Electronic Colloquium on Computational Complexity, Report No. 74 (2003)

Sixtors and Mod 6 Computations

Vince Grolmusz *

Abstract

We consider the following phenomenon: with just one multiplication we can compute $(3u+2v)(3x+2y) \equiv 3ux+4vy \pmod 6$, while computing the same polynomial modulo 5 needs 2 multiplications. We generalize this observation and we define some vectors, called sixtors, with remarkable zero-divisor properties. Using sixtors, we also generalize our earlier result (Computing Elementary Symmetric Polynomials with a Sub-Polynomial Number of Multiplications, ECCC Report TR02-052) for fast computation of much wider classes of multi-variate polynomials, modulo composites.

1 Introduction

It is an old question whether computations modulo non-prime-power composite numbers can be considerably faster than modulo primes or prime powers. One applicable property of the non-prime-power composites m can be the presence of zero-divisors in ring Z_m.

The zero divisors can speed up the computations as follows: Suppose that we want to compute the 4-variable polynomial $x_1y_1+x_2y_2$. Instead of the obvious 2 multiplications it is enough to do just one if we accept that some coefficients will not be computed exactly. That is, if we need that monomials with 0 coefficients should have 0 coefficients in our representation, but monomials with non-zero coefficients should be non-zero in the representation - say - modulo 6, then we can compute such a representation of this polynomial with only one multiplication modulo 6:

$$(2x_1+3x_2)(2y_1+3y_2) \equiv 4x_1y_1+3x_2y_2 \pmod 6.$$

It is easy to see that one can compute an a similar representation of the product of two 2×2 matrices with only 4 multiplications (instead of 8), applying four times this idea.

Clearly, these savings in the number of multiplications were based on the 0-divisors 2 and 3. But what can we do if we want to compute a similar representation of polynomial

$$S_n^2(x,y) = \sum_{1\le i\ne j\le n} x_iy_j$$

or the dot-product $x\cdot y = \sum_{i=1}^n x_iy_i$?

A straightforward solution were the following: Take $u_1,u_2,\ldots,u_n$ and $v_1,v_2,\ldots,v_n$ such that $u_iv_j \equiv 0 \pmod 6 \iff i=j$, then just one multiplication would suffice for computing such a representation of $S_n^2(x,y)$:

$$(x_1u_1+x_2u_2+\cdots+x_nu_n)(y_1v_1+y_2v_2+\cdots+y_nv_n).$$

ISSN 1433-8092

*Department of Computer Science, Eötvös University, Budapest, Pázmány P. stny. 1/C, H-1117 Budapest, Hungary; E-mail: grolmusz@cs.elte.hu

Unfortunately, it is easy to see that for $n \geq 3$ no such $u_i's$ and $v_i's$ exist in Z_6. However, we will still be able to define such u_i's and v_i's, called *sixtors* (from the words *six* and *vector*) in the next section (see Definition 5).

Here we would like to give a simple but non-trivial example for the demonstration of our results without lengthy definitions:

Suppose, that our goal is to compute the polynomial

$$S_6^2(x,y) = \sum_{1\leq i\neq j\leq 6} x_i y_j.$$

It is obvious that one can do this with 6 multiplications. But how can we save some multiplications if we were satisfied with some representation in a way that non-zero coefficients should be non-zero, and zero coefficients should be zero in the representation? The following example gives such a representation with only 2 multiplications:

Example 1 *Consider the following formal product:*

$$\left(\begin{pmatrix}2\\1\end{pmatrix}x_1+\begin{pmatrix}5\\1\end{pmatrix}x_2+\begin{pmatrix}2\\3\end{pmatrix}x_3+\begin{pmatrix}2\\2\end{pmatrix}x_4+\begin{pmatrix}1\\2\end{pmatrix}x_5+\begin{pmatrix}3\\5\end{pmatrix}x_6\right)\times$$

$$\left(\begin{pmatrix}5\\2\end{pmatrix}y_1+\begin{pmatrix}1\\1\end{pmatrix}y_2+\begin{pmatrix}3\\2\end{pmatrix}y_3+\begin{pmatrix}1\\5\end{pmatrix}y_4+\begin{pmatrix}2\\5\end{pmatrix}y_5+\begin{pmatrix}1\\3\end{pmatrix}y_6\right)$$

It is easy to see, that if the coefficient of x_i is vector u_i and the coefficient of y_j is vector v_j then $u_i \cdot v_j \equiv 0 \pmod 6 \iff i=j$ (where $u_i \cdot v_j$ denotes the dot-product of vectors u_i and v_j).

