JOURNAL OF COMPUTER AND SYSTEM SCIENCES 20, 77–95 (1980)

On the Complexity of Computing Bilinear Forms with {0, 1} Constants

TEOFILO GONZALEZ* AND JOSEPH JA'JA'†

Department of Computer Science, The Pennsylvania State University, University Park, Pennsylvania 16802

Received January 5, 1979; revised August 17, 1979

An important class of problems in arithmetic complexity is that of computing a set of bilinear forms, which includes many interesting problems such as the multiplication problems of matrices and polynomials. Recently, this class has been given considerable attention and several interesting results have emerged. However, most of the important issues remain unresolved and the general problem seems to be very difficult. In this paper, we consider one of the simplest cases of the general problem, namely evaluation of bilinear forms with {0, 1} constants, and prove that finding the optimal number of multiplications or the optimal number of additions is NP-hard. We discuss several related problems.

1. INTRODUCTION

Recently, the problem of evaluating a set of bilinear forms has been given a considerable emphasis in arithmetic complexity and one particular problem of this class, namely matrix multiplication, has been considered to be "the" problem of arithmetic complexity. Many interesting results have been established and more results are emerging (see, for example, [2, 3, 9, 16]). However, most of the important issues remain unresolved and the general problem seems to be very difficult. In this paper, we consider one of the simplest cases of the general problem, namely, evaluation of bilinear forms with {0, 1} constants, and prove that finding the optimal number of multiplications is difficult in a precise sense; i.e., it is NP-hard [10, 1]. Note that it is not known whether the general problem with integer constants is decidable or not [12].

We now define this class of problems precisely. Let R be a commutative ring and let $K \subseteq R$ such that $0, 1 \in K$. Suppose $x = (x_1, x_2, \ldots, x_p)^T$ and $y = (y_1, y_2, \ldots, y_q)^T$ are two column vectors of indeterminates; we have to compute m bilinear forms:

$$B_i = \sum_{j=1}^{p} \sum_{k=1}^{q} \alpha_{ijk} x_j y_k = x^T G_i y, \qquad i = 1, 2, \ldots, m,$$

where G_i is a $p \times q$ matrix with elements in K. The model of computation used for this class of problems is that of *bilinear programs*, where each program consists of a

* Supported in part by National Science Foundation under Grant MSC 77-21092.
† Supported in part by National Science Foundation under Grant MSC 78-06118.

0022-0000/80/010077-19$02.00/0

sequence of instructions of the form $f_i \leftarrow a_i \circ b_i$, $1 \leqslant i \leqslant r$, where $\circ$ stands for $+$ or $\times$ and each f_i is a new variable; a_i, b_i are either previously computed f_j's ($j < i$), or constants from K or indeterminates. Moreover, each multiplication step is either a *scalar multiplication*, i.e., a_i or $b_i \in K$, or a multiplication of a linear form in x by a linear form in y over K (*nonscalar multiplication*). This program computes the set $\{B_i\}_{i=1}^m$ if, for each i, there exists j_i such that $B_i = f_{j_i}$. The multiplicative complexity of computing $\{B_i\}_{i=1}^m$ is the number of nonscalar multiplications required by any bilinear program which computes this set.

It is apparent from the above that, if δ is the optimal number of multiplications needed to evaluate the bilinear forms B_i, $1 \leqslant i \leqslant m$, then δ is the smallest number such that

$$B_i = \sum_{k=1}^{\delta} a_{ik} r_k(x)\, r'_k(y), \qquad 1 \leqslant i \leqslant m,$$

where $a_{ik} \in K$, $r_k(x)$ is a linear form in x, say $r_k(x) = \langle b_k, x\rangle$[1] and $r'_k(y)$ is a linear form in y, say $r'_k(y) = \langle c_k, y\rangle$. Thus, the above expressions can be rewritten as

$$\begin{aligned} B_i = x^T G_i y &= \sum_{k=1}^{\delta} a_{ik} \langle b_k, x\rangle \langle c_k, y\rangle \\ &= x^T \left(\sum_{k=1}^{\delta} a_{ik} b_k c_k^T \right) y, \qquad 1 \leqslant i \leqslant m. \end{aligned}$$

Therefore we conclude that, over K, we have

$$G_i = \sum_{k=1}^{\delta} a_{ik} b_k c_k^T, \qquad 1 \leqslant i \leqslant m. \tag{*}$$

Since a matrix is of rank one if, and only if, it can be written as the outer product of two vectors, we see that the optimal number δ is equal to the smallest number of rank one matrices over K necessary to include the G_i's in their span. On the other hand, (*) also implies that

$$G_i = BA_iC, \qquad 1 \leqslant i \leqslant m,$$

where

$$B = [b_1, b_2, \ldots, b_\delta], \qquad C = \begin{bmatrix} c_1^T \\ c_2^T \\ \vdots \\ c_\delta^T \end{bmatrix},$$

[1] The notation $\langle x, y\rangle$ represents the inner product of x and y.

and

$$A_i = \begin{bmatrix} a_{i1} & & & \\ & a_{i2} & & \\ & & \ddots & \\ & & & a_{i\delta} \end{bmatrix}, \qquad 1 \leqslant i \leqslant m.$$

Another way of stating the above result is that δ is the smallest integer such that each G_i can be expressed as $G_i = BA_iC$, where B, A_i and C are, respectively, $p \times \delta$, $\delta \times \delta$, and $\delta \times q$ matrices over K. Before closing this section, we give an example. Consider the 2×2 matrix multiplication problem

$$\begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \begin{bmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{bmatrix} = \begin{bmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{bmatrix}.$$

The resulting problem consists of computing four bilinear forms z_{ij}, $1 \leqslant i, j \leqslant 2$, in the x's and the y's. One algorithm to compute the z_{ij}'s is the following. First, compute the products:

$$\begin{aligned}
m_1 &= (x_{12} - x_{22})(y_{21} + y_{22}), \\
m_2 &= (x_{11} + x_{22})(y_{11} + y_{22}), \\
m_3 &= (x_{11} - x_{21})(y_{11} + y_{12}), \\
m_4 &= (x_{11} + x_{12})\, y_{22}, \\
m_5 &= x_{11}(y_{12} - y_{22}), \\
m_6 &= x_{22}(y_{21} - y_{11}), \\
m_7 &= (x_{21} + x_{22})\, y_{11}.
\end{aligned}$$

The z_{ij}'s are given by the following formulas:

$$\begin{aligned}
z_{11} &= m_1 + m_2 - m_4 + m_6, \\
z_{12} &= m_4 + m_5, \\
z_{21} &= m_6 + m_7, \\
z_{22} &= m_2 - m_3 + m_5 - m_7.
\end{aligned}$$

Note that the number of multiplications used by the above algorithm is seven compared to eight multiplications required by the ordinary algorithm. Moreover, the constant set K consists of $\{0, 1, -1\} \subseteq Z$. The above algorithm was discovered by Strassen in 1969 [14] and has since then stimulated research in this area.

