CSC2429 / MAT1304: Circuit Complexity January 24, 2019

Lecture 3: Andreev's function, Nechiporuk's method, and BPP $\subseteq$ P/poly (randomness $<$ nonuniformity)

Instructor: Benjamin Rossman

Last week:

- p-random restriction $\mathbf{R}_p$
- $\mathbb{E}[\ \mathcal{L}(f\restriction \mathbf{R}_p)\ ] = O(p^2\mathcal{L}(f)+1)$ (we saw proof with $p^{1.5}$)
- Composition $f \otimes g$ of boolean functions f and g

Today:

- Andreev's function (1987): $\Omega(n^3/\text{polylog}n)$ lower bound for DeMorgan formulas
- Neciporuk's method (1966): $\Omega(n^2/\log n)$ lower bound for formulas in full binary basis
- BPP $\subseteq$ P/poly (randomness $<$ nonuniformity)
- Valiant (1984): polynomial-size monotone formulas for MAJORITY

1 Andreev's Function (1987)

Definition 1. For $f : \{0,1\}^k \to \{0,1\}$ and $g : \{0,1\}^m \to \{0,1\}$, the **composition** $f \otimes g : \{0,1\}^{k\times m} \to \{0,1\}$ is defined by

$$(f \otimes g)(X) := f(g(X_{1,1},\dots,X_{1,m}),\dots,g(X_{k,1},\dots,X_{k,m})).$$

Recall that $\mathcal{L}(f \otimes g) \le \mathcal{L}(f)\cdot\mathcal{L}(g)$. For example, $\mathcal{L}(f \otimes \text{XOR}_m) \le \mathcal{L}(f)\cdot O(m^2)$. The next lemma gives the reverse inequality (with a polylog(k) loss).

Lemma 2. *For every $f : \{0,1\}^k \to \{0,1\}$,*

$$\mathcal{L}(f \otimes \text{XOR}_m) \ge \mathcal{L}(f)\cdot\Omega\left(\frac{m}{\log k}\right)^2.$$

Remark: Tal (2014) gives an optimal lower bound $\mathcal{L}(f)\cdot\Omega(m^2)$. Lemma 2 is easier to prove and will be good enough for our purposes. Recent work of Dinur and Meir (2016) prove a generalization of Lemma 2 using communication complexity.

Proof. Let $p := 2\ln k/m$, and let $\mathbf{R}_p$ be the p-random restriction on the mk variables of $f \otimes \mathrm{XOR}_m$. Observe that if $\mathbf{R}_p$ has ≥ 1 star in every row, then $\mathcal{L}((f \otimes \mathrm{XOR}_m)\restriction \mathbf{R}_p) \geq \mathcal{L}(f)$. By a union bound,

$$\mathbb{P}[\ \mathbf{R}_p \text{ has a row with no stars }] \leq k(1-p)^m \leq ke^{-pm} \leq \frac{1}{k}.$$

Therefore,

$$1 - \frac{1}{k} \leq \mathbb{P}[\ \mathbf{R}_p \text{ has } \geq 1 \text{ star in every row }] \leq \mathbb{P}[\ \mathcal{L}((f \otimes \mathrm{XOR}_m)\restriction \mathbf{R}_p) \geq \mathcal{L}(f)\ ].$$

On the other hand, by Markov's inequality

$$\mathbb{P}[\ \mathcal{L}((f \otimes \mathrm{XOR}_m)\restriction \mathbf{R}_p) \geq \mathcal{L}(f)\ ] \leq \frac{\mathbb{E}[\ \mathcal{L}((f \otimes \mathrm{XOR}_m)\restriction \mathbf{R}_p)\ ]}{\mathcal{L}(f)}$$

By the shrinkage theorem:

$$\mathbb{E}[\ \mathcal{L}((f \otimes \mathrm{XOR}_m)\restriction \mathbf{R}_p)\ ] = O(p^2 \mathcal{L}(f \otimes \mathrm{XOR}_m) + 1).$$

(We can forget about this $+1$, since $p > 1/\sqrt{\mathcal{L}(f \otimes \mathrm{XOR}_m)} \geq 1/\sqrt{\mathcal{L}(\mathrm{XOR}_m)} \geq 1/m$.)

