ELSEVIER

Information Processing Letters 54 (1995) 111–119

Information Processing Letters

Message terminating algorithms for anonymous rings of unknown size

Israel Cidon [1], Yuval Shavitt *

Electrical Engineering Department, Technion – Israel Institute of Technology, Haifa 32000, Israel

Communicated by S. Zaks; received 13 August 1992; revised 12 November 1994

Abstract

We consider a ring of an unknown number of anonymous processors. We focus on message terminating algorithms, i.e., algorithms that terminate when no more messages are present in the system but the processors may lack the ability to detect this situation. This paper addresses the design of deterministic and probabilistic algorithms that message terminate with the correct result. For this model we show: (i) A deterministic ring orientation algorithm that employs symmetry breaking link markings and requires $O(n \log^2 n)$ bits for communication and $O(n)$ time. A probabilistic Las-Vegas version of this algorithm (that requires no link markings) has the same average communication and time complexities. (ii) A probabilistic Las-Vegas algorithm for partitioning an even size ring into pairs that requires $O(n \log n)$ communication bits and time. (iii) The impossibility of computing (via a Las-Vegas algorithm) most functions (the class of *nonsymmetric* functions) including: leader election, XOR and finding the ring size. The same technique can be applied to prove the impossibility of partitioning an odd size ring into a maximal number of pairs.

Keywords: Algorithms; Anonymous rings; Message terminating algorithms; Orientation

1. Introduction

Ring networks have traditionally been used as simple frameworks for evaluating distributed computation and communication systems. The ring topology can be used to demonstrate the implication of symmetry on the performance and feasibility of certain distributed tasks.

In this work we consider rings of an unknown number of indistinguishable processors that communicate by messages sent over bidirectional links (*anonymous rings*). We use an asynchronous model in which message delivery time over a link is arbitrarily long but finite. Algorithms for such asynchronous systems are generally message driven in the sense that a processor acts (changes its state, sends messages, performs computations, etc.) only upon the reception of a message. At all other times the processor is idling. We focus on *message terminating* algorithms, i.e., the algorithm terminates when no more messages are present in the system (within buffers or in transit at the transmission lines) and no processor is at a state from which it may initiate a message. As was shown in [9,10], the processors may lack the ability to recognize the termination of the algorithm and it might be detected only by an outside observer. The stronger property of *processor termination* (PT) where at least one of the processors can detect the termination of the algo-

* Corresponding author. Email: shavitt@tx.technion.ac.il.

[1] Currently with Sun Microsystems Labs, Mt. View, CA 94043, USA.

SSDI 0020-0190(94)00237-1

rithm is not achievable for most non-trivial problems in anonymous rings of unknown size. Attiya, Snir, and Warmuth [5] prove that no (deterministic) PT algorithm exists even for "simple" functions such as OR and AND. In fact, their proof can be easily extended for probabilistic PT algorithms as well.

Most of the algorithmic work in the area of anonymous networks has concentrated on models where some knowledge of the size of the network is known in advance (see [4,1,12]). In the absence of the ring size knowledge it was shown in [10] that functions such as computing the size of the ring or leader election can be computed by a probabilistic message terminating algorithm with some (arbitrarily small) error probability (Monte-Carlo algorithm). These results were extended in [17] for general topology networks.

In this paper we focus on message terminating algorithms for anonymous rings of unknown size that terminate correctly, either deterministically or with probability 1, while the average communication and time complexities are kept bounded. To the best of our knowledge this is the first time that non-trivial problems are solved under this model. However, most problems can not be solved under this model. We prove impossibility results for a large class of problems (the class of nonsymmetric problems). It is interesting to observe that if the model is changed to a known ring size, then some of the problems which are unsolvable in our model (such as XOR) can be solved as efficiently [5] as the problems we solve here (such as orientation). In other words, there are cases where the partition between solvable and unsolvable problems (in our model) completely vanishes (even in terms of different solution complexities) under the known ring size model.

