Complexity Theory
Problem Set 5

1. Prove that L is in $\mathbf{AC}^0$.
$L = \{x \mid x$ is a binary string of length $3k+1$ for some $k \geq 1$, such that x is a concatenation of three binary string a, b, and c, $|a| = |b| = k$ and $|c| = k+1$, and $a + b = c\}$

2. Prove that L is not in $\mathbf{NC}^0$.
$L = \{1^n \mid n \geq 0\}$

3. Prove that if *SAT* $\in$ $\mathbf{P_{/poly}}$, then *NP* $\in$ $\mathbf{P_{/poly}}$.

4. Prove that if *SAT* $\in$ $\mathbf{P_{/poly}}$, then there exists a polysize circuit family $\{C_n\}_{n\in\mathbb{N}}$ s.t. $C_{|\phi|}(\phi)$ outputs a satisfying assignment for ϕ, if ϕ is satisfiable.

5. A language L is sparse if there is a polynomial p such that $|L \cap \{0,1\}^n| \leq p(n)$ for every $n \in \mathbb{N}$. Show that every sparse language is in $\mathbf{P_{/poly}}$.

6. Prove that *MAJORITY* $\in \mathbf{AC}^0 \implies$ *PARITY* $\in \mathbf{AC}^0$.
MAJORITY $= \{x \mid x$ is a binary string in which the number of 1s $\geq$ the number of 0s$\}$

Solutions

1. *https://pages.cs.wisc.edu/~jyc/02-810notes/lecture13.pdf*

2. ***Hint:*** Prove by contradiction.
Suppose $L \in \mathbf{NC}^0$ and c be the depth of the $\mathbf{NC}^0$ circuit family C that decides L. Define depth of each node in a circuit as the length of the longest path from an input node to that node. Use induction on vertices of different depths to find out on at most how many input vertices the value of the output vertex depends. After that come up with two different inputs on which the output should be different but C gives the same output.

3. Let $L \in \mathbf{NP}$ be the language that we will show in $\mathbf{P_{/poly}}$. Since L is polytime reducible to *SAT*, $\exists$ a TM M that runs in n^c time such that $M(x) \in$ *SAT* iff $x \in L$. Clearly, $M(x)$'s length can be at most n^c. Consider another TM M' that runs in n^d time such that $M'(x) = 1M(x)$ (adds 1 in front of $M(x)$) if $|M(x)| = n^c$, else it adds some zeroes in the beginning of $1M(x)$ to make its length $n^c + 1$ and outputs it.

We can modify the proof of $\mathbf{P} \subseteq \mathbf{P_{/poly}}$ so that every polynomial-time computable function f (not

just boolean functions/languages) has a polynomial size circuit family. (These circuits may produce multiple outputs.)

Let f be the function computed by M' and C_n be the polysize circuit family that computes f. Let D_n be the polysize circuit family that decides *SAT*.

We can say that, $x \in L \iff M'(x)(= C_{|x|}(x))$ is a binary string of the form 0^i1w (for $i \geq 0$) such that $w \in$ *SAT* and $|0^i1w| = n^c + 1$.

Now we construct the circuit family F for L. Let F_n be the circuit for inputs of length n. F_n on input x first computes $M'(x)$ using C_n. Let $v_1, v_2, \ldots, v_{n^c+1}$ be the vertices that have the values corresponding to $M'(x)$. Then to check whether $M'(x)$ is a binary string of the form 0^i1w such that $w \in$ *SAT* and $|0^i1w| = n^c + 1$, F_n will use n^c pairs of circuits say $(A_1, C_{n^c}), (A_2, C_{n^c-1}), \ldots, (A_{n^c}, C_1)$ on vertices $v_1, v_2, \ldots, v_{n^c+1}$, where A_j will check if the $v_1, v_2, \ldots, v_j$ have values of the form $0^{j-1}1$ and C_{n^c+1-j} checks if values of $v_{j+1}, v_{j+2}, \ldots, v_{n^c+1}$ is in *SAT*. The final value of F_n will simply be the OR of AND of outputs of all n^c pairs.

Think about why adding 0^i1 in M' is necessary and 0^i alone will not work.

4. This isn't complete but should give you the idea.
https://lucatrevisan.wordpress.com/2010/04/28/cs245-lecture-6-karp-lipton.

5. Just take all the strings of length n in L as advice for strings of length n.

6. See lemma 8 here *https://sites.math.rutgers.edu/~sk1233/courses/topics-S13/lec3.pdf*.