Therefore,

$$\mathcal{L}(f \otimes \mathrm{XOR}_m) \geq \Omega\left(\frac{\mathcal{L}(f)}{p^2}\right) = \mathcal{L}(f) \cdot \Omega\left(\frac{m}{\log k}\right)^2. \qquad \square$$

Definition 3. Andreev's function with parameters $k, m \in \mathbb{N}$ is the function

$$\mathrm{ANDREEV}_{k,m} : \underbrace{\{k\text{-ary Boolean functions}\} \times (\{0,1\}^m)^k}_{\cong \{0,1\}^{2^k + mk}} \to \{0,1\}$$

defined by

$$\mathrm{ANDREEV}_{k,m}(f, X) := (f \otimes \mathrm{XOR}_m)(X).$$

We view $\mathrm{ANDREEV}_{k,m}$ as an n-ary Boolean function where $n = 2^k + mk$. (In the case $m = 1$, this is the function $(f, x) \mapsto f(x)$, also known as the *multiplexor function*.)

1.1 Lower bound

For every k-ary Boolean function f, there exists a restriction ρ that "hardwires" the truth table of f in the first 2^k variables (and leaves the remaining mk variables free). Note that $\mathrm{ANDREEV}_{k,m}\restriction \rho$ is the precisely the function $f \otimes \mathrm{XOR}_m$, hence

$$\mathcal{L}(\mathrm{ANDREEV}_{k,m}) \geq \mathcal{L}(f \otimes \mathrm{XOR}_m) \geq \mathcal{L}(f) \cdot \Omega((m/\log k)^2).$$

(Here we are using the obvious fact that $\mathcal{L}(f) \geq \mathcal{L}(f\restriction \rho)$ for any restriction ρ on the variables of f.) By choosing f with $\mathcal{L}(f) \geq \Omega(2^k/\log k)$ (the Riordan-Shannon counting argument for formulas) and setting $m = \Theta(2^k/k)$, we get $n = \Theta(2^k)$ and

$$\mathcal{L}(\mathrm{ANDREEV}_{k,m}) \geq \Omega(2^k/\log k) \cdot \Omega((m/\log k)^2) = \Omega\left(\frac{n^3}{(\log n)^2 (\log\log n)^3}\right).$$

Note: This lower bound is nearly tight: $\mathcal{L}(\text{ANDREEV}_{k,m}) = \widetilde{O}(n^3)$. Also note $\text{ANDREEV}_{k,m}$ has linear circuit size $O(2^k + km)$ (exercise to see why).

Remark: The best lower bound for Andreev's function is $\Omega(n^3/(\log n)^2(\log\log n))$ (Tal 2014). Tal also give an $\Omega(n^3/\log n(\log\log n)^2))$ lower bound for a variant of Andreev's function.

2 Nechiporuk's Method (1966)

So far, we have been considering lower bounds for DeMorgan formulas. We now consider formulas in the full binary basis $B_2 = \{\text{all 2-ary gate types}\}$. We write $\mathcal{L}_{B_2}(\cdot)$ for formula leafsize in this basis.

Note that the p-random restriction $\mathbf{R}_p$ is ineffective against B_2-formulas. We have $\mathbb{E}[\,\mathcal{L}_{B_2}(f\restriction\mathbf{R}_p)\,] \leq p\cdot\mathcal{L}_{B_2}(f)$ (by linearity of expectation over the leaves of f). However, unlike DeMorgan formulas, we do not have the inequality $\mathbb{E}[\,\mathcal{L}_{B_2}(f\restriction\mathbf{R}_p)\,] \leq O(p^{1+\varepsilon}\mathcal{L}_{B_2}(f)+1)$ for any $\varepsilon > 0$. (To see why, consider the case that f is a parity function.)

There is another technique due to Nechiporuk that gives nearly quadratic $\Omega(n^2/\log n)$ lower bounds (the best known for the B_2-formula size of explicit boolean functions). Nechiporuk's technique is based on counting the number of subfunctions of a boolean function over different subsets of input variables.

Definition 4. For any n-ary Boolean function f and $V \subseteq [n]$, let

$$\text{sub}_V(f) := \{f\restriction\rho : \text{restrictions } \rho : [n] \to \{0,1,*\} \text{ with } \rho^{-1}(*) = V\}.$$

be the set of V-**subfunctions** of f.

