RATAN NALUMSU * AND GANESH GOPALAKRISHNAN **

ratan@cup.hp.com, ganesh@cs.utah.edu

Cupertino Systems Lab Department of Computer Science
Heuillet-Packard University of Utah
Cupertino, CA, 95014 Salt Lake City, UT, 84112

Deriving Efficient Cache Coherence Protocols through Refinement

Revised April 30, 1999

Editor: Dominique Méry and Beverly Sanders

Abstract. We address the problem of developing efficient cache coherence protocols for use in distributed systems implementing distributed shared memory (DSM) using message passing. A serious drawback of traditional approaches to this problem is that the users are required to state the desired coherence protocol at the level of asynchronous message interactions involving request, acknowledge, and negative acknowledge messages, and handle unexpected messages by introducing intermediate states. Proofs of correctness of protocols described in terms of low level asynchronous messages are very involved. Often the proofs hold only for specific configurations and buffer allocations. We propose a method in which the users state the desired protocol directly in terms of the desired high-level effect, namely synchronization and coordination, using the synchronous rendezvous construct. These descriptions are much easier to understand and computationally more efficient to verify than asynchronous protocols due to their small state spaces. The rendezvous protocol can also be synthesized into efficient asynchronous protocols. In this paper, we present our protocol refinement procedure, prove its soundness, and provide examples of its efficiency. Our synthesis procedure applies to large classes of DSM protocols.

Keywords: Refinement, DSM protocols, Communication protocols.

1. Introduction

With the growing complexity of concurrent systems, automated procedures for developing protocols are growing in importance. In this paper, we are interested in protocol refinement procedures, which we define to be those that accept high-level specifications of protocols, and apply provably correct transformations on them to yield detailed implementations of protocols that run efficiently and have modest buffer resource requirements. Such procedures enable correctness proofs of protocols to be carried out with respect to high-level specifications, which can considerably reduce the proof effort. Once the refinement rules are shown to be sound, the detailed protocol implementations need not be verified. Also, if the refinement rules apply for a family of protocols, then case-specific proofs can be avoided.

In this paper, we address the problem of producing correct and efficient cache coherence protocols used in distributed shared memory (DSM) parallel computing systems. DSM systems have been widely researched in the academia as the next logical step in parallel processing [2,11,13]. High-end workstation manufacturers also have introduced DSM systems lately [4] thus providing added confirmation to the growing importance of DSM. A central problem in DSM systems is the design and implementation of distributed coherence protocols for shared cache lines using message passing [8]. The present-day approach to this problem consists of specifying the detailed interactions possible between computing nodes in terms of low-level requests, acknowledgments, negative acknowledgments, and dealing with “unexpected” messages. Difficulty of designing these protocols is compounded by the fact that verifying such low-level descriptions invites state explosion (when done using model-checking [5,6]) or tedious (when done using theorem-proving [19]) even for simple configurations. Often these low-level descriptions are model-checked for specific resource allocations (e.g. buffer sizes); it is often not known what would happen when these allocations are changed. Protocol refinement can

* The author was a student at University of Utah when the research was done. This research was supported in part by Graduate Fellowship from University of Utah.

** Supported in part by DARPA under contract #DABT6396C0094 (Utah Verifier), and NSF grant CCR-9800928
help alleviate this situation considerably. Our contribution in this paper is a protocol refinement procedure which can be applied to derive a large class of DSM cache protocols.

Most of the problems in designing DSM cache coherence protocols are attributable to the apparent lack of atomicity in the implementation behaviors. Although some of the designers of these protocols may begin with a simple atomic-transaction view of the desired interactions, such a description is seldom written down. Instead, what gets written down as the “highest level” specification is a detailed protocol implementation which was arrived at through ad hoc reasoning of the situations that can arise. In this paper, we choose CSP [9] as our specification language to allow the designers to capture their initial atomic-transaction view. The atomic-transaction protocol is then subjected to syntax-directed translation rules to modify the rendezvous communication primitives of CSP into asynchronous communication primitives yielding an efficient detailed implementation. We refer to the atomic-transaction view as rendezvous protocol and the detailed implementation as asynchronous protocol. We empirically show that the rendezvous protocols are, several orders of magnitude more efficient to model-check than their corresponding detailed implementations. In addition, we also show that in the context of a state of the art DSM machine project called the Avalanche [2], our procedure can automatically produce protocol implementations that are comparable in quality to hand-designed asynchronous protocols, where quality is measured in terms of (1) the number of request, acknowledge, and negative acknowledge (nack) messages needed for carrying out the rendezvous specified in the given specification, and (2) the buffering requirements to guarantee a precisely defined and practically acceptable progress criterion.

The rest of the paper is organized as follows. Section 2 presents related past work done on the derivation of protocols in related domains. Section 3 presents the structure of typical DSM protocols in distributed systems. Section 4 presents our syntax-directed translation rules, along with an important optimization called request/reply. Section 5 presents an informal argument that the refinement rules we present always produce correct result, and also points to a formal proof of correctness done using PVS [18]. Section 6 presents an example protocol developed using the refinement rules, and the efficiency of model-checking the rendezvous protocol compared to the efficiency of model-checking the asynchronous protocol. Section 7 presents a discussion on buffering requirements of the refined protocol and its impact on the forward progress made by the asynchronous protocol. Section 8 concludes the paper.

