Europ. J. Combinatorics (1989) **10**, 29–39

Interpolation Between Bases and the Shuffle Exchange Network

NATHAN LINIAL AND MICHAEL TARSI

Let $u_1, \ldots, u_n$ and $v_1, \ldots, v_n$ be bases of a vector space (the interesting case, when the underlying field is finite). Then there exist vectors $w_1, \ldots, w_{n-1}$ such that every n consecutive vectors in the sequence $u_1, \ldots, u_n, w_1, \ldots, w_{n-1}, v_1, \ldots, v_n$ from a basis. Similar statements hold in structures other then vector spaces. The case of a free Boolean algebra is shown equivalent to an open problem in switching network theory.

1. INTRODUCTION

Let S be a finitely generated algebraic structure. A generating set of the minimum size is called a *basis* for S. Let $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ be two ordered bases of S. We are interested in finding elements $z_1, \ldots, z_k$ of S which interpolate between them. That, is we want every n consecutive elements in the sequence

$$x_1, \ldots, x_n, z_1, \ldots, z_k, y_1, \ldots, y_n$$

to form a basis.

A sequence with the above-defined property is said to be *basic.*

For various structures S we consider the following questions:

(1) Do there exist for every two bases $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ elements $z_1, \ldots, z_k$ with $x_1, \ldots, x_n, z_1, \ldots, z_k, y_1, \ldots, y_n$ basic?

(2) For given n, what is at the least k such that for any two bases $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ there are $z_1, \ldots, z_k$ as above?

(3) Can $k = n - 1$ always be attained? Note that $k \geqslant n - 1$ is a lower bound because x_n may equal y_1, in which case they cannot belong to one basis.

We were led to study this class of problems by a question in switching network theory: How many passes through a Shuffle Exchange Network suffice to generate all input–output permutations? This problem had received a good deal of interest among computer scientists because of the usefulness of such networks in the design of computer architectures for parallel processing. It turns out, rather surprisingly, that this question can be stated in terms of the above problems when S is the free Boolean algebra on n generators. We were able to slightly improve the known results on these networks and our hope is that the final answer to this problem can be obtained by similar methods.

The paper is organized as follows. In Section 2 we obtain a complete solution to all problems for the case where S is a vector space. In Section 3 we present our results for Boolean algebras. In Section 4 we review relevant results for modules, groups and rings. In Section 5 we explain the problem on the Shuffle Exchange Network and why this question is equivalent to our general problem in the case of a Boolean algebra.

2. VECTOR SPACES

In this section we prove a theorem on vector spaces which answers all questions (1), (2) and (3):

THEOREM 2.1. *Let $u_1, \ldots, u_n$ and $v_1, \ldots, v_n$ be two sets of linearly independent vectors in a vector space V. Then there exist vectors $w_1, \ldots, w_{n-1}$ in V such that any n consecutive*

0195-6698/89/010029+11 $02.00/0 © 1989 Academic Press Limited

vectors in the sequence

$$v_1, \ldots, v_n, w_1, \ldots, w_{n-1}, u_1, \ldots, u_n$$

and linearly independent.

PROOF. Let us first comment that if V is a vector space over an infinite field then the assertion is trivial. One can construct $w_1, \ldots, w_{n-1}$ in order, requiring only that w_i creates no forbidden linear dependencies with the u's, v's and $w_1, \ldots, w_{i-1}$. These restrictions only forbid w_i from belonging to a finite number of proper subspaces. But a vector space over an infinite field is not the union of finitely many proper subspaces and so there always is a w_i satisfying the conditions. The situation is very different for vector spaces over a finite field. For example the n-dimensional vector space over GF(2) is the union of the three subspaces, given by the equations $x_1 = 0, x_2 = 0$ and $x_1 + x_2 = 0$. There are some known results on collections of proper subspaces which cover the whole space [5] but we do not enter this issue here.

LEMMA 2.2. *Let $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ be two collections of linearly independent vectors in a vector space V and let r, $n - 1 \geqslant r \geqslant 1$, be an integer. Suppose that for all i, $n - 1 \geqslant i \geqslant 1$, the vectors*

$$x_j, (n \geqslant j \geqslant i + 1) \quad \text{and} \quad y_j, (i - r \geqslant j \geqslant 1)$$

are linearly independent. Then there exists a vector z such that for all i, $n - 1 \geqslant i \geqslant 1$, the vectors

$$x_j, (n \geqslant j \geqslant i + 1), \quad z \quad \text{and} \quad y_j, (i - r \geqslant j \geqslant 1)$$

are linearly independent.