Another way of stating the above algorithm is to express each G_i as $G_i = CA_iB$, $1 \leqslant i \leqslant 4$, where C, A_i, and B are given as follows:

$$B = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 \\ -1 & 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \qquad C = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ -1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix},$$

$$A_1 = \begin{bmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & 0 & & & & \\ & & & -1 & & & \\ & & & & 0 & & \\ & & & & & 1 & \\ & & & & & & 0 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0 & & & & & & \\ & 0 & & & & & \\ & & 0 & & & & \\ & & & 1 & & & \\ & & & & 1 & & \\ & & & & & 0 & \\ & & & & & & 0 \end{bmatrix},$$

$$A_3 = \begin{bmatrix} 0 & & & & & & \\ & 0 & & & & & \\ & & 0 & & & & \\ & & & 0 & & & \\ & & & & 0 & & \\ & & & & & 1 & \\ & & & & & & 1 \end{bmatrix}, \quad A_q = \begin{bmatrix} 0 & & & & & & \\ & 1 & & & & & \\ & & -1 & & & & \\ & & & 0 & & & \\ & & & & 1 & & \\ & & & & & 0 & \\ & & & & & & -1 \end{bmatrix}.$$

2. The Case with {0, 1} Constants

In this paper, we investigate the complexity of the problem of determining the optimal number of multiplications required to compute a single bilinear form

$$B = \sum_{i=1}^{p} \sum_{j=1}^{q} \alpha_{ij} x_i y_j$$

over the set $K = \{0, 1\} \subseteq Z$ and we later extend the results to an arbitrary set of bilinear forms over $\{0, 1\}$. The main result states that computing the multiplicative complexity of these problems is NP-complete. In this section, we give a graph interpretation together with some mathematical characterizations of the multiplicative complexity of a single bilinear form. But first, we borrow a couple of definitions from graph theory [8, 11].

An *undirected graph* $G = (V, E)$ is an ordered pair consisting of a set V of *vertices* or *nodes* and a set E of *edges*, $E = \{\{v, w\} \mid v, w \in V, v \neq w\}$. G is called *bipartite* if the vertices consist of two nonoverlapping sets V_1 and V_2 such that each edge $e \in E$ has one vertex in V_1 and the other in V_2; we use the notation $G = (V_1, V_2, E)$ to denote the corresponding bipartite graph. A graph $G' = (V', E')$ is a *subgraph* of $G = (V, E)$ if $V' \subseteq V$ and $E' \subseteq E$. The *complete* (or *Kuratowski* graph) *bipartite graph* $K_{l,m}$ is a bipartite graph $G = (V_1, V_2, E)$ such that $|V_1| = l \mid V_2 \mid = m$ and

$$E = \{\{v_1, v_2\} \mid v_1 \in V_1 \text{ and } v_2 \in V_2\}.$$

Let $B = x^T R y = \sum_{i=1}^{p} \sum_{j=1}^{q} \gamma_{ij} x_i y_j$ be a bilinear form such that $\gamma_{ij} \in K = \{0, 1\} \subseteq Z$. We consider bilinear algorithms over K and we are interested in developing a method to determine the multiplicative complexity of B. We can associate with B the bipartite graph $G(B) = (V_1, V_2, E)$ defined as follows: $V_1 = \{v_i\}_{i=1}^{p}$ and $V_2 = \{w_j\}_{1=j}^{q}$ are two sets of distinct nodes corresponding respectively to the indeterminates $\{x_i\}_{i=1}^{p}$ and $\{y_j\}_{j=1}^{q}$;

an edge $e = \{v_i, w_j\}$ is in E if and only if $\gamma_{ij} = 1$. For example, the bilinear form $B = x_1y_1 + x_1y_2 + x_2y_1 + x_2y_2 + x_3y_3 + x_3y_2$ can be represented by the bipartite graph of Fig. 2.1. Note that the optimal algorithm for computing B can be described by the identity $B = (x_1 + x_2)(y_1 + y_2) + x_3(y_2 + y_3)$. The multiplication $(x_1 + x_2)(y_1 + y_2)$ corresponds to the complete subgraph $K_{2,2}$ defined on the vertices $\{v_1, v_2\}$ and $\{w_1, w_2\}$; the other multiplication corresponds to $K_{1,2}$ defined on $\{v_3\}$ and $\{w_2, w_3\}$. We call this a decomposition of G into the subgraphs $K_{2,2}$ and $K_{1,2}$ of length 2.

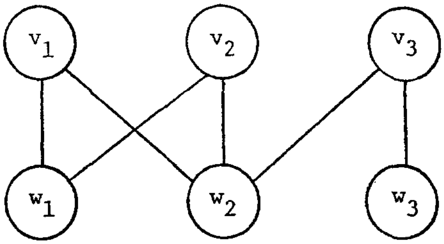


FIGURE 2.1

Let $G(B) = (V, W, E)$ be a bipartite graph associated with a bilinear form B over $\{0, 1\}$. A *decomposition* of $G(B)$ consists of a set of Kuratowski graphs $G_i = (V_i, W_i, E_i)$, $1 \leqslant i \leqslant r$, such that $\bigcup_{i=1}^{r} V_i = V$, $\bigcup_{i=1}^{r} W_i = W$, $\bigcup_{i=1}^{r} E_i = E$ and $E_i \cap E_j = \phi$ for $i \neq j$; r is called the *length* of the decomposition.

THEOREM 2.1. *Given a bilinear form over* $\{0, 1\}$ *with corresponding graph* $G(B)$, *the multiplicative complexity of* B *is equal to the minimal length of a decomposition of* $G(B)$.

Proof. The proof follows from the observation that B has a multiplication of the form $(x_{i_1} + x_{i_2} + \cdots + x_{i_l})(y_{j_1} + y_{j_2} + \cdots + y_{j_s})$ if, and only if, $G(B)$ has the complete bipartite subgraph $K_{l,s}$ whose node set consists of

$$\{v_{i_1}, v_{i_2}, \ldots, v_{i_l}\} \qquad \text{and} \qquad \{w_{j_1}, w_{j_2}, \ldots, w_{j_s}\}. \quad \blacksquare$$

We now give a different characterization of the complexity based on a "linear independence" concept.

