Circuit Complexity Homework Problems

Problem 1 (Application of Khrapchenko's Bound). *Let the threshold function, denoted* $\mathrm{THR}_{k,n}$ *for* $k \in [n]$, *be an* n*-ary Boolean function where* $\mathrm{THR}_{k,n}(\mathbf{x}) = 1 \iff |\mathbf{x}| \geq k$.

1. $\mathcal{L}(\mathrm{THR_{k,n}}) \geq k(n-k+1)$.

   Proof. Define sets $A = \{\mathbf{x} \in \{0,1\}^n : |\mathbf{x}| = k-1\}$ and $B = \{\mathbf{y} \in \{0,1\}^n : |\mathbf{y}| = k\}$ which are subsets of $\mathrm{THR}_{k,n}^{-1}(0)$ and $\mathrm{THR}_{k,n}^{-1}(1)$ respectively. Observe that every element $\mathbf{a} \in A$ is incident to $n-k+1$ different elements of B since we can flip any of the $n-k+1$ zeros in $\mathbf{a}$ to produce an element of B i.e. an n-ary string with k ones. By Khrapchenko's bound,

   $$\begin{aligned}\mathcal{L}(\mathrm{THR_{k,n}}) &\geq \frac{\left(\sum_{\mathbf{a}\in A}\sum_{\mathbf{b}\in B} M_{\mathbf{a},\mathbf{b}}\right)^2}{|A|\cdot|B|} \\ &= \frac{\left(\binom{n}{k-1}\cdot(n-k+1)\right)^2}{\binom{n}{k-1}\binom{n}{k}} = \frac{\binom{n}{k-1}(n-k+1)^2}{\binom{n}{k}} = \frac{n!k!(n-k)!(n-k+1)^2}{n!(k-1)!(n-k+1)!} \\ &= k(n-k+1)\end{aligned}$$

   as required. □

   Since $\mathrm{MAJ}_n \equiv \mathrm{THR}_{\lceil n/2\rceil,n}$, we have $\mathcal{L}(\mathrm{MAJ}_n) \in \Omega(n^2)$ by the above.

2. Khrapchenko's bound never exceeds n^2 for any n-ary Boolean function.

   Proof. Consider any n-ary Boolean function f and sets $A \subseteq f^{-1}(0)$ and $B \subseteq f^{-1}(1)$. Notice that $n \cdot |B| \geq \sum_{\mathbf{a}\in A}\sum_{\mathbf{b}\in B} M_{\mathbf{a},\mathbf{b}}$ and $n \cdot |A| \geq \sum_{\mathbf{a}\in A}\sum_{\mathbf{b}\in B} M_{\mathbf{a},\mathbf{b}}$ since each $\mathbf{a} \in A$ can be adjacent to at most n elements of B and vice versa. Thus

   $$\frac{\left(\sum_{\mathbf{a}\in A}\sum_{\mathbf{b}\in B} M_{\mathbf{a},\mathbf{b}}\right)^2}{|A|\cdot|B|} \leq \frac{\left(\sum_{\mathbf{a}\in A}\sum_{\mathbf{b}\in B} M_{\mathbf{a},\mathbf{b}}\right)^2}{|A|\cdot\frac{\sum_{\mathbf{a}\in A}\sum_{\mathbf{b}\in B} M_{\mathbf{a},\mathbf{b}}}{n}} = \frac{n\left(\sum_{\mathbf{a}\in A}\sum_{\mathbf{b}\in B} M_{\mathbf{a},\mathbf{b}}\right)}{|A|} \leq \frac{n^2|A|}{|A|} = n^2$$

   and Khrapchenko's bound can never exceed n^2 for any n-ary Boolean function. □

Problem 2 (UB Nechiporuk). *Nechiporuk's bound never exceeds* $O(n^2/\log n)$.