The theorem follows by repeated application of the lemma. Start with $x_1 = u_1, \ldots, x_n = u_n$, $y_1 = v_1, \ldots, y_n = v_n$ and $r = n - 1$ and let $w_1 = z$. Then successively let $j = 2, \ldots, n - 1$,

$$x_1 = u_j, \ldots, x_{n-j+1} = u_n, x_{n-j+2} = w_1, \ldots, x_n = w_{j-1},$$

and $r = n - j$, and define w_j to be z. It is easily seen that the vectors $w_1, \ldots, w_{n-1}$ constructed this way satisfy the theorem.

We now prove Lemma 2.2 by induction on n. The case $n = 1$ is trivial. For the induction step we denote by $\hat{x}$ the coset of x in the quotient space V/y_1. First we consider the case when $\hat{x}_2, \ldots, \hat{x}_n$ are linearly independent in V/y_1, or equivalently that $y_1 \notin Sp(x_2, \ldots, x_n)$. Apply the induction hypothesis to the vectors $\hat{x}_2, \ldots, \hat{x}_n$ and $\hat{y}_2, \ldots, \hat{y}_n$ and find a vector $\hat{z}$ satisfying the lemma. Lift $\hat{z}$ to some $\bar{z} \in V$. The vector $\bar{z}$ may fail to satisfy the lemma only in the case $i = 1$, namely

$$\bar{z} \in Sp(\hat{x}_j \mid n \geqslant j \geqslant 2).$$

But then we set $z = \bar{z} + y_1$ and since $y_1 \notin Sp(x_j \mid n \geqslant j \geqslant 2)$, the conclusion of the lemma is satisfied.

In the remaining case $y_1 \in Sp(x_2, \ldots, x_n)$, say

$$y_1 = \sum_{j=2}^{n} \alpha_j x_j.$$

Let t be the least index j for which $\alpha_j \neq 0$. Since

$$x_{r+2}, \ldots, x_n, y_1$$

are independent (case $i = r + 1$) it follows that $t \leqslant r + 1$. Now apply the induction hypothesis for $\hat{x}_1, \ldots, \hat{x}_{t-1}, \hat{x}_{t+1}, \ldots, \hat{x}_n$ and $\hat{y}_2, \ldots, \hat{y}_n$. Since $t \leqslant r + 1$, we only need to verify the assumption that

$$\hat{x}_1, \ldots, \hat{x}_{t-1}, \hat{x}_{t+1}, \ldots, \hat{x}_n$$

are linearly independent, i.e. that $y_1 \notin Sp(x_1, \ldots, x_{t-1}, x_{t+1}, \ldots, x_n)$ in V. But $x_1, \ldots, x_n$ are independent so x_t is in the support of y_1, and the conclusion follows. Now the induction hypothesis gives us a vector $\hat{z} \in V/y_1$. Lift $\hat{z}$ to any $z \in V$ which is the desired vector. If this is not so, z is not satisfactory for a set involving both x_t and y_1. But $t \leqslant r + 1$, so this is impossible and the proof is complete. □

3. Free Boolean Algebra

THEOREM 3.1. *Let B be the free Boolean algebra with $n \geqslant 3$ generators. Let $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ be two bases. Then there exist elements $z_1, \ldots, z_{2n-4} \in B$ such that the sequence*

$$x_1, \ldots, x_n, z_1, \ldots, z_{2n-4}, y_1, \ldots, y_n$$

is basic.

Before proving the theorem let us state the following:

CONJECTURE. Let $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ be two bases of a free Boolean algebra. Then there exist elements $z_1, \ldots, z_{n-1}$ such that the sequence

$$x_1, \ldots, x_n, z_1, \ldots, z_{n-1}, y_1, \ldots, y_n$$

is basic.

PROOF OF THEOREM 3.1. The elements of a Boolean algebra B freely generated by n elements can be thought of as subsets of a set of size 2^n, or equivalently as binary vectors of length 2^n. It is fairly easy to verify that in this representation a set $x_1, \ldots, x_n \in B$ is a basis iff the $2^n \times n$ matrix whose columns are $x_1, \ldots, x_n$ (thought of as binary vectors) has the property that all 2^n rows are distinct. We let $N = 2^n$ and define a 0–1 matrix $A_{N \times k}$: to be *balanced* if either

(1) $k \leqslant n$ and each of the 2^k 0–1 vectors appears 2^{n-k} times as a row of A, or

(2) $k < n$ and each n consecutive columns form a balanced matrix.