2. Related Work

Chandra et al [3] use a model based on continuations to help reduce the complexity of specifying the coherency protocols. The specification can then be model-checked and compiled into an efficient object code. In their approach, the protocol is still specified at a lower level than in our approach. Although rendezvous communication can be modeled, they do not provide an algorithm for handling unexpected messages received in transient states. A simple algorithm for this is provided in our work. In our approach, a user writes protocols using only the rendezvous primitive. Verification of the protocol at this level causes much less state explosion. The verified protocol can then be compiled into an efficient asynchronous protocol or object code. The automatic introduction of intermediate protocol states to handle unexpected messages can free a designer of a potentially very error-prone step. Our refinement algorithm also incorporates a buffer reservation scheme that guarantees forward progress in most practical situations.

Our work somewhat resembles that of Buckley and Silberschatz [1]. Buckley and Silberschatz consider the problem of implementing rendezvous using message-passing when the processes use generalized input/output guard. However, since the focus of their problem is for general-purpose implementation of rendezvous software, their solution is too expensive for DSM multiprocessor protocol implementations. In contrast, we focus on restrictions on the specification language such as allowing only star configurations of processes and restricting the allowed types of alternative commands to allow us to automatically synthesize asynchronous DSM protocols that handle intermediate states, deadlocks, and forward progress with much greater efficiency. The restrictions imposed on our specification language (a subset of CSP), while permitting efficient handling of these issues, do not, in our experience, stifle the expressiveness.

Gribomont [7] explored protocols where the rendezvous communication can be simply replaced by asynchronous communication without affecting the processes in any other way. In contrast, we show how to change the processes when the rendezvous communication is replaced by asynchronous communication.
Lamport and Schneider [12] have explored the theoretical foundations of comparing atomic transactions (e.g., rendezvous communication) and split transactions (e.g., asynchronous communication), based on left and right movers [14], but have not considered specific refinement rules such as we do.

The DSM protocols synthesized by our refinement procedure are similar to those employed in many modern DSM processors such as [2,11,13] where full-map directories are employed. Our refinement procedure does not currently generate protocols similar to those used in DSM systems where the full directory information is not kept (e.g., [17] and the ANSI/IEEE Std 1596-1992 Scalable Coherent Interface, or SCI).

3. Cache Coherency in Distributed Systems

In directory based cache coherent multiprocessor systems, the coherency of each line of shared memory is managed by a CPU node, called home node, or simply home. All nodes that may access the shared line are called remote nodes. The home node is responsible for managing access to the shared line by all nodes without violating the coherency policy of the system. A simple protocol used in Avalanche, called migratory, is shown in Figures 3 and 4.

The remote nodes and home node engage in the following activity. Whenever a remote node R wishes to access the information in a shared line, it first checks if the data is available (with required access permissions) in its local cache. If so, R uses the data from the cache. If not, it sends a request for permissions to the home node of the line. The home node may then contact some other remote nodes to revoke their permissions in order to grant the required permissions to R. Finally, the home node grants the permissions (along with any required data) to R. As can be seen from this description, a remote node interacts only with the home node, while the home node interacts with all the remote nodes. This suggests that we can restrict the communication topology of interest to a star configuration, with the home node as the hub, without losing any descriptive power. This decision helps synthesize more efficient asynchronous protocols, as we shall see later.

3.1. Complexity of Protocol Design

As already pointed out, most of the problems in the design of DSM protocols can be traced to lack of atomicity. For example, consider the following situation. A shared line is being read by a number of remote nodes. One of these remote nodes, say R1, wishes to modify the data, hence sends a request to the home node for write permission. The home node then contacts all other remote nodes that are currently accessing the data to revoke their read permissions, and then grants the write permission to R1. Unfortunately, it is incorrect to abstract the entire sequence of actions consisting of contacting all other remote nodes to revoke permissions and granting permissions to R1 as an atomic action. This is because when the home node is in the process of revoking permissions, a different remote node, say R2, may wish to obtain read permissions. In this case, the request from R2 must be either nacked or buffered for later processing. To handle such unexpected messages, the designers introduce intermediate states, also called transient states, leading to the complexity of the protocols. On the other hand, as we will show in the rest of the paper, if the designer is allowed to state the desired interactions using an atomic view, it is possible to refine such a description using a refinement procedure that introduces transient states appropriately to handle such unexpected messages.

3.2. Communication Model

We assume that the network that connects the nodes in the systems provides reliable, point-to-point in-order delivery of messages. This assumption is justified in many machines, e.g., DASH [13], and Avalanche [2]. We also assume that the network has infinite buffering, in the sense that the network can always accept new messages to be delivered. Without this assumption, the asynchronous protocol generated may deadlock. Unfortunately, this assumption is not satisfied in some networks. A solution to this problem that is orthogonal to the refinement process is given by Hennessy and Patterson [8]. They divide the messages into two categories: request and acknowledge. A request message may cause the recipient to generate more messages in order to complete the transactions, while an acknowledge message does not. The authors argue that if
the network always accepts *acknowledge* messages (as opposed to all messages in the case of a network with infinite buffer), such deadlocks are broken. As we shall see in Section 4, the asynchronous protocol has two *acknowledge* messages: ack and nack. Guaranteeing that the network always accepts these two *acknowledge* messages is beyond the scope of this paper.

