Abstract:

The aim of this paper is to illustrate by an example, the alternating bit protocol, the use of CESAR, an interactive system for aiding the design of distributed applications.

CESAR allows the progressive validation of the algorithmic description of a system of communicating sequential processes with respect to a given set of specifications. The algorithmic description is done in a high level language inspired from CSP and specifications are a set of formulas of a branching time logic, the temporal operators of which can be computed iteratively as fixed points of monotonic predicate transformers. The verification of a system consists in obtaining by automatic translation of its description program an Interpreted Petri Net representing it and evaluating each formula of the specifications.

I. INTRODUCTION

The aim of this paper is to illustrate by an example the use of the system CESAR for the analysis of the properties of parallel systems.

CESAR is a system for aiding the design and integration of distributed applications. Its input language is a high level language, inspired from CSP [Hoare 78], for the algorithmic description of systems of communicating sequential processes. CESAR allows a progressive validation during the design process by considering two complementary aspects in a description:

- coherence in data manipulation (static characteristics of data and exchanged variables, visibility and access rights...)
- validation of the dynamic behaviour of a description with respect to its specifications.

Behavioural analysis of a system described by a program in the input language is based on the study of a representation of it in terms of Interpreted Petri Nets (IPN). Figure 1 illustrates the general principle of the system CESAR: given an algorithmic description of a system by a program in a high level language, a model representing some aspects of the described functioning is obtained by automatic
This model (an IPN) is treated by an analyzer in order to verify the conformity of the described system to given specifications. Specifications are a set of formulas of a branching time logic and express correctness properties which must be satisfied by the system. Using branching time logic instead of linear time logic as it has often been done [Gabbay 80] [Lamport 80] [Manna 81], is one of the peculiarities of our approach. It is shown that in this logic it is possible to compute iteratively the interpretation of temporal operators as fixed points of monotonic predicate transformers.

Our approach presents some similarities to those followed in [Jensen 79] [Lauer 75] as far as the use of Petri nets as a model for the semantical analysis is concerned. The example considered throughout this paper is the alternating bit protocol. We have chosen this example because protocol modelling and verification is one of the principal application domains for CESAR. Furthermore, as protocols have been the object of many studies and especially the alternating bit protocol [Bartlett 69] [Bremer 79]
This paper is organized in four parts. In part 2, the features of the description language are given and an illustration of its use for the description of the AB-protocol. After presenting the specification language, a part of the specifications of this protocol is given (part 3). In part 4 are exposed the analysis principle applied in CESAR and the theoretical results on which it is based.

2. DESCRIPTION IN CESAR

2.1. The description language

A system is described as a set of communicating sequential processes. Communications are declared as names of "exchanged variables". Exchange is done by rendez-vous between two processes, the one executing an output operation \(!V:=\text{exp}\) and the other an input operation \(?V\) where \(V\) is the exchanged variable. The process executing the input operation has a local copy of the exchanged variable also denoted by \(V\) (not preceded by \(?\)).

In addition to exchanged variables, processes have internal variables (which cannot be used for communication). Internal and exchanged variables are typed. Usual standard types and type constructors are available but the user can also introduce non-specified types for which it is not necessary to make manipulation rules explicit.

The basic statement of the language is the vectorial assignment. An input or output operation can be executed simultaneously with a vectorial assignment. We denote by \(\text{nop}\) the assignment whose right member is the identity function.

Besides the usual control structures, the CESAR description language provides the two following non-deterministic composed statements:

\[
\begin{align*}
\text{if } b_1 & \Rightarrow s_1 / / b_2 \Rightarrow s_2 / / \ldots \text{ fi} \\
\text{do } b_1 & \Rightarrow s_1 / / b_2 \Rightarrow s_2 / / \ldots \text{ od}
\end{align*}
\]

where the \(b_i\)'s are boolean conditions (guards) and the \(s_i\)'s are sequences of statements. Their meaning is the following.

