On the Number of Multiplications Required for a Matrix-vector Product

AKIHIRO NOZAKI*

In this paper we strengthen Winograd's result on the number of multiplications required for a matrix-vector product, so that the multiplications by constant factors can also be counted. We show some examples for which sharp bounds can be obtained from our result.

1. Introduction

In practice, we are often asked to compute a given set of polynomials. Such a problem can be considered in many cases as the computation of the product of a matrix M and a column vector $\boldsymbol{x}$. The element of M are polynomials and the components of $\boldsymbol{x}$ are indivisual variables. In 1970, S. Winograd formulated this type of problems and considered the number of required multiplications for computing the product of such a matrix and a column vector. He defined the notion of **column rank** of a matrix, on the basis of a modified version of linear independence, and established a lower bound of the number of multiplications as following.

Any computation of $M\boldsymbol{x}$ requires at least q "active" multiplications, where q is the column rank of M.

This result is a basic tool for proving the optimality of some general algorithms, such as Horner's rule for evaluating arbitrary polynomials.

In this result, however, the multiplications by constant factors were disregarded. So the obtained lower bound was not always useful, especially in such specific cases as follows.

$$\begin{bmatrix}0.2 & 1.3\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} \tag{1}$$

$$\begin{bmatrix}1/2 & 1\\1 & 1/2\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} \tag{2}$$

$$\begin{bmatrix}1/2 & 1\\1 & 1/3\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} \tag{3}$$

The column ranks of these matrices are equal to zero and hence no "active" multiplications are required for these products. Nevertheless, if we count the multiplications by constants such as $1.3y$, a number of multiplications sould be indispensable.

In this paper, we introduce another variant of linear independence, **Z-independence**, and show the validity of an analogous result as following.

Any computation of a product $M\boldsymbol{x}$ requires at least s multiplications involving $\boldsymbol{x}$, where s is the number of Z-independent columns of M.

Our number s is not less than the column rank q of the matrix M. We shall see that one multiplication is sufficient for the product (1) and also for the product (3), while two multiplications are necessary for the product (2).

2. Formulation of the Problem

We shall review here basic notions mainly after Aho-Hopcroft-Ullman (1974).

We use variable names with or without suffices, e.g., x, y, x_1, x_2, etc. Some of these variables are called **input variables** or simply **inputs**, when they represents indeterminates in the polynomials to be multiplied.

A **computation** is a sequence of steps of the form $a \leftarrow b \delta c$, where δ is $+$, $-$ or $\times$, a is a non-input variable name, and b and c are either inputs, constant real numbers, or variable names appearing on the left of the arrow at some previous steps. For convenience, we allow also the steps $a \leftarrow 0$ and $a \leftarrow d^{-1}$, where d is a constant real number.

Example 1 Inputs are represented by x and y.

$$\begin{aligned} &s \leftarrow x+y, && v \leftarrow 1.1 \times u,\\ &t \leftarrow s+s, && w \leftarrow v-t.\\ &u \leftarrow t+y, \end{aligned}$$

Example 2 Inputs are represented by x and y.

$$\begin{aligned} &u_1 \leftarrow x-y, && u_5 \leftarrow u_4+u_4,\\ &u_2 \leftarrow u_1+u_1, && u_6 \leftarrow u_5+y,\\ &u_3 \leftarrow u_2+x, && u_7 \leftarrow u_6+u_4,\\ &u_4 \leftarrow (1/6)\times u_3, && u_8 \leftarrow u_7-u_1. \end{aligned}$$

We associate in the usual manner to each non-input variable u its **value** $v(u)$. For instance, in Example 1,

$$v(t)=2x+2y, \qquad v(w)=0.2x+1.3y.$$

Let $\boldsymbol{x}$ be a column vector of the form $[x_1, \ldots, x_q]^T$, where x_i's are distinct input variables. A multiplication

*Faculty of Engineering, Yamanashi University, Takeda-4, Kofu, Yamanashi 400, Japan.

involves x iff the value of one of the operands multiplied depends on one of these variables x_i's.

Let E be a column vector whose components are polynomials with input variables. A computation **computes** E iff for each component e of E there is some variable f in the computation such that $v(f)=e$. The computation in Example 1 computes the vector $[0.2x+1.3y]$, that is, the product (1) in Section 1. The computation in Example 2 computes the product (3) in Section 1, since

$$v(u_6)=x+(1/3)y \quad \text{and} \quad v(u_8)=(1/2)x+y.$$

Thus one multiplication is sufficient for the product (3) as well as for the product (1).