Proof. Let f be an n-ary Boolean function with variables $V = \{x_1, ..., x_n\}$. Let $V_1 \uplus \cdots \uplus V_k$ be a partition of V. We will show that

$$\frac{1}{4}\sum_{l=1}^{k} \log|\mathrm{sub}_{V_l}(f)| \in O\left(\frac{n^2}{\log n}\right). \tag{1}$$

In the following, we drop the factor of 1/4 since only the limiting behavior of Equation (1) matters.

The crux of our argument is the following observation: for any set $V_i \subseteq V$, there are two trivial upper bounds for $|\mathrm{sub}_{V_i}(f)|$. First, since the elements of $\mathrm{sub}_{V_i}(f)$ arise from restrictions of $V\backslash V_i$ to $\{0,1\}$

and there are most $2^{n-|V_i|}$ distinct restrictions, $|\text{sub}_{V_i}(f)| \leq 2^{n-|V_i|}$. Second, since the elements of $\text{sub}_{V_i}(f)$ are $|V_i|$-ary and there are at most $2^{2^{|V_i|}}$ such distinct Boolean functions, $|\text{sub}_{V_i}(f)| \leq 2^{2^{|V_i|}}$. Thus $|\text{sub}_{V_i}(f)| \leq \min\left(2^{n-|V_i|}, 2^{2^{|V_i|}}\right)$ with $2^{n-|V_i|} \in O\left(2^{2^{|V_i|}}\right)$ when $|V_i| \in O(\log(n - \log n))$.

Let $c = \lceil \log(n - \log n) \rceil$. Divide up the indices of $[k]$ into two sets $I = \{i : |V_i| \geq c\}$, the large sets, and $J = \{j : |V_j| < c\}$, the small sets. Since

$$\sum_{l=1}^{k} \log |\text{sub}_{V_l}(f)| = \sum_{i \in I} \log |\text{sub}_{V_i}(f)| + \sum_{j \in J} \log |\text{sub}_{V_J}(f)|,$$

we will bound each term on the RHS separately.

For $i \in I$, $|\text{sub}_{V_i}(f)| \leq \min\left(2^{n-|V_i|}, 2^{2^{|V_i|}}\right) = 2^{n-|V_i|}$. Since $|V_i| \geq c$ for all $i \in I$, $|I| \leq n/c$. Thus

$$\sum_{i \in I} \log |\text{sub}_{V_i}(f)| \leq \sum_{i \in I} n - |V_i| \leq \sum_{i \in I} n - c \leq \frac{n}{c}(n - c) \in O\left(\frac{n^2}{\log n}\right). \tag{2}$$

For $j \in J$, $|\text{sub}_{V_j}(f)| \leq \min\left(2^{n-|V_i|}, 2^{2^{|V_i|}}\right) = 2^{2^{|V_j|}}$. For $\gamma \in [c]$, let n_γ be the number of variables among all sets of size γ. Note that for each γ, there are n_γ/γ sets of size γ. Further observe that the ratio $2^\gamma/\gamma$ increases with γ. Thus

$$\sum_{j \in J} \log |\text{sub}_{V_j}(f)| = \sum_{\gamma=1}^{c} \frac{n_\gamma}{\gamma} \log 2^{2^\gamma} = \sum_{\gamma=1}^{c} n_\gamma \frac{2^\gamma}{\gamma} \leq \frac{2^c}{c}\left(\sum_{\gamma=1}^{c} n_\gamma\right) \leq \frac{2^c}{c} n \in O\left(\frac{n^2}{\log n}\right). \tag{3}$$

Combining Equations (2) and (3), we have $\sum_{l=1}^{k} \log |\text{sub}_{V_l}(f)| \in O\left(\frac{n^2}{\log n}\right)$ as required. □

Problem 3 (Leafsize Bounds on $\text{ANDREEV}_{k,m}$)**.** *Recall the Andreev function* $\text{ANDREEV}_{k,m} : \{$*k-variable Boolean function*$\} \times \{0,1\}^{k \times m} \to \{0,1\}$ *where*

$$\text{ANDREEV}_{k,m}(f, \mathbf{X}) = (f \otimes \text{XOR}_m)(\mathbf{X}) = f\left((x_{1,1} \oplus \cdots \oplus x_{1,m}), ..., (x_{k,1} \oplus \cdots \oplus x_{k,m})\right).$$

1. $\mathcal{L}_{B_2}(\text{ANDREEV}_{k,m}) \in \Omega(n^2/\log n)$.

