Verification of an Algorithm for Log-time Sorting by Square Comparison

J.C. Mulder
Programming Research Group, University of Amsterdam
P.O. Box 41882, 1009 DB Amsterdam, The Netherlands

W.P. Weijland
Centre for Mathematics and Computer Science
P.O. Box 4079, 1009 AB Amsterdam, The Netherlands

In this paper a concurrent sorting algorithm called RANKSORT is presented, able to sort an input sequence of length n in $\log n$ time, using n^2 processors. The algorithm is formally specified as a *delay-insensitive* circuit. Then, a formal correctness proof is given, using bisimulation semantics in the language ACP_τ. The algorithm has area-time$^2 = O(n^2 \log^4 n)$ complexity which is slightly sub-optimal with respect to the lower bound of $\mathrm{AT}^2 = \Omega(n^2 \log n)$.

1. INTRODUCTION

Many authors have studied the concurrency aspects of sorting, and indeed the n-time *bubblesort* algorithm (using n processors) is rather thoroughly analyzed already (e.g. see: Hennessy [3], Kossen and Weijland [4]). However, *bubblesort* is not the most efficient sorting algorithm in sequential programming, since it is n^2-time and for instance *heapsort* and *mergesort* are $n \log n$-time sorting algorithms. So, the natural question arises whether it would be possible to design an algorithm using even less than n-time.

In this paper we discuss a concurrent algorithm, capable of sorting n numbers in $O(\log n)$ time. This algorithm is based on the idea of *square comparison*: putting all numbers to be sorted in a square matrix, all comparisons can be made in $O(1)$ time, using n^2 processors (one for each cell of the matrix). Then, the algorithm only needs to evaluate the result of this operation.

The algorithm presented here, which is called RANKSORT, is not the only concurrent time-efficient sorting algorithm. Several *sub* n-time algorithms have been developed by others (see: Thompson [5]). For instance algorithms were presented of time-complexity $\sqrt{n}$, $\log^3 n$, $\log^2 n$ and $\log n$. Indeed, the square

Partial support received from the European Community under ESPRIT project no. 432, An Integrated Formal Approach to Industrial Software Development (METEOR).

comparison algorithm presented here, appeared in [5] as well. Its network has been given various names, like *mesh of trees* or *orthogonal tree network.*

In this paper we will show how a $\log n$-sorter can be constructed. Moreover we will present a formal specification of the algorithm and prove it correct using bisimulation semantics with asynchronous cooperation.

At this place we want to thank Niek van Diepen (University of Nijmegen) and Karl Meinke (University of Leeds) for their contributions to this paper. Moreover we thank Jaap Jan de Bruin for his assistance concerning the illustrations which were made on an Apple Macintosh. Finally, we thank Jos Baeten for his remarks on the early drafts of this paper.

2. Sorting by square comparison

Suppose we have a sequence $\langle a_0, a_1, a_2, \ldots, a_{n-1} \rangle$ of distinct numbers, for some $n>0$, and consider the problem of computing a non-decreasing permutation of this sequence. Note that, in fact, we can start from an arbitrary set of symbols and any linear ordering $>$, defined on this finite set. Now restrict this ordering to the n elements that are considered, then we obtain a finite ordering, which can be represented in a matrix as pictured in Figures 1 and 2.

$>$:1 $\leqslant$:0	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7
a_0								
a_1								
a_2								
a_3								
a_4								
a_5								
a_6								
a_7								

Figure 1. Defining $\geqslant$ by laying out a full matrix

In every cell (i,j) of the matrix in Figure 1 we write 1 if $a_i > a_j$, and 0 otherwise. Note that now the matrix has only 0's on its diagonal. Moreover it is antisymmetric, i.e.: if $i \neq j$ we have 1 in (i,j) if and only if we have 0 in (j,i). So in fact we only need one 'half' of the matrix.

The idea of square comparison now simply reads as follows: suppose we have a finite sequence of numbers to be sorted, then all the information relevant to the ordering problem can be computed in unit time, starting from the matrix above. Indeed, in one blow all n^2 individual cells (i,j) can do one comparison (between a_i and a_j), and next all information about $>$ is available. Note that we can set up this matrix in $O(\log n)$ time, starting from n processors containing the values to be sorted. Thus all ordering information can be computed in $O(\log n)$ time.

After $O(\log n)$ time we have computed a matrix which is full of 0's and 1's.

Note, that on the i-th row, we have a 1 for every a_j which is smaller than a_i. Hence the number of 1's in the i-th row is precisely the number of elements a_j out of $\langle a_0,a_1,a_2,\dots,a_{n-1}\rangle$, satisfying $a_j<a_i$. However, the number of elements less than a_i is exactly the index of a_i in the *sorted* sequence, i.e. represents the *place* of the number a_i in the sorted array.

Finally note that the number of 1's can simply be found, by computing the sum of all matrix values on the row considered. This computation can be done in $O(\log n)$ time, since we can repeatedly add pairs of numbers concurrently, until there is only one single value left. Thus we conclude that, for all input values, we can compute the 'sorted index' in $O(\log n)$ time.

In fact we have computed a *permutation* of the index values $\langle 0,1,2,\dots,n-1\rangle$. From this permutation one can compute the sorted array in $O(1)$ time, since all cells consider the computed index value, as an address to send the value to, they actually contain. Having enough wires to interconnect all cells, this can be done in one single computation step. (By putting the processors in a tree configuration once again, we can do this in $O(\log n)$ time, with many wires less.)

So, indeed, we can sort a sequence of numbers in $\log n$ time using n^2 processors. An example of this square comparison method is presented in Figure 2.

$\geqslant$ $>$	2	7	1	-5	11	2	3	8	
2	0	0	1	1	0	0	0	0	+ → 2
7	1	0	1	1	0	1	1	0	+ → 5
1	0	0	0	1	0	0	0	0	+ → 1
-5	0	0	0	0	0	0	0	0	+ → 0
11	1	1	1	1	0	1	1	1	+ → 7
2	1	0	1	1	0	0	0	0	+ → 3
3	1	0	1	1	0	1	0	0	+ → 4
8	1	1	1	1	0	1	1	0	+ → 6

FIGURE 2. An example of the square comparison method on the sequence $\langle 2,7,1,-5,11,2,3,8\rangle$

Here we have a small problem: suppose two numbers in the array are equal (the numbers are no longer distinct), then the matrix values, computed in Figure 1, would be equal for both numbers. Thus the problem is that the computed array of index values no longer is a permutation of $\langle 0,1,2,\dots,n-1\rangle$, since some of the computed indices might be equal.

In Figure 2, this problem is solved by slightly changing the former procedure. Now, the 'lower' cells, i.e. the cells below the main diagonal of the matrix, do not compare two values via '$>$' but via '$\geqslant$'. It turns out that the computed indices indeed are a permutation of $\langle 0,1,2,\dots,n-1\rangle$ and that the 'original order' of equal numbers is preserved in the sorted array.

In Figure 2 the sequence $\langle 2,7,1,-5,11,2,3,8\rangle$ is considered. Note that here, the computed index values ⟨2,5,1,0,7,3,4,6⟩ indeed form a permutation of ⟨0,1,2,3,4,5,6,7⟩. To be specific: note that the number 2 has two different computed indices (namely 2 and 3); without the adaptation mentioned above, both occurrences of the value 2 would yield the index value 2.

