

Due on October 13
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.

Each question is worth 10%.

1. $1 - \prod_{i=1}^n (1 - x_i)$
2. If $\text{OR}(x_1, \dots, x_n) = 0$, then $x_1 = \dots = x_n = 0$, so $q_i = 0$ for all i , so $1 - q_i = 1$ for all i , so their product p is 1, so $1 - p = 0$.

Each of the q_i is a sum of variables, i.e., of the form $(x_{i_1} + \dots + x_{i_l})$. If we multiply $O(\log(n))$ such terms, we obtain degree $O(\log(n))$. Note that the degree of a multivariate polynomial is calculated by writing it out as a sum of monomials—unique up to order of summation—and find the monomial with the highest degree, where the degree of $(x_1^{a_1} \dots x_l^{a_l})$ is $a_1 + \dots + a_l$.

3. Since the S_i form a non-ascending chain, it follows that $|T \cap S_i| > 1$ iff $|T \cap S_{\log(n)+2}| > 1$, which is true if at least two variables “survive” all the way from S_0 to $S_{\log(n)+2}$.

The probability of this happening is bounded above by $\binom{n}{2} 4^{-(\log(n)+2)} < \frac{1}{16}$, since there are $\binom{n}{2}$ ways to choose a pair of variables, and then there is a probability of $\frac{1}{2^{\log(n)+2}}$ that each “survives” until the end. Note that we could have given a tighter bound, since we are overcounting (these pairs intersect). We could have accomplished that with the “inclusion-exclusion principle”, but we don’t need such tight bounds in this case.

In fact, the following (even bigger) bound will do just fine for us:

$$\Pr[|T \cap S_{\log(n)+2}| > 1] \leq \Pr[|T \cap S_{\log(n)+2}| \geq 1] \leq \binom{n}{1} 2^{-(\log(n)+2)} = \frac{1}{4}.$$

4. Suppose that $|T \cap S_0| = 1$. Then we are set. Otherwise, $|T \cap S_0| = |T| > 1$, and let i be such that $|T \cap S_{i-1}| > 1$ and $|T \cap S_i| \leq 1$. Let $t = |T \cap S_{i-1}|$. The probability that $|T \cap S_i| = 1$ under the assumption that $t > 1$ and $|T \cap S_i| \leq 1$ is given by

$$\frac{t2^{-t}}{2^{-t} + t2^{-t}} = \frac{t}{t+1} \geq \frac{2}{3}$$

since $t2^{-t}$ is the probability that one of the t variables “survives”, and 2^{-t} is the probability that none of the t variables “survive.”

We now put case 1 and 2 together, to obtain a lower bound for $\Pr[\exists i \text{ with } |T \cap S_i| = 1]$. Case 1 does not occur with probability $\frac{3}{4}$, and in case 2 we get what we want with probability $\geq \frac{2}{3}$, and multiplying the two values we obtain $\geq \frac{1}{2}$.

5. The error probability of P is $\geq \frac{1}{2^t}$. We want $\frac{1}{2^t} < \varepsilon$, so $t > \log(\varepsilon^{-1})$. The polynomial for the $\text{AND}(x_1, \dots, x_n)$ is just the product of the p_i 's with x_j replaced by $(1 - x_j)$.
6. The degree of the polynomial approximating the AND and OR gates with error $\leq \frac{\varepsilon}{s}$ is $O(\log(\frac{s}{\varepsilon}) \log(n))$. So the degree of the polynomial approximating such a circuit of depth t is $O(\log^t(\frac{s}{\varepsilon}) \log^t(n)) = O(\log^{t+1}(\frac{s}{\varepsilon}))$, since $s = s(n)$ is a polynomial in n .
7. For a random polynomial thus generated, the expectation of the number of inputs for which it computes the circuit correctly is $(1 - \varepsilon)2^n$. Suppose no such polynomial \mathcal{P} exists. Then, for any \mathcal{P} , it answers correctly on $< (1 - \varepsilon)2^n$ many inputs. This is a contradiction.
8. If the number of 1s is odd, \mathcal{Q} is -1 , and if it is even it is $+1$, which corresponds to the multiplication.
9. The natural basis for $L(S)$ is B given by the set of functions $f_s : S \rightarrow \mathbb{R}$ where $f_s(s) = 1$ and $f_s(s') = 0$ for $s' \neq s$. Now, any function in $L(S)$ can be written as a linear combination of functions in B . Now note that any f_s can be represented by an n -degree multi-variate multilinear polynomial as follows:

$$f_{(s_1, \dots, s_n)}(x_1, x_2, \dots, x_n) \mapsto \frac{1}{2^n} (1 - s_1 \cdot x_1)(1 - s_2 \cdot x_2) \cdots (1 - s_n \cdot x_n)$$

write this polynomial as a sum of monomials. Each such monomial (without the constant coefficient multiplying it in front) is of the form $x_{i_1} x_{i_2} \cdots x_{i_k}$ with $k \leq n$.

Now consider such monomials in the representation of a given f_s . If a monomial has at most $n/2$ many variables, i.e., $k \leq n/2$, then leave it as it is. Otherwise, $k > n/2$, and replace this monomial by the polynomial $g = \mathcal{Q}(x_1, x_2, \dots, x_n) x_{j_1} x_{j_2} \cdots x_{j_{n-k}}$ where $\{x_{j_1}, x_{j_2}, \dots, x_{j_{n-k}}\} = \{x_{i_1}, x_{i_2}, \dots, x_{i_k}\}^c$. Two things about g . First, it is of degree $(\sqrt{n} + n)/2$, and second, on S it takes on the same values as the original monomial (do you see why?).

Thus, we just showed that any f_s can be represented with a multi-variate multi-linear polynomial of degree at most $(\sqrt{n} + n)/2$. We are not quite done yet; to show that $\dim(L(S)) \leq \dim(\text{POL})$, we need to show that this mapping ($f_s \xrightarrow{h} p \in \text{POL}$, where we extend h from $\text{basis}(L(S))$ to all of $L(S)$ in the natural way to obtain a vector space homomorphism) is such that $h(S)$ is linearly independent.

Suppose that $h(S)$ is linearly dependent. Then, there are $p_1, p_2, \dots, p_k \in h(S)$ such that $c_1 p_1 + c_2 p_2 + \cdots + c_k p_k = 0$ (assume all $c_i \neq 0$), i.e., it is the 0 polynomial. We now examine the pre-images of these p_i 's in $L(S)$, i.e., we look at $f_{s_1}, f_{s_2}, \dots, f_{s_k}$, where $h(f_{s_i}) = p_i$ (note that these pre-images are unique, i.e., $|S| = |h(S)|$). It follows that the function $f = c_1 f_{s_1} + c_2 f_{s_2} + \cdots + c_k f_{s_k}$ is mapped by h to the zero polynomial. It follows therefore that $f = 0$, i.e., f is the zero function. But $f(s_1) = c_1 f_{s_1}(s_1) = c_1 \neq 0$, contradiction.

10. We showed in 6 that the degree of a polynomial approximating a bounded depth circuit is poly-logarithmic. On the other hand, we need degree higher than $\frac{\sqrt{n}}{2}$ to approximate parity. Thus $\text{PARITY} \notin \mathbf{AC}^0$.