Note that for $k \geqslant n$ an $N \times k$ matrix is balanced iff the sequence of its columns is basic.

In terms of balanced matrices our claim is that for any two balanced $N \times n$ matrices A, B we can find an $N \times (2n - 4)$ matrix C so that the block matrix

$$[A, B, C]$$

(consisting of the columns of A, B and C, in that order) is balanced, and the conjecture is that there is such a C with $n - 1$ columns.

We say that a balanced $N \times (n - 1)$ matrix A and a vector x *agree* if on appending x to A as an additional column we obtain a balanced matrix. We prove the following:

LEMMA 3.1. *For $(n \geqslant 2)$, let A, B be two $N \times (n - 1)$ balanced matrices. Then there exists a vector x which agrees with both A and B.*

PROOF. Consider a graph G on N vertices which are in 1 : 1 correspondence with the rows of the matrices A, B. Vertices i, j are adjacent if the ith row and jth row of A are

identical or similarly in B. Since A, B are balanced, the edges induced by A constitute a perfect matching in G. The same conclusion holds for B. The union of the two edge subsets, which is the edge set of G, is thus a disjoint union of even cycles. Thus G can be 2-coloured. A colouring with colours 0 and 1 corresponds to a 0–1 column vector since vertices in G represent rows. The column vector thus obtained agrees with both A and B. □

LEMMA 3.2. *Let $A_{N\times n}$ be a* 0–1 *matrix with the property that any $N \times (n-1)$ submatrix obtained by deleting a column is balanced. Then the sum (over* GF(2)*) of the column vectors of A is the* 0 *vector or a vector of all* 1's *or A is balanced.*

PROOF. For any 0–1 row vector v of length n, let $r(v)$ be the number of rows in A which are identical with v. Let A' be any submatrix of A obtained by deleting a column of A. Matrix A' is balanced by assumption, so each 0–1 vector of length $n-1$ occurs twice as some row of A'. Let v_1 and v_2 be two row vectors of length n that agree in all components, except for exactly one. Consider the matrix A' which is obtained by deleting the column where v_1 and v_2 differ. Since every row vector appears twice as a row in A' it follows that $r(v_1) + r(v_2) = 2$. Consider now the zero vector. There are three possible cases, $r(0) = 0$, 1, 2. Assume first $r(0) = 2$. Then every vector v with exactly one entry of 1 and all other entries zero has $r(v) = 0$. This in turn implies that $r(v) = 2$ for every vector with exactly two 1 entries and 0 elsewhere. In general, for a 0–1 row vector v of length n, $r(v) = 0$ or 2 according to whether v has an odd or an even number of 1's, then the sum over GF(2) of the columns of A is the zero vector. Similarly if $r(0) = 0$, then the sum of the columns of A over GF(2) has all its entries 1. If we assume $r(0) = 1$ it follows that $r(v) = 1$ for any row vector v, i.e. A is balanced. □

We also need the following lemma:

LEMMA 3.3. *Let $A_{N\times k}$ be a balanced matrix with $k \leqslant n$, and let T be a non-singular $k \times k$ matrix. Then $A \cdot T$ is balanced (all the arithmetic is over* GF(2)*).*

PROOF. If $B = A \cdot T$, is unbalanced, then some row appears in B more then 2^{n-k} times. But then in $A = B \cdot T^{-1}$ the corresponding rows are identical too, contradicting the fact that A is balanced. □

Next we prove our theorem for $n = 3$, $N = 8$. Let $A_{8\times 3}$ and $B_{8\times 3}$ be balanced, and let their columns be $A = [a_1, a_2, a_3]$, $B = [b_1, b_2, b_3]$. We are looking for vectors x, y, so that $M = [a_1, a_2, a_3, x, y, b_1, b_2, b_3]$ is balanced.