How can we translate this remarkable zero-divisor property to the actual computation of the polynomials? As it will turn out in the remainder of the paper, the correct translation is as follows: We should compute the sum of two products: in the first product, we multiply the sum of the x_i's with coefficients in the first coordinate of the vectors with the sum of y_j's with coefficients in the first coordinate of the vectors; in the second product we should do the same with the second coordinate of the vectors; that is:

$$(2x_1+5x_2+2x_3+2x_4+x_5+3x_6)(5y_1+y_2+3y_3+y_4+2y_5+y_6)+$$

$$(x_1+x_2+3x_3+2x_4+2x_5+5x_6)(2y_1+y_2+2y_3+5y_4+5y_5+3y_6)$$

It is easy to verify that the coefficients of monomials $x_i y_i$ are zeroes modulo 6. For completeness, we list in the following matrix the modulo 6 reduced coefficients of $x_i y_j$ in position (i,j):

$$\begin{pmatrix}0&3&2&1&3&5\\3&0&5&4&3&2\\4&5&0&5&1&5\\2&4&4&0&2&2\\3&3&1&5&0&1\\1&2&1&4&3&0\end{pmatrix}$$

The length-2 vectors (with some more demanding properties) will be called sixtors in the next section.

Note, that in this example, the number of multiplications used corresponded to the length of the vectors.

1.1 Preliminaries

In [Gro02b] we have found a definition of a sort of representation of polynomials modulo non-prime power composite numbers (say 6), and we also have found that this representation of some polynomials can be computed much faster modulo composites than modulo primes. In [Gro03] we generalized that definition.

Note, that for prime or prime-power moduli, polynomials and all types of their representations (defined below), coincide. That may be the reason that these representations were not defined before.

Definition 2 ([Gro03]) *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, such that the degree of each variables is bounded by d:*

$$f(x_1, x_2, \ldots, x_n) = \sum_{\delta \in \{0,1,2,\ldots,d\}^n} a_\delta x_\delta,$$

where $a_\delta \in Z_m$, $x_\delta = \prod_{i=1}^n x_i^{\delta_i}$. Then we say that

$$g(x_1, x_2, \ldots, x_n) = \sum_{\delta \in \{0,1,2,\ldots,d\}^n} b_\delta x_\delta$$

is an

- alternative representation *of f modulo m, if*

$$\forall \delta \in \{0,1,2,\ldots,d\}^n \ \exists j \in \{1,2,\ldots,\ell\} : \quad a_\delta \equiv b_\delta \pmod{p_j^{e_j}};$$

- 0-a-strong representation *of f modulo m, if it is an alternative representation, and, furthermore, if for some i, $a_\delta \not\equiv b_\delta \pmod{p_i^{e_i}}$, then $b_\delta \equiv 0 \pmod{p_i^{e_i}}$;*
- 1-a-strong representation *of f modulo m, if it is an alternative representation, and, furthermore, if for some i, $a_\delta \not\equiv b_\delta \pmod{p_i^{e_i}}$, then $a_\delta \equiv 0 \pmod{m}$;*

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 a 0-a-strong representation of f modulo 6;

$$g(x_1, x_2, , x_3) = x_1x_2 + x_2x_3 + x_1x_3 + 3x_1^2 + 4x_2$$

is a 1-a-strong representation of f modulo 6;

$$g(x_1, x_2, , x_3) = 3x_1x_2 + 4x_2x_3 + x_1x_3 + 3x_1^2 + 4x_2$$

is an alternative representation modulo 6.

In other words, for modulus 6, in the alternative representation, each coefficient is correct either modulo 2 or modulo 3, but not necessarily both.

