ON THE REARRANGEABILITY OF SHUFFLE-EXCHANGE NETWORKS

HUNG Q. NGO AND DING-ZHU DU

Computer Science Department, University of Minnesota, Minneapolis, MN 55455, USA.
E-mail: {hngo,dzd}@cs.umn.edu.

Let $m(n)$ be the minimum positive integer k so that the Shuffle-Exchange network with k stages, $N = 2^n$ inputs and N outputs is rearrangeable. Beneš conjectured that $m(n) = 2n - 1$. The best bounds known so far are $2n - 1 \leq m(n) \leq 3n - 4$. In this paper, we verify Beneš conjecture for $n = 4$, and use this result to show that $m(n) \leq 3n - 5$.

1 Introduction

Shuffle-Exchange networks (SE networks for short) were initially proposed by Stone [1] (1971) to be an efficient interconnecting architecture for parallel processors. Various applications benefit from this interconnecting pattern such as FFT, matrix transposition, polynomial evaluation, ... A k-stage SE network with parameter n, denoted by $(SE_n)^k$, is a network with $N = 2^n$ inputs and N outputs, consisting of k SE stages, where each SE stage includes a *perfect shuffle* pattern [1] followed by an array of $\frac{N}{2}$ 2×2 crossbars. A typical drawing of a 7-stage SE network with $n = 4$ (i.e. $(SE_4)^7$) is shown in Figure 1.

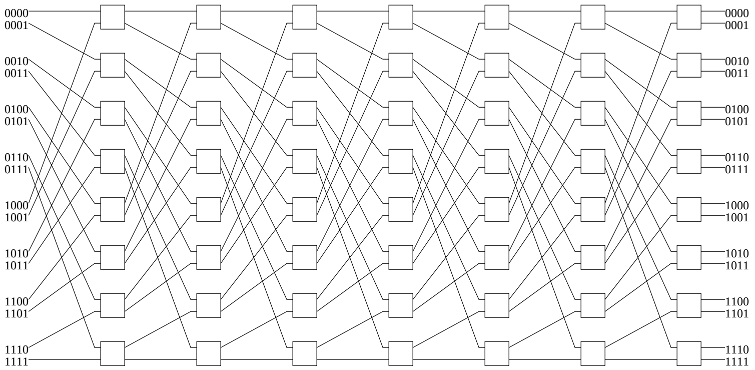


Figure 1. The 7-stage SE network for $N = 16$, i.e. $(SE_4)^7$

A standard question to be addressed on any multistage interconnection network (MIN) is that if the network is *rearrangeable.* An N-input N-output MIN is rearrangeable if and only if any one to one mapping from the inputs to the outputs is routable by the network. *Universality* is another term that is often used synonymously with *rearrangeability.* In the context of SE networks, a long standing question was that how many SE stages are sufficient for a SE network to be rearrangeable. In fact, it is not entirely clear that increasing the number of stages would increase the rearrangeability of a SE network. There has been a very slow progress toward answering this question. For convenience, let us use $m(n)$ to denote the minimum positive integer so that $(SE_n)^{m(n)}$ is rearrangeable. The algorithm discussed by Stone [1] showed that $m(n) \leq n^2$, thus $m(n)$ is well defined. Beneš conjectured in 1975 [2] that $2n-1$ SE stages is necessary and sufficient to route all $N!$ perfect matchings from the inputs to the outputs, i.e. $m(n) = 2n-1$. Parker [3] (1980) showed that $n+1 \leq m(n) \leq 3n$, where the lower bound was obtained by a counting argument, and the upper bound by group calculations plus the rearrangeability of the Beneš network. [4] Wu and Feng [5] (1981) gave an explicit algorithm to route all matchings, proving $m(n) \leq 3n-1$. Huang and Tripathi [6] (1986) improved the bound to $m(n) \leq 3n-3$. Raghavendra and Varma [7] (1987) verified the conjecture for $N = 8$. They used that result to show $m(n) \leq 3n-4$. [8] They also specified a permutation which $(SE_n)^k$ can not route if $k \leq 2n-2$, in effect showing $2n-1 \leq m(n)$. With a different formulation, Linial and Tarsi [9] (1989) also verified the conjecture for $N = 8$ and showed $m(n) \leq 3n-4$. From their formulation it is easy to see that at least $2n-1$ stages are needed to route all permutations. Feng and Seo [10] (1994) gave a proof of the conjecture, which was incomplete as pointed out by Kim, Yoon, and Maeng [11] (1997).

