Problem 1: Big languages in \(\text{P}_{/\text{poly}}\)

(a) We saw in the lecture that
\[
\text{UHALT} = \{1^n : n = \langle \alpha, x \rangle, M_\alpha(x) \text{ halts} \}
\]
is in \(\text{P}_{/\text{poly}}\). Show that \(\text{UHALT}\) is undecidable.

**Note:** There are two ways to do it (or more). One is by reducing to \(\text{HALT}\), the other is by redoing the proof of undecidability of \(\text{HALT}\). The reference solution will use the first way, but the second way is fine as well.

(b) Show that there is a decidable language \(L\) such that \(L \in \text{P}_{/\text{poly}}\) but \(L \notin \text{P}\).

**Hint:** Show that there exists a decidable language with \(L' \notin \text{DTIME}(2^{|x|^2})\). Construct the unary variant of \(L'\): \(L := \{1^n : n = x, x \in L'\}\). Show that \(L\) is decidable, show that \(L \in \text{P}_{/\text{poly}}\) (think of \(\text{UHALT}\)), and that \(L \notin \text{P}\) (assume that \(L \in \text{P}\), and from that construct a TM deciding \(L'\) in too little time).

Problem 2: Circuit lower bounds: Parity

Let
\[
\text{PARITY} := \{x : x \text{ has an odd number of } 1\text{'s} \}.
\]
(Or expressed differently: \(x \in \text{PARITY} \) iff \(x_1 \oplus x_2 \oplus \cdots \oplus x_n = 1\).)

We will show a lower bound on the circuit complexity of \(\text{PARITY}\). Namely, we show that constant-depth circuits cannot compute \(\text{PARITY}\).

For this, we first establish a bit of notation:

- The *height* of a node \(\nu\) in a circuit \(C\) is the longest path from \(\nu\) to any leaf. That is, leaves (variables) have height 0. And an inner node has the maximum height of its children, plus 1.

- The *depth* of a circuit is the height of its root.

- Given a polynomial \(p\) over the real numbers with \(n\) variables, and a Boolean function \(f : \{0,1\}^n \to \{0,1\}\), we say that \(p\) *computes* \(f\) iff \(\forall x_1, \ldots, x_n \in \{0,1\}. p(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)\). (Note: we do not care what \(p\) evaluates to when it gets inputs different from 0, 1.)
• We say $p$ computes a node $\nu$ in a circuit $C$ if $p$ computes the function $f$ evaluated by the node $\nu$. (That is, for any assignment to the variables $x_1, \ldots, x_n$ of $C$, the node $\nu$ has a well-defined value $\in \{0, 1\}$, so the node evaluates some function $f$ of $x_1, \ldots, x_n$. We want $p$ to compute that function.)

• The degree of a multivariate polynomial $p$ is the largest sum of the exponents in any monomial. (E.g., $6x_1x_2x_3^2 + x_2x_5$ has degree 4 from the first monomial.)

• We call a polynomial multilinear if no variable occurs with an exponent greater than 1. (That is, $6x_1x_2x_3 + x_2x_5$ is multilinear, but $6x_1x_2x_3^2 + x_2x_5$ is not multilinear.)

We now develop a proof that $\text{PARITY}$ cannot be computed by constant-depth circuits:

(a) Show: For each leaf $\nu$ of a circuit $C$, there is a polynomial $p$ of degree $\leq 1$ that computes $\nu$.

(b) Show: For each node $\nu$ of height $h$ in a circuit $C$, there is a polynomial of degree $2^h$ that computes $\nu$.

**Hint:** Induction over the height, using (a). Express each AND/OR/NOT node as a polynomial of its children’s values, and compute the degree of the polynomial when plugging in the inputs. Remember that all nodes have fan-in at most 2.

(c) **[Bonus points, tricky]** Let $f_n(x_1, \ldots, x_n) := x_1 \oplus \cdots \oplus x_n$. Assume that $p_n$ is a multilinear polynomial that computes $f_n$. Show that $p_n$ contains the monomial $\alpha x_1x_2\cdots x_n$ (with some coefficient $\alpha \neq 0$).

**Hint:** Show it for $n = 1$ first. Then do induction. Express the polynomial $p_n$ as $p_n = x_nq + r$. Relate the polynomials $r$, $1 - (q + r)$, $1 - (q + r) + r$, and finally $(1 - q)/2$ to $f_{n-1}$. Show that $q$ contains $\alpha x_1\cdots x_{n-1}$ using induction hypothesis.

(d) Let $f_n(x_1, \ldots, x_n) := x_1 \oplus \cdots \oplus x_n$. Assume that $p_n$ is a polynomial that computes $f_n$. Show that $p_n$ has degree at least $n$.

**Hint:** Transform $p_n$ into a multilinear polynomial by removing all exponents from $p_n$. Show that the resulting polynomial still computes $f_n$. Then use (c).

(e) Show that no circuit $C_n$ of depth $d < \log n$ with $n$ variables decides $\text{PARITY}$.

**Hint:** Use (b) and (d).