   Proof. Let $m = \lceil 2^k/k \rceil$ and $n = 2^k$. The inputs to $\text{ANDREEV}_{k,m}$ are a k-ary Boolean function f and a matrix $\mathbf{X} \in \{0,1\}^{k \times m}$. Defined f by the vector $\mathbf{f} = (f_0, ..., f_{2^k-1})$ where f_i is the value of f on the binary representation of i. Let the entries of $\mathbf{X}$ be $x_{i,j}$ for $i \in [k]$ and $j \in [m]$.

   Divide the $2^k + km$ variables of $\text{ANDREEV}_{k,n}$ into the following $m+1$ disjoint sets: $V_j = \{x_{1,j}, ..., x_{k,j}\}$ for $j \in [m]$ (the columns of $\mathbf{X}$) and $V_{m+1} = \{f_0, ..., f_{2^k-1}\}$. Observe that the sets V_j are symmetric so, by Nechiporuk's Bound, we have

$$\mathcal{L}_{B_2}(f) \geq \frac{1}{4} \sum_{j=1}^{m+1} \log |\text{sub}_{V_j}(f)| = \frac{1}{4}\left(m \log |\text{sub}_{V_1}(f)| + \log |\text{sub}_{V_{m+1}}(f)|\right). \tag{4}$$

Thus it suffices to lower bound $|\mathrm{sub}_{V_1}(f)|$ and $|\mathrm{sub}_{V_{m+1}}(f)|$.

Observe that there is a surjection between the elements of $\mathrm{sub}_{V_{m+1}}(f)$ and the set of projection functions on f of size 2^k. For every $\mathbf{y} \in \{0,1\}^k$, by fixing a particular choice of $\mathbf{X}$, namely $\mathbf{X} = [\mathbf{y}, \mathbf{0}, ..., \mathbf{0}]$, $\mathrm{ANDREEV}_{k,m}(f, \mathbf{X}) = f(\mathbf{y})$. Thus $|\mathrm{sub}_{V_{m+1}}(f)| \geq 2^k \in O(n)$.

Similarly there exists an surjection between $\mathrm{sub}_{V_1}(f)$ and the set of all k-ary Boolean functions. Pick a function f by specifying $\mathbf{f}$. For any fixed $x_{i,j}$, where $i \in [k]$ and $j \in \{2, ..., m\}$, as $(x_{1,1}, ..., x_{k,1})$ ranges through all values in $\{0,1\}^k$, $((x_{1,1} \oplus \cdots \oplus x_{1,m}), ..., (x_{k,1} \oplus \cdots \oplus x_{k,m}))$ also takes all values in $\{0,1\}^k$. Thus $|\mathrm{sub}_{V_1}(f)| \geq 2^{2^k}$.

Plugging these values into Equation (4), we have

$$\mathcal{L}_{B_2}(f) \geq \frac{1}{4}\left(m \log 2^{2^k} + \log 2^k\right) = \frac{1}{4}\left(m2^k + k\right) \in O\left(\frac{n^2}{\log n}\right)$$

since $m \in O(2^k/k)$ and $n \in O(2^k)$. $\square$

2. $\mathcal{L}_{B_2}(\mathrm{ANDREEV}_{k,m}) \in O(n^2/\log n)$.

Solution. Let the inputs to $\mathrm{ANDREEV}_{k,m}$ be as described in the previous part. We will construct a formula with $O(n^2/\log n)$ leaves.