In this paper, we give a proof that $m(4) = 7$ using a new method, and then adapting Linial and Tarsi's results to show that $m(n) \leq 3n-5$.

2 Preliminaries

This section presents related concepts and previous results on the problem. Throughout the paper, we shall assume that $n \in \mathbb{N}$ and $N = 2^n$. The following definitions and lemmas are from Linial and Tarsi. [9]

Definition 2.1. For $k \in \mathbb{N}$, a $N \times k$ 01-matrix A, denoted by $A_{N\times k}$ is said to be *balanced* if

(i) Either $k \leq n$ and every row vector $v \in \mathbb{F}_2^k$ occurs exactly 2^{n-k} times as rows of A.

(ii) or $k > n$ and every n consecutive column vectors of A form a balanced matrix.

Definition 2.2. Given a balanced matrix $A_{N\times(n-1)}$, a column vector $x \in \mathbb{F}_2^N$ is said to *agree* with A if appending x into A yields an $N \times n$ balanced matrix (the matrix $[A, x]$).

Lemma 2.3. *If A and B are two $N \times (n-1)$ balanced matrices, then there exists a vector $x \in \mathbb{F}_2^N$ that agrees with both A and B.*

Lemma 2.4. *Let $A_{N\times n}$ be a 01-matrix such that deleting any column of A yields a balanced $N \times (n-1)$ matrix. Then, either (i) A is balanced, or (ii) each row of A has an even number of 1's, or (iii) each row of A has an odd number of 1's.*

Lemma 2.5. *Let $A_{N\times k}$ be a balanced matrix with $k \le n$, and let T be a non-singular $k \times k$ 01-matrix, then AT is also balanced, where all the arithmetic is done modulo 2.*

Notice that when x agrees with A, we can insert x into any position between the columns of A to get a balanced matrix. It is also easy to see that $(SE_n)^m$ $(m > n)$ is rearrangeable if and only if for every two given balanced matrices $A_{N\times n}$ and $B_{N\times n}$ there exists an $N \times (m-n)$ balanced matrix M such that the matrix $[A, M, B]$ is balanced. Here the rows of A are binary representations of the inputs and the corresponding rows of B are binary representations of the matched outputs.

3 Main Results

To illustrate the idea and introduce notations needed for the main theorem, we first reproduce a known result [9,7] using the new method.