### 3.3. Methodology

We use rendezvous communication primitives of CSP [9] to specify the home node and the remote nodes to simplify the DSM protocol design. In particular, we use the direct addressing scheme of CSP, where every input statement in process $Q$ is of the form $P ? m(v)$ or $P ? m$, where $P$ is the identity of the process that sent the message, $m$ is an enumerated constant ("message type") and $v$ is a variable (local variable of $Q$) which would be set to the contents of the message, and every output statement in $Q$ is of the form $P ! m(e)$ or $P ! m$ where $e$ is an expression involving constants and/or local variables of $Q$. When $P$ and $Q$ rendezvous by $P$ executing $Q ! m(e)$ and $Q$ executing $P ? m(v)$, we say that $P$ is an active process and $Q$ is a passive process in the rendezvous.

The rendezvous protocol written using this notation is verified using either a theorem prover or a model-checker for desired properties, and then refined using the rules presented in Section 4 to obtain an efficient asynchronous protocol that can be implemented directly, for example in microcode.

### 3.4. Process Structure

We divide the states of processes in the rendezvous protocol into two classes: *internal* and *communication*. When a process is in an internal state, it cannot participate in rendezvous with any other process. However, we assume that such a process will eventually enter a communication state where rendezvous actions are offered (this assumption can be syntactically checked). The refinement process introduces *transient* states where all unexpected messages are handled.

We denote the $i^{th}$ remote node by $r_i$ and the home node by $h$. For simplicity, we assume that all the remote nodes follow the same protocol and that the only form of communication between processes (in both asynchronous and rendezvous protocols) is through messages, i.e., other forms of communication such as global variables are not available.

As discussed before, we restrict the communication topology to a star. Since the home node can communicate with all the remote nodes and behaves like a server of remote-node requests, it is natural to allow generalized input/output guards in the home node protocols (e.g., Figure 1(a)). In contrast, we restrict the remote nodes to contain only input non-determinism, i.e., a remote node can either specify that it wishes to be an active participant of a single rendezvous with the home node (e.g., Figure 1(b)) or it may specify that it is willing to be a passive participant of a rendezvous on a number of messages (e.g., Figure 1(c)). Also, as in Figure 1(c), we allow $\tau$ guards in the remote node to model autonomous decisions such as cache evictions. These decisions, empirically validated on a large number of real DSM protocols, help synthesize more efficient protocols. Finally, we assume that no fairness conditions are placed on the non-deterministic communication options available from a communication state, with the exception of the forward progress restriction imposed on the entire system (described below).

### 3.5. Forward Progress

Assuming that there are no $\tau$ loops in the home node and remote nodes, the refinement process guarantees that at least one of the refined remote nodes makes forward progress, if forward progress is possible in the rendezvous protocol. Notice that forward progress is guaranteed for some remote node, not for every remote node. This is because assuring forward progress for each remote node requires allocating too much buffer space at the home node. If there are $n$ remote nodes, to assure that every remote node makes progress, the home node needs a buffer that can hold $n$ requests. This is both impractical and non-scalable as $n$ in DSM machines can be as high as a few thousands. If we were to guarantee progress only for some remote node, a buffer that can hold 2 messages suffices, as we will see in Section 4. Incidentally, assuring forward progress
for each individual remote node corresponds to strong fairness, and assuring forward progress for at least one remote node corresponds to weak fairness [15].

4. The Refinement Procedures

We systematically refine the communication actions in \( h \) and \( r_i \) by inspecting the syntactic structure of the processes. This refinement algorithm is captured in Tables 1 and 2, and can be directly coded up as syntax-directed translation procedures in any standard programming notation. The technique is to split each rendezvous into two halves: a request for the rendezvous and an acknowledgment (ack) or negative acknowledgment (nack) to indicate the success or failure of the rendezvous. At any given time, a refined process is in one of three states: internal, communication, and transient. Internal and communication states of the refined process are same as in the corresponding unrefined process in the rendezvous protocol. Transient states are introduced by the refinement process in the following manner. Whenever a process \( P \) has \( Q!m(e) \) as one of the guards in a communication state, \( P \) sends a request to \( Q \) and awaits in a transient state for an ack/nack or a request for rendezvous from \( Q \). In the transient state, \( P \) behaves as follows:

R1. If \( P \) receives an ack from \( Q \), the rendezvous is successful, and \( P \) changes its state appropriately.

R2. If \( P \) receives a nack from \( Q \), the rendezvous has failed. \( P \) goes back to the communication state and tries the same rendezvous or a different rendezvous.

R3. If \( P \) receives a request from \( Q \), the action taken depends on whether \( P \) is the home node or a remote node. If \( P \) is a remote node (and \( Q \) is then the home node), \( P \) simply ignores the message. (This is because, as discussed in the next sentence, \( P \) "knows" that \( Q \) will get its request that is tantamount to a nack of \( Q \)'s own request.) If \( P \) is the home node, it goes back to the communication state as though it received a nack ("implicit nack"), and processes the \( Q \)'s request in the communication state.

The rules R1-R3 govern how the remote node and home node are refined, as will now be detailed.

4.1. Refining the Remote Node

Every remote node has a buffer to store one message from the home node. When the remote node receives a request from the home node, the request would be held in the buffer. When a remote node is at a communication or transient state, its actions are shown in Table 1. The rows of the table are explained below.

C1 When the remote node is in a communication state, and it wishes to be an active participant of the rendezvous, and no request from home node is pending in the buffer, the remote node sends a request for rendezvous to home, goes to a transient state and awaits for an ack/nack or a request for rendezvous from home node.
Table 1. The actions taken by the remote node when it enters a communication state or a transient state. After each action, the message in the buffer is removed.

