A $\sqrt{N}$ Algorithm for Mutual Exclusion in Decentralized Systems

MAMORU MAEKAWA
University of Tokyo

An algorithm is presented that uses only $c\sqrt{N}$ messages to create mutual exclusion in a computer network, where N is the number of nodes and c a constant between 3 and 5. The algorithm is symmetric and allows fully parallel operation.

Categories and Subject Descriptors: D.4.1 [**Operating Systems**]: Process Management—*mutual exclusion*; C.2.1 [**Computer Systems Organization**]: Network Architecture and Design—*network communications* C.2.4 [**Computer Systems Organization**]: Distributed Systems—*network operating systems*

General Terms: Algorithms, Design, Performance

Additional Key Words and Phrases: Computer networks, decentralized systems

1. INTRODUCTION

Proposed is an algorithm that uses only $c\sqrt{N}$ messages to create mutual exclusion in a computer network, where N is the number of nodes and c a constant between 3 and 5. It is assumed that the nodes communicate only by messages and do not share memory. An error-free underlying communications network supports message transfers in which transit times may vary but messages between two nodes are delivered in the order sent.

The creation of mutual exclusion in a computer network under distributed control is not trivial. Ricart and Agrawala [8] proposed an algorithm that uses $2(N - 1)$ messages: $(N - 1)$ messages to convey a request to all other nodes and $(N - 1)$ messages to obtain permissions from them. It is thus based on a unanimous consensus rule. The algorithm requires that each node requesting mutual exclusion communicate to all other nodes. It is a distributed algorithm, in the sense that each node always bears an equal amount of responsibility to control mutual exclusion and that each node is required to perform an equal amount of work to obtain mutual exclusion, such as the number of request messages. The voting technique used in Thomas [11] is based on a majority consensus rule and requires that a node requesting mutual exclusion obtain a permission vote from only a majority of the nodes. Thus, in the best case, the

Author's address: Department of Information Science, Faculty of Science, University of Tokyo, 7-3-1 Hongo, Bunkyo-ku Tokyo, 113 Japan.

number of permission messages required to obtain mutual exclusion is reduced to a half, $N/2$. It is also a distributed algorithm in the above sense. The approach was extended by Gifford [5] and Skeen [10] to allow nodes to cast more than one vote. In these weighted voting schemes, it was sufficient to obtain a majority of the votes to obtain mutual exclusion, not necessarily from a majority of the nodes. Garcia-Molina and Barbara then analyzed the relationship between weighted voting and sets of nodes with pairwise nonnull intersections [4]. These weighted voting schemes enjoy the same advantage as the protocol proposed in this paper, in that communication with all nodes in the system is not required. They are not distributed algorithms, however, because nodes with higher weights bear more responsibility to control mutual exclusion than others. In fact, if a particular node has a full weight and all others have no weight, the algorithm is reduced to a centralized control.

The algorithm presented in this paper is a distributed algorithm and requires only $3\sqrt{N}$ messages per mutual exclusion: $\sqrt{N}$ messages to convey a request, $\sqrt{N}$ messages to obtain permissions, and $\sqrt{N}$ messages to release mutual exclusion. It can be proven that this number is optimal for distributed algorithms. The approach taken parallels the voting technique used in Thomas. It also uses *deferral*, the technique used in Ricart and Agrawala. An additional technique, *relinquishment*, is used, however, to avoid deadlocks.

2. REQUEST RESOLUTION

In distributed systems, each network node issues a mutual exclusion request at an arbitrary time. In order to arbitrate these requests, any pair of two requests must be known to one of the arbitrators. Since nodes themselves must serve as arbitrators, any pair of two requests must reach to a certain common node. If we assume that node i obtains a permission from each member of a subset S_i of the nodes of the network to obtain mutual exclusion then there must exist at least one common node between a pair of S_i and S_j for any i and j so that the common node can serve as an arbitrator. Therefore, the S_i's must satisfy the pairwise nonnull intersection property. Assuming that the network consists of N nodes numbered from 1 to N, this nonnull intersection property is stated as follows:

(a) For any combination of i and j, $1 \leq i, j \leq N$, $S_i \cap S_j \neq \varnothing$.

