Philips Research Laboratory
2, av. Van Becelaere, Box 8
1170-Brussels, Belgium

The Construction of Cellular Permutation Networks

C. Ronse

Abstract

We study several operations for constructing permutation networks using smaller permutation networks as components. In particular the well-known networks of Benes, Waksman and Green can be defined with these operations. Finally we show that Joel's nested tree can be transformed into Waksman's network by suitable permutations of the inputs and outputs of the cells and of the network.

Running head :

Cellular Permutation Networks

Key phrases

Cellular permutation networks

Shuffles

Waksman's network

Joel's nested tree

§I Introduction.

A permutation network P on n bits is a switching circuit with n data input terminals, $I_0,\ldots,I_{n-1}$, a certain number of control input terminals, and n output terminals $O_0,\ldots,O_{n-1}$, which can realize the n! following input-output behaviours :

$$P(\pi) : \text{For } i=0,\ldots,n-1 ,$$
$$[I_i] = [O_{i\pi}] , \qquad (1)$$

where $[I_i]$ and $[O_j]$ are the signals on I_i and O_j respectively, π is an arbitrary permutation of $\{0,\ldots,n-1\}$, and $i\pi$ is the image of i under π . We say that P realizes π .

We will study several operations for constructing permutation networks using smaller permutation networks as components. We will restrict ourselves to loopless combinational circuits, although permutation networks can be built from sequential networks.

In particular, permutation networks built from small prefabricated permutation networks called cells, in other words cellular permutation networks, can be built with these operations. This is the case of the networks of Benes [2] , Waksman and Green[6,8,13] .

Finally our method allows us to compare the network of Waksman and Green with Joel's nested tree. We show how one can be obtained from the other by suitable permutations of the inputs and outputs of its cells, and finally of the network itself.

We deduce then that the "looping"algorithm [13] used for the control of Waksman's network can also be used for the control of a slightly modified version of Joel's network (which is isomorphic to it).

§II Notations and definitions.

For brievity's sake, we will write "input" for "data input terminal", "output" for "output terminal", and "control line" for "control input terminal". The inputs, outputs and control lines of an n-bit network N can be written $I_i(N)$, $O_j(N)$ and $C_k(N)$ respectively (with i,j=0,...,n-1 and k=0,...,p-1 for some p).

For a positive integer n we will write Z_n for the set {0,...,n-1}. The image of an element i of Z_n by a permutation π of Z_n is written $i\pi$.

Let us now consider networks which realize permutations.

First consider the simple connection S with one input and one output. It is the permutation network on 1 bit.

For a positive integer n and a set Π of permutations of Z_n, a partial permutation network $P(n,\pi)$ on n bits is a switching circuit P with n inputs, n outputs and, say, p control lines which can realize the input-output behaviour $P(\pi)$ for every π belonging to Π (see (1)). As control variables are binary, we must have :

$$p \geqslant \log_2(|\Pi|) \quad . \qquad (2)$$

We will generally write P(n) for a (partial) permutation network on n bits.

Given k partial permutation networks $P_i = P_i(n_i)$ (where $i=0,1,\ldots,k-1$) a set $I = \{I_0,\ldots,I_{n-1}\}$ of terminals called inputs, a set $O = \{O_0,\ldots, O_{n-1}\}$ of terminals called outputs (where $n \geq n_i$ for each $i=0,1,\ldots,k-1$) and a set Γ of connections between the terminals I_i, O_j, $I_r(P_u)$, $O_s(P_v)$, let us call $N(I,O; P_0,\ldots,P_{k-1}; \Gamma)$ the resulting network. We suppose that Γ consists only of connections of the type $(I_i, I_r(P_u))$, $(O_s(P_v), I_r(P_u))$, $(O_s(P_v), O_j)$ and (I_i, O_j). Then $N(I,O; P_0,\ldots,P_{k-1}; \Gamma)$ is a partial permutation network if :

(i) All connections are one-to-one.

(ii) The circuit contains no loop ; in other words there is an order relation, say, "is to the left of", on Z_k, such that if $(O_s(P_v), I_r(P_u)) \in \Gamma$, then v is to the left of u.

The first condition ensures that the input-output behaviours are one-to-one. The second condition is necessitated by our restriction to loopless combinational networks.

We call an m-cell a permutation network on m bits which is not built by the above construction. In many cases restricts oneself to 2-cells (also called β-elements [7]).

An m-cell is usually represented by a square or a vertical segment, with the inputs on the left and the outputs on the right (this is illustrated in Fig.1(a) for m=5. A 2-cell and its states are shown in Fig.1(b). The designs of a 2-cell using multiplexers or logical gates are shown in Fig. 2(a) and (b) respectively.

A cellular partial permutation network is a partial permutation network P of the form $N(I,O; P_0,\ldots,P_{k-1};\Gamma)$, where $P_0,\ldots,P_{k-1}$

are cells. If P is a permutation network, then we say that it is a cellular permutation network.

Consider two cellular partial permutation networks on n bits having both the same number k of cells, say $P=N(I,O; P_0,\ldots,P_{k-1}; \Gamma)$ and $Q=N(I',O'; Q_0, \ldots, Q_{k-1}; \Delta)$.

(1) P and Q are isomorphic and write $P \overset{\sim}{=} Q$ if there is a map $\phi: \{P_0,\ldots,P_{k-1}\} \to \{Q_0,\ldots,Q_{k-1}\}$ such that :

(i) For $i=0,\ldots,k-1$, P_i and $P_i\phi$ have the same number of inputs (or outputs)

(ii) The map ϕ' induced by ϕ on Γ , defined by

$$(I_i,O_j)\phi' = (I'_i, O'_j)$$
$$(I_i, I_r(P_u))\phi' = (I'_i, I_r(P_u\phi))$$
$$(O_s(P_v), I_r(P_u))\phi' = (O_s(P_v\phi), I_r(P_u\phi))$$
$$(O_s(P_v), O_j)\phi' = (O_s(P_v\phi), O'_j)$$

is a bijection $\Gamma \to \Delta$.

(2) P and Q are equivalent and write $P \overset{\sim}{=} Q$ if P is isomorphic to Q up to a relabelling of the inputs and outputs of Q.

(3) P and Q are quasiisomorphic and write $P \overset{\sim}{\approx} Q$ if P and Q are isomorphic up to a relabelling of the inputs and outputs of each Q_i.

(4) P and Q are quasiequivalent and write $P \sim Q$ if P and Q are equivalent up to a relabelling of the inputs and outputs of each Q_i.

These concepts are illustrated in Fig.3(a), (b), (c) and (d). These 4 relations are equivalence relations.

§III. Shuffles and generalized shuffles.

This section is a summary of [10] .

When making connections between different stages of cells, one often uses permutations called generalized shuffles. To define them, one needs first to define mixed radix number representation systems.

Let $b_0,\ldots,b_{n-1}$ be integers bigger than 1 ; let $q=b_0\times\ldots\times b_{n-1}$. Then any integer comprised between 0 and q-1 can be represented in a unique way as a vector $[a_{n-1},\ldots,a_0]$ with $a_i \in Z_{b_i}$ for i=0,...,n-1, by the following rule:

$$[a_{n-1},\ldots,a_0] = a_{n-1}b_{n-2}\times\ldots\times b_0+a_{n-2}b_{n-3}\times\ldots\times b_0+\ldots a_1b_0+a_0 \ . \qquad (3)$$

This representation of the elements of Z_q is called the mixed radix representation with respect to the basis $[b_{n-1},\ldots,b_0]$ (See [3]).

If has the following property : Suppose that for i=0,...,n-1 $b_i=b_{i,0}\times\ldots\times b_{i,m(i)-1}$. Let $m \in Z_q$. If m has $[a_{n-1},\ldots,a_0]$ as mixed radix representation with respect to the basis $[b_{n-1},\ldots,b_0]$ and if for i=0,...,n-1, a_i has $[a_{i,m(i)-1},\ldots,a_{i,0}]$ as mixed radix representation with respect to the basis $[b_{i,m(i)-1},\ldots,b_0]$, then m has

$$[a_{n-1,m(n-1)-1},\ldots,a_{n-1,0},\ldots,a_{i,m(i)-1},\ldots,a_{i,0},\ldots,a_{0,m(0)-1},\ldots,a_{0,0}] \qquad (4)$$

as mixed radix representation with respect to the basis

$$[b_{n-1,m(n-1)-1},\ldots,b_{n-1,0},\ldots,b_{i,m(i)-1},\ldots,b_{i,0},\ldots,b_{0,m(0)-1},\ldots,b_{0,0}] \qquad (5)$$

Let us now define the perfect shuffle. Let q=ab. Any element

m of Z_q can be written as ib+j (with $i \in Z_a$ and $j \in Z_b$) or as j'a+i' (with $i' \in Z_a$ and $j' \in Z_b$). The (a,b)-shuffle on Z_q is the permutation $\sigma(a,b)$ of Z_q defined as follows (see [3]) :

$$\sigma(a,b):m = ib+j \to m\sigma(a,b) = ja+i \qquad (i \in Z_a,\ j \in Z_b).$$

Thus $\sigma(a,b)$ maps [i,j] (in the basis [a,b]) onto [j,i] (in the basis [b,a])

Note that $\sigma(a,b)$ fixes 0 and q-1 and that $\sigma(b,a)$ is the inverse of $\sigma(a,b)$.

We now define a generalization of the perfect shuffle, called the <u>generalized shuffle</u>. Let q be an integer bigger than 1 and suppose that $q=b_{n-1}\times\ldots\times b_0$, where each b_i is an integer bigger than 1. Let $m \in Z_q$. If $\pi \in \mathrm{Sym}(n)$, then we can write m in the mixed radix representation with respect to the basis $[b_{(n-1)\pi},\ldots, b_{0\pi}]$:

$$m = a_{(n-1)\pi}\, b_{(n-2)\pi}\times\ldots\times b_{0\pi} + \ldots + a_{1\pi}\, b_{0\pi} + a_{0\pi}$$

$$= \sum_{i=0}^{n-1} \left(a_{i\pi} \prod_{j=0}^{i-1} b_{j\pi}\right), \text{ where } a_i \in Z_{b_i} \text{ for } i \in Z_n \ . \qquad (6)$$

(For i=0 the empty product $\prod_{j=0}^{i-1}$ is equal to 1)

Now, if ρ is another permutation of Z_q, then $a_{(n-1)\rho}\, b_{(n-2)\rho}\times\ldots\times b_{0\rho}+\ldots+a_{1\rho}b_{0\rho}+ a_{0\rho} = \sum_{i=0}^{n-1} \left(a_{i\rho} \prod_{j=0}^{i-1} b_{j\rho}\right)$ is the mixed radix representation of a number $m' \in Z_q$ with respect to the basis $[b_{(n-1)\rho},\ldots,b_{0\rho}]$.