We present a deterministic orientation algorithm for a ring of unknown size that uses link markings (similar to [8]) to break symmetry and has a communication complexity of $O(n \log^2 n)$ bits ($O(n \log n)$ messages) and time complexity of $O(n)$. Pachl [13] shows a matching lower bound for the message complexity for rings of unknown size with distinct identities. For the link marking we assume the existence of a daemon that marks each link with "1" on one side and "0" on the other side. We show how this daemon can be replaced by coin tossing to yield a Las-Vegas orientation algorithm, i.e., an algorithm that terminates correctly with probability 1 and maintains bounded average communication and time complexities. Interestingly, the Las-Vegas orientation algorithm has the same average bit and time complexities as the deterministic one. Another Las-Vegas algorithm is presented here for partitioning an even size ring to neighboring pairs (maximum matching).

Itai and Rodeh [9,10] present a message terminating Monte-Carlo algorithm that computes the ring size in $O(rn^3)$ messages of $O(\log n)$ bits, and an error probability of $O(2^{-nr/2})$. Note, that if the error probability is taken to zero (or r is taken to infinity) the message and time complexities approach infinity for any n. Other distributed Monte-Carlo algorithms can be found in [4,11].

We present an impossibility result for a class of tasks, termed *nonsymmetric* problems, by showing that they cannot be solved under the Las-Vegas model. Two of the problems in this class were shown to be unsolvable in the past: finding the ring size by Itai and Rodeh [9] and solitude detection (leader election) by Abrahamson et al. [2]. Other examples of nonsymmetric problems (which are the majority of the problems) are XOR and partitioning an odd size ring into a maximum number of pairs (maximum matching).

2. Orientation algorithms

Consider a ring of unknown number of anonymous processors. Each processor (node) has a local notion of a left and a right link which is termed the *orientation* of the node. Two neighboring nodes have the same orientation if the link connecting them is considered to be right at one of them and left at the other. Throughout the paper when we use directions, left or right, they are given according to the local orientation of the node we refer to or according to a common local orientation of a referred group of nodes. Our aim is to coordinate all the processors to have the same orientation. The fact that processors are anonymous creates a symmetry that prohibits a deterministic solution (see [3]). We overcome this impossibility by employing symmetry breaking link markings that enable neighboring processors to act deterministically. In section 2.4 we show how the link markings can be avoided and replaced by coin tossing.

In the course of the algorithm each node i is a member of a *segment* of consecutive nodes with the same

orientation and keeps a local variable called $length_i$ that specifies its relative position (left to right) in the segment. The leftmost node in the sequence (the tail) has *length* = 1, its right neighbor has *length* = 2, etc. Therefore, a segment is a sequence of adjacent nodes with the same orientation that satisfies: (1) The tail has *length* = 1. (2) If $length_i \neq 1$ then $length_i = length_{left(i)}+1$. (3) For the right most node (the head): $length_{right(i)} \neq length_i + 1$ OR $orientation_{right(i)} \neq orientation_i$. The *size* of a segment is defined as the *length* of its head.

2.1. General description

When a node wakes up, it determines an arbitrary orientation, forms a single node segment by setting *length* = 1, and sends the message RIGHT(1) over its right link. Upon the reception of a RIGHT(k) message from the left neighbor, the node does nothing except for recording the value $k+1$ in the variable *l_from_left*. Consequently, if all nodes initially decide on the same orientation, each node will receive a RIGHT(1) message over its left link and the algorithm terminates. However, if a node (which is in general the head of a segment) receives a RIGHT message over its right link, it learns that the node on its right has a conflicting orientation, and one of them must flip its orientation. A contest to resolve which node changes orientation (the loser) will be described shortly. The node that lost the contest reverses its orientation and joins the new segment by setting its variable *length* to be one higher than that of the winning node. After joining the new segment, the loser becomes the new head of the segment and spear-heads the algorithm by sending a RIGHT message with the new length to its new right neighbor.