Given m vectors $\{v_i\}_{i=1}^{m}$, whose entries are 0 or 1, we say that these vectors are *linearly dependent* over $\{0, 1\}$ if there exists k, $1 \leqslant k \leqslant m$, such that

$$v_k = \sum_{\substack{i=1 \\ i \neq k}}^{m} \alpha_i v_i, \qquad \alpha_i = 0, 1.$$

The vectors $\{v_i\}_{i=1}^{m}$ are called *linearly independent* if they are not linearly dependent. Note that, according to this definition, the vectors

$$\begin{bmatrix}1\\1\\0\\0\end{bmatrix}, \quad \begin{bmatrix}0\\0\\1\\1\end{bmatrix}, \quad \begin{bmatrix}1\\0\\1\\0\end{bmatrix}, \quad \begin{bmatrix}0\\1\\0\\1\end{bmatrix}$$

are linearly independent in spite of the fact that

$$\begin{bmatrix}1\\1\\0\\0\end{bmatrix}+\begin{bmatrix}0\\0\\1\\1\end{bmatrix}=\begin{bmatrix}1\\0\\1\\0\end{bmatrix}+\begin{bmatrix}0\\1\\0\\1\end{bmatrix}.$$

Let R be an $n \times m$ matrix with 0, 1 entries. Define the *column rank* of R as follows: suppose $\{c_i\}_{i=1}^{m}$ are the columns of R. If these vectors are linearly independent, then column rank $(R) = m$; otherwise, let c_k be the column which is the sum of some other columns, then column rank (R) = column rank $(\bar{R})$, where $\bar{R} = (c_1, c_2, \ldots, c_{k-1}, c_{k+1}, \ldots, c_m)$. It is important to notice that the column rank of R is *not* necessarily equal to the maximum number of linearly independent columns of R as the following example shows: let R be given by

$$R=\begin{bmatrix}1&0&1&1&0\\1&1&0&0&0\\0&0&0&1&1\\1&1&0&1&1\end{bmatrix}.$$

The columns

$$\begin{bmatrix}1\\1\\0\\1\end{bmatrix},\quad\begin{bmatrix}0\\1\\0\\1\end{bmatrix},\quad\begin{bmatrix}1\\0\\1\\1\end{bmatrix},\quad\begin{bmatrix}0\\0\\1\\1\end{bmatrix}$$

are linearly independent; however, column rank $(R) = 3$ since

$$\text{column rank }(R) = \text{column rank}\left(\begin{bmatrix}0&1&1&0\\1&0&0&0\\0&0&1&1\\1&0&1&1\end{bmatrix}\right)$$

$$= \text{column rank}\left(\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\\1&0&1\end{bmatrix}\right) = 3.$$

It is clear that the column rank is well defined; i.e., we get the same answer regardless of the order of the columns taken out of R. We can similarly define the *row rank* of R. We remakr that the column rank and the row rank of a matrix are in general different. The matrix

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

has column rank $(R) = 5$ and row rank $(R) = 4$.

The following theorem shows the usefulness of the above definitions.

THEOREM 2.2. *Let $B = x^T Ry$ be an $n \times m$ bilinear form over* $\{0, 1\}$. *The multiplicative complexity r of B is* $\leqslant$min(*row rank*(R), *column rank* (R)).

Proof. Let $\{c_i\}_{i=1}^m$ be the columns of R. Suppose

$$c_k = \sum_{\substack{i=1\\ i\neq k}}^{m} \alpha_i c_i , \qquad \alpha_i \in \{0, 1\},$$

for some k, $1 \leqslant k \leqslant m$. Note that $B = x^T Ry = \sum_{i=1}^m \langle x, c_i\rangle y_i$; thus

$$B = \langle x, c_k\rangle y_k + \sum_{\substack{i=1\\ i\neq k}}^{m} \langle x, c_i\rangle y_i .$$

Now since

$$c_k = \sum_{\substack{i=1\\ i\neq k}}^{m} \alpha_i c_i ,$$

we have

$$\begin{aligned} B &= \sum_{\substack{i=1\\ i\neq k}}^{m} \langle x, \alpha_i c_i\rangle y_k + \sum_{\substack{i=1\\ i\neq k}}^{m} \langle x, c_i\rangle y_i \\ &= \sum_{\substack{i=1\\ i\neq k}}^{m} \langle x, c_i\rangle(\alpha_i y_k + y_i). \end{aligned}$$

Therefore, we need at most $m - 1$ multiplications to compute B. Continuing in this fashion, it is easy to see that $\mu \leqslant$ column rank (R) Similarly, $\mu \leqslant$ row rank (R) and thus $\mu \leqslant$ min(column rank (R), row rank (R)). ▮

Unfortunately, we may have $\mu <$ min(column rank (R), row rank (R)) as the following example shows. Let R be given by

$$R = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

It is easy to check that row rank (R) = column rank $(R) = 5$. However, the following algorithm requires four multiplications only.

$$B = (x_1 + x_2)(y_1 + y_2) + (x_5 + x_6)(y_1 + y_3) + (x_3 + x_4)(y_3 + y_4) \\ + (x_1 + x_4)(y_5 + y_6).$$

Finally, we give the following characterization.

THEOREM 2.3. *Let $B = x^T R y$ be an $n \times m$ bilinear form with 0, 1 entries. The multiplicative complexity of B is the smallest r such that $R = XY$, where X and Y are $n \times r$ and $r \times m$ matrices with 0, 1 entries.*

Proof. Immediate from the fact that the multiplicative complexity is the smallest r such that $R = XDY$, where X, D and Y are respectively $n \times r$, $r \times r$ and $r \times m$ matrices with 0, 1 entries and where D is diagonal. ∎

3. Minimizing the Number of Multiplications is *NP*-Complete

In this section, we prove that the following problem (which we call the *MP* problem) is *NP*-complete: Given a $p \times q$ matrix with 0, 1 entries and given a positive integer m, does there exist two matrices A and B such that $R = AB$, A and B are respectively $p \times m$ and $m \times q$ matrices with 0, 1 entries? We reduce the 3-colorability problem [13] into an instance of the above problem.

The 3-*colorability* problem can be stated as follows: given an undirected graph $G = (N, E)$, does there exist three disjoint sets of vertices (S_1, S_2, S_3) such that $\bigcup_{i=1}^{3} S_i = N$ and if $\{v_i, v_j\} \in E$, then v_i and v_j are in different sets?

Actually, we use a slightly modified version of the 3-colorability problem which we call the $3 - m$ *colorability* problem and which can be stated as follows: given an undirected connected graph $G = (N, E)$ such that $\deg v \geqslant 4$, for all $v \in N$, and $|E| > 2|N| + 1$, is G 3-colorable?

