On Probabilistic ACC Circuits with an Exact-Threshold Output Gate

Richard Beigel*
Department of Computer Science, Yale University
New Haven, CT 06520-2158, USA. beigel-richard@cs.yale.edu

Jun Tarui†
Department of Computer Science, University of Warwick
Coventry, CV4 7AL, United Kingdom. jun@dcs.warwick.ac.uk

Seinosuke Toda
Department of Computer Science and Information Mathematics
University of Electro-Communications
Chofu-shi, Tokyo, 182, Japan. toda@pspace.cs.uec.ac.jp

Abstract

Let SYM^{+} denote the class of Boolean functions computable by depth-two size-$n^{\log^{O(1)} n}$ circuits with a symmetric-function gate at the root and AND gates of fan-in $\log^{O(1)} n$ at the next level, or equivalently, the class of Boolean functions f such that $f(x_1,\ldots,x_n)$ can be expressed as $f(x_1,\ldots,x_n) = h_n(p_n(x_1,\ldots,x_n))$ for some polynomial p_n over $\mathbf{Z}$ of degree $\log^{O(1)} n$ and norm (the sum of the absolute values of its coefficients) $n^{\log^{O(1)} n}$ and some function $h_n : \mathbf{Z} \to \{0,1\}$. Building on work of Yao [Yao90], Beigel and Tarui [BT91] showed that $\mathrm{ACC} \subseteq \mathrm{SYM}^{+}$, where ACC is the class of Boolean functions computable by constant-depth polynomial-size circuits with NOT, AND, OR, and MOD_m gates for some fixed m.

In this paper, we consider augmenting the power of ACC circuits by allowing randomness and allowing an exact-threshold gate as the output gate (an exact-threshold gate outputs 1 if exactly k of its inputs are 1, where k is a parameter; it outputs 0 otherwise), and show that every Boolean function computed by this kind of augmented ACC circuits is still in SYM^{+}.

Showing that some "natural" function f does not belong to the class ACC remains an open problem in circuit complexity, and the result that

*Supported in part by NSF grant CCR-8958528

†Supported in part by the ESPRIT II BRA Programme of the EC under contract # 7141 (ALCOM II). Part of the work was done while the author was a student at University of Rochester, and was supported in part by NSF grant CDA-8822724.

ACC $\subseteq$ SYM$^+$ has raised the hope that we may be able to solve this problem by exploiting the characterization of SYM$^+$ in terms of polynomials, which are perhaps easier to analyze than circuits, and showing that $f \notin$ SYM$^+$. Our new result and proof techniques suggest that the possibility that SYM$^+$ contains even more Boolean functions than we currently know should also be kept in mind and explored.

By a well-known connection [FSS84], we also obtain new results about some classes related to the polynomial-time hierarchy.

1 Introduction

Consider a sequence $\langle C_n : n = 1, \ldots \rangle$ of circuits computing a Boolean function $f : \{0,1\}^* \to \{0,1\}$, where C_n is a circuit for n Boolean variables computing f_n, the restriction of f to $\{0,1\}^n$. In *constant-depth* circuits, the depth of C_n is *fixed* as $n \to \infty$, and gates of *unbounded fan-in* are allowed.

In the last decade, strong lower bounds were established for the size of constant-depth circuits that compute explicit Boolean functions, in the case where the allowable gates are NOT, AND, OR, and MOD$_q$ for some fixed prime power q. (A MOD$_m$ gate on inputs $y_1, \ldots, y_\nu$ outputs 1 if $\sum y_i \equiv 0 \pmod{m}$; 0 otherwise.)

Furst, Saxe, and Sipser [FSS84] and, independently, Ajtai [Ajt83] first showed that constant-depth circuits with NOT, OR, and AND gates require superpolynomial size to compute PARITY. Yao [Yao85] improved this and gave an exponential bound, and later Hastad [Has87] simplified a proof, and gave a further improved near-optimal bound.

Razborov [Raz87] showed that to compute MAJORITY, constant-depth circuits with NOT, AND, OR, *and* PARITY gates require exponential size. Smolensky later extended this and showed that to compute the MOD$_q$ function, constant-depth circuits with NOT, AND, OR, and MOD$_{q'}$ gates require exponential size if q and q' are powers of distinct primes. (For more information about these results and general discussions on this line of research including history, motivations, and applications, see [Sip92] and [BS90].)

