Smaller ACC0 Circuits for Symmetric Functions*

Brynmor Chapman  
MIT

Ryan Williams†  
MIT

Abstract

What is the power of constant-depth circuits with MOD$_m$ gates, that can count modulo $m$? Can they efficiently compute MAJORITY and other symmetric functions? When $m$ is a constant prime power, the answer is well understood. In this regime, Razborov and Smolensky proved in the 1980s that MAJORITY and MOD$_m$ require superpolynomial-size MOD$_q$ circuits, where $q$ is any prime power not dividing $m$. However, relatively little is known about the power of MOD$_m$ gates when $m$ is not a prime power. For example, it is still open whether every problem decidable in exponential time can be computed by depth-3 circuits of polynomial-size and only MOD$_6$ gates.

In this paper, we shed some light on the difficulty of proving lower bounds for MOD$_m$ circuits, by giving new upper bounds. We show how to construct MOD$_m$ circuits computing symmetric functions with non-prime power $m$, with size-depth tradeoffs that beat the longstanding lower bounds for AC$^0[m]$ circuits when $m$ is a prime power. Furthermore, we observe that our size-depth tradeoff circuits have essentially optimal dependence on $m$ and $d$ in the exponent, under a natural circuit complexity hypothesis.

For example, we show that for every $\varepsilon > 0$, every symmetric function can be computed using MOD$_m$ circuits of depth 3 and $2^{\varepsilon n}$ size, for a constant $m$ depending only on $\varepsilon > 0$. In other words, depth-3 CC$^0$ circuits can compute any symmetric function in subexponential size. This demonstrates a significant difference in the power of depth-3 CC$^0$ circuits, compared to other models: for certain symmetric functions, depth-3 AC$^0$ circuits require $2^{\Omega(\sqrt{n})}$ size [Håstad 1986], and depth-3 AC$^0[p^k]$ circuits (for fixed prime power $p^k$) require $2^{\Omega(n^{1/6})}$ size [Smolensky 1987]. Even for depth-two MOD$_p \circ$ MOD$_m$ circuits, $2^{\Omega(n)}$ lower bounds were known [Barrington Straubing Thérien 1990].
1 Introduction

We consider constant-depth circuits in which every (unbounded fan-in) gate (called a MOD$_m$ gate) determines whether the sum of its inputs is divisible by a small constant integer $m$. Although the model looks rather peculiar, constant-depth circuits with constant moduli gates (a.k.a. CC$^0$ circuits, a.k.a. pure-ACC circuits [Yao90]) have been a longstanding and fundamental roadblock in the way of improved circuit complexity lower bounds. Since their identification over 30 years ago [Bar86, BT87], scant progress has been made on lower bounds against CC$^0$ circuits, and their close cousin ACC$^0$ which includes AND and OR in the gate basis. Some exceptions include work focusing on special cases of the problem (e.g., [BBR94, GT00, CGPT06, CW09]), uniform lower bounds [AG94], and work proving strong lower bounds but only for functions whose complexity is in QuasiNP or higher (e.g., [Wil11, CP19, MW20, CLW20]). If there has ever been a “circuit complexity winter”, CC$^0$ circuits are at least partly to blame.

Besides our own ignorance, could there be deeper reasons why CC$^0$ circuits have been so difficult for showing limitations? In this paper, we explore the possibility that CC$^0$ circuits may be powerful, focusing on the natural class of symmetric Boolean functions whose output depends only on the number of ones in the input. Although it has been conjectured for many years that the AND function does not have polynomial-size CC$^0$ circuits ([BIS90, Thé94, ST06])$^1$ our results show that low-depth MOD$_m$ circuits with arbitrary but fixed modulus $m$ can actually compute arbitrary symmetric Boolean functions (such as MAJORITY) much more efficiently than low-depth circuits with AND, OR, and MOD$_q$ gates, when $q$ is a prime power.

It is well-known that AC$^0$ circuits, which consist of AND, OR, NOT gates and have constant-depth, require $\exp(\Omega(n^{1/(d-1)})$ size to compute arbitrary symmetric functions in depth $d$ [Häs86]. In recent work, Oliveira, Santhanam, and Srinivasan [OSS19] have shown that PARITY gates (a.k.a. MOD$_2$ gates) can help compute symmetric functions more efficiently than what AND, OR, NOT can accomplish in constant depth. In particular, they show that AC$^0[2]$ circuits (with AND, OR, and PARITY) of depth 4 can compute MAJORITY in $\exp(\Omega(n^{1/4}))$ size, depth $d \geq 5$ can compute symmetric functions in size $\exp(\tilde{O}(n^{\frac{2}{2^{\ell}}}))$, and they show a size lower bound of $\exp(\Omega(n^{1/(2d-4)})$ for the MAJORITY function, improving [Raz87, Smo87].

Smaller MOD$_m$ Circuits. Even smaller circuits for symmetric functions are achievable using MOD$_m$ gates, for other composite $m$? It turns out that this is possible. In fact, even in depth three, any symmetric function can be computed with a MOD$_m$ circuit of size $2^m$ for any desired $\varepsilon > 0$.

**Theorem 1.1.** For every $\varepsilon > 0$, there is a modulus $m \leq (1/\varepsilon)^{2}/\varepsilon$ such that every symmetric function on $n$ bits can be computed by depth-3 MOD$_m$ circuits of $\exp(O(n^\varepsilon))$ size. In fact, the circuits have the form MOD$_{p_1} \circ$ MOD$_{p_2} \circ \ldots \circ$ MOD$_{p_r}$, where $p_1, \ldots, p_r$ are distinct primes.$^2$

That is, without any AND/OR gates, we can obtain CC$^0$ circuits that beat the longstanding lower bounds for AC$^0[q]$ circuits, for prime power $q$.

It has been known for decades [BST90] that depth-two MOD$_p \circ$ MOD$_m$ circuits (and CC$^0[p] \circ$ MOD$_m$ circuits) require $2^\Omega(m)$ size to compute the AND function, where $p$ is a prime and $m$ is an arbitrary composite, and that only certain restricted symmetric functions could be computed in subexponential-size and depth-two [GT00]. Theorem 1.1 shows that an additional layer of MOD$_p$ gates makes such circuits much more powerful.

It is well-known that for distinct primes $p, q$, every symmetric function on $n$ bits has a MOD$_{pq}$ circuit of size $\exp(O(n^\varepsilon))$ and depth $O(1/\varepsilon).$$^3$ Our result shows the depth can always be made 3, at the cost of increasing the modulus to a large enough constant. Hansen [Han06], building on Bhatnagar, Gopalan, and Lipton [BGL06], shows that for $m$ which is the product of $r$ primes, and sufficiently small $\ell$ (smaller than each of the prime factors of $m$), the MOD$_2$ function can be represented by a polynomial over $\mathbb{Z}_m$ of degree $O(n^{1/\ell})$. As a corollary of Hansen’s work, Gopalan observed [Gop06] that for every $\varepsilon > 0$ there is an $m$ such that the MOD$_2$ function has depth-3 MOD$_m$ circuits

---

$^1$See [HK10] for an interesting counterpoint. They show that probabilistic CC$^0$ circuits can in fact compute AND efficiently, and that the AND ? CC$^0$ problem is equivalent to a certain CC$^0$ derandomization question.

$^2$The $G \circ H \circ I$ notation means that the output gate has type $G$, on the middle layer there are gates only of type $H$, and on the bottom layer (nearest the inputs) there are only gates of type $I$.

$^3$The authors don’t know the origin of this construction. It follows from the fact that every function on $k$ bits has a depth-2 MOD$_{pq}$ circuit of size $2^\Theta(k)$, and that symmetric functions can be easily “decomposed” into smaller functions (as in [AK10]).
of size $2^{n^e}$. This naturally suggests the question of whether every symmetric function admits such a circuit, which is answered by our Theorem 1.1.

Allowing larger depths, we can obtain MOD$_m$ circuits with an interesting size-depth tradeoff.

**Theorem 1.2.** Let $d \geq 3$ be an integer, and let $m$ be a product of $r \geq 2$ distinct primes. Then every symmetric function on $n$ bits can be computed by depth-$d$ MOD$_m$ circuits of size $\exp(\tilde{O}(n^{1/(r+d-3)}))$.