The sorting machine considered in this paper is pictured in Figure 3, for $n=4$. Note that on the upper side we have n trees, one for every input value. Each input value is broadcast to n leaves in a row of the matrix, which is in the middle part of the machine. Then, the cells on the main diagonal will send the value received from the upper tree downwards to the bottom of the connected lower tree; this value is broadcast upwards again to n matrix cells, belonging to a column of the matrix. So, every matrix cell now contains two values, precisely in the way as in Figure 1. Then the n^2 comparisons are made and each cell sends a 1 or a 0 to its upper tree. In every node the addition of two input values is computed, and the result is sent upwards again. Finally, the computed index permutation can be read from the roots of the upper trees.

3. A FORMAL SPECIFICATION OF THE SORTING MACHINE

In this section we will present a formal specification of RANKSORT, using the language ACP. First, we have to name the channels of the machine (Figures 3-5) in order to be able to give a precise definition of the behaviour of the individual cells. For reasons of simplicity, in the following we will assume $n=2^k$ for some given $k>0$, n being the length of the array to be sorted.

In Figure 4 we present the names of the processes, corresponding to the vertices in the trees and the cells of the matrix. The upper trees are called $U_i\,(0\leqslant i<n)$ and the cells in these trees are numbered $U_{i,j}\,(0<j<n)$. Likewise, the lower trees are called L_j, with cells $L_{i,j}\,(0<i<n)$, and the matrix cells are called $M_{i,j}\,(0\leqslant i,j<n)$. The bottom cells will be called $B_j\,(0\leqslant j<n)$.

Note that for all i, U_i has depth ${}^2\log n=k$ and has $2^k-1=n-1$ cells. Further, the cells and channels in the trees are numbered 'left first/breadth first', as one can see in the Figures 4 and 5.

Now, let us present a more detailed description of the behaviour of the individual processes.

- A cell $U_{i,j}$ will receive a value from its upper neighbour. Next, it will send this value to both of its lower neighbours, and from both of them it will receive another value in return. Since both lower neighbours are independent processes, these send and receive actions are fully interleaved. Finally, having received two values from below, $U_{i,j}$ will send its sum up again.
- A matrix cell $M_{i,j}$ in the middle of the sorter will first receive a value from the upper neighbour. Then, if it is a *diagonal* cell, it will send this value downwards to its lower neighbour. For sake of simplicity, we will make *non-diagonal* cells send a value **nil** downwards as well. Next, the cell will receive a new value from below, and send up a 0 or a 1, depending on its position (see Figure 2) and the two input values.
- A cell $L_{i,j}$ from one of the lower trees, will first receive two values from above (in any order). Note that in any lower tree only one leaf, the one in

