BOUNDNESS, EMPTY CHANNEL DETECTION AND SYNCHRONIZATION FOR COMMUNICATING FINITE STATE MACHINES

Louis E. Rosier and Hsu-Chun Yen

Department of Computer Sciences
University of Texas at Austin
Austin, TX 78712

ABSTRACT

In this paper, we consider networks of communicating finite state machines (CFSM's), that explicitly allow zero testing (i.e., empty channel detection). In our main result, we show that the boundedness problem is decidable for the class of FIFO networks consisting of two such CFSM's, where one of the two machines is allowed to send only a single type of message to the other. This result, we feel, is somewhat surprising since the zero testing capability is precisely the required extension needed in order to render the problem undecidable for the related class of vector addition systems with states (VASS's) of dimension two. Note that both have the ability to store two nonnegative integers which can be conditionally tested for zero. The reason for the disparity appears to be that such a class of extended VASS's would be capable of more synchronized behavior (since the actions of the two counters can be controlled by a single finite state control). The rest of the paper examines other classes of networks which allow empty channel detection. These results seem to indicate that our main result cannot be extended.

1. INTRODUCTION

Models for distributed communication systems have included Petri nets, or equivalently Vector Addition Systems (VAS's), and more recently networks of communicating finite state machines (CFSM's). Many communication protocols can be modeled as a network of two finite state machines that communicate by exchanging messages over two one directional, FIFO channels [3, 4, 7, 19, 23, 26]. (Generalizations of this model permit any number of CFSM's, each pair of which communicate as above.) Such models have been shown useful in the detection of many protocol design errors. Design errors considered in the literature include state deadlocks, unspecified receptions, nonexecutable receptions, channel boundedness and channel overflow (c.f. [3, 4, 7, 19, 23, 26, 27]). Petri nets have also been used to model communication protocols. (See e.g. [2, 17, 24].)

Informally, the communication between two CFSM's machines is said to be bounded if there is a nonnegative integer k such that in each reachable state of the network, the number of messages in each channel is no more than k (i.e., the number of distinct reachable network states is finite). Similarly, a VAS is bounded if each vector position is so bounded. If the channels in any such protocol are bounded, then the protocol can be validated by generating the set of all reachable states and checking this set for any of the aforementioned problems. If the channels, on the other hand, are potentially unbounded, then the network cannot be built. Consequently, a basic problem to consider concerning CFSM's (and VAS's), is whether the communication in a given network is bounded. Unfortunately, this problem is known to be undecidable in general [4]. However, for VAS's and certain restricted classes of CFSM's this problem is decidable [4, 6, 7, 12, 18, 19, 26]. In this paper, we closely examine what features of a communication system, modeled by various extended types of VAS's and networks of CFSM's, contribute to the undecidability of the boundedness problem. We find that the asynchronous behavior of such systems plays an important role in this problem, and our results indicate that in some simple cases asynchronous systems may be easier to analyze than their synchronous counterparts. Before proceeding, however, we give some important historical background on known results concerning various types of VAS's and CFSM's.

In [6], the boundedness problem was studied for the class of networks consisting of an arbitrary number of CFSM's, each pair of which communicate by exchanging a single type of message. Since such networks can be modeled by VAS's [12], decision procedures for this class are well known [12, 18]. In particular, each such network can be represented by a VAS, where each channel corresponds to a potentially unbounded vector position and the state of each machine corresponds to a sequence of bounded vector positions. Equivalently, such a network can be modeled by a vector addition system with states (VASS) [9], where the channels are represented as above but where the states are represented in the states of the VASS (i.e., a state of the VASS contains a state for each CFSM in the
network). The main intuitive difference, in these models, is that a VAS does not readily illustrate the asynchronous behavior of the CFSM's; and in fact may camouflage it. On the other hand, a VAS may exhibit very synchronous behavior. For this reason, we feel that networks of CFSM's are somewhat better models for asynchronous communication systems as there is a clear way to see that two or more independent entities are executing simultaneously, which communicate, only by sending and receiving messages.