The winner of the contest is the node heading the longer segment. In case of a tie, a symmetry breaking marking for each link dictates the winner. One exception for this procedure is when the node has *length* = 1. As was previously described, a node with *length* = 1 that receives a RIGHT(k) message on its left link, saves the length ($k+1$) of the segment on its left in the variable *l_from_left*. In this case (only), if a segment from its right will try to capture it, the node might join the segment on its left (and will become its head). The decision which segment to join depends on the length of the two conflicting segments.[2] The algorithm eventually stops when all RIGHT messages arrive over left links.

2.2. Formal description

Each node uses the following variables: *length* – a node's position in a segment (from the left). *l_from_left* – used only when *length* = 1, and records the potential position of the node in the segment on its left, in case it will join it. *state* – the state of the node, *asleep* or *awake*.

Messages that are sent by the algorithm: WAKE_UP – an initialization message received from a higher level. RIGHT(l) – a message sent by a node over its right link, that contains its position in its segment (from left).

The algorithm is given in Fig. 1. Initially, all nodes have *state* = *asleep*.

2.3. Correctness and complexity

First, we show that the algorithm always terminates with a complete orientation of the ring. Then we analyze the message and time complexities of the algorithm. In order to save space we only state the main theorems and lemmas and omit some of the proofs. The missing parts can be found in [6].

Theorem 1 (Cidon and Shavitt [6]). *The algorithm terminates within finite number of messages. Upon termination, all nodes are awake and have the same orientation.*

Lemma 2 (Greene and Knuth [7]). *Let $F(m)$ be a discrete function with the following recursive definition:*

$$F(1) = 1,$$

$$F(m) = \max_{1 \leqslant i < m} \{F(i) + F(m-i) + \min\{i, m-i\}\}$$
$$= \max_{1 \leqslant i \leqslant m/2} \{F(i) + F(m-i) + i\}.$$

[2] This can be viewed as if the node queues the message from the left until it is captured by the segment from the right and then changes orientation and reacts to the message from its new right that causes it to change orientation again. In this scenario one extra message is sent. We term this version "the basic algorithm" and use it in some of the following proofs.

```
for WAKE_UP
⟨W.0⟩  set state ← awake; l_from_left ← −1
⟨W.1⟩  set length ← 1
⟨W.2⟩  Send RIGHT(length) on right link

for RIGHT(l) /* A message is received with parameter l */
⟨R.0⟩  if state = awake then
⟨R.1⟩    if received on right link then
⟨R.2⟩      if (l > length) OR (l = length AND NOT SYM_BREAK(right link)) then
⟨R.3⟩        if ((length = 1) AND (l_from_left > l OR
               (l_from_left = l AND SYM_BREAK(right link))) ) then
             /* join the long segment at your left */
⟨R.4⟩          length ← l_from_left
⟨R.5⟩          Send RIGHT(length) on right link
⟨R.6⟩        end
⟨R.7⟩        else /* the contest is lost - join the segment at your right */
⟨R.8⟩          change orientation
⟨R.9⟩          length ← l + 1
⟨R.10⟩         Send RIGHT(length) on right link
⟨R.11⟩       end
⟨R.12⟩   else /* A message is received on left link */
⟨R.13⟩     l_from_left ← l + 1
⟨R.14⟩ else /* node is asleep */
⟨R.15⟩   set link on which the message is received to be the left one
⟨R.16⟩   length ← l + 1
⟨R.17⟩   Send RIGHT(length)
⟨R.18⟩ end
```

Fig. 1. The orientation algorithm - A formal description.

Then for $m \geqslant 1$

$$F(m) = \begin{cases} 2F(\frac{m}{2}) + \frac{m}{2} \\ \quad \textit{for even } m, \\ F(\frac{m-1}{2}) + F(\frac{m+1}{2}) + \frac{m-1}{2} \\ \quad \textit{for odd } m. \end{cases}$$

Lemma 3 (Cidon and Shavitt [6]).

(a) *For all natural* k, $F(m) = m(1+\frac{1}{2}\log_2 m)$ *where* $m = 2^k$.

(b) $F(m) \leqslant m(1+\frac{1}{2}\log_2 m)$ *for all* $m > 2$.

Lemma 4. $F(m)$, *as defined in Lemma* 2, *is the maximum number of messages* [3] *that may be sent for creating a segment of size* m.