<table>
<thead>
<tr>
<th>Row</th>
<th>State</th>
<th>Buffer contents</th>
<th>Action</th>
</tr>
</thead>
</table>
| C1  | Communication (Active) | empty           | (a) Request for rendezvous  
(b) goto transient state       |
| C2  | Communication (Active) | request         | (a) delete the request  
(b) Request home for rendezvous  
(c) goto transient state       |
| C3  | Communication (Passive) | request         | Ack/nack the request                       |
| T1  | Transient           | ack             | Successful rendezvous                      |
| T2  | Transient           | nack            | go back to the communication state         |
| T3  | Transient           | request         | Ignore the request                         |

C2 This row is similar to C1, except that there is a request from home is pending in the buffer. In this case also, the remote sends a request to home and goes to a transient state. In addition, the request in the buffer is deleted. As explained in R3, when the home receives the remote’s request, it acts as though a nack is received (implicit nack) for the deleted request.

C3 When the remote node is in a communication state, and it is passive in the rendezvous, it waits for a request for rendezvous from home. If the request satisfies any guards of the communication state, it sends an ack to the home and changes state to reflect a successful rendezvous. If not, it sends a nack to home and continues to wait for a matching request. In both cases, the request is removed from the buffer.

T1, T2 If the remote node receives an ack, the rendezvous is successful, and the state of the process is appropriately changed to reflect the completion of the rendezvous. If the remote node receives a nack from the home, it is because the home node does not have sufficient buffers to hold the request. In this case, the remote node goes back to communication state and retransmits the request, and reenters the transient state.

T3 As explained in R3, if the remote node receives a request from home, it simply deletes the request from buffer, and continues to wait for an ack/nack from home.

4.2. Refining the Home Node

The home node has a buffer of capacity \( k \) messages (\( k \geq 2 \)). All incoming messages are entered into the buffer when there is space, with the following exception. The last buffer location (called the progress buffer) is reserved for an incoming request for rendezvous that is known to complete a rendezvous in the current state of the home. If no such reservation is made, a livelock can result. For example, consider the situation when the buffer is full and none of the requests in the buffer can enable a guard in the home node. Due to lack of buffer space, any new requests for rendezvous must be nacked, thus the home node can no longer make progress. In addition, when the home node is in a transient state expecting an ack/nack from \( r_t \), an additional buffer need to be reserved so that a message (ack, nack, or request for rendezvous) from \( r_t \) can be held. We refer to this buffer as ack buffer.

When the home is in a communication or transient state, the actions taken are shown in Table 2. The rows of this table are explained below.

C1 When the home is in a communication state, and it can accept one or more requests pending in the buffer, the home finishes rendezvous by arbitrarily picking one of these messages.
Table 2. Actions taken by the home node when it is in a communication state or transient state.

<table>
<thead>
<tr>
<th>Row</th>
<th>State</th>
<th>Condition</th>
<th>Action</th>
</tr>
</thead>
</table>
| C1  | Communication | buffer contains a request from \( r_i \) that satisfies a rendezvous       | (a) an ack is sent to \( r_i \)  
(b) delete request from buffer |
| C2  | Communication | (a) no request in the buffer satisfies any required rendezvous  
(b) home node can be active in a rendezvous with \( r_i \) on \( m_j \) (i.e. \( r_i/lm_j \) is a guard in this state)  
(c) no request from \( r_i \) is pending in buffer       | (a) ack buffer is allocated  
(if not enough buffer space a nack may be generated)  
(b) a request for rendezvous is sent to \( r_i \)  
(c) goto transient state |
| T1  | Transient | ack from \( r_i \)                                                     | rendezvous is completed                                               |
| T2  | Transient | nack from \( r_i \)                                                | rendezvous failed. Go back to the communication state and send next request. If no more requests left, repeat starting with the first guard. |
| T3  | Transient | (a) request from \( r_i \)  
(b) waiting for ack/nack from \( r_i \) | treat the request as a  
a nack plus a request             |
| T4  | Transient | (a) request from \( r_j \neq r_i \) has arrived  
(b) waiting for ack/nack from \( r_i \)  
(c) buffer has > 2 free entries | enter the request into buffer                                       |
| T5  | Transient | (a) request from \( r_j \neq r_i \) has arrived  
(b) waiting for ack/nack from \( r_i \)  
(c) buffer has 2 free entries  
(d) the request can satisfy a guard in the communication state | enter the request into progress buffer                                |
| T6  | Transient | request from \( r_j \) has arrived (all cases not covered above) | nack the request                                                     |

**C2** If no requests pending in the buffer can satisfy any guard of the communication state, and one of the guards of the communication state is \( r_i/lm_j \), home node sends a request for rendezvous to \( r_i \), and enters a transient state. As described above, before sending the message, it also reserves an additional buffer location, ack buffer, so that forward progress can be assured. This step may require the home to generate a nack for one of the requests in the buffer in order to free the buffer location. Also note that condition (c) states that no request from \( r_i \) is pending in the buffer. The rationale behind this condition is that, if there is a request from \( r_i \) pending, then \( r_i \) is at a communication state with \( r_j \) being the active participant of the rendezvous. Due to the syntactic restrictions placed on the description of the remote nodes, \( r_i \) can't satisfy any requests for rendezvous in this communication state. Hence it is wasteful to send any request to \( r_i \) in this case.

**T1** When the home is in transient state, if it receives an ack, the rendezvous is successful, and the state of the home is modified to reflect the completion of the rendezvous.