The request resolution rule then requires that when node i attempts to invoke mutual exclusion, it send a REQUEST message to every member of S_i and obtain a permission from all of them. Since each member of S_i serves as an arbitrator, the requesting node knows that it is the only node that has been granted mutual exclusion, when every member of S_i returns a permission message. Node S_i then proceeds to its critical section. This nonnull intersection property is a necessary condition for the S_i's so that mutual exclusion requests can be resolved. In addition, the following properties are required or desirable for truly distributed algorithms:

(b) S_i, $1 \leq i \leq N$, always contains i.
(c) The size of S_i, $|S_i|$, is K for any i. That is,

$$|S_1| = |S_2| = |S_3| = \cdots = |S_N| = K.$$

(d) Any j, $1 \leq j \leq N$, is contained in the D S_i's, $1 \leq i \leq N$.

Property (b) is included simply to reduce the number of messages to be sent and received by a node, respectively, because, if a requesting node i is itself a member of its own node subset S_i, a permission from itself is obtained without a message transmission. Properties (c) and (d) are included to have a truly distributed algorithm. Property (c) implies that each node needs to send and receive the same number of messages to obtain mutual exclusion. Property (d), on the other hand, implies that each node serves as an arbitrator for the same number of nodes. That is, each node bears an equal amount of responsibility for mutual exclusion control.

A centralized algorithm assigns a single node as a controller (arbitrator) for mutual exclusion management. It satisfies properties (a) and (c), where $K = 1$, but violates property (d). Ricart and Agrawala's algorithm satisfies all of the above properties, where $K = N$ and $D = N$. Thomas's majority consensus algorithm can also satisfy all the above properties, where $K = N$ and $D = N$. Weighted voting schemes satisfy property (a) but usually violate properties (c) and (d).

3. THE CHOICE OF S_i's

The selection of S_i's is not unique. There exists a number of ways to select a set of S_i's that satisfies the above properties. From properties (b) and (d), each member of S_i can be contained in $(D - 1)$ other subsets. Therefore, the maximum number of subsets that satisfy property (a) is given by

$$(D - 1)K + 1.$$

Since N is desired to be set to this maximum number so that K is minimized for a given N, we have

$$N = (D - 1)K + 1.$$

Furthermore, $K = D$ must always hold, because N is the number of distinct members, which is given by KN/D, the total number of members divided by the number of duplications of each member. N is thus related to K by

$$N = K(K - 1) + 1.$$

The problem of finding a set of S_i's that satisfies these conditions is equivalent to finding a finite projective plane of N points. It is known that there exists a finite projective plane of order k if k is a power p^m, of a prime p [1]. This finite projective plane has $k(k + 1) + 1$ points. Hence, in our terms, a set of S_i's exists if $(K - 1)$ is a power of a prime. For other values of k, we can create a set of S_i's by relaxing conditions (c) and (d) to some extent. For values of N, which cannot be expressed as $K(K - 1) + 1$, we can also apply the same method to create a degenerated set of S_i's. The creation of S_i's is discussed in detail in Section 7. Here, we only show examples for $K = 2$, 3, 4 and 5 (Figure 1).

From the above discussion, it is clear that K gives the optimal value for a given N when all the properties (a)–(d) are required. With a fractional error, we see that $K = \sqrt{N}$.

S_1	=	}1,	2{
S_3	=	}1,	3{
S_2	=	}2,	3{

(a)

S_1	=	}1,	2,	3{
S_4	=	}1,	4,	5{
S_6	=	}1,	6,	7{
S_2	=	}2,	4,	6{
S_5	=	}2,	5,	7{
S_7	=	}3,	4,	7{
S_3	=	}3,	5,	6{

(b)

S_1	=	}1,	2,	3,	4{
S_5	=	}1,	5,	6,	7{
S_8	=	}1,	8,	9,	10{
S_{11}	=	}1,	11,	12,	13{
S_2	=	}2,	5,	8,	11{
S_6	=	}2,	6,	9,	12{
S_7	=	}2,	7,	10,	13{
S_{10}	=	}3,	5,	10,	12{
S_3	=	}3,	6,	8,	13{
S_9	=	}3,	7,	9,	11{
S_{13}	=	}4,	5,	9,	13{
S_4	=	}4,	6,	10,	11{
S_{12}	=	}4,	7,	8,	12{

(c)