Proof. Let $G(m)$ be the maximum number of messages sent while a segment of size m is formed. Clearly $G(1) = 1$, since segments of size 1 are only formed when a node wakes up and sends a single message.

A segment of size m, $m > 1$ can be formed in one of the following three ways.

A segment of size $m-1$ sends a RIGHT message that wakes up a node which is *asleep*. That node sends one message as it joins the segment. The number of messages sent in this scenario is at most $G(m-1)+1$.

A segment of size i and a segment of size $m-i$ exchange RIGHT messages and the bigger one captures the other. The number of messages sent in this scenario is at most $G(i) + G(m-i) + \min\{i, m-i\}$. This is true since each processor in the captured segment changes orientation and sends a single message

[3] All the messages that are sent by the nodes of the segment from the moment they wake up until (and including) the RIGHT(m) message is sent are counted.

(lines ⟨R.8⟩–⟨R.10⟩ in Fig. 1). Note that if a segment of size $m+1-i$ captures a segment of size i except for its leftmost node (which joins its left side segment instead), the number of messages for forming a segment of size m takes only $G(m+1-i)+G(i)+i-1$. However, this situation should be viewed as if the segment grows to length $m+1$ and shrinks back, and indeed, the segment will eventually be captured by the bigger one from the left.

A segment of size $m-1$ is growing when the tail of the segment to its right (that has the same orientation) decides to join him (instead of joining the smaller winning segment on its right), i.e., a segment of size one with the same orientation merges with it. The number of messages sent in this scenario is at most $G(m-1)+G(1)+1$.

Therefore, we can bound $G(m)$ by the maximum of the above results:

$$
\begin{aligned}
&G(1) = 1\\
&G(m) \leqslant \max\{[G(m-1)+1],\\
&\qquad \max_{1\leqslant i<m}\{G(i)+G(m-i)\\
&\qquad\qquad +\min\{i, m-i\}\},\\
&\qquad [G(1)+G(m-1)+1]\}
\end{aligned}
$$

which yields

$$
G(m) \leqslant \max_{1\leqslant i<m}\{G(i)+G(m-i)+\min\{i, m-i\}\}.
$$

Therefore, $G(m) \leqslant F(m)$. □

Theorem 5. *The algorithm for a ring of size n terminates after no more than* $n(1+\frac{1}{2}\log_2 n)$ *messages are sent.*

Proof. By Lemma 4, $F(m)$ is an upper bound for the number of messages exchanged to form a segment of size m. Assume that the algorithm terminates when there are $k \leqslant n$ segments of sizes $m_1, m_2, \ldots, m_k$, where $m_1+m_2+\cdots+m_k = n$. If $k = 1$ the result follows. If $k > 1$ then the total number of messages sent is less or equal than

$$
\begin{aligned}
&F(m_1)+F(m_2)+\cdots+F(m_k)\\
&\quad \leqslant m_1(1+\frac{1}{2}\log m_1)+\cdots+m_k(1+\frac{1}{2}\log m_k)\\
&\quad \leqslant n+\frac{1}{2}(m_1+m_2+\cdots+m_k)\\
&\qquad \times \log(m_1+m_2+\cdots+m_k)\\
&\quad = n(1+\frac{1}{2}\log_2 n). \qquad \square
\end{aligned}
$$

For the purpose of time complexity analysis, we assume that a message is delivered after at most one time unit. In the basic algorithm, each node sends a message when it wakes up. We call the situation where two nodes send messages to each other on the same link a *conflict*. It is important to notice that a conflict can be created only when a node wakes up. After a conflict is created, one of the nodes changes its orientation and sends a message on its other link. This can lead to a conflict on that link and we shall say that the conflict *moves* one hop. Otherwise, we say that the conflict was resolved.

Lemma 6 (Cidon and Shavitt [6]). *In the basic orientation algorithm, delaying an incoming message, cannot cause any message to be sent earlier from this node.*

Lemma 7. *If all nodes are awakened together, after k time units there are no conflicts between segments that are both of size less than k.*

Proof. Using Lemma 6, for the worst case, we assume that messages always incur the maximal delay of a single time unit.