In the 0-a-strong representation, the 0 coefficients are always correct both modulo 2 and 3, the non-zeroes are allowed to be correct either modulo 2 or 3, and if they are not correct modulo one of them, say 2, then they should be 0 mod 2.

In the 1-a-strong representation, the non-zero coefficients of f are correct for both moduli in g, but the zero coefficients of f can be non-zero either modulo 2 or modulo 3 in g, but not both.

We considered elementary symmetric polynomials

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

in [Gro02b]. Elementary symmetric polynomials are known to be the building-blocks of symmetric polynomials. Moreover, their computational complexity were widely studied in the arithmetic circuit model of computation, e.g.: [RSV00], [Shp], [NW97].

We proved in [Gro02b] that for constant k's, 0-a-strong representations of elementary symmetric polynomials S_n^k can be computed dramatically faster over non-prime-power composites than over primes: we gave an algorithm with $n^{o(1)}$ multiplications, and, moreover, the algorithm was suitable to be implemented in the depth-3 multilinear arithmetic circuit model. We note, that over fields or prime moduli computing these polynomials on depth-3 multilinear circuits needs polynomial (i.e., $n^{\Omega(1)}$) multiplications [NW97].

The goal of the present work is to generalize the results of [Gro02b] for a wider set of polynomials and for a matrix operation of fundamental importance: matrix multiplication; further demonstrating the effectiveness of computations modulo composite numbers.

2 A Result for the Matrix Product

It is a long-time open question whether one can compute the product of two $n \times n$ matrices with using only $n^{2+o(1)}$ multiplications.

We note, that the naive algorithm uses n^3 multiplications. The famous result of Strassen [Str69] uses $n^{2.81}$ multiplications. The best known algorithm today was given by Coppersmith and Winograd [CW90], requires only $n^{2.376}$ multiplications.

In [Gro03] we have given an algorithm for computing the 1-a-strong representation of the matrix product with $n^{2+o(1)}$ multiplications. That algorithm also can be described as computation involving sixtors.

3 Sixtors

Definition 4 *Let $A = \{a_{ij}\}$ and $B = \{b_{ij}\}$ two $u \times v$ matrices over a ring R with unit element 1. Their* Hadamard-product *is an $u \times v$ matrix $C = \{c_{ij}\}$, denoted by $A \odot B$, and is defined as $c_{ij} = a_{ij}b_{ij}$, for $1 \le i \le u$, $1 \le j \le v$. Let $k \ge 2$. The k-wise dot product of vectors of length n, $a^{(1)}, a^{(2)}, \ldots, a^{(k)}$ is computed as*

$$(a^{(1)} \odot a^{(2)} \odot \cdots \odot a^{(k)}) \cdot \mathbf{1},$$

where $\mathbf{1}$ denotes the length n all-1 vector.

Definition 5 *Let n, k, m be positive integers. Then a collection of length-t vectors*

$$S(n,k,m) = (S_1, S_2, \ldots, S_k)$$

where $S_i = \{v_i^{(1)}, v_i^{(2)}, \ldots, v_i^{(n)}\}$, $v_i^{(\ell)} \in \{0, 1, \ldots, m-1\}^t$, are called **(n, k, m)-sixtors**, *if the following holds:*

$$v_1^{(j_1)} \odot v_2^{(j_2)} \odot \ldots \odot v_k^{(j_k)} \odot \mathbf{1} \equiv 0 \pmod m \iff \exists u \neq v : j_u = j_v. \tag{1}$$

An (n,k,m)-sixtor is a **proper sixtor**, *if the value of*

$$v_1^{(j_1)} \odot v_2^{(j_2)} \odot \ldots \odot v_k^{(j_k)} \odot \mathbf{1} \pmod 6$$

does not depend on the particular order of the pairwise different indices $j_1, j_2, \ldots, j_k$ (i.e., it is constant). Let $t(n,k,m)$ denote the minimum length t such that $S(n,k,m)$ is a proper sixtor. Let $t^*(n,k,m)$ denote the minimum length t such that $S(n,k,m)$ is a sixtor.