Lemma 3.1. *$m(3) = 5$, namely the network $(SE_3)^5$ is rearrangeable.*

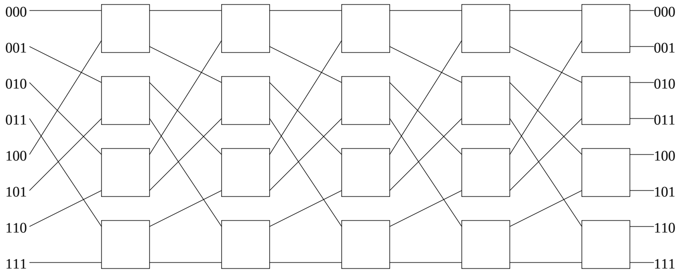


Figure 2. The 5-stage SE network for $N = 8$, i.e. $(SE_3)^5$

Proof. We use the same approach as that of Raghavendra and Varma, [7] namely from first principles. However, the method is different and more intuitive. Figure 2 shows a typical drawing of a 5-stage SE network for $N = 8$. For convenience, the network can be redrawn and the switches can be labeled as shown in Figure 3. In the figure, the inputs and outputs have been numbered in decimals for convenience. We write $x \in I_i$ ($y \in O_j$) if input x (output y) is connected to input switch I_i (output switch O_j). Given a perfect matching π (or permutation) from the inputs $\{0,4,2,6,1,5,3,7\}$ to the outputs $\{0,1,2,3,4,5,6,7\}$, we first construct a 4×4, 2-regular multi-bipartite graph $G(\pi) = (I, O, E)$ whose bipartitions are $I = O = \{0,1,2,3\}$. I and O correspond to the input and output switches respectively. We shall refer to $G(\pi)$ as G if π is clear from the context. $(i,j) \in E$ iff $\pi(x) = y$ for some $x \in I_i$ and $y \in O_j$, introducing multiple edges if necessary. We now need some notations. Suppose we have colored the edges of G with colors in $C = \{0,1,2,3\}$. For each $c \in C$, let $L(c)$ ($R(c)$) be the multi-set of the vertices in I (O) which are incident to an edge colored c. For each subset $S \subseteq C$, let $L(S) = \bigcup_{c \in S} L(c)$ and $R(S) = \bigcup_{c \in S} R(c)$, where the union is multi-set union. For each $e \in E$, let $l(e)$ ($r(e)$) denote the vertex in I (O) incident to e. Similarly, for any subset $A \subseteq E$, let $L(A) = \{l(e) \mid e \in A\}$ and $R(A) = \{r(e) \mid e \in A\}$.

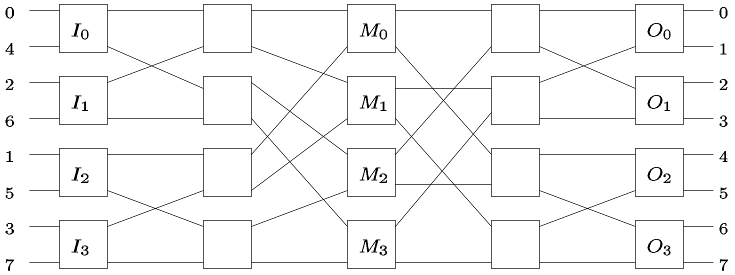


Figure 3. A redrawing of the $(SE_3)^5$ network

To this end, we observe from Figure 3 that the realizability of the matching is equivalent to the existence of a coloring of G with colors in C such that

(P_0) Each color appears exactly twice.

(P_1) For each $c \in C$, $L(c)$ has a representative from each of $\{0,1\}$ and $\{2,3\}$.

(P_2) $L(\{0,1\}) = L(\{2,3\}) = \{0,1,2,3\}$. In other words, $L(\{0,1\})$ and $L(\{2,3\})$ have distinct elements.

(P_1') For each $c \in C$, $R(c)$ has a representative from each of $\{0,1\}$ and $\{2,3\}$.

(P_2') $R(\{0,2\}) = R(\{1,3\}) = \{0,1,2,3\}$. In other words, $R(\{0,2\})$ and $R(\{1,3\})$ have distinct elements.

The conditions are chosen so that the two edges colored $c \in \{0,1,2,3\}$ will be routed through middle switch M_c. We will not state and prove the correctness of any routing algorithm based on the coloring here, as it is straightforward.

We now describe a procedure to properly color all such G as follows. Along the way, we shall also prove that our procedure works.

Phase 1. As G is 2 regular and bipartite, it is the union of even cycles. G thus can be decomposed into two 4×4 perfect matchings by taking alternate edges on each cycle. Let the matchings be M_1 and M_2 (whose vertex sets are the same as G.)

Phase 2. From each M_i ($i = 1,2$), construct a 2×2 2-regular bipartite graph G_i by combining within each bipartition of M_i the pairs of vertices $\{0,1\}$ and $\{2,3\}$. Figure 4 illustrates the results of our first two phases. Obviously, $L(E(G_i)) = R(E(G_i)) = \{0,1,2,3\}$, for $i = 1,2$. Here and henceforth the L and R functions are applied in the context of the original graph G.

