

# ONS WITH ALGEBRAIC IDENTITIES IS HARD

inary version)

z\* and Joseph Ja'Ja'\*

of Computer Science

nia State University

y Park, PA 16802

degree 2. We should note that our result holds also in the case where multiplication is commutative. On the other hand, in the case where it is possible to eliminate common subexpressions, the problem can be solved in polynomial time ([GJ]).

Other related problems in graph theory and arithmetic complexity are also shown to be NP-complete.

We now define precisely our general problem. Let  $\Sigma$  be a countable set of variable names and let  $\theta = \{+, *\}$  be the set of binary operators on  $\Sigma$  such that the following laws hold:

(i)  $+$  and  $*$  are associative, i.e.,

$$(a + b) + c = a + (b + c)$$

$$(a * b) * c = a * (b * c), \text{ for all } a, b, c \in \Sigma$$

(ii)  $+$  is commutative, i.e.,

$$a + b = b + a, \text{ for all } a, b \in \Sigma$$

(iii)  $*$  is distributive with respect to  $+$ , i.e.,

$$a * (b + c) = a * b + a * c$$

$$(b + c) * a = b * a + c * a, \text{ for all } a, b, c \in \Sigma.$$

The main reason we have not assumed that  $*$  is commutative is that the same techniques can be applied to a matrix expression (in parallel computation) to reduce the number of arithmetic operations. We should note that the results of section 2 will also hold when  $*$  is commutative.

A  $\sigma$ -dag is a dag with a single root whose interior nodes are either  $+$  or  $*$  from  $\theta$  and whose leaves are from  $\Sigma$ . Our problem can now be stated as follows: given a  $\sigma$ -dag  $D$ , find an equivalent dag  $D'$  with the fewest number of interior nodes.

## 2. NP-completeness result for expression dags

It is easy to check that if the given dag is a tree, the corresponding problem is trivial. The next simplest class of dags is that of leaf dags. Moreover, any arithmetic expression which involves both operators  $+$  and  $*$  got to be of degree at least 2. Therefore, the simplest type of  $\sigma$ -dags beyond trees is the class of leaf dags whose corresponding expressions are of degree 2. We define a subclass of these dags, namely those corresponding to bilinear arithmetic expressions. An arithmetic expression  $B$  is bilinear if it is of the form

$$B = x_{i_1} * y_{j_1} + x_{i_2} * y_{j_2} + \dots + x_{i_k} * y_{j_k},$$

where  $\{x_i\}$  and  $\{y_j\}$  are nonoverlapping sets of variables and  $(i_\ell, j_\ell) \neq (i_{\ell'}, j_{\ell'})$ .

A bilinear expression can also be represented as  $B = x^T R y$ , where  $r_{ij} = 1$  iff  $x_i * y_j$  appears in  $B$ , otherwise,  $r_{ij} = 0$ .

**Theorem 2.1:** Let  $B = x^T R y$  be an  $n \times m$  bilinear arithmetic expression. The fewest number of multiplications needed to compute  $B$  is equal to the smallest  $r$  such that  $R = XY$ , where  $X$  and  $Y$  are  $n \times r$  and  $r \times m$  matrices with 0, 1 entries.

Let  $B = x^T R y$  be a bilinear arithmetic expression. We can associate with  $B$  the bipartite graph<sup>†</sup>  $G(B) = (V_1, V_2, E)$  defined as follows:  $V_1 = \{v_i\}_{i=1}^p$  and  $V_2 = \{w_j\}_{j=1}^q$  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  $E$  iff  $r_{ij} = 1$ . A decomposition of  $G(B)$  consists of a set of Kuratowski (complete) subgraphs  $G_i = (V_i, W_i, E_i)$ ,  $1 \leq i \leq r$ , such that  $\bigcup_{i=1}^r V_i = V$ ,  $\bigcup_{i=1}^r W_i = W$ ,  $\bigcup_{i=1}^r E_i = E$  and  $E_i \cap E_j = \emptyset$  for  $i \neq j$ ;  $r$  is called the length of the decomposition.

