Depth Reduction for Circuits with a Single Layer of Modular Counting Gates

Kristoffer Arnsfelt Hansen

Department of Computer Science
Aarhus University[*]

arnsfelt@cs.au.dk

Abstract

We consider the class of constant depth AND/OR circuits augmented with a layer of modular counting gates at the bottom layer, i.e $\mathbf{AC^0} \circ \mathbf{MOD}_m$ circuits. We show that the following holds for several types of gates $\mathcal{G}$: by adding a gate of type $\mathcal{G}$ at the output, it is possible to obtain an equivalent probabilistic depth 2 circuit of quasipolynomial size consisting of a gate of type $\mathcal{G}$ at the output and a layer of modular counting gates, i.e $\mathcal{G} \circ \mathbf{MOD}_m$ circuits. The types of gates $\mathcal{G}$ we consider are modular counting gates and threshold-style gates. For all of these, strong lower bounds are known for (deterministic) $\mathcal{G} \circ \mathbf{MOD}_m$ circuits.

1 Introduction

A long standing problem in Boolean circuit complexity is to understand the computational power of constant depth AND/OR circuits augmented with modular counting (MOD_m) gates, i.e $\mathbf{ACC^0}$ circuits. One approach would be to consider restrictions on the occurrences of the MOD_m gates. Restricting circuit to contain MOD_m gates only at the layer below the output or to only contain *few* MOD_m gates have successfully resulted in lower bounds [9, 12, 21]. We believe that proving lower bounds for $\mathbf{ACC^0}$ circuits containing MOD_m only in a single layer would be an important next step towards understanding $\mathbf{ACC^0}$ circuits. The restriction we will study in this work is even stricter: we require that all MOD_m gates occur at the bottom layer. This still gives a class of circuits for which no strong lower bounds are known. In fact, no good lower bounds are known for depth 3 $\mathbf{ACC^0}$ circuits and this is true even when the MOD_m gates can occur only at the bottom layer.

More precisely, while strong lower bounds *are* known for $\mathbf{AND} \circ \mathbf{OR} \circ \mathbf{MOD}_m$ circuits, no strong lower bounds are known for $\mathbf{OR} \circ \mathbf{AND} \circ \mathbf{MOD}_m$ circuits. We remark that for these statements the precise definition of MOD_m gates is crucial[1]. Grolmusz proved that $\mathbf{MAJ} \circ \mathbf{OR} \circ \mathbf{MOD}_m$ circuits require size $2^{\Omega(n)}$ to compute the *inner product modulo 2* function IP_2. For the same class of circuits, Beigel and Maciel [4] proved that MOD_q requires size $2^{\Omega(n)}$, when $q \nmid m$, and that IP_p

---

[1]Two definitions are commonly used in the literature, one being the complement of the other. This also means that the lower bounds we review below are stated differently than their original statement.

requires size $2^{\Omega(\sqrt{n})}$. They also manage to show that $\mathbf{MAJ} \circ \mathbf{AND} \circ \mathbf{MOD}_{p^k}$ circuits require size $2^{\Omega(n)}$ to compute the MOD_q function, but only when p is a prime not dividing q. Also, Jukna uses *graph complexity* [14] to derive lower bounds for $\mathbf{AND} \circ \mathbf{OR} \circ \mathbf{MOD}_2$ circuits; this lower bound is easily extended to $\mathbf{AND} \circ \mathbf{OR} \circ \mathbf{MOD}_m$ circuits.

One of the strongest lower bounds obtained in Boolean circuit complexity is the lower bound for $\mathbf{AC^0}[p^k]$ circuits by Razborov [16] and Smolensky [17]. This result is proved in two steps. First a *depth reduction* is invoked, resulting in *probabilistic* $\mathbf{MOD}_p \circ \mathbf{AND}_{\log^{O(1)} n}$ circuits. Then a lower bound for these are derived from counting arguments. Depth reduction results for the entire class $\mathbf{ACC^0}$ obtained by Yao [22] and Beigel and Tarui [6] gave hope that a similar two step approach could be used to obtain lower bounds for $\mathbf{ACC^0}$. Indeed by results of Håstad and Goldmann [13] it is then sufficient to obtain strong lower bounds for multiparty communication complexity for $\log^{O(1)} n$ players in the "number on the forehead" model, but such a result currently seems out of reach.

We believe that it should be explored if a two step approach using depth reduction can be employed for subclasses of $\mathbf{ACC^0}$. Indeed, the depth reduction by Beigel and Tarui results in a class that is arguably too powerful. They show that any $\mathbf{ACC^0}$ circuit is simulated by a *deterministic* $\mathbf{SYM} \circ \mathbf{AND}_{\log^{O(1)}}$ circuit. Beigel, Tarui and Toda proved that this latter class of circuits can even simulate *probabilistic* $\mathbf{EMAJ} \circ \mathbf{ACC^0}$ circuits [7].