To contrast, recall that the lower bounds for AC$^0$ are $\exp(\Omega(n^{1/(d-1)}))$ size for depth $d$ [Häs86], and the lower bounds for AC$^0[p^k]$ (with AND, OR, and MOD$_{p^k}$ gates) are $\exp(\Omega(n^{1/(2d)}))$ [Raz87, Smo87] for prime power $p^k$ (where the constant factor depends on $p^k$). Thus for constant moduli $m$ with enough prime factors, one can beat both lower bounds with MOD$_m$ gates.

For large enough depth $d$, we can achieve even smaller circuits with a size bound of the form $\exp(n^{O(1)/(r-d)})$, multiplying $r$ and $d$ in the denominator, instead of adding them.

**Theorem 1.3.** There is a universal constant $c \geq 1$ such that, for all sufficiently large depths $d$, and all composite $m$ with $r$ prime factors, every symmetric function can be computed by a MOD$_m$ gate circuit of depth $d$ and size $\exp(O(n^{r/((d-c)(r-1))}))$.

We remark that the constant $c$ in the above construction is not terribly small. In concurrent (very recently released) work, [IKK21] give a circuit construction with a similar tradeoff (but better constants) for the special case of the AND function, building on the polynomials of [BBR94].

**Even Smaller Circuits in ACC$^0$.** Allowing AND and OR gates in our circuit, the size of our circuit constructions can be further improved. Say that a product $m$ of primes $q_1, \ldots, q_e$ is **good** if every prime factor of $\phi(m)$ divides $m$. We note that the primorial $m = p_r\#$, the product of the first $r$ primes, is good.

**Theorem 1.4.** Let $m$ be a good product of $r$ primes. For every symmetric function $f$ on $n$ inputs and every depth $d \geq 4$ congruent to 1 modulo 3, there exists an AC$^0[m]$ circuit of depth $d$ and size $\exp(\tilde{O}(n^{3/(r+3)(d-1)-3}))$ computing $f$.

In the proof of Theorem 1.4, we make use of several tools from the recent AC$^0[2]$ circuits of [OSS19] (circuits for elementary symmetric polynomials and circuits for the coin problem), along with known results on computing elementary symmetric polynomials modulo a prime.

Applying standard tricks (seen in [HP10, Wil14, OSS19]), Theorem 1.4 extends to linear threshold functions.

**Corollary 1.1.** Let $m$ be a good product of $r$ primes. For every linear threshold function $f$ on $n$ inputs and every depth $d \geq 4$ congruent to 1 modulo 3, there exists an AC$^0[m]$ circuit of depth $d + 2$ and size $\exp(\tilde{O}(n^{3/(r+3)(d-1)-3}))$ computing $f$.

This follows directly from the fact that every linear threshold function can be written as an OR of poly($n$) ANDs of poly($n$) symmetric functions on $n$-bit inputs [HP10]. In general, Theorem 1.4 implies that TC$^0$ circuits (composed of MAJORITY and NOT gates) with small fan-in also have a nontrivial simulation.

**Corollary 1.2.** Every TC$^0$ circuit of depth $e$ in which every gate has fan-in at most $s$ has an equivalent MOD$_m$ circuit of depth $d \cdot e$ and size at most $\exp(\tilde{O}(s^{3/(r+3)(d-1)-3}))$, where $m$ is a good product of $r$ primes.

The corollary follows from direct substitution of each MAJORITY gate with depth-$d$ circuits from our Theorem 1.4. Note that such depth-$e$ TC$^0$ circuits have at most $O(s^{e-1})$ gates.

\footnote{Our $c$ is at least 6; this matters if one cares about very small $d$ and $r$.}

\footnote{Indeed, for all $i = 1, \ldots, r$, the prime factors of $q_i - 1$ are contained in $\{q_1, \ldots, q_{i-1}\}$, all of which divide $m = p_r\#$.}
Can’t you do any better? Theorem 1.4 shows that for certain $m$ which are products of $r$ primes, one can compute arbitrary symmetric functions in depth $d$ and size $\exp(n^{\tilde{f}})$ where $c > 0$ is a constant. We give evidence that it may be difficult to improve asymptotically on the dependence of $r$ and $d$ in the exponent of $n$, based on a natural hypothesis regarding $\text{TC}^0$ circuits, which are constant-depth circuits composed of MAJORITY and NOT gates. (Of course it is difficult to prove anything unconditional here, because as far as we know, polynomial-size depth-3 $\text{MOD}_6$ circuits could compute every $\exp$ function. Thus we settle for conditional hardness.)

Recall that a $\text{SYM} \circ \text{AND}$ circuit is a depth-two circuit where the output is a symmetric function and the bottom layer computes ANDs of input variables and negations. The hypothesis is that subexponential-size $\text{SYM} \circ \text{AND}$ circuits cannot compute $\text{TC}^0$ circuits in which each gate has linear fan-in.

**Hypothesis 1** (SYM ○ AND Hypothesis). There are constants $c,k > 1$ such that for sufficiently large $n$, there is a function $f : \{0,1\}^n \rightarrow \{0,1\}$ computable by $\text{TC}^0$ circuits of depth $c$ with at most $\tilde{O}(n)$ gates where each gate has fan-in $\tilde{O}(n)$, such that $f$ does not have an $\exp(\tilde{O}(n^{1/k}))$ size $\text{SYM} \circ \text{AND}$ circuit.

A well-known result in circuit complexity is that every $\text{ACC}^0$ circuit of size $s$ can be simulated by a $\text{SYM} \circ \text{AND}$ circuit of size $s^{\text{polylog}(s)}$ [BT94, CP19]. Therefore, the SYM ○ AND Hypothesis is a strengthening of the longstanding hypothesis that $\text{TC}^0 \not\subset \text{ACC}^0$: the SYM ○ AND Hypothesis implies exponential lower bounds for simulating $\text{TC}^0$ circuits with $\text{ACC}^0$ circuits. Indeed, the hypothesis implies that our $\text{ACC}^0$ circuits for symmetric functions are nearly size-optimal in their dependence on depth and modulus.

**Theorem 1.5** (Near-Optimality Modulo a Conjecture). Assuming the SYM ○ AND Hypothesis, there is a fixed $\alpha > 0$ such that for every $m$ and $d$, every depth-$d$ $\text{ACC}^0[m]$ circuit computing the MAJORITY function on $n$ inputs requires size at least $\exp(n^{\tilde{f}})$ for sufficiently large $n$, where $r$ is the number of distinct prime factors of $m$.

The proof of Theorem 1.5 is in Appendix A. Therefore, we view size bounds of the form $\exp(n^{1/\Theta(rd)})$ (as seen in our results) as a natural barrier to better upper bounds on $\text{MOD}_m$ circuits: any function with significantly smaller $\text{MOD}_m$ circuit complexity (as a function of $n$, $r$, and $d$) would also yield a highly non-trivial $\text{SYM} \circ \text{AND}$ circuit simulation of $\text{TC}^0$. In order to achieve significantly smaller circuits as a function of $n$, $d$, and $r$, one has to at least refute the hypothesis. Of course, even assuming Hypothesis 1, our circuits can probably be improved by constant factors in the exponents.

## 2 Preliminaries

We assume basic familiarity with computational complexity [AB09] and Boolean circuit complexity [Juk12], although we have tried to keep the paper relatively self-contained.

**Notation.** For a binary vector $x$, we use $|x|_1$ to denote the $\ell_1$-norm, i.e., the number of ones in $x$.

Besides $\text{AC}^0$, $\text{ACC}^0$, $\text{CC}^0$, and $\text{TC}^0$, we also use the following additional notation for various circuit types, all of which is standard. A circuit of type $\text{SYM}$ is a symmetric Boolean function. An $\text{EMAJ}$ function outputs 1 on an input $(x_1, \ldots, x_n) \in \{0,1\}^n$ if and only if $\sum x_i = T$ for a fixed target $T$. A circuit of type $G_1 \circ \cdots \circ G_d$ notation is a circuit where the output gate has type $G_1$, the next layer of gates all have type $G_2$, and so on, and the bottom layer (nearest the inputs) only contains gates of type $G_d$.