In particular, if vectors $v_i^{(j)}$ are 0-1 vectors, then $v_i^{(j)}$ can be seen as characteristic vectors of sets $V_i^{(j)}$ of the t-element base-set, then for their intersection the following holds:

$$|\bigcap_{i=1}^{k} V_i^{(j_i)}| \equiv 0 \pmod m \iff \exists u \neq v : j_u = j_v. \tag{2}$$

Note, that $(n, 2, m)$-sixtors were called co-orthogonal codes in [Gro02a].

Note, that from this point on, instead of the more correct notation for vectors v with upper index i: $v^{(i)}$, we will write simply v^i.

3.1 Some algebraic remarks

Let $R = Z_m[x_1, x_2, \ldots, x_n]$ denote the ring of n-variable polynomials over Z_m. The we are interested in a *module* M over R, generated by vectors of Z_m^t. All the elements of this module can be written into the form of

$$\sum f_i v^i, \quad f_i \in R, v^i \in Z_m^t.$$

We also need to use Hadamard-products on module M; it is easy to see that

$$(\sum_i f_i u^i) \odot (\sum_i g_i v^i) = \sum_{i,j} f_i g_j (u^i \odot v^j), \quad f_i, g_j \in R, u^i, v^j \in Z_m^t.$$

3.2 Using sixtors for fast computing of polynomials

In [Gro02b] we have shown how to compute a 0-a-strong representation of the second elementary symmetric polynomial, S_n^2 with only $\exp(O(\sqrt{\log n \log\log n}))$ multiplication in the most restricted depth-3 arithmetic circuit model of computation. In the terms of sixtors, we can re-formulate that algorithm as follows: Consider $(n, 2, m)$ proper sixtors $((v_1^1, v_1^2, \ldots, v_1^n), (v_2^1, v_2^2, \ldots, v_2^n))$, and take the following Hadamard-product:

$$(x_1 v_1^1 + x_2 v_1^2 + \cdots + x_n v_1^n) \odot (x_1 v_2^1 + x_2 v_2^2 + \cdots + x_n v_2^n) \odot \mathbf{1} =$$

$$\sum_i x_i^2(v_1^i \odot v_2^i \odot \mathbf{1}) + 2\sum_{i\neq j} x_i x_j (v_1^i \odot v_2^j \odot \mathbf{1}). \tag{5}$$

Here the first sum is 0, and for any odd m, each coefficient of the second sum is non-zero (here we used that our sixtor is proper), so this is really a 0-a-strong representation of S_n^2. How many multiplications were used? For answering this question, let us denote $v_s^i(\ell) \in Z_m$ the ℓ^{th} coordinate of vector v_s^i, $s = 1, 2$. Then from the distributive law, quantity (5) is equal to

$$\sum_{\ell=1}^{t} \left(x_1 v_1^1(\ell) + x_2 v_1^2(\ell) + \cdots + x_n v_1^n(\ell)\right)\left(x_1 v_2^1(\ell) + x_2 v_2^2(\ell) + \cdots + x_n v_2^n(\ell)\right). \tag{6}$$

Clearly, (6) contains $t = t(n, 2, m)$ multiplications.

For computing an a-strong representation of the k^{th} elementary symmetric polynomial S_n^k, we take proper (n, k, m)-sixtors $(S_1, S_2, \ldots, S_n)$, such that $S_i = \{v_i^1, v_i^2, \ldots, v_i^n\}$, and compute

$$\bigodot_{i=1}^{k}(x_1 v_i^1 + x_2 v_i^2 + \cdots + x_n v_i^n) \odot \mathbf{1} = 0 + k! \sum_{\substack{I\subset\{1,2,\ldots,n\}\\ |I|=k}} \left(\prod_{j\in I} x_j\right) v(I), \tag{7}$$

Where $v(I)$ stands for the value

$$v_1^{j_1} \odot v_2^{j_2} \odot \cdots \odot v_k^{j_k} \odot \mathbf{1}, \text{ where } I = \{j_1, j_2, \ldots, j_k\}.$$

Note, that – because of the proper sixtor property – the value of $v(I)$ is independent of the particular choice of vectors $v_i^{j_i}$, it depends only on set I.