We define the $\binom{(n-1)\pi,\ldots,\ 0\pi}{(n-1)\rho,\ldots,\ 0\rho}$-shuffle on Z_q as the following permutation of Z_q :

$$\sigma\binom{(n-1)\pi,\ldots,0\pi}{(n-1)\rho,\ldots,0\rho} : \sum_{i=0}^{n-1}\left(a_{i\pi}\prod_{j=0}^{i-1} b_{j\pi}\right) \to \sum_{i=0}^{n-1}\left(a_{i\rho}\prod_{j=0}^{i-1} b_{j\rho}\right) . \qquad (7)$$

It corresponds to the following change of basis in a mixed radix representation of Z_N :

$$[b_{(n-1)\pi},\ldots, b_{0\pi}] \to [b_{(n-1)\rho},\ldots,b_{0\rho}] . \qquad (8)$$

If n=2, then $\sigma(b_1,b_0)= \sigma\binom{1,0}{0,1}$ with respect to the basis $[b_1,b_0]$.

If n=3, then we will write $b_2\ \sigma(b_1,b_0)$ for $\sigma\binom{2,1,0}{2,0,1}$ and $\sigma(b_2,b_1)b_0$ for $\sigma\binom{2,1,0}{1,2,0}$. It is easily seen that $b_2\ \sigma(b_1,b_0)$ is the union of b_2 copies of $\sigma(b_1,b_0)$, while $\sigma(b_2,b_1)b_0$ induces $\sigma(b_2,b_1)$ on b_2b_1 sets of size b_0.

The generalized shuffles have the following two properties :

(1°): If $\pi,\rho,\tau \in \mathrm{Sym}(n)$, then we have :

$$\sigma\binom{(n-1)\pi,\ldots,0\pi}{(n-1)\rho,\ldots,0\rho}\ \sigma\binom{(n-1)\rho,\ldots,0\rho}{(n-1)\tau,\ldots,0\tau} = \sigma\binom{(n-1)\pi,\ldots,0\pi}{(n-1)\tau,\ldots,0\tau} \qquad (9)$$

In particular, $\sigma\binom{(n-1)\rho,\ldots,0\rho}{(n-1)\pi,\ldots,0\pi}$ is the inverse of $\sigma\binom{(n-1)\pi,\ldots,0\pi}{(n-1)\rho,\ldots,0\rho}$.

(2°): If for $i \in Z_n$, $b_i=b_{i,0}\cdot\ldots\cdot b_{i,m(i)-1}$, then $\sigma\binom{(n-1)\pi,\ldots,0\pi}{(n-1)\rho,\ldots,0\rho}$ (with respect to the basis $[b_{n-1},\ldots,b_0]$)

$$= \sigma\binom{((n-1)\pi,m((n-1)\pi)-1),\ldots,((n-1)\pi,0),\ldots,(0\pi,m(0\pi)-1),\ldots,(0\pi,0)}{((n-1)\rho,m((n-1)\rho)-1),\ldots,((n-1)\rho,0),\ldots,(0\rho,m(0\rho)-1),\ldots,(0\rho,0)} \qquad (10)$$

(with respect to the basis $[b_{n-1,m(n-1)-1},\ldots,b_{n-1,0},\ldots,b_{0,m(0)-1},\ldots,b_{0,0}]$).

Example. If n=4, then $\sigma\binom{3,2,1,0}{1,0,3,2}= \sigma(b_3b_2,b_1\ b_0)$.

Property (2°) is to be linked to (4) and (5).

§IV. Operations on partial permutation networks.

We will define here ten operations on partial permutation networks.

(i) Dual. This operation is defined for cellular partial permutation networks only. Let $P=N(I,O;\ P_0,\ldots,P_{k-1};\Gamma)$, where $P_0,\ldots,P_{k-1}$ are cells. Then the dual P^* of P is built as follows : $P^*=N(I,O;\ P_0,\ldots,P_{k-1};\Delta)$, where $\Delta=\{(Y^*,X^*) \mid (X,Y)\in\Gamma\}$, with $I_i^*=O_i$, $O_j^*=I_j$, $I_r(P_u)^* = O_r(P_u)$ and $O_s(P_v)^*=I_s(P_v)$

Thus P^* is built from P by inverting inputs and outputs in all cells and all connections. This construction is illustrated in Fig.4.

Clearly, if P realizes the set Π of permutation, then P^* realizes $\Pi^{-1}=\{x^{-1} \mid \pi\in\Pi\}$.

(ii) Union. Let $A_0,\ldots,A_{n-1}$ be partial permutation networks. Then we define the partial permutation network $A_0\cup\ldots\cup A_n$ by taking pairwise disjoint copies of $A_0,\ldots,A_n$, taking $I(A_0)\cup\ldots\cup I(A_n)$ as set of inputs and $O(A_0)\cup\ldots\cup O(A_n)$ as set of outputs and considering the resulting network.

(iii) Left scalar multiplication. Let m be a positive integer and A a partial permutation network on n bits. Let $A^{(0)},\ldots,A^{(m-1)}$ be m disjoint copies of A. Label the ith input/output of $A^{(j)}$ ($i\in Z_n$, $j\in Z_m$) nj+i. Then $mA=A^{(0)}\cup\ldots\cup A^{(m-1)}$ with this labelling.

(iv) Right scalar multiplication. We do as in (iii), but label the ith input/output of $A^{(j)}$ mi+j. Then we get the netwok Am. Note that mA and Am are equivalent.

(v) Composition. Let $A_0,\ldots,A_{m-1}$ be partial permutation networks on n bits. For $i=0,\ldots,m-2$ and $j=0,1,\ldots,n-1$, connect $O_j(A_i)$ with $I_j(A_{i+1})$. Take $I(A_0)$ as set of inputs and $O(A_{m-1})$ as set of outputs. Then the resulting network is $A_0.A_1\ldots A_{m-1}$.

In the five preceding operations, one can replace a partial permutation network by a permutation (which can be considered as a cellular permutation network without cell and without control line). If π and ρ are permutations, then $\pi^*=\pi^{-1}$ and the composition $\pi.\rho$ is the group-theoretic product of π by ρ. Note that the definitions of $m\sigma(a,b)$ and $\sigma(a,b)m$ given in §III are identical to the ones given in (iii) and (iv) of this section.

Let us now define five more constructions using the perfect shuffle :

(vi) Product [9]. Let A and B be partial permutation networks on a and b bits respectively. Then the product A×B is the partial permutation network $bA.\sigma(b,a).aB$.

(vii) Extended product [9]. Take A and B as in (6). Suppose that A is cellular. Then the extended product A××B is the partial permutation network $bA.\sigma(b,a).aB.\sigma(a,b).bA^*$.

If A and B are permutation networks, then A××B is a permutation network by the theorem of Slepian and Duguid [2,4,12].

(viii) The Goldstein-Leibholtz construction [5].

Let A and B be as in (vii).

Then the Goldstein-Leibholz construction $A \wedge B$ is built as follows : Take the extended product A××B, delete the first copy of A^* in the third stage

and replace it by aS, where S is a simple connection.

If A and B are permutation networks, then $A \wedge B$ is a permutation network by Theorem 1 of [5].

(ix) A construction of Benes [1,2 (p. 114, Theorem 3.10)].

Let $A_0,\ldots, A_{n-1}$ be cellular partial permutation networks on $a_0,\ldots,a_{n-1}$ bits respectively. Let $q=a_0\cdot\ldots\cdot a_{n-1}$. Then we define $F(A_0,\ldots,A_{n-1})=$

$$\prod_{i=0}^{n-2} (\tfrac{q}{a_i} A_i\ \sigma(a_{i+1}, \tfrac{q}{a_i a_{i+1}}))\tfrac{q}{a_{n-1}} A_{n-1} \cdot \prod_{i=n-2}^{0} (\sigma(\tfrac{q}{a_{i+1}}, a_{i+1})\tfrac{q}{a_i} A_i^*) .$$

Benes showed that if $A_0,\ldots,A_{n-1}$ are permutation networks, then $F(A_0,\ldots,A_{n-1})$ is a permutation network. We will show later that $F(A_0,\ldots,A_{n-1})$ is equivalent to $A_0 \times\times (A_1 \times\times (\ldots \times\times (A_{n-2} \times\times A_{n-1})\ldots))$ (which generalizes Benes' result).

(x) The truncation method. This method, designed by several authors ([6, 8], etc.), can be used to build permutation networks on m bits when m is of the form rn-k, with $k \in Z_n$, $n > 1$ and $r > 1$.

Indeed, let r and n be integers larger than 1 and let $k \in Z_n$. Let A, A', B and B' be partial permutation networks on n, n-k, r and r-1 bits respectively (a partial permutation network on 1 bit is the simple connection S). Suppose that A is cellular.

Now (A,A',B,B') is defined as follows : Take $A \wedge B$. Replace the first copy of A in the first stage by $kS \cup A'$. Replace the k first copies of B in the second stage by k copies of $S \cup B'$. Then I_i is connected to O_i for $i \in Z_k$. Remove these k inputs, outputs and all interconnections between the

There remains a partial permutation network on rn-k bits, written (A,A',B,B').

We will show later that if A,A',B and B' are permutation networks, then (A,A',B,B') is a permutation network. Note that for k=0, we have $(A,A,B,B')=A \wedge B$.

The constructions (vi), (vii), (viii) and (x) are illustrated on Fig. 5,6,7 and 8 respectively.

Let us now prove the two announced results. We need first the following :

LEMMA 1. If B is a partial permutation network on n bits and if $\pi \in Sym(m)$, then $\pi n.mB.(\pi n)^{-1} \underset{=}{\sim} mB$.

The proof is elementary and is left to the reader.

PROPOSITION 2. Let $A_0,\ldots,A_{n-1}$ be cellular partial permutation networks. Then $F(A_0,\ldots,A_{n-1})$ is equivalent to $A_0 \times\times (A_1 \times\times (\ldots \times\times (A_{n-2} \times\times A_{n-1})\ldots))$.