- **IF**: wait until one of the conditions is true and execute the corresponding sequence of statements.
- **DO**: repetition of an IF statement until a statement EXIT is encountered during the execution of some \(s_i\).

For both of these constructs, if more than one conditions are true, the choice is non-deterministic. If a statement \(s_i\) begins with an input or output operation, the condition "the exchange can be executed" (i.e. the rendez-vous is possible) implicitly strengthens the guard \(b_i\). The interpretation of the IF and DO constructs are
2.2. Translation of description programs into interpreted Petri nets

Given a program in the input language, the translator generates an Interpreted Petri Net (IPN) representing the main aspects of its behaviour. It performs also the type verification and deletes the internal variables of non-specified types.

The IPN corresponding to a program is obtained by composing the IPN's representing its sequential processes. The translation method of the process uses a graph grammar, every rule of which is associated with a rule of the grammar of the description language [Queille 81].

An IPN is a Petri net with:
- a vector of variables $X$,
- a mapping associating with each transition of the net a guarded command $c_i \rightarrow a_i$
where $c_i$ is a condition on $X$ and $a_i$ is a vectorial assignment $a_i = (X:=\neg i(X))$.

Functioning rules of an IPN are those of standard Petri nets, with the addition of the following rules:
- a transition can fire only when its associated condition is true,
- when a transition fires, its associated action is executed.

IPN's are a useful tool for representing parallel programs in a non-deterministic way [Keller 76]. They can be graphically represented by the corresponding Petri net, the transitions of which are inscribed by the associated guarded commands. By convention, the always true condition and the identity assignment can be omitted. Thus, if a transition has no inscription its firing rule is the same as in a standard Petri net.

The translation method is such that each net representing a sequential process is a safe state graph. The composition rule expresses the rendez-vous by merging transitions and so, it preserves safety of each process. This property is used by the analyzer in order to simplify predicate manipulations.

2.3 Example : The Alternating Bit Protocol

2.3.1 Presentation of the protocol

The Alternating Bit Protocol (AB-Protocol) introduced in [Barlett 69] to provide a reliable full-duplex transmission over half-duplex links, is a protocol where the control information of each transmitted message or acknowledgement is a single control bit which can be used to detect loss of messages or acknowledgements and recover from them. In this paper, we are not interested in transmission errors which at the protocol level are not distinguished from losses. Since this protocol is completely symmetrical we suppose transmission of data in a single direction and describe it by considering a Sender and a Receiver as follows:
The Sender sends messages to the Receiver, which answers by sending acknowledgements. The Sender associates with each message a control bit which takes alternating values. After sending a message, the Sender does not change the control bit and does not send the next message before the reception of the corresponding acknowledgement (an acknowledgement with the same control bit). To recover from loss of messages or of acknowledgements, the Sender awaits the acknowledgement during a finite delay (measured by an arbitrary local clock) and then repeats the same message (without changing the control bit).

The Receiver behaves symmetrically. After receiving a message, it sends an acknowledgement with the same control bit and then awaits the next message (with a control bit of alternate value). If the next message does not arrive within an arbitrary local delay, the Receiver repeats the previous acknowledgement.

If we assume that the line cannot lose all the messages and acknowledgements (i.e. the line is not cut), this protocol ensures the correct transmission of each message after a sufficient number of repetitions. Message duplication does not cause any problem because the protocol guarantees that any sequence of received messages with the same control bit are duplications of the same message and the bit is changed by the Sender for all new messages. Thus, the Receiver has just to skip all the messages of such sequences except the first one. Symmetrically, the Sender has to skip duplications of acknowledgements in the same way.

2.3.2 Description programs and IPN's for the AB-protocol

We introduce two non-specified types:
- \texttt{data} to represent the data part of the messages
- \texttt{pattern} to represent the pattern of bits which is recognized as an acknowledgement.