We need several results before proving our main result. We start with the following definitions:

**3-colorability problem:** 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?

**3-m colorability problem:** Given an undirected connected graph  $G = (N, E)$  such that the degree of each node is at least 4 and  $|E| \geq 2|N| + 1$ , is  $G$  3 colorable?

**Theorem 2.2:** The 3-m colorability problem is NP-complete.

**Proof:** We use a reduction from the 3-colorability problem which is known to be NP-complete [S].  $\square$

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

**Proof:** The proof is simple and will be omitted.  $\square$

Our main result is to prove that the following problem (which we call the MP problem) is NP-complete: Given a  $p \times q$  matrix with

<sup>†</sup>See [H] and [L] for definitions.

g sets

pre-

:

= 0.

a

est

ate B

$R = XY$ ,

tic

ie bi-

ed as

are

l and

iff

sts

hs

:

ie

ng our

defi-

idi-

re

s

and

are

undi-

such

least

orable?

m is

ora-

complete

g  $v \geq 4$ ,

at

mit-

fol-

problem)

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 into an instance of the above problem.

Theorem 2.3: 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  $|E| \geq 2|N| + 1$ . Let  $N = \{v_1, v_2, \dots, v_n\}$  and  $E = \{e_1, e_2, \dots, e_r\}$ , 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  $\{r_{ij}\}$  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

$$r_{ij} = r_{n+i, r+j} = r_{2n+i, 2r+j} = r_{3n+3r+1, 3r+n+j}$$

$$r_{3r+4n+i, 4r+n+j} =$$

$$r_{3r+5n+i, 5r+n+j} = 1.$$

a2) for each  $i$ ,  $1 \leq i \leq n$ , set

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

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

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

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

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

a5) set all other  $r_{ij}$  to zero.

Figure 2.1 shows the matrix  $R = (r_{ij})$ .

$G_0$  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.

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.

	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							

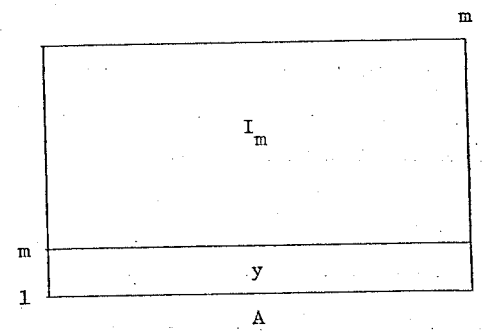


Figure 2.1

	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	$G_0$
B							

Figure 2.2

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

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 figure 2.2 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

$$\sum_{\ell=1}^m y_{\ell} b_{j\ell} = 1, \text{ for all } j=1, 2, \dots, 6r+n. \quad (*)$$

We distinguish several cases.

Case 1:  $1 \leq j \leq r$ .

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

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

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:  $r+1 \leq j \leq 3r$  or  $3r+n+1 \leq j \leq 6r+n$ .

The proof is similar to that of case 1.

Case 3:  $3r+1 \leq j \leq 3r+n$ .

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

$$\sum_{\ell=1}^m y_{\ell} b_{j\ell} = 1. \quad \square$$

Proof of Theorem 2.3 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 figure 2.1 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 figure 2.2.

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  $A=I_n$  and  $B=\bar{R}$ . The proof ~~is based upon the characterization given in theorem 2.1.~~ <sup>uses the graph formulation</sup> ~~after~~

The bipartite graph  $G(\bar{R})$  corresponding to  $\bar{R}$  is given in figure 2.3 where there are two types of edges:

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

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

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

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

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

We	$x_1$	o	o $y_1$
main		.	.
.		.	.
.1 and		.	.
q	$x_n$	o	o $y_r$
Then	$x_{n+1}$	o	o $y_{r+1}$
		.	.
if		.	.
out the	$x_{2n}$	o	o $y_{2r}$
re	$x_{2n+1}$	o	o $y_{2r+1}$
$I_m$ and		.	.
cter-		.	.
		.	.
to $\bar{R}$	$x_{3n}$	o	o $y_{3r}$
o types	$x_{3n+1}$	o	o $y_{3r+1}$
		.	.
ce		.	.
g sets	$x_{3n+r}$	o	o $y_{3r+n}$
	$x_{3n+r+1}$	o	o $y_{3r+n+1}$
		.	.
,		.	.
r},	$x_{3n+2r}$	o	o $y_{4r+n}$
, ...,	$x_{3n+3r+1}$	o	o $y_{4r+n+1}$
		.	.
, ...,		.	.
	$x_{3n+3r}$	o	o $y_{5r+n}$
, ...,	$x_{3n+3r+1}$	o	o $y_{5r+n+1}$
		.	.
		.	.
$x_i$ and	$x_{4n+3r}$	o	o $y_{6r+n}$
nd only	$x_{4n+3r+1}$	o	
		.	
$e_j$		.	
and		.	
odes:	$x_{5n+3r}$	o	
	$x_{5n+3r+1}$	o	
		.	
		.	
$r+n$ },		.	
$3r+n$ },	$x_{6n}$	o	
		.	
		.	
$y_{2r}$ },		.	
...		.	

Figure 2.3

Notice that  $G(\bar{R})$  has only two types of complete subgraphs  $K_{1,\ell}$  and  $K_{r,1}^*$ , where  $r, \ell \geq 1$ . The statement of the lemma can be reformulated as follows:  $G(\bar{R})$  has only one 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

\*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.

of the proof is to show that any decomposition of  $G(\bar{R})$  which contains complete subgraphs of the type  $K_{r,\ell}$ ,  $r > 1$ , 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  $\alpha$  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  $\alpha$  can be expressed as

$\alpha = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7$ , where  $\alpha_i$  is the number of  $K_{r,1}$  subgraphs with  $j_r$  belonging to the  $i^{\text{th}}$  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  $\alpha_4$  subgraphs, then, at most,  $\min(\frac{\alpha_1}{2}, \alpha_4) + \min(\frac{\alpha_2}{2}, \alpha_4) + \min(\frac{\alpha_3}{2}, \alpha_4)$  of the  $x_i$ 's will disappear completely (Lemma 3.2). Deleting the next  $\alpha_5$  subgraphs can cause at most  $\min(\alpha_5, \alpha_1) + \frac{\alpha_5}{2}$   $x_i$  nodes to disappear. Similarly, taking out the remaining subgraphs can result in the removal of at most  $\min(\alpha_6, \alpha_2) + \frac{\alpha_6}{2} + \min(\alpha_7, \alpha_3) + \frac{\alpha_7}{2}$   $x_i$  nodes.

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

$$\begin{aligned} \mu = & \min(\frac{\alpha_1}{2}, \alpha_4) + \min(\frac{\alpha_2}{2}, \alpha_4) + \min(\frac{\alpha_3}{2}, \alpha_4) + \\ & \min(\alpha_5, \alpha_1) + \frac{\alpha_5}{2} + \min(\alpha_6, \alpha_2) + \frac{\alpha_6}{2} + \\ & \min(\alpha_7, \alpha_3) + \frac{\alpha_7}{2}. \end{aligned}$$

Three cases arise:

(i)  $\alpha_4 \geq 1$ . Using the fact that

$\min(k_1, k_2) \leq \frac{k_1 + k_2}{2}$  and  $\min(k_1, k_2) \leq k_1$  or  $k_2$ , we obtain the following

$$\begin{aligned} \mu \leq & (\frac{\alpha_1}{2} + \frac{\alpha_2}{2} + \frac{\alpha_3}{2}) + (\frac{\alpha_5 + \alpha_1}{2}) + \frac{\alpha_5}{2} + \\ & (\frac{\alpha_6 + \alpha_2}{2}) + \frac{\alpha_6}{2} + (\frac{\alpha_7 + \alpha_3}{2}) + \frac{\alpha_7}{2}, \end{aligned}$$

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

But since all the remaining subgraphs of  $\mathcal{D}$  are of the type  $K_{1,\ell}$ , then  $\mathcal{D}$  must have at least



ion  
of  
than

$6n+3r-(\alpha-\alpha_4)$  such complete subgraphs.