S_1	=	}1,	2,	3,	4,	5{
S_6	=	}1,	6,	7,	8,	9{
S_{10}	=	}1,	10,	11,	12,	13{
S_{14}	=	}1,	14,	15,	16,	17{
S_{18}	=	}1,	18,	19,	20,	21{
S_2	=	}2,	6,	10,	14,	18{
S_7	=	}2,	7,	11,	15,	19{
S_8	=	}2,	8,	12,	16,	20{
S_9	=	}2,	9,	13,	17,	21{
S_{11}	=	}3,	6,	11,	17,	20{
S_3	=	}3,	7,	10,	16,	21{
S_{13}	=	}3,	8,	13,	15,	18{
S_{12}	=	}3,	9,	12,	14,	19{
S_{15}	=	}4,	6,	12,	15,	21{
S_4	=	}4,	7,	13,	14,	20{
S_{17}	=	}4,	8,	10,	17,	19{
S_{16}	=	}4,	9,	11,	16,	18{
S_{19}	=	}5,	6,	13,	16,	19{
S_5	=	}5,	7,	12,	17,	18{
S_{21}	=	}5,	8,	11,	14,	21{
S_{20}	=	}5,	9,	10,	15,	20{

(d)

Fig. 1. Subsets of integers with pairwise nonnull intersection property. (a) $K = 2$; (b) $K = 3$; (c) $K = 4$; (d) $K = 5$

4. ALGORITHM

Each node executes an identical algorithm. The algorithm is based on the fact that, if node i locks all members of S_i, no other node can capture all its members because of property (a). Therefore, when it invokes mutual exclusion, node i tries to lock all members of S_i. If it succeeds, it can enter its critical section. If it fails, it waits for all its member nodes to be freed, at which point it captures and locks them. It then enters its critical section. Since there is a danger of deadlock when more than one node simultaneously requests mutual exclusion, a node will yield to others if the priority of its request is lower than that of any other conflicting request. The request's priority is determined by the sequence number (timestamp) of the request's corresponding REQUEST message. A REQUEST with a smaller sequence number is given higher priority and is said to *precede* other REQUESTs with larger sequence numbers. If a newly arrived REQUEST at a member node precedes the current locking REQUEST, the node sends an INQUIRE message to the node originating the current locking REQUEST to inquire whether the originating node will really succeed in capturing all its members. The originating node will return a RELINQUISH message when it becomes apparent that the node will not be able to capture all its members. On the other hand, if the originating node has succeeded in capturing all its members, it will return a RELEASE message only after it has completed its critical section operation.

The algorithm is now described below:

(1) When node i invokes mutual exclusion, it sends a REQUEST message to every member of S_i. Node i pretends to have received a REQUEST. The REQUEST message is given a sequence number greater than any REQUEST message sent, received, or observed at this node.

(2) Upon receiving a REQUEST, a member node of S_i marks itself *locked* for the REQUEST if it is not currently locked for another REQUEST, and then returns a LOCKED message to the requesting node i. If the node is locked for a REQUEST from another node, the REQUEST from node i is placed in the WAITING QUEUE of the node. (These REQUEST messages placed in the WAITING QUEUE are called *outstanding REQUESTs*.) It is then tested to determine whether the current locking REQUEST or any other outstanding REQUEST at the node precedes the received REQUEST. (See below for the definition of the *locking REQUEST*.) If so, a FAILED message is returned to node i. Otherwise, an INQUIRE message is sent to the node originating the current locking REQUEST to inquire whether this originating node has succeeded in locking all its members. If an INQUIRE has already been sent for a previous REQUEST and its reply message (either RELINQUISH or RELEASE) has not yet been received, it is not necessary to send in INQUIRE. REQUEST A is said to precede REQUEST B if (the sequence of number $A <$ the sequence number of B) or ((the sequence of number $A =$ the sequence number of B) and (the node number of $A <$ the node number of B)). Each node can be locked by only one REQUEST at a time, and this REQUEST is called the locking REQUEST. Any subsequent REQUESTs arrived at the node are placed in the WAITING QUEUE of the node in decreasing order of the precedence defined above.

(3) When a node receives an INQUIRE message, it returns a RELINQUISH message if it knows that it will not succeed in locking all its members; that is, it has received a FAILED message from some of its members. By so doing, the node relinquishes its member node to a more preceding REQUEST. This breaks a circular locking, which is necessary to avoid deadlocks. The node cancels the LOCKED message previously received from the member node. When the node has succeeded in locking all its members and is in its critical section, it returns a RELEASE message, but only after

it has completed its critical section. If an INQUIRE message has arrived before it is known whether the node will succeed or fail to lock all its members, a reply is deferred until this becomes known. If an INQUIRE message has arrived after the node has sent a RELEASE message, it is simply ignored.