The boundedness problem was examined for networks consisting of two CFSM's, each of which could only send a single type of message to the other machine, in [26], and a more efficient algorithm than the one given in [6], was presented. This result was extended in [19], where the class of communication networks consisting of two CFSM's, in which one of the machines sends only one type of message (the communication in the other direction is not constrained), was shown to have a decidable boundedness problem. In fact, the problem was shown to be nondeterministic logspace complete and thus boundedness can be decided in polynomial time[5]. Both of the preceding results[19,26], were derived by taking advantage of the networks asynchronous properties. As a result, the techniques do not appear to generalize to the related class of VAS's which have no more than two potentially unbounded positions (or equivalently, to the class of VASS's of dimension two).

These models of communication systems have not allowed (with the exception of [20]) the communicating entities to realize or act upon any information regarding the channels, with the exception of reading the next available message. For example, no process is allowed to determine if a channel is devoid of messages and move accordingly. Examples illustrating the limitations of the modelling power of VAS's are considered in [1] and [13]. See also [15-17]. In both cases, the limiting factor is precisely the inability of the VAS to test a potentially unbounded position for zero and take action on the outcome of the test. As a result, the literature contains many extensions to the basic model of VAS's (Petri nets). Such extensions use a variety of mechanisms each of which allows zero testing. These include *inhibitor arcs*, *constraints*, *priorities*, *timing constraints*, etc. (c.f. [8,17]). Recently, priority networks of CFSM's were introduced, where messages are received based on a fixed, partial-ordered priority relation[7]. This model is equivalent, in computational power, to certain classes of extended Petri nets, in particular those with priority tokens[8]. The results in [7] focus on the boundedness problem for restricted classes of priority networks. If the priority relation is the null set (i.e. all messages are received on a random basis), then the boundedness problem is essentially the same as that of a VAS. (Such machines are called Random CFSM's in [7].)

In most of the extended VAS models, where zero testing is allowed, only two potentially unbounded positions are necessary to render the boundedness problem undecidable. This is also the case for the undecidability results concerning Priority CFSM's. The reason is that such extended VAS's or networks can utilize the potentially unbounded positions (or channels) to store two nonnegative integers and thus can be used to simulate the computation of a two-counter machine [14] with no input. See [7,8,17]. Since the computational power of two-counter machines is equivalent to that of TM's, the result follows.

In this paper, we consider networks of CFSM's (FIFO, Priority and Random), that explicitly allow zero testing (i.e. empty channel detection). In section 3, we consider FIFO networks of two CFSM's, only one of which is restricted to send a single type of message, where each machine can, make the following types of transitions:

1. moves in which a message is sent or received,
2. -moves,
3. conditional moves in which the input channel is checked for emptiness,
4. conditional moves in which the output channel is checked for emptiness.

For this class, we are able to show that the boundedness problem is nondeterministic logspace complete. Such machines are clearly a generalization of those studied in [19], where only moves of the first type were allowed. The approach taken in [19] was to construct a deterministic one counter automaton (DOCA)[25], that would simulate, in some sense, the computation of a given network. The results then followed from properties of DOCA. Here, however, we consider a class of networks that cannot, in general, be simulated by DOCA; and hence the techniques of [19] do not appear to generalize when moves of type 3-4 are allowed. In order to overcome this difficulty, we introduce a *new* more powerful simulating automaton which has three restricted counters. (The restrictions prevent the simulating automaton from allowing too much synchronization between the actions of its counters and thus do not allow it the power of a general two-counter machine.) The result then follows from subsequently derived properties of the simulating automaton. The difference in the networks considered here, of course, is that the two channels can be conditionally tested for zero (and nonzero) by each machine. Note, that since a machine can test both its input and output channel for emptiness, it can therefore ascertain something about the computation of the