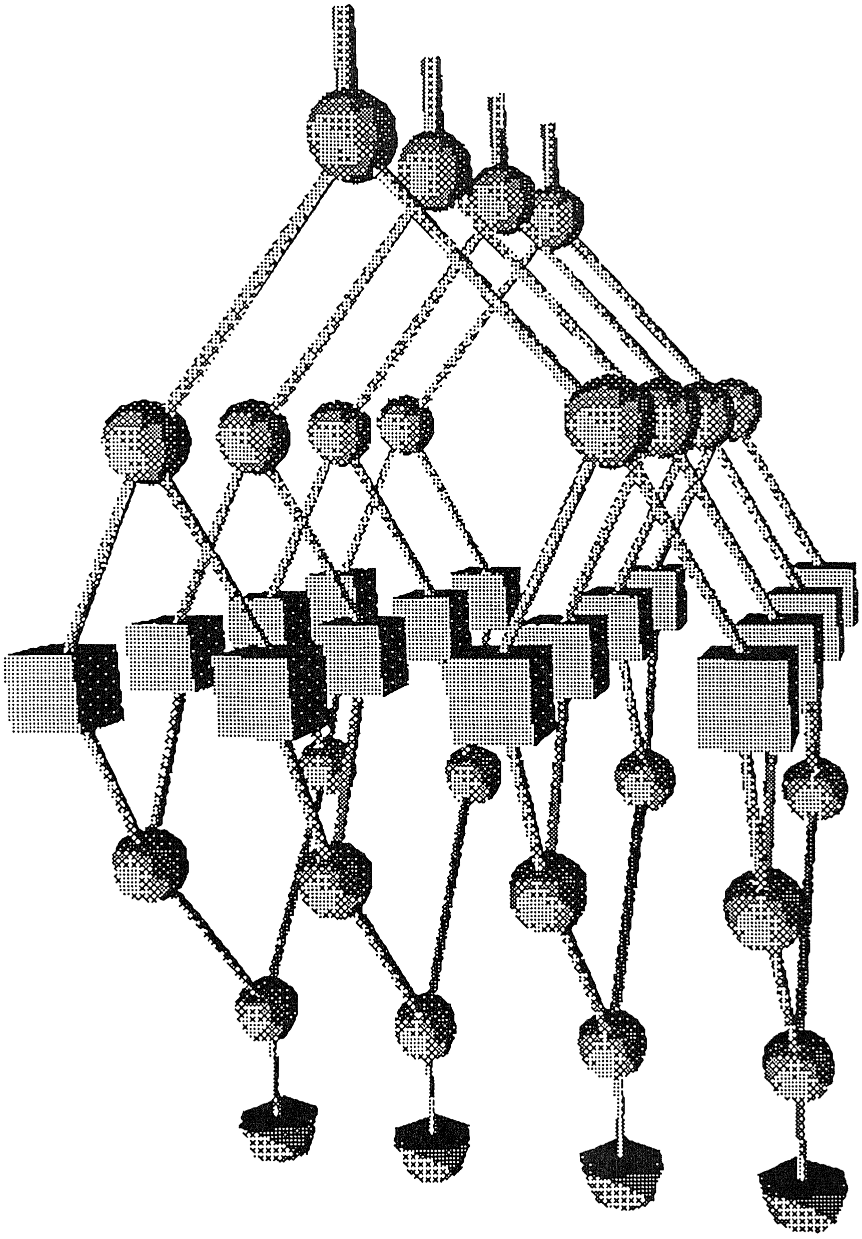

FIGURE 3. A 'mesh of trees'; the circuit configuration of RANKSORT

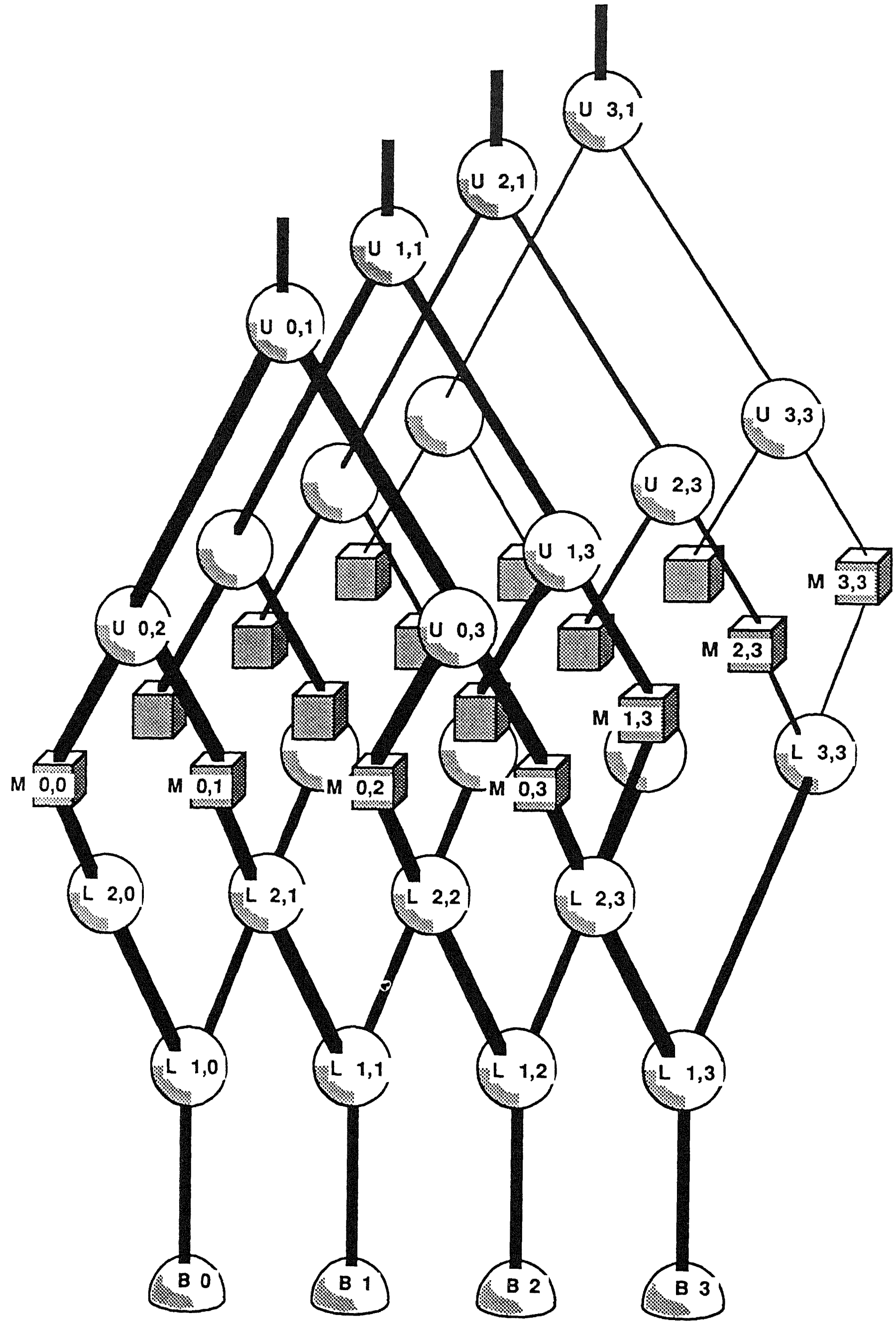

FIGURE 4. The names of the individual cells in the sorter

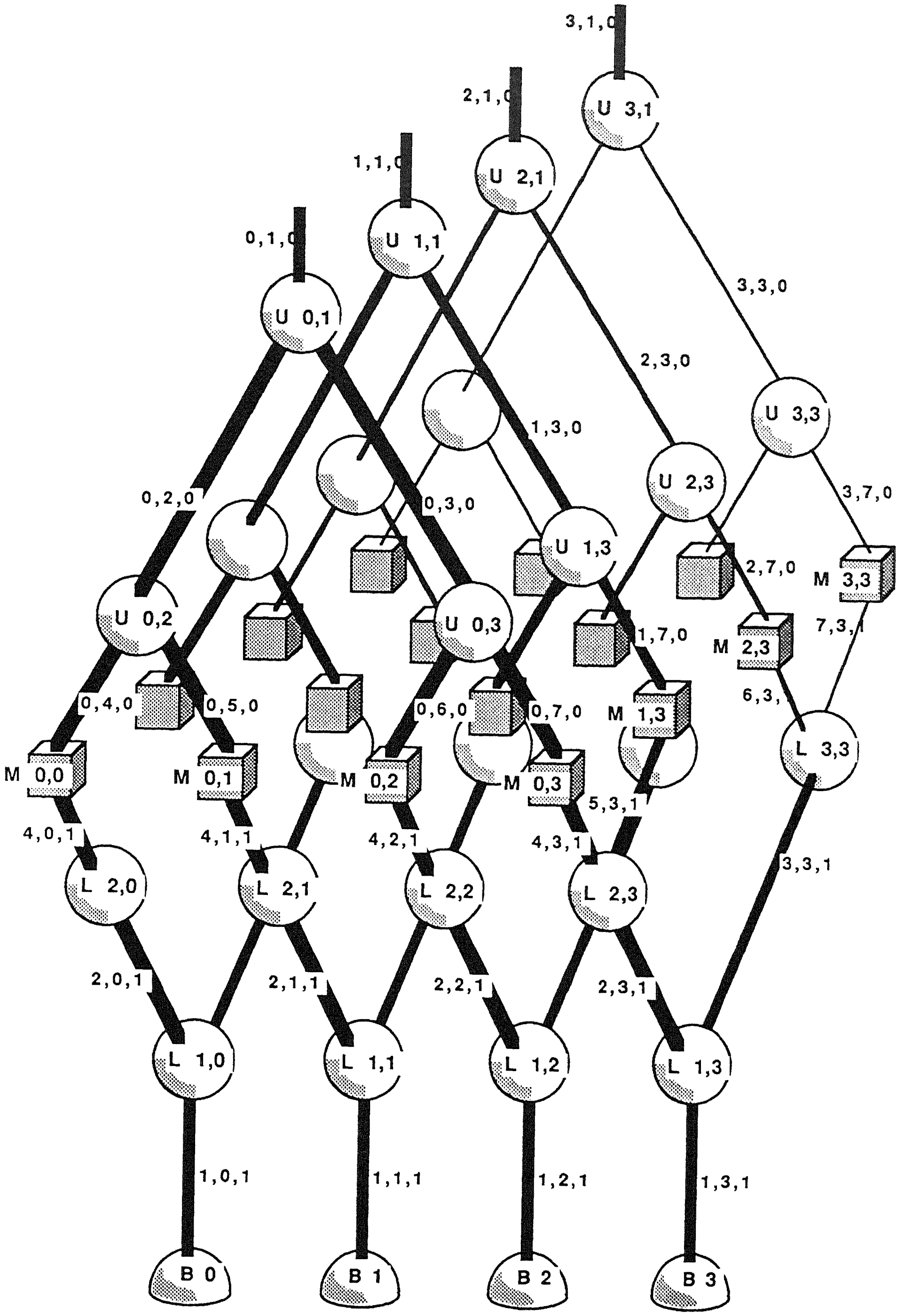

FIGURE 5. The channel numbers are in 'left first/breadth first' order

the diagonal of the matrix, will send down a number. The others will only send down **nil**. Now, if one of the values received from above is not **nil**, $L_{i,j}$ will send this value to its lower neighbour. Otherwise it will send down just **nil**. Next a value is received from below and 'broadcast' upwards, just like in $U_{i,j}$, by sending it to its upper neighbours.

