Discrete Mathematics and Theoretical Computer Science **4**, 2001, 247–254

A Degree-Decreasing Lemma for $(MOD_q - MOD_p)$ *Circuits*

Vince Grolmusz[†]

Department of Computer Science, Eötvös University, Budapest.
Address: Pázmány P. stny. 1/C, Room 3-614, H-1117 Budapest, Hungary.
Email: `grolmusz@cs.elte.hu`

received Jun 15, 2001, accepted Sep 15, 2001.

Consider a $(\mathrm{MOD}_q, \mathrm{MOD}_p)$ circuit, where the inputs of the bottom MOD_p gates are degree-d polynomials with integer coefficients of the input variables (p, q are different primes). Using our main tool — the Degree Decreasing Lemma — we show that this circuit can be converted to a $(\mathrm{MOD}_q, \mathrm{MOD}_p)$ circuit with *linear* polynomials on the input-level with the price of increasing the size of the circuit. This result implies special cases of the Constant Degree Hypothesis of Barrington, Straubing and Thérien [3], and implies also a generalization of the lower bound results of Yan and Parberry [21], Krause and Waack [12] and Krause and Pudlák [11]. Perhaps the most important application is an exponential lower bound for the size of $(\mathrm{MOD}_q, \mathrm{MOD}_p)$ circuits computing the fan-in n AND, where the input of each MOD_p gate at the bottom is an *arbitrary* integer valued function of cn variables $(c < 1)$ plus an arbitrary linear function of n input variables.

Keywords: Circuit complexity, modular circuits, composite modulus

1 Introduction

Boolean circuits are one of the most interesting models of computation. They are widely examined in VLSI design, in general computability theory and in complexity theory context as well as in the theory of parallel computation.

Almost all of the strongest and deepest lower bound results for the computational complexity of finite functions were proved using the Boolean circuit model of computation ([13], [22], [9], [14], [15], or see [20] for a survey).

Even these famous and sophisticated lower bound results were proven for very restricted circuit classes.

Bounded depth and polynomial size is one of the most natural restrictions. Ajtai [1], Furst, Saxe, and Sipser [5] proved that no polynomial sized, constant depth circuit can compute the PARITY function. Yao [22] and Håstad [9] generalized this result for sub-logarithmic depths.

[†]A preliminary version of this work appeared in the Proceedings of ICALP'98, Springer Verlag, LNCS 1443, pp. 215-222.

Since the modular gates are very simple to define, and they are immune to the random restriction techniques in lower bound proofs for the PARITY function, the following natural question was asked by several researchers: How powerful will become the Boolean circuits if — beside the standard AND, OR and NOT gates — MOD_m gates are also allowed in the circuit? Here a MOD_m gate outputs 1 iff the sum of its inputs is in a set $A \subset \{0,1,2,\ldots,m-1\}$ modulo m.

Razborov [14] showed that for computing MAJORITY with AND, OR, NOT and MOD_2 gates, exponential size is needed with constant depth. This result was generalized by Smolensky [15] for MOD_p gates instead of MOD_2 ones, where p denotes a prime.

Very little is known, however, if both MOD_p and MOD_q gates are allowed in the circuit for different primes p,q, or, if the modulus is a non-prime power composite, e.g., 6. For example, it is consistent with our present knowledge that depth-3, linear-size circuits with MOD_6 gates *only*, recognize the Hamiltonian graphs (see [3]). The existing lower bound results use diverse techniques from Fourier-analysis, communication complexity theory, group-theory and several forms of random restrictions (see [3], [11], [17], [18], [16], [8], [6], [7], [2], [10]).

It is not difficult to see that constant-depth circuits with MOD_p gates only (p prime), cannot compute even simple functions: the fan-in n OR or AND functions, since they can only compute constant degree polynomials of the input variables over GF_p (see [15]).

But depth-2 circuits with MOD_2 and MOD_3 gates, or MOD_6 gates can compute the n-fan-in OR and AND functions [10], [3]. Consequently, these circuits are more powerful than circuits with MOD_p gates only.