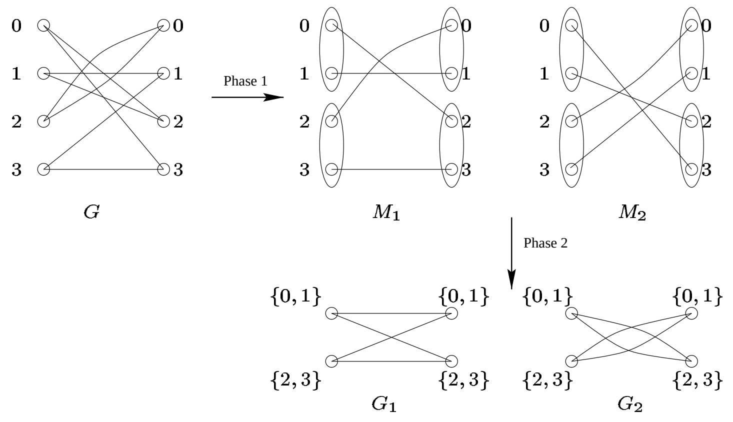


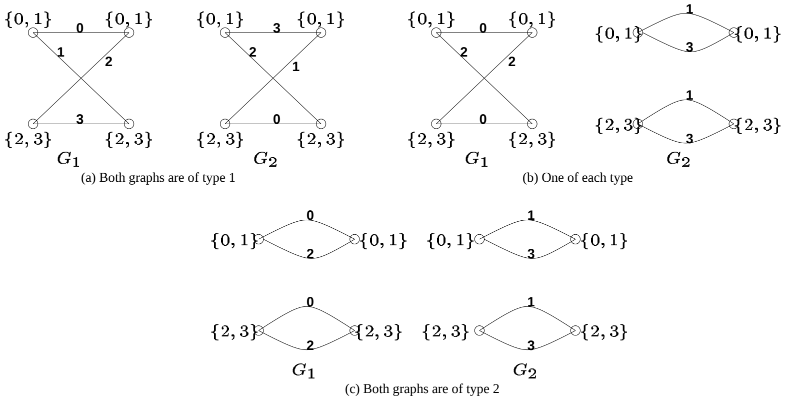
Figure 4. An illustration of the first two phases

We call the graphs G_1 and G_2 the *basic components* of G. Since the basic components are 2×2 2-regular bipartite graphs, they can only be either a 4-cycle or a union of two 2-cycles. A basic component is said to be of *type 1* if it is a 4-cycle and of *type 2* otherwise. In Figure 4, G_1 is of type 1 and G_2

is of type 2.

Phase 3. As each coloring of G_1 and G_2 induces uniquely a coloring of G, we are to color G_1 and G_2 so that the coloring satisfy conditions P_0, P_i and P'_i, $1 \leq i \leq 2$. We call an edge whose color is $c \in C$ a *c-edge*. Consider two cases:

Case 1. Both G_1 and G_2 are of type 1. In this case we color the graphs as shown in Figure 5a. It is easy to see that the coloring satisfies all prescribed conditions. The basic idea is that as we have used each color exactly twice, to enforce P_1 and P'_1 we need to make sure that if there is a c-edge going from $\{0,1\}$ to $\{0,1\}$, then the other c-edge must go from $\{2,3\}$ to $\{2,3\}$ in either basic components, and similarly if a c-edge going from $\{0,1\}$ to $\{2,3\}$ then the other c-edge must go from $\{2,3\}$ to $\{0,1\}$. To enforce P_2 and P'_2, on the left side (the I side) we *separate* each color pair $\{0,1\}$ and $\{2,3\}$, while on the right (the O side) we separate the pairs $\{0,2\}$ and $\{1,3\}$.



(a) Both graphs are of type 1

(b) One of each type

(c) Both graphs are of type 2

Figure 5. Illustration of the colorings when $n = 3$

Case 2. There is one graph of type 2. Without loss of generality, assume G_2 is of type 2 as illustrated in Figures 5b and 5c. In this case we color G_1 with $\{0,2\}$ and G_2 with $\{1,3\}$. Notice that P_0, P_1, P'_1, and P'_2 are satisfied even if we switch colors in one (or both) 2-cycles of G_2. To ensure P_2, we do this switching if necessary at each 2 cycle of G_2.