If m and $k!$ are relative primes then (7) is a 0-a-strong representation of S_n^k and it contains only $t = t(n, k, m)$ products (or $(k-1)t$ multiplications), since (7) can be written in a similar form as (6).

3.3 Further applications of sixtors for computing polynomials

Example 6 *For two integers d and d', for computing an 0-a-strong representation of a sum of $x_i y_j$ products, where i and j are incongruent modulo d, and exactly one of them is a multiple of d', can be easily computed with sixtors. For example, for $d = 2, d' = 3$ this means that the parities of i and j differs and exactly one of i and j is a multiple of 3. Now we can write*

$$(x_1 v_1^1 \odot v_2^3 + x_2 v_1^2 \odot v_2^3 + x_3 v_1^1 \odot v_2^4 + x_4 v_1^2 \odot v_2^3 + x_5 v_1^1 \odot v_2^3 + x_6 v_1^2 \odot v_2^4)\odot$$

$$\odot(y_1 v_3^1 \odot v_4^3 + y_2 v_3^2 \odot v_4^3 + y_3 v_3^1 \odot v_4^4 + y_4 v_3^2 \odot v_4^3 + y_5 v_3^1 \odot v_4^3 + y_6 v_3^2 \odot v_4^4) \odot \mathbf{1}$$

and this product will give us an a-strong representation of

$$x_1y_6 + x_2y_3 + x_3y_2 + x_3y_4 + x_4y_3 + x_5y_6 + x_6y_1$$

3.4 A construction of sixtors

Let $M = \{m_{j_1,j_2,\ldots,j_k}\}$ be an $\overbrace{n \times n \times n \times \cdots \times n}^{k}$ (k-dimensional) matrix, with elements $m_{j_1,j_2,\ldots,j_k}$. A for index-sets $I_i \subset \{1,2,\ldots,n\}$ we define the k-dimensional box (or simply, a box) as the set of entries

$$R(I_1, I_2, \ldots, I_k) = \{m_{j_1,j_2,\ldots,j_k} : j_i \in I_i\}.$$

Clearly, the intersection of any finite set of boxes is a (possibly empty) box.

We have proved implicitly the following theorem in [Gro02b]. We show here how these results follow from that paper.

Theorem 7 *Let m be a positive integer with r different prime divisors. Then there exists an explicitly constructible box-cover $R_1, R_2, \ldots, R_w$ of the $\overbrace{n \times n \times n \times \cdots \times n}^{k}$ (k-dimensional) matrix $M = \{m_{j_1,j_2,\ldots,j_k}\}$, such that the following properties hold:*

(i) Those and only those matrix-entries $m_{j_1,j_2,\ldots,j_k}$ has covering multiplicity different from 0 modulo m whose indices are pairwise different numbers: $j_u \neq j_v$ if $u \neq v$.

(ii) The multiplicity of covering the element $m_{j_1,j_2,\ldots,j_k}$ with pairwise different indices depends only on the set $I = \{j_1, j_2, \ldots, j_k\}$, and not on the particular order of the indices.

(iii)

$$w = \exp(\exp(O(k))(\log n)^{1/r} \log\log n).$$

Note, that this circuit-size is sub-polynomial (that is, $n^{o(1)}$) 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 $c > 0$.

Note, that higher dimensional matrices are called tensors sometimes. We avoided that term since we have not used anything from tensor-algebra.

Proof: In [Gro02b] we defined polynomial

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

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 $j = 1,2,\ldots,k$. Then we proved the following

Theorem 8 ([Gro02b], Theorem 3.4) *Let $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$. Then there exists an 0-a-strong representation of $S_n^k(x^{(1)}, x^{(2)}, \ldots, x^{(k)})$ modulo m,*

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

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

We proved in [Gro02b] that the homogeneous circuit contains products which, in turn, corresponds to the box-cover of the non-diagonal elements of the k-dimensional matrix with entries $x^{(1)}_{i_1} x^{(2)}_{i_2} \cdots x^{(k)}_{i_k}$. The same box-cover will satisfy the requirements of Theorem 7 if applied to the k-dimensional matrix M.