Let us define a few helper functions to simplify our exposition. First, for $i \in [k]$, let $\oplus_i$ compute the xor of the i^{th} row of $\mathbf{X}$, i.e. $\oplus_i = x_{i,1} \oplus \cdots \oplus x_{i,m}$. Notice that $\mathcal{L}_{B_2}(\oplus_i) = m$. Next, let the two bit multiplexer function be $\mathrm{MUX} : \{0,1\}^3 \to \{0,1\}$ such that

$$\mathrm{MUX}(b_0, b_1, s) = b_s$$

shown in Figure 1. Notice that $\mathcal{L}_{B_2}(\mathrm{MUX}(b_0, b_1, s)) = \mathcal{L}_{B_2}(b_0) + \mathcal{L}_{B_2}(b_1) + 2\mathcal{L}_{B_2}(s)$.

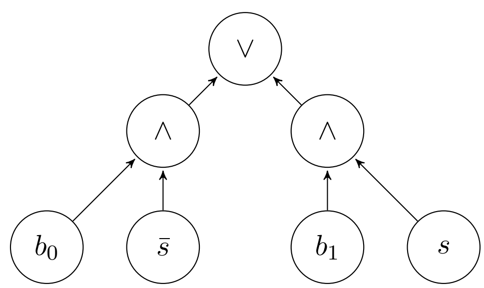

Figure 1: Circuit for $\mathrm{MUX}(b_0, b_1, s)$. The output of the function is the value at the $\vee$ gate.

Recursively construct a depth k tree of MUX-gates. At the bottom are the bits $f_0, ..., f_{2^k-1}$. Above them are 2^{k-1} MUX-gates labeled $\mathrm{MUX}_{k,0}, ..., \mathrm{MUX}_{k,2^{k-1}-1}$ where

$$\mathrm{MUX}_{k,i} = \mathrm{MUX}(b_{f_{2i}}, b_{f_{2i+1}}, \oplus_k).$$

Level j of the tree has 2^{j-1} MUX-gates labeled with $\mathrm{MUX}_{j,0}, ..., \mathrm{MUX}_{j,2^{j-1}-1}$ where

$$\mathrm{MUX}_{j,i} = (\mathrm{MUX}_{j+1,2i}, \mathrm{MUX}_{j+1,2i+1}, \oplus_j)$$

for all $j \in [k]$. See Figure 2 for a small example.

There are 2^k leaves labeled by $f_0, ..., f_{2^k-1}$. Each of the $2^k - 1$ MUX-gates uses two $\oplus_i$ subtrees each containing m leaves. This formula has $2^k + (2^k - 1) \cdot 2m \in O(n^2/\log n)$ leaves. Thus $\mathcal{L}_{B_2}(\mathrm{ANDREEV}_{k,m}) \in \Theta(n^2/\log n)$ with lower bound from the previous part.

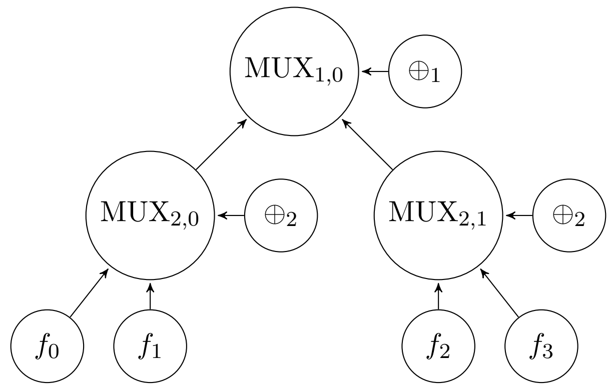

Figure 2: Example of the constructed tree with $k = 2$.

Problem 4 (LB Circuit Size of Monotone functions)**.** *Almost all monotone n-ary functions f have DeMorgan circuits of size $\mathcal{C}(f) \in \Omega(2^n/n^{1.5})$.*