In this paper we derive a number of depth reduction results for $\mathbf{AC^0} \circ \mathbf{MOD}_m$ circuits. Let $\mathcal{G}$ denote a class of modular counting gates (modulo a prime p), exact threshold gates, majority gates or threshold gates, i.e MOD_p, ETHR, MAJ or THR gates. Then by adding a gate of type $\mathcal{G}$ at the output of the $\mathbf{AC^0} \circ \mathbf{MOD}_m$ circuit allows one to obtain a depth reduction to probabilistic $\mathcal{G} \circ \mathbf{MOD}_m$ circuits.

For each of these classes strong lower bounds are known for *deterministic* circuits. For $\mathbf{MOD}_p \circ \mathbf{MOD}_m$ circuits lower bounds was obtained by Barrington, Straubing and Thérien [3] (See also [2, 18, 11, 15]). Lower bounds for $\mathbf{MAJ} \circ \mathbf{MOD}_m$ circuits was obtained by Goldmann [10] and finally lower bounds for $\mathbf{THR} \circ \mathbf{MOD}_m$ circuits was obtained by Krause and Pudlák [15].

Our depth reduction reduction proof will use two ingredients. First, as previous results of this kind we will use constructions of probabilistic polynomials. Secondly we will use representations of Boolean function as Fourier sums. We will present these in Section 2 and Section 3, respectively. Finally in Section 4 we combine these to obtain our main results. In the remainder of this section we briefly review the necessary circuit definitions.

1.1 Constant Depth Circuits

We consider circuits built from families of unbounded fanin gates. Inputs are allowed to be Boolean variables and their negations as well as the constants 0 and 1. In addition to AND, OR and NOT we consider MOD_m gates and threshold style gates. Let $x_1, \ldots, x_n$ be n Boolean inputs. For a positive integer m, let MOD_m be the function that outputs 1 if and only if $\sum_{i=1}^n x_i \not\equiv 0 \pmod{m}$. The majority function, MAJ, is 1 if and only if $\sum_{i=1}^n x_i \geq \frac{n}{2}$. Similarly, the exact majority function, EMAJ, is 1 if and only if $\sum_{i=1}^n x_i = \frac{n}{2}$. Let $w \in \mathbf{R}^n$ and let t be any real number. The threshold function with weights w and threshold t, $\mathrm{THR}_{w,t}$ is 1 if and only if $\sum_{i=1}^n w_i x_i \geq t$. Similarly, the exact threshold function with weights w and threshold t, $\mathrm{ETHR}_{w,t}$ is 1 if and only if $\sum_{i=1}^n w_i x_i = t$.

Let $\mathbf{AND}$ and $\mathbf{OR}$ denote the families of unbounded fanin AND and OR gates. Let $\mathbf{MOD}_m$, $\mathbf{EMAJ}$, $\mathbf{MAJ}$, $\mathbf{ETHR}$, $\mathbf{THR}$ denote the families of MOD_m, EMAJ, MAJ, $\mathrm{ETHR}_{w,t}$ and $\mathrm{THR}_{w,t}$

gates, for arbitrary w and t. If $\mathcal{G}$ is a family of boolean gates and $\mathcal{C}$ is a family of circuits we let $\mathcal{G} \circ \mathcal{C}$ denote the class of circuits consisting of a $\mathcal{G}$ gate taking circuits from $\mathcal{C}$ as inputs.

$\mathbf{AC^0}$ is the class of functions computed by constant depth circuits built from AND, OR and NOT gates. $\mathbf{AC^0}[m]$ is the class of functions computed by constant depth circuits built from AND, OR and MOD_m gates. $\mathbf{ACC^0}$ is the union of the classes $\mathbf{AC^0}[m]$.

2 Probabilistic Polynomials

Razborov [16] and Smolensky [17] (cf. [1]) gave a simple construction of probabilistic polynomials over $\mathbf{Z}_p$ computing the OR function.

Theorem 1 (Razborov, Smolensky) *For any prime p and any $\epsilon > 0$ there is a family of polynomials over $\mathbf{Z}_p$ of degree $O(\log(\frac{1}{\epsilon}))$ that probabilistically compute the OR function with one-sided positive error at most ϵ.*

This also gives a family of low degree polynomials that probabilistically compute the AND function with small one-sided negative error.

Fermat's little theorem gives a polynomial over $\mathbf{Z}_p$ of constant degree $p - 1$, computing the MOD_p function and the following extension gives the same for the MOD_{p^k} function (see e.g [6] for a proof).

Lemma 2 *Let $q = p^k$ for a prime p. Then the MOD_q function is computed by polynomial over $\mathbf{Z}_p$ of degree $q - 1$.*

Combining Theorem 1 and Lemma 2 and composing polynomials then gives the following.