Remark We do not claim that the computations in these examples are of practical interest, unless multiple precision arithmetic is involved. However, it should be noted that in certain domains multiplications are arbitrarily more costly than additions and subtractions.

We denote by $\boldsymbol{R}$ the whole set of real numbers and by $\boldsymbol{Z}$ the whole set of integers. We represent by $\boldsymbol{R}[a_1, \ldots, a_n]$ the set of all real polynomials over the indeterminates $a_1, \ldots, a_n$.

In what follows, we consider a matrix M with p rows and q columns, whose elements are in $\boldsymbol{R}[a_1, \ldots, a_n]$, and a column vector $\boldsymbol{x}$ of the form $[x_1, \ldots, x_q]^T$, where $x_1, \ldots, x_q$ are variable names distinct from $a_1, \ldots, a_n$. Our aim is to give a lower bound to the number of multiplications involving $\boldsymbol{x}$ for evaluating the product $M\boldsymbol{x}$.

Definition 1 Suppose that $\boldsymbol{v}(1), \ldots, \boldsymbol{v}(t)$ are p-dimensional vectors whose components are in $\boldsymbol{R}[a_1, \ldots, a_n]$.

1) These vectors are said to be **Z-dependent** iff there exist integers $k_1, \ldots, k_t$ satisfying the following conditions.

$$k_1 \cdot \boldsymbol{v}(1)+\ldots+k_t \cdot \boldsymbol{v}(t) \in \boldsymbol{Z}^p, \tag{1a}$$

$$\mathrm{GCD}(k_1, \ldots, k_t)=1, \tag{1b}$$

where GCD stands for the greatest common divisor. For convenience, we define: $\mathrm{GCD}(m)=|m|$, $\mathrm{GCD}(0)=0$ and

$$\mathrm{GCD}(0, \ldots, 0, k, \ldots, h)=\mathrm{GCD}(k, \ldots, h).$$

For $\boldsymbol{v}=(v_1, \ldots, v_t)$, we denote $\mathrm{GCD}(v_1, \ldots, v_t)$ by $\mathrm{GCD}(\boldsymbol{v})$.

2) These vectors are said to be **Z-independent** iff they are not $\boldsymbol{Z}$-dependent, or equivalently, iff for any integers $k_1, \ldots, k_t$, the condition (1a) implies that

$$\mathrm{GCD}(k_1, \ldots, k_t) \neq 1. \tag{1c}$$

For instance, the vectors [0.2] and [1.3] are $\boldsymbol{Z}$-dependent. The following sets of vectors are $\boldsymbol{Z}$-independent.

1) [1.3]

2) [0.2], $[\sqrt{2}]$, $[\pi]$

3) $\begin{bmatrix}1/2\\1\end{bmatrix}\begin{bmatrix}1\\1/2\end{bmatrix}$

3. Integer Matrix Invertible in the Domain Z

In this section, we shall give some preliminary lemmas on integer matrices whose inverses are also integer matrices.

An integer matrix is said to be **invertible in the domain Z**, or **Z-invertible** in short, iff it is a square matrix and its determinant is equal to $+1$ or -1. If a matrix is $\boldsymbol{Z}$-invertible, then it is nonsingular and its inverse is again a $\boldsymbol{Z}$-invertible integer matrix. If both of the matrices N and N' are $\boldsymbol{Z}$-invertible, then so is their product NN'.

Example 1 The following matrices are $\boldsymbol{Z}$-invertible.

$$\begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\5 & -2 & -1\end{bmatrix}\begin{bmatrix}-1 & 3 & 0\\0 & 1 & 0\\0 & -7 & 1\end{bmatrix}$$

More generally, a matrix is $\boldsymbol{Z}$-invertible if it satisfies the following conditions.

(a) Each of its diagonal elements is either $+1$ or -1.

(b) There is at most one row or one column which contains non-zero non-diagonal elements.

Example 2 Let us consider the matrix $P(i, j)$ obtained from the identity matrix by exchanging its i-th row and j-th row. Then it is always $\boldsymbol{Z}$-invertible.