□

Based on Theorem 7, we construct proper (n, k, m)-sixtors as follows:

Theorem 9 *Let m be a positive integer with r different prime divisors. Then there exists an explicitly constructible proper (n, k, m)-sixtor with length $t(n, k, m) = \exp(\exp(O(k))(\log n)^{1/r} \log\log n)$. In particular, there are proper $(n, 2, m)$-sixtors of length $\exp(O(\sqrt{\log n \log\log n}))$.*

Proof: We do not prove here the stronger statement for $(n, 2, m)$-sixtors, it is implicit in [Gro02b].

For proving the statement for (n, k, m)-sixtors, first let us consider the box-cover of k-matrix M, given in Theorem 7. Note, that this cover contains $\exp(\exp(O(k))(\log n)^{1/r} \log\log n)$ boxes.

We show that from this box-cover one can easily get sets of vectors $(S_1, S_2, \ldots, S_k)$, where $S_i = \{v_i^{(1)}, v_i^{(2)}, \ldots, v_i^{(n)}\}$, $v_i^{(\ell)} \in \{0,1\}^t$, where t is exactly the cardinality of the box-cover, that is, $t = \exp(\exp(O(k))(\log n)^{1/r} \log\log n)$. Moreover, these vectors have the following property:

$$v_1^{j_1} \odot v_2^{j_2} \odot \cdots \odot v_k^{j_k} \odot \mathbf{1}$$

is just the box-covering multiplicity of $m_{j_1 j_2 \ldots j_k}$.

First assume that $k = 2$. Then for any box we correspond a 0-1 matrix, with 1's exactly in the points (or elements) of the box.

For example,

$$\begin{bmatrix} 0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&1&1&1&1&1&0\\ 0&0&0&0&1&1&1&1&1&0\\ 0&0&0&0&1&1&1&1&1&0\\ 0&0&0&0&1&1&1&1&1&0\\ 0&0&0&0&1&1&1&1&1&0\\ 0&0&0&0&1&1&1&1&1&0\\ 0&0&0&0&0&0&0&0&0&0 \end{bmatrix}$$

This 0-1 matrix (of rank 1) can be got from the diadic product of two 0-1 vectors: $u = (0,0,0,1,1,1,1,1,1,0)$ and $v = (0,0,0,0,1,1,1,1,1,0)$. Similarly, the matrix-sum of the rank-1 matrices, corresponding to the members of the box-cover of cardinality t can be got from the product of an $n \times t$ 0-1 matrix U and a $t \times n$ 0-1 matrix V. In this case, the vectors of set S_1 will be the rows of U and the vectors of set S_2 will be the columns of V. It is obvious from the properties of the box cover (see Theorem 7), that the sixtor-properties (together with the properness) are satisfied.

A similar construction works for k-dimensional boxes: Now the (k-dimensional) 0-1 matrix, corresponding to box $R(I_{1,2},\dots,I_k)$ is the k-times diadic product of the following k 0-1 vectors of length n: w^j, where w^j is just the characteristic vector of set I_j. We have t boxes, each defines a k-tuple of vectors. Now, if we take vectors w^j as column-vectors, then the elements of S_j will be the rows of the matrix, constructed from the t vectors w^j as columns (we have one w^j for each box), $j = 1,2,\dots,k$.□

3.5 A remark on tensor-rank

Upper bounds to the rank of the matrix-product tensor [Str73] is of utmost importance in finding fast matrix multiplication algorithms. Here we also find covers with a small number of rectangles/boxes, that is, we also bound the rank of certain tensors. We have chosen to use the k-dimensional matrix (that is, k-dimensional array) terms because we thought that the geometric intuition helps in the description of our results.