Proof. First we will show that there are at least $2^{\binom{n}{\lfloor 2/n \rfloor}}$ n-ary monotone functions. Consider the subsets of $[n]$ ordered by inclusion i.e. $\emptyset$ is at the bottom, $[n]$ is at the top, and an edge (S_1, S_2) between $S_1, S_2 \subset [n]$ if $S_1 \subset S_2$. The family $\mathcal{M}$ of all subsets containing $\lfloor n/2 \rfloor$ elements is an anti-chain of size $\binom{n}{\lfloor n/2 \rfloor}$. Consider maps $h : \mathcal{M} \to \{0, 1\}$. For each h, we can define a n-ary monotone function as follows. Let $M \in \mathcal{M}$. If $h(M) = 0$, then for all proper supersets $M_{sup} \supset M$, $f(M_{sup}) = 1$. Otherwise if $h(M) = 1$, then for all proper subsets $M_{sub} \subset M$, $f(M_{sub}) = 0$. This defines a monotone function since the value of f on a chain is monotonically increasing. Since there are $2^{\binom{n}{\lfloor n/2 \rfloor}} = 2^{\Omega(2^n/\sqrt{n})}$ maps, there are at least this many n-ary monotone functions.

Using the above and Shannon's lower bound for general n-ary Boolean functions, we can show that almost all monotone functions have DeMorgan circuit size $\Omega(2^n/n^{1.5})$.

Let $s = 2^n/n^{1.5}$ and A be the set of all circuits with size at most s. The set B of monotone circuits of size at most s is a subset of A. Note that $|A| \leq 2^s(s + 2n)^{2s}$ since each of the s gates can be an $\wedge$ or $\vee$ and each gate can take two inputs from any of the s gates or $2n$ literals. Further notice that any function f with a circuit in A also has $s!$ distinct circuits in A. Suppose $n \geq 22$ ($n^{1.5} > 100$). The number of monotone functions with circuit size at most s is bounded above by

$$\frac{|B|}{s!} \leq \frac{|A|}{s!} \leq \frac{18^s s^{2s}}{\left(\frac{s}{e}\right)^s} \leq 50^s s^s \leq \left(\frac{50}{n^{1.5}}\right)^{2^n/n^{1.5}} 2^{2^n/\sqrt{n}} \leq 2^{2^n/\sqrt{n} - 2^n/n^{1.5}}.$$

Thus at least 2^s monotone functions has circuit size greater than s. ☐

Problem 5 (δ-Approximate Majority)**.** *For $\delta \in (0, 1/2)$, a n-ary Boolean functions f is a δ-approximate majority if for all $\mathbf{x} \in \{0,1\}^n$,*

$$\frac{|\mathbf{x}|}{n} \leq \frac{1}{2} - \delta \implies f(\mathbf{x}) = 0$$
$$\frac{|\mathbf{x}|}{n} \geq \frac{1}{2} + \delta \implies f(\mathbf{x}) = 1$$

Suppose a, b, c are positive integers such that

$$\left(1-\left(1-\left(\frac{1}{2}-\delta\right)^{a}\right)^{b}\right)^{c} < 2^{-n} \text{ and } \left(1-\left(1-\left(\frac{1}{2}+\delta\right)^{a}\right)^{b}\right)^{c} > 1-2^{-n}. \tag{5}$$

1. There exists Π_3 formulas of leafsize abc that compute a δ-approximate majority.

Proof. This will be similar to the proof that MAJ_n has poly-sized monotone formulas. In particular we will build a Π_3 formula with fan-in c, b, and a respectively from top to bottom. Then populate the bottom-most level with values from a random projection.

Let F be the formula as described above. The output of F is a $\wedge$-gate, t, with fan-in c. The children of t are $\vee$-gates, $r_1, ..., r_\gamma$ with fan-in b. The children of each r_i are $\wedge$-gates $d_{i,1}, ..., d_{i,b}$ with fan-in a. The children of each gate $d_{i,j}$ are literals $y_{i,j,1}, ..., y_{i,j,a}$. Let the input to F be $\mathbf{y} \in \{0,1\}^{abc}$, π be a random projection from $\mathbf{y} \to \mathbf{x}$, and $F_\pi(\mathbf{x})$ be the formula with input $\pi(\mathbf{y})$. Let A be the event that F computes δ-approximate majority.