**T2** When the home is in transient state, if it receives a nack the rendezvous failed. Hence the home goes back to the communication state. From the communication state, it checks if any new request in the buffer can satisfy any guard of the communication state. If so, an ack is generated corresponding to that request, and that rendezvous is completed. If not, the home tries the next output guard of the communication state. If there are no more output guards, it starts all over again with the first output guard. The reason for this is that, even though a previous attempt to rendezvous has failed, it may now succeed, because the remote node in question might have changed its state through a \( \tau \) guard in its communication state.
T3 When the home is expecting an ack/nack from \( r_i \), if it receives a request from \( r_i \) instead, it uses the implicit nack rule, R3. It first assumes that a nack is received, hence it goes to the communication state, where all the requests, including the request from \( r_i \), are processed as in row T2.

T4 If the home receives a request from \( r_j \), when it is expecting an ack/nack from a different remote \( r_i \), and there is sufficient room in the buffer, the request is added to the buffer.

T5 When the home is in a transient state, and has only two buffer spaces, if it receives a message from \( r_j \), it adds the request to buffer according to the buffer reservation scheme, i.e., the request is entered into the progress buffer iff the request can satisfy one of the guards of the communication state. If the request can't satisfy any guards, it would be handled by row T6.

T6 When a request for rendezvous from \( r_j \) is received, and there is insufficient buffer space (all cases not covered by T4 and T5), home sends a nack to \( r_j \), \( r_j \) would retransmit the message.

4.3. Request/Reply Communication

The generic scheme outlined above replaces each rendezvous action with two messages: a request and an ack. In some cases, it is possible to avoid ack message. An example is when two messages, say \( \text{req} \) and \( \text{repl} \) are used in the following manner: \( \text{req} \) is sent from the remote node to home node for some service. The home node, after receiving the \( \text{req} \) message, performs some internal actions and/or communications with other remote nodes and sends a \( \text{repl} \) message to the remote node. In this case, it is possible to avoid exchanging ack for both \( \text{req} \) and \( \text{repl} \). If statements \( h\text{req}(e) \) and \( h\text{repl}(v) \) always appear together as \( h\text{req}(e); h\text{repl}(v) \) in remote node, and \( r_i\text{repl} \) always appears after \( r_i\text{req} \) in the home node, then the acks can be dropped. This is because whenever the home node sends a \( \text{repl} \) message, the remote node is always ready to receive the message, hence the home node doesn’t have to wait for an ack. In addition, a reception of \( \text{repl} \) by the remote node also acts as an ack for \( \text{req} \). Of course, if the remote node receives a nack instead of \( \text{repl} \), the remote node would retransmit the request for rendezvous.

This scheme can also be used when \( \text{req} \) is sent by the home node and the remote node responds with a \( \text{repl} \). In this case, of course, after receiving \( \text{req} \), the remote node performs local actions only (i.e., no rendezvous actions) and responds with a \( \text{repl} \).

5. Correctness

We argue that the refinement is correct by analyzing the different scenarios that can arise during the execution of the asynchronous protocol. The argument is divided into two parts: (a) all rendezvous that happen in the asynchronous protocol are allowed by the rendezvous protocol, and (b) forward progress is assured for at least one remote node. Note that the forward progress is not assured for any given remote node due to buffer considerations (Section 3.5).

The rendezvous finished in the asynchronous protocol when the remote node executes rows C1, C3, or T1 of Table 1 and the home node executes rows C1 or T1 of Table 2. To see that all the rendezvous are in accordance with the rendezvous protocol, consider what happens when a remote node is the active participant in the rendezvous (the case when the home node is the active participant is similar). The remote node \( r_i \) sends out a request for rendezvous to the home \( h \) and starts waiting for an ack/nack. There are three cases to consider.

1. \( h \) does not have sufficient buffer space. In this case the request is nacked. In this case, no rendezvous has taken place.

2. \( h \) has sufficient buffer space, and it is in either an internal state or a transient state where it is expecting an ack/nack from a different remote node, \( r_j \). In this case, the message is entered into the \( h \)'s buffer. When \( h \) enters a communication state where it can accept the request, it sends an ack to \( r_i \), completing the rendezvous. Clearly, this rendezvous is allowed by the rendezvous protocol. If \( h \) has to send a nack to \( r_i \) later to make some space in buffer by row C2, \( r_i \) would retransmit the request, in which case no rendezvous has taken place.
3. \( h \) has sent a request for rendezvous to \( r_i \) and is waiting for an ack/nack from \( r_i \) in a transient state. (This corresponds to R3 of page 5). In this case, \( r_i \) simply ignores the request from \( h \). \( h \) knows that its request would be dropped. Hence it treats the request from \( r_i \) as a combination of ack for the request it already sent and a request for rendezvous. Thus, this case becomes exactly like one of the two cases above, and \( h \) generates an ack/nack accordingly; hence if an ack is generated it would be allowed by the rendezvous protocol.

As can be seen from this case analysis, an ack is generated only in case 2, and in this case the rendezvous is allowed by the rendezvous protocol.