□

Secondly, we use the idea to derive a more elaborate proof for the case where $N = 16$. Firstly, we redraw the network as shown in Figure 6, so that it is easier to derive the conditions similar to the P_i and P'_i. From the figure, the

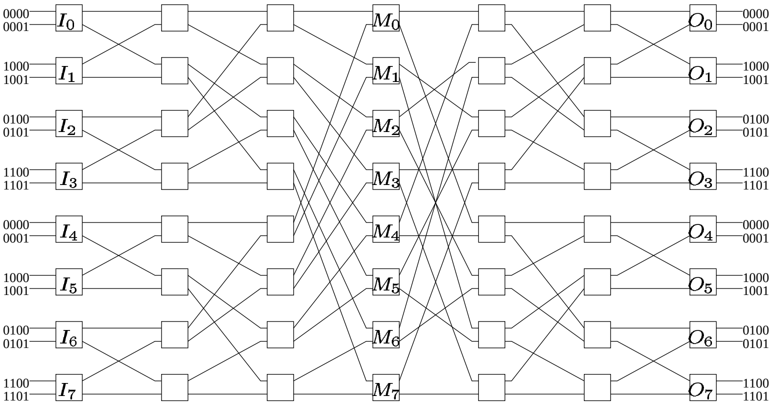


Figure 6. A redrawing of the $(SE_4)^7$ network

following proposition is easy to see. We reuse all notations introduced in the proof of Lemma 3.1. Again, as a valid coloring induces a routing algorithm in a straightforward way, we shall not describe the algorithm here.

Proposition 3.2. *The fact that $(SE_4)^7$ is rearrangeable is equivalent to the fact that for any 8×8 2-regular multi-bipartite graph $G = (I, O)$ with bipartitions $I = O = \{0, \ldots, 7\}$, there exists an edge coloring of G using colors in $C = \{0, \ldots, 7\}$ satisfying the following conditions:*

(P_0) Each $c \in C$ appears exactly twice.

(P_1) For each $c \in C$, $L(c)$ has a representative from each of $\{0, 1, 2, 3\}$ and $\{4, 5, 6, 7\}$.

(P_2) For each pair $\{c_1, c_2\} \in \{\{0, 1\}, \{2, 3\}, \{4, 5\}, \{6, 7\}\}$, $L(\{c_1, c_2\})$ has a representative from each of $\{0, 1\}$, $\{2, 3\}$, $\{4, 5\}$, and $\{6, 7\}$.

(P_3) $L(\{0, 1, 2, 3\}) = L(\{4, 5, 6, 7\}) = \{0, 1, \ldots, 7\}$. In other words, the elements of $L(\{0, 1, 2, 3\})$ and $L(\{4, 5, 6, 7\})$ are all distinct.

(P'_1) For each $c \in C$, $R(c)$ has a representative from each of $\{0, 1, 2, 3\}$ and $\{4, 5, 6, 7\}$.

(P'_2) For each pair $\{c_1, c_2\} \in \{\{0, 4\}, \{2, 6\}, \{1, 5\}, \{3, 7\}\}$, $R(\{c_1, c_2\})$ has a representative from each of $\{0, 1\}$, $\{2, 3\}$, $\{4, 5\}$, and $\{6, 7\}$.

(P'_3) $R(\{0, 4, 2, 6\}) = R(\{1, 5, 3, 7\}) = \{0, 1, \ldots, 7\}$. In other words, the elements of $R(\{0, 4, 2, 6\})$ and $R(\{1, 5, 3, 7\})$ are all distinct.

Note that the conditions were specifically chosen so that each pair of edges with the same color $c \in C$ shall be routed through middle switch M_c without causing any conflict. From now on, we shall refer to a *valid* coloring of G as the coloring satisfying the prescribed conditions in Proposition 3.2.

Theorem 3.3. *$m(4) = 7$, namely the network $(SE_4)^7$ is rearrangeable.*

Proof. Given any perfect matching π from the inputs to the outputs, we first construct the 8×8 2-regular multi-bipartite graph G in a similar way as the G in Lemma 3.1. The bipartitions of G are $I = O = \{0, \ldots, 7\}$, and $(i,j) \in E(G)$ if for some $x \in \{0, \ldots, 15\}$ we have $x \in I_i$ and $\pi(x) \in O_j$. To color G properly, i.e. the coloring satisfies the conditions of Proposition 3.2, we decompose G into 4 basic components. The decomposition is formally described below. Figure 7 illustrates the decomposition procedure.

Phase 1 Decompose G into two edge disjoint 8×8 perfect matchings M_1 and M_2.

