Let \( (5) \) Show that the number of monotone functions \( (4) \)

Consider the function \( \text{ANDREEV} \)

For \( 1 \)

Homework Problems

CSC2429 / MAT1304: Circuit Complexity, Winter 2019

Show that Nechiporuk’s bound never exceeds \( (2) \)

Suppose \( a, b, c \)

Remark: It is known that \( L \)

(a) Give a matching upper bound \( \Omega((n) \)

(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.)

(c) Show that there exist \( \Pi_3 \) formulas of leafsize \( abc \) that compute a \( \delta \)-approximate majority.

\[
\left| \frac{\delta}{n} \right| \leq \frac{1}{2} - \delta \implies f(x) = 0, \quad \left| \frac{\delta}{n} \right| \geq \frac{1}{2} + \delta \implies f(x) = 1.
\]

(1) For \( 1 \leq k \leq n \), let \( \text{THR}_{k,n} : \{0,1\}^n \to \{0,1\} \) be the threshold function \( \text{THR}_{k,n}(x) = 1 \iff |x| \geq k \) where \( |x| = \sum_{i=1}^{n} x_i \).

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

(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

\[
\frac{1}{4} \sum_{i=1}^{k} \log |\text{sub}_i(f)| = O(n^2 / \log n).
\]

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

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

(a) With \( m = \lceil 2^k / k \rceil \) and viewing \( \text{ANDREEV}_{k,m} \) 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 \( L_{B_2}(\text{ANDREEV}_{k,m}) = \Omega(n^2 / \log n) \).

(c) Give a matching upper bound \( L_{B_2}(\text{ANDREEV}_{k,m}) = O(n^2 / \log n) \).

(4) Show that the number of monotone functions \( \{0,1\}^n \to \{0,1\} \) is at least \( 2^{(\frac{n}{2^k})} \) \( (= 2^{O(2^n / \sqrt{n})}) \).

Conclude that almost all monotone functions \( f \) have DeMorgan circuit size \( C(f) = \Omega(2^n / n^{1.5}) \).

Remark: It is known that \( C(f) \leq C_{\text{mon}}(f) = O(2^n / n^{1.5}) \) for all monotone \( f : \{0,1\}^n \to \{0,1\} \).

It follows that \( C_{\text{mon}}(f) = O(C(f)) \) 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 \( \delta \)-approximate majority if, for all \( x \in \{0,1\}^n \),

\[
\frac{|x|}{n} \leq \frac{1}{2} - \delta \implies f(x) = 0, \quad \frac{|x|}{n} \geq \frac{1}{2} + \delta \implies f(x) = 1.
\]

Suppose \( a, b, c \) are positive integers such that

\[
(1 - (1 - (\frac{1}{2} - \delta)^a)^b)^c < 2^{-n}, \quad (1 - (1 + (\frac{1}{2} + \delta)^a)^b)^c > 1 - 2^{-n}.
\]

(a) Show that there exist \( \Pi_3 \) formulas of leafsize \( abc \) that compute a \( \delta \)-approximate majority.
(b) Now show that there are polynomial-size $\Pi_3$ 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 $\Pi_{d+3}$ 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 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 $c$. 