5.1. PVS proof of correctness

The above argument is formalized with the help of PVS [18] and proved that the refinement rules are safety preserving, i.e., if the a transition is taken in the refined protocol, then it is allowed in the original rendezvous protocol. Such proofs are normally done by establishing a “commuting diagram” as shown in Figure 2. \( A_1 \) and \( A_2 \) are two states in the asynchronous protocol, and \( \text{abs} \) is a function that maps a state in asynchronous protocol into a state in the rendezvous protocol. If the asynchronous protocol has a transition that takes \( A_1 \) to \( A_2 \), then the rendezvous protocol must have a transition that takes \( R_1 = \text{abs}(A_1) \) to \( R_2 = \text{abs}(A_2) \). If \( S_a \) represents the set of states in the asynchronous protocol, \( S_r \) represents the set of states in the rendezvous protocol, \( \rightarrow_a \) represents the set of transitions of the asynchronous protocol, and \( \rightarrow_r \) represents the set of transitions of the rendezvous protocol, the figure can be expressed as:

\[
\forall A_1, A_2 \in S_a : A_1 \rightarrow_a A_2 \Rightarrow \text{abs}(A_1) \rightarrow_r \text{abs}(A_2). \tag{1}
\]

This equation cannot be used directly with the refinement procedure because some of the moves made by asynchronous protocol are invisible; in other words, for some asynchronous transitions, \( \text{abs}(A_1) = \text{abs}(A_2) \). Hence the following equation can be established.

\[
\forall A_1, A_2 \in S_a : A_1 \rightarrow_a A_2 \Rightarrow \text{abs}(A_1) = \text{abs}(A_2) \lor \text{abs}(A_1) \rightarrow_r \text{abs}(A_2). \tag{2}
\]

Establishing Equation 2 constitutes only a partial proof. For example, if \( \text{abs} \) maps every state in \( S_a \) to the same state in rendezvous protocol, then the equation holds, i.e., the equation can be made to hold vacuously by artificially making \( \text{abs}(A_1) = \text{abs}(A_2) \) for every \( A_1 \) and \( A_2 \). Hence the full proof requires establishing that \( \text{abs} \) is not a vacuous function by establishing existence of a function \( \text{aug} \) that maps a state of the rendezvous protocol to a state of the asynchronous protocol satisfying the following conditions, as done in [20].

\[
\text{aug}(R_i) = A_i \tag{3}
\]

\[
\forall R \in S_r : \text{abs}(\text{aug}(R)) = R \tag{4}
\]

\[
\forall R_1, R_2 \in S_r : R_1 \rightarrow_r R_2 \Rightarrow \text{aug}(R_1) \rightarrow_a^+ \text{aug}(R_2) \tag{5}
\]

\( R_i \) and \( A_i \) are the initial states of the rendezvous protocol and the asynchronous protocols respectively, and \( \rightarrow_a^+ \) represents a sequence of one or more transitions from \( \rightarrow_a \). Equation 3 states that \( \text{aug} \) maps the initial

![Figure 2. Commute Diagram](attachment:commute_diagram.png)
state of the rendezvous protocol to the initial state of the asynchronous protocol, Equation 4 states that abs
is inverse of aug, and Equation 5 states that every transition of the rendezvous protocol is imitated by a
sequence of transitions in the asynchronous protocol. In other words, Equation 2 shows that every transition
allowed under asynchronous protocol is also allowed under the rendezvous protocol, Equation 5 shows that
every transition of rendezvous protocol is mimicked by a sequence of transitions in the asynchronous protocol,
and Equations 3 and 4 are sanity checks to ensure that aug and abs are consistent with each other.

5.1.1. Construction of abs To construct abs satisfying Equation 2, it is necessary to characterize $S_\alpha$.
One possible characterization of $S_\alpha$ is simply obtained from the syntactic description, i.e., $S_\alpha$ contains all
reachable as well as unreachable states. Using such a simple characterization, it is not possible to construct
a abs satisfying Equation 2 other than the trivial function that maps every state in $S_\alpha$ to the same state.
Hence the following inductive invariant is used as $S_\alpha$.

1. At any given time there is at most one ack towards any node.
2. Every remote node has at most one pending rendezvous transaction at any time, i.e., no remote node
   sends more than one request for rendezvous to home until a response (ack or nack) is received from home.
3. The home node has at most one pending rendezvous transaction at any given time, i.e., home node
   never sends a request for rendezvous until a response (ack, nack, or implicit nack) is received for the last
   rendezvous request.

Using these constraints, abs can be constructed as follows.

1. All requests for rendezvous in the medium and buffers are discarded by abs. If a request for rendezvous
   from a process P is discarded, the state of P is modified from transient state back to the communication
   state, i.e., abs modifies the system as though the request was never sent.
2. If there is an ack towards a process P, the ack is discarded, and the state of P is modified to the state
   which P would attain after consuming the ack.
3. All nacks in the medium and buffers are also discarded. If a nack sent to P is discarded, the state of P
   is changed from transient state back to the communication state.

Using the higher-order functions available in PVS, it is shown that $\rightarrow_\alpha$ as defined by Tables 1 and 2, along
with the above abs function satisfies Equation 2. The PVS theory files and proofs can be obtained from [16].