By the famous results of Yao [23] and Beigel and Tarui [4], and Toda [19], every polynomial-size, constant-depth circuit with AND, OR, NOT and MOD_m gates can be converted to a depth-2 circuit with a SYMMETRIC gate at the top and quasi-polynomially many AND gates of poly-logarithmic fan-in at the bottom. One might hope that this result is an excellent tool for bounding the power of circuits containing modular gates. Unfortunately, the existing lower bound techniques are not strong enough to bound the computational power of these circuits.

Our main contribution here is a lemma, the Degree Decreasing Lemma, which yields a tool for dealing with low-fan-in AND gates at the bottom of $(\mathrm{MOD}_q,\mathrm{MOD}_p)$ circuits. We believe that – in the light of the result of Yao, Beigel and Tarui – our result may have further important consequences in modular circuit theory.

2 Preliminaries

Definition 1 *A fan-in n gate is an n-variable Boolean function. Let $G_1,G_2,\ldots,G_\ell$ be gates of unbounded fan-in. Then a*

$$(G_1,G_2,\ldots,G_\ell;d)-\ \textit{circuit}$$

denotes a depth-ℓ circuit with a G_1-gate on the top, G_2 gates on the second level, G_3 gates on the third level from the top,..., and G_ℓ gates on the last level. Multi-linear polynomials (i.e., polynomials where the exponent of every variable is 0 or 1) with integer coefficients and of input-variables $x_1,x_2,\ldots,x_n$ of degree at most d are connected to G_ℓ gates on the last level. The size of a circuit is defined to be the total number of the gates $G_1,G_2,\ldots,G_\ell$ in the circuit.

All of our gates are of unbounded fan-in, and we allow to connect inputs to gates or gates to gates with multiple wires. Let us remark, that we are interested mainly in circuits with modular gates and with constant moduli; consequently, the number of wires is polynomially related to the number of gates.

In the literature MOD_m gates are sometimes defined to be 1, iff the sum of their inputs is divisible by m, and sometimes they are defined to be 1, iff the sum of their inputs is not divisible by m. The following, more general definition covers both cases.

Definition 2 *We say that gate G is a* MOD_m-gate, *if there exists a non-empty $A \subset \{0,1,\ldots,m-1\}$, such that*

$$G(x_1,x_2,\ldots,x_n) = \begin{cases} 1, \text{ if } \sum_{i=1}^n x_i \bmod m \in A \\ 0 \text{ otherwise.} \end{cases}$$

A is called the 1-set of G. MOD_m *gates with 1-set A are denoted by* MOD_m^A.

Definition 3 *Let p be a prime. We say that polynomial $P(x_1,x_2,\ldots,x_n)$ over the p element field is a depth-d polynomial, if it can be computed by an arithmetic circuit from inputs $x_1,x_2,\ldots,x_n$ and constants 1 and 0, as follows: the arithmetic circuit is levelled, the variables and constants 0 and 1 are situated on the lowest level, and multiple wires (i.e., constant multipliers) are allowed in the circuit. The levels of the circuit contains ADDITION and MULTIPLICATION gates, the ADDITION gates are of unbounded fan-in, the MULTIPLICATION gates are of fan-in 2. There are only d levels where MULTIPLICATION gates occur, and within the same level, one input of each MULTIPLICATION gates are connected to the same node (called the common multiplier on the level), situated one level lower.*

In other words, if on the same level there are several MULTIPLICATION gates, and one of them computes PQ, then all the other MULTIPLICATION gates on the same level should compute PR_1, PR_2,...,PR_s or, alternatively, R_1Q, R_2Q,...,R_sQ, where P, Q and R_i for $i = 1,2,\ldots,s$ denote polynomials, computed in the nodes just below our level.

Note, that we have not bounded the number of gates in the arithmetic circuit, just the number of levels containing multiplications and the structure within the levels.

Lemma 4 *Any multi-linear polynomial with n variables is a depth-$(n-1)$ polynomial.*

Proof: We prove by induction. Our induction hypothesis is the following: If $P(x_1,x_2,\ldots,x_n)$ is a multi-linear polynomial of n variables, then it can be computed by an arithmetic circuit of Definition 3 such that on the first (lowest) multiplication level the common multiplier is x_2, on the second multiplication level the common multiplier is x_3, ..., on the $n-1$st multiplication-level the common multiplier is x_n.