Theorem 3 (Razborov, Smolensky) *Let $q = p^k$ for a prime p. Let C be a depth d $\mathbf{AC^0}[q]$ circuit of size S and let $\epsilon > 0$. Then there is a family of probabilistic polynomials of degree $O(\log(\frac{S}{\epsilon})^d)$ that compute the output of C with error at most ϵ.*

Based on a theorem by Valiant and Vazirani [20], Beigel et al. [5] and Tarui [19] gave probabilistic polynomials over the integers computing the OR function, thereby generalizing Theorem 1, albeit at the expense of a slightly larger degree. As with Theorem 1 it also gives probabilistic polynomials computing the AND function.

Theorem 4 (Beigel et al., Tarui) *For any $\epsilon > 0$ there is a family of polynomials over $\mathbf{Z}$ of degree $O(\log(\frac{1}{\epsilon}) \log n)$ and having coefficients of absolute value $2^{O(\log(\frac{1}{\epsilon}) \log(n))}$ that probabilistically compute the OR function with one-sided positive error at most ϵ.*

Let $P(x)$ denote a polynomial from this family. Tarui[2] considered the family of polynomials given by $Q(x) = 1 - (x_1 + \cdots + x_n + 1)(P(x) - 1)^2$ he obtained a family of polynomials computing the OR function with zero-sided error. With these polynomials Tarui obtained probabilistic polynomials computing the output of $\mathbf{AC^0}$ circuits with zero-sided error as well. Beigel et al. subsequently gave a simpler construction for obtaining this, that we will review next.

---

[2]Tarui actually stated his results in terms of the NOR function making the polynomials slightly different.

Theorem 5 (Tarui) *Let C be a depth d $\mathbf{AC^0}$ circuit of size S and let $\epsilon > 0$. Then there is a family of polynomials over $\mathbf{Z}$ of degree $O((\log(\frac{S}{\epsilon}) \log(S))^d)$ and having coefficients of absolute value $2^{O((\log(\frac{S}{\epsilon}) \log(S))^d)}$ that compute the output of C with zero-sided error at most ϵ.*

Proof (Beigel et al.) By composing the polynomials given by Theorem 4 we get a family of polynomials of degree $O((\log(\frac{S}{\epsilon}) \log(S))^d)$ and having coefficients of absolute value at most $2^{O((\log(\frac{S}{\epsilon}) \log(S))^d)}$ that probabilistically compute the output of C with error at most ϵ. Let F denote a member of this family. Let g be any gate of C taking inputs $g_1, \ldots, g_m$. Let P_g denote a member of the family of polynomials computing g in variables $y_1, \ldots, y_m$. If g is an OR gate define E_g by $E_g(y) = (y_1 + \cdots + y_m)(P(y) - 1)$. We then have that $E_g(y) = 0$ if and only if $P_g(y) = \mathrm{OR}(y)$. When g is an AND gate then similarly we define $E_g(y) = (y_1 + \cdots + y_n - n)P(y)$ and we have that $E_g(y) = 0$ if and only if $P_g(y) = \mathrm{AND}(y)$.

Now, define $E(x) = \sum_{g \in C}(E_g(x))^2$. Then $E(x) = 0$ whenever all gates in C are computed correctly. Then finally we have that the family of polynomials given

$$G(x) = F(x) - ((F(x))^2 + 1)E(x)$$

compute the output of C with zero-sided error at most ϵ.

Clearly these polynomials are of degree $O((\log(\frac{S}{\epsilon}) \log(S))^d)$ and have coefficients of absolute value $2^{O((\log(\frac{S}{\epsilon}) \log(S))^d)}$ as well. $\qquad\square$

3   Fourier Sum Representation

In this section we will derive representations of circuits of the form $\mathcal{G} \circ \mathbf{AND}_d \circ \mathbf{MOD}_m$ for several choices of a family of Boolean gates $\mathcal{G}$ by Fourier sums over a field with an mth root of unity. Conversely we will derive $\mathcal{G} \circ \mathbf{MOD}_m$ circuits computing the Boolean functions represented by such representations. Combining these two types of results then implies that the layer of $\mathbf{AND}_d$ gates can be eliminated.

When $\mathcal{G}$ is a family of modular counting gates the appropriate setting will be Fourier sums over a finite field. When $\mathcal{G}$ is a family of threshold style gates the appropriate setting will instead be Fourier sums over complex number fields.

3.1   Modular counting gates

Representations of $\mathbf{MOD}_p \circ \mathbf{AND}_d \circ \mathbf{MOD}_m$ circuits by Fourier sums over a finite field was introduced in the work of Barrington, Straubing and Thérien [3] and is made entirely explicit by Barrington and Straubing [2] and further results were obtained by Straubing and Thérien [18]. All these works actually consider depth $d + 1$ $(\mathbf{MOD}_{p^k})^d \circ \mathbf{MOD}_m$ circuits, which are converted into $\mathbf{MOD}_p \circ \mathbf{AND}_{O(d)} \circ \mathbf{MOD}_m$ circuits as the first step in constructing the representation. We will next review these results.