For π such that $\pi(y_i)$ is chosen independently and uniformly from all elements of $\mathbf{x}$, we will show that $\Pr[A] > 1-2^{-n}$. Let E_1 and E_2 be the events $|\mathbf{x}|/n \leq \frac{1}{2}-\delta$ and $|\mathbf{x}|/n \geq 1/2+\delta$ respectively. By conditioning, we have

$$\Pr[A] = \Pr\left[F_\pi(\mathbf{x}) = 0 | E_1\right] \Pr\left[E_1\right] + \Pr\left[F_\pi(\mathbf{x}) = 1 | E_2\right] \Pr\left[E_2\right]$$

Since at most one of $\Pr[E_1] = 1$ or $\Pr[E_2] = 1$, we just need to show that both conditional probabilities on the RHS are bounded below by $1-2^{-n}$.

First condition on E_1 and let $p = \frac{1}{2}-\delta$. For any $d_{i,j}$,

$$\Pr[d_{i,j}(\pi(y_{i,j,1}), ..., \pi(y_{i,j,a})) = 1 | E_1] \leq \left(\frac{1}{2}-\delta\right)^{a}$$

since $\pi(y_{i,j,1}) \sim \mathrm{Bern}(p)$. Similarly for any r_i,

$$\Pr[r_i(d_{i,1}, ..., d_{i,b}) = 1 | E_1] = 1 - \Pr[r_i(d_{i,1}, ..., d_{i,b}) = 0 | E_1] \leq 1 - \left(1-\left(\frac{1}{2}-\delta\right)^{\alpha}\right)^{b}.$$

Finally for t,

$$\Pr[t(r_1, ..., r_c) = 1 | E_1] \leq \left(1-\left(1-\left(\frac{1}{2}-\delta\right)^{\alpha}\right)^{b}\right)^{c}.$$

Together, with the inequalities given by the problem statement, we have

$$\Pr[F_\pi(\mathbf{x}) = 0 | E_1] = 1 - \Pr[F_\pi(\mathbf{x}) = 1 | E_1] = 1 - \Pr[t(r_1, ..., r_c) = 1 | E_1] > 1 - \frac{1}{2^n}.$$

Next condition on E_2 and let $p = \frac{1}{2}+\delta$. Using a similar argument, we have

$$\begin{aligned}
\Pr\left[F_\pi(\mathbf{x}) = 1 | E_2\right] &= \Pr\left[t(r_1, ..., r_c) = 1 | E_2\right] \\
&= \left(\Pr\left[r_i(d_{i,1}, ..., d_{i,b}) = 1 || E_2\right]\right)^c \\
&= \left(1 - \Pr\left[r_i(d_{i,1}, ..., d_{i,b}) = 0 | E_2\right]\right)^c \\
&= \left(1 - \left(1 - \Pr\left[d_{i,j}(\pi(y_{i,j,1}), ..., \pi(y_{i,j,a})) = 1 | E_2\right]\right)^b\right)^c \\
&\geq \left(1-\left(1-\left(\frac{1}{2}+\delta\right)^{a}\right)^{b}\right)^{c} \\
&> 1 - 2^n
\end{aligned}$$

so $\Pr[A] \geq 1 - 2^{-n}$ as required. Taking a union bound over all 2^n inputs, we see that there must exist some projection π for which $F_\pi(\mathbf{x})$ is a δ-approximate majority. Return the Π_3 formula obtained by hard-wiring π into F. $\square$

2. There are *polynomial-sized* Π_3 formulas that compute a $\frac{1}{4}$-approximate majority[1].

   Solution. Using the previous section, it suffices to take $\delta = 1/4$ and find a, b, c which satisfy Equation (5). From the upper bound we have

$$\begin{aligned}\left(1 - \left(1 - \left(\frac{1}{4}\right)^a\right)^b\right)^c &\leq \left(1 - \left(1 - \frac{b}{4^a}\right)\right)^c \\ &\leq \left(\frac{b}{4^a}\right)^c \\ &< \frac{1}{2^n}\end{aligned}$$

   and from the lower bound we have

$$\begin{aligned}\left(1 - \left(1 - \left(\frac{3}{4}\right)^a\right)^b\right)^c &\geq \left(1 - \exp\left(-b\left(\frac{3}{4}\right)^a\right)\right)^c \\ &\geq 1 - c\exp\left(-b\left(\frac{3}{4}\right)^a\right) \\ &> 1 - \frac{1}{2^n}.\end{aligned}$$