We prove the lemma by an induction on the integer k. After one time unit, all segments are of length 1, and the lemma holds. We assume that the hypothesis holds for all time values less or equal to $k-1$, and prove for k.

Assume that at time k there are two conflicting segments of sizes $s_1 \geqslant s_2$, respectively. If the two segments were already at conflict at time $k-1$, then at that time the larger among them had a size of s_1-1 and the other had a size of s_2+1 (at time k $s_1 > s_2$ for this case and the larger segment always absorbs the smaller segment). Given that the hypothesis holds at time $k-1$, it must be that $s_1 \geqslant k$. If the two segments were not in a conflict at time $k-1$ then at least one of them has been in a conflict at time $k-1$ with a segment of size 1 (in order for them to be in a direct conflict at time k). Therefore, by the hypothesis

either $s_1 - 1 \geqslant k - 1$ or $s_2 - 1 \geqslant k - 1$. □

Corollary 8. *If all nodes are awakened together, the algorithm terminates after no more than n time units.*

A simple addition to the algorithm enables termination for a ring of size n after no more than $\lceil 3n/2 \rceil$ time units. Every node that receives a message for the first time (wakes up) sends immediately a wake-up message on the other link (on both links). It is clear that after $\lceil n/2 \rceil$ time units all the processors are awakened, and the extra cost is only $2n$ messages. Using Lemma 6, from this time on the algorithm cannot terminate later than an algorithm that is executed over an identical ring where all the nodes are awakened together (by Lemma 7, it takes at most n time units). Thus, the algorithm terminates after $\lceil 3n/2 \rceil$ time units.

Another simple version of the algorithm suggested by one of our anonymous reviewers, performs the above orientation algorithm without the use of the *length* field. The link markings are used to determine the orientation of the links. Two types of ties are possible: two links that point to a node (*sink*) or two links that point away from a node (*source*). A sink node chooses an arbitrary direction, and sends a message to flip the links in that side of it until the next source node. This algorithm improves the bit complexity by a factor of $\log n$ but possesses a time complexity of $O(n \log n)$.

2.4. A Las-Vegas orientation algorithm

The orientation algorithm presented above, uses a deterministic function to break symmetry among adjacent nodes. Consequently, it requires some predefined consistent input for each pair of neighboring nodes. These predefined markings can be replaced by a probabilistic tie breaking procedure. In order to break symmetry among neighbors, each node tosses a fair coin and sends the result to its competing neighbor. If they both toss the same value, another round of coin tossing is performed, until exactly one of the nodes gets "1". The expected number of rounds for such a contest process is $\sum_{i=1}^{\infty} i \cdot (\frac{1}{2})^i = 2$. Therefore, the expected message complexity for the probabilistic orientation algorithm remains $O(n \cdot \log n)$. Similar to its deterministic counterpart, the probabilistic algorithm is partially correct, i.e., it outputs the correct result for every finite execution [9]. It message terminates with probability 1, and therefore it constitutes a message terminating Las-Vegas algorithm.

3. Partitioning an even size ring into pairs

We assume a bidirectional un-oriented ring with an unknown but even number of anonymous processors. We present a maximum matching algorithm for this ring.

The algorithm operates in phases: In each phase, a node sends and receives a single message over both links. (We delay messages which arrive out of phase until the next phase starts, and there can be at most one such outstanding message per node.) Nodes are either *single* or *married*. Only *single* nodes initiate the communication of the next phase. Two messages are used: *invite* and *reject*. At the beginning of a phase (or upon wake-up) a *single* node randomly selects one of its links, marks it as *candidate*, sends an *invite* message over that link and sends a *reject* message over the other link. If it receives an *invite* message over the *candidate* link, it marks the link as a *spouse* and becomes *married*. Otherwise, it waits until it has received a message over both links and starts a new phase. A *married* node only forwards the messages it gets to the opposite direction. In the case that both messages of the same phase are *invite*, the *married* node swaps its *spouse*, i.e., it removes the *spouse* marking from one of the links and marks the other as *spouse*. The change of the *spouse* marking shifts the matches of all the couples between two single nodes and repartitions these nodes and the two single nodes into neighboring couples. If all nodes are *married* after a phase completes, the algorithm terminates as no processor initiates a new phase.