The following basic fact is useful to keep in mind.

**Proposition 2.1.** For all positive $m, n \in \mathbb{Z}$, any $\text{MOD}_m$ gate of fan-in $t$ can be simulated by a $\text{MOD}_{nm}$ of fan-in $nt$.

**Proof.** For any positive integer $t, m | t$ if and only if $nm | nt$. So $\text{MOD}_m(x_1, \ldots, x_t) = \text{MOD}_{nm}(n \cdot x_1, \ldots, n \cdot x_t)$. \qed

**Tools.** We make use of several known results. First, we note that AND circuits of small fan-in have efficient depth-two $\text{MOD}_m$ circuits. A version was first used in [BIS90] in the context of $\text{MOD}$ circuits, and more recently a strengthening was used to reduce the size-depth tradeoff for simulating $\text{ACC}^0$ circuits with $\text{SYM} \circ \text{AND}$ circuits [CP19]. (Chen and Papakonstantinou [CP19] call this “linearization”.)
Proposition 2.2 ([BIS90, CP19]). Let \( a, b \geq 2 \) be fixed integers with \( \gcd(a, b) = 1 \). Every AND of \( k \) \( \text{MOD}_b \) gates can be represented by an \( \text{MOD}_a \circ \text{MOD}_b \) circuit of \( O(b^k) \) gates. Furthermore, on all \( k \)-bit inputs, the sum of the inputs to the output gate of the circuit is always 0 (mod \( a \)) or 1 (mod \( a \)).

Our next tool is an old number-theoretic theorem on elementary symmetric polynomials modulo \( p \), masterfully applied by Beigel, Barrington, and Rudich [BBR94] in their non-trivial degree polynomials for the OR functions over composite moduli.

Theorem 2.1 (Lucas’ Theorem [Luc78]). For all primes \( p \) and natural numbers \( n \),

\[
\binom{n}{p^i} \mod p
\]

is the \( i \)-th digit in the \( p \)-ary representation of \( n \).

Lucas’ theorem has the following direct consequence for polynomial representations of Boolean functions.

Lemma 2.1 ([BBR94]). Let \( p \) be a prime, let \( n \) be a natural number, and let \( e_i(x) \) denote the \( i \)-th elementary symmetric polynomial on \( n \) variables. For a binary vector \( x \), let

\[
\sum y_i \cdot p^i = |x|_1
\]

be the \( p \)-ary expansion of \( |x|_1 \). Then for every \( i \), \( e_p(x) \equiv y_i \mod p \).

In order to apply the elementary symmetric polynomials, our construction also involves arithmetic circuits over prime fields. These circuits will be translated into Boolean circuits with \( \text{MOD}_m \) gates.

Lemma 2.2 ([COST16, OSS19]). Let \( p \) be a prime, let \( n, i \in \mathbb{N} \), and let \( d \geq 2 \) be even. There is an arithmetic circuit over \( \mathbb{F}_p \) of depth \( d \) and size \( n^{O(2^d)} \) computing the \( i \)-th elementary symmetric polynomial (over \( \mathbb{F}_p \)) on \( n \) inputs, where the output gate is a \( \times \) gate.

We also use \( \text{AC}^0 \) circuits for the coin problem. These were also used by [OSS19] in their improved \( \text{AC}^0 [2] \) circuits for symmetric functions.

In the following, we let \( i, j \in \{0, 1, \ldots, n\} \), and let \( D_{i, j} \) be any partial function satisfying the properties:

\[
D_{i, j}(x) = 1 \text{ if } |x|_1 = i, \text{ and} \\
D_{i, j}(x) = 0 \text{ if } |x|_1 = j.
\]

Lemma 2.3 ([OW07, Ama09, OSS19]). Let \( d \geq 2 \) and \( n \) be natural numbers, and let \( i \neq j \). Then there is an \( \text{AC}^0 \) circuit of depth \( d \) and size \( \exp(O(d (n/|i - j|)^{1/(d-1)})) \) computing \( D_{i, j} \) on \( n \) inputs, where the output gate is an \( \text{AND} \).

Intuitively, Lemma 2.3 will be useful when \( |i - j| \) is “large”.

3 CC0 Circuits for Symmetric Functions

We begin by giving efficient depth-3 \( \text{CC}^0 \) circuits for symmetric functions.

Reminder of Theorem 1.1. For every \( \varepsilon > 0 \), there is a modulus \( m \leq (1/\varepsilon)^{2/\varepsilon} \) such that every symmetric function on \( n \) bits can be computed by depth-3 \( \text{MOD}_m \) circuits of \( \exp(O(n^\varepsilon)) \) size. In fact, the circuits have the form \( \text{MOD}_{p_1} \circ \text{MOD}_{p_2} \circ \cdots \circ \text{MOD}_{p_r} \), where \( p_1, \ldots, p_r \) are distinct primes.

After that, we will generalize the result to a size-depth tradeoff in the next subsection. That tradeoff will be further improved in Section 4 when we allow the use of AND and OR gates.

As a warm-up, we first consider the special case where \( \varepsilon > 1/3 \) and \( m = 30 \).
Theorem 3.1. Every symmetric Boolean function on \( n \) variables has a depth-three circuit of the form \( \text{MOD}_2 \circ \text{MOD}_6 \circ \text{MOD}_5 \), of size \( \exp(O(n^{1/3} \log n)) \). Furthermore, the output gate is a linear sum which always evaluates to either 0 or 1 modulo 5.

Note that the upper bound of Theorem 3.1 already beats the well-known lower bounds for depth-3 \( \text{AC}^0 \) [Hås86].

The remainder of this section is devoted to the proof. A key component is a low-degree multivariate polynomial over \( \mathbb{Z}_6 \) that vanishes on a Boolean vector if and only if the sum of the ones in the vector equals a particular value.

Theorem 3.2. For every \( n \in \mathbb{N} \) and every \( T \in \{0,1,\ldots,n\} \), there is a polynomial \( P_T(x_1,\ldots,x_n) \) of degree at most \( 3\sqrt{n} \) such that for all \( a \in \{0,1\}^n \), \( P_T(a) \equiv 0 \mod 6 \) if and only if \( \sum_j a_j = T \).

Proof. We want a polynomial \( p \) on \( n \) variables such that for all \( y_1,\ldots,y_n \in \{0,1\} \) and \( T \in \{0,1,\ldots,n\} \),

\[
p(y_1,\ldots,y_n) \equiv 0 \mod 6 \iff \sum_j y_j = T.
\]

For the elementary symmetric polynomial \( e_J(y_1,\ldots,y_n) \) of degree \( J \), and for all \( a_1,\ldots,a_n \in \{0,1\} \),

\[
e_J(a_1,\ldots,a_n) = \left( \sum_i a_i \right)^J.
\]

Thus by Lucas’ Theorem (Theorem 2.1), \( e_J(a_1,\ldots,a_n) \mod p \) equals the \( i \)-th digit in the \( p \)-ary representation of \( \sum_i a_i \).

Let \( s \) and \( t \) be integers so that \( 2\sqrt{n} \geq 2^s > \sqrt{n} \) and \( 3\sqrt{n} \geq 3^t > \sqrt{n} \).

Suppose when we write \( T \in \{0,1,\ldots,n\} \) in binary notation, the \( s \) low order bits are \( b_{2s-1},\ldots,b_0 \). Furthermore, when we write \( T \) in ternary notation, the \( t \) low order trits are \( c_{t-1},\ldots,c_0 \).

Define the polynomials

\[
p_2(y_1,\ldots,y_n) := 1 - \prod_{j=0}^{s-1} (1 - (b_j - e_2(y))) \mod 2
\]

and

\[
p_3(y_1,\ldots,y_n) := 1 - \prod_{j=0}^{t-1} (1 - (c_j - e_3(y))^2) \mod 3.
\]

Note the degrees of \( p_2 \) and \( p_3 \) are \( O(\sqrt{n}) \). In particular, \( \deg(p_2) = \sum_{j=0}^{s-1} 2^j = 2^s - 1 \) and \( \deg(p_3) = \sum_{j=0}^{t-1} (2 \cdot 3^j) = 2(3^s - 1)/2 = 3^s - 1 \).