3.6 An application for matrix-product

Take $(n,2,m)$ sixtors of length $t = t(n,2,m) = \exp(O(\sqrt[r]{\log n \log\log n}))$, and compute

$$c'_{ij} = (\sum_{k=1}^n a_{ik})(\sum_{k=1}^n b_{kj}) - (a_{i1}v_1^1 + a_{i2}v_1^2 + \cdots + a_{in}v_1^n) \odot (b_{1j}v_2^1 + b_{2j}v_2^2 + \cdots + b_{nj}v_2^n) \odot \mathbf{1} \quad (10)$$

each with t multiplications. Since

$$(a_{i1}v_1^1 + a_{i2}v_1^2 + \cdots + a_{in}v_1^n) \odot (b_{1j}v_2^1 + b_{2j}v_2^2 + \cdots + b_{nj}v_2^n) \odot \mathbf{1}$$

gives a 0-a-strong representation of $S_n^2(a^i,b^j)$, (10) gives the 1-a-strong representation of $(\sum_{k=1}^n a_{ik})(\sum_{k=1}^n b_{kj}) - S_n^2(a^i,b^j)$, that is, the 1-a-strong representation of the dot product

$$\sum_{k=1}^n a_{ik}b_{kj}.$$

Since we have n^2 c'_{ij}'s, it follows that a 1-a-strong representation of the matrix-product can be computed with $n^{2+o(1)}$ multiplications.

4 A Lower Bound for the Length of Sixtors

We proved the following theorem in [Gro02b]:

Theorem 10 ([Gro02b]) *Let*

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

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.

□

It is not difficult to prove a lower bound to the length of $(2, 2\lceil\log n\rceil, 6)$ sixtors, using Theorem 10:

Corollary 11

$$t^*(2, 2\lceil\log n\rceil, 6) = \Omega(n).$$

Proof: Let $\ell = \lceil\log n\rceil$. Let us consider a $(2, 2\ell, 6)$-sixtor. Then the product

$$\left(\sum_{i=0}^{n-1} x_{i+1}(v_1^{i_1} \odot v_2^{i_2} \odot \cdots \odot v_\ell^{i_\ell}\right)\left(\sum_{i=0}^{n-1} y_{i+1}(v_{\ell+1}^{1-i_1} \odot v_{\ell+2}^{1-i_2} \odot \cdots \odot v_{2\ell}^{1-i_\ell}\right)$$

where $i_1 i_2 \dots i_\ell$ denote the binary form of index i, computes an a-strong representation of the dot-product of length n vectors x and y with $t^*(2, 2\log n, 6)$ multiplications; consequently, from Theorem 10, $t^*(2, 2\log n, 6) = \Omega(n)$.

□

The Corollary above holds for all moduli m instead of 6.

5 Open problems

It would be interesting to compute a 0-a-strong representations of the matrix product or the matrix-vector product using fewer multiplications than the currently best known algorithms for computing the exact values.

Acknowledgment.

The author acknowledges the partial support of the Széchenyi István fellowship.

References

[CW90] Don Coppersmith and Shmuel Winograd. Matrix multiplication via arithmetic progressions. *J. Symbolic Comput.*, 9(3):251–280, 1990.

[Gro02a] Vince Grolmusz. Co-orthogonal codes. In Oscar H. Ibarra and Louxin Zhang, editors, *COCOON*, volume 2387 of *Lecture Notes in Computer Science*, pages 144–152. Springer, 2002.

[Gro02b] Vince Grolmusz. Computing elementary symmetric polynomials with a subpolynomial number of multiplications. Technical Report TR02-052, ECCC, 2002. To appear in the SIAM Journal on Computing.

[Gro03] Vince Grolmusz. Near quadratic matrix multiplication modulo composites. Technical Report TR03-001, ECCC, 2003. ftp://ftp.eccc.uni-trier.de/pub/eccc/reports/2003/TR03-001/index.html.

[NW97] Noam Nisan and Avi Wigderson. Lower bounds on arithmetic circuits via partial derivatives. *Computational Complexity*, 6(3), 1997.

[RSV00] Jaikumar Radhakrishnan, Pranab Sen, and Sundar 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.

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

[Str69] V. Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13:354–356, 1969.

[Str73] Volker Strassen. Vermeidung von Divisionen. *J. Reine Angew. Math.*, 264:184–202, 1973.

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'