Let m be a positive integer and let p be a prime that does not divide m. Choose k such that m divides $p^k - 1$. Then the finite field $F = \mathrm{GF}(p^k)$ contains an m'th root of unity ω. We will consider expressions in variables $x_1, \ldots, x_n$ of the form

$$\sum_{i=1}^{S} c_i \omega^{a_{i,1}x_1 + \ldots a_{i,n}x_n} .$$

where c_i are elements of F and $a_{i,j}$ are elements of $\mathbf{Z}_m$. We will call that a Fourier sum over F of size S. We say such an expression $E(x)$ computes a Boolean function f if $E(x) = f(x)$ for all $x \in \{0,1\}^n$ and we say $E(x)$ represents a Boolean function f if $E(x) \in \mathbf{Z}_p$ for all x and moreover $E(x) = 0$ if and only if $f(x) = 0$ for all $x \in \{0,1\}^n$.

When $x_1, \ldots, x_n$ are variables from $\mathbf{Z}_m$ then these expressions can in fact be viewed as Fourier transforms of functions $f : (\mathbf{Z}_m)^n \to F$, thereby justifying our terminology. For details about this we refer to the works of Barrington et al. [3, 2, 18]. We have the following.

Lemma 6 *A* MOD_m *gate can be computed by a Fourier sum of size* $2^{|F|-1}$.

Proof A MOD_m gate with inputs $x_1, \ldots, x_n$ can be computed by the expression

$$(\omega^{x_1 + \cdots + x_n} - 1)^{|F|-1}$$

since

$$(\omega^a - 1)^{|F|-1} = \begin{cases} 0 & \text{if} \quad a \equiv 0 \pmod{m} \\ 1 & \text{if} \quad a \not\equiv 0 \pmod{m} \end{cases}$$

thereby giving a Fourier sum of size $2^{|F|-1}$. $\qquad\square$

Then taking sums of these expressions shows that a $\mathbf{MOD}_p \circ \mathbf{MOD}_m$ circuit of size S can be computed by a Fourier sum of size at most $S2^{(|F|-1)(p-1)}$. But at the expense of increasing the size of the circuit we can even introduce small fanin AND gates as a middle layer.

Proposition 7 (Barrington et al.) *Let p be a prime not dividing m. For any* $\mathbf{MOD}_p \circ \mathbf{AND}_d \circ \mathbf{MOD}_m$ *circuit of size S there is a Fourier sum representing the output of the circuit of size at most $S2^{d(|F|-1)}$.*

Proof We interpret the top two layers of the circuit as a polynomial over $\mathbf{Z}_p$ in S variables with at most S terms and of degree d. Express each MOD_m gate of the circuit as a Fourier sum of size $2^{|F|-1}$. Substituting these for the variables in the polynomial and expanding then yields the required Fourier sum representing the output of the circuit of size at most $S2^{d(|F|-1)}$. $\qquad\square$

Proposition 8 (Straubing and Thérien) *Suppose a Boolean function f can be represented by a Fourier sum of size S. Then f is computed by a* $\mathbf{MOD}_p \circ \mathbf{MOD}_m$ *circuit of size $m(p-1)S$.*

Proof The field F is a vector space over $\mathbf{Z}_p$. We can thus pick a basis $v_1, \ldots, v_k$ of F where we can choose $v_1 = 1$. Let $\pi_1 : F \to \mathbf{Z}_p$ be the projection of an element of F onto the first coordinate in the basis $v_1, \ldots, v_k$. By linearity we have

$$\pi_1 \left(\sum_{i=1}^{S} \omega^{a_{i,1}x_1 + \ldots a_{i,n}x_n} \right) \equiv \sum_{i=1}^{S} \pi_1(\omega^{a_{i,1}x_1 + \ldots a_{i,n}x_n}) \pmod{p} \ .$$

Thus to compute the sum we can compute each term $\pi_1(\omega^{a_{i,1}x_1 + \ldots a_{i,n}x_n})$ individually. For every $0 < a < m$ we will have $(a(p-1) \mod p)$ copies of a MOD_m gate that evaluate to 1 if $a_{i,1}x_1 + \cdots + a_{i,n}x_n \not\equiv a \pmod{m}$. Furthermore we feed a copies of the constant 1. The sum of these will be $a \mod p$ when the term has value a and will be 0 otherwise. Thus taking the sum for every a gives $m(p-1)$ MOD_m gates that compute the given term. $\qquad\square$

Combining Proposition 7 and Proposition 8 we obtain the following somewhat surprising result, showing that a middle layer of small fanin AND gates can be absorbed at the cost of a reasonable increase of the size of the circuit.

Theorem 9 (Straubing and Thérien) *Let p be a prime not dividing m. Then any function computed by a $\mathrm{MOD}_p \circ \mathrm{AND}_d \circ \mathrm{MOD}_m$ circuit of size S is also computed by a $\mathrm{MOD}_p \circ \mathrm{MOD}_m$ circuit of size $S2^{O(d)}$.*

3.2   Threshold style gates

It was suggested by Barrington and Straubing [2] to use Fourier representations over the complex numbers to study $\mathbf{THR} \circ \mathbf{MOD}_m$ circuits. The case of $m = 2$ is known as polynomial threshold functions [8] and these circuits are precisely representations by the sign of a Fourier sum. We will derive representations for $\mathcal{G} \circ \mathbf{AND}_d \circ \mathbf{MOD}_m$ circuits when $\mathcal{G}$ is a family of threshold, exact threshold or majority gates.