Phase 2 For each $i = 1, 2$, construct the graph G_i by collapsing the pairs of vertices $\{0,1\}$, $\{2,3\}$, $\{4,5\}$, and $\{6,7\}$ on each bipartition of M_i. It is clear that the graphs G_i are 4×4 2-regular bipartite graphs.

Phase 3 For each $i = 1, 2$, decompose G_i into two edge disjoint 4×4 perfect matchings M_{i1} and M_{i2}.

Phase 4 For each $i = 1, 2$ and $j = 1, 2$, construct the graph G_{ij} by collapsing the pairs of vertices $\{01, 23\}$ and $\{45, 67\}$ on each bipartition of M_{ij}. As before, the G_{ij} are called *basic components* of G, and can only be one of two types: (a) type 1 corresponds to a 4-cycle and (b) type 2 corresponds to two 2 cycles. We are now ready to color the basic components so that the (uniquely) induced coloring on G is valid.

As we have seen in the proof of Lemma 3.1, the number of type-2 basic components can roughly be thought of as the degree of flexibility in finding a valid coloring for G. Our basic idea is to give different colorings of G based on the number of basic components of type-2. Although the idea is simple, the cases are quite tricky and long. Due to limited space, the reader is referred to Ngo and Du [12] (2000) for the full proof. □

To this end, we use the formulation of Linial and Tarsi to show an auxiliary lemma and then combine the lemma with Theorem 3.3 to improve the upper bound of $m(n)$. The following lemma has been shown by Varma and Raghavendra [8], however the proof was rather long. We straightforwardly extend Theorem 3.1 in Linial and Tarsi work [9] to obtain a much shorter proof.

Lemma 3.4. *If $m(k) = 2k - 1$ for a fixed $k \in \mathbb{N}$, then $(SE_n)^{3n-k-1}$ is rearrangeable whenever $n \geq k$.*