Following Lemma 3.1 we construct z which agrees both with $[a_2, a_3]$ and with $[b_1, b_2]$. Next construct y which agrees both with $[a_3, z]$ and with $[b_1, b_2]$. If $[z, y, b_1]$ turns out to be balanced, let $x = z$ and M is balanced. If it is not balanced, notice that every pair of vectors our of z, y, b_1 determines a balanced 8×2 matrix, since each can be completed to a balanced 8×3 matrix. By Lemma 3.2, $y = z + b_1$, or $y + z + b_1 = \mathbf{1}$, the vector of all 1's. The latter case can be reduced to the former one by replacing y by its complement. This change is valid since any balanced matrix remains balanced after replacing any column by its complement. It is claimed that M is balanced with $y = z + b_1$ and $x = z + a_3$. We only need to verify that the following matrices are balanced:

$$[a_2, a_3, z + a_3], \quad [a_3, z + a_3, z + b_1], \quad [z + a_3, z + b_1, b_1], \quad [z + b_1, b_1, b_2].$$

The proofs are very similar, so we only deal with the first matrix. The matrix $[a_2, a_2, z]$ is balanced by the construction of z and

$$[a_2, a_3, z + a_3] = [a_2, a_3, z]\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

is balanced by Lemma 3.3

Now let $A = [a_1, \ldots, a_n]$ and $B = [b_1, \ldots, b_n]$ be given $N \times n$ balanced matrices. We wish to construct an $N \times (2n - 4)$ matrix M so that $[A, M, B]$ is balanced. First we describe how to construct M and then prove balancedness.

PHASE 1. Repeatedly apply Lemma 3.1 and construct vectors $u_1, \ldots, u_{n-3}$ so that $U = [u_1, \ldots, u_{n-3}]$ and $U^R = [u_{n-3}, \ldots, u_1]$ are such that

$$[A, U] \quad \text{and} \quad [U^R, B]$$

are both balanced.

PHASE 2. We wish to construct vectors x, y so that

$$[A, U, x, y] \quad \text{and} \quad [x, y, U^R, B]$$

are both balanced. Since U is balanced, any row in it is repeated 8 times. Accordingly, the rows of the above matrices fall into 2^{n-3} classes of 8 rows each. If v is one of the columns in those matrices, we denote by $v^{(i)}$ $(2^{n-3} - 1 \geqslant i \geqslant 0)$ the subvector of v with entries in the rows of the ith class. The vector $v^{(i)}$ has length 8.

Now for $i = 0, \ldots, 2^{n-3} - 1$

$$A^{(i)} = [a_{n-2}^{(i)}, a_{n-1}^{(i)}, a_n^{(i)}]$$

and

$$B^{(i)} = [b_1^{(i)}, b_2^{(i)}, b_3^{(i)}]$$

are balanced 8×3 matrices so our solution for the case $n = 3, N = 8$ may be applied to yield vectors $x^{(i)}$ and $y^{(i)}$ so that

$$[A^{(i)}, x^{(i)}, y^{(i)}, B^{(i)}]$$

is balanced. This defines vectors x and y by pasting the $x^{(i)}$-s and $y^{(i)}$-s together.

PHASE 3. Define

$$w_i = \begin{cases} u_i & \dfrac{n-3}{2} \geqslant i \geqslant 1 \\ u_i + u_{n-i-3} & n - 4 \geqslant i \geqslant \dfrac{n-2}{2} \\ u_{n-3} + a_n & i = n - 3 \end{cases}$$

$$W = [w_1, \ldots, w_{n-3}]$$

The matrix

$$[A, W, x, y, U^R, B]$$

is balanced.

VALIDITY OF THE CONSTRUCTION. We first prove that the construction of x and y in Phase 2 assures that

$$[A, U, x, y]$$

and

$$[x, y, U^R, B]$$

are balanced.
Since

$$[A, U] \quad \text{and} \quad [U^R, B]$$

are balanced it suffices to consider

$$[a_{n-2}, a_{n-1}, a_n, U, x, y]$$

and

$$[x, y, U^R, b_1, b_2, b_3]$$

We discuss only the first of these since the proof for the second one is similar. Any set of n consecutive columns in

$$[a_{n-2}, a_{n-1}, a_n, U, x, y]$$

contains all $n - 3$ columns of U, which is known to be balanced. Therefore it suffices to know that any three consecutive columns in

$$[a_{n-2}^{(i)}, a_{n-1}^{(i)}, a_n^{(i)}, x^{(i)}, y^{(i)}]$$

define a balanced 8×3 matrix ($2^{n-3} - 1 \geqslant i \geqslant 0$). But this is ensured by our 8×3 construction.