Let m be a positive integer and let $\omega = e^{\frac{2\pi i}{m}}$ be an m'th root of unity. Similarly to the previous section we consider expressions in variables $x_1, \ldots, x_n$ of the form

$$\sum_{i=1}^{S} c_i \omega^{a_{i,1}x_1 + \ldots a_{i,n}x_n} \quad ,$$

where c_i complex numbers and $a_{i,j}$ are elements of $\mathbf{Z}_m$. We will call that a Fourier sum over $\mathbf{C}$ of size S and we will call the numbers c_i the coefficients. We say such an expression $E(x)$ computes a Boolean f if $E(x) = f(x)$ for all $x \in \{0,1\}^n$. We say that $E(x)$ sign represents a Boolean function f if $E(x) \in \mathbf{R} \setminus \{0\}$ for all $x \in \{0,1\}^n$ and moreover $E(x) > 0$ if and only if $f(x) = 1$ for all $x \in \{0,1\}^n$. Finally we say that $E(x)$ equality represents a Boolean function f if $E(x) \in \mathbf{R}$ for all $x \in \{0,1\}^n$ and moreover $E(x) = 0$ if and only $f(x) = 1$ for all $x \in \{0,1\}^n$.

As the previous case of finite fields, when $x_1, \ldots, x_n$ are variables from $\mathbf{Z}_m$ then these expressions can be viewed as Fourier transforms of functions $f : (\mathbf{Z}_m)^n \to \mathbf{C}$.

Lemma 10 *A MOD_m gate can be computed by a Fourier sum of size $m + 1$ where the coefficients are either 1 or $\frac{1}{m}$.*

Proof A MOD_m gate with inputs $x_1, \ldots, x_n$ can be computed by the expression

$$1 - \frac{1}{m} \sum_{b=0}^{m-1} \omega^{b(x_1 + \cdots + x_n)}$$

since

$$\sum_{b=0}^{m-1} \omega^{ba} = \begin{cases} m & \text{if} \quad a \equiv 0 \pmod{m} \\ 0 & \text{if} \quad a \not\equiv 0 \pmod{m} \end{cases} .$$

thereby giving a Fourier sum of size $m + 1$. $\qquad\square$

With this we can now derive Fourier sum representations of different classes of circuits. First we consider circuits with a threshold gate at the output.

Proposition 11 *For any* $\mathbf{THR} \circ \mathbf{AND}_d \circ \mathbf{MOD}_m$ *circuit of size S there is a Fourier sum of size at most $S(m+1)^d + 1$ sign representing the output of the circuit.*

Proof We will assume that the threshold value of the output gate is 0. This can then afterward be corrected by increasing the size of the obtained Fourier sum by 1. We interpret the top two layers of the circuit as a polynomial over $\mathbf{R}$ in S variables with at most S terms and of degree d. Express each $\mathbf{MOD}_m$ gate of the circuit as a Fourier sum of size $m+1$. Substituting these for the variables in the polynomial yields the required Fourier sum sign representing the output of the circuit of size at most $S(m+1)^d$. □

With the same proof but switching to equality representation we obtain the same with an exact threshold gate at the output.

Proposition 12 *For any* $\mathbf{ETHR} \circ \mathbf{AND}_d \circ \mathbf{MOD}_m$ *circuit of size S there is a Fourier sum of size at most $S(m+1)^d + 1$ equality representing the output of the circuit.*

With a majority gate at the output, we observe that the proof of Proposition 11 gives a Fourier sum where all coefficients are of the form $\frac{1}{m^i}$ for $i \in \{0, \ldots, d\}$, by Lemma 10. Then since all coefficients of the polynomial given by the top two layers are 1, multiplying by m^d yields a Fourier sign representation as stated below.

Proposition 13 *For any* $\mathbf{MAJ} \circ \mathbf{AND}_d \circ \mathbf{MOD}_m$ *circuit of size S there is a Fourier sum with integer coefficients of total absolute value at most $S((m+1)^d m^d + 1)$ sign representing the output of the circuit.*

Proposition 14 *Suppose a Boolean function f can be sign represented by a Fourier sum over $\mathbf{C}$ of size S. Then f is computed by a $\mathbf{THR} \circ \mathbf{MOD}_m$ circuit of size mS.*

Proof By linearity we have

$$\mathrm{Re}(\sum_{i=1}^{S} c_i \omega^{a_{i,1}x_1 + \ldots a_{i,n}x_n}) = \sum_{i=1}^{S} \mathrm{Re}(c_i \omega^{a_{i,1}x_1 + \ldots a_{i,n}x_n}) \ .$$

Thus to compute the sum we can compute each term $\mathrm{Re}(c_i \omega^{a_{i,1}x_1 + \ldots a_{i,n}x_n})$ individually. For every $0 < a < m$ we will have a $\mathbf{MOD}_m$ gate that evaluate to 1 if $a_{i,1}x_1 + \ldots a_{i,n}x_n \not\equiv 0 \pmod{m}$. This $\mathbf{MOD}_m$ gate is given the coefficient $-\mathrm{Re}(c_i\omega^a)$ and we add $\mathrm{Re}(c_i\omega^a)$ to the threshold value of the output gate, which effectively makes the $\mathbf{MOD}_m$ gate contribute the correct value to the sum. □

With the same proof we obtain a similar result for equality representation.