For purposes of induction, it will be convenient to also define the set

$$\text{sub}^*_V(f) := \{\underline{0}, \underline{1}, f', 1-f' : f' \in \text{sub}_V(f)\}.$$

(Here $\underline{0}$ and $\underline{1}$ stand for the identically 0 and identically 1 functions on $\{0,1\}^V$.) That is, $\text{sub}^*_V(f)$ consists of V-subfunctions of f, their negations, and constant functions $\underline{0}$ and $\underline{1}$. Note that $|\text{sub}^*_V(F)| \leq 4\cdot|\text{sub}_V(F)|$ (in fact, $|\text{sub}^*_V(F)| \leq 2\cdot|\text{sub}_V(F)|+2$).

Definition 5. For an n-ary formula F and $V \subseteq [n]$, let $\ell_V(F)$ denote the number of leaves of F labeled by variables in the set V. Clearly $\text{leafsize}(F) = \ell_V(F) + \ell_{[n]\setminus V}(F)$.

Two useful observations the V-subfunctions of any formula F:

(1) If $F = \mathsf{gate}(G,H)$ (where gate is any 2-ary function $\{0,1\}^2 \to \{0,1\}$), then clearly

$$\text{sub}_V(F) \subseteq \{\mathsf{gate}(g,h) : g \in \text{sub}_V(G),\ h \in \text{sub}_V(H)\}.$$

Therefore, $|\text{sub}_V(F)| \leq |\text{sub}_V(G)|\cdot|\text{sub}_V(H)|$.

(2) If $F = \mathsf{gate}(G,H)$ and moreover $\ell_V(H) = 0$, then $\text{sub}^*_V(F) \subseteq \text{sub}^*_V(G)$.

This is because $\ell_V(H) = 0$ implies that $H\restriction\rho \in \{\underline{0},\underline{1}\}$ for each restriction $\rho : [n] \to \{0,1,*\}$ with $\rho^{-1}(*) = V$. Therefore,

$$F\restriction\rho = \mathsf{gate}(G\restriction\rho, H\restriction\rho) \in \{\mathsf{gate}(G\restriction\rho,\underline{0}), \mathsf{gate}(G\restriction\rho,\underline{1})\} \subseteq \{G\restriction\rho, 1-G\restriction\rho, \underline{0}, \underline{1}\}.$$

This shows that $\text{sub}_V(F) \subseteq \text{sub}^*_V(G)$. It follows that $\text{sub}^*_V(F) \subseteq \text{sub}^*_V(G)$.

Lemma 6. *If F is an n-ary formula and $V \subseteq [n]$ such that $\ell_V(F) \geq 1$, then*

$$|\mathrm{sub}^*_V(F)| \leq 4 \cdot 16^{\ell_V(F)-1}.$$

Proof. By induction on the leafsize of F. In the base case where F has leafsize 1, F is must be a variable x_i where $i \in V$ (since $\ell_V(F) \geq 1$). In this case, $|\mathrm{sub}^*_V(F)| = 4$.

For the induction step, assume $F = \mathsf{gate}(G, H)$. Clearly $\ell_V(F) = \ell_V(G) + \ell_V(H)$. We consider a few cases.

If $\ell_V(H) = 0$, then $\mathrm{sub}^*_V(F) \subseteq \mathrm{sub}^*_V(G)$ by Observation (2). Therefore, $|\mathrm{sub}^*_V(F)| \leq |\mathrm{sub}^*_V(G)| = 4 \cdot 16^{\ell_V(G)-1} = 4 \cdot 16^{\ell_V(F)-1}$ by the induction hypothesis applied to G. Similarly, the lemma holds in the case $\ell_V(G) = 0$.

We are left with the case that $\ell_V(G), \ell_V(H) \geq 1$. In this case,

$$\begin{aligned}
|\mathrm{sub}^*_V(F)| \leq 4 \cdot |\mathrm{sub}_V(F)| &\leq 4 \cdot |\mathrm{sub}_V(G)| \cdot |\mathrm{sub}_V(H)| \\
&\leq 4 \cdot |\mathrm{sub}^*_V(G)| \cdot |\mathrm{sub}^*_V(H)| \\
&\leq 4 \cdot (4 \cdot 16^{\ell_V(G)-1}) \cdot (4 \cdot 16^{\ell_V(H)-1}) \\
&= 4 \cdot 16^{\ell_V(F)-1}.
\end{aligned}$$

□

Corollary 7. *If F is an n-ary formula and $V \subseteq [n]$, then $|\mathrm{sub}_V(F)| \leq 16^{\ell_V(F)}$.*