We return to proving that

$$[A, W, x, y, U^R, B]$$

is balanced. The balancedness of $[x, y, U^R, B]$ is already established, so it suffices to consider $[A, W, x, y, U^R]$:

(a) Consider submatrices of the form

$$[a_i, \ldots, a_n, w_1, \ldots, w_{i-1}], n - 2 \geqslant i \geqslant 2.$$

Any such matrix is balanced by Lemma 3.3 since it can be obtained from $a_i, \ldots, a_n$, $u_1, \ldots, u_{i-1}$, which is known to be balanced, by a linear invertible transformation. Indeed the inverse transformation is as follows:

$$(i - 1 \geqslant j \geqslant 1)u_j = \begin{cases} w_j & \dfrac{n-3}{2} \geqslant j \geqslant 1; \\ w_j + w_{n-j-3} & n - 4 \geqslant j \geqslant \dfrac{n-2}{2}; \\ w_j + a_n & j = n - 3. \end{cases}$$

Proposition 3 applies and balancedness is proved. Similar arguments apply to the column submatrices with n columns, where a_{n-2}, a_{n-1} or a_n, is the leftmost one.

(b) Next we have to consider matrices of the form

$$[w_i, \ldots, w_{n-3}, x, y, u_n, u_{n-1}, \ldots, u_{n-i-2}], \qquad n - 3 \geqslant i \geqslant 1 .3.$$

This matrix can be obtained via an invertible transformation from

$$[a_n, u_1, \ldots, u_{n-3}, x, y].$$

The easily derived details are omitted. □

Most of the results and problems in this section can be extended to deal with matrices whose entries come from a d-element set $0, \ldots, d-1$ for some $d \geqslant 2$.

For d prime this turns out to be a special case of our general problem. A vector of length $N = d^n$ with entries in $0, \ldots, d-1$ is considered as an element in F_d^n, the ring which is the direct sum of n copies of F_d, the field with d elements. The size of a basis in F_d^n is n and bases are characterized by:

PROPOSITION 3.1. *Let d be a prime and $N = d^n$. An $N \times n$ matrix A with entries from F_d is balanced iff the columns of A are a basis of F_d^n.*

PROOF. If A is not balanced it has two identical rows, then this is also so for every vector generated by the columns of A. Therefore the columns of A are not a basis. Conversely, we now show that the columns of A span F_d^n. By linearity it suffices to generate, for every $n \geqslant i \geqslant 1$, an element of F_d^n which is non-zero in the ith coordinate and zero elsewhere. If the ith row of A is $[a_{i1}, \ldots, a_{in}]$ then consider the polynomial

$$\prod_{j=1}^{n} \prod_{\alpha \neq a_{ij}} (x_j - \alpha)$$

in variables $x_1, \ldots, x_n$. When evaluated at $x_j =$ the jth column of A, $(j = 1, \ldots, n)$ its ith coordinate is the single non-zero coordinate. The free term α of the above polynomial should be taken as $\alpha \cdot 1$, where 1 is the identity of F_d^n, the vector of all 1's. □

For the rest of this section d denotes a positive integer, not necessarily a prime. We let N be d^n now and define a matrix $A_{N \times k}$ over $\mathbb{Z}_d$, the cyclic group of order d, to be *balanced* if:

$k \leqslant n$ and each row in A appears d^{n-k} times, or

$k > n$ and each n consecutive columns form a balanced matrix.

We extend our previous conjecture to:

CONJECTURE. Let A and B be $N \times n$ balanced matrices over $\mathbb{Z}_d$. Then there is an $N \times (n-1)$ matrix M so that $[A, M, B]$ is balanced.

The best result that we have in this context is:

THEOREM 3.2. *Given A, B balanced $N \times n$ matrices over $\mathbb{Z}_d$, there exists an $N \times (2n-3)$ matrix M so that $[A, M, B]$ is balanced ($(n \geqslant 2, N = d^n)$.*

The proof is very similar to that of Theorem 3.1 with the following modification: Lemma 3.2 does not extend to general d and we do not know what it should be replaced by. Therefore, we do not know how to solve the $d^3 \times 3$ case for general d. However, Lemma 3.3 can easily be extended. The only comment that should be made here is that addition, which is done over GF(2) originally is replaced by mod d addition. (Lemma 3.3 uses matrix *multiplication* terminology, but in terms of elementary operations we can only *add* one column to another, and this operation is invertible over any group.)