Proposition 15 *Suppose a Boolean function f can be equality represented by a Fourier sum over $\mathbf{C}$ of size S. Then f is computed by a $\mathbf{ETHR} \circ \mathbf{MOD}_m$ circuit of size mS.*

To be able to compute sign representations with bounded integer coefficients we will need a slightly more involved approach, since we will only be able to compute the sum with limited precision.

We consider the cyclotomic field $\mathbf{Q}(\omega)$. Let $\omega_1, \ldots, \omega_{\phi(m)}$ be the conjugates of ω, where ϕ is Euler's totient function. Let $z = g(\omega)$ where $g \in \mathbf{Q}[X]$. The *norm* $N(z)$ is then given by

$$N(z) = \prod_{i=1}^{\phi(m)} g(\omega_i) \ .$$

It is well known that the norm has the property that $N(z) \in Q$ and $N(z) = 0$ if and only if $z = 0$. Furthermore, when $g \in \mathbf{Z}[X]$ we have that $N(z) \in \mathbf{Z}$.

Proposition 16 *Let $z \in \mathbf{Q}(\omega)$ be nonzero and assume $z = g(\omega)$, where $g(X) \in \mathbf{Z}[X]$ have integer coefficients of total absolute value at most M. Then we have*

$$|z| \geq \frac{1}{M^{\phi(m)-1}} \ .$$

Proof Since $g(X) \in \mathbf{Z}[X]$ we have that $N(z) \in \mathbf{Z}$. Furthermore since the coefficients of g are of total absolute value at most M we have $|g(\omega_i)| \leq M$ for all i. Thus we have

$$1 \leq |N(z)| \leq \left| \prod_{i=1}^{\phi(m)} g(\omega_i) \right| = \prod_{i=1}^{\phi(m)} |g(\omega_i)| \leq |g(\omega)| M^{\phi(m)-1}$$

from which the result follows. □

Corollary 17 *Let $z \in \mathbf{Q}(\omega)$ be such that $\mathrm{Re}(z) \neq 0$ and assume $z = g(\omega)$, where $g(X) \in \mathbf{Z}[X]$ have integer coefficients of total absolute value at most M. Then we have*

$$|\mathrm{Re}(z)| \geq \frac{1}{2(2M)^{\phi(m)-1}} \ .$$

Proof Since $\mathrm{Re}(z) = \frac{1}{2}(z + \bar{z})$ Proposition 16 gives

$$|z + \bar{z}| \geq \frac{1}{(2M)^{\phi(m)-1}}$$

from which the result follows. □

Proposition 18 *Suppose a Boolean function f can be sign represented by a Fourier sum over $\mathbf{C}$ of size S with integer coefficients of absolute value at most M. Then f is computed by a $\mathbf{MAJ}\circ\mathbf{MOD}_m$ circuit of size $4mS(2M)^{\phi(m)}$.*

Proof We will construct a $\mathbf{THR} \circ \mathbf{MOD}_m$ circuit and carefully track the size of the integer coefficients. Following the proof of Proposition 14 we derive

$$\mathrm{Re}(\sum_{i=1}^{S} c_i \omega^{a_{i,1}x_1 + \dots a_{i,n}x_n}) = \sum_{i=1}^{S} \mathrm{Re}(c_i \omega^{a_{i,1}x_1 + \dots a_{i,n}x_n}) \ .$$

Now from Corollary 17 the absolute value of the left-hand side is at least $\frac{1}{2(2M)^{\phi(m)-1}}$. We will approximate each term $\mathrm{Re}(c_i \omega^{a_{i,1}x_1 + \dots a_{i,n}x_n})$ individually. Let x be arbitrary and define $a_i = a_{i,1}x_1 + \dots a_{i,n}x_n$. For every $0 \leq a < m$ define

$$\hat{c}_{i,a} = \lfloor 4S(2M)^{\phi(m)-1} \mathrm{Re}(c_i \omega^a) \rfloor \ .$$

We then have that

$$\left| 4S(2M)^{\phi(m)-1} \operatorname{Re}(\sum_{i=1}^{S} c_i \omega^{a_i}) - \sum_{i=1}^{S} \hat{c}_{i,a} \right| \leq S \ .$$