5.1.2. Construction of aug Given a state $R \in S_\alpha$, aug($R$) is obtained by adding empty communication
channels to $R$. The initial state of the asynchronous protocol, $A_\alpha$, is defined as aug($r_1$), hence proving
Equation 3 is trivial. Similarly, proving Equation 4 is also trivial as it involves simply expanding the
definitions of abs and aug. To prove Equation 5, the following strategy is used. If the transition that
takes $R_1$ to $R_2$ is an internal transition, then the same transition shows that aug($R_1$) $\rightarrow_\alpha^+$ aug($R_2$). If the
transition is a rendezvous transition with a remote node $r_i$ as the active participant and the home node,
h, as the passive participant, then the sequence (a) $r_i$ sending a request for rendezvous, (b) h receiving
the request and sending an ack, and (c) $r_i$ receiving the ack shows aug($R_1$) $\rightarrow_\alpha^+$ aug($R_2$). Similarly, if the
transition is a rendezvous transition with a remote node $r_i$ as the active participant and the home node,
h, as the active participant, then the sequence (a) h sending a request for rendezvous, (b) $r_i$ receiving the
request and sending an ack, and (c) h receiving the ack shows aug($R_1$) $\rightarrow_\alpha^+$ aug($R_2$).

5.2. Proof of forward progress

To see that at least one of the remote nodes makes forward progress, we observe that when the home node h
makes forward progress, one of the remote nodes also makes forward progress. Since we disallow any process
to stay in internal states forever, from every internal state h eventually reaches a communication state from
which it may go to a transient state. Note that because of the same restriction, when h sends a request
to a remote node, the remote would eventually respond with an ack, nack, or a request for rendezvous. If any forward progress is possible in the rendezvous protocol, we show that $h$ would eventually leave the communication or the transient state by the following case analysis.

1. $h$ is in a communication state, and it completes a rendezvous by row C1 of Table 2. Clearly, progress is being made.

2. $h$ is in a communication state, and conditions for row C1 and C2 of Table 2 are not enabled. $h$ continues to wait for a request for rendezvous that would enable a guard in it. Since a buffer location is used as progress buffer, if progress is possible in the rendezvous protocol, at least one such request would be entered into the buffer, which enables C1.

3. $h$ is in a communication state, row C2 of Table 2 is enabled. In this case, $h$ sends a request for rendezvous, and goes to transient state. Cases below argue that it eventually makes progress.

4. $h$ is in a transient state, and receives an ack. By row T1 of Table 2, the rendezvous is completed, hence progress is made.

5. $h$ is in a transient state, and receives a nack (row T2 of Table 2) or an implicit nack (row T3 of Table 2). In response to the nack, the home goes back to the communication state. In this case, the progress argument is based on the requests for rendezvous that $h$ has received while it was in the transient state, and the buffer reservation scheme. If one or more requests received enable a guard in the communication state, at least one such request is entered into the buffer by rows T4 or T5. Hence an ack is sent in response to one such request when $h$ goes back to the communication state (row C1), thus making progress. If no such requests are received, $h$ sends request for rendezvous corresponding to another output guard (row C2) and reenters the transient state. This process is repeated until $h$ makes progress by taking actions in C1 or T1. If any progress is possible, eventually either T1 would be enabled, since $h$ keeps trying all output guards repeatedly, or C1 would be enabled, since $h$ repeatedly enters communication state repeatedly from T2 or T3, and checks for incoming requests for rendezvous. So, unless the rendezvous protocol is deadlocked, the asynchronous protocol makes progress.

6. Example Protocol

We take the rendezvous specification of migratory protocol of Avalanche and show how the protocol can be refined using the refinement rules described above. (The architectural team of Avalanche had previously developed the asynchronous migratory protocol without using the refinement rules described in this paper.) The protocol followed by the home node is shown in Figure 3, and the protocol followed by the remote nodes is shown in Figure 4. Initially the home node starts in state F (free) indicating that no remote node has access permissions to the line. When a remote node $r_i$ needs to read/write the shared line, it sends a req message to the home node. The home node then sends a gr (grant) message to $r_i$ along with data. In addition, the home node also records the identity of $r_i$ in a variable o (owner) for later use. Then the home node goes to state E (exclusive). When the owner no longer needs the data, it may relinquish the line (LR message). As a result of receiving the LR message, the home node goes back to F. When the home node is in E, if it receives a req from another remote node, the home node revokes the permissions from the current owner and then grants the line to the new requester. To revoke the permissions, it either sends an inv (invalidate) message to the current owner o and waits for the new value of data (obtained through ID (invalid done) message), or waits for a LR message from o. After revoking the permissions from the current owner, a gr message is sent to the new requester, and the variable o is modified to reflect the new owner.

The remote node initially starts in state I (invalid). When the CPU tries to read or write (shown as rw in the figure), a req is sent to the home node for permissions. Once a gr message arrives, the remote node changes the state to V (valid) where the CPU can read or write a local copy of the line. When the line is evicted (for capacity reasons, for example), a LR is sent to the home node. Or, when another remote node attempts to access the line, the home node may send an inv. In response to inv, an ID (invalid done) is sent to the home node and the line reverts back to the state I.
To refine the migratory protocol, we note that the messages req and gr can be refined using the request/reply strategy. This is because the remote node after sending a req message immediately waits for a gr message from the home node. The home node, on the other hand, after receiving a req message, either sends a gr message (resulting in state change from F to E) or may have to contact a remote node and then send a gr message (resulting in a state change from E back to E, via E-I1-I3-E or E-I1-I2-I3-E). Similarly, the messages inv and ID can be refined using request/reply, except that in this case inv is sent by the home node, and the remote node responds with an ID. By following the request/reply strategy, a pair of consecutive rendezvous such as r_i?req; r_i!gr or r_i!inv; r_i?ID (data) takes only 2 messages as in Figures 5 and 6.

