CSC2429 / MAT1304: Circuit Complexity, Winter 2019
Homework Problems

(1) For $1 \le k \le n$, let $\mathrm{THR}_{k,n} : \{0,1\}^n \to \{0,1\}$ be the threshold function $\mathrm{THR}_{k,n}(x) = 1 \overset{\text{def}}{\iff} |x| \ge k$ where $|x| = \sum_{i=1}^n x_i$.

(a) Using Khrapchenko's bound, show that $\mathcal{L}(\mathrm{THR}_{k,n}) \ge k(n-k+1)$. (In particular, this shows $\mathcal{L}(\mathrm{MAJ}_n) = \Omega(n^2)$.)

(b) Show that Khrapchenko's bound never exceeds n^2 for any n-variable boolean function. (Alternatively, show this for the stronger bound of Koutsoupias.)

(2) Show that Nechiporuk's bound never exceeds $O(n^2/\log n)$. That is, for any function $f : \{0,1\}^n \to \{0,1\}$ and partition $V_1 \cup \cdots \cup V_k = [n]$, show that

$$\frac{1}{4}\sum_{i=1}^{k} \log |\mathsf{sub}_{V_i}(f)| = O(n^2/\log n).$$

(3) Consider the function $\mathrm{ANDREEV}_{k,m} : \{k\text{-variable boolean functions}\} \times \{0,1\}^{k\times m} \to \{0,1\}$ defined by

$$\mathrm{ANDREEV}_{k,m}(f, X) = (f \otimes \mathrm{XOR}_m)(X) = f((X_{1,1} \oplus \cdots \oplus X_{1,m}),\ \ldots,\ (X_{k,1} \oplus \cdots \oplus X_{k,m})).$$

(a) With $m = \lceil 2^k/k \rceil$ and viewing $\mathrm{ANDREEV}_{k,m}$ as a boolean function $\{0,1\}^n \to \{0,1\}$ where $n = 2^k + km = \Theta(2^k)$, use Nechiporuk's bound to show that $\mathcal{L}_{B_2}(\mathrm{ANDREEV}_{k,m}) = \Omega(n^2/\log n)$.

(b) Give a matching upper bound $\mathcal{L}_{B_2}(\mathrm{ANDREEV}_{k,m}) = O(n^2/\log n)$.

(4) Show that the number of monotone functions $\{0,1\}^n \to \{0,1\}$ is at least $2^{\binom{n}{\lfloor n/2 \rfloor}}$ $(= 2^{\Omega(2^n/\sqrt{n})})$. Conclude that *almost all* monotone functions f have DeMorgan circuit size $\mathcal{C}(f) = \Omega(2^n/n^{1.5})$.

Remark: It is known that $\mathcal{C}(f) \le \mathcal{C}_{\mathrm{mon}}(f) = O(2^n/n^{1.5})$ for <u>all</u> monotone $f : \{0,1\}^n \to \{0,1\}$. It follows that $\mathcal{C}_{\mathrm{mon}}(f) = \Theta(\mathcal{C}(f))$ for *almost all* monotone functions f.

(5) Let $\delta \in (0, \frac{1}{2})$. A function $f : \{0,1\}^n \to \{0,1\}$ is a δ-**approximate majority** if, for all $x \in \{0,1\}^n$,

$$\tfrac{|x|}{n} \le \tfrac{1}{2} - \delta \implies f(x) = 0,$$
$$\tfrac{|x|}{n} \ge \tfrac{1}{2} + \delta \implies f(x) = 1.$$

Suppose a, b, c are positive integers such that

$$(1 - (1 - (\tfrac{1}{2} - \delta)^a)^b)^c < 2^{-n},$$
$$(1 - (1 - (\tfrac{1}{2} + \delta)^a)^b)^c > 1 - 2^{-n}.$$

(a) Show that there exist Π_3 formulas of leafsize abc that compute a δ-approximate majority.