We observe a few properties of the polynomials \( p_2 \) and \( p_3 \):

Proposition 3.1. For all \( a \in \{0,1\}^n \), \( p_2(a) \equiv 0 \mod 2 \) if and only if the binary representation of \( \sum_i a_i \) equals \( b_{2s-1} \cdots b_0 \) in the last \( s \) bits. Analogously, \( p_3(a) \equiv 0 \mod 3 \), and \( p_3(a) \equiv 0 \mod 3 \) if and only if the ternary representation of \( \sum_i a_i \) equals \( c_{t-1} \cdots c_0 \) in the last \( t \) trits.

Proof. We prove the proposition for \( p_3 \); the case of \( p_2 \) is analogous. Let \( a \in \{0,1\}^n \). Each difference \( (e_j - e_3(a))^2 \) is either 0 or 1 modulo 3, and it is 0 if and only if \( e_j = e_3(a) \). Thus the product \( \prod_{j=0}^{t-1} (1 - (e_j - e_3(a))^2) \) equals 1 if and only if \( e_j = e_3(a) \) for all \( j = 0,\ldots,t-1 \), hence \( p_3(a) \equiv 0 \mod 3 \) if and only if \( e_j = e_3(a) \) mod 3 for all \( j = 0,\ldots,t-1 \). Recalling that \( (e_3(a) \mod 3) \) equals the \( j \)-th trit of \( \sum_i a_i \), the result follows.

We note that in general, working modulo a prime \( q \), we may construct a polynomial with degree \( (q^2 - 1) \) of the form

\[
p_q(y_1,\ldots,y_n) = 1 - \prod_{j=0}^{q-1} (1 - (c_j - e_q(y))^{q-1}).
\]

(1)
By the above proposition, it follows that for all \( a \in \{0,1\}^n \),
\[
p_2(a) \equiv 0 \mod 2 \iff \sum_i a_i \equiv T \mod 2^t
\]
and
\[
p_3(y) \equiv 0 \mod 3 \iff \sum_i a_i \equiv T \mod 3^t.
\]
Since \( \sum_i a_i \) and \( T \) are both in \( \{0,\ldots,n\} \) and \( 2^t \cdot 3^t > n \), by the Chinese Remainder Theorem we have
\[
\sum_i a_i = T \iff (\sum_i a_i \equiv T \mod 2^t) \land (\sum_i a_i \equiv T \mod 3^t)
\]
\[
\iff (p_2(y) \equiv 0 \mod 2) \land (p_3(y) \equiv 0 \mod 3) \iff 3p_2(y) + 2p_3(y) \equiv 0 \mod 6.
\]
Thus \( 3p_2(y) + 2p_3(y) \) is a polynomial of degree \( O(\sqrt{n}) \) which equals 0 mod 6 if and only if \( \sum_i y_i = T \). This completes the proof of Theorem 3.2. \( \square \)

We now proceed with the proof of Theorem 3.1.

**Proof.** Let \( f \) be a symmetric function and let \( g : \{0, 1, \ldots, n\} \to \{0,1\} \) be its companion function. That is, for every \( x, f(x) = g(\{x\}_1) \).

The output gate will be a \( \text{MOD}_5 \) gate that
\[
\begin{align*}
\text{• (a) sums over possible choices of } T & \in \{0, 1, \ldots, n\} \text{ such that } g(T) = 1 \\
\text{• (b) sums over all ways to partition } T \text{ into a sum of } t = \lceil n^{1/3} \rceil \text{ parts } T_1, \ldots, T_t \in \{0, 1, \ldots, T\}.
\end{align*}
\]

There are \( 2^{O(n^{1/3} \log n)} \) choices over (a) and (b). We associate each part \( T_i \) with a disjoint set \( S_i \) of at most \( \lceil n^{2/3} \rceil \) variables from the input. For each of the choices from (a) and (b), we wish to verify that, for all \( i = 1, \ldots, t \), the sum of all variables in \( S_i \) equals \( T_i \). Note that there is at most one choice from (a) and from (b) that could possibly be consistent with the given input, so we can use a modulo-5 sum (not just a \( \text{MOD}_5 \) gate) to sum over these choices. This modulo-5 sum will always be either 0 or 1 modulo 5.

By our construction of EMAJ polynomials, each sum over the set \( S_i \) of \( n^{2/3} \) variables can be checked with a \( \text{MOD}_6 \) gate of \( 2^{O(n^{1/3} \log n)} \) fan-in, where each input to the \( \text{MOD}_6 \) gate is the output of an AND of fan-in \( O(n^{1/3}) \). Putting these \( \text{MOD}_5 \circ \text{AND} \) circuits below each wire of the modulo-5 sum, at this point, we have a modulo-5 sum of \( 2^{O(n^{1/3} \log n)} \) ANDs of fan-in \( O(n^{1/3}) \) of \( \text{MOD}_6 \) and \( O(n^{1/3}) \) of ANDs of fan-in \( O(n^{1/3}) \). To eliminate the AND gates, we apply Proposition 2.2, yielding that an AND of \( f \) MOD_{12} gates can be represented by a modulo-p sum of \( O(q^{1/2}) \) MODq gates, as long as \( \gcd(p,q) = 1 \). In particular, for the “middle” ANDs we set \( p = 5 \) and \( q = 6 \), and for the “bottom” ANDs we set \( p = 6 \) and \( q = 5 \). We obtain a modulo-5 sum of \( 2^{O(n^{1/3} \log n)} \) \( \text{MOD}_5 \) of fan-in \( 2^{O(n^{1/3})} \) of \( \text{MOD}_5 \) of fan-in \( O(n^{1/3}) \).

The above construction has several interesting corollaries; here is one.

**Corollary 3.1.** Every circuit of the form \( \text{MOD}_5 \circ \text{SYM} \) of size \( 2^{O(n^{1/3} \log n)} \) can be simulated by a depth-three \( \text{MOD}_5 \circ \text{MOD}_5 \) circuit of size \( 2^{O(n^{1/3} \log n)} \).

**Proof.** We simply replace each SYM gate (which takes \( n \) inputs) in the \( \text{MOD}_5 \circ \text{SYM} \) circuit with a modulo-5 sum of \( \text{MOD}_5 \circ \text{MOD}_5 \) as in the previous theorem. \( \square \)

We are now ready to generalize to Theorem 1.1.

**Reminder of Theorem 1.1.** For every \( \varepsilon > 0 \), there is a modulus \( m \leq (1/\varepsilon)^{2/\varepsilon} \) such that every symmetric function on \( n \) bits can be computed by depth-3 \( \text{MOD}_m \) circuits of \( \exp(O(n^\varepsilon)) \) size. In fact, the circuits have the form \( \text{MOD}_{p_1} \circ \text{MOD}_{p_2} \circ \cdots \circ \text{MOD}_{p_r} \), where \( p_1, \ldots, p_r \) are distinct primes. 6
Proof: Let $\varepsilon > 0$, and let $f$ be a symmetric function. Take $k := \lceil 1 + 1/\varepsilon \rceil$, let $m$ be the product of the first $k$ primes, and let $m' = m/2$.

We use a similar construction as in Theorem 3.1 to get a MOD$_2 \circ$ MOD$_{m'} \circ$ MOD$_2$ circuit for $f$.

The differences are that we partition the target $T \in \{0, 1, \ldots, n\}$ into a sum of $\lceil n^{1/k} \rceil$ parts where each part is over $v := n^{1-1/k}$ variables, and by using $k - 1$ primes instead of two, we can obtain a polynomial for EMAJ on $v$ variables of degree $O(v^{1/(k-1)}) \leq O(n^{1/k})$ in an analogous way.

More precisely, let $T' \in \{0, 1, \ldots, v\}$ be a target value. For the first $k - 1$ odd primes $q_1, \ldots, q_{k-1}$, we take $k - 1$ polynomials $p_{q_1}(x_1), \ldots, p_{q_{k-1}}(x_k)$ as defined in (1) such that each $p_{q_i}(x)$ has degree $(q_i)^v - 1$, where the $t_i$ are chosen such that for all $i \in [k]$,

- $(q_i)^v = \Theta((1)^{1/(k-1)})$,
- $T' \leq v < \prod_i (q_i)^v$, and
- for all $a \in \{0, 1\}^v$ we have $p_{q_i}(a) = 0 \mod q_i \iff \sum_{i} a_i \equiv T' \mod (q_i)^v$.