The base case is obvious. The induction step: If $P(x_1,x_2,\ldots,x_n)$ is a multi-linear polynomial, then $P = x_nQ + R$ where Q and R are multi-linear polynomials of variables $x_1,x_2,\ldots,x_{n-1}$. Consequently, for Q and R the induction hypothesis is satisfied with depth $n-2$, so we are done. □

We remark, that linear polynomials are depth-0 polynomials. Polynomial

$$(x_1+x_2+x_3+x_4+x_5)(x_2+x_4+x_5)^2(x_3+x_5+2)+(x_2+x_4+x_5)(x_3+x_1+x_5)+12$$

is a depth-2 polynomial.

Definition 5 *Let p and q be two different primes, and let d be a non-negative integer. Then*

$$(\mathrm{MOD}_q, \mathrm{MOD}_p; \mathrm{depth} - d)$$

denotes a $(\mathrm{MOD}_q, \mathrm{MOD}_p)$ circuit, where the input of each MOD_p*-gate is a depth-d polynomial.*

3 The Degree-Decreasing Lemma

The following lemma is our main tool. It exploits a surprising property of $(\mathrm{MOD}_p, \mathrm{MOD}_q)$-circuits, which lacks in $(\mathrm{MOD}_p, \mathrm{MOD}_p)$ circuits, since constant-depth circuits with MOD_p gates are capable only to compute a constant degree polynomial of the inputs, and this constant depends on the depth, and not on the size.

Remark 1. Generally, the inputs of the modular gates are Boolean variables. Here, however, for wider applicability of the lemma, we allow input x for a general MOD_m gate to be chosen from set $\{0,1,\dots,m-1\}$. This will allow us to substitute polynomials into the variables of the lemma.

Remark 2. The output of the general MOD_m gates depend only on the sum of the inputs. In the next lemma it will be more convenient to denote $\mathrm{MOD}_m^A(y_1,y_2,\dots,y_\ell)$ *i.e.,* gate MOD_m^A with inputs $y_1,y_2,\dots,y_\ell$, by $\mathrm{MOD}_m^A(y_1+y_2+\cdots+y_\ell)$.

Lemma 6 *(Degree Decreasing Lemma) Let p and q be different primes, and let x_1,x_2,x_3 be variables with values from $\{0,1,\dots,p-1\}$. Then*

$$\mathrm{MOD}_q^B(\mathrm{MOD}_p^A(x_1x_2+x_3)) = \mathrm{MOD}_q^B(H_0+H_1+\cdots+H_{p-1}+\beta),$$

where H_i abbreviates

$$H_i = \alpha\sum_{j=0}^{p-1}\mathrm{MOD}_p^A(ix_2+x_3+j(x_1-i))$$

for $i=0,1,\dots,p-1$, where α is the multiplicative inverse of p modulo q: $\alpha p \equiv 1 \pmod q$, and β is a positive integer satisfying $\beta = -|A|(p-1)\alpha \bmod q$.

In the special case of $(\mathrm{MOD}_3, \mathrm{MOD}_2^{\{1\}})$ circuit, the statement of Lemma 6 is illustrated on Figure 1.

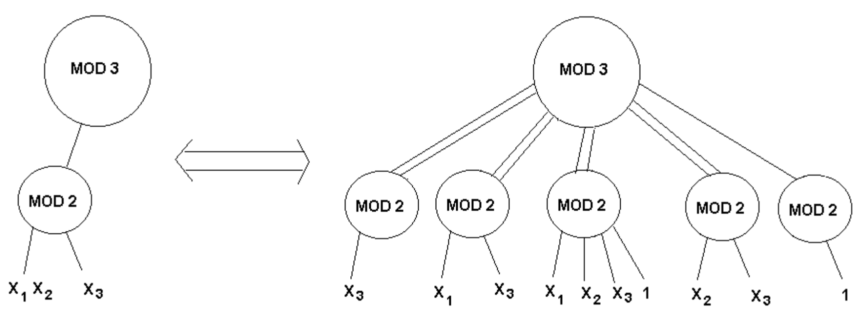

Fig. 1: Degree-decreasing in the $(\mathrm{MOD}_3, \mathrm{MOD}_2^{\{1\}})$ case: on the left the input is a degree-2 polynomial, on the right the inputs are linear polynomials.