It remains an open problem, however, to show a limitation for constant-depth circuits with MOD$_m$ gates for some fixed composite m: The class ACC, first considered by Barrington [Bar89], consists of Boolean functions computable by constant-depth polynomial-size circuits with NOT, AND, OR, and MOD$_m$ gates for some fixed m. At present, we cannot prove that some explicit function, e.g., a function in NP, does not belong to ACC.

The first nontrivial *upper* bound on the computing power of ACC circuits was shown by Yao [Yao90], and it was later improved by Beigel and Tarui [BT91]. We first explain some conventions and definitions.

For a multivariate polynomial over $\mathbf{Z}$, define its *norm* to be the sum of the absolute values of its coefficients. A function $g(y_1, \ldots, y_\nu)$ is *symmetric* if g is fixed under any permutation of $\{1, \ldots, \nu\}$, which is equivalent to saying that $g(y_1, \ldots, y_\nu)$

only depends on $\sum y_i$ in the case y_i's are Boolean. As usual, we assume that NOT gates appear in a circuit only in the form of a negated input literal $\overline{x_i}$.

Let SYM$^+$ denote the class of Boolean functions computable by depth-two size-$n^{\log^{O(1)} n}$ circuits with an output gate labelled by a Boolean-valued symmetric function and AND gates of fan-in $\log^{O(1)} n$ at the next level. Similarly define the class FSYM$^+$ of integer-valued functions on $\{0,1\}^*$ by allowing an output gate labelled by an integer-valued symmetric function. (In [BT91], the class SYM$^+$ was called SYMMC. For general discussions of *quasipolynomial*-size (size $n^{\log^{O(1)} n}$) circuit classes, see the recent survey by Barrington [Bar92], which also includes the suggestion to use the name SYM$^+$.)

The following are immediate: A Boolean function f is in SYM$^+$ if and only if f can be expressed as $f(x_1,\ldots,x_n) = h_n(p_n(x_1,\ldots,x_n))$ for some polynomial p_n over $\mathbf{Z}$ of degree $\log^{O(1)} n$ and norm $n^{\log^{O(1)} n}$ and some function $h_n : \mathbf{Z} \to \{0,1\}$. By allowing $h_n : \mathbf{Z} \to \mathbf{Z}$, a similar characterization of FSYM$^+$ is obtained.

Improving the earlier result by Yao [Yao90], Beigel and Tarui [BT91] showed that ACC $\subseteq$ SYM$^+$. This result says that low-degree small-norm polynomials can represent a surprising rich class of Boolean functions. At the same time, it has raised the hope that we may be able to solve the ACC problem by exploiting the characterization of SYM$^+$ in terms of polynomials, which are perhaps easier to analyze than circuits, and showing that some explicit function does not belong to SYM$^+$.

In this paper, we show some additional representational power of low-degree small-norm polynomials in two settings. Our new results and the techniques we develop suggest that the possibility that SYM$^+$ contains even more Boolean functions than we currently know should also be kept in mind and explored.

In Section 2, we state our two results and the key lemma we use in proving them. In Section 3, we prove the two results assuming the key lemma, and we prove the key lemma in Section 4.

2 Results

For Boolean inputs $y_1,\ldots,y_\nu$, an *Exact*$_k$ gate outputs 1 if $\sum y_i = k$, and 0 otherwise; and a *Count* gate outputs the nonnegative integer $\sum y_i$. When we consider an Exact$_k$ gate, the parameter k may grow as the size of input approaches infinity. A circuit with a Count gate as its single output gate is a natural circuit analogue of a counting Turing machine, the notion introduced by Valiant [Val79] to define the class #P; and such a circuit computes a function from $\{0,1\}^n$ to $\mathbf{Z}^{\geq 0}$, the set of nonnegative integers. *ACC circuits* consists of AND, OR, and MOD$_m$ gates for some fixed m. We consider augmenting the power of ACC circuits by allowing randomness and allowing an Exact gate or a Count gate as the output gate.