By the Chinese Remainder Theorem, and similar reasoning as in Theorem 3.1, there are fixed coefficients $M_i \in [m']$ such that

$$\sum_{i=1}^{k-1} M_i \cdot p_{q_i}(a) \equiv 0 \mod m' \iff \bigwedge_{i=1}^{k-1} [p_{q_i}(a) \equiv 0 \mod q_i] \iff \sum_i a_i = T'. $$

Thus we have a polynomial of degree $O(v^{1/(k-1)})$ that vanishes modulo $m'$ precisely when the sum of $v$ variables equals the target $T'$. Naturally we might write this polynomial as a MOD$_{m'} \circ$ AND circuit of $\exp(\Omega(v^{1/(k-1)}))$ size; by replacing each AND with a modulo-$m'$ sum of MOD$_2$ gates (Proposition 2.2), we can express it as a MOD$_{m'} \circ$ MOD$_2$ circuit. Our final circuit has the form MOD$_2 \circ$ MOD$_{m'} \circ$ MOD$_2$ and size $\exp(O(n^{1/k})) \leq \exp(\Theta(n^2))$. \hfill \qed

### 3.1 Size-Depth Tradeoff with CC0

Allowing depth $d$ circuits for $d > 3$, the size of the above construction can be improved as a function of the number of distinct primes $r$ in the modulus. Here we only briefly describe the construction, as the size bound will be improved significantly (as a function of $d$ and $r$) in the following section.

**Reminder of Theorem 1.2.** Let $d \geq 3$ be an integer and let $m$ be a product of $r \geq 2$ distinct primes. Then every symmetric function on $n$ bits can be computed by depth-$d$ MOD$_m$ circuits of size $\exp(\Theta(n^{1/(r+d-3)}))$.

**Proof.** Let $p$ and $q$ be the smallest prime factors of $m$. We prove by induction on $d$ that there are circuits of size $\exp(\Theta(n^{1/(r+d-3)} \log n))$, and we prove additionally that the output gate is a MOD$_p$ gate when $d$ is odd and a MOD$_q$ gate when $d$ is even.

For $d = 3$, we use the construction of Theorem 1.1 to obtain a MOD$_p \circ$ MOD$_{m/p} \circ$ MOD$_p$ circuit of depth $3$ and size $\exp(\Theta(n^{1/\log n}))$.

For the inductive step, we proceed similarly to the proof of Theorem 1.1, except that we now use a MOD$_p$ or MOD$_q$ gate as the output gate (depending on the parity of $d$). We partition the target $T$ into a sum of $t = \lceil n^{1/(r+d-3)} \rceil$ parts, where each part contains at most $\lceil n^{(r+d-4)/(r+d-3)} \rceil$ variables, and our circuit sums over all $\exp(\Theta(t \log n))$ choices for the number of true variables in each part. Since EMMAJ is a symmetric function, we can inductively compute each EMMAJ on $\lceil n^{(r+d-4)/(r+d-3)} \rceil$ variables with a circuit of depth $d - 1$, as guaranteed by the inductive hypothesis. These circuits have size $\exp(\Theta(n^{(r+d-4)/(r+d-3)} \log n)) = \exp(\Theta(n^{1/(r+d-3)} \log n))$, and their output gates have fan-in $\exp(\Theta(n^{1/(r+d-3)} \log n))$. WLOG assume $d$ is odd. Then the depth-$(d-1)$ circuits for EMMAJ described above have the form

$$\text{MOD}_q \circ \cdots \circ \text{MOD}_p \circ \text{MOD}_{m/p} \circ \text{MOD}_p,$$

and our entire circuit has the form

$$\text{MOD}_p \circ \text{AND} \circ \text{MOD}_q \circ \cdots \circ \text{MOD}_p \circ \text{MOD}_{m/p} \circ \text{MOD}_p,$$
where the ANDs have fan-in $t$. As before, each AND $\circ \text{MOD}_q$ can be replaced by a modulo-$p$ sum of MOD$_q$ gates using Proposition 2.2, which only increases the circuit size by a factor of $2^{O(t)}$.

Our final circuit has depth $d$ and size $\exp(O(n^{1/(r+d-3)\log n}))$. $\square$

**A Better Dependence on Depth and Modulus.** We can give a \text{CC}$^0$ circuit construction with a better asymptotic tradeoff (in the double-exponent). We will keep the description of this construction brief and to the point, as its size will be further improved (replaced by better constants) in the next section, using OR and AND gates.

**Reminder of Theorem 1.3.** There is a universal constant $c \geq 1$ such that, for all sufficiently large depths $d$, and $m$ which is the product of the first $r$ prime factors, every symmetric function can be computed by a MOD$_m$ gate circuit of depth $d$ and size $\exp(O(n^{c/((d-c)(r-1))}))$.

*Proof.* First, we recall that every symmetric function $f$ on $n$ variables can be expressed as a MAJORITY of $O(n)$ MAJORITY gates over the $n$ variables (see for example [BBL92] for a reference). Thus it suffices to give a circuit for MAJORITY.

Allender and Koucky [AK10, Theorem 3.8] give a downward self-reduction for the MAJORITY function: they prove that there is a universal constant $a \geq 1$ such that for every $k \geq 1$, the MAJORITY function on $n$ bits can be computed by a TC$^0$ circuit of depth at most $ak$ where each MAJORITY gate has fan-in at most $O(n^{1/k})$. Applying these circuits to the depth-two TC$^0$ circuits described in the previous paragraph, we obtain an analogous circuit of depth $2ak$ for any given symmetric function $f$.

Replace each MAJORITY gate of fan-in at most $O(n^{1/k})$ with a depth-3 MOD$_m$ circuit of size at most

$$\exp(\widetilde{O}(n^{1/(k(r-1))})),$$

as provided by Theorem 1.2. (Note that each NOT gate can always be replaced by a single MOD$_m$ gate, if we do not want to allow NOT gates in our \text{CC}$^0$ circuit.) This results in a circuit of depth $6ak$ and size

$$\exp(\widetilde{O}(n^{1/(k(r-1))})) \leq \exp(\widetilde{O}(n^{1/(k(r-1))})).$$

Thus for depths $d = 6ak$ where $k$ is a positive integer, the size bound is at most $\exp(n^{6a/(d(r-1))})$. For depths $d$ that are not divisible by $6a$, we can simply use the construction for $d' = 6ak$ where $d' < d < 6a(k+1)$, which has size at most $\exp(n^{6a/(d'(r-1))}) < \exp(n^{6a/((d-6a)(r-1))})$. $\square$

The above construction is not useful for $d < 6$ and small $r$, which are of interest. In the next section, we will show that much better constants are obtainable in the \text{ACC}$^0$ setting.

## 4 Size-Depth Tradeoff With \text{ACC}$^0$

We now turn to showing how adding AND and OR gates can help improve the circuits even further. We begin with a result using the concrete modulus 42.

**Theorem 4.1.** For every symmetric function $f$ on $n$ inputs and every depth $d$ with $d \equiv 2 \bmod 6$, there exists an \text{AC}$^0[42]$ circuit of depth $d$ and size $\exp(\widetilde{O}(n^{\frac{c}{(d-2d-2)}}))$ computing $f$.

Observe that, for sufficiently large $d$, the circuit size of Theorem 4.1 already drops below Smolensky’s \text{AC}$^0[p^k]$ depth-$d$ lower bound of $\exp(\Omega(n^{1/(2d^2)}))$ size [Smo87] for computing MOD$_q$ when $\gcd(p,q) = 1$.

We build on the results of Oliveira et al. [OSS19] for computing symmetric functions in \text{AC}$^0[2]$. At a high level, we note that every symmetric function can be written as an OR of AND of (partial) functions of the form $D_{i,j}$, where

$$D_{i,j}(x) = 1 \text{ if } |x|_1 = i, \text{ and}$$

$$D_{i,j}(x) = 0 \text{ if } |x|_1 = j,$$

recalling that $|x|_1$ is the number of 1’s in $x$. Note that $D_{i,j}$ could have arbitrary behavior on any other Boolean inputs.
When \( |i - j| \) is large, the function \( D_{i,j} \) can be simulated by the standard Coin Problem, for which there are known AC\(^0\) circuits (see the Preliminaries). When \( |i - j| \) is small, we give a new construction of AC\(^0\)[42] circuits for \( D_{i,j} \).