Proof. We can suppose that each A_i is on a_i bits. Let $q=a_0\ldots a_{n-1}$. Then we can write $F(A_0,\ldots,A_{n-1})$ as :

$$\prod_{i=0}^{n-2} \left(\frac{q}{a_i} A_i \ \beta(i,i+1)\right). \frac{q}{a_{n-1}} A_{n-1} \cdot \prod_{i=n-2}^{0} \left(\beta(i+1,i) \frac{q}{a_i} A_i^*\right) ,$$

where $\beta(i,i+1)=\sigma(a_{i+1}, \frac{q}{a_{i+1}})$ and $\beta(i+1,i)=\beta(i,i+1)^{-1}$.

By induction, we verify that $A_0 \times\times (A_1 \times\times (\ldots \times (A_{n-2} \times A_{n-1})\ldots))$ can be written as :

$$\prod_{i=0}^{n-2} \left(\frac{q}{a_i} A_i . \pi(i,i+1)\right). \frac{q}{a_{n-1}} A_{n-1} \cdot \prod_{i=n-2}^{0} \left(\pi(i+1,i) . \frac{q}{a_i} A_i^*\right) ,$$

where $\pi(i,i+1)=a_0.....a_{i-1}\ \sigma(a_{i+1}.....a_{n-1},a_i)$ and $\pi(i+1,i)=\pi(i,i+1)^{-1}$.

With respect to the basis $[a_{n-1},...,a_0]$, we can write for $i=0,...,n-2$:

$$\pi(i,i+1) = \sigma\begin{pmatrix}0,...,i-1, & n-1, & ....., & i\\ 0,..... , & i, & n-1,..., & i+1\end{pmatrix}$$

and $$\beta(i,i+1) = \sigma\begin{pmatrix}i+1,... ...., & n-1,0, & ..., & i\\ i+2,..., & n-1, & 0, ..., & i+1\end{pmatrix}.$$

For $i=0,...,n-2$, define :

$$\psi(i) = \sigma\begin{pmatrix}0 , ..., & i-1, & n-1, & ..., & i\\ i+1, ..., & n-1, & 0 , ..., & i\end{pmatrix}.$$

Let $\psi(n-1)$ be the identity. Then we can easily check that for $i=0,...,n-2$, we have :

$$\psi(i).\beta(i,i+1) = \pi(i,i+1).\psi(i+1) .$$

Thus we get :

$$\beta(i,i+1) = \psi(i)^{-1}.\pi(i,i+1).\psi(i+1) \text{ and}$$

$$\beta(i+1,i) = \psi(i+1)^{-1}.\pi(i+1,i).\psi(i) .$$

Hence $F(A_0,...,A_{n-1})$

$$= \prod_{i=0}^{n-2} \left(\frac{q}{a_i} A_i.\psi(i)^{-1}\pi(i,i+1)\psi(i+1)\right). \frac{q}{a_{n-1}} A_{n-1} . \prod_{i=n-2}^{2} \left(\psi(i+1)^{-1}\pi(i+1,i)\psi(i).\frac{q}{a_i} A_i^*\right)$$

$$= \psi(0)^{-1} \prod_{i=0}^{n-2} (B_i.\pi(i,i+1)) . B_{n-1}. \prod_{i=n-2}^{0} (\pi(i+1,i).B_i^*) .\psi(0) ,$$

where $B_i=\psi(i).\frac{q}{a_i} A_i\ \psi(i)^{-1}$ for $i \in Z_n$.

Now for $i \in Z_n$, $\psi(i)=\phi(i)a_i$ for some $\phi(i) \in \mathrm{Sym}(\frac{q}{a_i})$.

By Lemma 1, it follows that $B_i \overset{\sim}{=} \frac{q}{a_i} A_i$. Thus $F(A_0,\ldots,A_{n-1})$

$$\overset{\sim}{=} \psi(0)^{-1} \prod_{i=0}^{n-2} \left(\frac{q}{a_i} A_i\ \pi(i,i+1)\right) \frac{q}{a_{n-1}} A_{n-1} \prod_{i=n-2}^{0} \left(\pi(i+1,i) \frac{q}{a_i} A_i^*\right).\psi(0)$$

$$\overset{\sim}{=} \psi(0)^{-1}.\ (A_0 \times\times (A_1 \times\times (\ldots (A_{n-2} \times A_{n-1}) \ldots))).\psi(0).$$

Therefore the proposition follows.

Let us now prove our second announced result:

PROPOSITION 3. Let A,A',B and B' be the permutation networks on n, n-k, r and r-1 bits respectively, where r and n are integers bigger than 1 and $k \in Z_n$. Then (A,A',B,B') is a permutation network.

Proof. Consider $A \wedge B$. It is a permutation network. It can therefore realize all permutations of $\Pi=\{\pi \in \mathrm{Sym}(rn) \mid i\pi=i \text{ for } i \in Z_k\}$. Let $\pi \in \Pi$. If $A \wedge B$ is in a state realizing π, then $I_i(A \wedge B)$ must be connected to $O_i(A \wedge B)$ for $i \in Z_k$. Now $I_i(A \wedge B)$ is connected by $A^{(0)}$ to some $O_j(A^{(0)})$, which is connected to $I_0(B^{(j)})$, where $j \in Z_n$. Now $O_i(A \wedge B)$ is connected to $O_0(B^{(i)})$. As $I_0(B^{(j)})$ must be connected to $O_0(B^{(i)})$, we have i=j. Thus for $i \in Z_k$, $I_i(A \wedge B)=I_i(A^{(0)})$ is connected to $O_i(A^{(0)})$ and $I_0(B^{(i)})$ is connected to $O_0(B^{(i)})$. Thus, if we replace $A^{(0)}$ by $kS \cup A'$ and each $B^{(i)}$ $(i \in Z_k)$ by a copy of $S \cup B'$, then the resulting network realizes Π. If we delete for each $i \in Z_k$ $I_i(A \wedge B)$, $O_i(A \wedge B)$ and the connections between them, then the resulting network, which is (A,A',B,B'), can realize every permutation of Sym(rn-k), and so it is a permutation network.

The following result links the different operations studied up to now. The proof is elementary and is omitted.

PROPOSITION 4. For any partial permutation networks A and B on a and b bits respectively, for all positive integers m and n, we have :

(i) $(A \cup B)^* = A^* \cup B^*$.

(ii) $(mA)^* = m(A^*)$.

(iii) $(Am)^* = (A^*)m$.

(iv) $(A \cdot B)^* = B^* \cdot A^*$ (when a=b) .

(v) $(A \times B)^* = B^* \times A^*$.

(vi) $(A \times\times B)^* = A \times\times B^*$.

(vii) $Am \overset{\sim}{=} \sigma(a,m).\ mA.\ \sigma(m,a)$.

(viii) $m(A.B) = (mA) . (mB)$.

(ix) $(A.B)m = (Am) . (Bm)$.

(x) $m(nA) = (mn)A$.

(xi) $(Am)n = A(mn)$.

(xii) $(mA)n = m(An)$.

Note that in these equalities, one can replace A or B by a permutation.

The following result is due to Pippenger [9] :

PROPOSITION 5. Let A,B and C be partial permutation networks. Then :

(i) $A \times (B \times C) \overset{\sim}{=} (A \times B) \times C$

(ii) If A and B are cellular, then $A \times\times (B \times\times C) \overset{\sim}{=} (A \times B) \times\times C$

Proof. Suppose that A,B and C are on a,b and c bits respectively. Then it is easy to check that :

$(A \times B)\times C = bcA.c\sigma(b,a).acB.\sigma(c,ab).abC.$

$A\times(B \times C) = bcA.\sigma(bc,a).caB.a\sigma(c,b).abC.$

Now $\sigma(bc,a) = c\sigma(b,a).\sigma(c,a)b$ and

$a\sigma(c,b) = (\sigma(c,a)b)^{-1}.\sigma(c,ab).$

By Lemma 1, $caB \overset{\sim}{=} \sigma(c,a)b.acB.(\sigma(c,a)b)^{-1}$ and

so $(A \times B)\times C \overset{\sim}{=} bcA.c\sigma(b,a).(\sigma(c,a)b.acB.(\sigma(c,a)b)^{-1}).\sigma(c,ab).abC$

$= A\times(B \times C)$

Hence (i) follows. Now (ii) is proved in the same way.

§V. The network of Waksman and Green and Joel's nested tree.

These cellular permutation networks use 2-cells. For any positive integer n, Waksman's network $W(2^n)$ and Joel's nested tree $T(2^n)$ are cellular permutation networks on 2^n bits. For any integer $m \geqslant 2$, Green defined a cellular permutation network G(m) on m bits ; for $m=2^n$, we have $G(m)=W(m)$.

We will show that $T(2^n)$ is quasi equivalent to the dual of $W(2^n)$.

A. The network of Waksman-Green.

Waksman's network $W(2^n)$ $(n=1,2,3,\ldots)$ is defined inductively as follows :

- $W(2)=P(2)$, where P(2) is the elementary 2-cell
- For $n=2,3,4,\ldots$, set $W(2^n)=P(2) \wedge W(2^{n-1})$.

Green's network G(m) (m=2,3,...) is defined inductively as follows :

- $G(2) = P(2)$

- For $m > 2$, set : $G(m) = P(2) \wedge G(\frac{m}{2})$ if is even.

  : $G(m) = (P(2), S, G(\frac{m+1}{2}), G(\frac{m-1}{2}))$ if m is odd.

(Here S is the simple connection on 1 bit).

It is easily seen that for $m=2^n$, $G(m)=W(m)$.

Remark. G(m) has an inductive control algorithm, called "looping" (see [8,13]).

B. Joel's nested tree [7] .

Let P(2) be the elementary 2-cell. Define $Y(2)=P(2)$ and $Y(2^k)=Y(2^{k-1})\times P(2)$ for k=2,3,4,...

Joel builds the nested tree $T(2^k)$ ($k > 1$) as follows :

. For n=1,...,k, take a copy of $Y(2^n)$

. Take 2^k inputs $I_0,\ldots,I_{2^k-1}$ and 2^k outputs $O_0,\ldots,O_{2^k-1}$.

. Make the following connections :

(1°) For n=1,...,k-1 and $m \in Z_{2^{n-1}}$ connect

$I_{2^{k-n}(2m+1)-1}$ with $I_{2m}(Y(2^n))$.

$I_{2^{k-n}(2m+1)}$ with $I_{2m+1}(Y(2^n))$.

$O_{2m}(Y(2^n))$ with $I_{2^{k-n}(2m+1)-1}(Y(2^k))$.

$O_{2m+1}(Y(2^n))$ with $I_{2^{k-n}(2m+1)}(Y(2^k))$.