The following theorem shows that the above problem is also *NP*-complete.

THEOREM 3.1. *The $3 - m$ colorability problem is NP-complete.*

Proof. It is simple to check that the $3 - m$ colorability problem is in *NP*. To complete the proof, we reduce the 3-colorability problem to an instance of the above problem.

Let $G_0 = (N_0, E_0)$ be any graph; without loss of generality, we can assume that G_0 is connected. Create three distinct copies $G_1 = (N_1, E_1)$ $G_2 = (N_2, E_2)$ and $G_3 = (N_3, E_3)$ of G_0 and consider the graph $G = (V, E)$ such that $V = N_0 \cup N_1 \cup N_2 \cup N_3$ and

$$E = E_0 \cup E_1 \cup E_2 \cup E_3 \cup \{\{v_i^{(0)}, v_j^{(1)}\}, \{v_i^{(0)}, v_j^{(2)}\}, \{v_i^{(0)}, v_j^{(3)}\}, \{v_i^{(1)}, v_j^{(2)}\}, \\ \{v_i^{(1)}, v_j^{(3)}\}, \{v_i^{(2)}, v_j^{(3)}\} \mid \{v_i^{(0)}, v_j^{(0)}\} \in E\}.$$

Note that $|E| = 10|E_0|$ and $|V| = 4|N_0|$; since G_0 is connected, we have that $|E_0| \geqslant |N_0| - 1$ and hence $|E| = 10|E_0| \geqslant 10|N_0| - 10 = (5/2)|N| - 10 \geqslant 2|N| + 1$, wherever $|N_0| \geqslant 5$, which we can assume without loss of generality.

We claim that G_0 is 3-colorable iff G is

(1) Suppose G_0 is 3-colorable and let $(S_1^{(0)}, S_2^{(0)}, S_3^{(0)})$ be the corresponding partition of nodes of G_0. Define $S_i^{(j)} = \{v_l^{(j)} \mid v_l^{(0)} \in S_i^{(0)}\}$, for $i = 1, 2, 3$ and $j = 1, 2, 3$. Consider the partition of the nodes of G, $(S_1^{(0)} \cup S_1^{(1)} \cup S_1^{(2)} \cup S_1^{(3)}, S_2^{(0)} \cup S_2^{(1)} \cup S_2^{(2)} \cup S_2^{(3)}, S_3^{(0)} \cup S_3^{(1)} \cup S_3^{(2)} \cup S_3^{(3)})$. Clearly, this defines a 3-coloration of G.

(2) Suppose now that G is 3-colorable with induced partition (S_1, S_2, S_3). Let $S_i^{(0)} = \{v_k^{(0)} \mid v_k^{(0)} \in S_i)$ for $i = 1, 2, 3$. It is easy to see that $(S_1^{(0)}, S_2^{(0)}, S_3^{(0)})$ defines a 3-coloration for G_0. ∎

We need one lemma before establishing the main theorem of this section.

LEMMA 3.2. *Given a graph* $G = (N, E)$, $\deg v \geqslant 4$, $v \in N$, *the elimination of k edges leaves at most k/2 nodes of degree zero.*

Proof. Let S be the set of nodes whose degrees becomes zero after the elimination of the k edges. Suppose k_1 of the edges eliminated were adjacent to two nodes in S and k_2 of the edges eliminated were adjacent to only one node in S. Clearly $k \geqslant k_1 + k_2$. Since each node in S had degree at least four then $2k_1 + k_2 \geqslant 4|S|$. Hence, $4|S| \leqslant 2k$ or $|S| \leqslant k/2$. ∎

THEOREM 3.3. *The MP problem is NP-complete.*

Proof. It is straightforward to check that MP is in NP. We now show how to reduce the $3 - m$ colorability problem to MP in polynomial time.

Let $G = (N, E)$ be an undirected graph in which each vertex is of degree greater than or equal to 4 and $|E| > 2|N| + 1$. Let $N = \{v_1, v_2, ..., v_n\}$ and $E = \{e_1, e_2, ..., e_r\}$, where $n = |N|$ and $r = |E|$. From G, we construct the following instance of the MP problem. Take $p = 6n + 3r + 1$, $q = 6r + n$ and $m = 3r + 6n$; clearly, $q > m$.

The set of constants $\{\gamma_{ij}\}$ defining R is constructed as follows:

(a1) for each vertex $v_i \in N$ and all edges $e_j \in E$ incident upon v_i, set

$$\begin{aligned}\gamma_{ij} &= \gamma_{n+i,r+j} = \gamma_{2n+i,2r+j} = \gamma_{3n+3r+i,3r+n+j}\\ &= \gamma_{3r+4n+i,4r+n+j} = \gamma_{3r+5n+i,5r+n+j} = 1.\end{aligned}$$

(a2) for each i, $1 \leqslant i \leqslant n$, set

$$\gamma_{i,3r+i} = \gamma_{n+i,3r+i} = \gamma_{2n+i,3r+i} = 1.$$

(a3) for each j, $1 \leqslant j \leqslant 3r$, set

$$\gamma_{3n+j,j} = \gamma_{3n+j,3r+n+j} = 1.$$

(a4) for j, $1 \leqslant j \leqslant 6r + n$, set

$$\gamma_{3r+6n+1,j} = 1.$$

(a5) set all other γ_{ij} to zero.

Figure 3.1 shows the matrix $R = (\gamma_{ij})$. G_0 is the incidence matrix of the graph G, i.e., it is an $n \times r$ matrix such that the entry (i, j) is equal to 1 if and only if v_i is incident upon e_j. I_k represents the identity matrix of size k. Row x consists of a sequence of consecutive 1's.

	r	r	r	n	r	r	r
n	G_0	0	0	I_n	0	0	0
n	0	G_0	0	I_n	0	0	0
n	0	0	G_0	I_n	0	0	0
r	I_r	0	0	0	I_r	0	0
r	0	I_r	0	0	0	I_r	0
r	0	0	I_r	0	0	0	I_r
n	0	0	0	0	G_0	0	0
n	0	0	0	0	0	G_0	0
n	0	0	0	0	0	0	G_0
				x			

FIGURE 3.1

We will prove that G is 3-colorable if, and only if, R can be expressed as $R = AB$, where A and B are $p \times m$ and $m \times q$ matrices with 0, 1 entries (recall that $m = 3r + 6n$).