Therefore, the length of  $\mathcal{G}$  is at least

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

of  
com-  
each

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

say

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

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

$$\min(\alpha_7, \alpha_3) + \frac{\alpha_7}{2}.$$

is

$$\text{Thus } \mu \leq \alpha_5 + \alpha_6 + \alpha_7 + \frac{\alpha_1}{2} + \frac{\alpha_2}{2} + \frac{\alpha_3}{2}.$$

so

ine

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

are

ab-

(iii)  $\alpha_4 = 0$  and  $\alpha_1 + \alpha_2 + \alpha_3 = 0$ . It is

clear that  $\mu \leq \frac{\alpha_5 + \alpha_6 + \alpha_7}{2}$  and the proof is similar to the previous cases.

at

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

or.

s

,

Proof of Theorem 2.3 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 figure 2.2. Note that row  $y$  of  $A$  has not been specified. Define the following three sets of nodes in  $G$ :

$x_i$

$$D_1 = \{v_j | y[j] = 1\},$$

$$D_2 = \{v_j | y[n+j] = 1\},$$

) +

$$D_3 = \{v_j | y[2n+j] = 1\}.$$

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

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

r

are  
ast

We now prove that no edge has (two nodes in one set  $D_i$ . Suppose  $e_j = \{v_i, v_k\}$  is such

that  $v_i$  and  $v_\ell$  are in  $D_k$ . Multiplying  $y$  by the  $((k-1)r+j)^{\text{th}}$  column of  $B$  results in a number greater than one since  $y[(k-1)n+i] = y[(k-1)n+\ell] = 1$ . It follows that the above partition of vertices defines a 3-coloration for  $G$  and the proof of the theorem is complete.  $\square$

### 3. Complexity of Related Problems

Another context where these results are relevant is that of computing a set of bilinear forms in algebraic complexity ([BD], [BM], [J], [W]). Note that it is not known whether the general problem with integer constants is decidable [M]. Let  $R$  be a commutative ring and let  $K \subseteq R$  such that  $0, 1 \in K$ . Suppose  $x = (x_1, x_2, \dots, x_p)^T$  and  $y = (y_1, y_2, \dots, y_q)^T$  are two column vectors of indeterminates; we have to compute  $m$  bilinear forms:

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

where  $G_i$  is a  $p \times q$  matrix with elements in  $K$ .

**Theorem 3.1:** Given a bilinear form  $B$  over  $K = \{0, 1\}$  and given a positive integer  $\delta$ , the problem of determining whether or not  $B$  can be computed with  $\delta$  multiplications is NP-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  $\delta$ , the problem of determining whether or not these bilinear forms can be computed with  $\delta$  multiplications is NP-complete.  $\square$

The above results rely heavily on the fact that the constant set is  $\{0, 1\} \subseteq \mathbb{Z}$ . A much more interesting case is when the constant set consists of  $\{0, 1, -1\}$  as in most of the published algorithms ([St]). 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  $B = \sum_{i,j} r_{ij} x_i y_j$ ,  $r_{ij} = 0, 1$ , the introduction of subtraction can reduce the number of multiplications.

As we have seen in section 2, the multiplicative complexity of a single bilinear arithmetic expression is related to the length of a decomposition of the associated bipartite graph  $G(B)$ . In view of Theorem 2.3, we have the following immediate result.