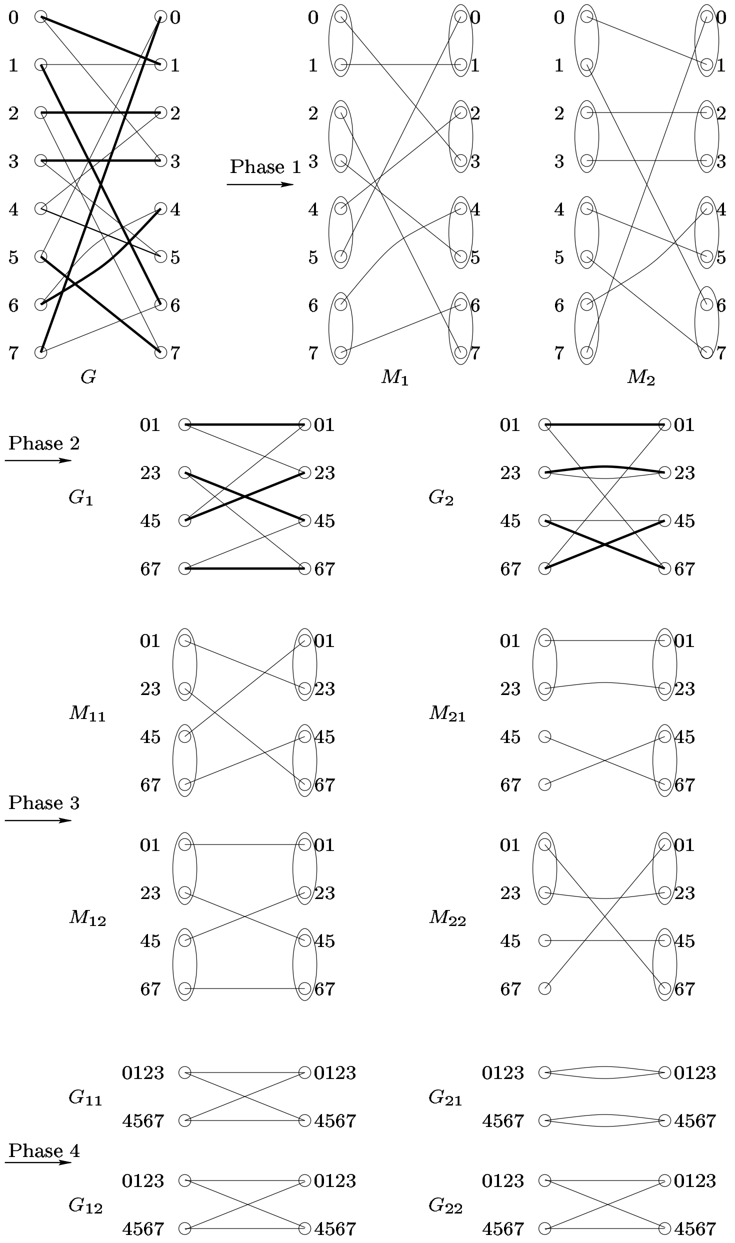


Figure 7. An illustration of the basic component decomposition

Proof. The assertion in the lemma is equivalent to the fact that if we know $m(k) = 2k - 1$, then for every two $N \times n$ balanced matrices $A = [a_1, \dots, a_n]$ and $B = [b_1, \dots, b_n]$, there exists an $N \times (2n - k - 1)$ balanced matrix M such that the matrix $[A, M, B]$ is balanced. Here a_i and b_i are the i^{th} columns of A and B respectively. We shall construct the $(2n - k - 1)$ column vectors which form M. The construction takes several steps as follows.

Step 1. Repeatedly apply Lemma 2.3 to constructs vectors $\{u_1, \dots, u_{n-k}\}$ such that for $i = 1, \dots, n - k$, u_i agrees with $[a_{i+1}, \dots, a_n, u_1, \dots, u_{i-1}]$ and $[u_{i-1}, \dots, u_1, b_n, \dots, b_{i+1}]$. Let $U = [u_1, \dots, u_{n-k}]$ and $U^R = [u_{n-k}, \dots, u_1]$, then after this step both $[A, U]$ and $[U^R, B]$ are balanced.

Step 2. We want to construct vectors $x_1, \dots, x_{k-1}$ such that if we let $X = [x_1, \dots, x_{k-1}]$, then $[A, U, X]$ and $[X, U^R, B]$ are both balanced. Notice that as U is an $N \times (n-k)$ balanced matrix, each row of U occurs exactly 2^k times, and so do the rows of U^R in the same positions. Hence, the rows of U and U^R can be partitioned into 2^{n-k} classes of 2^k identical row vectors in each partition. For v be any column of U or U^R, let $v^{(i)}$ be the subvector of v with entries in the i^{th} partition, where $0 \leq i \leq 2^{n-k} - 1$. Notice that $v^{(i)} \in \mathbb{F}_2^k$ for each i. Also, for each $i = 0, \dots, 2^{n-k} - 1$, let

$$A^{(i)} = [a_{n-k+1}^{(i)}, \dots, a_n^{(i)}]$$

and

$$A^{(i)} = [b_n^{(i)}, \dots, b_{n-k+1}^{(i)}]$$

Then, since Beneš conjecture is true for k (i.e. $m(k) = 2k - 1$), there exist vectors $x_1^{(i)}, \dots, x_{k-1}^{(i)}$ such that $[A^{(i)}, X^{(i)}, B^{(i)}]$ is balanced. The vectors $x_1, \dots, x_{k-1}$ are obtained by pasting together the $x_j^{(i)}$ preserving the positions of the partitions.

After this step, $[A, U, X]$ is balanced because at the positions where the rows of U are identical we have $[A^{(i)}, X^{(i)}]$ being a $2^k \times k$ balanced matrix. The fact that $[X, U^R, B]$ is balanced can be shown similarly.

Step 3. Now we define an $N \times (n - k)$ matrix W from U such that $[A, W, X, U^R, B]$ is balanced. Define W as follows (all arithmetics are done over $\mathbb{F}_2$).