- Finally, a cell B_j from the bottom of the machine, acts as a reflector: it will receive a value from its upper neighbour, and simply return it. Note that B_j will actually receive the number ($\neq$**nil**) which is sent down by $M_{j,j}$.

Now we will translate these informal descriptions into the algebraical specification language ACP. To do this we need the definitions of the following functions.

DEFINITION. We need a function **diag** to specify the value that will actually be sent down by $M_{i,j}$ after having received d:

$$\mathbf{diag}(i,i,d) = d$$

$$\mathbf{diag}(i,j,d) = \mathbf{nil} \quad (i \neq j).$$

DEFINITION. We also need a function **comp** to express what boolean value, 0 or 1, will be sent up by $M_{i,j}$ again, after having received d and e. So in **comp** we actually use the square comparison method (see Figure 2):

```
comp(i,j,d,e) = if i>j then if d≥e then 1 else 0 fi
else        if d>e then 1 else 0 fi
                fi ;
```

DEFINITION. Finally we need a kind of *exclusive or* on strings of symbols, to express what value is sent down by $L_{i,j}$ after having received two values:

$$\mathbf{xor}(d,\mathbf{nil}) = \mathbf{xor}(\mathbf{nil},d) = d$$

$$\mathbf{xor}(d,e) = \mathbf{xor}(\mathbf{nil},\mathbf{nil}) = \mathbf{nil} \quad (d,e \in D).$$

Inductively, we will define **xor** on arbitrary strings of length $n = 2^k$:

$$\mathbf{xor}(d_1,d_2,\ldots,d_{2^k}) = \mathbf{xor}(\mathbf{xor}(d_1,\ldots,d_{2^{k-1}}),\mathbf{xor}(d_{2^{k-1}+1},\ldots,d_{2^k}))(d_i \in D \cup \{\mathbf{nil}\}).$$

Note, that if exactly one value out of $\{d_1,\ldots,d_n\}$, d_i say, is not equal to **nil**, then $\mathbf{xor}(d_1,\ldots,d_n) = d_i$. So **xor** 'picks' out the unique value $\neq$ **nil**, assuming this unique value exists. This more general definition will be needed later, to describe the specific behaviour of the lower trees, since all of its leaves will send down **nil** except for the leaf on the diagonal of the matrix.

Now we will turn to the formal specification of the cells (see Table 1). In this specification we have atomic actions $r_{i,j,m}(d)$ and $s_{i,j,m}(d)$ for *receiving* and *sending* a datum d from and to the channel $[i,j,m]$. Note that receive and send actions do not have a fixed 'direction' in the channel. We assume D to be a (finite) set of numbers. All (bound) variables are written in italics.

$$
\begin{aligned}
U_{i,j} &= \sum_{d\in D} r_{i,j,0}(d)\cdot\left[\left\{s_{i,2j,0}(d)\cdot\sum_{n\in\mathbb{N}} r_{i,2j,0}(n)\right\}\parallel\right. \\
&\qquad\qquad \left.\parallel\left\{s_{i,2j+1,0}(d)\cdot\sum_{m\in\mathbb{N}} r_{i,2j+1,0}(m)\right\}\right]\cdot s_{i,j,0}(n+m) \\
M_{i,j} &= \sum_{d\in D} r_{i,j+n,0}(d)\cdot s_{i+n,j,1}(\mathbf{diag}(i,j,d))\cdot \\
&\qquad\qquad \cdot\sum_{e\in D} r_{i+n,j,1}(e)\cdot s_{i,j+n,0}(\mathbf{comp}(i,j,d,e)) \\
L_{i,j} &= \left[\sum_{d\in D\cup\{\mathbf{nil}\}} r_{2i,j,1}(d)\parallel\sum_{e\in D\cup\{\mathbf{nil}\}} r_{2i+1,j,1}(e)\right]\cdot s_{i,j,1}(\mathbf{xor}(d,e))\cdot \\
&\qquad\qquad \cdot\sum_{f\in D} r_{i,j,1}(f)\cdot\left[s_{2i,j,1}(f)\parallel s_{2i+1,j,1}(f)\right] \\
B_j &= \sum_{d\in D} r_{1,j,1}(d)\cdot s_{1,j,1}(d)
\end{aligned}
$$

TABLE 1. Specification of the cells in the sorter

As a shorthand, the scope rules of Σ are violated in the first equation. Writing out $\parallel$ using the axioms CM1-4 of [1], $U_{i,j}$ can easily be specified correctly (see also [4] and [6]). It takes some effort to check all the indices, corresponding to the names of the channels. However, making use of the regular configuration of the circuit, and comparing the specification with Figures 3 and 4, one can find out that they are presented correctly here. Furthermore, in the next section we will concentrate on a formal proof of correctness of the sorter, and from any such proof it follows immediately that the channel numbers in the specification above are correct.

Now we present the final specification of the sorting machine as a whole by simply interconnecting all cells (see Table 2).

$$
\textsc{Ranksort}(n) = \mathop{\parallel}_{i,j<n}\left\{U_{i,j}\parallel M_{i,j}\parallel L_{i,j}\right\}\parallel\mathop{\parallel}_{i<n} B_i
$$

TABLE 2. Specification of RANKSORT

So this is the specification, in detail, of RANKSORT. Indeed, it is not clear at all why such a complex machine would be a sorting machine. In the next section we will hide almost all of the internal actions of the machine (only actions via channels $[i,1,0]$ are of interest to the user). Then we will prove the result to be a sorting machine, and hence prove RANKSORT correct.

4. FORMULATING A CORRECTNESS THEOREM

In this section we will present a formal theorem of correctness for RANKSORT, i.e.: abstracting from internal actions, we will state that RANKSORT indeed behaves like a sorting machine. To do this, we first have to specify what actually *is* a sorting machine.

DEFINITION. In the following we define the *sorted indices* of a given sequence of numbers. Suppose $a = \langle a_0, a_1, a_2, \dots, a_{n-1} \rangle$ is such a sequence of numbers, then we have:

(i) $\langle p_0(a), \dots, p_{n-1}(a) \rangle \in PERM(\langle 0, \dots, n-1 \rangle)$,
(ii) $p_i(a) < p_j(a)$ implies $a_i \leqslant a_j$,
(iii) $p_i(a) < p_j(a)$ & $a_i = a_j$ implies $i < j$.

Because of part (iii) of the definition the permutation $p_i(a)_{0 \leqslant i < n}$ satisfying all three conditions, is uniquely determined.

Note that from the sorted indices $p_i(a)_{0 \leqslant i < n}$ we can immediately compute the sorted sequence itself: assume we have n processors $P_0, \dots, P_{n-1}$, containing the values $p_0(a), \dots, p_{n-1}(a)$ and $a_0, \dots, a_{n-1}$ respectively, and suppose all processors are interconnected by channels (wires) then in one step every process P_i can send the number a_i to the 'address' given by $p_i(a)$, i.e.: to $P_{p_i(a)}$.

Next we will formulate a crucial proposition, stating a criterion for correctness of the square comparison method. A proof of this proposition is omitted.