Let us show now how Lemma 3.1 is extended.

LEMMA 3.4. *Let A, B be balanced $N \times (n-1)$ matrices over $\mathbb{Z}_d$. Then there is a vector x such that both $[A, x]$ and $[B, x]$ are balanced ($N = d^n$).*

PROOF. Define a bipartite multigraph as follows. For every vector v of length n over $\mathbb{Z}_d$, we have two vertices a_v and b_v. For every i, $N \geqslant i \geqslant 1$ we define an edge that connects a_u

to b_v if u is the ith row vector of A and v is the ith row vector of B. The resulting multigraph is d-regular because A, B are balanced. By König's Theorem [2, p. 250] the edges of the multigraph can be d-coloured. Let the colours be $0, \ldots, d-1$. Since we have a $1:1$ correspondence between edges in the multigraph and rows in the matrix, the colouring defines a column vector x with entries from $\mathbb{Z}_d$, it follows from the definition of colouring that $[A, x]$ and $[B, x]$ are balanced. □

THEOREM 3.2 is now proved, by modifying the proof of Theorem 3.1 as follows. In Phase 1 construct U with $n-1$ columns (instead of $n-3$). Delete Phase 2. In Phase 3 define

$$w_i = \begin{cases} u_i & \frac{n-1}{2} \geqslant i \geqslant 1 \\ u_i + u_{n-i-1} & n-2 \geqslant i \geqslant \frac{n}{2} \\ u_{n-1} + a_n & i = n-1 \end{cases}$$

$$W = [w_1, \ldots, w_{n-1}]$$

Then the matrix

$$[A, W, U^R, B]$$

is balanced. □

4. Relevant Work on Other Structures

The rather satisfying results obtained in Section 2 for vector spaces already fail for modules: consider $\mathbb{Z}^2$, the two-dimensional module over the integers. A pair $u_1 = (x_1, y_1)$, $u_2 = (x_2, y_2)$ of elements in $\mathbb{Z}^2$ constitute a basis for $\mathbb{Z}^2$ iff

$$\det \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix} = \pm 1.$$

So ordered bases for $\mathbb{Z}^2$ are in $1:1$ correspondence with elements of the group $SL(2, \mathbb{Z})$. As we shall see next, a finite interpolation always exists, but there is no upper bound on the length of such an interpolation.

PROPOSITION 4.1. *Let u_1, u_2 and v_1, v_2 be two bases for $\mathbb{Z}^2$. Then there exist $w_1, \ldots, w_t \in \mathbb{Z}^2$ for which*

$$u_1, u_2, w_1, \ldots, w_t, v_1, v_2$$

is basic. However, t cannot be bounded from above.

PROOF. The first part of our claim is proved in Proposition 4.2. As for the second part, if u_1, u_2, u_3 is basic, where $u_i = (x_i, y_i)$ then

$$\begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & n \end{pmatrix} = \begin{pmatrix} x_2 & x_3 \\ y_2 & y_3 \end{pmatrix},$$

for some $n \in \mathbb{Z}$. We shall call a matrix of the form

$$\begin{pmatrix} 0 & -1 \\ 1 & n \end{pmatrix}$$

an elementary matrix. The first part of this proposition implies that every matrix from $SL(2, \mathbb{Z})$ can be represented as $\pm \Pi_{i=1}^{t} A_i$, where the A_i's are elementary matrices. We now show that t has no upper bound.

It is known (see [N]) that every matrix from $SL(2, \mathbb{Z})$ has a unique representation as plus-or-minus a product of the matrices T and U, where

$$T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad U = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

in which no two consecutive T's nor three consecutive U's appear ($U^3 = -T^2 = I$, the 2×2 identity matrix).

One can easily verify that

$$(UT)^{n-1}U = (-1)^n \begin{pmatrix} 0 & -1 \\ 1 & n \end{pmatrix}.$$

Thus, in a product of at most t elementary matrices, represented as a word in T, U, the factor U^2 appears at most t times. Hence there are matrices in $SL(2, \mathbb{Z})$ which cannot be generated this way if t is bounded. □

For groups we have the following result.

