# Ex2: Depth reduction for formulae and arithmetic circuits

1. Prove:
   If we can compute $f(x_1, ..., x_n)$ by a uniform circuit of size $s$ and depth $d$ that uses $AND$, $OR$ and $NOT$ gates of fan-in 2 and unbounded fan-out, then there exists a uniform circuit of size $O(s)$ and depth $d$ that computes $f$ using only $AND$ and $OR$ gates over the inputs $x_1, ..., x_n, \overline{x_1}, ..., \overline{x_n}$.

2. $Parity(x_1, \ldots, x_n) = x_1 \oplus x_2 \ldots \oplus x_n$. Show a depth three Boolean circuit computing $Parity$ with $O(\sqrt{n} \cdot 2^{\sqrt{n}})$ gates of unbounded fan-in. NOT gates are allowed only at the input level and are not counted in the depth complexity.

3. (Depth reduction for non-uniform formulae) Let $f$ be a family of functions $\{f_n\}_{n \in \mathbb{N}}$, $f_n : \{0,1\}^n \to \{0,1\}^n$.

   (a) Prove that $f$ has *non-uniform* polynomial size formulae (of arbitrary depth) iff $f$ is in *non-uniform*-$\mathsf{NC}^1$.

   (b) Can you prove that every *uniform* $\mathsf{NC}^1$ language has uniform polynomial size formulae?

   (c) Can you prove that every *uniform* polynomial size formulae can be solved in $\mathsf{NC}^1$?

   A formula: A circuit whose underlying graph is a tree.

4. (Homogenization of arithmetic circuits): Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a homogenous, degree $deg$ polynomial. Prove: If there exists a size $S$, depth $Depth$ arithmetic circuit $C$ computing $f$, then there exists a *homogenous* circuit $C'$ of size $O(S \cdot deg^2)$ and depth $O(Depth \cdot \log(deg))$ computing $f$.

   (Notice that $C$ might not be homogenous)

   State and prove a uniform version of the above statement.

5. Define a partial order on $\{0,1\}^n$ by $x \leq y$ iff $x_i \leq y_i$ for all $i = 1, \ldots, n$. $f : \{0,1\}^* \to \{0,1\}^*$ is monotone if $x \leq y$ implies $f(x) \leq f(y)$. A circuit $C$ is monotone if it has only "and" and "or" gates.

   Prove that a monotone circuit computes a monotone function, and every monotone function has a monotone circuit.

6. Prove that $(x+1)^n - x^n - 1 \pmod{n}$ is the zero polynomial in $\mathbb{Q}[x_1, \ldots, x_n]$ iff $n$ is prime.