Theorem 2.1. *Suppose that a Boolean function $f : \{0,1\}^* \to \{0,1\}$ is computed with error probability bounded away from $1/2$ by some constant-depth polynomial-size probabilistic ACC circuits with an Exact gate as the output gate. Then $f \in SYM^+$.*

It is known [ABO84] that allowing randomness alone does not enable constant-depth polynomial-size ACC circuits to compute a function outside of ACC; and in [BT91], it was shown that allowing a symmetric-function output gate does not enable constant-depth polynomial-size deterministic ACC circuits to compute a function outside SYM^+. But to prove Theorem 2.1, which concerns augmented ACC circuits in which randomness *and* an Exact output gate are allowed, we need to develop new techniques.

Theorem 2.2. *Suppose that a function $f : \{0,1\}^* \to \mathbf{Z}^{\geq 0}$ is computed with error probability bounded away from $1/2$ by some constant-depth polynomial-size probabilistic ACC circuits with a Count gate as the output gate. Then $f \in FSYM^+$.*

The following lemma will be the key to prove the two theorems above. Let p_j denote the j-th smallest prime. For a finite multiset S of integers, a prime p_j, and a residue $r \in \{0, \ldots, p_j - 1\}$, let $M_{j,r}(S)$ denote the number of elements in S that are congruent to r mod p_j.

Lemma 2.3. *Let a sequence $\langle l_n : n = 1, \ldots \rangle$ of positive integers of order $\log^{O(1)} n$ be given. Then, there is a sequence $\langle q_n(x_1, \ldots, x_n) : n = 1, \ldots \rangle$ of polynomials over $\mathbf{Z}$ of degree $\log^{O(1)} n$ and norm $n^{\log^{O(1)} n}$ such that the following holds for each n: For any integers $a_1, \ldots, a_n$, every prime p_j with $j \leq l_n$, and every residue $r \in \{0, \ldots, p_j - 1\}$, $M_{j,r}(a_1, \ldots, a_n)$ can be determined from $q_n(a_1, \ldots, a_n)$.*

There is a well-known connection [FSS84] between constant-depth circuit classes and some complexity classes between P and PSPACE. In particular, the class of Boolean functions computable by constant-depth quasipolynomial-size AND/OR circuits corresponds to the class PH, the polynomial-time hierarchy (for a definition, see, e.g., [Joh90]). It will be clear from the proofs that the conclusions of Theorems 1 and 2 in fact hold for augmented ACC circuits of constant depth and *quasipolynomial* size; and we can obtain new results about some classes related to PH. The classes SYM^+ and FSYM^+ correspond to $\mathrm{P}^{\#\mathrm{P}[1]}$ and $\mathrm{FP}^{\#\mathrm{P}[1]}$, respectively. Below we state two new results corresponding to Theorems 1 and 2. (More precisely, they correspond to the versions of Theorems 1 and 2 stated in terms of constant-depth quasipolynomial-size AND/OR circuits.) Further discussions of these results are omitted from this paper.

Proposition 2.4.

$$\mathrm{BP} \cdot \mathrm{C}_{=} \cdot \mathrm{PH} \subseteq \mathrm{P}^{\#\mathrm{P}[1]}.$$

Proposition 2.5.

$$\mathrm{BP} \cdot \# \cdot \mathrm{PH} \subseteq \mathrm{FP}^{\#\mathrm{P}[1]}.$$

3 Proofs of Theorems from the Key Lemma

For a circuit C for n variables $x_1, \ldots, x_n$, we let $C(x_1, \ldots, x_n)$ denote the function that C computes. First we explain the following nonconstructive argument:

Proposition 3.1. *Let D_n be a probabilistic circuit for n Boolean variables that computes $f_n : \{0,1\}^n \to \{0,1\}$ with error probability at most ε_n. Then, for any constant $\delta > 0$, there is a multiset of $N = O(1/\varepsilon_n \cdot n)$ deterministic circuits $C_1, \ldots, C_N$, each obtained by fixing a setting of random bits in D_n, such that for every $x \in \{0,1\}^n$, $C_i(x) = f_n(x)$ except for at most $(1+\delta)\varepsilon_n$ fraction of i's $(1 \le i \le N)$.*