Proof: Let $x_1 = k$ and let $0 \le i \le p-1,\ k \ne i$. Then

$$H_k = \alpha \sum_{j=0}^{p-1} \mathrm{MOD}_p^A(kx_2+x_3) = \alpha p \mathrm{MOD}_p^A(kx_2+x_3) \equiv \mathrm{MOD}_p^A(x_1x_2+x_3) \pmod q,$$

and

$$H_i = \alpha \sum_{j=0}^{p-1} \mathrm{MOD}_p^A(ix_2+x_3+j(k-i)) = \alpha|A|,$$

since for any fixed x_2, x_3, i, k expression $ix_2+x_3+j(k-i)$ takes on every value exactly once modulo p while $j = 0, 1, \ldots, p-1$; so $\mathrm{MOD}_p^A(ix_2+x_3+j(k-i))$ equals to 1 exactly $|A|$ times. Consequently,

$$\begin{aligned}\mathrm{MOD}_q^B(H_0+H_1+\cdots+H_{p-1}+\beta) &= \mathrm{MOD}_q^B(\mathrm{MOD}_p^A(x_1x_2+x_3)+(p-1)\alpha|A|+\beta)\\ &= \mathrm{MOD}_q^B(\mathrm{MOD}_p^A(x_1x_2+x_3)).\end{aligned}$$

□

4 Applications of the Degree Decreasing Lemma

The following theorem facilitates the applications of the Degree Decreasing Lemma:

Theorem 7 *Suppose, that function* $f : \{0,1\}^n \to \{0,1\}$ *can be computed by a* $(\mathrm{MOD}_q^B, \mathrm{MOD}_p^A; \mathrm{depth}-d)$ *circuit of size s, where p and q are two different primes, and d is a non-negative integer. Then f can also be computed by a* $(\mathrm{MOD}_q^B, \mathrm{MOD}_p^A; 1)$ *circuit of size*

$$(p^{2d}+1)s.$$

Proof:

We first show, that our $(\mathrm{MOD}_q^B, \mathrm{MOD}_p^A; \mathrm{depth}-d)$ circuit of size s can be converted into a $(\mathrm{MOD}_q^B, \mathrm{MOD}_p^A; \mathrm{depth}-(d-1))$ circuit of size at most p^2s+1. Repeating this conversion $d-2$ times, the statement follows.

We know that the input of every MOD_p^A-gate can be constructed with at most d multiplications in an arithmetic circuit. Let us consider a fixed MOD_p^A-gate. Suppose, that the last multiplication, which computes its input-polynomial is $PQ+R$, where P, Q, R are depth-$(d-1)$ multi-linear polynomials of n variables. This MOD_p^A-gate, using the Degree Decreasing Lemma (Lemma 6), can be converted to at most p^2 MOD_p^A-gates, each with depth-$(d-1)$ polynomials as inputs, plus (possibly) a leftover MOD_p^A-gate with input 1 (which may be connected to the MOD_q^B gate with multiple wires) such that the sum of these gates give the same output modulo q as the original one. If the conversion is done for all MOD_p^A-gates, the result is a $(\mathrm{MOD}_q^B, \mathrm{MOD}_p^A; \mathrm{depth}-(d-1))$ circuit of size at most p^2s+1, since the "leftover" MOD_p^A-gate with input 1 should be counted once. □

4.1 Constant Degree Hypothesis

Barrington, Straubing and Thérien in [3] conjectured that any $(\mathrm{MOD}_q^B, \mathrm{MOD}_p^A; d)$ circuit needs exponential size to compute the fan-in n AND function. They called it the *Constant Degree Hypothesis* (CDH), and proved the $d = 1$ case, with group-theoretic techniques.