Lemma 1 Let $\boldsymbol{k}$ be a k-dimensional integer vector and N a $\boldsymbol{Z}$-invertible matrix with k rows and k columns. Then it is the case that

$$\mathrm{GCD}(\boldsymbol{k})=\mathrm{GCD}(N\boldsymbol{k}).$$

Proof Every component of $N\boldsymbol{k}$ is a linear combination of the components of $\boldsymbol{k}$ with integer coefficients, and hence is an integer multiple of $\mathrm{GCD}(\boldsymbol{k})$. Thus $\mathrm{GCD}(N\boldsymbol{k})$ is an integer multiple of $\mathrm{GCD}(\boldsymbol{k})$. The converse is also true, since

$$\boldsymbol{k}=(N^{-1})(N\boldsymbol{k}).$$

Lemma 2 Let M be a matrix with p rows and q columns, whose elements are in $\boldsymbol{R}[a_1, \ldots, a_n]$. Let N be a $\boldsymbol{Z}$-invertible matrix with q rows and q columns.

The set of all columns of M are $\boldsymbol{Z}$-independent iff so is the set of all columns of MN.

Proof We prove the contrapositive statement: the columns of M are $\boldsymbol{Z}$-dependent iff so are the columns of MN.

If the columns of M are $\boldsymbol{Z}$-dependent, then there is an integer vector $\boldsymbol{k}$ such that $M\boldsymbol{k} \in \boldsymbol{Z}^p$ and $\mathrm{GCD}(\boldsymbol{k})=1$. It follows that

$$(MN)(N^{-1}\boldsymbol{k}) \in \boldsymbol{Z}^p$$

and by Lemma 1,

$$\mathrm{GCD}(N^{-1}\boldsymbol{k})=1.$$

Thus the columns of MN are also Z-dependent. The converse is also true, since N^{-1} is Z-invertible.

Lemma 3 For any integer vector u, there is a Z-invertible matrix N such that

$$Nu=[0, 0, \ldots, 0, \mathrm{GCD}(u)]^T.$$

Proof The proof proceeds by induction on the minimum absolute value h of non-zero components of u:

$$h=\mathrm{Min}\{|u_i| \mid u_i \neq 0\}.$$

Let q be the dimension of the vector u.

Basis. $h=1$. Suppose that $|u_q|=1$. Then the condition of the lemma is satisfied by the following matrix N_0, which can be obtained from the identity matrix by replacing its q-th column by $[-u_1u_q, \ldots, -u_{q-1}u_q, u_q]^T$.

$$N_0=\begin{bmatrix} 1 & & & * \\ & 1 & & * \\ & & \ddots & \\ & & 1 & * \\ & & & u_q \end{bmatrix}$$

For the case when $|u_i|=1$ and $i \neq q$, we define N_0 for the vector $P(i, q)u$ and apply the product $N_0 \cdot P(i, q)$ to u.

Inductive step. $h>1$. Suppose that $|u_i|=h$. We consider the values k_j and h_j defined by the following relations.

$$u_j=k_ju_i+h_j, \quad 0 \leqq h_j < h$$

for $j \neq i$, and

$$k_i=-u_i/h, \quad h_i=h.$$

Now let N_1 be the matrix obtained from the identity matrix by replacing its i-th column by $[-k_1, \ldots, -k_i, \ldots, -k_q]^T$. Then

$$N_1u=[h_1, \ldots, h_q]^T.$$

Let h' be the minimum absolute value of non-zero components of N_1u. If $h'=h$, then $h_j=0$ for all $j \neq i$. It follows that

$$h=h_i=\mathrm{GCD}(N_1u)=\mathrm{GCD}(u).$$

Hence the condition of the lemma is satisfied by the product $P(i, q) \cdot N_1$. Now suppose that $h'<h$. By inductive assumption, there is a Z-invertible matrix N_2 such that

$$N_2h=[0, \ldots, 0, d]^T,$$

where $h=[h_1, \ldots, h_q]^T$ and

$$d=\mathrm{GCD}(h)=\mathrm{GCD}(N_1u)=\mathrm{GCD}(u).$$

Thus the condition of the lemma is satisfied by $N=N_2N_1$.

4. Main Theorem

Lemma 4 The product Mx can be obtained without multiplication involving x, iff all elements of M are integers.

Proof (If) Obvious, since a multiplication by an integer can, at least in principle, be replaced by successive additions or subtractions.

(Only if) If an element y_i of the product Mx is obtained without multiplication involving x, then the value of y_i can be represented by the following expression:

$$c_1x_1+ \ldots +c_qx_q+P,$$

where $c_1, \ldots, c_q$ are integers and P is a polynomial in $R[a_1, \ldots, a_n]$. Therefore every component of the i-th row of the matrix M must be an integer. Since i is arbitrary, M is an integer matrix.