We will utilize arithmetic circuits for elementary symmetric polynomials. To that end, the following lemma shows how to generically translate low-depth arithmetic circuits over \( \mathbb{F}_p \) into AC\(^0\)[\( p(p - 1) \)] circuits, in a way that only increases the circuit depth by a 3/2 multiplicative factor. (Getting some constant factor increase is not too difficult; [AAD00] first showed a correspondence between AC\(^1\) and arithmetic circuits over finite fields.)

**Lemma 4.1.** Let \( p \) be prime, and let \( C \) be an arithmetic circuit over \( \mathbb{F}_p \) of size \( s \) and depth \( 2d \) (with alternating layers of + and \( \times \) gates) on \( n \) inputs, such that for every \( x \in \{0, 1\}^n \), \( C(x) \in \{0, 1\} \). Then \( C \) is equivalent to an AC\(^0\)[\( p(p - 1) \)] circuit \( C' \) of size \( O(s \cdot p) \) and depth \( 3d \).

**Proof.** We represent an element \( x \) of \( \mathbb{F}_p \) in unary, by \( p \) indicator bits

\[
b_0(x), b_1(x), \ldots, b_{p-1}(x),
\]

where \( b_0(x) = 0 \) iff \( x = 0 \), and for \( i \neq 0 \), we let \( b_i(x) = 1 \) iff \( x = i \). (We treat the 0-th indicator bit as a special case to make later constructions easier.) We now obtain \( C' \) by replacing each gate in \( C \) with a small AC\(^0\)[\( p(p - 1) \)] gadget circuit.

For each addition gate of \( C \) computing

\[
x = \sum_{j=1}^{k} x_j,
\]

we replace that gate with \( p \) parallel MOD\(_p\) gates, so that

\[
b_i(x) = \begin{cases} 1 & \Leftrightarrow (p - i) + \sum_{j=1}^{k-1} \sum_{l=1}^{p-1} i \cdot b_r(x_j) \equiv 0 \mod p. \end{cases}
\]

(As a special case, we output the negation of the right hand side in the case of \( b_0(x) \).) To see why this works, we observe that the inner sum computes \( x_j \), and so the outer sum computes \( x \). Now \( x + (p - i) \equiv 0 \mod p \) precisely when \( x = i \).

Take \( g \) to be a generator of the multiplicative group \( \mathbb{F}_p^\times \) of \( \mathbb{F}_p \), and let \( \log_g(n) \) denote the discrete logarithm base \( g \) in \( \mathbb{F}_p \) (i.e., \( g^{\log_g(n)} = n \mod p \)). For each multiplication gate of \( C \) computing

\[
x = \prod_{j=1}^{k} x_j,
\]

we replace that gate with an AND gate placed in parallel with \( p - 1 \) AND \( \circ \) MOD\(_{p-1}\) circuits, implementing the conditions

\[
b_0(x) = \bigwedge_{j=1}^{k} b_0(x_j),
\]

and for \( i \neq 0 \),

\[
b_i(x) = G_i \land \bigwedge_{j=1}^{k} b_0(x_j).
\]

where \( G_i \) is a MOD\(_{p-1}\) gate such that

\[
G_i = 1 \iff (p - \log_g(i)) + \sum_{j=1}^{k} \sum_{l=2}^{p-1} b_r(x_j) \cdot \log_g(i') \equiv 0 \mod p - 1.
\]

To see why this works, we observe that the inner sum computes the discrete logarithm of \( x_j \) (for the same reason that the inner sum in the addition case computes \( x_j \)). Since \( x = \prod x_j \), we have (for non-zero \( x \)) \( \log_g x = \sum \log_g x_j \), so the outer sum computes the discrete logarithm of \( x \). Now \( (\log_g x) + (p - \log_g i) \equiv 0 \mod p - 1 \) precisely when \( x = i \).

Finally, we take the output wire of \( C' \) to be the negation of the \( b_0 \) wire from the output gate of \( C \). \( \square \)
We note that as a special case, an arithmetic circuit over \( \mathbb{F}_2 \) can be viewed directly as an \( \text{AC}^0[2] \) circuit (with the same size and depth), since an element of \( \mathbb{F}_2 \) is simply a bit, addition in \( \mathbb{F}_2 \) is \( \text{MOD}_2 \), and multiplication is AND. Additionally, when \( p-1 \) is not square-free, we can improve the modulus in the circuit above.

**Lemma 4.2.** Let \( p \) be prime, and let \( C \) be an arithmetic circuit over \( \mathbb{F}_p \) of size \( s \) and depth \( 2d \) (with alternating layers of + and \( \times \) gates) on \( n \) inputs, such that for every \( x \in \{0,1\}^n \), \( C(x) \in \{0,1\} \). Then \( C \) is equivalent to an \( \text{AC}^0[pm] \) circuit of size \( O(s^{p-1}p^{(p-1)\log(p-1)}) \) and depth \( 3d \), where \( m \) is the product of the distinct prime factors of \( p-1 \).

**Proof.** We start with the circuit \( C' \) given by Lemma 4.1. We now use Theorem 2.1 and the Chinese Remainder Theorem to simulate each MOD\(_{p-1} \) gate of fan-in \( f \) using an AND \( \circ \) MOD\(_{m} \circ \) AND, where the three layers of gates have fan-in at most \( \log(p-1) \), \( f^{p-1} \), and \( p-1 \), respectively. The bottom layer of AND gates have MOD\(_{p} \) gates as inputs, so can be replaced with a sum \( (\text{mod } m) \) of fan-in \( O(p^{f-1}) \) using Proposition 2.2. This can be absorbed into the layer of MOD\(_{m} \) gates. The top layer of AND gates can similarly be converted into a sum \( (\text{mod } p) \) of fan-in at most \( p^{\log(p-1)} \), which can be absorbed into the MOD\(_{p} \) gates for which they are inputs (since MOD\(_{p-1} \) gates in \( C' \) can only be inputs to MOD\(_{p} \) gates).

Putting these results together, we obtain the following:

**Theorem 4.2.** Let \( d \) be a multiple of 6, let \( n \) be a natural number, and let \( \alpha \in (0,1] \). Set

\[
s := \left\lceil \frac{3\alpha \log_2 n}{7} \right\rceil, \quad t := \left\lceil \frac{2\alpha \log_3 n}{7} \right\rceil, \quad u := \left\lceil \frac{2\alpha \log_7 n}{7} \right\rceil,
\]

and \( m := 2^s3^t7^u \). Then there is an \( \text{AC}^0[42] \) circuit of depth \( d+1 \) and size \( 2^{O(n^{6/7})} \) computing the MOD\(_m \) function on \( n \) inputs, where the output gate is an AND gate.

**Proof.** Applying Lemma 2.2, we construct:

- arithmetic circuits \( C_1, C_2, \ldots, C_{2^s} \) over \( \mathbb{F}_2 \) of depth \( d \), where \( C_i \) computes the \( i \)-th elementary symmetric polynomial modulo 2,
- arithmetic circuits \( D_1, D_3, \ldots, D_{2^t} \) over \( \mathbb{F}_3 \) of depth \( 2d/3 \), where \( D_i \) computes the \( i \)-th elementary symmetric polynomial modulo 3, and
- arithmetic circuits \( E_1, E_7, \ldots, E_{2^u} \) over \( \mathbb{F}_7 \) of depth \( 2d/3 \), where \( E_i \) computes the \( i \)-th elementary symmetric polynomial modulo 7,

all of which have size \( n^{O(n^{6/7d})} \) given our parameters.

We convert each of the \( D_i \) and \( E_i \) into \( \text{AC}^0[42] \) circuits \( D'_i \) and \( E'_i \) using Lemma 4.1, and as previously observed, the \( C_i \) are already \( \text{AC}^0[2] \) circuits.