We turn to the cost analysis of the presented algorithm. At each phase a single node becomes married with probability 1/2. Therefore, on the average half of the single nodes become married after each phase. Consequently, it is easy to show that the average number of phases is logarithmic in the number of nodes. Each phase requires exactly one message over every link in each direction, which totals to $O(n \cdot \log n)$ messages. Since there are only two message types (*invite* and *reject*), the communication bit complexity is also $O(n \cdot \log n)$.

The above algorithm for partitioning an even size ring to pairs can be generalized to partitioning a ring of size km to m groups of k neighboring nodes.

3.1. Formal description

As in the previous section each node has a local orientation. We denote the left (right) link by the Boolean value "0" ("1"). Consequently, if the Boolean variable x contains the left (right) link identity then its complement $\bar{x}$ holds the opposite link identity.

The algorithm is given in Fig. 2.

The following procedures are used by the algorithm: *Receive*(m, l) – Writes in m the type of message that is at the head of the queue l and removes the message from the queue. If the queue is empty *Receive* first waits for a message arrival. *Random* – returns a random Boolean value (with equal probabilities).

Each node uses the following variables: cs – the current *candidate/spouse* link. *state* – the state of the node, *single* or *married*. $m1$ and $m2$ – the type of the received messages at queues 1 and 2. Initially all nodes have *state* = *asleep*.

Messages that are sent or received by the algorithm: WAKE_UP – an initialization message received from a higher level. *invite*, *reject* – as explained above.

4. Impossibility results

Let $f : \Sigma^* \to T$ be a function computed on anonymous rings defined over some alphabet Σ. f is *symmetric* if for every string $s \in \Sigma^*$ and for every natural k, $f(s) = f(s^k)$. Otherwise f is *nonsymmetric*. (It is easy to realize that most functions f are nonsymmetric.)

An algorithm is *partially correct* if it outputs the correct result for every finite execution. Itai and Rodeh [9] prove the impossibility of calculating the ring size when the processors are anonymous, and the algorithm is partially correct. In the sequel we shall extend this proof in two directions. First we prove that the ring size cannot be calculated by algorithms that have bounded bit complexity and are partially correct with probability 1, where in [9] algorithms that err with probability 0 were not considered. Second we generalize this to all *nonsymmetric* functions.

Examples for *nonsymmetric* functions are leader election, XOR and computing the ring size. For XOR, $f(s) \neq f(s^k)$ whenever s contains an odd number of 1s and k is even. For computing the ring size, $f(s)$ never equals $f(s^k)$ if $k > 1$. For leader election there are no input values (except for the size) and the function return value is a bit that tells each processor whether it is the leader, it is clear that the vector $\vec{f}(s^k)$ never equals the concatenation of the k vectors of $\vec{f}(s)$.

The proof is constructed for a synchronous algorithm and thus holds for asynchronous algorithms as well.

Theorem 9. *There is no algorithm for computing a nonsymmetric function in a ring of unknown number of anonymous processors that is partially correct with probability* 1 *and its average bit complexity is bounded.*