Yan and Parberry [21] – using Fourier-analysis – proved also the $d = 1$ case for $(\mathrm{MOD}_q^{\{1,2,\ldots,q-1\}}, \mathrm{MOD}_2^{\{1\}}; 1)$ circuits, but their method also works for the special case of the CDH where the sum of the degrees of the monomials g_i on the input-level satisfies:

$$\sum_{\deg(g_i)\geq 1} (\deg(g_i) - 1) \leq \frac{n}{2(q-1)} - O(1).$$

Our Theorem 7 yields the following generalization of this result:

Theorem 8 *For any prime p there exists a constant* $0 < c_p < 1$, *such that for any* $0 < c < c_p$ *there exists a* $0 < c' < 1$, *such that if a* $(\mathrm{MOD}_q^B, \mathrm{MOD}_p^A, \mathrm{depth} - \lfloor cn \rfloor)$ *circuit computes the n-fan-in AND function, then its size is at least* $2^{c'n}$.

Proof: From the result of [3] and from Theorem 7 the statement is immediate. □

We should add, that Theorem 8 does not imply the CDH, but it greatly generalizes the lower bounds of [21] and of [3], and it works not only for the constant degree, but degree-*cn* polynomials as well.

Corollary 9 *For any prime p there exists a constant* $0 < c_p < 1$, *such that for any* $0 < c < c_p$ *there exists a* $0 < c' < 1$, *such that if the fan-in n AND function is computed by a circuit with a* MOD_q^B *gate at the top,* MOD_p^A *gates at the next level, where the input of each* MOD_p^A *gate is* an arbitrary integer-valued function *of cn variables plus an arbitrary linear polynomial of n variables, then the circuit must contain at least* $2^{c'n}$ MOD_p^A *gates.*

Proof: First we convert the integer-valued function of *cn* variables into a polynomial over GF(p), for each MOD_p^A gates. These polynomials have degree at most *cn*, and depend on at most *cn* variables. Consequently, the circuit is a $(\mathrm{MOD}_q^B, \mathrm{MOD}_p^A, \mathrm{depth} - (\lfloor cn \rfloor - 1))$ circuit, and Theorem 8 applies. □

We should mention, that Corollary 9 is much stronger than Yan and Parberry's result [21], since here the degree-sum of the inputs of each MOD_p^A gate can be even exponentially large in n, *vs.* the small linear upper bound of [21].

4.2 The ID function

Krause and Waack [12], using communication-complexity techniques, showed that any $(\mathrm{MOD}_m^{\{1,2,\ldots,m-1\}}, \mathrm{SYMMETRIC}; 1)$ circuit, computing the ID function:

$$\mathrm{ID}(x,y) = \begin{cases} 1, & \text{if } x = y, \\ 0 & \text{otherwise,} \end{cases}$$

for $x, y \in \{0,1\}^n$, should have size at least $2^n / \log m$, where SYMMETRIC is a gate, computing an arbitrary symmetric Boolean function.

Using this result, we prove:

Theorem 10 *Let p and q be two different primes. If a*

$$(\mathrm{MOD}_q^{\{1,2,\ldots,m-1\}}, \mathrm{MOD}_p^A, \mathrm{depth} - \lfloor (1-\varepsilon)n \rfloor)$$

circuit computes the $2n$-fan-in ID *function, then its size is at least $2^{c\varepsilon n}$, where $0 < c < 1$ depends only on p.*

Proof: From the result of [12] and from Theorem 7 the statement is immediate. □

Unfortunately, the methods of [12] do not generalize for MOD_q^B gates with unrestricted B's.

4.3 The MOD_r function

Krause and Pudlák [11] proved that any $(\mathrm{MOD}_{p^k}^{\{0\}}, \mathrm{MOD}_q^{\{0\}}; 1)$ circuit which computes the $\mathrm{MOD}_r^{\{0\}}$ function has size at least $2^{c''n}$, for some $c'' > 0$, where p, q and r are different primes. We also generalize this result as follows:

Theorem 11 *There exist $0 < c' < c < 1$ for different primes p, q, r, and positive integer k, if circuit $(\mathrm{MOD}_{p^k}^{\{0\}}, \mathrm{MOD}_q^{\{0\}}; \mathrm{depth} - \lfloor cn \rfloor)$ computes $\mathrm{MOD}_r^{\{0\}}(x_1, x_2, \ldots, x_n)$, then its size is at least $2^{c'n}$.*

Proof: From the result of [11] and from Theorem 7 the statement is immediate. □

Acknowledgment. The author is indebted to Dániel Varga, Katalin Friedl, Zoltán Király, and Gábor Tardos for fruitful discussions on this work. Supported in part by grants OTKA T030059, FKFP 0607/1999.

