Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 52 (2002)

Computing Elementary Symmetric Polynomials with a Sub-Polynomial Number of Multiplications

Preliminary Version

Vince Grolmusz *

Abstract

Elementary symmetric polynomials S_n^k are used as a benchmark for the bounded-depth arithmetic circuit model of computation. In this work we prove that for constant k's, S_n^k modulo composite numbers $m = p_1p_2$ can be computed by homogeneous circuits with much fewer multiplications than over any field, if the coefficients of monomials $x_{i_1}x_{i_2}\cdots x_{i_k}$ are allowed to be 1 either mod p_1 or mod p_2 but not necessarily both. More exactly, we prove that for any constant k such a representation of S_n^k can be computed modulo p_1p_2 using only $\exp(O(\sqrt{\log n}\log\log n))$ multiplications on the most restricted depth-3 arithmetic circuits, for $\min(p_1,p_2) > k!$. Moreover, the number of multiplications remain sublinear while $k = O(\log\log n)$. In contrast, the well-known Graham-Pollack bound yields an $n-1$ lower bound for the number of multiplications even for the second elementary symmetric polynomial S_n^2. Our results generalize for other non-prime power composite moduli as well. The proof uses perfect hashing functions and the famous BBR-polynomial of Barrington, Beigel and Rudich.

1 Introduction

Surprising ideas sometimes lead to considerable improvements in algorithms even for the simplest computational tasks, let us mention here the integer-multiplication algorithm of Karatsuba and Ofman [16] and the matrix-multiplication algorithm of Strassen [25].

A new field with surprising algorithms is quantum computing. The most famous and celebrated results are Shor's algorithm for integer factorization [22] and Grover's database-search algorithm [14].

Since realizable quantum computers can handle only very few bits today, there are no practical applications of these fascinating quantum algorithms.

Computations involving composite, non-prime-power moduli (say, 6), on the other hand, can actually be performed on any desktop PC, but, unfortunately, we have only little evidence on the power or applicability of computations modulo composite numbers (see, e.g., the circuit given by Kahn and Meshulam [15], or the low-degree polynomial of Barrington, Beigel and Rudich [3]).

One of the problems here is the interpretation of the output of the computation. Several functions are known to be hard if computed modulo a prime. If we compute the same

*Department of Computer Science, Eötvös University, Budapest, Pázmány P. stny. 1/C, H-1117 Budapest, Hungary; E-mail: grolmusz@cs.elte.hu. The first version of this work appeared as an arXiv preprint on July 3, 2002, with number cs.CC/0207009 at http://arxiv.org/abs/cs.CC/0207009.

ISSN 1433-8092

function f with 0-1 values modulo 6, then it will also be computed modulo - say - 3, since $f(x) \equiv 1 \pmod 6 \Longrightarrow f(x) \equiv 1 \pmod 3$ and $f(x) \equiv 0 \pmod 6 \Longrightarrow f(x) \equiv 0 \pmod 3$, consequently, computing f this way cannot be easier mod 6 than mod 3. This difficulty is circumvented in a certain sense by the definition of the weak representation of Boolean functions by mod 6 polynomials, defined in [26] and [3].

We will consider here another interpretation of the output, called a-strong representation (Definition 2). This definition will be more suitable for computations, where the output is a polynomial and not just a number.

Our goal is to compute elementary symmetric polynomials

$$S_n^k = \sum_{\substack{I \subset \{1,2,\ldots,n\} \\ |I|=k}} \prod_{i \in I} x_i \tag{1}$$

modulo non-prime-power composite numbers with a much smaller number of multiplications than it is possible over rationals or prime moduli.

Our model of computation is the arithmetic circuit model of depth 3, circuits in this model are often called $\Sigma\Pi\Sigma$ circuits [18], [23].

$\Sigma\Pi\Sigma$ circuits perform computations of the following form:

$$\sum_{i=1}^{r} \prod_{j=1}^{s_i} (a_{ij1}x_1 + a_{ij2}x_2 + \cdots + a_{ijn}x_n + b_{ij}).$$

If all the $b_{ij} = 0$ and all the s_i's are the same number, then the circuit is called a homogeneous circuit, otherwise it is inhomogeneous. The size of the circuit is the number of gates in it: $1 + r + \sum_{i=1}^{r} s_i$.

A special class of homogeneous $\Sigma\Pi\Sigma$ circuits is called in [18] *the graph model*: here all $s_i = 2$ and all $a_{ij\ell}$ coefficients are equal to 1, and, moreover, the clauses of a product cannot contain the same variable twice. Consequently, such a product corresponds to a complete bipartite graph on the variables as vertices.