The refined home node is shown in Figure 5 and the refined remote node is shown in Figure 6. In these figures, the operators "??" and "!!" are used instead of "?" and "!" to emphasize that the communication is asynchronous. In both these figures, transient states are shown as dotted circles (the dotted arrows are explained later). As discussed in Section 4.2, when the refined home node is in a transient state, if it receives a request from the process from which it is expecting an ack/nack, it would be treated as a combination of a nack and a request. To emphasize this, we write [nack] to imply that the home node has received the nack as either an explicit nack message or an implicit nack. Again, as discussed in Section 4.2, when the home node doesn't have sufficient number of empty buffers, it nacks the requests, irrespective of whether the node is in an internal, transient, or communication state. For the sake of clarity, we left out all such nacks other than the one on transient state (labeled r(x)?msg/nack).

As explained in Section 4.1, when the remote node is in a transient state, if it receives a message from the home node, the remote node ignores the message; no ack/nack is ever generated in response to this request. In Figure 6, we showed this as a self loop on the transient states, labeled h??

The asynchronous protocol designed by the Avalanche design team differs from the protocol shown in Figures 5 and 6 in that in their protocol the dotted lines are τ actions, i.e., no ack is exchanged after an LR message. We believe that the loss of efficiency due to the extra ack is small. We are currently in the process of quantifying the efficiency of the asynchronous protocol designed by hand and the asynchronous protocol obtained by the refinement procedure.
Efficiency

As can be expected, verifying of the rendezvous protocols is much simpler than verifying the asynchronous protocol. We verified the rendezvous and asynchronous versions of the migratory protocol above and invalidate, another DSM protocol used in Avalanche, using the SPIN [10] model-checker. The properties verified were deadlock freedom (for all cases), at most one non-invalid copy (for migratory), and only one exclusive/dirty copy (for invalidate). The number of states visited by SPIN on these two protocols is shown in Figure 3. The complexity of verifying the hand designed migratory or invalidate is comparable to the verification of asynchronous protocol. As can be seen, verifying of the rendezvous protocol generates far fewer states and takes much less run time than verifying the asynchronous protocol. In fact, the rendezvous migratory protocol could be model-checked for up to 64 nodes using 32MB of memory, while the asynchronous protocol can be model-checked for only two nodes using 64MB of memory. Currently we are developing a simulation environment to evaluate the performance of the various asynchronous protocols.

7. Buffer Requirements and Fairness

In Section 3.5, we mentioned that the refinement process preserves forward progress for at least one remote node, but doesn’t guarantee forward progress for any given remote node. This means that, it is possible that one of the nodes may starve. For example, a request for a rendezvous from a remote node might be continually nacked by the home node. This problem can be solved if the size of the buffer in the home node is $n$, where $n$ is the number of the remote nodes. In this case, the home node never generates a nack. If the messages in the home node’s buffer are processed in a fair manner, one can show that no remote node is starved.

However, this requires too much memory to be reserved for buffers. For example, in a multiprocessor with 64 nodes, if each node of the multiprocessor acts as home for 1024 lines (a modest number of lines), the node needs to reserve a total of 64K messages to be used as buffer space. Clearly, it is impractical to reserve such
Table 3. Number of states visited and time taken in seconds for reachability analysis of the rendezvous and asynchronous versions of the migratory and invalidate protocols. All verifications were limited to 64MB of memory. N represents the number of nodes.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>N</th>
<th>Asynchronous protocol</th>
<th>Rendezvous protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migratory</td>
<td>2</td>
<td>2336/2.84</td>
<td>54/0.1</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Unfinished</td>
<td>235/0.4</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>Unfinished</td>
<td>965/0.5</td>
</tr>
<tr>
<td>Invalidate</td>
<td>2</td>
<td>193389/19.23</td>
<td>546/0.6</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Unfinished</td>
<td>18696/2.3</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>Unfinished</td>
<td>228234/18.4</td>
</tr>
</tbody>
</table>

a large amount of space for buffer. Hence, it is impractical to guarantee forward progress per each remote node by refinement alone. However, it is usually not difficult to ensure the forward progress when other properties of modern CPUs are considered. A modern CPU can have a small number, say 8, of transactions outstanding. If the home node were to reserve a buffer that can handle 513 messages (512 = 64 × 8 for requests for rendezvous, 1 for ack/nack) and the buffer pool is managed as a resource shared by all the 1024 shared lines, forward progress can be assured per each shared line per each remote node.

8. Conclusions and Future Directions

We presented a framework to specify the protocols implementing distributed shared memory at a high-level using rendezvous communication. These rendezvous protocols can be efficiently verified, for example using a model-checker. After such verification, the protocol can be translated into an efficient asynchronous protocol using the refinement rules presented in this paper. The refinement rules add transient states to handle unexpected messages. The rules also address buffering considerations. To assure that the refinement process generates an efficient asynchronous protocol, some syntactic restrictions are placed on the processes. These restrictions, namely enforcing a star configuration and restricting the use of generalized guard, are inspired by domain specific considerations.

To further improve the efficiency of the asynchronous protocol, one may let two remote nodes communicate directly without involving the home node, thus relaxing the star configuration for the synthesized protocol. While this relaxation will make it more convenient to define synchronous protocols, it will also make the refinement algorithm more complex. It is not clear whether, or in what contexts, such a tradeoff would be a win.

Notes

1. The home for different cache lines can be different. We will derive protocols focusing on one cache line, as is usually done.
2. The proof may be accessed from the world-wide web address: http://www.cs.utah.edu/~ganesh/verpapers/refine.html.

References