Using the standard type \texttt{boolean}, we can define both the type \texttt{msg} for the messages and the type \texttt{ack} for the acknowledgements as two structures:

\begin{verbatim}
  type msg = ( MESSAGE : data ;
               B : boolean ) ;
  type ack = ( ACKNOWLEDGEMENT : pattern ;
               B : boolean ) ;
\end{verbatim}

The program for the sender is given in the following page (\texttt{\texttt{&}} means \texttt{true} ; ^ is the complementation operator).
process SENDER
  ( output M : msg ;
    input A : ack ) ;

X : data ;
Y : boolean := 0 ;

begin

loop
  send: !M := (X, Y) ; -- send the message
  do
    receiveack: T -> ?A ; -- receive acknowledgement
    if
      acceptack: A.B = Y -> Y := Y ; -- expected acknowledgement
        exit //
    skipack: A.B # Y -> nop -- else skip
    fi //
  repeat:
    T -> !M := (X, Y) -- repeat the message
  od
end loop

end SENDER ;

The program for the Receiver is the following :

process RECEIVER
  ( input N : msg ;
    output A : ack ) ;

Z : boolean := 0 ;

begin

loop
  do
    receive: T -> ?N ; -- receive
    if
      accept: N.B = Z -> exit // -- expected message
    skip: N.B # Z -> nop -- else skip
    fi //
  repeatack: T -> !A := ("ack", Z) -- repeat previous acknowledgement
  od;
  !A := ("ack", Z), Z := Z -- send acknowledgement
end loop

end RECEIVER ;

The transmission line is described by the two following processes :

process SENDTORECEIVE
  ( input M : msg ;
    output MM : msg ) ;

begin

loop
  get: ?M ; -- message is sent
  if
    transmit: T -> !MM := M // -- message is transmitted
  loose: T -> nop -- message is lost
  fi
end loop

end SENDTORECEIVE ;

342
process RECEIVETOSEND
  ( input AA : ack ;
     output A : ack ) ;

begin
  loop
    getack: ?AA ;
    if
      transmitack: T -> !A := AA /
      looseack: T -> nop
    fi
  end loop
end RECEIVETOSEND ;

Figure 2 presents the IPN obtained by translation of the description program.
3. SPECIFICATION IN CESAR

3.1 The specification language

The specification language of CESAR is a branching time logic $L$ [Lamport 80] [Rescher 71] constructed from a set of propositional variables $F$ and the constants true, false, by using the logical connectives $\neg$, $\land$, $\lor$, $\Rightarrow$ and the unary temporal operators $\text{POT}$ and $\text{INEV}$. The abbreviations $\text{ALL}(f)$ and $\text{SOME}(f)$ are used for respectively $\neg\text{POT}(\neg f)$ and $\neg\text{INEV}(\neg f)$.

The formulas of $L$ represent assertions about the functioning of a given system if we consider that propositional variables represent predicates on its state and give a precise meaning to the operators $\text{POT}$ and $\text{INEV}$. In order to do this, we consider transition systems as a model for $L$ since IPN's can be given a semantics in terms of them [Keller 76].

A transition system is defined as a doublet $S = (Q, \rightarrow)$ where $Q$ is a set of states and $\rightarrow$ is a binary relation on $Q$ ($\rightarrow \subseteq Q \times Q$). The relation $\rightarrow$ represents the actions or transitions of the system: $q \rightarrow q'$ means that there is an action executable from $q$ which after its execution leads to a state $q'$. An execution sequence from a given state $q_0$ is a sequence $s$ of states such that if $s$ is finite then its last element $q_t$ is a sink state (i.e. $\neg q(q_t \rightarrow q_t)$). In order to simplify the notations we take $s(k)$ to be equal to the $k$-th element of $s$ if it is defined; if not, we take $s(k) = M$ where $M$ represents some fictitious non accessible state adjoined to $Q$ such that $\neg q(M \rightarrow q_0)$. Thus, relation $s(0) \rightarrow s(k)$ is satisfied iff $s(k) \neq M$. The set of all the execution sequences from a state $q$ will be denoted by $\text{EX}(q)$.