Graham and Pollack [6] asked that how many edge-disjoint bipartite graphs can cover the edges of an n-vertex complete graph. They proved that $n-1$ bipartite graphs are sufficient and necessary. Later, Tverberg gave a very nice proof for this statement [28]. Having relaxed the disjointness-property, Babai and Frankl [2] asked that what is the minimum number of bipartite-graphs, which covers every edge of an n-vertex complete graph by an odd multiplicity. Babai and Frankl proved that $(n-1)/2$ bipartite graphs are necessary. The optimum upper bound for the odd-cover was proved by Radhakrishnan, Sen and Vishwanathan [18]. Radhakrishnan, Sen and Vishwanathan also gave matching upper bounds for covers, when the off-diagonal elements of matrix M are covered by multiplicity 1 modulo a prime.

By a result of Ben-Or [23], every elementary symmetric polynomial S_n^k can be computed over fields by size-$O(n^2)$ inhomogeneous $\Sigma\Pi\Sigma$ circuits, using one-variable polynomial interpolation. This result shows the power of arithmetic circuits over Boolean circuits with MOD p gates, since as it was proved by Razborov [21] and Smolensky [24] that MAJORITY – a symmetric function – needs exponential size to be computed on any bounded-depth Boolean circuit.

Note, that our construction with homogeneous circuits modulo non-prime-power composites beats Ben-Or's bound for k's less than $c \log\log n$ (for some positive c's).

Nisan and Wigderson [17] showed that any homogeneous $\Sigma\Pi\Sigma$ circuit needs size $\Omega((n/2k)^{k/2})$ for computing S_n^k. This result shows that the homogeneous circuits are much weaker in computing elementary symmetric polynomials than the inhomogeneous ones. Nisan and Wigderson also examined bilinear and multi-linear circuits in [17]. Note that the circuits in our constructions for $S_n^2(x,y)$ and for $S_n^k(x^1,x^2,\ldots,x^k)$ are also multi-linear circuits.

We should note, that exponential lower bounds were proved recently for simple functions for $\Sigma\Pi\Sigma$ circuits by Grigoriev and Razborov [8] and by Grigoriev and Karpinski [7].

Most recently, Raz and Shpilka got nice lower bound results for arithmetic circuits [20], and Raz [19] proved a $\Omega(n^2\log n)$ lower bound for matrix-multiplication in the model where the constants in the arithmetic circuits are bounded, solving a long-standing open problem.

1.1 Alternative strong representation of polynomials

S_n^k can be naturally computed by $\binom{n}{k}$ product-gates by a homogeneous $\Sigma\Pi\Sigma$ circuit over any ring by the circuit of (1). One can save a little bit from the cost of this obvious construction (e.g., for $k=2$ $n-1$ multiplications instead of $\binom{n}{2}$ is enough), but, as we already mentioned, by the result of Nisan and Wigderson [17], size $\Omega((n/2k)^{k/2})$ is needed to compute S_n^k on homogeneous $\Sigma\Pi\Sigma$ circuits.

It is quite plausible to think that if we change the non-zero coefficients of the monomials of S_n^k to some other non-zero coefficients, then the computational complexity of this modified polynomial will not be changed much: simply because even in the modified polynomial we should still need to generate the monomials with the non-zero coefficients somehow.

This intuition is verified by the next lemma (proven in the last section), in the case of finite fields:

Lemma 1 *Suppose that a homogeneous $\Sigma\Pi\Sigma$ circuit computes polynomial*

$$g(x)=\sum_{\substack{I\subset\{1,2,\ldots,n\}\\|I|=k}} a_I\prod_{i\in I}x_i$$

over the q element field F_q with u gates, where $a_I\neq 0$ in F_q. Then S_n^k can be computed by a $\Sigma\Pi\Sigma$ circuit of size $O(u^{q-1})$.

From this lemma and from the $\Omega((n/2k)^{k/2})$-lower bound of Nisan and Wigderson [17] it is obvious that computing g over finite fields needs

$$\Omega((n/2k)^{\frac{k}{2(q-1)}})$$

multiplication gates.

Consequently, we cannot save much by computing g instead of S_n^k: if computing S_n^k needs polynomially many gates in n, then computing g still needs polynomially many gates in n (for any constant k).

Our main result is, however, that we *can save* much by computing certain strong representations of the elementary symmetric polynomials – say – over the modulo 15 integers, Z_{15}. More exactly, such representations can be computed by $\Sigma\Pi\Sigma$ circuits containing sub-polynomially many multiplication gates; (We call a function $h(n)$ sub-polynomial, if for all $\varepsilon>0$: $h(n)=O(n^{\varepsilon})$.)

Several authors (e.g., [26], [3]) defined the weak and strong representations of Boolean functions for integer moduli. Here we need the definition of a sort of strong representation of polynomials modulo composite numbers. We call this representation *alternative-strong* representation, abbreviated *a-strong representation*:

Definition 2 *Let m be a composite number $m = p_1^{e_1} p_2^{e_2} \cdots p_\ell^{e_\ell}$. Let Z_m denote the ring of modulo m integers. Let f be a polynomial of n variables over Z_m:*

$$f(x_1, x_2, \dots, x_n) = \sum_{I \subset \{1,2,\dots,n\}} a_I x_I,$$

where $a_I \in Z_m$, $x_I = \prod_{i \in I} x_i$. Then we say that

$$g(x_1, x_2, \dots, x_n) = \sum_{I \subset \{1,2,\dots,n\}} b_I x_I,$$

is an a-strong representation *of f modulo m, if*

$$\forall I \subset \{1, 2, \dots, n\} \;\; \exists j \in \{1, 2, \dots, \ell\}: \quad a_I \equiv b_I \pmod{p_j^{e_j}},$$

and if for some i, $a_I \not\equiv b_I \pmod{p_i^{e_i}}$, then $b_I \equiv 0 \pmod{p_i^{e_i}}$.

