

**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.

10 questions in total, 10% per question.

In this assignment we are going to give a slightly different proof of  $\text{PARITY} \notin \text{AC}^0$ , which also uses the probabilistic argument, but with a dash of linear algebra.

$\text{AND}(x_1, \dots, x_n)$ , can be represented by the polynomial  $\prod_{i=1}^n x_i = x_1 x_2 \dots x_n$ , over, say,  $\mathbb{R}$ .

- Using  $(1 - x)$  to represent NOT, and de Morgan laws, give a polynomial representation of the OR function.

The problem with this is that our polynomials have degree  $n$ . This can be improved by a probabilistic method. We construct a random polynomial as follows: let  $S_0 = \{1, \dots, n\}$ . Let  $S_i \supseteq S_{i+1}$ , for  $i \in \{0, \dots, \log(n) + 1\}$ , where  $S_{i+1}$  is chosen randomly so that for all  $j \in S_i$ ,  $\Pr[j \in S_{i+1}] = \frac{1}{2}$ . Let  $q_i = \sum_{j \in S_i} x_j$  be a random polynomial (of degree 1).

- If  $\text{OR}(x_1, \dots, x_n) = 0$ , show that  $1 - p = 0$ , where  $p$  is the polynomial given by the product  $\prod_{i=0}^{\log(n)+2} (1 - q_i)$ . What is the degree of the polynomial  $p$ ?

If, on the other hand,  $\text{OR}(x_1, \dots, x_n) = 1$ , then there is at least one  $x_i = 1$ . We are going to show now that in this case, the probability is  $\geq \frac{1}{2}$  that one of the polynomials  $q_i$  has the value exactly 1, and so  $\Pr[1 - p = 1] \geq \frac{1}{2}$ . We need to argue that for any choice of a non-empty  $T \subseteq S_0$ , the probability is at least  $\frac{1}{2}$  that there is at least one  $i \in \{0, 1, \dots, \log(n) + 2\}$  such that the size of  $T \cap S_i$  is exactly 1. We accomplish this by cases.

- Case 1.** For all  $i \in \{0, 1, \dots, \log(n) + 2\}$ , we have that  $|T \cap S_i| > 1$ .  
Give an upper bound for this undesirable case.
- Case 2.** There is an  $i \in \{0, 1, \dots, \log(n) + 2\}$  with  $|T \cap S_i| \leq 1$ .

So the polynomial  $(1 - p)$  approximates the OR, but with a success rate of only  $\frac{1}{2}$ . But we can improve this by selecting independent polynomials  $p_1, p_2, \dots, p_t$ , and then using  $P = 1 - \prod_{i=1}^t p_i$ , which has degree  $O(t \log(n))$ .

- What is the error probability of  $P$ ? How large must  $t$  be to get an error probability below a given constant  $\varepsilon$ ? Construct also the corresponding polynomial for the AND function.

We want to simulate an  $\mathbf{AC}^0$  circuit with size  $s$  and depth  $t$  using our polynomials, so that the error probability is at most  $\varepsilon$ . We replace all the gates with our polynomials, making sure that the error probability for each gate is  $\leq \frac{\varepsilon}{s}$ .

6. What is the degree of the resulting polynomial, as a function of  $\varepsilon, s, t$ ? (Give big-Oh notation.) If  $s$  is a polynomial in  $n$  and  $\varepsilon$  a constant, what sort of function is this (in terms of growth)?

Thus, for every  $\mathbf{AC}^0$  function  $f$ , a polynomial  $p$  can be randomly generated that has very small degree and such that for any  $(a_1, \dots, a_n) \in \{0, 1\}^n$  the probability is at least  $(1 - \varepsilon)$  that  $f(a_1, \dots, a_n) = p(a_1, \dots, a_n)$ .

7. Conclude from this that there must be at least one choice of a *fixed* polynomial  $\mathcal{P}$  for which  $f(a_1, \dots, a_n) = \mathcal{P}(a_1, \dots, a_n)$  for all  $(a_1, \dots, a_n) \in S$ , where  $|S| \geq (1 - \varepsilon)2^n$ .

Identify TRUE with  $-1$  and FALSE with  $+1$ . The linear function that maps  $0$  to  $1$  and  $1$  to  $-1$  is  $x \mapsto 1 - 2x$ . The inverse is  $x \mapsto \frac{(1-x)}{2}$ . Apply this linear function to the polynomial  $\mathcal{P}$  that correctly simulates  $f$  on  $(1 - \varepsilon)2^n$ -many inputs to obtain a polynomial  $\mathcal{Q}$  of the same degree—which now correctly simulates  $f$  transformed to use  $\{-1, +1\}^n$ , again over  $(1 - \varepsilon)2^n$ -many inputs.

Suppose that the parity function is in  $\mathbf{AC}^0$ . Then there must be such a polynomial  $\mathcal{Q}$  for parity.

8. Show that for  $(1 - \varepsilon)2^n$ -many input strings (in  $\{-1, +1\}^n$ ),  $\mathcal{Q}(y_1, \dots, y_n) = \prod_{i=1}^n y_i$ , i.e.,  $\mathcal{Q}$  corresponds exactly to multiplication.

Finally, we show that there is no polynomial  $\mathcal{Q}$  of degree  $\frac{\sqrt{n}}{2}$  that correctly represents the function  $\prod_{i=1}^n y_i$  for  $(1 - \varepsilon)2^n$  strings in  $\{-1, +1\}^n$ .

9. Prove the assertion in the above paragraph. Here is the outline of a possible proof: let  $S = \{(y_1, \dots, y_n) \in \{-1, +1\}^n \mid \prod_{i=1}^n y_i = \mathcal{Q}(y_1, \dots, y_n)\}$  where  $\mathcal{Q}$  is a polynomial of degree  $\frac{\sqrt{n}}{2}$  that correctly represents  $\prod_{i=1}^n y_i$  on  $(1 - \varepsilon)2^n$  many strings in  $\{-1, +1\}^n$ . Thus,  $|S| \geq (1 - \varepsilon)2^n$ . You can assume that  $\mathcal{Q}$  is *multilinear*, that is, no variable has exponent larger than  $1$ . (Why can you assume that?) Let  $L(S)$  be the vector space (over  $\mathbb{R}$ ) of functions  $f : \mathbf{S} \rightarrow \mathbb{R}$ . Check that the dimension of  $L(S)$ ,  $\dim(L(S))$ , is  $|S|$ . On the other hand, let POL be the set of  $n$ -variable multi-linear polynomials of degree  $\frac{(n + \sqrt{n})}{2}$ . Then, POL is also a vector space (over  $\mathbb{R}$ ), with the usual polynomial addition and multiplication by scalars in  $\mathbb{R}$ . Show that  $\dim(\text{POL})$  is  $\sum_{i=0}^{\frac{(n + \sqrt{n})}{2}} \binom{n}{i}$ , and use the Stirling approximation to show that it is strictly smaller than  $|S|$ . Now argue that  $\dim(L(S)) \leq \dim(\text{POL})$ , to get a contradiction.

10. Conclude that PARITY  $\notin \mathbf{AC}^0$ .