Finally, from Lemma 2.1 and the Chinese Remainder Theorem, all of the \( C_i(x), D'_i(x), \) and \( E'_i(x) \) output 1 if and only if \( |x|_1 \equiv 0 \) mod \( m \). Our final circuit for MOD\(_m \) is obtained by taking the AND of all of these circuits.

We are now ready to prove Theorem 4.1.

**Proof.** Let \( d \equiv 2 \) mod 6, let \( f \) be a symmetric function on \( n \) inputs, and let \( g \) be its companion function; that is, for every \( x, f(x) = g(|x|_1) \). We begin with the same opening move as Oliveira, Santhanam, and Srinivasan [OSS19], observing that

\[
f(x) = \bigvee_{i \in g^{-1}(1)} \bigwedge_{j \neq i} D_{i,j},
\]

where \( D_{i,j}(x) = 1 \) if \( |x|_1 = i \) and \( D_{i,j}(x) = 0 \) if \( |x|_1 = j \) (and has otherwise arbitrary behavior). Thus it suffices to construct circuits \( C_{i,j} \) computing functions consistent with \( D_{i,j} \).

When \( |i - j| \geq n^{7/13} \), Lemma 2.3 gives an \( \text{AC}^0 \) circuit \( C_{i,j} \) of depth \( d-1 \) and size \( \exp(O(n^{6/(13(d-2)})\) computing \( D_{i,j} \).
When \(|i - j| \leq n^7/13\), we observe that a circuit for \(\text{MOD}_m\) suffices, with \(m > n^7/13\). We take \(\alpha = 7/13\) in Theorem 4.2. Then we have a circuit \(C_{i,j}^\alpha\) of depth \(d - 1\) and size \(\exp(\tilde{O}(n^{6/(13(d-2))}))\) computing the \(\text{MOD}_m\) function on \(2n\) inputs, where \(m > n^7/13\). We now take \(C_{i,j}(x) = C_{i,j}^\alpha(x1^{m-i}(0^{r-m+i})\). Finally, we set

\[ C = \bigvee_{i \in \mathbb{Z}^N} \bigwedge_{j \neq i} C_{i,j}. \]

We can collapse the output AND gates of all of the \(C_{i,j}\) into the second layer AND gates, so \(C\) has depth \(d\) and size \(\exp(\tilde{O}(n^{6/(13(d-2))}))\), as desired. \(\square\)

More generally, for certain \(m\) which are the product of \(r\) primes, we can improve the results of Theorem 4.1. Recall from the introduction that we defined a product \(m\) of primes \(q_1, \ldots, q_r\) to be good if every prime factor of \(\phi(m)\) divides \(m\), and we noted that the primorial \(m = p_r\#\), the product of the first \(r\) primes, is good.

**Reminder of Theorem 1.4.** Let \(m\) be a good product of \(r\) primes. For every symmetric function \(f\) on \(n\) inputs and every depth \(d \geq 4\) congruent to 1 modulo 3, there exists an \(\text{AC}^0[m]\) circuit of depth \(d\) and size \(\exp(\tilde{O}(n^{3/(r+3)(d-1)-3}))\) computing \(f\).

**Proof.** Let

\[ m = \prod_{a=1}^{r} p_a \]

be a good product of \(r\) primes. For each \(a \in [r]\), let \(s_a = \lfloor \alpha \log_{p_a} n \rfloor\) for some \(\alpha\) to be defined later. By Lemma 2.2, there are arithmetic circuits \(C_{a,b}\) over \(\mathbb{F}_{p_a}\) of depth \((2/3)(d - 1)\) and size \(n^{O(n^{\theta/\phi(m)})}\) computing the \(p_a\)-th elementary symmetric polynomial in \(2n\) inputs over \(\mathbb{F}_{p_a}\). By Lemma 4.2, we can convert these into \(\text{AC}^0[m]\) circuits \(C_{a,b}^\prime\) of depth \(d - 1\) and size \(2^{O(n^{m/(d-1)})}\). When \(|i - j| \leq n^{\alpha r}, i \not\equiv j \mod p_a\) for at least one \(a\) by the Chinese Remainder Theorem, so we can construct a circuit \(E_{i,j}\) computing \(D_{i,j}\) by taking

\[ E_{i,j}(x) = -C_{a,b}^\prime(x, 0^{s_a_i - j}1^{n + j - p_a^r}) \]

for some pair \((a, b)\). When \(|i - j| \geq n^{\alpha r}\), we use Lemma 2.3 to get a circuit \(E_{i,j}\) of depth \(d - 1\) and size \(\exp(\tilde{O}(n^{(1-\alpha r)/(d-2)}))\) computing \(D_{i,j}\). All of the \(E_{i,j}\) have AND gates as output gates, so we take \(\alpha = \frac{d-1}{(r+3)(d-1)-3}\) to balance the sizes of the two circuit constructions and complete the proof as per Theorem 4.1. \(\square\)

It is worth noting that when \(2 \mid m\), we can improve this construction slightly. When \(2 \mid m\) (and \(6 \mid d - 1\)), the \((r+3)(d-1)-3\) in the denominator of the double exponent instead becomes \((r+2)(d-1)-3\).

**5 Conclusion**

We believe our work demonstrates that \(\text{CC}^0\) circuits are not as weak as conventional wisdom anticipates, even at depth three. We hope that researchers seriously consider (possibly refuting) the SYM \(\circ\) AND hypothesis, as it stands in the way of obtaining significantly smaller \(\text{CC}^0\) and \(\text{ACC}^0\) circuits for symmetric functions.

A natural next step would be to explore how much further our constructions can be pushed beyond symmetric functions. Our Theorem 1.5 already demonstrates that \(\text{TC}^0\) circuits with linearly many gates and linear fan-in can be non-trivially simulated with \(\text{CC}^0\) circuits in subexponential size. Another question is whether \(\text{NC}^1\) circuits or Boolean formulas can be simulated similarly. For another example, it is well-known that time \(r\) and space \(s\) computations can be simulated with depth-three \(\text{AC}^0\) circuits of size \(2^{O(\sqrt{rs})}\); this follows from efficient simulations in the polynomial hierarchy of space-bounded computation [Nep70]. Could the size of this construction be improved, using \(\text{MOD}_m\) gates? If such an improved circuit could be constructed in a uniform way, it would likely imply new time-space lower bounds for decision problems in \(\text{PP}\) or the counting hierarchy [AKR01]. However, even a non-uniform construction would be very interesting.
Acknowledgements. We thank Arkadev Chattopadhyay and Kristoffer Arnsfelt Hansen for useful pointers and discussion.

References

[AAD00] Manindra Agrawal, Eric Allender, and Samir Datta. On $\text{TC}^0$, $\text{AC}^0$, and arithmetic circuits. J. Comput. Syst. Sci., 60(2):395–421, 2000.

[AB09] Sanjeev Arora and Boaz Barak. Computational Complexity - A Modern Approach. Cambridge University Press, 2009.

[AG94] Eric Allender and Vivek Gore. A uniform circuit lower bound for the permanent. SIAM J. Comput., 23(5):1026–1049, 1994.

[AK10] Eric Allender and Michal Koucký. Amplifying lower bounds by means of self-reducibility. JACM, 57(3), 2010.

[AKR+01] Eric Allender, Michal Koucký, Detlef Ronneburger, Sambuddha Roy, and V. Vinay. Time-space trade-offs in the counting hierarchy. In Proceedings of the 16th Annual IEEE Conference on Computational Complexity, Chicago, Illinois, USA, June 18-21, 2001, pages 295–302. IEEE Computer Society, 2001.

[Ama09] Kazuyuki Amano. Bounds on the size of small depth circuits for approximating majority. In Automata, Languages and Programming, 36th International Colloquium, ICALP 2009, Rhodes, Greece, July 5-12, 2009, Proceedings, Part I, volume 5555 of Lecture Notes in Computer Science, pages 59–70. Springer, 2009.

[Bar86] David A. Mix Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in $\text{NC}^1$. J. Comput. Syst. Sci., 38(1):150–164, 1989. See also STOC’86.

[BBL92] Paul Beame, Erik Brisson, and Richard E. Ladner. The complexity of computing symmetric functions using threshold circuits. Theor. Comput. Sci., 100(1):253–265, 1992.