Example 3 *Let $m = 6$, and let $f(x_1, x_2, x_3) = x_1x_2 + x_2x_3 + x_1x_3$, then $g(x_1, x_2, , x_3) = 3x_1x_2 + 4x_2x_3 + x_1x_3$ is an a-strong representation of f modulo 6.*

Note, that the requirements in Definition 2 are stronger than the requirements for f in Lemma 1. Note also, that the earlier (strong-, weak-) representations of functions contained constraints for the *value* of certain functions. Now we are requiring that the *form* of the representation satisfy modular constraints.

Our goal in this work is to show that the elementary symmetric polynomials have a-strong representations modulo composites which can be computed by much smaller homogeneous $\Sigma\Pi\Sigma$ arithmetic circuits than the original polynomial.

Unfortunately, we cannot hope for such results for all multivariate polynomials, as it is shown by the next Theorem:

Theorem 4 *Let*

$$f(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n) = \sum_{i=1}^{n} x_i y_i$$

the inner product function. Suppose that a $\Sigma\Pi\Sigma$ circuit computes an a-strong representation of f modulo 6. Then the circuit must have at least $\Omega(n)$ multiplication gates.

Proof: Let g be the a-strong representation of f. Then in g, at least the half of monomials $x_i y_i$ has coefficients equal to 1 modulo either 2 or 3. Without restricting the generality, let us assume that monomials $x_1y_1, x_2y_2, \dots, x_{\lceil n/2 \rceil} y_{\lceil n/2 \rceil}$ have coefficients 1 modulo 3. When we compute g modulo 6 we will learn also the inner product of two vectors modulo 3, each consisting of the first $\lceil n/2 \rceil$ variables. It is well known that the communication complexity of computing the inner product mod 3 is $\Omega(n)$ (see e.g., [9]).

Since arithmetic $\Sigma\Pi\Sigma$ circuits modulo 6 with u multiplication-gates of in-degree 2 can be evaluated by a 2-party communication protocol using only $O(u)$ bits, we get: $u = \Omega(n)$. $\Box$

2 Our Constructions

First we construct a-strong representations with a small number of multiplications for the following polynomial:

$$S_n^2(x,y) = \sum_{\substack{i,j\in\{1,2,\ldots,n\}\\ i\neq j}} x_i y_j,$$

and for $x = y$ we will get that $2S_n^2(x) = S_n^2(x,x)$, and this will imply our result for any composite, odd, non-prime-power moduli m:

Theorem 5 *(i) Let $m = p_1p_2$, where $p_1 \neq p_2$ are primes. Then an a-strong representation of $S_n^2(x,y)$ modulo m:*

$$\sum_{\substack{i,j\in\{1,2,\ldots,n\}\\ i\neq j}} a_{ij} x_i y_j \tag{2}$$

can be computed on a homogeneous $\Sigma\Pi\Sigma$ circuit of size

$$\exp(O(\sqrt{\log n \log\log n})).$$

Moreover, this representation satisfies that $\forall i \neq j : a_{ij} = a_{ji}$.

(ii) Let the prime decomposition of $m = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$. Then an a-strong representation of $S_n^2(x,y)$ modulo m of the form (2) can be computed on a homogeneous $\Sigma\Pi\Sigma$ circuit of size

$$\exp\left(O\left(\sqrt[r]{\log n(\log\log n)^{r-1}}\right)\right).$$

Moreover, this representation satisfies that $\forall i \neq j : a_{ij} = a_{ji}$.

Corollary 6 *(i) Let $m = p_1p_2$, where $p_1 \neq p_2$ are odd primes. Then an a-strong representation of the second elementary symmetric polynomial $S_n^2(x)$ modulo m can be computed on a homogeneous $\Sigma\Pi\Sigma$ circuit of size*

$$\exp(O(\sqrt{\log n \log\log n})).$$

(ii) Let the prime decomposition of the odd m be $m = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$. Then an a-strong representation of the second elementary symmetric polynomial $S_n^2(x)$ modulo m can be computed on a homogeneous $\Sigma\Pi\Sigma$ circuit of size

$$\exp\left(O\left(\sqrt[r]{\log n(\log\log n)^{r-1}}\right)\right).$$

Since the $\Sigma\Pi\Sigma$ circuit in our construction correspond to the graph-model [18], we have the following graph-theoretical corollary, showing a cover with much fewer bipartite graphs than in the linear lower bound of Graham and Pollack:

Corollary 7 *For any $m = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$, there exists an explicitly constructible bipartite cover of the edges of the complete n-vertex-graph, such that for all edges e there exists an $i : 1 \leq i \leq r$, that the number of the bipartite graphs, covering e is congruent to 1 modulo $p_i^{e_i}$. Moreover, the total number of the bipartite graphs in the cover is*

$$\exp\left(O\left(\sqrt[r]{\log n(\log\log n)^{r-1}}\right)\right).$$

2.1 Our results for larger k's

The following theorem gives our result for general k. Our goal is to compute an a-strong representation of polynomials $S_n^k(x)$ for $n \geq k \geq 2$. Let us first define

$$S_n^k(x^{(1)}, x^{(2)}, \ldots, x^{(k)}) = \sum_{i_1, i_2, \ldots, i_k} x_{i_1}^{(1)} x_{i_2}^{(2)} \cdots x_{i_k}^{(k)},$$

where the summation is done for all $k!$ orders of all k-element-subsets $I = \{i_1, i_2, \ldots, i_k\}$ of $\{1, 2, \ldots, n\}$, and $x^{(j)} = (x_1^{(j)}, x_2^{(j)}, \ldots, x_n^{(j)})$, for $j = 1, 2, \ldots, k$.

Theorem 8 *Let $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$. Then an a-strong representation of $S_n^k(x^{(1)}, x^{(2)}, \ldots, x^{(k)})$ modulo m,*

$$\sum_{i_1, i_2, \ldots, i_k} a_{i_1, i_2, \ldots, i_k} x_{i_1}^{(1)} x_{i_2}^{(2)} \cdots x_{i_k}^{(k)},$$

can be computed on a homogeneous multi-linear $\Sigma\Pi\Sigma$ circuit of size

$$\exp\left(\exp(O(k)) \sqrt[r]{\log n} \log\log n\right).$$

Moreover, coefficients $a_{i_1, i_2, \ldots, i_k}$ depends only on set $a\{i_1, i_2, \ldots, i_k\}$, and not on the particular order of indices $i_1, i_2, \ldots, i_k$.

Note, that this circuit-size is sub-polynomial in n for any constant k and for large enough n. Moreover, the sub-polynomiality holds while $k < c \log\log n$, for a small enough $c > 0$.

For moduli m, relative prime to $k!$, this implies:

Corollary 9 *If m is relative prime to $k!$, then an a-strong representation of $S_n^k(x)$ modulo m can be computed on a homogeneous $\Sigma\Pi\Sigma$ circuit of size*

$$\exp\left(\exp(O(k)) \sqrt[r]{\log n} \log\log n\right).$$

2.2 The construction for computing S_n^2

Proof of Theorem 5:

We prove the more general case (ii) of the Theorem.

Note, that $S_n^2(x, y)$ contains the sum of the monomials $x_i y_j$ for all $i \neq j$. Let us arrange these monomials as follows: Let the x_i's and y_j's be assigned to the rows and columns of an $n \times n$ matrix M, respectively, and let the position in row i and column j contain monomial $x_i y_j$:

$$M = \begin{array}{c} \\ x_1 \\ x_2 \\ \vdots \\ x_n \end{array} \begin{array}{c} \begin{array}{cccc} y_1 & y_2 & \cdots & y_n \end{array} \\ \begin{pmatrix} x_1 y_1 & x_1 y_2 & \cdots & x_1 y_n \\ x_2 y_1 & x_2 y_2 & \cdots & x_2 y_n \\ \vdots & \vdots & \ddots & \vdots \\ x_n y_1 & x_n y_2 & \cdots & x_n y_n \end{pmatrix} \end{array} \tag{3}$$

Then any product of the form

$$(x_{i_1} + x_{i_2} + \cdots + x_{i_v})(y_{j_1} + y_{j_2} + \cdots + y_{j_w}) \tag{4}$$

naturally corresponds to a $v\times w$ submatrix of matrix M. We call these submatrices rectangles. Clearly, any a-strong representation modulo m of polynomial $S_n^2(x,y)$ can be got from a cover of matrix M by rectangles of the form (4), satisfying the following properties:
Property (a): The number of the rectangles covering any elements of the diagonal is a multiple of $m=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$;
Property (b): Any non-diagonal element x_iy_j of M is covered by d_{ij} rectangles, where

- there exists a $k\in\{1,2,\ldots,r\}$: $d_{ij}\equiv 1 \pmod{p_k}$ and either it is 0 or 1 mod p_2,
- for all $k\in\{1,2,\ldots,r\}$: $d_{ij}\equiv 0 \pmod{p_k}$ or $d_{ij}\equiv 1 \pmod{p_k}$.

Clearly, a (bilinear) $\Sigma\Pi\Sigma$ circuit compute an a-strong representation of polynomial $S_n^2(x,y)$ if and only if the corresponding rectangle-cover satisfies Properties (a) and (b). The construction of such a low-cardinality rectangle cover is implicit in papers [10] and [11]. We present here a short direct proof which is easily generalizable for proving the results in the next section for higher dimensional matrices.