Proof. The case $\ell_V(F) \geq 1$ is handled by the lemma, as $|\mathrm{sub}_V(F)| \leq |\mathrm{sub}^*_V(F)| \leq 4 \cdot 16^{\ell_V(F)-1} < 16^{\ell_V(F)}$. In the case $\ell_V(F) = 0$, $\mathrm{sub}_V(F)$ is either $\{\underline{0}\}$ or $\{\underline{1}\}$. In either case, $|\mathrm{sub}_V(F)| = 1 = 16^0$. □

Theorem 8 (Nechiporuk's bound)**.** *For any n-ary Boolean function f and partition $V_1 \uplus \cdots \uplus V_t$ of the set $[n]$,*

$$\mathcal{L}_{B_2}(f) \geq \frac{1}{4} \sum_{i=1}^{t} \log |\mathrm{sub}_{V_i}(f)|.$$

Proof. Let F be an optimal B_2-formula for f. Then

$$\mathcal{L}_{B_2}(f) = \mathrm{leafsize}(F) = \sum_{i=1}^{t} \ell_{V_i}(F) \geq \sum_{i=1}^{t} \log_{16} |\mathrm{sub}_{V_i}(F)| = \frac{1}{4} \sum_{i=1}^{t} |\mathrm{sub}_{V_i}(f)|.$$

□

We obtain an $\Omega(n^2/\log n)$ lower bound by applying Nechiporuk's bound to the following boolean function.

Definition 9. For $k \in \mathbb{N}$ and $n = 2^k \cdot 2k$, the *element distinctness* function $\mathrm{ED}_n : \{0,1\}^{2^k \times 2k} \to \{0,1\}$ is defined by

$$\mathrm{ED}_n(X_1, \ldots, X_{2^k}) = \begin{cases} 1 & \text{if } X_1, \ldots, X_{2^k} \text{ are distinct elements of } \{0,1\}^{2k}, \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 10. $\mathcal{L}_{B_2}(\mathrm{ED}_n) = \Omega(n^2/\log n)$.

Proof. Let $V_1 \uplus \cdots \uplus V_{2^k} = [n]$ partition the variables into coordinates for $X_1, \ldots, X_{2^k}$.

For each function $h : \{0,1\}^{2k} \to \{0,1\}$ with $|h^{-1}(0)| = 2^k - 1$, we have $h \in \mathrm{sub}_{V_i}(\mathrm{ED}_n)$ by considering any restriction ρ which fixes $\{0,1\}^{V_j}$ to the distinct elements of $h^{-1}(0)$ for $j \in [2^k] \setminus \{i\}$. Therefore,

$$|\mathrm{sub}_{V_i}(\mathrm{ED}_n)| \geq \binom{4^k}{2^k - 1} \geq (4^k - 2^k + 1)^{2^k - 1}.$$

By Nechiporuk's theorem,

$$\begin{aligned}\mathcal{L}_{B_2}(\mathrm{ED}_n) &\geq \frac{1}{4} \sum_{i=1}^{2^k} \log |\mathrm{sub}_{V_i}(\mathrm{ED}_n)| \\ &= \frac{1}{4} 2^k (2^k - 1) \log(4^k - 2^k + 1) \quad = \quad \Omega(k 4^k) \quad = \quad \Omega(n^2 / \log n).\end{aligned}$$

□

Remark: This lower bound is tight (even for DeMorgan formulas), as we have $\mathcal{L}(\mathrm{ED}_n) = O(n^2/\log n)$.

Remark: Nechiporuk's method also gives an $\widetilde{\Omega}(n^2)$ lower bound for $\mathcal{L}_{B_2}(\mathrm{ANDREEV}_{k,m})$ (with appropriate k and m).

Homework exercise: Show that $\Omega(n^2/\log n)$ is the limit of the lower bounds using Nechiporuk's method.