Since we also have that

$$\left| 4S(2M)^{\phi(m)-1} \operatorname{Re}(\sum_{i=1}^{S} c_i \omega^{a_i}) \right| \geq 2S \ ,$$

the approximation has the correct sign. We can now conclude as in the proof of Proposition 14. For every $0 < a < m$ we will have a MOD_m gate that evaluate to 1 if $a_{i,1}x_1 + \ldots a_{i,n}x_n \not\equiv 0 \pmod{m}$. This MOD_m gate is given the coefficient $-\hat{c}_{i,a}$ and we add $\hat{c}_{i,a}$ to the threshold value of the output gate. The total absolute value of the coefficients is bounded by $m4S(2M)^{\phi(m)-1}M$ and the size of the resulting $\mathbf{MAJ} \circ \mathbf{MOD}_m$ circuit is then at most $4mS(2M)^{\phi(m)}$. $\square$

As the case of modular counting gates we obtain that a middle layer of AND gates can be absorbed at the a reasonable increase in the size of the circuit by combining the results above.

Theorem 19 *Any* $\mathbf{THR} \circ \mathbf{AND}_d \circ \mathbf{MOD}_m$ *circuit of size S is computed by* $\mathbf{THR} \circ \mathbf{MOD}_m$ *circuit of size $S2^{O(d)}$. Any* $\mathbf{ETHR} \circ \mathbf{AND}_d \circ \mathbf{MOD}_m$ *circuit of size S is computed by* $\mathbf{ETHR} \circ \mathbf{MOD}_m$ *circuit of size $S2^{O(d)}$. Any* $\mathbf{MAJ} \circ \mathbf{AND}_d \circ \mathbf{MOD}_m$ *circuit of size S is computed by* $\mathbf{MAJ} \circ \mathbf{MOD}_m$ *circuit of size $S^{O(1)}2^{O(d)}$.*

4 Depth Reduction for Circuits

In this section we will combine the results about probabilistic polynomials with the Fourier sum representations to derive the stated depth reduction result for circuits with a single layer of MOD_m gates.

Theorem 20 *Let $\epsilon > 0$. Then any depth $h+1$* $\mathbf{AC^0}[p] \circ \mathbf{MOD}_m$ *circuit of size S is computed by a probabilistic* $\mathbf{MOD}_p \circ \mathbf{MOD}_m$ *circuit of size $2^{O(\log(S)\log(\frac{S}{\epsilon})^h)}$ with error at most ϵ.*

Proof Let C be a depth $h+1$ $\mathbf{AC^0}[p] \circ \mathbf{MOD}_m$ circuit of size S. We first use Theorem 3 on the $\mathbf{AC^0}[p]$ circuit given by the top h layers of C. This gives a probabilistic $\mathbf{MOD}_p \circ \mathbf{AND}_d$ circuit of size S^d, where $d = O(\log(\frac{S}{\epsilon})^h)$, which in turn gives a probabilistic $\mathbf{MOD}_p \circ \mathbf{AND}_d \circ \mathbf{MOD}_m$ circuit of size S^d computing C with error at most ϵ. Then Theorem 9 gives a probabilistic $\mathbf{MOD}_p \circ \mathbf{MOD}_m$ circuit of size $S^d2^{O(d)} = 2^{O(\log(S)d)}$. $\square$

Theorem 21 *Let $\epsilon > 0$. Then any depth $h+2$* $\mathbf{THR} \circ \mathbf{AC^0} \circ \mathbf{MOD}_m$ *circuit of size S is computed by a probabilistic* $\mathbf{THR} \circ \mathbf{MOD}_m$ *circuit of size $2^{O(\log(S)^{h+1}\log(\frac{S}{\epsilon})^h)}$ with one-sided error at most ϵ.*

Proof Let C be a depth $h+2$ $\mathbf{THR} \circ \mathbf{AC^0} \circ \mathbf{MOD}_m$ circuit of size S, and let $C_1, \ldots, C_S$ be the $\mathbf{AC^0} \circ \mathbf{MOD}_m$ subcircuits that feed the output gate. We first use Theorem 5 on the top d layers of $C_1, \ldots, C_S$. This gives probabilistic integer polynomials of degree $d = O((\log(\frac{S}{\epsilon})\log(S))^h)$ with one-sided error ϵ/S, and we feed all terms of C_i to output gate, with weight given by the product of the coefficient of the term and the weight of C_i, for all i. This gives a probabilistic $\mathbf{THR} \circ \mathbf{AND}_d$ circuit for the first $d+1$ layers of C with one-sided error ϵ of size S^{d+1}, and thus a probabilistic

$\textbf{THR} \circ \textbf{AND}_d \circ \textbf{MOD}_m$ circuit for C. Finally Theorem 19 gives a $\textbf{THR} \circ \textbf{MOD}_m$ circuit of size $S^{d+1}2^{O(d)} = 2^{O(\log(S)d)}$. □

With a similar proofs we also obtain.