(b) Now show that there are *polynomial-size* Π_3 formulas (i.e. AND-OR-AND formulas) that compute a $\frac{1}{4}$-approximate majority. (Find suitable a, b, c using inequalities $1 - p \leq e^{-p}$ and $(1-p)^t \geq 1 - tp$ for $p \in (0,1)$ and $t \geq 1$.)

Remark: For all $d \geq 1$, there existing polynomial-size Π_{d+3} formulas that compute a $\frac{1}{(\log n)^d}$-approximate majority.

(6) A **symmetric function** is a boolean function $f : \{0,1\}^n \to \{0,1\}$ such that $f(x)$ only depends on the Hamming weight $|x|$ of x. XOR_n, MAJ_n and $\mathrm{THR}_{k,n}$ are examples of symmetric functions. In this problem, you will show that every symmetric function can be computed by (explicit, non-random) DeMorgan circuits of size $O(n)$ and depth $O(\log n)$.

(a) Warm-up: Let $f : \{0,1\}^n \to \{0,1\}$ be the function $f(x) = 1 \iff |x|$ is congruent to 1 or 3 modulo 5. Show that f can be computed by DeMorgan circuits size $O(n)$ and depth $O(\log n)$.

(b) Show that there are DeMorgan circuits of constant depth which take three n-bit numbers x, y, z and output two $(n+1)$-bit numbers u, v such that $x + y + z = u + v$. (These circuits have $3n$ input variables and $2(n+1)$ output gates.)

(c) Show that there are DeMorgan circuits of depth $O(\log n)$ which take an input $x \in \{0,1\}^n$ and outputs an $\lceil \log n \rceil$-bit number u such that $u = |x|$. (Hint: View x as a sequence of n 1-bit numbers.)

(d) Complete the proof that every symmetric function can be computed by DeMorgan circuits of size $O(n)$ and depth $O(\log n)$.

(7) Show that every function $\{0,1\}^n \to \{0,1\}$ can be computed by a constant-depth AC^0 circuit with $O(2^n/n)$ gates.

For a greater challenge: Show this with $O(2^{n/2} \cdot n^c)$ gates for some constant c.

(8) Show that the n-variable MOD_4 function is computable by a polynomial-size constant-depth $\mathrm{AC}^0[2]$ circuits.

Convince yourself that a similar construction shows that MOD_{p^k} is computable by polynomial-size constant-depth $\mathrm{AC}^0[p]$ circuits for all p and k (that is, by $\mathrm{AC}^0[p]$ circuits of size $O(n^c)$ and depth d for constants $c(p,k)$ and $d(p,k)$ that depend on p and k alone).

(9) Note that every threshold function $\mathrm{THR}_{k,n}(x_1, \ldots, x_n)$ is a subfunction of $\mathrm{MAJ}_{2n+1}(x_1, \ldots, x_n, y_1, \ldots, y_{n+1})$ (by setting an appropriate number of y_i's to 0 or 1).

Using this observation, show that every symmetric function $f : \{0,1\}^n \to \{0,1\}$ is computable by a polynomial-size $\mathrm{MAJ} \circ \mathrm{MAJ}$ circuit (that is, two layers of majority gates with inputs that are literals or constants).

(10) Show that every boolean function $f : \{0,1\}^n \to \{0,1\}$ is computable by a DeMorgan circuit C of size $\mathcal{C}(f) + O(n^{\text{constant}})$ such that C contains at most $O(\log n)$ NOT gates.

Hint: Construct subcircuits for functions $\text{SORT}_n, \text{NEGATE}_n : \{0,1\}^n \to \{0,1\}^n$ defined by

$$\text{SORT}_n(x) = (\underbrace{1,\ldots,1}_{|x| \text{ times}}, 0,\ldots,0), \qquad \text{NEGATE}_n(x) = (1 - x_1, \ldots, 1 - x_n).$$

Use the idea behind Berkowitz's theorem (see Lecture 4) that $\mathcal{C}_{\text{mon}}(s) \leq \mathcal{C}(s) + O(n^{\text{constant}})$ for slice functions $s : \{0,1\}^n \to \{0,1\}$.