[BBR94] David A. Mix Barrington, Richard Beigel, and Steven Rudich. Representing Boolean functions as polynomials modulo composite numbers. Comput. Complexity, 4:367–382, 1994.

[BGL06] Nayantara Bhatnagar, Parikshit Gopalan, and Richard J. Lipton. Symmetric polynomials over $\mathbb{Z}_m$ and simultaneous communication protocols. J. Comput. Syst. Sci., 72(2):252–285, 2006.

[BIS90] David Barrington, Neil Immerman, and Howard Straubing. On uniformity within $\text{NC}^1$. Journal of Computer and System Sciences, 41, 1990.

[BST90] David A. Mix Barrington, Howard Straubing, and Denis Thérien. Non-uniform automata over groups. Inf. Comput., 89(2):109–132, 1990.

[BT94] Richard Beigel and Jun Tarui. On ACC. Computational Complexity, pages 350–366, 1994.

[BT87] David A. Mix Barrington and Denis Thérien. Finite monoids and the fine structure of $\text{NC}^1$. J. ACM, 35(4):941–952, 1988. See also STOC’87.

[CGPT06] Arkadev Chattopadhyay, Navin Goyal, Pavel Pudlák, and Denis Thérien. Lower bounds for circuits with $\text{MOD}_m$ gates. In 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2006), 21-24 October 2006, Berkeley, California, USA, Proceedings, pages 709–718. IEEE Computer Society, 2006.

[CLW20] Lijie Chen, Xin Lyu, and R. Ryan Williams. Almost-everywhere circuit lower bounds from non-trivial derandomization. In 61st IEEE Annual Symposium on Foundations of Computer Science, FOCS 2020, Durham, NC, USA, November 16-19, 2020, pages 1–12. IEEE, 2020.
[COST16] Xi Chen, Igor Carboni Oliveira, Rocco A. Servedio, and Li-Yang Tan. Near-optimal small-depth lower bounds for small distance connectivity. In Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016, pages 612–625. ACM, 2016.

[CP19] Shiteng Chen and Periklis A. Papakonstantinou. Depth reduction for composites. SIAM J. Comput., 48(2):668–686, 2019.

[CW09] Arkadev Chattopadhyay and Avi Wigderson. Linear systems over composite moduli. In 50th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2009, pages 43–52. IEEE Computer Society, 2009.

[Gop06] Parikshit Gopalan. Computing with polynomials over composites. PhD thesis, Georgia Institute of Technology, 2006.

[GT00] Vince Grolmusz and Gábor Tardos. Lower bounds for (MODp-MODm) circuits. SIAM J. Comput., 29(4):1209–1222, 2000.

[Han06] Kristoffer Arnsfelt Hansen. On modular counting with polynomials. In 21st Annual IEEE Conference on Computational Complexity (CCC 2006), pages 202–212. IEEE Computer Society, 2006.

[Hås86] Johan Håstad. Almost optimal lower bounds for small depth circuits. In STOC, pages 6–20, 1986.

[HK10] Kristoffer Arnsfelt Hansen and Michal Koucký. A new characterization of ACC0 and probabilistic CC0. Comput. Complex., 19(2):211–234, 2010.

[HP10] Kristoffer Arnsfelt Hansen and Vladimir V Podolskii. Exact threshold circuits. In CCC, pages 270–279, 2010.

[IKK21] Paweł M Idziak, Piotr Kawalek, and Jacek Krzaczkowski. Complexity of modular circuits. arXiv preprint arXiv:2106.02947, 2021.

[Juk12] Stasys Jukna. Boolean Function Complexity: Advances and Frontiers. Springer-Verlag, 2012.

[Luc78] Edouard Lucas. Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques suivant un module premier. Bulletin de la Société Mathématique de France, 6:49–54, 1878.

[MW20] Cody D. Murray and R. Ryan Williams. Circuit lower bounds for nondeterministic quasi-polynomial time from a new easy witness lemma. SIAM J. Comput., 49(5), 2020.

[Nep70] V. Nepomnjasscii. Rudimentary predicates and Turing calculations. Soviet Mathematics - Doklady, 11(6):1462–1465, 1970.

[OSS19] Igor Carboni Oliveira, Rahul Santhanam, and Srikanth Srinivasan. Parity helps to compute majority. In 34th Computational Complexity Conference, CCC 2019, July 18-20, 2019, New Brunswick, NJ, USA, volume 137 of LIPIcs, pages 23:1–23:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

[OW07] Ryan O’Donnell and Karl Wimmer. Approximation by DNF: examples and counterexamples. In Automata, Languages and Programming, 34th International Colloquium, ICALP 2007, Wroclaw, Poland, July 9-13, 2007, Proceedings, volume 4596 of Lecture Notes in Computer Science, pages 195–206. Springer, 2007.

[Raz87] Alexander A. Razborov. Lower bounds on the size of bounded-depth networks over the complete basis with logical addition. Mathematical Notes of the Academy of Sciences of the USSR, 41(4):333–338, 1987.

[Smo87] Roman Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In STOC, pages 77–82, 1987.

[ST06] Howard Straubing and Denis Thérien. A note on MODp - MODm circuits. Theory Comput. Syst., 39(5):699–706, 2006.
A Proof of Theorem 1.5

Let us recall the SYM \circ AND Hypothesis and its consequence stated in the introduction.

**Reminder of Hypothesis 1.** There are constants \(c, k > 1\) such that for sufficiently large \(n\), there is a function \(f : \{0, 1\}^n \rightarrow \{0, 1\}\) computable by \(TC^0_c\) circuits of depth \(c\) with at most \(\tilde{O}(n)\) gates where each gate has fan-in \(\tilde{O}(n)\), such that \(f\) does not have an \(exp(\tilde{O}(n^{1/k}))\) size SYM \circ AND circuit.

**Reminder of Theorem 1.5.** Assuming the SYM \circ AND Hypothesis (Hypothesis 1), there is a fixed \(\alpha > 0\) such that for every \(m\) and \(d\), every depth-\(d\) \(ACC^0[m]\) circuit computing the MAJORITY function on \(n\) inputs requires size at least \(exp(n^{\frac{\alpha}{r}})\) for sufficiently large \(n\), where \(r\) is the number of distinct prime factors of \(m\).

We prove the contrapositive. We start with the negation of the theorem’s conclusion:

Suppose for every \(\alpha > 0\), there is some modulus \(m\) which is a product of \(r\) primes, along with some depth \(d\), such that MAJORITY can be computed by a depth-\(d\) \(ACC^0[m]\) circuit of size \(exp(O(n^{\frac{\alpha}{r}}))\).

Assuming the above, we will refute the SYM \circ AND Hypothesis: we will show for all \(c, k > 1\) and every function \(f\) computable by the appropriate depth-\(c\) \(TC^0_c\) circuits, \(f\) has an \(exp(O(n^{1/k}))\) size SYM \circ AND circuit.

Let \(c, k > 1\) be arbitrary. Let \(C\) be a \(TC^0_c\) circuit \(C\) with depth \(c\) and \(\tilde{O}(n)\) gates each of fan-in at most \(\tilde{O}(n)\). Suppose we substitute each MAJORITY gate of \(C\) with a copy of the assumed \(ACC^0[m]\) circuit. We obtain a \(ACC^0[m]\) circuit \(C'\) of depth at most \(c \cdot d\) and of size \(exp(\tilde{O}(n^{\frac{\alpha}{r}}))\) such that \(C'\) is equivalent to \(C\).

Chen and Papakonstantinou [CP19] prove that for every depth-\(d'\) size-\(s\) circuit \(D\) over AND, OR, and MOD\(_m\) gates, where \(m\) is the product of \(r\) distinct primes, \(D\) is equivalent to a SYM \circ AND circuit \(D'\) of size at most

\[
S'(s, m, r, d') = 2^{(m \log s)^{10\alpha d'}}.
\]

Applying their reduction to our \(C'\), we obtain a SYM \circ AND circuit \(C''\) of size \(exp(\tilde{O}(n^{10\alpha c}))\) that is equivalent to our original circuit \(C\). For all \(\alpha < 1/(10ck)\), we obtain a SYM \circ AND circuit equivalent to \(C\) with size \(exp(O(n^{1/k}))\).