Proof. We assume to the contrary that such an algorithm exists and show a contradiction. Let $\mathcal{A}$ be such an algorithm for computing the function f in a ring with an unknown number of anonymous processors, and let E be the average number of bits sent by the algorithm. We examine a ring with n processors $(p_1, p_2, \ldots, p_n)$ with inputs $s = (s_1, s_2, \ldots, s_n)$. Let $f_i(s)$ be the value that processor p_i holds when the algorithm (message) terminates for inputs s, let $\vec{f}(s) = (f_1(s), f_2(s), \ldots, f_n(s))$, and let $\vec{f}^k(s) = (\vec{f}(s), \vec{f}(s), \ldots, \vec{f}(s))$ be the concatenation of k output vectors $\vec{f}(s)$. Select s and k such that $\vec{f}^k(s) \neq \vec{f}(s^k)$, where $\vec{f}(s^k)$ is the output vector for a ring of size kn with inputs s^k (k concatenations of the vector s). We select an execution [4] $\mathcal{R}$ of positive (greater than zero) probability that terminates after a finite number of bits were sent, and yields $\vec{f}(s)$ as an output vector. We now show that such $\mathcal{R}$ with probability greater than zero exists. By definition $E = \sum_{i=1}^{\infty} ip(i)$, where $p(i)$ is the probability that $\mathcal{A}$ terminates after i bits were sent. Applying the Markov inequality (see [16]) we get $\sum_{i \geqslant 2E} p(i) \leqslant \frac{1}{2}$, and thus $\sum_{i \leqslant 2E} p(i) \geqslant \frac{1}{2}$. Since the number of executions that uses at most $2E$ bits is finite (recall that we are dealing with a synchronous model here) we can

[4] An execution is defined by the messages that are sent (received) and by their transmission (reception) times.

```
for WAKE_UP or message reception and state = asleep
⟨W.1⟩  cs ← Random
⟨W.2⟩  send invite on link cs
⟨W.3⟩  send reject on link c̄s
⟨W.4⟩  state ← single

for a message arrival on link l
⟨M.1⟩  if state = asleep then
⟨M.2⟩    do WAKE_UP procedure
⟨M.3⟩  if state = married then
⟨M.4⟩    Receive(m1, l)
⟨M.5⟩    Send(m1, l)
⟨M.6⟩    Receive(m2, l̄)
⟨M.7⟩    Send(m2, l̄)
⟨M.8⟩    if m1 = m2 = invite then
⟨M.9⟩      cs ← c̄s
⟨M.10⟩ if state = single then
⟨M.11⟩   receive(m1, cs)
⟨M.12⟩   receive(m2, c̄s)
⟨M.13⟩   if m1 = invite then
⟨M.14⟩     state ← married
⟨M.15⟩   else
⟨M.16⟩     cs ← Random
⟨M.17⟩     Send invite on link cs
⟨M.18⟩     Send reject on link c̄s
```

Fig. 2. The partitioning algorithm – A formal description.

deduce that at least one such execution has a positive probability termed ε.

Examine a system of k rings each of n nodes and an input vector s. All the rings are stochastically independent. Since the probability space of this system is the Cartesian product of k identical probability spaces of the ring discussed before, the probability for $\mathcal{R}$ to be executed simultaneously at all the rings is ε^k.

Now cut all the above rings at the same place, say between processors p_i and p_{i+1}. Then, connect all the k strips into a ring of kn processors such that every processor p_i of ring j is connected to processor p_{i+1} of ring $j+1$ (modulo k): $(p_{i+1}^1, \ldots, p_n^1, p_1^1, \ldots, p_i^1, p_{i+1}^2, \ldots, p_i^2, p_{i+1}^3, \ldots, p_i^k)$. Since the processors are anonymous there is no way for a processor to tell if it is in the system of k rings that each one of them has $\mathcal{R}$ executed at, or whether it is in a ring of kn nodes that has k "copies" of $\mathcal{R}$ executed at its k sections. The probability space of the concatenated ring and the k ring system is identical. All the events in the probability space that cause simultaneous execution in the k ring system cause also simultaneous execution of k copies of $\mathcal{R}$ at the concatenated ring and yields $\vec{f}^k(s) = (\vec{f}(s), \vec{f}(s), \ldots, \vec{f}(s))$ as output. These events are selected with the same probabilities at both systems. Therefore, the probability to get $\vec{f}^k(s)$ as output in the concatenated ring is at least ε^k. □

A direct corollary of this theorem is that deterministic algorithms for nonsymmetric functions do not exist.

The rationale for our restriction to algorithms with bounded average bit complexity can be demonstrated by the following simple algorithm. Each node selects a real number in the range (0..1). Since the probability for two nodes to choose the same real number is zero the ring's nodes possess a unique identities with probability 1, a model that was studied in depth in the literature (see [14], [15, Chapter 2, Section 5], and

the references therein). Leader election can now be easily performed with $O(n \log n)$ messages but each one of them carry an infinite number of bits.