Rectangles, covering M, will be denoted

$$R(I,J)=(\sum_{i\in I}x_i)(\sum_{j\in J}y_j).$$

We define now an initial cover of the non-diagonal elements of M by rectangles.

Let $N=\lceil\log n\rceil$, and for $1\le i,j\le n$, let $i=(i_1,i_2,\ldots,i_g)$ and $j=(j_1,j_2,\ldots,j_g)$ denote their N-ary forms (i.e., $0\le i_t,j_t\le N-1$, for $t=1,2,\ldots,g$, where $g=\lceil\log_N(n+1)\rceil$.)

Then let us define for $t=1,2,\ldots,g$ and $\ell=0,1,\ldots,N-1$:

$$I_t^\ell=\{i: i_t=\ell\},\quad J_t^\ell=\{j: j_t\ne\ell\}.$$

Now consider the cover given by the following rectangles:

$$R(I_t^\ell,J_t^\ell): t=1,2,\ldots,g,\ \ell=0,1,\ldots,N-1.$$

Now, in this cover, any element x_iy_j of M will be covered by $H_N(i,j)$-times, where $H_N(i,j)$ stands for the Hamming-distance of the N-ary forms of i and j, that is, at most g-times. Note, that the diagonal elements are not covered at all, so Property (a) is satisfied, while Property (b) is typically not. Moreover, x_iy_j is covered by the same number of rectangles as x_jy_i, that is, $H_N(i,j)$-times.

The total number of covering rectangles is $h=gN=O((N\log n)/\log N)$.

Now, our goal is to turn this cover to another one, which already satisfies not only Property (a), but also Property (b). For this transformation we need to apply a multivariate polynomial f to our rectangle-cover in a very similar way as we applied polynomials to set-systems in [12] and to codes in [13]:

Definition 10 *Let $R_1,R_2,\ldots,R_h$ be a rectangle-cover of a matrix $M=\{x_iy_j\}$, and let f be a h-variable multi-linear polynomial written in the following form:*

$$f(z_1,z_2,\ldots,z_h)=\sum_{K\subset\{1,2,\ldots,h\}}a_Kz_K,$$

where $0\le a_K\le m-1$ are integers, and $z_K=\prod_{k\in K}z_k$. Then the f-transformation of the rectangle-cover $R_1R_2,\ldots,R_h$ contains $\sum_{K\subset\{1,2,\ldots,h\}}a_K$ rectangles, each corresponding to a monomial of f. $z_K=\prod_{k\in K}z_k$ is corresponded to the (possibly empty) rectangle of $\bigcap_{k\in K}R_k$.

Note, that another way of interpreting this definition is as follows: the variables z_k correspond to the rectangles of the cover, and if we imagine the rectangles filled with 1's, then the product of the variables, i.e., the monomials, correspond to the Hadamard-product (see e.g., [12]) of the corresponding all-1 rectangles, resulting an all-1 rectangle, which, in turn, equals to their intersection.

Note also, that polynomial f is, in fact, considered over the ring Z_m, along with a fixed (small) representation of its coefficients from the set of non-negative integers.

Lemma 11 *Let $u^{ij} \in \{0,1\}^h$ characterize the rectangle-cover of the entry $x_i y_j$ of matrix M as follows:*

$$R_s \text{ covers } x_i y_j \iff u_s^{ij} = 1.$$

Then entry $x_i y_j$ is covered by exactly $f(u^{ij})$ rectangles from the f-transformation of the rectangle-cover $R_1, R_2, \ldots, R_h$

Proof: In $f(z)$, exactly those monomials z_K contributes 1 to the value of $f(u^{ij})$ whose variables are all-1 in vector u^{ij}. This happens exactly when $u_k^{ij} = 1$ for all $k \in K$, that is, $x_i y_j$ is covered by the intersection of rectangles $\bigcap_{k\in K} R_k$. □

The proof of the following lemma is obvious:

Lemma 12 *The intersection of finitely many rectangles is a (possibly empty) rectangle. Any rectangle, covering a part of matrix M of (3) corresponds to a single (bilinear) multiplication.*

□

It remains to prove that there exists an f, with a small number of monomials, and with properties which leads to a cover, satisfying Properties (a) and (b). We will use the famous BBR polynomial of Barrington, Beigel and Rudich [3]:

Theorem 13 (Barrington, Beigel, Rudich) *Let $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$. For any integers d, ℓ, $1 \leq d \leq \ell$ there exists an $f_{d,\ell}$ explicitly constructible, symmetric, ℓ-variable, degree-$O(d^{1/r})$ multilinear polynomial with coefficients from Z_m, such that*

(i) for any $z \in \{0,1\}^\ell$, which contains at most d 1's:

$$f_{d,\ell}(z) \equiv 0 \pmod{m} \iff z = 0,$$

(ii) If $f_{d,\ell}(z) \not\equiv 0 \pmod{m}$, then there exists $i \in \{1,2,\ldots,r\}$: $f_{d,\ell}(z) \equiv 1 \pmod{p_i^{e_i}}$, and if $f_{d,\ell}(z) \not\equiv 1 \pmod{p_j^{e_j}}$, then $f_{d,\ell}(z) \equiv 0 \pmod{p_j^{e_j}}$.