PROPOSITION. *For all sequences* $a = \langle a_0, \dots, a_{n-1} \rangle$ *and all* $0 \leqslant i < n$ *we have:*

$$\sum_{j=0}^{n-1} \mathbf{comp}(i,j,a_i,a_j) = p_i(a).$$

Clearly, the proposition states that the square comparison method provides us with the sorted indices of the input sequence. Using this proposition we will be able to prove RANKSORT correct, in the sense that RANKSORT turns out to calculate precisely $\Sigma_{0 \leqslant j < n} \mathbf{comp}(i,j,a_i,a_j)$ for all sequences $\langle a_0, \dots, a_{n-1} \rangle$.

DEFINITION. Suppose a process SORT(n) satisfies the equation

$$\text{SORT}(n) = \left[\mathop{\|}_{0 \leqslant i < n} \left[\sum_{x_i} r_{i,1,0}(x_i) \right] \right] \cdot \left[\mathop{\|}_{0 \leqslant i < n} s_{i,1,0}(p_i(x)) \right],$$

and $x = \langle x_0, \dots, x_{n-1} \rangle$, then SORT($n$) is called a *sorting machine* of size n.

So we agree that any machine that receives a sequence of n numbers, and consequently outputs all sorted indices of this input sequence, may be called a sorting machine. Now we will return to RANKSORT again.

Let D be a (finite) set of numbers. Suppose $n=2^k$, $k\geqslant 0$. The *communication function* $|$ is defined by

$$(r_{i,j,m}(d)|s_{i,j,m}(d)) = (s_{i,j,m}(d)|r_{i,j,m}(d))=c_{i,j,m}(d) \quad \text{for all } i,j,m,$$

all other communication actions result in deadlock, δ.

The *encapsulation sets* M_n, B_n, H_n and E_n are defined by

$$M_n = \{s_{i,j+n,0}(d),r_{i,j+n,0}(d): d\in D\cup\mathbb{N},\ i,j<n\}\cup$$
$$\{s_{i+n,j,1}(d),r_{i+n,j,1}(d): d\in D\cup\{\mathbf{nil}\},\ i,j<n\}$$

corresponding to all channels connected with the matrix cells $M_{i,j}$,

$$B_n = \{s_{1,j,1}(d), r_{1,j,1}(d): d\in D\cup\{\mathbf{nil}\},\ j<n\}$$

corresponding to the channels connected with the bottom cells B_j,

$$H_n = \{s_{i,j,m}(d), r_{i,j,m}(d): d\in D\cup\mathbb{N}\cup\{\mathbf{nil}\};\ \text{for all } i,j,m, \text{ such that:}$$
$$(j,m)\neq(1,0) \text{ and } (i,m)\neq(1,1) \text{ and } i,j<n\}$$

which is the set of all communicating actions, except for actions from M_n or B_n or the ones corresponding to the input/output channels $[i,1,0]$ $(i<n)$,

$$E_n = H_n\cup M_n\cup B_n.$$

Finally, the *abstraction set* I is defined by

$$I = \{c_{i,j,m}(d): d\in D\cup\{\mathbf{nil}\};\ \text{for all appropriate } i,j,m\}.$$

The definition of the communication function says, that receive and send actions only result in a communication $c_{i,j,m}(d)$ if they correspond to the same channel $[i,j,m]$ and the same datum d. If not, a deadlock occurs, e.g. if $d_1\neq d_2$ then $(r_{2,7,0}(d)|s_{5,2,1}(d)) = (r_{i,j,m}(d_1)|s_{i,j,m}(d_2)) = (r_{i,j,m}(d)|r_{i,j,m}(d))=\delta$. The choice of the encapsulation sets M_n, B_n and H_n is quite standard: we want no single receive or send actions to happen without direct communication with their 'partner', since otherwise data would be sent to a channel but never read from it. Except for the receive and send actions on the channels $[i,1,0]$ $(0\leqslant i<n)$: they are the input and output channels of the machine, and are ready for communication with the outside world. The encapsulation sets, M_n and B_n, are defined separately from H_n, to simplify the proofs that will be presented later. At the end of the proof, however, we will encapsulate all actions from $E_n=H_n\cup M_n\cup B_n$.

The abstraction set I has no index n since it contains *all* communication actions $c_{i,j,m}(d)$. By renaming all actions from I into τ we can *hide* internal communication actions from the outside world. Note that any user of RANKSORT will indeed not be interested in the internal communications of the machine; only the outside behaviour will be observed, i.e.: $\tau_I\partial_{E_n}(\text{RANKSORT}(n))$.

Now a correctness theorem can easily be formulated as follows:

THEOREM (CORRECTNESS OF RANKSORT). *For all $k \geqslant 0$ and $n=2^k$, we have*

$$\text{ACP}_\tau \vdash \tau_I\partial_{E_n}(\text{RANKSORT}(n)) = \text{SORT}(n)$$

where SORT(n) *is specified earlier.*

This theorem states that $\tau_I\partial_{E_n}(\text{RANKSORT}(n))$ is indeed a sorting machine in the sense of the definition of SORT(n). The proof will be presented in the next section.

5. A FORMAL PROOF OF CORRECTNESS

In this section we will present the final proof of the correctness theorem. First we will simplify the problem by stating and proving two lemmas. Combining both of them we can easily find the proof we are looking for.

First we will formulate what we expect the i-th upper tree $U_{i,1}\|\cdots\|U_{i,n-1}$ to behave like. This is done in Lemma 1 below.

LEMMA 1. *Assume $n=2^k$, for some given $k>0$. Then in the theory* ACP$_\tau$ *we can prove*

$$\tau_I\partial_{H_n}(U_{i,1}\|\cdots\|U_{i,n-1}) = \sum_{x_i} r_{i,1,0}(x_i)\cdot \mathop{\|}_{0\leqslant j<n}\left[s_{i,j+n,0}(x_i)\cdot\sum_{y_{i,j}} r_{i,j+n,0}(y_{i,j})\right]\cdot s_{i,1,0}\left(\sum_{j=0}^{n-1} y_{i,j}\right)$$

PROOF. By induction on k.

$k=1$: Now $n=2$, so $\tau_I\partial_{H_n}(U_{i,1}\|\cdots\|U_{i,n-1})=\tau_I\partial_{H_2}(U_{i,1})=U_{i,1}$, and the lemma directly follows from the definition of $U_{i,1}$.

$k+1$: Suppose the lemma holds for $n=2^k$. Now we prove it to hold for $2n=2^{k+1}$ as well:

$$\tau_I\partial_{H_{2n}}(U_{i,1}\|\cdots\|U_{i,2n-1}) =$$

$$= \tau_I\partial_{H_{2n}}(\tau_I\partial_{H_n}(U_{i,1}\|\cdots\|U_{i,n-1})\|U_{i,n}\|\cdots\|U_{i,2n-1})$$

$$= \tau_I\partial_{H_{2n}}\left(\left\{\sum_{x_i} r_{i,1,0}(x_i)\cdot \mathop{\|}_{0\leqslant j<n}\left[s_{i,j+n,0}(x_i)\cdot\sum_{y_{i,j}} r_{i,j+n,0}(y_{i,j})\right]\cdot\right.\right.$$

$$\left.\left.\cdot\, s_{i,1,0}\left(\sum_{j=0}^{n-1} y_{i,j}\right)\right\} \| \mathop{\|}_{0\leqslant j<n} U_{i,j+n}\right)$$