Proof. Fix $x \in \{0,1\}^n$ and consider $\overline{D}_1(x), \ldots, \overline{D}_N(x)$, where $\overline{D}_i$'s are N independent copies of D_n. Let E be the number of errors among $\overline{D}_i$'s, i.e., let $E = |\{i : 1 \le i \le N : \overline{D}_i(x) \ne f_n(x)\}|$. By the Chernoff bound [Che52] on the tails of Bernoulli trials, we can take $N = O(1/\varepsilon_n \cdot n)$ and have

$$\mathrm{Prob}(E > (1+\delta)\varepsilon_n N) < 2^{-n}.$$

¿From this, the proposition readily follows. ∎

Proof of Theorem 2.1. Let D_n be a constant-depth polynomial-size probabilistic ACC circuit with an Exact_{b_n} output gate of fan-in K and AND/OR/MOD_m gates elsewhere that computes $f_n : \{0,1\}^n \to \{0,1\}$ with error probability at most $1/4$. (It will be clear that the proof works for any error probability bounded away from $1/2$.) By using a standard probabilistic simulation of AND/OR by MOD_m gates (we can either use Valiant and Vazirani's lemma [VV86] as in [AH90] or the Razborov-Smolensky simulation [Raz87, Smo87]) and by the argument explained above, obtain $N = O(n)$ deterministic ACC circuits $C_1, \ldots, C_N$ consisting of MOD_m gates and fan-in-$\log^{O(1)} n$ AND gates such that for every $x \in \{0,1\}^n$,

$$\begin{aligned} f_n(x) = 0 \quad &\Longrightarrow \quad |\{i : 1 \le i \le N : C_i(x) = 1\}| \le \frac{1}{3}N; \\ f_n(x) = 1 \quad &\Longrightarrow \quad |\{i : 1 \le i \le N : C_i(x) = 1\}| \ge \frac{2}{3}N. \end{aligned}$$

Thus, if we let $\{g_i^{(1)}, \ldots, g_i^{(K)}\}$ be the set of MOD_m gates that are connected to the output gate of C_i $(1 \le i \le N)$, one of the following two cases holds for each input x, where $g_i^{(j)}$ below denotes the $\{0,1\}$-value of that gate on input x.

$$\text{Case 1:} \qquad |\{i : 1 \le i \le N, \sum_{j=1}^{K} g_i^{(j)} = b_n\}| \le \frac{1}{3}N.$$

$$\text{Case 2:} \qquad |\{i : 1 \le i \le N, \sum_{j=1}^{K} g_i^{(j)} = b_n\}| \ge \frac{2}{3}N.$$

If there is a degree-$\log^{O(1)} n$ norm-$n^{\log^{O(1)} n}$ polynomial q in KN variables such that which of Cases (1) and (2) holds can be determined from the value of $q(g_1^{(1)}, \ldots, g_1^{(K)}, \ldots, g_N^{(1)}, \ldots, g_N^{(K)})$, then by the same argument as in [BT91, Proof of Lemma 5], we can conclude that $\{f_n\}_{n=0}^{\infty} \in \mathrm{SYM}^+$.

The following lemma says that such a polynomial indeed exists (substitute $\sum_{j=1}^{K} g_i^{(j)}$ for each variable x_i in a polynomial given in the lemma). ∎

Lemma 3.2. *Let $k \geq 1$ and let $\langle b_n : n = 1, \ldots \rangle$ be a sequence of integers with $|b_n| \leq n^k$. Then, there is a sequence $\langle q_n(x_1, \ldots, x_n) : n = 1, \ldots \rangle$ of polynomials of degree $\log^{O(1)} n$ and norm $n^{\log^{O(1)} n}$ and a sequence $\langle h_n : n = 1, \ldots \rangle$ of functions from $\mathbf{Z}$ to $\{0, 1\}$ with the following property: For any integers $a_1, \ldots, a_n$ with $|a_i| \leq n^k$,*

$$|\{i : a_i = b_n\}| \leq \frac{1}{3}n \quad \Longrightarrow \quad h_n(q_n(a_1, \ldots, a_n)) = 0;$$
$$|\{i : a_i = b_n\}| \geq \frac{2}{3}n \quad \Longrightarrow \quad h_n(q_n(a_1, \ldots, a_n)) = 1.$$