Theorem 22 *Let $\epsilon > 0$. Then any depth $h+2$ $\textbf{ETHR} \circ \textbf{AC}^\textbf{0} \circ \textbf{MOD}_m$ circuit of size S is computed by a probabilistic $\textbf{ETHR} \circ \textbf{MOD}_m$ circuit of size $2^{O(\log(S)^{h+1} \log(\frac{S}{\epsilon})^h)}$ with error at most ϵ. And any depth $h+1$ $\textbf{AC}^\textbf{0} \circ \textbf{MOD}_m$ circuit of size S is computed by a probabilistic $\textbf{ETHR} \circ \textbf{MOD}_m$ circuit of size $2^{O(\log(S)^{h+1} \log(\frac{S}{\epsilon})^h)}$ with one-sided error at most ϵ.*

Theorem 23 *Let $\epsilon > 0$. Then any depth $h+2$ $\textbf{MAJ} \circ \textbf{AC}^\textbf{0} \circ \textbf{MOD}_m$ circuit of size S is computed by a probabilistic $\textbf{MAJ} \circ \textbf{MOD}_m$ circuit of size $2^{O(\log(S)^{h+1} \log(\frac{S}{\epsilon})^h)}$ with one-sided error at most ϵ.*

5   Acknowledgments

References

[1] E. Allender and U. Hertrampf. Depth reduction for circuits of unbounded fan-in. *Information and Computation*, 112(2):217–238, 1994.

[2] D. A. M. Barrington and H. Straubing. Lower bounds for modular counting by circuits with modular gates. *Computational Complexity*, 8(3):258–272, 1999.

[3] D. A. M. Barrington, H. Straubing, and D. Thérien. Non-uniform automata over groups. *Information and Computation*, 89(2):109–132, 1990.

[4] R. Beigel and A. Maciel. Upper and lower bounds for some depth-3 circuit classes. *Computational Complexity*, 6(3):235–255, 1997.

[5] R. Beigel, N. Reingold, and D. Spielman. The perceptron strikes back. In *Proceedings of the 6th Annual Conference on Structure in Complexity Theory*, pages 286–293. IEEE Computer Society Press, 1991.

[6] R. Beigel and J. Tarui. On **ACC**. *Computational Complexity*, 4(4):350–366, 1994.

[7] R. Beigel, J. Tarui, and S. Toda. On probabilistic ACC circuits with an exact-threshold output gate. In *Proceedings of the 3rd International Symposium on Algorithms and Computation*, volume 650 of *Lecture Notes in Computer Science*, pages 420–429. Springer, 1992.

[8] J. Bruck. Harmonic analysis of polynomial threshold functions. *SIAM Journal on Discrete Mathematics*, 3(2):168–177, 1990.

[9] A. Chattopadhyay and K. A. Hansen. Lower bounds for circuits with few modular and symmetric gates. In *32nd Annual International Colloquium on Automata, Languages and Programming*, volume 3580 of *Lecture Notes in Computer Science*, pages 994–1005. Springer, 2005.

[10] M. Goldmann. A note on the power of majority gates and modular gates. *Information Processing Letters*, 53(6):321–327, 1995.

[11] V. Grolmusz and G. Tardos. Lower bounds for $(MOD_p - MOD_m)$ circuits. *SIAM Journal on Computing*, 29(4):1209–1222, 2000.

[12] K. A. Hansen. Lower bounds for circuits with few modular gates using exponential sums. Technical Report 79, Electronic Colloquium on Computational Complexity, 2006.

[13] J. Håstad and M. Goldmann. On the power of small-depth threshold circuits. *Computational Complexity*, 1:113–129, 1991.

[14] S. Jukna. On graph complexity. *Combinatorics, Probability & Computing*, 15(6):855–876, 2006.

[15] M. Krause and P. Pudlák. On the computational power of depth-2 circuits with threshold and modulo gates. *Theoretical Computer Science*, 174(1–2):137–156, 1997.

[16] A. A. Razborov. Lower bounds for the size of circuits of bounded depth with basis $(\wedge, \oplus)$. *Mathematical Notes of the Academy of Science of the USSR*, 41(4):333–338, 1987.

[17] R. Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proceedings of the 19th annual ACM Symposium on Theory of Computing*, pages 77–82, 1987.

[18] H. Straubing and D. Thérien. A note on MOD_p - MOD_m circuits. *Theory of Computing Systems*, 39(5):699–706, 2006.

[19] J. Tarui. Probabilistic polynomials, $\mathbf{AC}^0$ functions and the polynomial-time hierarchy. *Theoretical Computer Science*, 113(1):167–183, 1993.

[20] L. G. Valiant and V. V. Vazirani. NP is as easy as detecting unique solutions. *Theoretical Computer Science*, 47(1):85–93, 1986.

[21] E. Viola. Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates. *SIAM Journal on Computing*, 36(5):1387–1403, 2007.

[22] A. C. Yao. On ACC and threshold circuits. In *31st Annual Symposium on Foundations of Computer Science*, pages 619–627. IEEE Computer Society Press, 1990.