(2°) Connect : I_0 with $I_0(Y(2^k))$

$I_{2^{k-1}}$ with $I_{2^{k-1}}(Y(2^k))$

and $O_j(Y(2^k))$ with O_j for every $j \in Z_{2^k}$. (12)

This construction is illustrated in Fig. 9 for k=4.

Joel's nested tree $T(2^k)$ is not equivalent to the dual $W(2^k)^*$ of Waksman's network. This can be seen in Fig. 10 for k=2. Indeed, if all the cells are put in the 0-state, then two outputs (in both T(4) and $W(4)^*$) are reached after two stages. But in T(4), these two outputs are not connected to the same cell, while in $W(4)^*$ they are.

In fact, we can prove the following :

PROPOSITION 6. For any $k \geq 2$, $T(2^k) \sim W(2^k)^*$.

The proof of this result is long and intricate. It can be found in the appendix.

The idea is to use induction on k. Define T(2)=P(2). We replace $T(2^k)$ (k=1,2,...) by $T'(2^k)$, which is built as follows :

-$T'(2)=T(2)$

-For $k > 1$, we replace $Y(2^n)$

(n=1,...,k-1) by $Z(2^n)=Y(2^n)^*$ in the design of $T(2^k)$.

As $Z(2^n)$ is isomorphic to $Y(2^n)$, $T'(2^k)$ is isomorphic to $T(2^k)$.

Now for $k > 1$ $T'(2^k)$ has a first stage of $2^{k-1}-1$ 2-cells and a last stage of 2^{k-1} 2-cells. If one deletes these two stages, then one gets two copies of $T'(2^{k-1})$.

By induction hypothesis, $T'(2^{k-1}) \sim W(2^{k-1})^+$, and we extend this to : $T'(2^k) \sim W(2^k)^*$. Indeed, $W(2^k)^*$ has also a first stage of $2^{k-1}-1$ 2-cells and a last stage of 2^{k-1} 2-cells ; if one deletes these two stages, then one also gets two copies of $W(2^{k-1})^*$.

It follows that the looping algorithm can be applied for the control of $T'(2^k)$.

Conclusion. The operations that we have defined in §IV can successfully handle binary cellular permutation networks such as the networks of Benes, Waksman and Green, and Joel's nested tree. In particular, the algebraic formalism that we introduce allows us to prove equivalence properties between different networks, especially between Green's network and Joel's nested tree.

Appendix. Proof of Proposition 6.

Let us define $T(2)=P(2)$. Then clearly $T(2)=W(2)^*$. Define $Z(2)=P(2)$ and $Z(2^k)=P(2)\times Z(2^{k-1})$ for $k=2,3,4,\ldots$ Then $Z(2^k)\overset{\sim}{=}Y(2^k)$ for any $k \geq 1$ by Proposition 5(i). Thus we can replace $T(2^k)$ $(k \geq 1)$ by $T'(2^k)$, which is built as follows :

- $T'(2)=T(2)$
- If $k > 1$, then for $n=1,\ldots,k-1$, replace $Y(2^n)$ by $Z(2^n)$ in the construction of $T(2^k)$.

Now clearly $T'(2^k)\overset{\sim}{=}T(2^k)$. The rest of the proof consists of 8 steps :

Step 1. The following eight maps are permutations of Z_{2^k} :

(1) $\alpha(k) = (0,2^k-1)$ $\qquad (k=1,2,3,\ldots)$

(2) $\beta(k) = 2\alpha(k-1)=(0,2^{k-1}-1)(2^{k-1},2^k-1)$ $\qquad (k=2,3,4,\ldots)$

(3) $\delta(k) = (1,2)\ldots(2^k-3,2^k-2)$ $\qquad (k=2,3,4,\ldots)$

(4) $\varepsilon(k) = (0,1)\ldots(2^k-2,2^k-1)$ $\qquad (k=1,2,3,\ldots)$

(5) $\tau(k) : x \to x \oplus 2^{k-1} \pmod{2^k}$ $\quad (k=1,2,3,\ldots)$.

(6) $\pi(k)$ fixes $0, 2^{k-1}-1, 2^{k-1}, 2^k-1$ and for $n=2, \ldots, k-1$ (if $k \geq 3$) and $v \in Z_{2^{n-2}}$, $\pi(k)$ maps

$$2^{k-n}(4v+1)-1 \quad \text{on} \quad 2^{k-n}(2v+1)-1 ,$$

$$2^{k-n}(4v+3)-1 \quad \text{on} \quad 2^{k-n}(2v+1) ,$$

$$2^{k-n}(4v+1) \quad \text{on} \quad 2^{k-1}+2^{k-n}(2v+1)-1$$

and $$2^{k-n}(4v+3) \quad \text{on} \quad 2^{k-1}+2^{k-n}(2v+1) \qquad (k=2,3,4,\ldots) .$$

(7) $\rho(k)$ maps 0 on 0, 2^k-1 on 1, and for $n=1,\ldots,k-1$ and $m \in Z_{2^{n-1}}$ (if $k \geq 2$), $\rho(k)$ maps :

$$2^{k-n}(2m+1)-1 \quad \text{on} \quad 2^n+2m$$

and $$2^{k-n}(2m+1) \quad \text{on} \quad 2^n+2m+1 \qquad (k=1,2,3,\ldots)$$

(8) $\gamma(k) = \rho(k-1) \cup (\alpha(k-1).\rho(k-1)) \qquad (k=2,3,4,\ldots)$

It can be checked that $\gamma(k)$ maps 0 on 0, $2^{k-1}-1$ on 1, 2^{k-1} on $2^{k-1}+1$, 2^k-1 on 2^{k-1} and for $u=2,\ldots,k-1$ and $m \in Z_{2^{u-2}}$ (if $k \geq 3$), it maps :

$$2^{k-u}(2m+1)-1 \quad \text{on} \quad 2^{u-1}+2m ,$$

$$2^{k-u}(2m+1) \quad \text{on} \quad 2^{u-1}+2m+1 ,$$

$$2^{k-1}+2^{k-u}(2m+1)-1 \quad \text{on} \quad 2^{k-1}+2^{u-1}+2m$$

and $$2^{k-1}+2^{k-u}(2m+1) \quad \text{on} \quad 2^{k-1}+2^{u-1}+2m+1 \qquad (k=2,3,4,\ldots)$$

<u>Step 2.</u> If $k \geq 2$ and if $x \in Z_{2^k} \setminus \{0, 2^{k-1}-1, 2^{k-1}, 2^k-1\}$, then $x\delta(k)\,\pi(k) = x\pi(k)\,\tau(k)$.

Indeed $\{x, x\delta(k)\}$ is a pair of the form $\{2m-1, 2m\}$.

Now it is easily checked that $\pi(k)$ maps such a pair on a pair $\{n, n+2^{k-1}\} = \{n, n\tau(k)\}$, where $n \in Z_{2^{k-1}}$. As $\delta(k) = \delta(k)^{-1}$ and $\tau(k) = \tau(k)^{-1}$, the result follows.

Step 3. If $k \geq 2$, then $\tau(k)\,\sigma(2, 2^{k-1}) = \sigma(2, 2^{k-1})\varepsilon(k)$.

This is due to the fact that if $m \in Z_{2^{k-1}}$, then $\sigma(2, 2^{k-1})$ maps m on $2m$ and $m+2^{k-1}$ on $2m+1$, and that $\tau(k)$ permutes the pairs $\{m, m+2^{k-1}\}$, while $\varepsilon(k)$ permutes the pairs $\{2m, 2m+1\}$

Step 4. If $k \geq 2$, then $\alpha(k)\delta(k)\pi(k) = \pi(k)\tau(k)\beta(k)$.

Proof. Clearly, both $\pi(k)$ and $\tau(k)$ preserve the set $\{0, 2^{k-1}, 2^{k-1}, 2^k-1\}$. It follows that if $x \in Z_{2^k} \setminus \{0, 2^{k-1}-1, 2^{k-1}, 2^k-1\}$, then $x\pi(k)\tau(k) \neq 0, 2^{k-1}, 2^{k-1}-1, 2^k-1$. Thus $x\pi(k)\tau(k)\beta(k) = x\pi(k)\tau(k)$

$= x\delta(k)\pi(k)$ (by Step 2)

$= x\alpha(k)\delta(k)\pi(k)$ since $\alpha(k)$ fixes x.

Now we check that :

$0\alpha(k)\delta(k)\pi(k) = (2^k-1)\delta(k)\pi(k) = (2^k-1)\pi(k) = 2^k-1$

$= 2^{k-1}\,\beta(k) = 0\tau(k)\beta(k) = 0\pi(k)\tau(k)\beta(k)$.

$(2^{k-1}-1)\alpha(k)\delta(k)\pi(k) = (2^{k-1}-1)\delta(k)\pi(k) = 2^{k-1}\pi(k) = 2^{k-1}$

$= (2^k-1)\beta(k) = (2^{k-1}-1)\tau(k)\beta(k) = (2^{k-1}-1)\pi(k)\tau(k)\beta(k)$.

$2^{k-1}\alpha(k)\delta(k)\pi(k) = 2^{k-1}\delta(k)\pi(k) = (2^{k-1}-1)\pi(k) = 2^{k-1}-1$

$= 0\beta(k) = 2^{k-1}\tau(k)\beta(k) = 2^{k-1}\pi(k)\tau(k)\beta(k)$.

$(2^k-1)\alpha(k)\delta(k)\pi(k) = 0\delta(k)\pi(k) = 0\pi(k) = 0$

$= (2^{k-1}-1)\beta(k) = (2^k-1)\tau(k)\beta(k) = (2^k-1)\pi(k)\tau(k)\beta(k)$.

Step 5. If $k \geqslant 2$, then $\pi(k)\gamma(k)=\rho(k)\sigma(2^{k-1},2)$.

Proof. If $m \in Z_{2^{k-1}}$, then $\sigma(2^{k-1},2)$ maps $2m$ on m and $2m+1$ on $m+2^{k-1}$.
Now we check that :

$0\pi(k)\gamma(k) = 0\gamma(k) = 0$,

$(2^{k-1}-1)\pi(k)\gamma(k) = (2^{k-1}-1)\gamma(k) = 1$,

$2^{k-1}\pi(k)\gamma(k) = 2^{k-1}\gamma(k) = 2^{k-1}+1$,

$(2^{k}-1)\pi(k)\gamma(k) = (2^{k}-1)\gamma(k) = 2^{k-1}$,

and for $n=2,\ldots,k-1$ and $v \in Z_{2^{n-2}}$ if $(k \geqslant 3)$, we have :

$(2^{k-n}(4v+1)-1)\pi(k)\gamma(k) = (2^{k-n}(2v+1)-1)\gamma(k) = 2^{n-1}+2v$,

$(2^{k-n}(4v+3)-1)\pi(k)\gamma(k) = (2^{k-n}(2v+1))\gamma(k) = 2^{n-1}+2v+1$,

$(2^{k-n}(4v+1))\pi(k)\gamma(k) = (2^{k-1}+2^{k-n}(2v+1)-1)\gamma(k) = 2^{k-1}+2^{n-1}+2v$,

$(2^{k-n}(4v+3))\pi(k)\gamma(k) = (2^{k-1}+2^{k-n}(2v+1))\gamma(k) = 2^{k-1}+2^{n-1}+2v+1$.