Note, that we needed the conditional axioms to prove the first step. Using the definition of $U_{i,j+n}$ we immediately find

$$= \tau_I \partial_{H_{2n}} \Bigg(\Bigg\{ \sum_{x_i} r_{i,1,0}(x_i) \cdot \mathop{\|}_{0 \leqslant j < n} \Big[s_{i,j+n,0}(x_i) \cdot \sum_{y_{i,j}} r_{i,j+n,0}(y_{i,j}) \Big] \cdot s_{i,1,0} \Big(\sum_{j=0}^{n-1} y_{i,j} \Big) \Bigg\} \|$$

$$\| \mathop{\|}_{0 \leqslant j < n} \sum_{d_j \in D} r_{i,j+n,0}(d_j) \cdot \Bigg[\Big\{ s_{i,2(j+n),0}(d_j) \cdot \sum_{n_{i,j} \in \mathbb{N}} r_{i,2(j+n),0}(n_{i,j}) \Big\} \|$$

$$\| \Big\{ s_{i,2(j+n)+1,0}(d_j) \cdot \sum_{m_{i,j} \in \mathbb{N}} r_{i,2(j+n)+1,0}(m_{i,j}) \Big\} \Bigg] \cdot s_{i,j+n,0}(n_{i,j} + m_{i,j}) \Bigg)$$

Note that for every $0 \leqslant j < n$ we have two communications: the first one binding the variable d_j and the value x_i, and the second one binding $y_{i,j}$ and $n_{i,j} + m_{i,j}$. So we find:

$$= \tau_I \partial_{H_{2n}} \Bigg(\sum_{x_i} r_{i,1,0}(x_i) \cdot \mathop{\|}_{0 \leqslant j < n} \Bigg\{ c_{i,j+n,0}(x_i) \cdot$$

$$\cdot \Bigg[\Big\{ s_{i,2(j+n),0}(x_i) \cdot \sum_{n_{i,j} \in \mathbb{N}} r_{i,2(j+n),0}(n_{i,j}) \Big\} \|$$

$$\| \Big\{ s_{i,2(j+n)+1,0}(x_i) \cdot \sum_{m_{i,j} \in \mathbb{N}} r_{i,2(j+n)+1,0}(m_{i,j}) \Big\} \Bigg] \cdot c_{i,j+n,0}(n_{i,j} + m_{i,j}) \Bigg\} \cdot$$

$$\cdot s_{i,1,0} \Big(\sum_{j=0}^{n-1} (n_{i,j} + m_{i,j}) \Big) \Bigg)$$

$$= \sum_{x_i} r_{i,1,0}(x_i) \cdot \mathop{\|}_{0 \leqslant j < n} \Bigg[\Big\{ s_{i,2(j+n),0}(x_i) \cdot \sum_{n_{i,j} \in \mathbb{N}} r_{i,2(j+n),0}(n_{i,j}) \Big\} \|$$

$$\| \Big\{ s_{i,2(j+n)+1,0}(x_i) \cdot \sum_{m_{i,j} \in \mathbb{N}} r_{i,2(j+n)+1,0}(m_{i,j}) \Big\} \Bigg] \cdot s_{i,1,0} \Big(\sum_{j=0}^{n-1} (n_{i,j} + m_{i,j}) \Big)$$

using the equation $(\tau x \| y) = \tau(x \| y)$, which can be derived directly from the axioms of ACP$_\tau$. Thus we have

$$= \sum_{x_i} r_{i,1,0}(x_i) \cdot \mathop{\Big\|}_{0 \leqslant j < 2n} \left[s_{i,j+2n,0}(x_i) \cdot \sum_{y_{i,j} \in \mathbb{N}} r_{i,j+2n,0}(y_{i,j}) \right] \cdot s_{i,1,0}\left(\sum_{j=0}^{2n-1} y_{i,j} \right)$$

renaming the n's and m's into y's again. □

So indeed, the i-th upper tree first will receive a number x_i from channel $[i,1,0]$, i.e.: from its own root. Next, after some time, we will see all of its leaves send this value downward to the cells in the matrix, getting some other value in return. All processes in the leaves of the tree are interleaved, precisely as we expected. Finally, after some time, we will find the sum of all values being sent up from the leaves, appears at the root channel $[i,1,0]$ again.

In the same way we can describe what the j-th lower tree acts like, as is done in Lemma 2.

LEMMA 2. *Assume $n=2^k$, for some given $k>0$. Then we have (for $j<n$)*

$$\tau_I \partial_{H_n}(L_{1,j} \| \cdots \| L_{n-1,j}) = \mathop{\Big\|}_{0 \leqslant i < n} \left[\sum_{z_{i,j} \in D \cup \{\mathbf{nil}\}} r_{i+n,j,1}(z_{i,j}) \right] \cdot$$

$$\cdot s_{1,j,1}(\mathbf{xor}(z_{0,j}, \ldots, z_{n-1,j})) \cdot \sum_{u_j \in D} r_{1,j,1}(u_j) \cdot \mathop{\Big\|}_{0 \leqslant i < n} s_{i+n,j,1}(u_j)$$

PROOF. By induction on k.

$k=1$: Now $n=2$, so the result directly follows from the definition of $L_{1,j}$.

$k+1$: $\tau_I \partial_{H_{2n}}(\tau_I \partial_{H_n}(L_{1,j} \| \cdots \| L_{n-1,j}) \| L_{n,j} \| \cdots \| L_{2n-1,j}) =$

$$= \tau_I \partial_{H_{2n}} \left(\mathop{\Big\|}_{0 \leqslant i < n} \left[\sum_{z_{i,j} \in D \cup \{\mathbf{nil}\}} r_{i+n,j,1}(z_{i,j}) \right] \cdot s_{1,j,1}(\mathbf{xor}(z_{0,j}, \ldots, z_{n-1,j})) \cdot \right.$$

$$\cdot \sum_{u_j \in D} r_{1,j,1}(u_j) \cdot \mathop{\Big\|}_{0 \leqslant i < n} s_{i+n,j,1}(u_j) \ \|$$

$$\| \mathop{\Big\|}_{0 \leqslant i < n} \left[\sum_{d_{i,j} \in D \cup \{\mathbf{nil}\}} r_{2i+2n,j,1}(d_{i,j}) \| \sum_{e_{i,j} \in D \cup \{\mathbf{nil}\}} r_{2i+1+2n,j,1}(e_{i,j}) \right] \cdot$$

$$\cdot s_{i+n,j,1}(\mathbf{xor}(d_{i,j}, e_{i,j})) \cdot$$

$$\left. \cdot \sum_{f_{i,j} \in D} r_{i+n,j,1}(f_{i,j}) \cdot \left[s_{2i+2n,j,1}(f_{i,j}) \| s_{2i+1+2n,j,1}(f_{i,j}) \right] \right)$$

using the definition of $L_{i,j}$ and the lemma for $n=2^k$

$$= \tau_I \partial_{H_{2n}} \left(\underset{0 \leqslant i < n}{\|} \left[\sum_{d_{i,j} \in D \cup \{\mathbf{nil}\}} r_{2i+2n,j,1}(d_{i,j}) \,\|\, \sum_{e_{i,j} \in D \cup \{\mathbf{nil}\}} r_{2i+1+2n,j,1}(e_{i,j}) \right] \cdot \right.$$