   Together we require that $c\,(2a - \log b) > n$ and $b\,(3/4)^a \log e - \log c > n$. Choose $a = \log n$, $b = 2(4/3)^a \cdot n$, and $c = n$. Then, since $\log b = 1 + a\log(4/3) + \log n$,

$$c\,(2a - \log b) = n \log n \left(1 - \log\left(\frac{4}{3}\right) - \frac{1}{\log n}\right) \geq n$$

   for sufficiently large n such that $\log n > 3$ and $1 - \log(4/3) - (\log n)^{-1} > 1/3$. Further

$$b\,(3/4)^a \log e - \log c = 2n \log e - \log n > n.$$

   Thus these values of a, b, and c suffice, resulting in a Π_3 formula of leafsize

$$abc = 2(4/3)^{\log n} n^2 \log n \in O(n^3 \log n)$$

   for $\frac{1}{4}$-approximate majority.

[1] For all $d \geq 1$, there exists poly-sized Π_{d+3} formulas that compute a $\frac{1}{(\log n)^d}$-approximate majority.

Problem 7 (UB AC^0 Circuit Size)**.** *Every n-ary Boolean function f can be computed by an AC^0 circuit with $O(2^{n/2} \cdot n^c)$ gates for some constant c.*

Proof. Suppose f is computed by DNF $F = C_1 \vee \cdots \vee C_k$ where the literals in each clause are arranged in lexicographical order. We will modify F so that every clause has exactly n literals. W.l.o.g suppose some clause $C_i = x_1 x_2 \cdots x_t$ has fewer than n literals. Then we will remove C_i from F and add 2^{n-t} clauses with every possible combination of the variables $x_{t+1}, ..., x_n$ and their negation. For example, with $n = 4$, if $C_1 = x_1 x_2$ then we will remove C_1 and add clauses $D_0 = x_1 x_2 \bar{x}_3 \bar{x}_4$, $D_1 = x_1 x_2 \bar{x}_3 x_4$, $D_2 = x_1 x_2 x_3 \bar{x}_4$, and $D_3 = x_1 x_2 x_3 x_4$. Let $F' = C_1' \vee \cdots \vee C_{k'}'$. Observe that $F(\mathbf{x}) = F'(\mathbf{x})$ for all inputs $\mathbf{x} \in \{0,1\}^n$.

Intuitively, the circuit divides the variables in-half and, for all settings of the first half which result in a satisfying assignment, checks to see if any of the matching second halves are satisfied.

Formally, we construct the following circuit C from F'. Divide $[n]$ into two sets $A = \{1, ..., n/2\}$ and $B = \{n/2 + 1, ..., n\}$ of size $n/2$ (we can assume that n is even). Let $x_i^1 := x_i$ and $x_i^0 := \bar{x}_i$. For $\mathbf{b} \in \{0,1\}^B$, let

$$\wedge_{\mathbf{b}} = \bigwedge_{j \in \mathbf{b}} x_j^{b_j}.$$

For every $\mathbf{a} \in \{0,1\}^A$ define a $\wedge$-gate, $\pi_{\mathbf{a}}$, and a $\vee$-gate, $\sigma_{\mathbf{a}}$. Let $T_{\mathbf{a}} = \{\mathbf{b} : F'(\mathbf{a}, \mathbf{b}) = 1\}$, then

$$\pi_{\mathbf{a}} = \bigvee_{\mathbf{b} \in T_{\mathbf{a}}} \wedge_{\mathbf{b}} \text{ and } \sigma_{\mathbf{a}} = \left(\bigwedge_{i \in \mathbf{a}} x_i^{a_i} \right) \wedge \pi_{\mathbf{a}}.$$

Let $T = \{\mathbf{a} : \exists \mathbf{b} \in B \text{ such that } F(\mathbf{a}, \mathbf{b}) = 1\}$. The output of C is $\vee_{\mathbf{a} \in T} \sigma_{\mathbf{a}}$.