**Theorem 3.2:** 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.

### References

[AHU] Aho, A. V., J. E. Hopcroft, and

- ing y  
[ts in a  
+i]=  
rove  
tion for  
ete. □
- are  
ilinear  
], [J],  
the  
s de-  
ing and  
= (x<sub>1</sub>,  
are two  
re to
- , 2, ...,  
n,  
ents in
- over  
δ, the  
B can be  
complete.  
rollary.
- ms  
ative  
whether  
uted with
- the fact  
A much  
ant set  
the pub-  
corres-  
in this  
above  
h mention-  
form  
duction of
- ultiplica-  
multipli-  
arithmetic  
a de-  
e graph  
the fol-
- G and a  
etermining  
aght k is
- J. D. Ullman, "The Design and Analysis of Computer Algorithms," Addison Wesley, MA, 1974.
- [AJ] Aho, A. V., and S. C. Johnson, "Optimal Code Generation of Expression Trees," JACM 23, 3(July 1976), 488-501.
- [AJU] Aho, A. V., S. C. Johnson, and J. D. Ullman, "Code Generation for Expressions with Common Subexpressions," JACM 24, 1(Jan. 1977), pp. 146-160.
- [AU] Aho, A. V., and J. D. Ullman, "The Theory of Parsing, Translation of Compiling, Vol. II: Compiling," Prentice-Hall, Englewood Cliffs, NJ, 1973.
- [A] Anderson, J. P., "A Note on Some Compiling Algorithms," Comm. ACM 7, (March 1964), 149-150.
- [BM] A. Borodin and I. Munro, "Computational Complexity of Algebraic and Numeric Problems," American Elsevier Publishing Company, 1975.
- [B] Breuer, M. A., "Generation of Optimal Code for Expression via Factorization," Comm. ACM 12, 6(June 1969), 33-340.
- [BD] R. W. Brockett and D. Dobkin, "On the Optimal Evaluation of a Set of Bilinear Forms," Linear Algebra and Its Applications 19, 207-235 (1978).
- [BSe] Bruno, J. L., and R. Sethi, "Code Generation for a One-Register Machine," JACM 23, 3(July 1976), 502-510.
- [DS] Downey, P. J., and R. Sethi, "Variations on the Common Subexpression Problem" unpublished manuscript.
- [GJo] Garey, M. R. and D. S. Johnson, "Computers and Intractability, A Guide to the Theory of NP-completeness," Freeman and Company, 1979.
- [GJ] 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.
- [H] F. Harary, "Graph Theory," Addison-Wesley, Reading, MA 1969.
- [J] J. Ja'Ja', "On the Algebraic Complexity of Classes of Bilinear Forms," Ph.D. thesis, Harvard University, September 1977.
- [JMMW] Johnson, D. B., W. Miller, B. Minnihan, and C. Wrathall, "Reducibility Among Floating-Point Graphs," Tech. Rep., Dept. of Math., U. of California (Santa Barbara), 1978.
- [K] Karp, R. M., "Reducibility among Combinatorial Problems." In Complexity of Computer Computations, R. E. Miller and J. W. Thatcher, Eds., Plenum Press, New York 1972, pp. 85-104.
- [L] E. L. Lawler, "Combinatorial Optimization: Networks and Matroids," Holt, Rinehart and Winston, 1976.
- [M] Y. Matijasevic, "Enumerable Sets are Diaphantine," (Russian), Dokl. Acad. Nauk, SSSR 191 (1970), pp. 279-282.

- [N] Nakata, I., "On Compiling Algorithms for Arithmetic Expressions," Comm. ACM 10, 8(Aug. 1967), 492-494.)
- [R] Redziejowski, R. R., "On Arithmetic Expressions and Trees," Comm. ACM 12, 2(Feb. 1969), 81-84.
- [S] L. J. Stockmeyer, "Planar 3-Colorability is Polynomial Complete," ACM SIGACT News 5, 3(1973), 19-25.
- [St] V. Strassen, "Gaussian Elimination is not Optimal," Numerische Mathematik 13 (1969), pp. 354-356.
- [SU] *Sethi* R., and J. D. Ullman, "The Generation of Optimal Code for Arithmetic Expressions," JACM 17, 4(Oct. 1970), 715-728.
- [W] 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, Aug. 1978.