PROPOSITION 4.2. *If $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ are bases for a group G, then there exist elements $c_1, \ldots, c_t$ for which $a_1, \ldots, a_n, c_1, \ldots, c_t, b_1, \ldots, b_n$ is basic. There is, in general, no upper bound on t.*

PROOF. The first part is an immediate consequence of the theory of Nielsen Transformation [9, Ch. 3]. The second half was established in Proposition 4.1.

The situation for rings of polynomials is described in the following result of Jung [7]:

PROPOSITION 4.3. *Let R be a ring with a unity and let $R_k = R[x_1, \ldots, x_k]$ be the ring of polynomials in k variables over R. Then R_1, R_2 have the property of finite interpolation between bases with no upper bound on the length.*

Note that finite interpolation is conjectured for every R_k, but this is still open to the best of our knowledge, for $k \geqslant 3$. For some extensions of [7], see [3] and [4].

5. The Shuffle Exchange Network

The Shuffle Exchange Network (= SE network) is a member in a class of interconnection networks which has received a considerable amount of interest among computer scientists. These networks are used to interconnect processors and memory for purposes of parallel computing. See [12] for a description of one of the major projects in the area of parallel processing which is based on the SE network. See [6] for a collection of articles on networks considered for the same purpose, msot of which are in fact very closely related to SE in their structure. In every step of parallel processing the interconnection network has to realize a communication request. Each of the processing units specifies the memory module it needs for the current step. The interconnecting network has to efficiently serve these communication requests. This amounts to realizing a permutation in the network. Now let us describe the SE network in detail.

The SE network is a module which can perform any one of a set of permutations. It has $N = 2^n$ input lines which are first subject to the perfect shuffle permutation. The input lines are denoted by indices $N - 1 \geqslant x \geqslant 0$ and the perfect shuffle permutation maps x to $2x$ (mod N). Thus exactly two lines, namely y and $y + 2^{n-1}$, $0 \leqslant y \leqslant 2^{n-1} - 1$, now have $2y$ as index. In the exchange part we then assign the index $2y$ to one of the two lines, and $2y + 1$ to the other one. Thus a passage through SE has $2^{N/2}$ possible outcomes. We iterate through SE until the desired permutation is achieved. For given n, what is the least number of passes through SE which suffices to generate any one of the possible $N!$ permutations? We denote this number by $f(n)$. *A priori* it is not a clear that such a number exists, but this is known as we explain below.

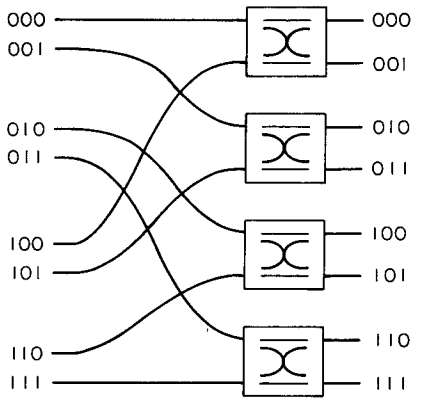

FIGURE 1. The SE network for $n = 3$, $N = 8$.

Let us define the class $SE_n \subseteq S_N (N = 2^n)$ of permutations realizable by one SE pass, applied to the permutation 0, 1, . . . , $N - 1$, i.e.,

$$SE_n = \{\pi \in S_N \mid \pi(x) = 2x \text{ (mod } N) \text{ or } 2x + 1 \text{ (mod } N), 0 \leqslant x \leqslant N - 1\}.$$

The problem is to find the least $f = f(n)$ such that $(SE_n)^f = S_N$.

That $f(n)$ does exist and in fact $f(n) = O(n^2)$ was shown by Stone [14]. This was improved by Parker [11] to $f(n) \leqslant 3n$ and slightly further improved to $f(n) \leqslant 3n - 1$ [15]. It is implied by the present article that $f(n) \leqslant 3n - 4$, for $(n \geqslant 3)$, while it is conjectured that $f(n) = 2n - 1$. We think that the main contribution of this paper towards solution of the problem is not the slight improvement of the bound, but lies in the following reformulation in terms of balanced matrices.