Proof. Let b_n and $a_1, \ldots, a_n$ be integers whose absolute values are at most n^k. Let S be the set of a_i's such that $a_i \neq b_n$. Take $l = 4k \log_2 n + O(1)$ so that the following holds: For each $a \in S$, if j is picked at random from $\{1, \ldots, l\}$, $a \equiv b_n \pmod{p_j}$ with probability at most $1/4$. Then, there exists $j \in \{1, \ldots, l\}$ such that

$$|\{a \in S : a \equiv b_n \pmod{p_j}\}| \leq \frac{1}{4}|S|.$$

Now assume that either (1) $|S| \geq \frac{2}{3}n$ or (2) $|S| \leq \frac{1}{3}n$ holds. The argument above shows that Case (2) holds if and only if $M_{j,(b_n \bmod p_j)}(a_1, \ldots, a_n) \geq \frac{2}{3}n$ for all $j = 1, \ldots, l$. Using Lemma 2.3, we can finish the proof. ∎

Proof of Theorem 2.2. Similar reasoning as in the proof of Theorem 2.1 yield the following. Below we use the same notation as in the proof of Theorem 2.1. For each input x, there exists c_n such that

$$|\{i : 1 \leq i \leq N, \sum_{j=1}^{K} g_i^{(j)} = c_n\}| \geq \frac{2}{3}N.$$

The following lemma says that there is a degree-$\log^{O(1)} n$ norm-$n^{\log^{O(1)} n}$ polynomial q in KN variables such that c_n can be determined from the value of $q(g_1^{(1)}, \ldots, g_1^{(K)}, \ldots, g_N^{(1)}, \ldots, g_N^{(K)})$. ∎

Lemma 3.3. *Let $k \geq 1$ and let $\langle b_n : n = 1, \ldots \rangle$ be a sequence of integers with $|b_n| \leq n^k$. Then, there is a sequence $\langle q_n(x_1, \ldots, x_n) : n = 1, \ldots \rangle$ of degree-$\log^{O(1)} n$ norm-$n^{\log^{O(1)} n}$ polynomials and a sequence $\langle h_n : n = 1, \ldots \rangle$ of functions from $\mathbf{Z}$ to $\mathbf{Z}$ with the following property: For any integers $a_1, \ldots, a_n$ with $|a_i| \leq n^k$,*

$$(\exists c)\ |\{i : a_i = c\}| \geq \frac{2}{3}n \Longrightarrow h_n(q_n(a_1, \ldots, a_n)) = c.$$

Proof. Take $l = k \log_2 n + O(1)$ so that we have $P = \prod_{j=1}^{l} p_j > 2n^k + 1 = |\{-n^k, \ldots, n^k\}|$. By determining $M_{j,r}(a_1, \ldots, a_n)$ for each prime p_j $(1 \leq j \leq l)$, we can determine such c as above if it exists. Using Lemma 2.3, we can finish the proof. ∎

4 Proof of the Key Lemma

Say that a singe-variate polynomial $A(x)$ over $\mathbf{Z}$ is *degree-d modulus-amplifying* if for arbitrary integers N and m,

$$\begin{aligned} N \equiv 0 \pmod{m} &\implies A(N) \equiv 0 \pmod{m^d}; \\ N \equiv 1 \pmod{m} &\implies A(N) \equiv 1 \pmod{m^d}. \end{aligned}$$

The following lemma is essentially due to Toda [Tod91], and was proved in the form below with simplified analysis and optimal degree in [BT91].

Lemma 4.1. *For each $d \geq 1$, there is a unique degree-$(2d-1)$ polynomial that is degree-d modulus-amplifying.*

In what follows, we let $A_d(x)$ denote the unique degree-d modulus-amplifying polynomial given in Lemma 4.1. When d is of order $\log^{O(1)} n$, the norm of A_d is of order $n^{\log^{O(1)} n}$.

For convenience, we restate Lemma 2.3.

Lemma 2.3. Let a sequence $\langle l_n : n = 1, \ldots \rangle$ of positive integers of order $\log^{O(1)} n$ be given. Then, there is a sequence $\langle q_n(x_1, \ldots, x_n) : n = 1, \ldots \rangle$ of polynomials over $\mathbf{Z}$ of degree $\log^{O(1)} n$ and norm $n^{\log^{O(1)} n}$ such that the following holds for each n: For any integers $a_1, \ldots, a_n$, every prime p_j with $j \leq l_n$, and every residue $r \in \{0, \ldots, p_j - 1\}$, $M_{j,r}(a_1, \ldots, a_n)$ can be determined from $q_n(a_1, \ldots, a_n)$.