(1) Suppose that G is 3-colorable and let $\{S_1, S_2, S_3\}$ be the corresponding partition of the nodes of G. Let A and B be the following matrices shown in Fig. 3.2. Row y of A is constructed as follows:

n	n	n	r	r	r	n	n	n
S_1	S_2	S_3	(S_2, S_3)	(S_1, S_3)	(S_1, S_2)	S_1	S_2	S_3

where

(b1) for all $v_i \in S_k$, $y[(k-1)n + i] = y[3r + (k-1)n + i] = 1$,

(b2) for all edges e_j incident upon a vertex in S_2 and a vertex in S_3, set

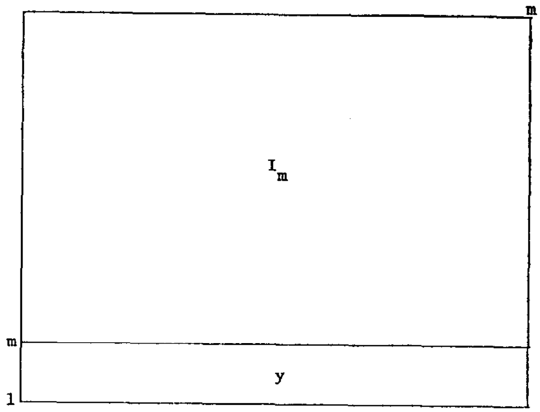
$$y[3n + j] = 1,$$

(b3) for all edges e_j incident upon a vertex in S_1 and a vertex in S_3, set

$$y[3n + r + j] = 1,$$

(b4) for all edges e_j incident upon a vertex in S_1 and a vertex in S_2, set

$$y[3n + 2r + j] = 1.$$



A

$$\begin{array}{c|ccccccc|}
 & r & r & r & n & r & r & r \\
\hline
n & G_0 & 0 & 0 & I_n & 0 & 0 & 0 \\
n & 0 & G_0 & 0 & I_n & 0 & 0 & 0 \\
n & 0 & 0 & G_0 & I_n & 0 & 0 & 0 \\
r & I_r & 0 & 0 & 0 & I_r & 0 & 0 \\
r & 0 & I_r & 0 & 0 & 0 & I_r & 0 \\
r & 0 & 0 & I_r & 0 & 0 & 0 & I_r \\
n & 0 & 0 & 0 & 0 & G_0 & 0 & 0 \\
n & 0 & 0 & 0 & 0 & 0 & G_0 & 0 \\
n & 0 & 0 & 0 & 0 & 0 & 0 & G_0 \\
\hline
\end{array}$$

B

FIGURE 3.2

To prove that $R = AB$, it is clear that we only have to verify that $yB = x$, whose proof is given by the following lemma.

LEMMA 1. *Let y and B be as defined in Fig. 3.2 and let x be a row vector consisting of 1's. Then we have $yB = x$.*

Proof of Lemma 1. The equation $yB = x$ is equivalent to

$$\sum_{l=1}^{m} y_l b_{jl} = 1, \qquad \text{for all} \quad j = 1, 2,..., 6r + n. \tag{*}$$

We distinguish several cases.

Case 1. $1 \leqslant j \leqslant r$.
Let $e_j = \{v_i, v_k\}$. It is easy to see from the construction of B that

$$b_{ij} = b_{kj} = b_{3n+j,j} = 1 \qquad \text{and} \qquad b_{ij} = 0 \text{ otherwise.}$$

Either one of v_i or v_k belongs to S_1 or $v_i \in S_2$ and $v_k \in S_3$ (say). In the first case, precisely one of $y[i]$ or $y[k]$ is equal to 1 and $y[3n + j] = 0$; in the second case, $y[3n + j] = 1$ and $y[i] = y[k] = 0$. In either case, (*) is satisfied.

Case 2. $r + 1 \leqslant j \leqslant 3r$ or $3r + n + 1 \leqslant j \leqslant 6r + n$.
The proof is similar to that of Case 1.

Case 3. $3r + 1 \leqslant j \leqslant 3r + n$.

The only nonzero elements in row j of matrix B are $b_{j,3r+j}$, $b_{n+j,3r+j}$, and $b_{2n+j,3r+j}$. If $v_j \in S_k$, then $y[(k-1)n + j] = 1$ and $y[(k'-1)n + j] \neq 1$ for all $k' \neq k$. Thus $\sum_{l=1}^{m} y_l b_{jl} = 1$. ∎

Proof of Theorem 3.3 (*continued*). The above lemma completes the proof that, if G is 3-colorable, then $R = AB$, where A and B are $p \times (3r + 6n)$ and $(3r + 6n) \times q$ matrices with 0, 1 entries.

(2) Suppose that $R = AB$ with $m = 3r + 6n$. We will prove that G is 3-colorable. The main proof is contained in the following lemma.

LEMMA 2. *Let R be as given in Fig.* 3.1 *and let A and B be any two $p \times m$ and $m \times q$ matrices of* 0*'s and* 1*'s such that $R = AB$. Then A and B must be of the form given in Fig.* 3.2.

Proof of Lemma 2. We actually prove that if $\bar{R} = AB$, where $\bar{R}$ is the same as R without the last row (i.e., row x) and A and B are $(p - 1) \times m$ and $m \times q$ matrices, then $A = I_m$ and $B = \bar{R}$. The proof is based upon the characterization given in Theorem 2.1.
The bipartite graph $G(\bar{R})$ corresponding to $\bar{R}$ is given in Fig. 3.3, where there are two types of edges:

(a) edges which represent the incidence matrix and which exist among the following sets of nodes:

$\{x_1, \ldots, x_n\}$	and	$\{y_1, \ldots, y_r\}$,
$\{x_{n+1}, \ldots, x_{2n}\}$	and	$\{y_{r+1}, \ldots, y_{2r}\}$,
$\{x_{2n+1}, \ldots, x_{3n}\}$	and	$\{y_{2r+1}, \ldots, y_{3r}\}$,
$\{x_{3n+3r+1}, \ldots, x_{4n+3r}\}$	and	$\{y_{3r+n+1}, \ldots, y_{4r}\}$,
$\{x_{4n+3r+1}, \ldots, x_{5n+3r}\}$	and	$\{y_{4r+n+1}, \ldots, y_{5r+n}\}$,
$\{x_{5n+3r+1}, \ldots, x_{6n+3r}\}$	and	$\{x_{5r+n+1}, \ldots, y_{6r+n}\}$.

Note that, for example, an edge between x_i and y_j, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant r$, exists if and only if the node v_i of G is incident upon e_j.