3 Summary and next topics

3.1 Lower bounds we've seen so far

model	method	best lb	limit
DeMorgan circuits (random)	counting	$2^n/n$	$2^n/n + o(2^n/n)$
DeMorgan formulas (random)	counting	$2^n/\log n$	$2^n/\log n + o(2^n/n)$
DeMorgan circuits	gate elim.	$5n - o(n)$	$O(n)$ [GHKK'18]
B_2-circuits	gate elim.	$3.01n - o(n)$	$O(n)$ [GHKK'18]
DeMorgan formulas	Khrapchenko/Koutsoupias	n^2	n^2
DeMorgan formulas	shrinkage + clever function	$\widetilde{\Omega}(n^3)$	unclear
B_2-formulas	Nechiporuk	$\Omega(n^2/\log n)$	$O(n^2/\log n)$

3.2 Restricted classes

We will focus on the both the power and limitations (upper and lower bounds) in *restricted classes* of circuits and formulas. The main settings are:

- *Monotone circuits and formulas* (no negations).

  We write $\mathcal{C}_{\mathrm{mon}}(f)$ and $\mathcal{L}_{\mathrm{mon}}(f)$ for the monotone circuit / formula size of a monotone function f.

- *Bounded-depth circuits* with negations and unbounded fan-in gates AND, OR, MOD_m, MAJ.

Some bounded-depth circuit classes:

- AC^0: constant-depth, poly-size, $\{AND, OR, NOT\}$-circuits
- $\mathsf{AC}^0[m]$: constant-depth, poly-size $\{AND, OR, NOT, MOD_m\}$-circuits
- TC^0 (T is for Threshold): constant-depth, poly-size $\{AND, OR, NOT, MAJ\}$-circuits
  Remark: we can compute arbitrary threshold function
- NC^1: $O(\log n)$-depth, poly-size circuits = poly-size formulas
- P/poly: poly-size circuits
- We will see

$$\mathrm{AC}^0 \subsetneqq \mathrm{AC}^0[2] \subsetneqq \mathrm{AC}^0[6] \subseteq \mathrm{TC}^0 \subseteq \mathrm{NC}^1$$

- We won't focus on classes between NC^1 and P/poly, but there are several interesting ones:

$$\mathrm{NC}^1 \subseteq \mathrm{L/poly} \subseteq \mathrm{NL/poly} \subseteq \mathrm{NC}^2 \subseteq \mathrm{NC} \subseteq \mathrm{P/poly}.$$

4 BPP/poly $\subseteq$ P/poly: Nonuniformity is more powerful than randomness

Definition 11. A *randomized circuit* for a Boolean function $f : \{0,1\}^n \to \{0,1\}$ is a circuit $C(x, y)$ of $n + m$ variables (i.e. an input $x \in \{0,1\}^n$ and a random seed $y \in \{0,1\}^m$) such that

$$\mathop{\mathbb{P}}_{y \in \{0,1\}^m}[\ C(x,y) = 1\ ] \begin{cases} \leq 1/3 & \text{if } f(x) = 0, \\ \geq 2/3 & \text{if } f(y) = 1. \end{cases}$$

$\mathsf{BPP/poly}$ is the class of boolean functions computable by polynomial-size randomized circuits. This is the nonuniform version of the complexity class BPP (randomized polynomial time). This class remains the same if 1/3 and 2/3 above are replaced by a and b for any constants $0 < a < b < 1$.

Theorem 12 (Adelman 1978)**.** *If $f : \{0,1\}^n \to \{0,1\}$ is computable by a polysize randomized circuit, then it is computable by a polysize circuit (that is, $\mathsf{BPP/poly} \subseteq \mathsf{P/poly}$).*

Proof. We will use the fact that MAJ_n has polynomial-size circuits (in fact, it has $O(n)$ size circuits). You will see one way of showing this in homework exercises; a different method will be presented later (in fact, we will show that MAJ_n has polynomial-size monotone formulas).

Recall that $\text{Bin}(n, p)$ is the binomial random variable with density function $\mathbb{P}[\ \text{Bin}(n,p) = k\ ] = \binom{n}{k} p^k (1-p)^{n-k}$. We will use Chernoff bounds:

$$\mathbb{P}[\ \text{Bin}(n,p) \geq (1+\varepsilon)pn\ ] \leq \exp\left(-\frac{\varepsilon^2 pn}{2+\varepsilon}\right),$$

$$\mathbb{P}[\ \text{Bin}(n,p) \leq (1-\varepsilon)pn\ ] \leq \exp\left(-\frac{\varepsilon^2 pn}{2}\right) \text{ for } 0 < \varepsilon < 1.$$