PROPOSITION 5.1. *Let $M_{N \times m}$ be a balanced matrix, $m \geqslant n$. For $i = 1, \ldots, N$, let $a_i(b_i)$ be the integer whose binary representation is given by the n first (last) entries of the ith row of M. The permutation given by $a_i \to b_i$, $N \geqslant i \geqslant 1$, can be attained by $m - n$ passes through the SE network. Moreover, all the permutations that can be attained by $m - n$ SE passes are represented in this way.*

PROOF. Notice that the $a_i(b_i)$, $i = 1, \ldots, N$, are mutually distinct, by definition of balance, so $a_i \to b_i$ is in fact a permutation on 0, . . . , $N - 1$. It suffices to prove the lemma for $M = n + 1$ since the general result follows by repeated application of this case. To handle the case $m = n + 1$, notice that any permutation which can be performed by a single SE pass has the form $x \Rightarrow 2x + E_x (\text{mod } N)$ $(0 \leqslant x \leqslant N - 1)$, where each E_x is either zero or one with the condition that if $0 \leqslant x \leqslant 2^{n-1} - 1$, then $E_x \neq E_{x+2^{n-1}}$. By

definition of a_i and b_i it follows that either

$$b_i = 2a_i \pmod{N}$$

or

$$b_i = 2a_i + 1 \pmod{N}$$

The condition $E_x \neq E_{x+2^{n-1}}$ is equivalent to M being balanced. □

A consequence of our work in Section 3 is a very short proof for a fact usually proved in the context of Benes Network [1]: with SE_n as defined above denote by $\Omega_n = (SE_n)^n$ the set of permutations which can be generated by iterating SE n times. Also $\Omega_n^{-1} = \{\pi^{-1} \mid \pi \in \Omega_n\}$. We have:

PROPOSITION 5.2. $\Omega_n \cdot \Omega_n^{-1} = S_N$ *(that is, every permutation from* S_N *is the product* $\pi_1 \cdot \pi_2^{-1}$ *for some* $\pi_1, \pi_2 \in \Omega$*).*

PROOF. In the terminology of this paper, the proposition is equivalent to the claim that for any $N \times n$ balanced matrices A and B there is an $N \times n$ matrix C such that both $[A, C]$ and $[B, C]$ are balanced. This is just Lemma 3.1 iterated n times. □

REFERENCES

1. V. E. Benes, *Mathematical Theory of Connecting Networks and Telephone Traffic*. Academic Press, 1965.
2. C. Berge, *Graphs and Hypergraphs*. North Holland, Amsterdam, 1976.
3. A. J. Czerniakiewicz, Automorphisms of free associative algebra of rank 2, I. *Trans. Amer. Math. Soc.* **160** (1971), 393–401.
4. A. J. Czerniakiewicz, Automorphisms of free associative algebras of rank 2, II. *Trans. Amer. Math. Soc.* **171** (1972), 309–315.
5. O. Heden, The Frobenius number and partitions of a finite vector space. *Archiv. Math.* **42** (1984), 185–192.
6. *IEEE Trans. Comput.* **C-30**, Spril 1981 (a special issue on interconnection networks).
7. H. W. E. Jung, Über ganze birationale Transformation der Ebene. *J. Reine Angew. Math.* **184** (1942), 161–174.
8. D. H. Lawrie, Access and alignment of data in an array processor. *IEEE. Trans. Comput.* **C-24** (1976).
9. W. Magnus, A. Karrass and D. Solitar, *Combinatorial Group Theory*. Dover, New York, 1976.
10. M. Newman, *Integral Matrices*. Academic Press, New York, 1972.
11. D. S. Parker, Note on shuffle/exchange-type switching networks. *IEEE Trans. Comput.* **C-2** (1980), 213–222.
12. J. T. Schwartz, Ultracomputers. *ACM Trans. Programm. Lang. Systems* **2** (1980), 484–521.
13. H. J. Siegel, The universality of various types of SIMD machine interconnection networks, In *Proc. 4th Ann. Symp. Computer Archit.* 23–25 March, 1977.
14. H. S. Stone, parallel processing with the perfect shuffle. *IEEE Trans. Comput.* **C-20** (1971), 153–161.
15. C. L. Wu and T. Y. Feng, The universality of the shuffle-exchange network. *IEEE Trans. Comput.* **C-30** (1981), 324–331.

Received 14 February 1985 and in revised form 1 July 1987

NATHAN LINIAL
Institute of Mathematics and Computer Science,
Hebrew University, Jerusalem 91904, Israel
and
MICHAEL TARSI
School of Mathematical Sciences,
Tel Aviv University, Ramat Aviv, 69978 Israel