Week 2: Fine Finite Computation

Authors: Benjamin (iad4de, aqn9yv, jmn4fms, ht6xd, lw7jz, dlb2ru)

Problem 1 *Compare n bit numbers* (Exercise 3.2 in TCS book)

Theorem 1 *For any CMP_{2n} method, there exists a constant c where for every n there is a Boolean circuit (using AND, OR, and NOT gates) with at most $c \cdot n$ gates and computes $CMP_{2n} : \{0,1\}^{2n} \to \{0,1\}$ such that $CMP_{2n}(a_0...a_{n-1}, b_0...b_{n-1}) = 1$ if and only if $a_0...a_{n-1} > b_0...b_{n-1}$.*

Proof. Consider a Boolean circuit that compares two n-bit numbers. We will prove by induction on n.

Base Case if $n = 1$, $CMP_{2n}(a, b) = AND(a, NOT(b))$. There are 2 gates required, so any arbitrary value of c bigger than 2 would satisfy the theorem that the number of gates required is smaller than $c \cdot n$.

Induction Assume that there exists a number c such that the number of gates required to compute CMP_{2n} is less than $c \cdot n$. We want to show $CMP_{2(n+1)}$ requires less than or equal to $c(n+1) = c \cdot n + c$ gates.

We implement $CMP_{2(n+1)}$ by comparing the most significant bits, a^* and b^*, such that $CMP_{2(n+1)}$ returns 1 if $a^* > b^*$, and returns CMP_{2n} if $a^* = b^*$. Therefore, $CMP_{2(n+1)}$ can be computed as

$$OR(AND(a^*, NOT(b^*)),\\ AND(XNOR(a^*, b^*), CMP_{2n})),$$

where $XNOR(a, b)$ is expressed as

$$OR(AND(a, b), AND(NOT(a), NOT(b))$$

using AON. Therefore $CMP_{2(n+1)}$ takes 9 more gates than CMP_{2n}. Since CMP_{2n} requires at most $c \cdot n$ gates, $CMP_{2(n+1)}$ would require at most $c \cdot n + 9$ gates, which is less than or equal to $c(n+1)$ for any arbitrary number of c larger or equal to 9.

Conclusion By proving in the base case that there exists a c such that the number of gates of $CMP_{2\cdot(1)}$ is bounded by $c \cdot n$, and by showing that the existence of a c bounding the number of gates for CMP_{2n} implies an upper bound on $CMP_{2(n+1)}$, we have sufficiently shown that there exists a c such that the number of gates to compute CMP_{2n} is less than $c \cdot n$ for all $n \in \mathbb{N}^+$.

□