

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. Question 2,3,4 are due to Greg Herman.

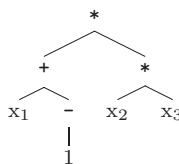
1. Recall the definition of a polytime proof system $F(x, y)$. Suppose that we allow F to be a *randomized polytime algorithm*. We present an extension of **NP** which we shall call **GF**, which stands for **G**andalf and **F**rodo. Gandalf¹ is an all-powerful wizard that tries to convince Frodo, who is a probabilistic polytime verifier, that an input string x is in some language.

If the string x is in the language, then Gandalf can make Frodo accept most of the time (by providing him with a suitable y). If the string x is not in the language, then no matter what Gandalf does (i.e., what y he produces), Frodo will reject most of the time.

Formally, L is in **GF** if there is a non-deterministic polytime (in $|x|$) TM F such that,

$$\begin{aligned} x \in L & \text{ then } \exists y, F(x, y) \text{ accepts on } 3/4 \text{ of the paths} \\ x \notin L & \text{ then } \forall y, F(x, y) \text{ rejects on } 3/4 \text{ of the paths.} \end{aligned}$$

An *arithmetic formula* over some fixed field \mathbb{F} is a tree whose leaves are labeled by variables or constants from \mathbb{F} , and whose inner nodes are labeled by arithmetic operations from among $\{+, -, *\}$. Each arithmetic formula $f(x_1, \dots, x_n)$ computes some polynomial $p(x_1, \dots, x_n)$ over \mathbb{F} . For example, the formula f given by



corresponds to the polynomial $p = x_1x_2x_3 - x_2x_3$. The same polynomial $p(x_1, \dots, x_n)$ may or may not be computed by a smaller formula, where the size of a formula is just the number of leaves (4 in our example). We say that a formula is *optimal* if it is the smallest formula computing the given polynomial. Let $L = \{ \langle f \rangle \mid f \text{ is a non-optimal arithmetic formula} \}$.

For simplicity, assume $\mathbb{F} = \mathbb{Z}$.

- (a) Use the Schwartz-Zippel lemma to show that $L \in \mathbf{GF}$.
- (b) Show that $\mathbf{GF} \subseteq \Sigma_2^p$.

¹Actually, a better name would be Sauron, “The Dark Lord”, since this entity may be malicious, and want to convince Frodo that $x \in L$ whether it’s true or not.

2. We have shown that every (n, d, λ) -expander has logarithmic diameter. Provide a different proof of this fact using the notion of vertex expansion.

An undirected graph $G = (V, E)$ is called an ϵ -expander (for $\epsilon > 0$) if for every set S of vertices with $|S| \leq \frac{1}{2}|V|$ we have

$$|\{u \in V | \exists v \in S, \{u, v\} \in E\}| \geq (1 + \epsilon)|S|$$

Show that:

- for every $\lambda < 1$ there exists an $\epsilon > 0$ such that every (n, d, λ) -expander is an ϵ -expander
 - every ϵ -expander has logarithmic diameter
3. Complete the proof of the fact that every connected, non-bipartite, d -regular graph on n vertices is an $(n, d, 1 - \frac{1}{dn^2})$ -expander by showing that the second largest eigenvalue λ_2 of its normalized adjacency matrix A satisfies

$$\lambda_2 \leq 1 - \frac{1}{dn^2}.$$

Hint: Consider a unit length eigenvector x corresponding to λ_2 . Show that

$$1 - \lambda_2 = x^T(I - A)x = \frac{1}{d} \sum_{\{i,j\} \in E} (x_i - x_j)^2$$

and then bound the value of the sum by $\frac{1}{n^2}$.

4. Presented logarithmic space algorithm for undirected reachability relies on having (for some constant D) a $(D^{16}, D, \frac{1}{2})$ -expander H . Prove that we can construct one in space $O(1)$.

Hint: We have shown a construction of a $(q^2, q, q^{-\frac{1}{2}})$ -expander for every prime power q . Use it!