Thus $\pi(k)\gamma(k)$ is known. Then we check that :

$0\rho(k)\sigma(2^{k-1},2) = 0\sigma(2^{k-1},2) = 0$,

$(2^{k-1}-1)\rho(k)\sigma(2^{k-1},2) = 2\sigma(2^{k-1},2) = 1$,

$2^{k-1}\rho(k)\sigma(2^{k-1},2) = 3\sigma(2^{k-1},2) = 2^{k-1}+1$,

$(2^{k}-1)\rho(k)\sigma(2^{k-1},2) = 1\sigma(2^{k-1},2) = 2^{k-1}$,

and for $n=2,\ldots,k-1$ and $v \in Z_{2^{u-2}}$ (if $k \geqslant 3$), we have :

$(2^{k-n}(4v+1)-1)\rho(k)\sigma(2^{k-1},2) = (2^{n}+4v)\sigma(2^{k-1},2) = 2^{n-1}+2v$,

$(2^{k-n}(4v+3)-1)\rho(k)\sigma(2^{k-1},2) = (2^{n}+4v+2)\sigma(2^{k-1},2) = 2^{n-1}+2v+1$,

$(2^{k-n}(4v+1))\rho(k)\sigma(2^{k-1},2) = (2^{n}+4v+1)\sigma(2^{k-1},2) = 2^{k-1}+2^{n-1}+2v$,

$(2^{k-n}(4v+3))\rho(k)\sigma(2^{k-1},2)=(2^{n}+4v+3)\sigma(2^{k-1},2)= 2^{k-1}+2^{n-1}+2v+1$.

We see then that $\pi(k)\gamma(k) =\rho(k)\sigma(2^{k-1},2)$.

Step 6. For $k \geq 2$, define $R_2(k)=2^{k-1}\ P(2)$ and $R_1(k) = S \cup ((2^{k-1}-1)P(2)) \cup S$. Then we have the following :

$$T'(2^k) = R_1(k).\pi(k).(2T'(2^{k-1})).\sigma(2,2^{k-1}).R_2(k).$$

Proof. Delete the last stage of copies of P(2) in $Y(2^k)$. Then there remains two copies of $Y(2^{k-1})$. For $n=1,\ldots,k-1$, delete the first stage of copies of P(2) in $Z(2^n)$. Then there remains two copies of $Z(2^{n-1})$ if $n \geq 2$ and 2 copies of S if $n=1$. Now, by definition of $T'(2^k)$, it is easily seen that the copies of $Z(2^{n-1})$ $(n=2,\ldots,k-1)$ and $Y(2^{k-1})$ form together two copies of $T'(2^{k-1})$. Clearly, the first stage of copies of P(2) which has been deleted is equal to $R_1(k)$, while the last one is equal to $R_2(k)$. Thus :

$$T'(2^k) = R_1(k)\ .\pi.(2T'(2^{k-1})).\sigma.R_2(k)\ ,$$

where σ is the interconnection permutation in the last stage of $Z(2^k)$ and π is the interconnection permutation linking the first stage of copies of P(2) to the two copies of $T'(2^{k-1})$. Now $Z(2^k)=Z(2^{k-1})\times P(2)=Z(2^{k-1}).\sigma(2,2^{k-1}).R_2(k)$ by definition of the product $\times$. Thus $\sigma=\sigma(2,2^{k-1})$.

Let us now look at π. Clearly π fixes 0 and 2^{k-1}. Now $2^{k-1}-1$ and 2^{k-1} are also fixed by π, since $I_{2^{k-1}-1}$ and $I_{2^{k-1}}$ are connected to Z(2). If $x \in Z_{2^k} \setminus \{0, 2^k-1, 2^{k-1}-1, 2^{k-1}\}$, then I_x is connected to some $I_u(Z(2^n))$, and $I_{x\pi}$ is connected to $I_{u\sigma(2^{n-1},2)}(Z(2^n))$, because $\sigma(2^{n-1},2)$ is the interconnection permutation between the first stage of copies of P(2) and the two copies of $Z(2^{n-1})$ in $Z(2^n)$. Thus we get the following for $n=2,\ldots,k-1$ and $v \in Z_{2^{n-2}}$:

$$x \to u \to u\sigma(2^{n-1},2) \to x\pi$$

$$2^{k-n}(4v+1)-1 \to 4v \to 2v \to 2^{k-n}(2v+1)-1$$

$$2^{k-n}(4v+3)-1 \to 4v+2 \to 2v+1 \to 2^{k-n}(2v+1)$$

$$2^{k-n}(4v+1) \to 4v+1 \to 2v+2^{n-1} \to 2^{k-n}(2v+2^{n-1}+1)-1$$

$$2^{k-n}(4v+3) \to 4v+3 \to 2v+1+2^{n-1} \to 2^{k-n}(2v+2^{n-1}+1) .$$

Thus $\pi=\pi(k)$ and the result follows.

Note : Step 6 is illustrated in Fig. 11.

Step 7. For any $k \geqslant 1$, $T'(2^k) \approx \alpha(k)\ T'(2^k)$

Proof. We use induction on k. The result is obviously true for k=1.

Suppose that $k > 1$ and that the result is true for k-1. By Step 6, we have :

$$T'(2^k)=R_1(k).\pi(k).(2T'(2^{k-1})).\sigma(2,2^{k-1}).R_2(k)$$
$$\tilde{=}R_1(k).\pi(k).\tau(k).(2T'(2^{k-1})).\tau(k).\sigma(2,2^{k-1}).R_2(k)$$

by Lemma 1, since $\tau(k)=\tau(1).2^{k-1}$. By Step 3, we get :

$$T'(2^k)\tilde{=} R_1(k).\pi(k).\tau(k).(2T'(2^{k-1})).\sigma(2,2^{k-1}).(\varepsilon(k).R_2(k))$$
$$\approx R_1(k).\pi(k)\tau(k).(2T'(2^{k-1})).\sigma(2,2^{k-1}).R_2(k)$$
$$\approx \alpha(k).R_1(k).\alpha(k)^{-1}.\pi(k).\tau(k).(2T'(2^{k-1})).\sigma(2,2^{k-1}).R_2(k)$$

since $R_1(k)$ does not act on 0 and 2^k-1. Using induction hypothesis, we have $T'(2^{k-1})\approx\alpha(k-1).T'(2^{k-1})$ and so $2T'(2^{k-1})\approx 2(\alpha(k-1).T'(2^{k-1}))\tilde{\approx}(2\alpha(k-1)).(2T'(2^{k-1}))\tilde{\approx}\beta(k).(2T'(2^{k-1}))$ by Proposition 4(viii). Thus :

$$T'(2^k) \tilde{\approx} \alpha(k).R_1(k).\alpha(k)^{-1}.\pi(k).\tau(k).\beta(k).(2T'(2^{k-1})).\sigma(2,2^{k-1}).R_2(k)$$
$$\approx \alpha(k).R_1(k).\alpha(k)^{-1}.\alpha(k).\delta(k).\pi(k).(2T'(2^{k-1})).\sigma(2,2^{k-1}).R_2(k)$$
$$\tilde{\approx} \alpha(k).(R_1(k).\delta(k)).\pi(k).(2T'(2^{k-1})).\sigma(2,2^{k-1}).R_2(k)$$

by Step 4. Hence :

$$T'(2^k) \approx \alpha(k).R_1(k).\pi(k).(2T'(2^{k-1})).\sigma(2,2^{k-1}).R_2(k)$$

$$\approx \alpha(k)\ T'(2^k)$$

and the result follows.

Step 8. For any $k \geq 1$, $T'(2^k) \approx \rho(k).W(2^k)^*$.

Proof. We use induction on k. The result is true for k=1. Suppose that $k > 1$ and that the result if true for k-1. Then we have :

$T'(2^{k-1}) \approx \rho(k-1).W(2^{k-1})^*$ and

$T'(2^{k-1}) \approx \alpha(k-1).T'(2^{k-1}) \approx \alpha(k-1).\rho(k-1).W(2^{k-1})^*$

by Step 7. It follows that :

$$2T'(2^{k-1}) = T'(2^{k-1}) \cup T'(2^{k-1})$$

$$\approx (\rho(k-1).W(2^{k-1})^*) \cup (\alpha(k-1).\rho(k-1).W(2^{k-1})^*).$$

$$\approx (\rho(k-1) \cup (\alpha(k-1)\rho(k-1))).(2W(2^{k-1})^*).$$

$$\approx \gamma(k).(2W(2^{k-1})^*)$$

Using Step 6, we get :

$$T'(2^k) \approx R_1(k).\pi(k).\gamma(k).(2W(2^{k-1})^*).\sigma(2,2^{k-1}).R_2(k).$$

$$\approx R_1(k).\rho(k).\sigma(2^{k-1},2).(2W(2^{k-1})^*).\sigma(2,2^{k-1}).R_2(k)$$

by Step 5.

Now let $R_0(k)=2S \cup ((2^{k-1}-1)(P(2))$. Then

$R_1(k) \cong \rho(k).R_0(k).\rho(k)^{-1}$ and so we get :

$$T'(2^k) \approx \rho(k).R_0(k).\rho(k)^{-1}.\rho(k).\sigma(2^{k-1},2).(2W(2^{k-1})^*).\sigma(2,2^{k-1}).R_2(k)$$

$$\approx \rho(k).R_0(k).\sigma(2^{k-1},2).(2W(2^{k-1})^*).\sigma(2,2^{k-1}).R_2(k)$$

$$\approx \rho(k).W(2^k)^*.$$

It follows then that $T(2^k) \sim W(2^k)^*$.

Remark. From Step 6 it follows that the "looping" algorithm used for the control of Waksman's network [13] can also be used for the control of $T'(2^k)$.