Suppose $f : \{0,1\}^n \to \{0,1\}$ is in $\mathsf{BPP/poly}$ and let $C(x,y)$ be a polynomial-size randomized circuit for f on $n+m$ variables (where $m = n^{O(1)}$ without loss of generality). For any $t \in \mathbb{N}$, let $g_t : \{0,1\}^n \times \{0,1\}^{t \times m} \to \{0,1\}$ be the boolean function

$$g_t(x, Y) := \mathrm{MAJ}_t(f(x, Y_1), \ldots, f(x, Y_t))$$

where $Y_i = (Y_{i,1}, \ldots, Y_{i,m}) \in \{0,1\}^m$. Note that g_t is computable by a circuit of size $t \cdot \mathrm{size}(C) + \mathcal{C}(\mathrm{MAJ}_t)$, namely, take an optimal circuit for MAJ_t and replace the ith input with the circuit $C(x, Y_i)$. So long as $t = n^{O(1)}$, we have $\mathcal{C}(g_t) = n^{O(1)}$.

For any fixed $x \in \{0,1\}^n$, we claim that

$$\mathop{\mathbb{P}}_{Y \in \{0,1\}^{k \times m}}[\ g_t(x, Y) \neq f(x)\ ] \leq \mathbb{P}[\ \mathrm{Bin}(t, 1/2) \geq t/2\ ].$$

Without loss of generality, assume that $f(x) = 0$. (The argument is analogous if $f(x) = 1$.) Let $p_x := \mathbb{P}_{y \in \{0,1\}^m}[\ C(x,y) = 1\ ]$. We have $p_x \leq 1/3$ by definition of $C(x,y)$ being a randomized circuit for f. Next, note that random variables $C(x, Y_1), \ldots, C(x, Y_t)$ are independent (for uniform random $Y \in \{0,1\}^{t \times m}$). Therefore,

$$\begin{aligned}
\mathop{\mathbb{P}}_{Y \in \{0,1\}^{k \times m}}[\ g_t(x, Y) \neq f(x)\ ] &= \mathop{\mathbb{P}}_{Y \in \{0,1\}^{k \times m}}[\ g_t(x, Y) = 1\ ] \\
&= \mathop{\mathbb{P}}_{Y \in \{0,1\}^{k \times m}}[\ \mathrm{MAJ}_t(C(x, Y_1), \ldots, C(x, Y_t)) = 1\ ] \\
&= \mathop{\mathbb{P}}_{Y \in \{0,1\}^{k \times m}}[\ C(x, Y_1) + \cdots + C(x, Y_t) \geq t/2\ ] \\
&= \mathop{\mathbb{P}}_{Y \in \{0,1\}^{k \times m}}[\ \mathrm{Bin}(t, p_x) \geq t/2\ ] \\
&\leq \mathop{\mathbb{P}}_{Y \in \{0,1\}^{k \times m}}[\ \mathrm{Bin}(t, 1/3) \geq t/2\ ] \quad (p_x \leq 1/3) \\
&\leq \exp\left(-\frac{(3/2)^2 (t/3)}{2 + (3/2)}\right) \quad \text{(Chernoff bound).}
\end{aligned}$$

By choosing $t = 10n$ (say), we get

$$\mathop{\mathbb{P}}_{Y \in \{0,1\}^{k \times m}}[\ g_{10n}(x, Y) \neq f(x)\ ] < \frac{1}{2^n}.$$

If we now take a union bound over all inputs $x \in \{0,1\}^n$, we have

$$\begin{aligned}
\mathop{\mathbb{P}}_{Y \in \{0,1\}^{k \times m}}[\ \bigvee_{x \in \{0,1\}^n} g_{10n}(x, Y) \neq f(x)\ ] &\leq \sum_{x \in \{0,1\}^n} \mathop{\mathbb{P}}_{Y \in \{0,1\}^{k \times m}}[\ g_{10n}(x, Y) \neq f(x)\ ] \\
&< \sum_{x \in \{0,1\}^n} \frac{1}{2^n} \quad = \quad 1.
\end{aligned}$$

By the magic of the probabilistic method, it follows that there exist some fixed setting of $Y \in \{0,1\}^{k \times m}$ such that $g_{10n}(x, Y) = f(x)$ for all $x \in \{0,1\}^n$. By hardwiring this setting of Y in the circuit computing g, we get a deterministic (though nonexplicit) circuit computing f correctly on all inputs. □

In homework exercise, you will be asked to show a similar result for $\mathsf{AC^0}$ circuits.