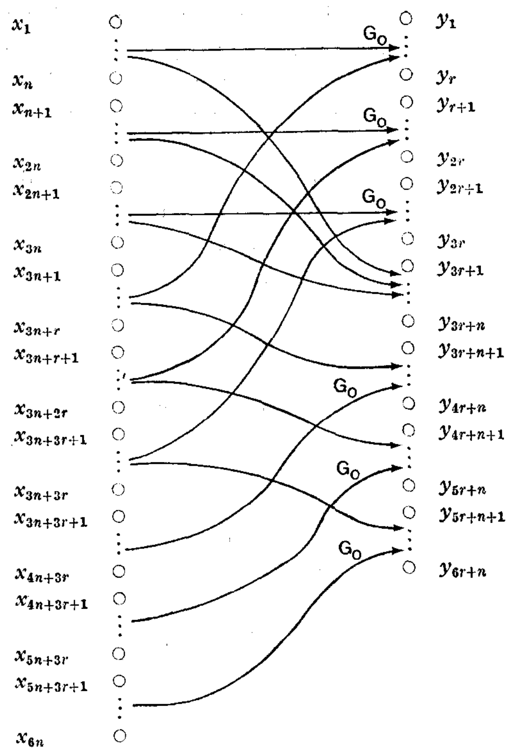


FIGURE 3.3

(b) edges which represent I_n or I_r and which exist among the following set of nodes:

$\{x_1, \ldots, x_n\}$	and	$\{y_{3r+1}, \ldots, y_{3r+n}\}$,
$\{x_{n+1}, \ldots, x_{2n}\}$	and	$\{y_{3r+1}, \ldots, y_{3r+n}\}$,
$\{x_{2n+1}, \ldots, x_{3n}\}$	and	$\{y_{3r+1}, \ldots, y_{3r+n}\}$,
$\{x_{3n+1}, \ldots, x_{3n+r}\}$	and	$\{y_1, \ldots, y_r\}$,
$\{x_{3n+r+1}, \ldots, x_{3n+2r}\}$	and	$\{y_{r+1}, \ldots, y_{2r}\}$,
$\{x_{3n+2r+1}, \ldots, x_{3n+3r}\}$	and	$\{y_{2r+1}, \ldots, y_{3r}\}$,
$\{x_{3n+1}, \ldots, x_{3n+r}\}$	and	$\{y_{3r+n+1}, \ldots, y_{4r+n}\}$,
$\{x_{3n+r+1}, \ldots, x_{3n+2r}\}$	and	$\{y_{4r+n+1}, \ldots, x_{5n+n}\}$,
$\{x_{3n+2r+1}, \ldots, x_{3n+2r}\}$	and	$\{y_{5r+n+1}, \ldots, y_{6r+n}\}$.

Note that $G(\bar{R})$ has only two types of complete subgraphs $K_{1,l}$ and $K_{r,1}$,[2] where r, $l \geqslant 1$. The statement of the lemma can be reformulated as follows: $G(\bar{R})$ has only one

[2] Note that $K_{m,n}$ is the complete graph based on m nodes among the x_i's and n nodes among the y_j's.

decomposition of length $3r + 6n$ and this decomposition is obtained by taking each x_i and constructing the complete subgraph consisting of all edges incident upon x_i. The main idea of the proof is to show that any decomposition of $G(\bar{R})$ which contains complete subgraphs of the type $K_{r,l}$, $r > 1$, has length greater than $3r + 6n$. We now prove this fact.

Consider any decomposition D of $G(\bar{R})$ of length $3r + 6n$ and suppose it contains α complete subgraphs of the type $K_{r,1}$, $r > 1$. Each such $K_{r,1}$ has one vertex among the y_j's, say y_{j_r}. Therefore α can be expressed as $\alpha = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7$, where α_i is the number of $K_{r,1}$ subgraphs with j_r belonging to the ith set of nodes which form the y_j's.

We now remove the edges corresponding to the above $K_{r,1}$ subgraphs and try to determine the number of the x_i's nodes whose degrees are nonzero. Removing the first $\alpha_1 + \alpha_2 + \alpha_3$ subgraphs destroys no x_i's. If we next remove the α_4 subgraphs, then, at most, $\min(\alpha_1/2, \alpha_4) + \min(\alpha_2/2, \alpha_4) + \min(\alpha_3/2, \alpha_4)$ of the x_i's will disappear completely (Lemma 3.2). Deleting the next α_5 subgraphs can cause at most $\min(\alpha_5, \alpha_1) + (\alpha_5/2)$ x_i nodes to disappear. Similarly, taking out the remaining subgraphs can result in the removal of at most $\min(\alpha_6, \alpha_2) + \alpha_6/2 + \min(\alpha_7, \alpha_5) + \alpha_7/2$ x_i nodes.

It follows that the maximum number of x_i nodes which could disappear is given by

$$\mu = \min\left(\frac{\alpha_1}{2}, \alpha_4\right) + \min\left(\frac{\alpha_2}{2}, \alpha_4\right) + \min\left(\frac{\alpha_3}{2}, \alpha_4\right)$$
$$+ \min(\alpha_5, \alpha_1) + \frac{\alpha_5}{2} + \min(\alpha_6, \alpha_2) + \frac{\alpha_6}{2} + \min(\alpha_7, \alpha_3) + \frac{\alpha_7}{2}.$$

Three cases arise:

(i) $\alpha_4 \geqslant 1$. Using the fact that $\min(k_1, k_2) \leqslant (k_1 + k_2)/2$ and $\min(k_1, k_2) \leqslant k_1$ or k_2, we obtain

$$\mu \leqslant \left(\frac{\alpha_1}{2} + \frac{\alpha_2}{2} + \frac{\alpha_3}{2}\right) + \left(\frac{\alpha_5 + \alpha_1}{2}\right) + \frac{\alpha_5}{2} + \left(\frac{\alpha_6 + \alpha_2}{2}\right) + \frac{\alpha_6}{2} + \left(\frac{\alpha_7 + \alpha_3}{2}\right) + \frac{\alpha_7}{2}$$

$$\mu \leqslant \alpha_1 + \alpha_2 + \alpha_3 + \alpha_5 + \alpha_6 + \alpha_7 = \alpha - \alpha_4.$$

But since all the remaining subgraphs of $\mathscr{D}$ are of type $K_{1,l}$, then $\mathscr{D}$ must have at least $6n + 3r - (\alpha - \alpha_4)$ such complete subgraphs. Therefore, the length of $\mathscr{D}$ is at least

$$\alpha + (6n + 3r - (\alpha - \alpha_4)) = 6n + 3r + \alpha_4 > 6n + 3r,$$

which contradicts the assumption that the length of $\mathscr{D}$ is $6n + 3r$.