Proof: The proof of part (i) is given in [3] (see also [11]).
The proof of part (ii):

We consider $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ to be a constant. Let us define $q_i = m/p_i^{e_i}$, and let $q_i^{-1} q_i \equiv 1 \pmod{p_i^{e_i}}$, for $i = 1, 2, \ldots, r$.

Let w denote the (symmetric) polynomial satisfying the requirements of (i).

Suppose first that $e_k = 1$ for $k = 1, 2, \ldots, r$. Then

$$f_{d,\ell} = \sum_{i=1}^{r} q_i q_i^{-1} w^{p_i - 1}$$

is also symmetric, and clearly satisfies the requirements of (ii). Indeed, if $w(z) \not\equiv 0 \pmod{p_i}$, then $f_{d,\ell}(z) \equiv 1 \pmod{p_i}$, and if $w(z) \equiv 0 \pmod{p_i}$, then $f_{d,\ell}(z) \equiv 0 \pmod{p_i}$. Moreover, the degrees of $f_{d,\ell}$ and w differ only in a constant multiplier.

In general, let us first consider the polynomial w which satisfies (i) for modulus $m' = p_1 p_2 \cdots p_r$. From the results of Toda [27], Yao [29] and Beigel and Tarui [4], for every k there exist polynomials P_k of degree $O(k)$, satisfying

$$\begin{aligned} P_k(x) &\equiv 0 \pmod{x^k} \\ P_k(x+1) &\equiv 1 \pmod{x^k} \end{aligned}$$

Now, let us define

$$f_{d,\ell} = \sum_{i=1}^{r} q_i q_i^{-1} P_{e_i}(w^{p_i - 1}).$$

It is easy to verify that (ii) is satisfied for this polynomial, and the degree is still $O(d^{1/r})$. Moreover, $f_{d,\ell}$ is also symmetric.

□

Now we can prove Theorem 5; let us consider the more general statement of (ii). Let $\ell = h = gN$, $d = g$. Then $f_{g,gN}$ has

$$\binom{h}{O(g^{1/r})} \tag{5}$$

monomials. Consequently, if we transform our cardinality-h rectangle cover by Definition 10 with polynomial $f_{g,gN}$, then the resulting cover satisfies Properties (a) and (b) and has cardinality (5). This implies an $\exp(O(\sqrt[r]{\log n(\log\log n)^{r-1}}))$ cover. By Lemma 12, a $\Sigma\Pi\Sigma$ circuit is immediate with $\exp(O(\sqrt[r]{\log n(\log\log n)^{r-1}}))$ multiplication-gates. Since the original, cardinality-h rectangle cover covered $x_i y_j$ and $x_j y_i$ with the same number of rectangles, and since $f_{g,gN}$ is a symmetric polynomial, by Lemma 11 our transformed rectangle-cover will also cover $x_i y_j$ and $x_j y_i$ with the same number of rectangles. □

2.3 The construction in general

In this section we prove Theorem 8.

We describe a construction similarly as in the case $k = 2$.

Note, that in this section, instead of the more correct notation for vectors x with upper index u: $x^{(u)}$, we will write simply x^u.

First, let $M' = \{m_{i_1, i_2, \ldots, i_k}\}$ be a k-dimensional analogon of M of equation (3), that is, an $\overbrace{n \times n \times n \times \cdots \times n}^{k}$ matrix, where $m_{i_1, i_2, \ldots, i_k} = x^1_{i_1} x^2_{i_2} \cdots x^k_{i_k}$.

Now we should again construct a cover of M', this time with k-dimensional boxes, corresponding to k-linear products:

$$R(I_1, I_2, \ldots, I_k) = \prod_{i=1}^{k} \sum_{j \in I_i} x^i_j,$$

satisfying that only those entries will be covered, which have no two equal (lower) indices, and the covering multiplicity of these entries should be non-zero modulo m. Additionally, we also require that the covering multiplicity of entry $m_{i_1,i_2,\ldots,i_k}$ depend only on the set $\{i_1, i_2, \ldots, i_k\}$, and not on the particular order of the indices $i_1, i_2, \ldots, i_k$.

First we need to define an initial box-cover of those entries of the k-dimensional matrix M', which have no two identical indices.

For our proof it is very important, that this initial cover has low multiplicity: every covered element of M' should be covered only by $O(\log n)$ k-dimensional boxes for constant k's. The construction of such initial cover in the $k = 2$ case was quite easy, now we must use some more intricate approach.