(4) When a node receives a RELINQUISH message, it relieves itself of the current locking REQUEST and then locks itself for the most preceding REQUEST in the WAITING QUEUE. Thus, regardless of which REQUEST had caused the sending of an INQUIRE, the node is locked for the REQUEST that happens to be most preceding when a RELINQUISH message is received. The current locking REQUEST is placed in the WAITING QUEUE, whereas the most preceding REQUEST is removed from it. A LOCKED message is then returned to the node originating the new locking REQUEST.

(5) If all members of S_i have returned a LOCKED message, node i enters its critical section.

(6) Upon completing the critical section, node i sends a RELEASE message to each member of S_i.

(7) When a node receives a RELEASE message, it relieves itself from the current locking REQUEST. It deletes this locking REQUEST and then relocks itself for the most preceding REQUEST in the WAITING QUEUE if the queue is not empty. A LOCKED message is returned to the node originating the new locking REQUEST. If the WAITING QUEUE is empty, the node marks itself *unlocked.*

(8) The above steps (1)–(7) are repeated for each mutual exclusion request.

5. AN EXAMPLE

Imagine a 13-node network using this algorithm. Initially, the sequence number at each node is zero.

Figure 2a shows a sequence of mutual exclusion invocations in which nodes 7, 8, and 11 invoke mutual exclusion in the order below. They all send a REQUEST message with a sequence number 1 to their respective members.

(1) Node 11 is the first to attempt mutual exclusion. Its REQUESTs have arrived at nodes 12 and 13 and have locked them, but its REQUEST to node 1 is still on its way.

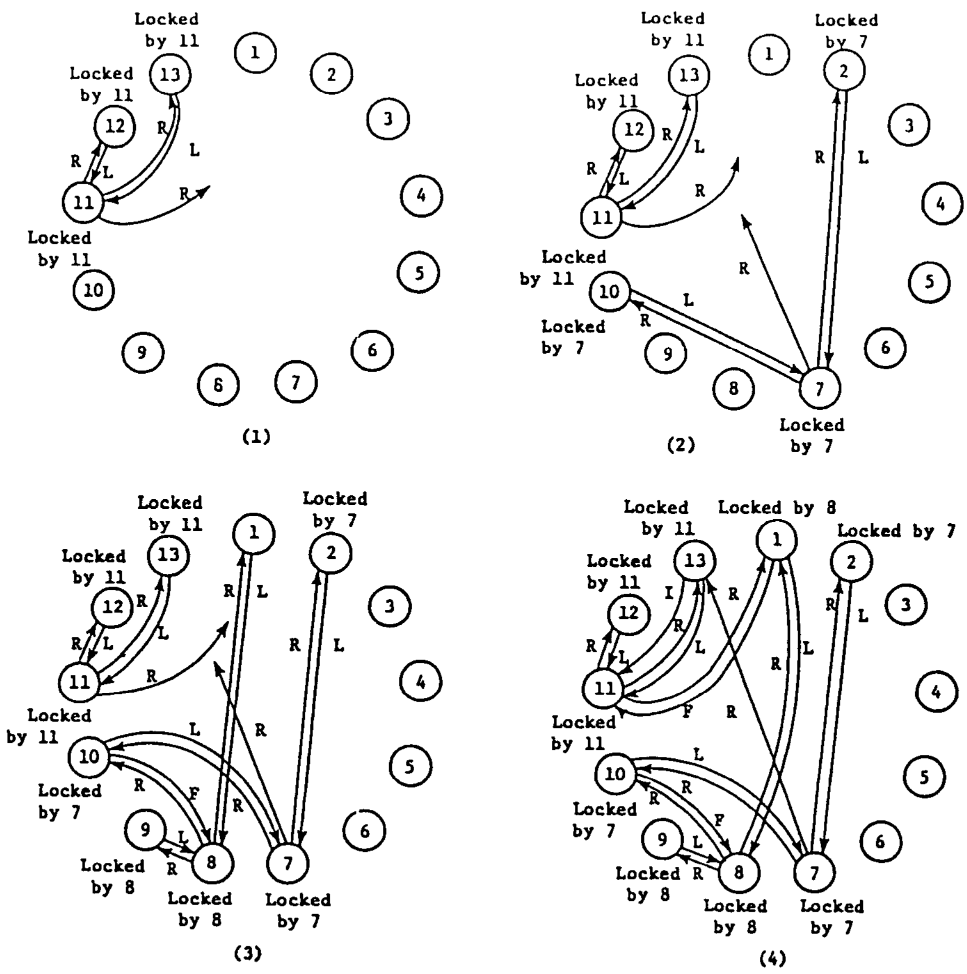
(2) Node 7 then invokes mutual exclusion. Its REQUESTs have arrived at nodes 2 and 10 and have locked them but its REQUEST to node 13 is still on its way.