(ii) $\alpha_4 = 0$ and $\alpha_1 + \alpha_2 + \alpha_3 \geqslant 1$. In this case,

$$\mu = \min(\alpha_5, \alpha_1) + \frac{\alpha_5}{2} + \min(\alpha_6, \alpha_2) + \frac{\alpha_6}{2} + \min(\alpha_7, \alpha_3) + \frac{\alpha_7}{2}.$$

Thus

$$\mu \leqslant \alpha_5 + \alpha_6 + \alpha_7 + \frac{\alpha_1}{2} + \frac{\alpha_2}{2} + \frac{\alpha_3}{2}.$$

It is easy to check that $\mu \leqslant \alpha_1 + \alpha_2 + \alpha_3 + \alpha_5 + \alpha_6 + \alpha_7 - 1$ and the proof carries as before.

(iii) $\alpha_4 = 0$ and $\alpha_1 + \alpha_2 + \alpha_3 = 0$. It is clear that $\mu \leqslant (\alpha_5 + \alpha_6 + \alpha_7)/2$ and the proof is similar to proofs in the previous cases.

Therefore any decomposition of $G(\bar{R})$ which contains subgraphs of the type $K_{r,1}$, > 1, has to be of length greater than $6n + 3r$. ▌

Proof of Theorem 3.3 (*continued*). We now know that for any A and B such that $R = AB$, both A and B must be of the form given in Fig. 3.2. Note that row y of A has not been specified. Define the following three sets of nodes in G:

$$\begin{aligned} D_1 &= \{v_j \mid y[j] = 1\}, \\ D_2 &= \{v_j \mid y[n+j] = 1\}, \\ D_3 &= \{v_j \mid y[2n+j] = 1\}. \end{aligned}$$

These sets are pairwise disjoint because if $v_K \in D_1 \cap D_2$, say, then multiplying y by the $(3r + k)$th column of B produces a sum of 2 which is not correct. Moreover, these sets exhaust all the nodes of G by the fact that

$$y \begin{bmatrix} I_n \\ I_n \\ I_n \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = [\overbrace{1 \quad 1 \quad \cdots \quad 1}^{n}].$$

We now prove that no edge has its two nodes in one set D_i. Suppose $e_j = \{v_i, v_l\}$ is such that v_i and v_l are in D_k. Multiplying y by the $((k-1)r + j)$th column of B results in a number greater than one since $y[(k-1)n + i] = y[(k-1)n + l] = 1$. It follows that the above partition of vertices defines a 3-coloration for G and the proof of the theorem is complete. ▌

We have the following immediate corollary.

COROLLARY. *Given a set of bilinear forms $\{B_i\}_{i=1}^{m}$ over $\{0, 1\}$ and given a positive integer δ, the problem of determining whether or not these bilinear forms can be computed with δ multiplications is NP-complete.*

All of the above results rely heavily on the fact that the constant set is $\{0, 1\} \subseteq Z$. A much more interesting case is when the constant set consists of $\{0, 1, -1\}$ as in most of the published algorithms. Finding the corresponding complexity seems to be harder in this case; however, we could not extend the above proofs to cover this case. It is worth mentioning that, for a given single bilinear form $B = \sum_{i,j} \gamma_{ij} x_i y_j$, $\gamma_{ij} = 0, 1$, the introduction of subtraction can reduce the number of multiplications as the following example shows.

Let $B = x^T R y$, where R is the following 8×8 matrix:

$$R = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

It is simple to check that seven multiplications are necessary and sufficient to compute B over $\{0, 1\}$. However, the following algorithm over $\{0, 1, -1\}$ uses only six multiplications.

$$\begin{aligned} B = {} & (x_1 + x_2 + x_4)(y_1 + y_2 + y_4) + (x_3 + x_6)(y_1 + y_6) \\ & + (x_1 + x_2 + x_5)(y_3 + y_5) + (x_3 + x_7)(y_2 + y_7) + (x_3 + x_8)(y_3 + y_8) \\ & - (x_1 + x_2 + x_3)(y_1 + y_2 + y_3). \end{aligned}$$

4. Complexity of Related Problems

As we have seen in Section 2, the multiplicative complexity of a single bilinear form B over $\{0, 1\}$ is related to the length of a decomposition of the associated bipartite graph $G(B)$. In view of Theorem 3.3, we have the following immediate result.

THEOREM 4.1. *Given a bipartite graph G and a positive integer k, the problem of determining whether G has a decomposition of length k is NP-complete.*

We can use the graph formulation of the problem to prove that even the following problem is NP-complete: Given a bilinear form B over $\{0, 1\}$ and given a positive integer l does there exist a bilinear algorithm to compute B with one multiplication of the form $(x_{i_1} + x_{i_2} + \cdots + x_{i_l})(y_{j_1} + y_{j_2} + \cdots + y_{j_l})$?

THEOREM 4.2. *Given an $n \times n$ bilinear form B over $\{0, 1\}$ and an integer l, the problem of determining whether there exists an algorithm with one multiplication of the form $(x_{i_1} + x_{i_2} + \cdots + x_{i_l})(y_{j_1} + y_{j_2} + \cdots + y_{j_l})$ is NP-complete.*

Proof. This can be obtained from a simple reduction from the clique problem (see also [7]). ∎

The above results are all related to the number of multiplications required to compute a bilinear form. We now focus on the number of additions. We note that the following problem is known to be NP-complete [4, 7].

PROBLEM. Given a set of expressions with one commutative and associative operator $+$ and given an integer l. Is it possible to compute this set of expressions with l additions?

Using the above fact, it is easy to see that the following is true.

LEMMA 4.3. *Given a bilinear form B over $\{0, 1\}$ and given an integer l, the problem of determining whether B can be computed with l additions is NP-complete even if we fix the number of multiplications.*

Another context in which these results are relevant is that of evaluation of arithmetic expressions [5]. Given an arithmetic expression A, it is ordinary to represent A by a *directed acyclic graph* (dag) which identifies the common subexpressions. For example, the expression $(d + f) * (a + b) + (a + b) * c$ can be represented by the dag of Fig. 4.1. Note that an interior node represents an operator and a leaf represents a variable

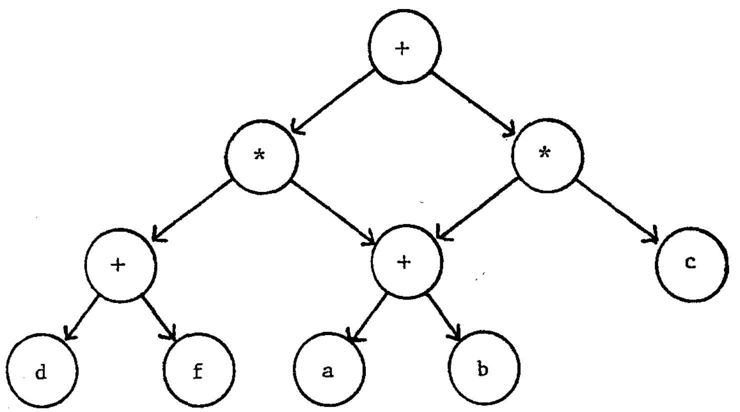


FIGURE 4.1

name. The order of the children is important; the left child represents the first operand and the right child represents the second operand. Assuming that the standard arithmetic laws hold (associativity, commutativity, and distributivity of multiplication with respect to addition), an interesting problem in code optimization is to find, for a given dag, an equivalent dag which has the fewest number of interior nodes. A bilinear expression can be viewed as represented by a special type of dags, namely leaf dags; a *leaf dag* is a dag such that all the *shared* nodes (a *shared node* is a node with more than one parent) are leaves. For example, the bilinear expression $x_1 * y_1 + (x_1 * y_2 + x_2 * y_2)$ can be represented by the leaf dag of Fig. 4.2. The above results show that evaluating arithmetic expressions is hard even for leaf dags.