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

We are left to show that $[A, W, X, U^R, B]$ is balanced. The balancedness of $[X, U^R, B]$ has already been established, so we only need to show that

$[A, W, X, U^R]$ is balanced. We do this by considering the following types of submatrices:

(a) Submatrices of the form $[a_i, \dots, a_n, w_1, \dots, w_{i-1}]$ where $2 \leq i \leq n - k + 1$. We apply Lemma 2.5 and use the fact that $[a_i, \dots, a_n, u_1, \dots, u_{i-1}]$ is balanced. $[a_i, \dots, a_n, w_1, \dots, w_{i-1}]$ can be obtained from $[a_i, \dots, a_n, u_1, \dots, u_{i-1}]$ by an invertible linear transformation with the invert map preserves the a_j $(i \leq j \leq n)$ and

$$u_j = \begin{cases} w_j & 1 \leq j \leq \frac{n-k}{2} \\ w_j + w_{n-i-k} & \frac{n-k}{2} + 1 \leq j \leq n - k - 1 \\ w_{n-k} + a_n & j = n - k \end{cases}$$

(b) Submatrices of the form $[a_i, \dots, a_n, w_1, \dots, w_{n-k}, x_1, \dots, x_{k+i-n-1}]$ where $n - k + 2 \leq i \leq n$. Similarly, in this case we use Lemma 2.5 and the balancedness of the matrix $[a_i, \dots, a_n, u_1, \dots, u_{n-k}, x_1, \dots, x_{k+i-n-1}]$

(c) Submatrices of the form $[w_i, \dots, w_{n-k}, x_1, \dots, x_{k-1}, u_{n-k}, \dots, u_{n-k-i+1}]$ where $1 \leq i \leq n - k$. Here we use the fact that $[a_n, u_1, \dots, u_{n-k}, x_1, \dots, x_{k-1}]$ is balanced.

□

Theorem 3.5. *For $n \in \mathbb{N}$ and $n \geq 4$, a SE network with $3n - 5$ stages is rearrangeable.*

Proof. This is immediate from Theorem 3.3 and Lemma 3.4. □

4 Discussions

In this paper, we have verified that the 7-stage SE network for $n = 4$ is rearrangeable. This result and an extension of another formulation were used to show that $3n - 5$ SE stages are sufficient for the rearrangeability of the SE network with 2^n inputs and 2^n outputs.

It was conjectured that $2n - 1$ SE stages are necessary and sufficient for the SE network to be rearrangeable. However, there has been very slow progress on proving the conjecture. We hope that our work, besides improving the bound, contribute to the effort of attacking this difficult problem.

Acknowledgments

This work was supported in part by the National Science Foundation under grant CCR-9530306.

References

1. H.S. Stone. Parallel processing with perfect shuffle. *IEEE Trans. Comput.*, 20:153–161, 1971.
2. V. E. Beneš. Proving the rearrangeability of connecting networks by group calculations. *Bell System Tech. J.*, 54:421–434, 1975.
3. D. Stott Parker, Jr. Notes on shuffle/exchange-type switching networks. *IEEE Trans. Comput.*, 29(3):213–222, 1980.
4. V. E. Beneš. *Mathematical theory of connecting networks and telephone traffic.* Academic Press, New York, 1965. Mathematics in Science and Engineering, Vol. 17.
5. Chuan Lin Wu and Tse Yun Feng. The universality of the shuffle-exchange network. *IEEE Trans. Comput.*, 30(5):324–332, 1981.
6. Shing Tsaan Huang and Satish K. Tripathi. Finite state model and compatibility theory: New analysis tools for permutation networks. *IEEE Trans. Comput.*, 35(7):509–601, 1986.
7. C. S. Raghavendra and Anujan Varma. Rearrangeability of the five-stage shuffle/exchange network for $N = 8$. *IEEE Trans. Comm.*, 35(8):808–812, 1987.
8. A. Varma and C. Raghavendra. Rearrangeability of multistage shuffle/exchange networks. *IEEE Trans. Comm.*, COM-36, 10:1138–1147, 1988.
9. Nathan Linial and Michael Tarsi. Interpolation between bases and the shuffle exchange network. *European J. Combin.*, 10(1):29–39, 1989.
10. Tse-yun Feng and Seung-Woo Seo. A new routing algorithm for a class of rearrangeable networks. *IEEE Trans. Comput.*, 43(11):1270–1280, 1994.
11. M.K. Kim, H. Yoon, and S.R. Maeng. On the correctness of inside-out routing algorithm. *IEEE Trans. Comput.*, 46(7):820–823, 1997.
12. Hung Q. Ngo and Ding-Zhu Du. On the rearrangeability of shuffle-exchange networks. Technical Report TR00-045, Dept of Computer Science, University of Minnesota, 2000.