Theorem 1 Let M be a matrix with p rows and q columns, whose elements are in $R[a_1, \ldots, a_n]$. Let x be a vector of the form $[x_1, \ldots, x_q]^T$, where x_i's are variables distinct from a_j's.

If the matrix M has s, Z-independent columns, then any computation of Mx requires at least s multiplications involving x.

Proof We assume without loss of generality that the first s columns of M are Z-independent. We denote by $u(i)$ the i-th column of M. We consider a submatrix

$$M'=[u(1), \ldots, u(s)]$$

of M and a vector $x'=[x_1, \ldots, x_s]^T$.

(A) If r multiplications involving x' are required for the product $M'x'$, then r multiplications involving x are indispensable for the product Mx.

Suppose that t multiplications are sufficient for Mx. Then, we can evaluate the product

$$M'x'=M \cdot [x_1, \ldots, x_s, 0, \ldots, 0]^T$$

in t multiplications involving x. Since no multiplications independent of x can involve x', it is the case that

$$r \leqq t.$$

Hereafter, we assume that M has exactly s columns.

(B) If all columns of M are Z-independent, then s $(=q)$ multiplications involving x are required for the computation of Mx.

The proof proceeds by induction on s.

Basis. $s=1$. Since $u(1)$ is Z-independent, it is not an integer vector. By Lemma 4, at least one multiplication involving x is indispensable.

Inductive step. $s>1$. Let C be a computation of Mx which contains t multiplications involving x. Again by Lemma 4, $t \neq 0$. Suppose that $f \leftarrow g \times h$ is the first multiplication involving x in C. Then without loss of generality, we can assume

$$v(g)=c_1x_1+ \ldots +c_sx_s+P,$$

where $c=[c_1, \ldots, c_s]^T$ is a non-zero integer vector and P is a polynomial in $R[a_1, \ldots, a_n]$. By Lemma 3, there is a Z-invertible matrix N such that

$$Nc=[0, \ldots, 0, d]^T,$$

where $d=\mathrm{GCD}(c)$.

Now let $v(1), \ldots, v(s)$ be the columns of the product $M(N^T)$. By Lemma 2, these vectors are Z-independent. Therefore, its subset $v(1), \ldots, v(s-1)$ are also Z-independent. By inductive assumption, any computation of the product

$$z=[v(1), \ldots, v(s-1)][y_1, \ldots, y_{s-1}]^T$$

requires at least $s-1$ multiplications involving $y=[y_1, \ldots, y_{s-1}]^T$.

We shall now construct a computation C' which evaluates the value of z in $t-1$ multiplications involving y. We utilize the following relation.

$$\begin{aligned} z&=[v(1), \ldots, v(s-1)]y \\ &=[v(1), \ldots, v(s)][y_1, \ldots, y_{s-1}, -d^{-1}P]^T \\ &\quad +v(s)(d^{-1}P) \\ &=M(N^T[y_1, \ldots, y_{s-1}, -d^{-1}P]^T)+v(s)(d^{-1}P). \end{aligned}$$

First, we determine the value of x as follows.

$$x=N^T[y_1, \ldots, y_{s-1}, -d^{-1}P]^T.$$

Since N^T is an integer matrix, this can be done without multiplication involving y. Then we compute the product Mx for this value of x, utilizing the computation C with $f \leftarrow g \times h$ replaced by $f \leftarrow 0$. The validity of this modification is verified in the following manner.

$$\begin{aligned} v(g)&=[c_1, \ldots, c_s][x_1, \ldots, x_s]^T+P \\ &=[c_1, \ldots, c_s](N^T[y_1, \ldots, y_{s-1}, -d^{-1}P]^T)+P \\ &=(Nc)^T[y_1, \ldots, y_{s-1}, -d^{-1}P]^T+P \\ &=[0, \ldots, 0, d][\ \ldots, -d^{-1}P]^T+P \\ &=-P+P=0. \end{aligned}$$

Finally, we calculate the term $v(s)(d^{-1}P)$ and add it to Mx. By the relation shown above, the result is equal to z. Since this term is independent of x, no multiplications involving x are required for this calculation.

After all, $t-1$ multiplications involving x are sufficient for the evaluation of z. Since only these multiplications can involve y, we can say that $t-1$ multiplications involving y are sufficient for evaluating z. It follows that

$$s-1 \leqq t-1,$$

that is, t is not less than s. This completes the proof of the theorem.