(3) Node 8 then invokes mutual exclusion. It locks itself and sends a REQUEST to nodes 1, 9, and 10 but fails to lock node 10 because node 10 has already been locked by a preceding REQUEST from node 7.

(4) The REQUEST message originating at node 11 has finally arrived at node 1, while the REQUEST message from node 7 arrives at node 13. Node 1 then returns a FAILED, whereas node 13 sends an INQUIRE message to node 11.

This sequence creates a situation where nodes 7, 8, and 11 circularly lock each other. Node 8 receives a FAILED message and cannot enter its critical section. Likewise, node 11 cannot enter its critical section because it receives a FAILED message from node 1. Node 7 still waits because it has not received a LOCKED from all its member nodes.

When an INQUIRE message has been received at node 11, node 11 knows that it cannot enter its critical section and thus returns a RELINQUISH message to node 13. This will cause node 13 to be released for the most preceding REQUEST in its waiting queue, which is the REQUEST from node 7. This REQUEST then locks node 13 and returns a LOCKED to node 7. Node 7 then can enter its critical section (Figure 2b).



S_1	=	{1,	2,	3,	4}
S_2	=	{2,	5,	8,	11}
S_3	=	{3,	6,	8,	13}
S_4	=	{4,	6,	10,	11}
S_5	=	{1,	5,	6,	7}
S_6	=	{2,	6,	9,	12}
S_7	=	{2	7,	10,	13}
S_8	=	{1,	8,	9,	10}
S_9	=	{3,	7,	9,	11}
S_{10}	=	{3,	5,	10,	12}
S_{11}	=	{1,	11,	12,	13}
S_{12}	=	{4,	7,	8,	12}
S_{13}	=	{4,	5,	9,	13}

Fig. 2a. Circular locking. R = Request; L = Locked; F = Failed; I = Inquire; Q = Relinquish.

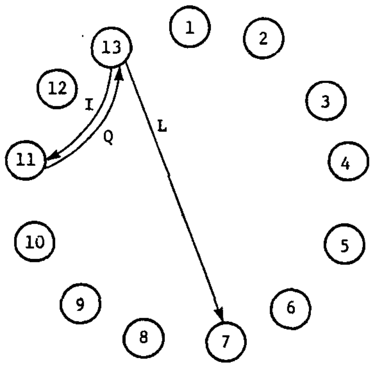


Fig. 2b. Relinquishing.

Upon completing the critical section, node 7 deletes its REQUEST from its member nodes by sending a RELEASE message. This will cause node 8 to successfully lock all its members and enter its critical section. Finally node 11 completes its critical section.

It is possible that a new REQUEST is initiated during the above process. Suppose that a REQUEST from node 3 has arrived at node 13 after the INQUIRE message was sent but before the RELINQUISH message from node 11 arrives at node 13. Since this REQUEST precedes any REQUEST at node 13, and since it is known that an INQUIRE was sent, the REQUEST waits for a RELINQUISH. When the RELINQUISH message is received at node 13, the REQUEST from node 3 locks node 13 instead of the REQUEST from node 7. Node 3 will then succeed in locking all its members when node 8 relinquishes itself to node 3.

6. PROOF

6.1 Mutual Exclusion

Assume the contrary, that more than one node are simultaneously in the critical section. The following arguments show that this is not possible:

(1) All the nodes in the critical section must have received a LOCKED message from all their respective member nodes (step 5).

(2) Since a node in a critical section never releases its member nodes until it completes its critical section (step (6)), and since each member node returns a LOCKED message only when it locks itself for the corresponding REQUEST (steps (2) and (4)), there must be a node that is simultaneously locked for more than one REQUEST owing to property (a).

(3) However, this contradicts the specification of the algorithm that allows only one REQUEST to lock a node at any instance (steps (2) and (4)).

(4) Therefore, more than one node cannot simultaneously be in the critical section.

6.2 Deadlock

Assume that deadlock is possible. Then there must exist a circular waiting among the nodes requesting mutual exclusion. This is not possible, however, because