp\| \\
\lambda \sqrt{\frac{n-k}{nk}} &\geq \sqrt{\frac{n-m}{nm}} \\
m(\lambda^2(n-k) + k) &\geq kn \\
\frac{k}{m} &\leq \frac{\lambda^2(n-k) + k}{n} \\
&= \lambda^2 + \frac{k}{n}(1 - \lambda^2) \\
&\leq \lambda^2 + \frac{1}{2}(1 - \lambda^2) \\
&= \frac{1 + \lambda^2}{2}
\end{aligned}$$

which finally yields

$$\frac{|T|}{|S|} = \frac{m}{k} \geq \frac{2}{1 + \lambda^2} = 1 + \frac{1 - \lambda^2}{1 + \lambda^2} = 1 + \epsilon$$

as required.

For the second part, denote by $\eta_i(v)$ the set of vertices reachable from v in at most i steps. Simple induction on i shows that if G is an ϵ -expander, $|\eta_i(v)| > \min\{(1 + \epsilon)^i, \frac{n}{2}\}$. Now taking any two vertices u and v and setting $k = \log_{1+\epsilon}(\frac{n}{2})$ we get $|\eta_k(u)|, |\eta_k(v)| > \frac{n}{2}$. Therefore $\eta_k(u)$ and $\eta_k(v)$ cannot be disjoint, and we can find a vertex x with paths of length at most k to both u and v . It follows that the distance between u and v , and thus also the diameter of G , is at most $2k = O(\log_2(n))$.

3. According to the hint, we let x be a unit length eigenvector corresponding to λ_2 . Elementary algebra shows that (letting e_{ij} be the number of edges between i and j)

$$\begin{aligned}
1 - \lambda_2 &= x^T x - x^T(\lambda_2 x) = x^T I x - x^T(Ax) \\
&= \sum_i x_i^2 - \sum_{i,j} A_{ij} x_i x_j \\
&= \frac{1}{d} \left(\sum_i dx_i^2 - \sum_{i,j} e_{ij} x_i x_j \right)
\end{aligned}$$

There are two things to consider making the next step. First, $\sum_i dx_i^2 = \sum_{\{i,j\} \in E} (x_i^2 + x_j^2)$. To see why this is true, notice that we are summing *over edges* in the RHS, *not over ordered pairs*, so $\{i, j\}$ and $\{j, i\}$ count as one and the same edge. Each vertex i has exactly d edges coming out of it, so it will appear d many times in the LHS. Now, when we do the sum $\sum_{i,j} e_{ij} x_i x_j$ in the line above, we are summing *over ordered pairs*, so each edge $\{i, j\}$ counts twice as an ordered pair, as (i, j) and as (j, i) , and hence the factor of 2 in the line below.

$$\begin{aligned}
&= \frac{1}{d} \sum_{\{i,j\} \in E} (x_i^2 - 2x_i x_j + x_j^2) \\
&= \frac{1}{d} \sum_{\{i,j\} \in E} (x_i - x_j)^2.
\end{aligned}$$

Now pick u and v such that x_u, x_v are the largest and smallest component of x , respectively. As the graph is connected, we know that there exists a path of length $k < n$ from u to v . Let r_i be the i -th vertex on that path:

$$\begin{aligned} r_0 &= u, \\ r_k &= v, \\ \{r_i, r_{i+1}\} &\in E. \end{aligned}$$

All components of our sum are non-negative. Therefore we can achieve a lower bound by adding up only some of them – namely those for the edges on our path from u to v :

$$\sum_{\{i,j\} \in E} (x_i - x_j)^2 \geq \sum_{i=0}^{k-1} (x_{r_i} - x_{r_{i+1}})^2$$

and we use the “arithmetical vs. the quadratic mean inequality”, $\frac{1}{n} \sum_i a_i \leq \left(\frac{1}{n} \sum_i a_i^2\right)^{\frac{1}{2}}$, to conclude

$$\begin{aligned} &\geq \frac{1}{k-1} \left(\sum_{i=0}^{k-1} x_{r_i} - x_{r_{i+1}} \right)^2 \\ &> \frac{1}{n} (x_u - x_v)^2 \end{aligned}$$

The components of x add up to 0, because it is orthogonal to the “all-ones” vector corresponding to λ_1 . Therefore $x_u > 0 > x_v$, and therefore $x_u - x_v > x_u$. Additionally, we can assume that $|x_u| \geq |x_v|$ (if not, pick $-x$ instead of x). Then x_u is the component with the largest absolute value and, as $\|x\| = 1$,

$$1 = \sum_i x_i^2 \leq n x_u^2.$$

From the above two we conclude that

$$1 - \lambda_2 \geq \frac{1}{d} \frac{1}{n} \frac{1}{n} = \frac{1}{dn^2},$$

as required. (Note that we need both $|\lambda_n|, |\lambda - 2| < \lambda$ to show that every such graph is an expander, but we showed that $|\lambda_n| < \lambda$ in class.)

- Pick $q = p^2$ (the prime p will be determined later), and construct X as shown in class to be a $(p^4, p^2, \frac{1}{p})$ -expander. Then let

$$\begin{aligned} H_0 &= X^2 \\ H_{i+1} &= H_i \otimes X \end{aligned}$$

Now prove by induction that H_i is a $(p^{4(i+1)}, p^4, \frac{2^i}{p})$ -expander. The base case for $i = 0$ follows from the properties of X . For the induction step we know that H_i and X have second largest eigenvalues α and β , bounded by $\frac{2^i}{p}$ and $\frac{1}{p}$, respectively. From the analysis

of the zig-zag product presented in class we know that the resulting graph H_{i+1} will have its second eigenvalue bounded by $\sqrt{\alpha^2 + \beta^2 + \alpha\beta + \beta^4}$. But clearly,

$$\begin{aligned}\alpha^2 &\leq \frac{4^i}{p^2}, \\ \beta^2 &\leq \frac{1}{p^2}, \\ \alpha\beta &\leq \frac{2^i}{p^2}, \\ \beta^4 &\leq \frac{1}{p^4} < \frac{1}{p^2},\end{aligned}$$

and so this eigenvalue is bounded by $\frac{\sqrt{4^i + 2^i + 2}}{p}$. As $4^i + 2^i + 2 \leq 4^{i+1}$, the induction is established.

We now look at H_{15} . It is a $(p^{64}, p^4, \frac{32}{p})$ -expander. Thus, picking $D = p^4$ for any prime $p > 64$ we have constructed a $(D^{16}, D, \frac{1}{2})$ -expander, as required. As neither D nor p depend on n , the whole construction can be performed in space $O(1)$ – in fact, we can simply embed the “precomputed” H_{15} into the reachability algorithm.