Let us consider a family of perfect hash functions (see e.g., [5], or the work [1] for an explicit (i.e., de-randomized) construction), and let us list their respective values in the column of a matrix. This way, for integers n, k, b: $2 \le k \le b = O(k)$, $k \le n$, we can obtain a matrix $H(n,k,b) = \{h_{ij}\}$ with $u = \exp(O(k)) \log n$ rows and n columns, with entries from the set $\{0, 1, \ldots, b-1\}$, such that for any k-element subset J of the n columns, there exists a row $i : 1 \le i \le u$:

$$h_{ij} : j \in J$$

are pairwise different elements of the set $\{0, 1, \ldots, b-1\}$.

This matrix $H(n,k,b)$ will be used for the definition of our initial cover as follows:

For any $i : 1 \le i \le u$, and any $\sigma : \{1, 2, \ldots, k\} \to \{0, 1, \ldots, b-1\}$ injective function we define the k-dimensional box:

$$R(i,\sigma) = \{m_{j_1,j_2,\ldots,j_k} : h_{ij_1} = \sigma(1), h_{ij_2} = \sigma(2), \ldots, h_{ij_k} = \sigma(k)\}.$$

There are u possible i's and $k^{O(k)}$ possible σ's, so there are $k^{O(k)} \log n$ boxes in this cover. Box $R(i,\sigma)$ covers only $m_{j_1,j_2,\ldots,j_k}$'s with pairwise different indices.

It is important to note, that even for a fixed i, the covering multiplicities of the elements $m_{j_1,j_2,\ldots,j_k}$ and $m_{\pi(j_1)\pi(j_2)\ldots,\pi(j_k)}$ are the same for any permutations π of the numbers $\{j_1, j_2, \ldots, j_k\}$.

Any $m_{j_1,j_2,\ldots,j_k}$ with pairwise different indices is covered by exactly that many k-dimensional boxes from this cover, as the number of rows with pairwise different elements of the sub-matrix, containing column j_1, column j_2, ..., column j_k of matrix $H(n,k,b)$. This number is at least 1 (from the perfect-hashing property) and at most u (that is, the number of rows of $H(n,k,b)$).

Now, exactly as in the proof of the S_n^2 case, we would like to apply the polynomial $f_{d,\ell}$ of Theorem 13 with $d = u$, $\ell = k^{O(k)} \log n$, to this box-cover.

However, first we need to give the higher-dimension analogues of Definition 10 and Lemma 11:

Definition 14 *Let $R_1, R_2, \ldots, R_h$ be a box-cover of a matrix M', and let f be a h-variable multi-linear polynomial written in the following form:*

$$f(z_1, z_2, \ldots, z_h) = \sum_{K \subset \{1,2,\ldots,h\}} a_K z_K,$$

where $0 \le a_K \le m-1$ are integers, and $z_K = \prod_{k \in K} z_k$. Then the f-transformation of the box-cover $R_1 R_2, \ldots, R_h$ contains $\sum_{K \subset \{1,2,\ldots,h\}} a_K$ boxes, each corresponding to a monomial of f. $z_K = \prod_{k \in K} z_k$ is corresponded to the (possibly empty) box of $\bigcap_{k \in K} R_k$.

Lemma 15 *Let $u^{i_1,i_2,\ldots,i_k} \in \{0,1\}^h$ characterize the box-cover of the entry $m_{i_1,i_2,\ldots,i_k}$ of matrix M' as follows:*

$$R_s \text{ covers } m_{i_1,i_2,\ldots,i_k} \iff u_s^{i_1,i_2,\ldots,i_k} = 1.$$

Then entry $m_{i_1,i_2,\ldots,i_k} = x^1_{i_1} x^2_{i_2} \cdots x^k_{i_k}$ is covered by exactly $f(u^{i_1,i_2,\ldots,i_k})$ boxes from the f-transformation of the box-cover $R_1, R_2, \ldots, R_h$

Proof: In $f(z)$, exactly those monomials z_K contributes 1 to the value of $f(u^{i_1,i_2,\ldots,i_k})$ whose variables are all-1 in vector $u^{i_1,i_2,\ldots,i_k}$. This happens exactly when $u_s^{i_1,i_2,\ldots,i_k} = 1$ for all $s \in K$, that is, $m_{i_1,i_2,\ldots,i_k} = x^1_{i_1} x^2_{i_2} \cdots x^k_{i_k}$ is covered by the intersection of boxes $\bigcap_{k \in K} R_k$. □

Note, that for any symmetric polynomial f and any box-cover, which has covering multiplicity on $m_{i_1,i_2,\ldots,i_k}$, depending only on set $\{i_1, i_2, \ldots, i_k\}$, the f-transformation of the cover will also have the same multiplicity on $m_{j_1,j_2,\ldots,j_k}$ and on $m_{\pi(j_1)\pi(j_2)\ldots,\pi(j_k)}$ for any permutations π of the numbers $\{j_1, j_2, \ldots, j_k\}$.