Proof. We will gradually explain a construction of polynomials satisfying the conclusion of the lemma. Below we use "mod" as in "$a \equiv 0 \pmod{m}$" and also as a binary operator as in "$a \bmod m \in \{0, \ldots, m-1\}$".

Let $R_p(x, r)$ be the polynomial in x and r defined by $R_p(x, r) = 1 - (x - r)^{p-1}$. Then, by Fermat's little theorem, for an integer a, a prime p, and a residue $r \in \{0, \ldots, p-1\}$,

$$R_p(a, r) \bmod p = (1 - (a - r)^{p-1}) \bmod p = \begin{cases} 1 & \text{if } a \equiv r \pmod{p}; \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

First we explain a construction for *one* prime p_j; write p for p_j and $M_r(a_1, \ldots, a_n)$ for $M_{p_j,r}(a_1, \ldots, a_n)$. Define the polynomial $Q_{p,d}(x_1, \ldots, x_n)$ by

$$Q_{p,d}(x_1, \ldots, x_n) = \sum_{i=1}^{n} \sum_{r=0}^{p-1} A_d(R_p(x_i, r))(n+1)^r.$$

Assume that $p^d > (n+1)^p$. Let $a_1, \ldots, a_n$ be arbitrary integers. We claim that $M_r(a_1, \ldots, a_n)$ can be determined from $Q_{p,d}(a_1, \ldots, a_n)$.

Fix $i \in \{1, \ldots, n\}$ and consider the value $\sigma(a_i)$ of the inner sum. By (1) and degree-d modulus amplification of A_d,

$$\sigma(a_i) \bmod p^d = (n+1)^{(a_i \bmod p)} \tag{2}$$

Since $(n+1)^{(a_i \bmod p)} \leq (n+1)^{p-1}$ and we have assumed that $(n+1)^p < p^d$,

$$\sum_{i=1}^{n} (\sigma(a_i) \bmod p^d) \leq n(n+1)^{p-1} < p^d,$$

and thus

$$\left(\sum_{i=1}^{n} \sigma(a_i)\right) \bmod p^d = \sum_{i=1}^{n} \left(\sigma(a_i) \bmod p^d\right). \tag{3}$$

Let $N = n+1$. Then, using (3) and (2) to get, respectively, the second and the third equalities below, we have

$$\begin{aligned} Q_{p,d}(a_1, \ldots, a_n) \bmod p^d &= \left(\sum_{i=1}^{n} \sigma(a_i)\right) \bmod p^d \\ &= \sum_{i=1}^{n} (\sigma(a_i) \bmod p^d) \\ &= \sum_{i=1}^{n} N^{(a_i \bmod p)} \\ &= \sum_{r=1}^{p-1} M_r(a_1, \ldots, a_n) N^r. \end{aligned}$$

Since $0 \leq M_r(a_1, \ldots, a_n) \leq n < N = n+1$, we can write $(Q_{p,d}(a_1, \ldots, a_n) \bmod p^d)$ in base N and obtain $M_r(a_1, \ldots, a_n)$ as the $(r+1)$-th least significant digit for each $r = 0, \ldots, p-1$.

Using the Chinese remainder theorem, we can construct a polynomial from which $M_{j,r}$ can be determined for *all* the primes $p_1, \ldots, p_{l_n}$.

Now we describe the full construction using the notation above.

Let $\langle l_n : n = 1, \ldots \rangle$ be as in the lemma. Consider n fixed and write l for l_n. Let $N = n+1$ as above, and take $d = p_l \cdot \log N$ $(= \log^{O(1)} n)$ so that for each prime p_j $(1 \leq j \leq l)$, we have $(p_j)^d > N^{p_j}$.

Let $P = \prod_{j=1}^{l} (p_j)^d$ $(= n^{\log^{O(1)} n})$. By the Chinese remainder theorem, for each prime p_j $(1 \leq j \leq l)$, find a unique $\overline{p_j} \in \{0, \ldots, P-1\}$ such that

$$\overline{p_j} \equiv \begin{cases} 1 & (\bmod\ (p_j)^d); \\ 0 & (\bmod\ (p_{j'})^d) \quad \text{for each } j' \neq j,\ 1 \leq j' \leq l. \end{cases} \tag{4}$$