Given $L$ and a transition system $S = (Q, \rightarrow)$ we define an interpretation of $L$ as a function $\llbracket \cdot \rrbracket$ associating to each formula of $L$ a truth-valued function of the system state in the following manner:

- $\forall f \in F$ $|f| \in [Q \rightarrow \{tt, ff\}]$ where $[Q \rightarrow \{tt, ff\}]$ is the set of the unary predicates on $Q$
- $\forall q \in Q$ $\llbracket \text{true} \rrbracket (q) = tt$
- $\forall f \in L$ $\llbracket \neg f \rrbracket (q) = tt$ iff $\llbracket f \rrbracket (q) = ff$
- $\forall f_1, f_2 \in L$ $\llbracket f_1 \land f_2 \rrbracket (q) = tt$ iff $\llbracket f_1 \rrbracket (q) = tt$ and $\llbracket f_2 \rrbracket (q) = tt$
- $\forall f \in L$ $\llbracket \text{POT}(f) \rrbracket (q) \equiv \exists s \in \text{EX}(q) \exists k \in \mathbb{N}$ $[k \uparrow s(k) \land |f| (s(k))]$
- $\forall f \in L$ $\llbracket \text{INEV}(f) \rrbracket (q) \equiv \forall s \in \text{EX}(q) \exists k \in \mathbb{N}$ $[k \downarrow s(k) \land |f| (s(k))]$

Obviously, $|\text{POT}(f)|$ represents the set of the states $q$ of $S$ such that there exists an execution sequence starting from $q$ containing a state satisfying $|f|$. We say that $|\text{POT}(f)|$ is the set of the states from which some state of $|f|$ is potentially reachable. In the same way, $|\text{INEV}(f)|$ is the set of the states from which $|f|$ is inevitably reachable in the sense that every execution sequence starting from a state of this set contains a state satisfying $|f|$. 

344
The interpretation of the dual operators \( \text{ALL} \) and \( \text{SOME} \) is,

\[
|\text{ALL}(f)| (q) \equiv \forall s \in Xq \forall k \in \mathbb{N} \left[ q \overset{k}{\underset{i=1}{\Rightarrow}} s(k) \implies |f| (s(k)) \right]
\]

\[
|\text{SOME}(f)| (q) \equiv \exists s \in Xq \forall k \in \mathbb{N} \left[ q \overset{k}{\underset{i=1}{\Rightarrow}} s(k) \implies |f| (s(k)) \right]
\]

Remark that if the state \( q \) of a transition system satisfies \( |\text{ALL}(f)| \) then all the states of all the execution sequences from \( q \) verify \(|f|\). Also, if a state \( q \) satisfies \( |\text{SOME}(f)| \) then there exists some execution sequence from \( q \) such that all its states verify \(|f|\).

The properties of a branching time logic similar to \( L \) have been studied in [Ben-Ari 81] where a decision procedure and a complete deduction system are given.

3.2 Example

In this section we give examples illustrating the use of the specification language for expressing system properties. The formulas of this languages are constructed from the following set of propositional variables:

- propositional variables representing predicates on the variables of the description program (only program variables of specified types are considered),
- the propositional variable \( \text{Init} \) which characterizes the set of all the possible initial (control and data) states,
- propositional variables on the control of the system referring to names of actions (labels) defined in the description program; for each labelled action \( a \), the propositional variables \( \text{enable} a \) and \( \text{after} a \) are introduced such that \( |\text{enable} a| \) and \( |\text{after} a| \) characterize respectively the set of the states from which this action can be executed and the set of the states reached just after the termination of this action. The following abbreviations are used:

\[
\text{enable} (a_1, \ldots, a_k) = \bigwedge_{i=1}^{k} \text{enable} a_i, \text{ where } \{a_1, \ldots, a_k\} \text{ is a set of actions,}
\]

\[
\text{enable} P = \text{enable} A(P) \text{ where } P \text{ is a process the set of the actions of which is } A(P),
\]

\[
\text{after} (a_1, \ldots, a_k) = \bigwedge_{i=1}^{k} \text{after} a_i, \text{ where } \{a_1, \ldots, a_k\} \text{ is a set of actions.}
\]

