CIRCUIT COMPLEXITY

Question 1

We used the following theorem in class:

Theorem 1. *For sufficiently large $n \in \mathbb{N}$, there is a Boolean function $f : \{0,1\}^n \to \{0,1\}$, such that the best circuit computing it has size at least $2^n/n$ (equivalently depth $n - \log n$).*

The proof of this theorem is done in two parts. Answer the following questions and prove the theorem.

(a) Count the number of n bit Boolean functions. (1 point)

(b) Count the number of different size s circuits. You can assume that the internal gates are labeled by $\wedge, \vee$ gates of fan-in 2 and leaf gates are labeled by $2n$ literals. (4 points)

Hint I[1], Hint II[2]

KRW CONJECTURE

Question 2

We showed that KRW conjecture implies $\mathsf{P} \neq \mathsf{NC}^1$. We did this by constructing a function that had Formula depth complexity $\omega(\log n)$. The best unconditional lower bound we can prove on formula depth complexity of an explicit Boolean function $\approx 3\log n - O(\log\log n)$. Prove this result assuming the KRW conjecture for the following function :

$$\mathsf{And}_n(x, y) = h_x(z_1, \ldots, z_{\log n})$$

where $x, y \in \{0,1\}^n$, $h_x : \{0,1\}^{\log n} \to \{0,1\}$ is the Boolean function whose truth table is x and z_i is the parity of the i^{th} consecutive block of $\log n$ bits of y.

(a) Assuming KRW conjecture prove that $D(\mathsf{And}_n) \approx 3\log n$. (1 point)

You can use the following theorem.
Theorem 2. *Any formula computing the parity function on k bits has depth at least $2\log k$.*

Now prove that this function is very explicit and the lower bound is almost tight by answering the following questions.

1 (Prove that the number of circuits is upper bounded by $s^{O(s)}$)

2 (When counting the circuits check for the symmetries. That is the circuits which compute the same function)

(b) Show that the Andreev function And$_n$ described above can be computed by a polynomial time algorithm given x, y. (1 point)

(c) Show that the Andreev function And$_n$ described above can be computed by a size n^3 formula. (3 points)

Hint I[3]

Question 3

We saw in class that given a de-Morgan formula F computing a function f, we can come up with a protocol Π solving KW$_f$ whose communication complexity is $D(F)$ (depth of the formula F). Prove the reverse direction. That is given a deterministic protocol Π solving KW$_f$ come up with a formula F computing f whose depth is at most CC(Π) (the communication complexity of Π). (5 points) Hint I[4] Hint II[5]

[3] (The function h_x is equivalent to a table lookup on x. For example $h_x(0^n) = x_1$, the first bit of x.)

[4] (Prove by induction)

[5] (Map Alice,Bob to $\{\vee, \wedge\}$ based on the proof we used in the other direction)