$$\cdot\, c_{i+n,j,1}(\mathbf{xor}(d_{i,j},e_{i,j})) \cdot s_{1,j,1}(\mathbf{xor}(\mathbf{xor}(d_{0,j},e_{0,j}),\ldots,\mathbf{xor}(d_{n-1,j},e_{n-1,j}))) \cdot$$

$$\left. \cdot \sum_{u_j \in D} r_{1,j,1}(u_j) \cdot \underset{0 \leqslant i < n}{\|} \left\{ c_{i+n,j,1}(u_j) \cdot \left[s_{2i+2n,j,1}(u_j) \| s_{2i+1+2n,j,1}(u_j) \right] \right\} \right)$$

binding $\mathbf{xor}(d_{i,j},e_{i,j})$ and $z_{i,j}$; moreover the variables u_j and $f_{i,j}$ are identified, for all i,j. Note that $\mathbf{xor}(\mathbf{xor}(d_{0,j},e_{0,j}),\ldots,\mathbf{xor}(d_{n-1,j},e_{n-1,j})) =$ $\mathbf{xor}(d_{0,j},e_{0,j},\ldots,d_{n-1,j},e_{n-1,j})$; renaming $d_{i,j}$ and $e_{i,j}$ into $z_{2i,j}$ and $z_{2i+1,j}$ respectively, we find

$$= \underset{0 \leqslant i < 2n}{\|} \left[\sum_{z_{i,j} \in D \cup \{\mathbf{nil}\}} r_{i+2n,j,1}(z_{i,j}) \right] \cdot$$

$$\cdot\, s_{1,j,1}(\mathbf{xor}(z_{0,j},\ldots,z_{2n-1,j})) \cdot \sum_{u_j \in D} r_{1,j,1}(u_j) \cdot \underset{0 \leqslant i < 2n}{\|} s_{i+2n,j,1}(u_j)$$

□

From Lemma 2 we read that the j-th lower tree first will receive n values (probably with some **nil**'s) from its leaves, say $z_{0,j},\ldots,z_{n-1,j}$. Then it will send $\mathbf{xor}(z_{0,j},\ldots,z_{n-1,j})$ to the bottom. Next it waits until it gets a value u_j from the bottom in return, and it will broadcast this value up to the leaves again, i.e.: after some time all leaves, in any order, will send up u_j. Using both lemmas we can now easily find the final proof of the correctness theorem.

Proof of the correctness theorem

Let $n = 2^k$ for some $k \geqslant 0$. Using the conditional axioms of [1], one easily verifies

$$\tau_I \partial_{H_n \cup M_n}(U_{i,1} \| \cdots \| U_{i,n-1} \| M_{i,0} \| \cdots \| M_{i,n-1}) =$$

$$= \tau_I \partial_{H_n \cup M_n}(\tau_I \partial_{H_n}(U_{i,1} \| \cdots \| U_{i,n-1}) \| M_{i,0} \| \cdots \| M_{i,n-1}).$$

Then, using Lemma 1 and the definition of $M_{i,j}$ we find

$$\tau_I \partial_{H_n}(U_{i,1} \| \cdots \| U_{i,n-1}) \| M_{i,0} \| \cdots \| M_{i,n-1} =$$

$$= \sum_{x_i} r_{i,1,0}(x_i) \cdot \underset{0 \leqslant j < n}{\|} \left[s_{i+n,j,1}(\mathbf{diag}(i,j,x_i)) \cdot \sum_{w_{i,j}} r_{i+n,j,1}(w_{i,j}) \right] \cdot$$

$$\cdot\, s_{i,1,0} \left(\sum_{j=0}^{n-1} \mathbf{comp}(i,j,x_i,w_{i,j}) \right).$$

Using the conditional axioms once again we have

$$\tau_I \partial_{E_n}(L_{1,j} \| \cdots \| L_{n-1,j} \| B_j) = \tau_I \partial_{E_n}(\tau_I \partial_{H_n}(L_{1,j} \| \cdots \| L_{n-1,j}) \| B_j).$$

From the definition of B_j and Lemma 2 we find directly

$$\tau_I \partial_{E_n}(\tau_I \partial_{H_n}(L_{1,j} \| \cdots \| L_{n-1,j}) \| B_j) =$$

$$= \mathop{\|}\limits_{0 \leqslant i < n} \left[\sum_{z_{i,j}} r_{i+n,j,1}(z_{i,j}) \right] \cdot \mathop{\|}\limits_{0 \leqslant i < n} s_{i+n,j,1}(\mathbf{xor}(z_{0,j}, \dots, z_{n-1,j}))$$

so we have

$$\tau_I \partial_{E_n}(\textsc{Ranksort}(n)) =$$

$$= \tau_I \partial_{E_n} \left(\mathop{\|}\limits_{0 \leqslant i < n} \left[\tau_I \partial_{H_n \cup M_n}(\tau_I \partial_{H_n}(U_{i,1} \| \cdots \| U_{i,n-1}) \| M_{i,0} \| \cdots \| M_{i,n-1}) \right] \| \right.$$

$$\left. \| \mathop{\|}\limits_{0 \leqslant j < n} \left[\tau_I \partial_{E_n}(L_{1,j} \| \cdots \| L_{n-1,j} \| B_j) \right] \right)$$

$$= \tau_I \partial_{E_n} \left(\mathop{\|}\limits_{0 \leqslant i < n} \left\{ \sum_{x_i} r_{i,1,0}(x_i) \cdot \mathop{\|}\limits_{0 \leqslant j < n} c_{i+n,j,1}(\mathbf{diag}(i,j,x_i)) \right\} \cdot \right.$$

$$\cdot \mathop{\|}\limits_{0 \leqslant i < n} \left\{ \mathop{\|}\limits_{0 \leqslant j < n} \left[c_{i+n,j,1}(\mathbf{xor}(\mathbf{diag}(0,j,x_0), \dots, \mathbf{diag}(n-1,j,x_{n-1}))) \right] \cdot \right.$$

$$\left. \left. \cdot s_{i,1,0} \left(\sum_{j=0}^{n-1} \mathbf{comp}(i,j,x_i,\mathbf{xor}(\mathbf{diag}(0,j,x_0), \dots, \mathbf{diag}(n-1,j,x_{n-1}))) \right) \right\} \right)$$

$$= \tau_I \partial_{E_n} \left(\mathop{\|}\limits_{0 \leqslant i < n} \left\{ \sum_{x_i} r_{i,1,0}(x_i) \cdot \mathop{\|}\limits_{0 \leqslant j < n} c_{i+n,j,1}(\mathbf{diag}(i,j,x_i)) \right\} \cdot \right.$$

$$\left. \cdot \mathop{\|}\limits_{0 \leqslant i,j < n} c_{i+n,j,1}(x_j) \cdot s_{i,1,0} \left(\sum_{j=0}^{n-1} \mathbf{comp}(i,j,x_i,x_j) \right) \right)$$

$$= \mathop{\|}\limits_{0 \leqslant i < n} \left[\sum_{x_i} r_{i,1,0}(x_i) \right] \cdot \mathop{\|}\limits_{0 \leqslant i < n} s_{i,1,0} \left(\sum_{j=0}^{n-1} \mathbf{comp}(i,j,x_i,x_j) \right)$$

$$= \mathop{\|}\limits_{0 \leqslant i < n} \left[\sum_{x_i} r_{i,1,0}(x_i) \right] \cdot \mathop{\|}\limits_{0 \leqslant i < n} s_{i,1,0}(p_i(x))$$

$$= \textsc{Sort}(n)$$

using the proposition of Section 4 for the last but one equality. □

6. Some remarks about the complexity of ranksort

It is beyond the subject of this paper to study the complexity of the machine described in the former sections. Still, some obvious remarks can be made to indicate that Ranksort in fact is only slightly suboptimal with respect to other well-known algorithms. All of these remarks are from [5], in which a review over thirteen VLSI sorting algorithms is presented.