It could perhaps be possible to design nested trees on n^k bits with copies of the n-cell P(n). Then the result might be quasiequivalent to $P(n) \wedge (P(n) \wedge (\ldots \wedge (P(n) \wedge P(n)) \ldots))$.

References.

[1] V. E. Benes : Permutation Groups, Complexes, and Rearrangeable Connecting Networks. B.S.T.J., Vol. 43, pp. 1619-1640, 1964.

[2] V. E. Benes : Mathematical Theory of Connecting Networks and Telephone Traffic. Academic Press, N. Y., 1965.

[3] M. Davio : Kronecker Products and Shuffle Algebra. IEEE Trans. Computers, Vol. C-30 n°2, pp.116-125 [1981] .

[4] A. M. Duguid : Structural properties of switching networks, Brown Univ. Progr. Rep. BTL-7, 1959.

[5] L. J. Goldstein, S. W. Leibholz : On the Synthesis of Signal Switching Networks with Transient Blocking. IEEE Trans. on Elec. Comp., Vol. C-16, N°5, pp. 637-641, 1967.

[6] M. W. Green, unpublished manuscript.

[7] A. E. Joel, Jr. : On Permutation Switching Networks. B. S. T. J. Vol. 47, pp. 813-822, 1968.

[8] D. C. Opferman, N. T. Tsao-Wu : On a class of rearrangeable switching networks. BSTJ Vol. 50, pp. 1579-1600, 1971.

[9] N. Pippenger : On rearrangeable and non-blocking networks . J. of Comput. & Syst. Sciences 17, pp. 145-162, 1978.

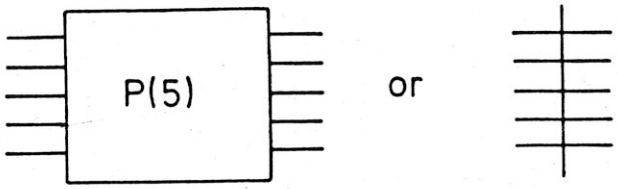
[10] C. Ronse : A Generalization of the Perfect Shuffle. Report R413, MBLE Research Laboratory, December 1979. To appear in Discrete Applied Mathematics.

[11] C. Ronse : Cellular Permutation Networks : A Survey . Report R415, MBLE Research Laboratory, December 1979.

[12] S. Slepian : Two theorems on a particular crossbar switching network. Unpublished manuscript, 1952.

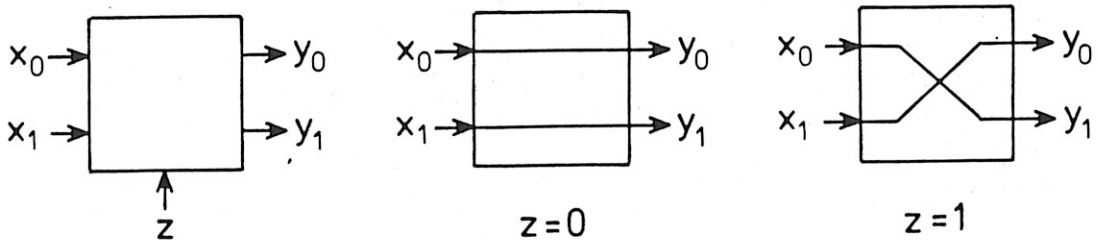
[13] A. Waksman : A permutation network. J. Assoc. Comput. Mach., Vol. 15, n°1, pp. 159-163, 1968.

(a)



A 5 - cell

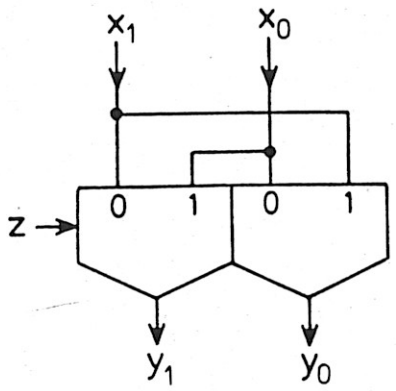
(b)



A2 - cell and its 2 states

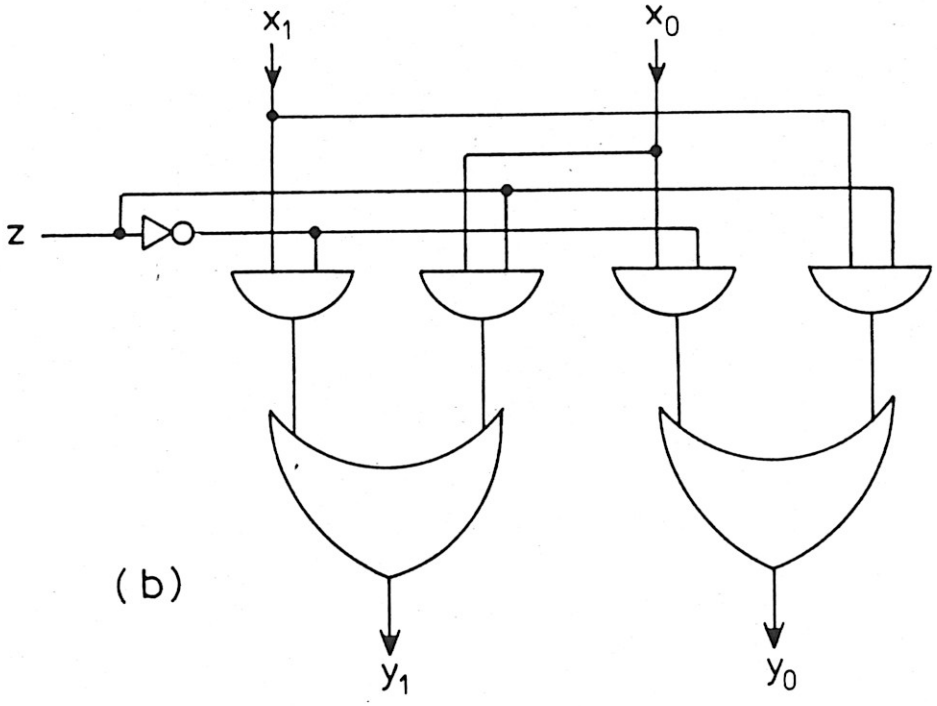
FIG. 1

(a)



Design of a 2-cell using multiplexers

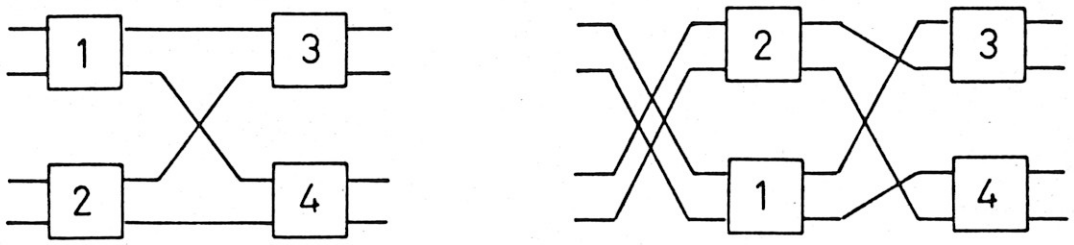
(b)



Design of a 2-cell using logical gates.

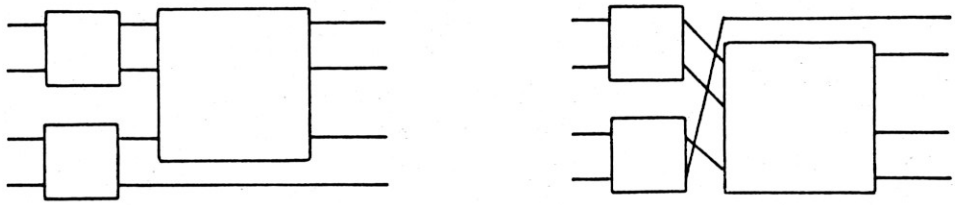
FIG. 2

(a)



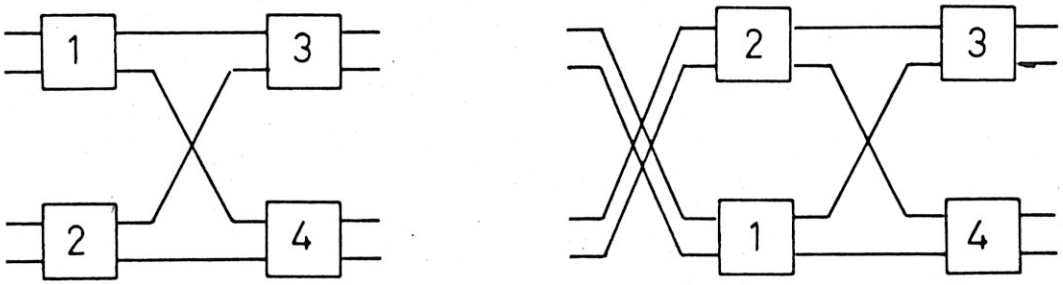
Two isomorphic networks

(b)



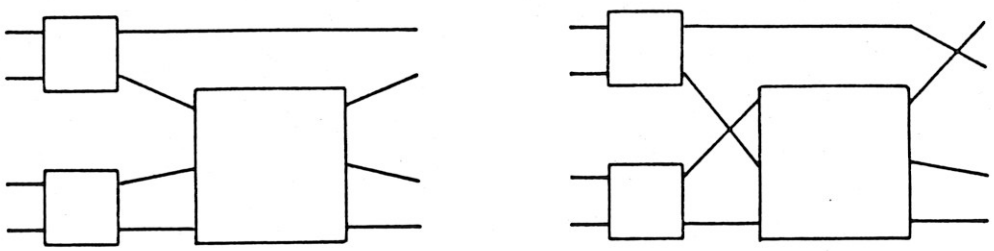
Two equivalent networks

(c)



Two quasiisomorphic networks

(d)