Put

$$
\begin{aligned}
q_n(x_1, \ldots, x_n) &= \sum_{j=1}^{l} \overline{p_j}\, Q_{p_j,d}(x_1, \ldots, x_n) \\
&= \sum_{j=1}^{l} \sum_{i=1}^{n} \sum_{r=0}^{p_j-1} \overline{p_j}\, A_d\big(R_{p_j}(x_i, r)\big)\, N^r.
\end{aligned}
$$

By (4), for any integers $a_1, \ldots, a_n$ and for each $j \in \{1, \ldots, l\}$,

$$
q_n(a_1, \ldots, a_n) \bmod (p_j)^d = Q_{p_j,d}(a_1, \ldots, a_n) \bmod (p_j)^d,
$$

and thus $M_{j,r}(a_1, \ldots, a_n)$ can be determined as explained above.

Finally, it is easy to check that q_n has degree $\log^{O(1)} n$ and norm $n^{\log^{O(1)} n}$. ∎

References

[ABO84] M. Ajtai and M. Ben-Or. A theorem on probabilistic constant depth circuits. In *Proceedings of the 16th Annual ACM Symposium on Theory of Computing*, pages 471–474. ACM Press, 1984.

[AH90] E. Allender and U. Hertrampf. On the power of uniform families of constant depth threshold circuits. In *Proceedings of the 15th International Symposium on Mathematical Foundations of Computer Science*, pages 158–164. Springer-Verlag, 1990. Lecture Notes in Computer Science, vol. 452.

[Ajt83] M. Ajtai. Σ_1^1 formulae on finite structures. *Ann. Pure Appl. Logic*, 24:1–48, 1983.

[Bar89] D. Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1. *J. Comput. System Sci.*, 38(1):150–164, February 1989.

[Bar92] D. Barrington. Quasipolynomial size circuit classes. In *Proceedings of the 7th Annual Conference on Structure in Complexity Theory*, pages 86–93. IEEE Computer Society Press, 1992.

[BS90] R. Boppana and M. Sipser. The complexity of finite functions. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science: Vol. A*, pages 757–804. North-Holland, Amsterdam, 1990.

[BT91] R. Beigel and J. Tarui. On ACC. In *Proceedings of the 32nd IEEE Symposium on Foundations of Computer Science*, pages 783–792. IEEE Computer Society Press, 1991.

[Che52] H. Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *Annals of Mathematical Statistics*, 23:493–507, 1952.

[FSS84] M. Furst, J. Saxe, and M. Sipser. Parity, circuits and the polynomial-time hierarchy. *Math. Systems Theory*, 17:13–27, 1984.

[Has87] J. Hastad. *Computational Limitations of Small-Depth Circuits.* MIT Press, 1987.

[Joh90] D. Johnson. A catalog of complexity classes. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science: Vol. A*, pages 67–161. North-Holland, Amsterdam, 1990.

[Raz87] A. Razborov. Lower bounds for the size of circuits of bounded depth with basis $\{\wedge, \oplus\}$. *Mathematical Notes of the Academy of Sciences of the USSR*, 41(4):333–338, September 1987.

[Sip92] M. Sipser. The history and status of the P versus NP question. In *Proceedings of the 24th Annual ACM Symposium on Theory of Computing*, pages 603–618. ACM Press, 1992.

[Smo87] 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. ACM Press, 1987.

[Tod89] S. Toda. On the computational power of PP and $\oplus$P. In *Proceedings of the 30th IEEE Symposium on Foundations of Computer Science*, pages 514–519. IEEE Computer Society Press, 1989.

[Tod91] S. Toda. PP is as hard as the polynomial-time hierarchy. *SIAM J. Comput.*, 20(5):865–877, 1991. Earlier version appeared as [Tod89].

[Val79] L. Valiant. The complexity of computing the permanent. *Theoret. Comput. Sci.*, 7:189–201, 1979.

[VV86] L. Valiant and V. Vazirani. NP is as easy as detecting unique solutions. *Theoret. Comput. Sci.*, 47:85–93, 1986.

[Yao85] A. Yao. Separating the polynomial-time hierarchy by oracles. In *Proceedings of the 26th IEEE Symposium on Foundations of Computer Science*, pages 1–10. IEEE Computer Society Press, 1985.

[Yao90] A. Yao. On ACC and threshold circuits. In *Proceedings of the 31st IEEE Symposium on Foundations of Computer Science*, pages 619–627. IEEE Computer Society Press, 1990.