As it turns out, Ranksort works with n^2 processors and in $\log n$ time. So one could say, comparing this complexity behaviour with for instance the $n\log n$ time sequential mergesort algorithm, a factor $O(n)$ time can be 'won' by exchanging it for a large amount of space. In some well-known models of VLSI complexity this notion of 'space' is worked out in more detail (see: Bilardi & Preparata [2] and Thompson [5]). A convenient unit of *area* of a VLSI chip is the square of the minimum separation between parallel wires. Every square unit on the chip surface may contain a *wire* element, or a piece of a *gate*, i.e.: a localized set of transistors or other switching elements, which perform a simple logical function. Starting from a square tessellation of the chip surface, some restrictions on the design of the chip are made. For instance, no pieces of gates may overlap (i.e.: any square unit only contains a part of at most one gate) and only two (or perhaps three, depending on the model) wires can pass over the same point (any square unit can represent the crossing of at most two wires).

The unit of time can be taken to be the time of one clock pulse, so the time behaviour of the chip can be expressed as a number of pulses. Note, that the specification of Ranksort, as given in Section 4, can be implemented in an *unclocked* network, since we have asynchronous cooperation between individual processes. A *clocked* network, however, is a special case of the general network in which no restrictions on timing are made, so a clock can do no 'harm' to the correct behaviour of the machine.

Of course, the list of restrictions mentioned here is not complete. In [2] all restrictions are formulated in detail, as rules on the underlying graphs representing the VLSI networks.

In [2] and [5], VLSI models are used to find lower and upper bounds for the complexity behaviour of sorting algorithms. Assume a VLSI chip has area A and needs time T to do its task, then a useful complexity measure turns out to be $A\cdot T^2$ (although AT and $AT/\log A$ can be used as well). In [5] a lower bound for the complexity of any sorting algorithm is put at $AT^2=\Omega(n^2\log n)$. Moreover about thirteen VLSI sorting algorithms are examined, ranging from $O(n^2\log^2 n)$ to $O(n^2\log^5 n)$, and hence all are only slightly suboptimal in AT^2 behaviour.

Although we have $O(n^2)$ wires in the network, we need some more wire unit elements to implement the orthogonal tree network on a VLSI chip. The Ranksort algorithm turns out to be $A=O(n^2\log^2 n)$, and thus $AT^2=O(n^2\log^4 n)$, which can be understood by making the following observation.

As we can see, the orthogonal tree network consists of $O(n^2)$ processors, interconnected by a number of wires. Note that every wire has width $O(1)$, not 0. Now consider the projection of the orthogonal tree network on a plane, as pictured in Figure 6. We see we have to leave at least $\log n$ units of space between two rows or columns of matrix cells, since this is the minimum area needed to construct a tree in between these cells. So, we may conclude that the width of the whole circuit is $O(n \log n)$, since the distance between two matrix processors is $O(\log n)$, and any processor is $O(\log n)$ square. So we find directly that the total area of the orthogonal tree network is $O(n^2 \log^2 n)$. Since the sorting task can be done in $O(\log n)$ time, we have $AT^2 = O(n^2 \log^4 n)$.

Indeed, Ranksort can be said to be slightly suboptimal with respect to the lower bound $AT^2 = \Omega(n^2 \log n)$. Clearly, however, the strong time performance of the algorithm takes a large amount of area, so we may not expect the circuit to be of much interest until chip area is cheap enough.

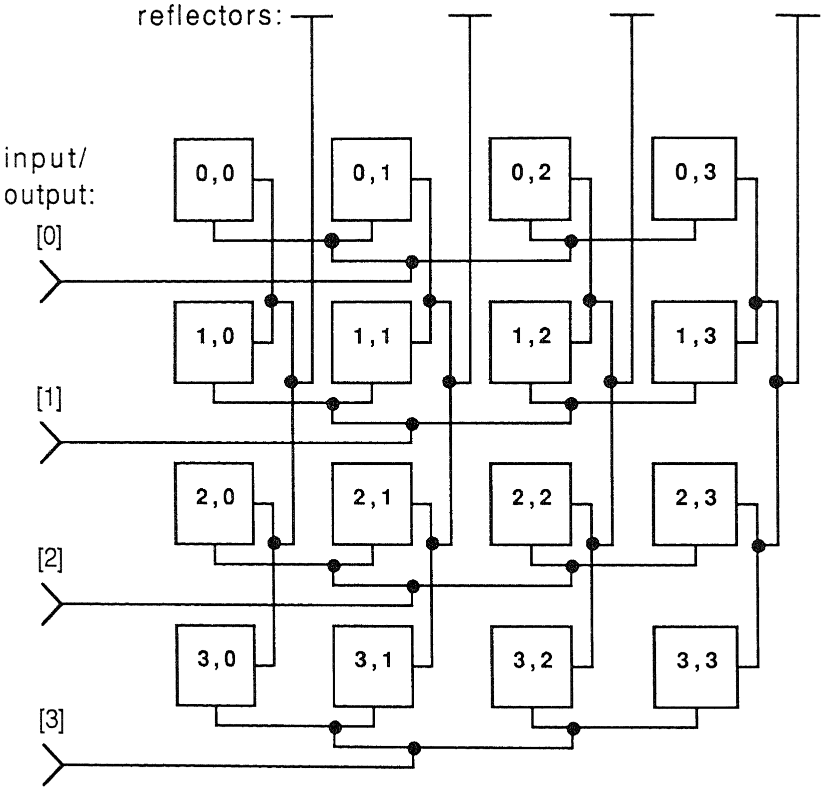

Figure 6. A two dimensional projection of the orthogonal tree network with $n = 4$

REFERENCES

1. J.A. BERGSTRA, J.W. KLOP (1989). *An Introduction to Process Algebra.* This volume.
2. G. BILARDI, F.P. PREPARATA (1986). Area-time lower-bound techniques with applications to sorting. *Algorithmica 1,* 65-91.
3. M. HENNESSY (1986). Proving systolic systems correct. *TOPLAS 8(3),* 344-387.
4. L. KOSSEN, W.P. WEIJLAND (1989). *Correctness Proofs for Systolic Algorithms: Palindromes and Sorting.* This volume.
5. CLARK D. THOMPSON (1983). The VLSI complexity of sorting. *IEEE Transactions on Computers: Vol. C-32, 12,* December 1983.
6. W.P. WEIJLAND (1987). A systolic algorithm for matrix-vector multiplication. *Proc. SION Conference CSN 1987,* Centre for Mathematics and Computer Science, Amsterdam, 143-160.