Two quasiequivalent networks

FIG. 3

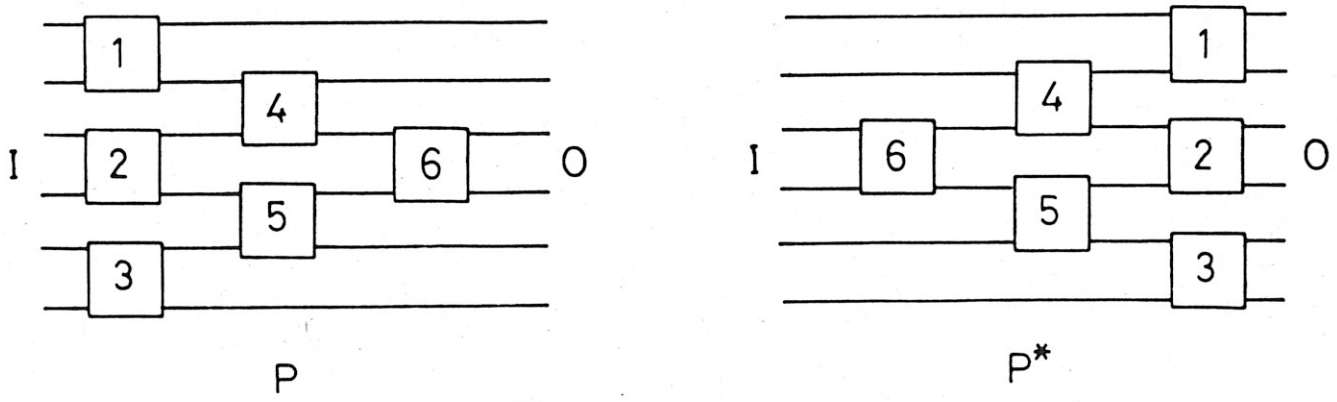


FIG. 4 A network and its dual

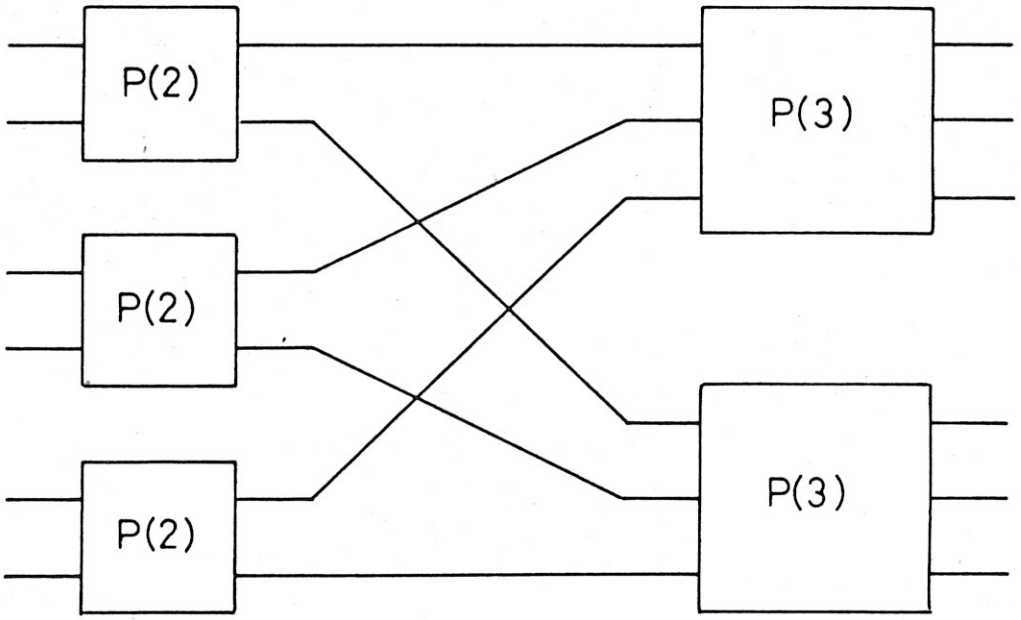


FIG. 5 P(2) x P(3)

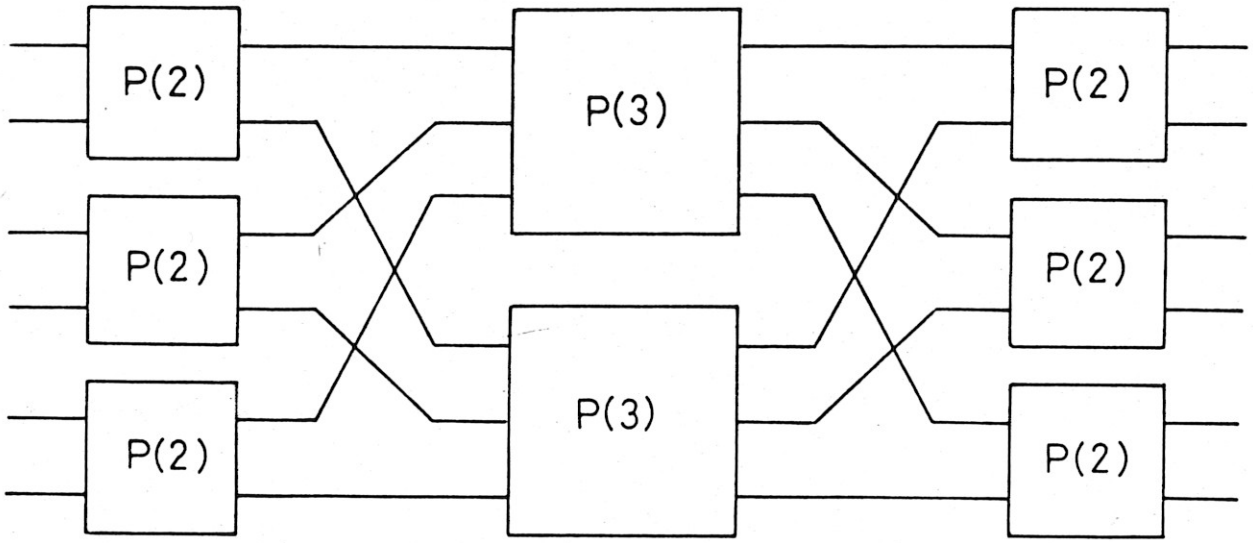


FIG. 6 P(2) xx P(3)

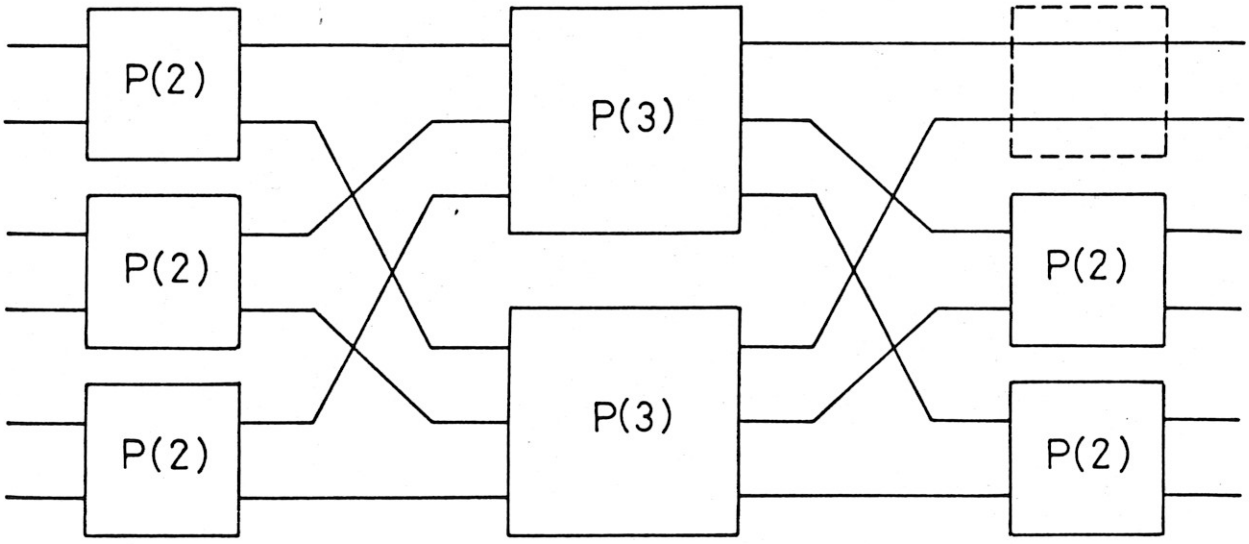


FIG. 7 P(2) ∧ P(3)