5. Concluding remarks

We presented message terminating algorithms for the problems of ring orientation and partitioning an even size ring into pairs. An algorithm for the problem of General Pattern Searching (GPS) can be found in [6]. Simple implementation of this algorithm can be used to compute the functions OR and AND (a search for a "1" or a "0", respectively) with $O(n)$ bit and time complexity.

Some problems are more difficult to describe in terms of functions. However our impossibility result still holds for such problems if they possess an asymmetric behavior. Such examples are: partitioning a ring of size $n \neq km$ to a maximal number of groups of k neighboring nodes; evaluating the size of the longest sequence of consecutive "1", where in the case that all inputs are "1" this translates into finding the ring size (which was also proved in [9]).

Acknowledgment

The authors are thankful to the anonymous reviewers for their constructive comments and suggestions that helped to improve the presentation of the paper.

References

[1] K. Abrahamson, A. Adler, L. Higham and D. Kirkpatrick, Randomized function evaluation on a ring, in: J. van Leeuwen, ed., *Proc. 2nd Internat. Workshop on Distributed Algorithms* Lecture Notes in Computer Science **312** (Springer, Berlin, 1987) 324–331.

[2] K. Abrahamson, A. Adler, L. Higham and D. Kirkpatrick, Optimal algorithms for probabilistic solitude detection on anonymous rings, Tech. Rept. TR 90-3, University of British Columbia, 1990.

[3] D. Angluin, Local and global properties in networks of processes, in: *Proc. 12th Ann. ACM symp. on Theory of Computing* (1980) 82–93.

[4] H. Attiya and M. Snir, Better computing on the anonymous ring, *J. Algorithms* **12** (2) (1991) 204–238.

[5] H. Attiya, M. Snir and M.K. Warmuth, Computing on the anonymous ring, *J. ACM* **35** (4) (1988) 845–875.

[6] I. Cidon and Y. Shavitt, Message terminate algorithms for rings of unknown size, EE Pub. 793, Dept. of Electrical Engineering, Technion – Israel Institute of Technology, Haifa 32000, Israel, 1991.

[7] D.H. Greene and D.E. Knuth, *Mathematics for the Analysis of Algorithms* (Birkhauser, Basel, 2nd ed., 1982).

[8] A. Israeli and M. Jalfon, Uniform self-stabilizing ring orientation, *Inform. and Comput.* **104** (2) (1993) 175–196.

[9] A. Itai and M. Rodeh, Symmetry breaking in distributed networks, in: *Proc. 22nd Ann. IEEE Symp. of Foundations of Computer Science* (1981) 150–158.

[10] A. Itai and M. Rodeh, Symmetry breaking in distributed networks, *Inform. and Comput.* **88** (1) (1990) 60–87.

[11] Y. Matias and Y. Afek, Simple and efficient election algorithms for anonymous networks, in: *Proc. 3rd Internat. Workshop on Distributed Computing*, Lecture Notes on Computer Science **392** (Springer, Berlin, 1989) 183–194.

[12] S. Moran and M.K. Warmuth, Gap theorems for distributed computation, in: *Proc. 5th Ann. ACM Symp. on Principles of Distributed Computing* (1986) 141–150.

[13] J.K. Pachl, A lower bound for probabilistic distributed algorithms, *J. Algorithms* **8** (1987) 53–65.

[14] J. Pachl, E. Korach and D. Rotem, Lower bounds for distributed maximum-finding algorithms, *J. ACM* **31** (4) (1984) 905–918.

[15] M. Raynal, *Distributed Algorithms and Protocols* (Wiley, New York, 1988), translated from French.

[16] S.M. Ross, *Probabilities Models* (Academic Press, New York, 3rd ed., 1985).

[17] B. Schieber and M. Snir, Calling names on nameless networks, in: *Proc. 8th Ann. ACM Symp. on Principles of Distributed Computing* (1989) 319–328.