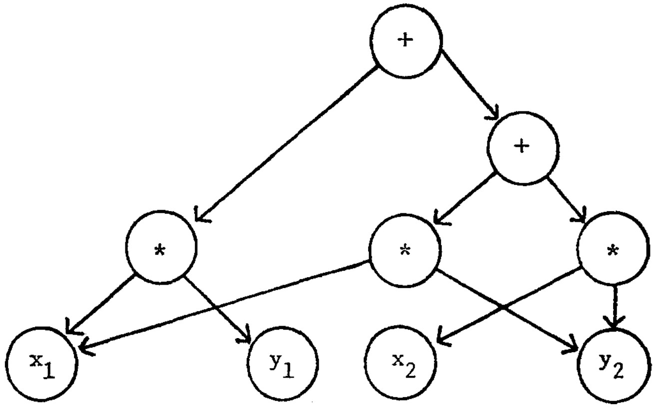


FIGURE 4.2

THEOREM 4.4. *Given a leaf dag which corresponds to a bilinear arithmetic expression, the following two problems are NP-hard*:

(1) *minimizing the number of nodes corresponding to* $\circledast$.

(2) *minimizing the number of* $\oplus$ *nodes with the number of* $\circledast$ *nodes fixed.*

5. EXTENSION TO COMMUTATIVE ALGORITHMS

The bilinear algorithms we have been considering are noncommutative in the sense that the indeterminates do not commute, i.e., $x_i y_j \neq y_j x_i$. However, it is clear that the multiplicative complexity of a single bilinear form is the same whether or not the indeterminates commute. However, we feel that the commutative case is harder and we will justify this fact by displaying a class of bilinear forms whose complexity is easy to obtain in the noncommutative case but which is NP-complete in the commutative case.

Let $\{x_i\}_{i=1}^k$ be a set of indeterminates and let g be one indeterminate different from all x_i's. We are interested in investigating the complexity of computing a set of arithmetic expressions of the form

$$B_i = g x_{i_1} x_{i_2}, \qquad 1 \leqslant i \leqslant m, \quad i_1 \neq i_2,$$

where $\{x_{i_1}, x_{i_2}\} \neq \{x_{j_1}, x_{j_2}\}$ for $i \neq j$. If we do not allow commutativity, there is a simple efficient algorithm which computes $\{B_i\}_{i=1}^m$ optimally. However, if we allow commutativity, the following theorem shows that the above problem is NP-complete.

THEOREM 5.1. *Given a set of expressions $\{B_i\}_{i=1}^m$ of the above form and given an integer l, the problem of determining whether this set can be computed with l multiplications in the commutative case is NP-complete.*

Proof. This problem can be viewed as the multiplicative dual of the one stated before Lemma 4.3 and precisely the same proof carries in this case. ∎

6. Conclusion

An important class of arithmetic problems has been identified as a member of the family of NP-complete problems. As we mentioned earlier, the restriction to the constants $\{0, 1\}$ is crucial to the proofs, and no cancellation whatsoever was allowed. It is our belief that the problem remains NP-complete even if we allow negation, but a more algebraic approach is needed in this case. Our restriction here conforms with that of the monotone models, and our results can be directly translated in the terminology of monotone models.

7. References

1. A. Aho, J. Hopcroft, and J. Ullman, "The Design and Analysis of Computer Algorithmas, Addison–Wesley Reading, Mass., 1974.
2. R. W. Brockett and D. Dobkin, On the optimal evaluation of a set of bilinear forms, *Linear Algebra and Appl.* **19** (1978), 207–235.
3. A. Borodin and I. Munro, "Computational Complexity of Algebraic and Numeric Problems," American Elsevier, New York, 1975.
4. P. Downey and R. Sethi, Variations on the common subexpression problem, unpublished manuscript.
5. T. Gonzalez and J. Ja'Ja', "Evaluation of Arithmetic Expressions with Algebraic Identities," Technical Report 78-13, Department of Computer Science, The Pennsylvania State University, August 1978.
6. M. R. Garey, D. S. Johnson, and L. J. Stockmeyer, Some somplified NP-complete graph problems, *Theoret. Comput. Sci.* **1**, 1976, 237–267.
7. M. R. Garey and D. S. Johnson, "Computers and Intractibility: A Guide to the Theory of NP-completeness," Freeman, San Francisco (1979).
8. F. Harary, "Graph Theory," Addison–Wesley, Reading, Mass., 1969.
9. J. Ja'Ja', "On the Algebraic Complexity of Classes of Bilinear Forms," Ph.D. thesis, Harvard University, September 1977.
10. R. Karp, Reducibilities among combinatorial problems, *in* "Complexity of Computer Computations" (R. E. Miller and J. W. Thatcher, Eds.), pp. 85–104, Plenum, New York, 1972.
11. E. L. Lawler, "Combinatorial Optimization: Networks and Matroids," Holt, Rinehart & Winston, 1976.
12. Y. Matijasevic, Enumerable sets are diaphantine, *Dokl. Acad. Nauk SSSR* **191** (1970), 279–282.
13. L. J. Stockmeyer, Planar 3-colorability is polynomial complete, *ACM SIGACT News* **5**, 3 (1973), 19–25.
14. V. Strassen, Gaussian elimination is not optimal, *Numer. Math.* **13** (1969), 354–356.
15. L. G. Valiant, Negation can be exponentially powerful, *in* "Proceedings, Eleventh Annual ACM Symposium on Theory of Computing, Atlanta, Georgia, 1979."
16. S. Winograd, Arithmetic complexity computations, Lecture Notes, given at the Conference on Algebraic Complexity and Its Applications to Problems in Engineering and Computer Science, University of Pittsburgh, August 1978.