The proof of the following lemma is obvious:

Lemma 16 *The intersection of finitely many boxes is a (possibly empty) box. Any box, covering a part of matrix M' corresponds to a single (multi-linear) product.*

□

The result of applying $f_{d,\ell}$ with $d = u$, $\ell = k^{O(k)} \log n$, to our initial box-cover of cardinality ℓ is a box-cover of cardinality

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

proving Theorem 8.□

2.4 The proof of Lemma 1

Let $R_1, R_2, \ldots, R_h$ be the covering boxes, defined by the homogeneous $\Sigma\Pi\Sigma$ circuit. Let us remark that every degree-k monomial $\prod_{i \in I} x_i$ with pairwise different indices are covered by $a_I \neq 0$ boxes in this cover. In F_q, for any non-zero element s, $s^{q-1} = 1$. Now, let us apply polynomial

$$f(z_1, z_2, \ldots, z_h) = (z_1 + z_2 + \cdots + z_h)^{q-1}$$

to the box-cover $R_1, R_2, \ldots, R_h$, according to Definition 14. Then, by Lemma 15, the covering multiplicity of the degree-k monomials $\prod_{i \in I} x_i$ with pairwise different indices will be 1 in F_q, while all the other's will remain 0. That is, the corresponding $\Sigma\Pi\Sigma$ circuit computes S_n^k over F_q.□

Acknowledgment.

The author is grateful for Gábor Tardos for discussions on the subject. The author also acknowledges the partial support of János Bolyai Fellowship, and research grants EU FP5 IST FET No. IST-2001-32012, OTKA T030059 and an ETIK grant.

References

[1] N. Alon and M. Naor. Derandomization, witnesses for Boolean matrix multiplication and construction of perfect hash functions. *Algorithmica*, 16(4-5):434–449, 1996.

[2] L. Babai and P. Frankl. *Linear algebra methods in combinatorics*. Department of Computer Science, The University of Chicago, September 1992. preliminary version.

[3] 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.

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

[5] M. L. Fredman and J. Komlós. On the size of separating systems and families of perfect hash functions. *Siam J. Alg. Disc. Meth.*, 5(1):61–68, March 1984.

[6] R. Graham and H. Pollak. On embedding graphs in squashed cubes. *Lecture Notes in Mathematics*, 303:99–110, 1972.

[7] D. Grigoriev and M. Karpinski. An exponential lower bound for depth 3 arithmetic circuits. In *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pages 577–582. ACM Press, 1998.

[8] D. Grigoriev and A. A. Razborov. Exponential lower bounds for depth 3 arithmetic circuits in algebras of functions over finite fields. *Applicable Algebra in Engineering, Communication and Computing*, 10(6):465–487, 2000.

[9] 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.

[10] V. Grolmusz. Low-rank co-diagonal matrices and Ramsey graphs. *The Electronic Journal of Combinatorics*, 7:R15, 2000. www.combinatorics.org.

[11] V. Grolmusz. Superpolynomial size set-systems with restricted intersections mod 6 and explicit Ramsey graphs. *Combinatorica*, 20:73–88, 2000.

[12] V. Grolmusz. Constructing set-systems with prescribed intersection sizes. Technical Report DIMACS TR 2001-03, DIMACS, January 2001. ftp://dimacs.rutgers.edu/pub/dimacs/TechnicalReports/TechReports/2001/2001-03.ps.gz, to appear in the Journal of Algorithms.

[13] V. Grolmusz. Pairs of codes with prescribed hamming distances and coincidences. Technical Report DIMACS TR 2002-9, DIMACS, February 2002.

[14] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219. ACM Press, 1996.

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

[16] A. Karatsuba and Y. Ofman. Multiplication of multidigit numbers on automata. *Sov. Phys.-Dokl. (Engl. transl.)*, 7(7):595–596, 1963.

[17] N. Nisan and A. Wigderson. Lower bounds on arithmetic circuits via partial derivatives. *Computational Complexity*, 6(3), 1997.

[18] J. Radhakrishnan, P. Sen, and S. Vishwanathan. Depth-3 arithmetic circuits for $s_n^2(x)$ and extensions of the Graham-Pollack theorem. In *LNCS 1974, Proceedings of FSTTCS, New Delhi, India, December 13-15, 2000.*, 2000.

[19] R. Raz. On the complexity of matrix product. In *Proceedings of the thirty-fourth annual ACM symposium on Theory of computing.* ACM Press, 2002.

[20] R. Raz and A. Shpilka. Lower bounds for matrix product, in bounded depth circuits with arbitrary gates. In *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pages 409–418. ACM Press, 2001.

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

[22] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[23] A. Shpilka. PhD. Thesis, Hebrew University 2001. http://www.cs.huji.ac.il/~amirs/publications/my_main.ps.gz.

[24] 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.

[25] V. Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13:354–356, 1969.

[26] 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.

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

[28] H. Tverberg. On the decomposition of K_n into complete bipartite graphs. *Journal of Graph Theory*, 6:493–494, 1982.

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

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'