References

[1] M. Ajtai. Σ_1^1 formulae on finite structures. *Annals of Pure and Applied Logic*, 24:1–48, 1983.

[2] D. A. M. Barrington, R. Beigel, and S. Rudich. Representing Boolean functions as polynomials modulo composite numbers. *Comput. Complexity*, 4:367–382, 1994. Appeared also in *Proc. 24th Ann. ACM Symp. Theor. Comput.*, 1992.

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

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

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

[6] V. Grolmusz. A weight-size trade-off for circuits with mod m gates. In *Proc. 26th Ann. ACM Symp. Theor. Comput.*, pages 68–74, 1994.

[7] V. Grolmusz. On the weak mod m representation of Boolean functions. *Chicago Journal of Theoretical Computer Science*, 1995(2), July 1995.

[8] V. Grolmusz. Separating the communication complexities of MOD m and MOD p circuits. *J. Comput. System Sci.*, 51(2):307–313, 1995. also in Proc. 33rd Ann. IEEE Symp. Found. Comput. Sci., 1992, pp. 278–287.

[9] J. Håstad. Almost optimal lower bounds for small depth circuits. In *Proc. 18th Ann. ACM Symp. Theor. Comput.*, pages 6–20, 1986.

[10] J. Kahn and R. Meshulam. On mod p transversals. *Combinatorica*, 10(1):17–22, 1991.

[11] M. Krause and P. Pudlák. On the computational power of depth 2 circuits with threshold and modulo gates. In *Proc. 26th Ann. ACM Symp. Theor. Comput.*, 1994.

[12] M. Krause and S. Waack. Variation ranks of communication matrices and lower bounds for depth-two circuits having nearly symmetric gates with unbounded fan-in. *Mathematical Systems Theory*, 28(6):553–564, Nov./Dec. 1995.

[13] A. Razborov. Lower bounds for the monotone complexity of some Boolean functions. *Sov. Math. Dokl.*, 31:354–357, 1985.

[14] A. Razborov. Lower bounds on the size of bounded depth networks over a complete basis with logical addition, (in Russian). *Mat. Zametki*, 41:598–607, 1987.

[15] R. Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proc. 19th Ann. ACM Symp. Theor. Comput.*, pages 77–82, 1987.

[16] R. Smolensky. On interpolation by analytic functions with special properties and some weak lower bounds on the size of circuits with symmetric gates. In *Proc. 31st Ann. IEEE Symp. Found. Comput. Sci.*, pages 628–631, 1990.

[17] M. Szegedy. Functions with bounded symmetric communication complexity and circuits with MOD m gates. In *Proc. 22nd ANN. ACM SYMP. THEOR. COMPUT.*,, pages 278–286, 1990.

[18] G. Tardos and D. A. M. Barrington. A lower bound on the MOD 6 degree of the OR function. *Comput. Complex.*, 7:99–108, 1998.

[19] S. Toda. PP is as hard as the polynomial-time hierarchy. *SIAM J. Computing*, 20:865–877, 1991.

[20] J. van Leeuwen, editor. *Handbook of Theoretical Computer Science*, volume A, chapter 14. The complexity of finite functions, by R.B. Boppana and M. Sipser. Elsevier-MIT Press, 1990.

[21] P. Yan and I. Parberry. Exponential size lower bounds for some depth three circuits. *Information and Computation*, 112:117–130, 1994.

[22] A. C. Yao. Separating the polynomial-time hierarchy by oracles. In *Proc. 26th Ann. IEEE Symp. Found. Comput. Sci.*, pages 1–10, 1985.

[23] A. C. Yao. On ACC and threshold circuits. In *Proc. 31st Ann. IEEE Symp. Found. Comput. Sci.*, pages 619–627, 1990.