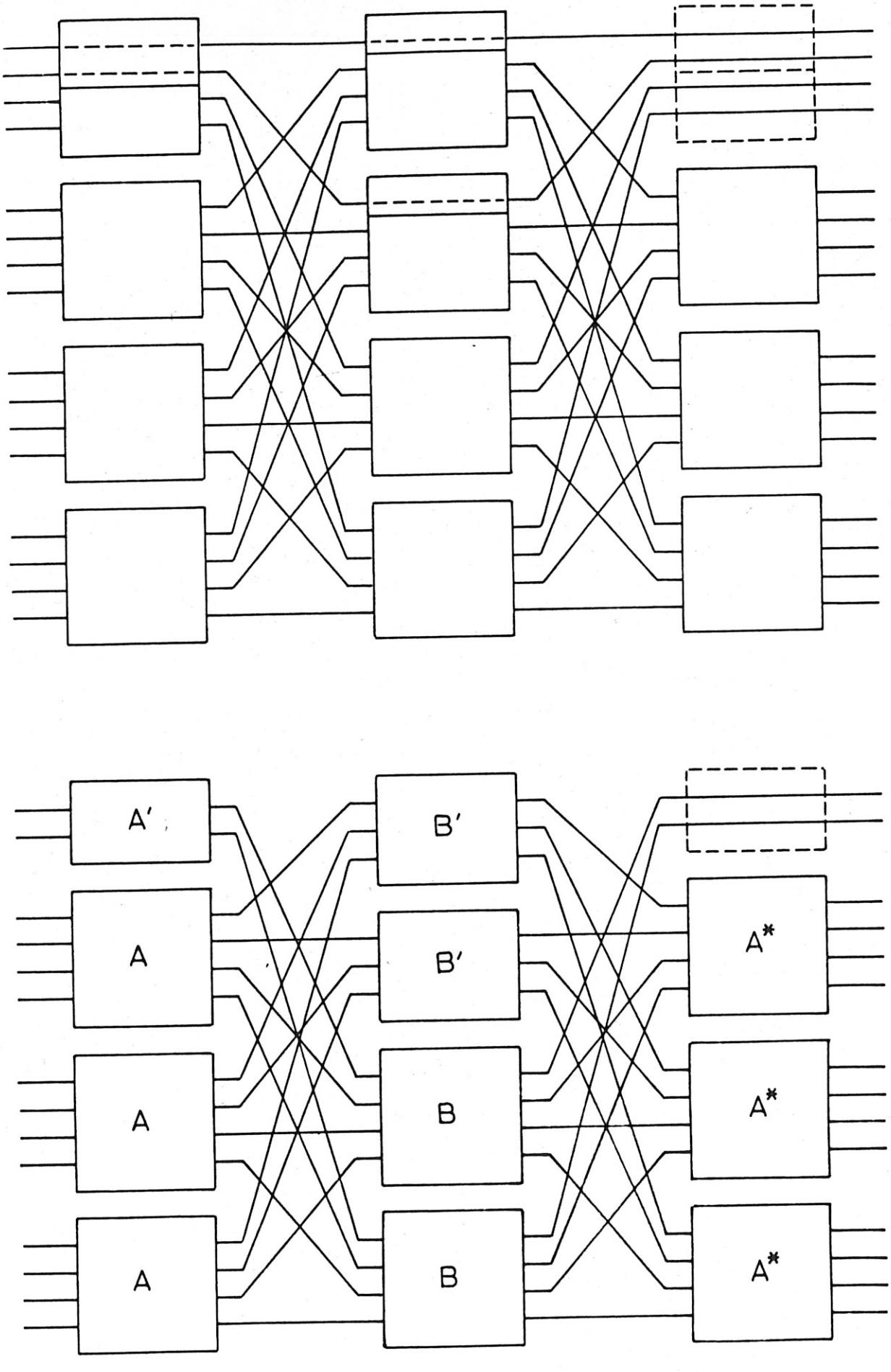


FIG. 8 (A, A', B, B') from $A \wedge B$

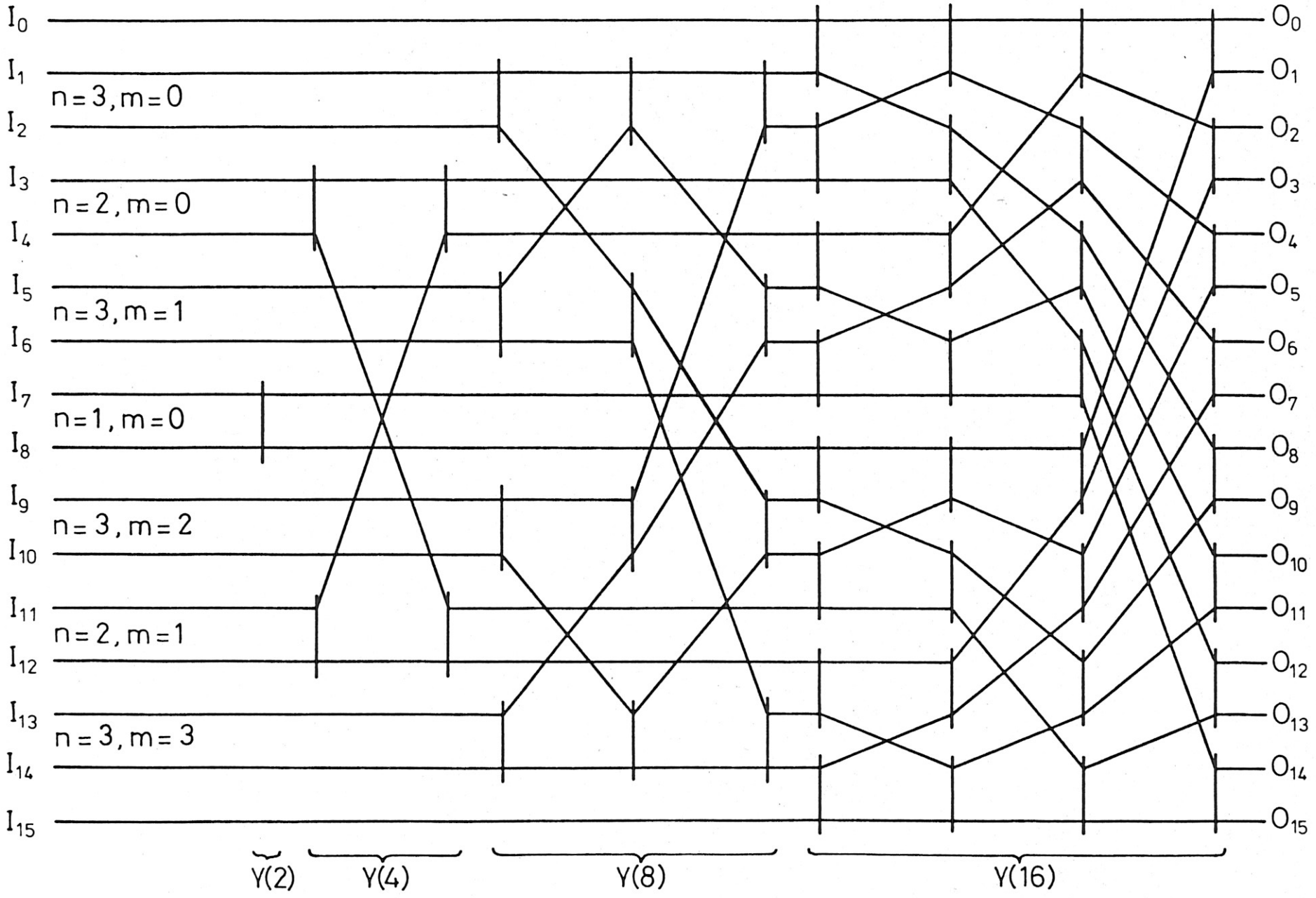

I0
I1
I2
I3
I4
I5
I6
I7
I8
I9
I10
I11
I12
I13
I14
I15
n = 3, m = 0
n = 2, m = 0
n = 3, m = 1
n = 1, m = 0
n = 3, m = 2
n = 2, m = 1
n = 3, m = 3
O0
O1
O2
O3
O4
O5
O6
O7
O8
O9
O10
O11
O12
O13
O14
O15
Y(2)
Y(4)
Y(8)
Y(16)

FIG. 9 T(16)

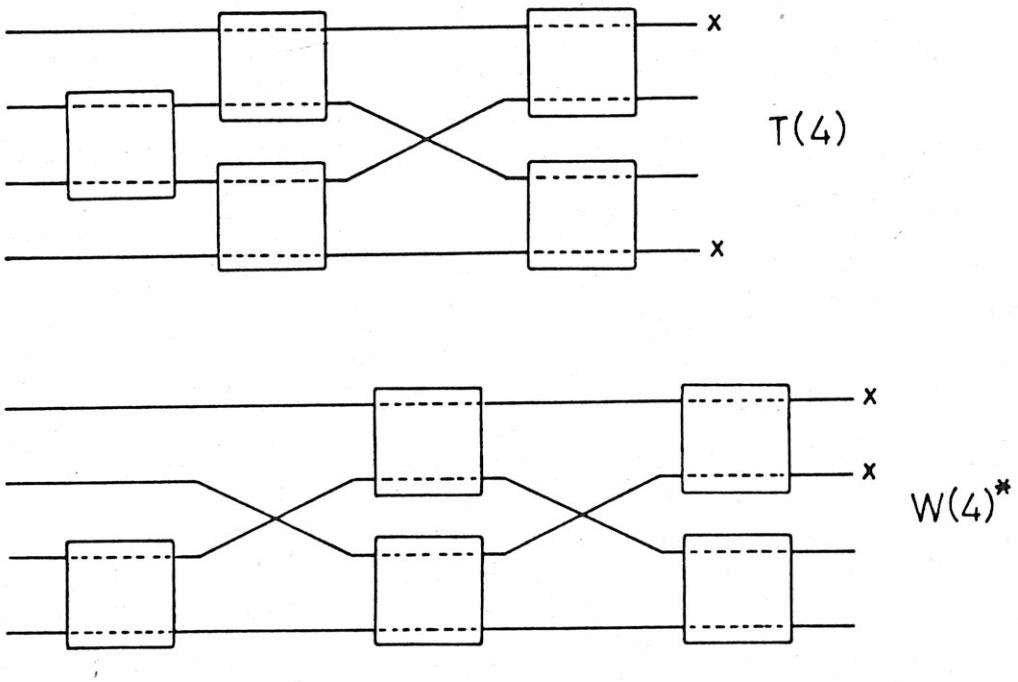


FIG. 10

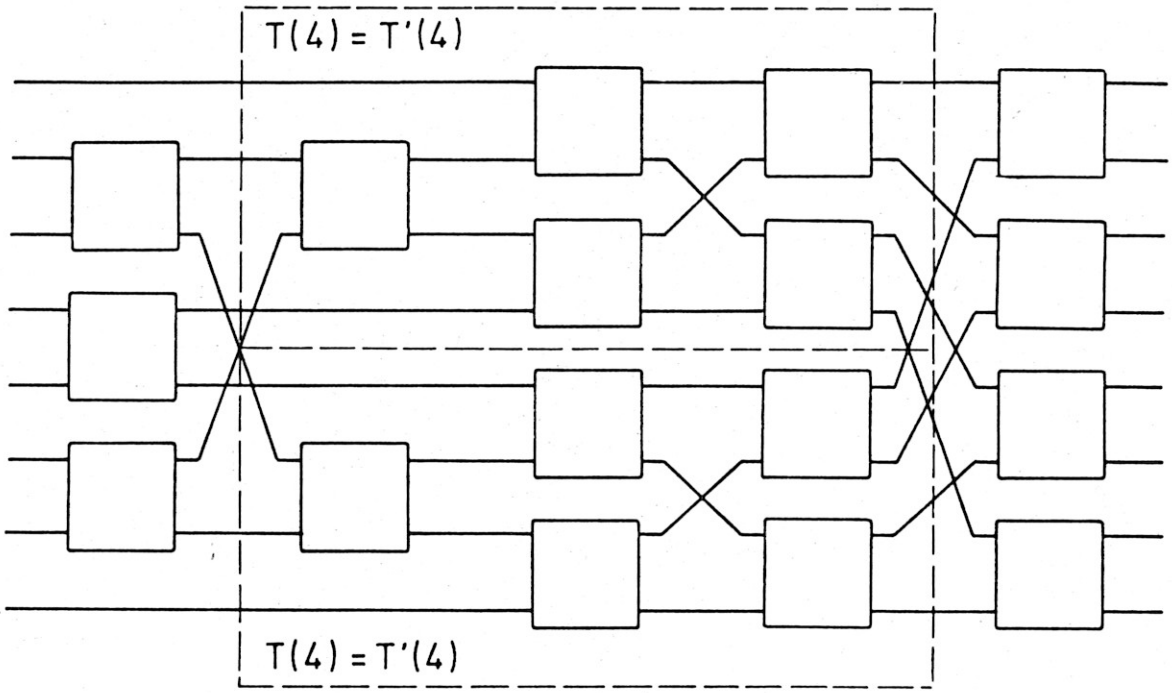


FIG. 11 T(8) = T'(8)