It is now immediate that the product $[0.2\ \sqrt{2}\ \pi][x\ y\ z]^T$ requires at least three multiplications. The product (2) in Section 1 requires at least two multiplications, since the vectors

$$\begin{bmatrix} 1/2 \\ 1 \end{bmatrix}, \quad \begin{bmatrix} 1 \\ 1/2 \end{bmatrix}$$

are Z-independent.

4. Miscellaneous Results

On the number of multiplications, other lower bounds were given by Fiduccia (1971). We can state analogous theorems in terms of Z-independence.

Theorem 2 Let M be a matrix with elements from $R[a_1, \ldots, a_n]$ and let x be the column vector $[x_1, \ldots, x_q]^T$. If the matrix M has s Z-independent rows, then any computation of Mx requires at least s multiplications.

Theorem 3 Suppose that a matrix M has a submatrix S with h rows and k columns, satisfying the following condition.

For any vectors u and v in Z^h and in Z^k, respectively,

$$(u^T)Sv \text{ is an integer iff } u=v=0.$$

Then any computation of Mx requires at least $h+k-1$ multiplications.

The proofs of these theorems are quite similar to those of Theorem 12.1 and Theorem 12.3 in Aho-Hopcroft-Ullman (1974) and therefore are omitted.

Remark If the rows of an integer matrix N are linearly dependent, there is a non-zero integer vector y such that $y^TN=0$. Besides, by reducing common divisors, we can assume without loss of generality that $\mathrm{GCD}(y)=1$. By this fact, we can convert Fiduccia's proofs into the proofs of our theorems.

When the columns of a matrix M are not Z-independent, we can transform the product Mx into $M'y$, where M' is a matrix with at least one integer column. We describe briefly how this can be done.

If the columns of a matrix M are Z-dependent, then by definition there is an integer vector v satisfying the following conditions.

(a) The vector Mv is an integer vector.

(b) $\mathrm{GCD}(v)=1$.

By Lemma 3, there is a Z-invertible matrix N such that

$$Nv=[0, \ldots, 0, 1]^T.$$

Then obviously,

$$Mx=(MN^{-1})(Nx)=M'y,$$

where $M'=MN^{-1}$ and $y=Nx$. The last column b of M' is an integer vector, as it is verified in the following manner.

$$b=(MN^{-1})[0, \ldots, 0, 1]^T=Mv.$$

Example

$$Mv=\begin{bmatrix} 1/2 & 1 \\ 1 & 1/3 \end{bmatrix}\begin{bmatrix} -2 \\ 3 \end{bmatrix}=\begin{bmatrix} 2 \\ -1 \end{bmatrix}$$

$$Nv=\begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} -2 \\ 3 \end{bmatrix}=\begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

and

$$N^{-1}=\begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix}.$$

Therefore,

$$\begin{bmatrix} 1/2 & 1 \\ 1 & 1/3 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}=\begin{bmatrix} 1/2 & 1 \\ 1 & 1/3 \end{bmatrix}N^{-1}N\begin{bmatrix} x \\ y \end{bmatrix}$$
$$=\begin{bmatrix} -1/2 & 2 \\ 2/3 & -1 \end{bmatrix}\begin{bmatrix} 3x+2y \\ x+y \end{bmatrix}$$
$$=\begin{bmatrix} -3 \\ 4 \end{bmatrix}\cdot(1/6)\cdot(3x+2y)+\begin{bmatrix} 2 \\ -1 \end{bmatrix}(x+y).$$

A similar computation to Example 2 in Section 2 can be obtained from the last expression.

We have considered as the base set only the set $\boldsymbol{R}$ of real numbers. But in fact we can replace $\boldsymbol{R}$ by any commutative domain F containing a prime field of characteristic zero. In that case, the set $\boldsymbol{Z}$ of integers should be replaced by the ring generated by the identity of multiplication in F.

References

1. WINOGRAD, S. On the number of multiplications necessary to compute certain functions, *Comm. Pure and Applied Math.*, **23**, (1970), 165–179.
2. FIDUCCIA, C. M. Fast matrix multiplication, *Proc. 3rd Annual ACM Symposium on Theory of Computing*, (1971), 45–49.
3. AHO, A. V., HOPCROFT, J. E. and ULLMAN, J. D. The design and analysis of computer algorithms, Addison-Wesley, Massachusetts. (1974).

(Received March 9, 1978; revised May 22, 1978)