Notice that C is a depth four circuit. Further, since there are $2^{n/2}$ $\wedge_{\mathbf{b}}$ gates and two gates $\pi_{\mathbf{a}}$ and $\sigma_{\mathbf{a}}$ for each of the $2^{n/2}$ values of $\mathbf{a}$, $\mathcal{C}(F') \in O(2^{n/2})$ as required.

Problem 8 (MOD_{p^k} for Prime p)**.** *The n-variable* MOD_4 *function is computable by a polynomial-sized constant-depth* $\mathsf{AC}^0[2]$ *circuit.*

Solution. Let the input to MOD_4 be $\mathbf{x} \in \{0,1\}^n$ with entries x_i. Let gates $m_i = \mathrm{MOD}_2(x_1, ..., x_i)$ for $i \in [n]$ and gates $p_j = m_j \wedge m_{j+1}$ for $j \in [n-1]$. We claim that

$$\mathrm{MOD}_4(\mathbf{x}) = \overline{m}_n \wedge \mathrm{MOD}_2(m_1, ..., m_n, p_1, ..., p_{n-1}).$$

To see why this is, consider the sequence $(m_1, ..., m_n)$. Divide this sequence into maximal blocks $b_1 \cdots b_k$ consisting of the same bit value. Let k_0 and k_1 be the number of 0 and 1 blocks respectively such that $k_0 + k_1 = k$. For example,

$$(0,1,0,0,1,1,1,1,1,1,0) \implies b_1 = 0, b_2 = 1, b_3 = 00, b_4 = 111111, b_5 = 0$$

$k_0 = 3$ and $k_1 = 2$. We claim that $\sum_{i=1}^n x_i \equiv 0 \mod 4$ if and only if $k_1 \equiv 0 \mod 2$ and $m_n = 0$. First $\mathrm{MOD}_4(x_1, ..., x_n) = 0 \implies m_n = \mathrm{MOD}_2(x_1, ..., x_n) = 0$. Assuming that $m_n = 0$, consider a maximal block of consecutive ones $m_i m_{i+1} \cdots m_j$ in the sequence. Since the block is maximal, $m_{i-1} = 0$ or $i = 1$ so there are an even number of ones among $x_1, ..., x_{i-1}$ and $x_i = 1$. Further

$x_{i+1}, ..., x_j = 0$ since the parity $m_{i+1}, ..., m_j$ remains unchanged. Finally $m_{j+1} = 0$, since the block is maximal, so $x_{j+1} = 1$. Thus such a block of consecutive ones and the subsequent zero accounts for a pair of 1s in the input. If there are an even number of pairs of 1s, then $\sum_{i=1}^{n} x_i \equiv 0 \mod 4$.

It remains to show that $\mathrm{MOD}_2(m_1, ..., m_n, p_1, ..., p_{n-1})$ is equivalent to the parity of k_1 — the number of maximal blocks of 1s. Again suppose that $m_i \cdots m_j$ is a maximal block of 1s. Observe that $p_i, p_{i+1} \cdots p_{j-1} = 1$. Thus

$$\mathrm{MOD}_2(m_i, ..., m_j, p_i, ..., p_{j-1}) = \underbrace{1 \oplus \cdots \oplus 1}_{2(j-i)+1} = 1.$$

This is the case for all maximal blocks of 1. Note that for all other p_ℓ such that $x_\ell = 0$ or $x_{\ell+1} = 0$, $p_\ell = 0$. Since parity is a commutative operation, by grouping the m_is and p_is by maximal blocks of 1s, $\mathrm{MOD}_2(m_1, ..., m_n, p_1, ..., p_{n-1})$ is exactly the parity of k_1.

□