Obviously, a large number of properties can be formulated concerning the behaviour of a system. For methodological reasons, it is interesting to classify the most important of them as this has already been done for linear time logic in [Gabby 80] [Lamport 80] and [Manna 81]. Hereafter we introduce three families of properties and give specifications of the AB-protocol in terms of them.

**Invariant properties**

Invariant properties express the fact that a predicate \( P \), constructed by using only logical operators, is always true.

They are formulas of the type: \( \text{Init} \Rightarrow \text{ALL}(P) \)

In the case of the AB-protocol such formulas can be used to express:
* \( \text{Init} \implies \text{ALL}(\text{after}(\text{send, repeat}) \implies (M.B = Y)) \)
  
i.e. after the emission of a message the value of the control bit emitted
  \( M.B \) is equal to the control bit \( Y \) of the SENDER.
* \( \text{Init} \implies \text{ALL}(\text{after receive} \implies (MM = M)) \)
  
i.e. after the reception of a message the value of the received message \( MM \) is
  equal to the value of the emitted message \( M \), i.e. the line does not modify
  the transmitted information.
* \( \text{Init} \implies \text{ALL}(\text{after receive} \implies (MM.B = Y)) \)
  
i.e. after reception of a message the value of the received control bit \( MM.B \)
  is equal to the value of the control bit of the SENDER at the same time.

**Liveness properties**

These properties express the fact that an action can always be executed.

- **Liveness of an action** \( a \) : from every state \( q \), successor of a state satisfying \( \text{Init} \),
  there exists an execution sequence of \( \text{EXq} \) containing a state which enables \( a \). This
  is expressed by the formula : \( \text{Init} \implies \text{ALL} \ (*) \text{POT enable } a \)

- **Liveness of a set of actions** \( \{ a_1, \ldots, a_k \} \) : each one of the actions \( a_i \) is live. This
  can be expressed by the formula : \( \text{Init} \implies \bigwedge_{i=1}^k \ (* \text{POT enable } a_i \).

Or, by distributivity of \( \text{ALL} \) with respect to \( \wedge \) : \( \text{Init} \implies \text{ALL}(\bigwedge_{i=1}^k \ (* \text{POT enable } a_i \).)

- **Absence of deadlock for a set of actions** \( \{ a_1, \ldots, a_k \} \) : from every state \( q \), successor
  of a state satisfying \( \text{Init} \), there exists an execution sequence of \( \text{EXq} \) which contains
  a state enabling at least one of the actions \( a_i \). This is expressed by :
  \( \text{Init} \implies \text{ALL} \ (** \text{POT enable } (a_1, \ldots, a_k) \).

Some interesting liveness properties of the given example are (starting from the
weakest ones) :

* \( \text{Init} \implies \text{ALL} \ (** \text{POT enable } (\text{SENDER}) \), i.e. absence of deadlock for the SENDER
* \( \text{Init} \implies \text{ALL} \ (** \text{POT enable } (\text{RECEIVER}) \), i.e. absence of deadlock for the RECEIVER
* \( \text{Init} \implies \text{ALL} \ (** \text{POT enable } \text{send} \), i.e. the action of emitting a new message is live
* \( \text{Init} \implies \text{ALL} \ (** \text{POT enable } \text{accept} \), i.e. the action of receiving a new message is
  live.

**Properties of response to an action**

They are properties expressing the fact that an action \( b \) is a consequence of an
action \( a \).

- **Possible response** : if an action \( a \) is executed then it is possible that an action
  \( b \) becomes executable. This is expressed by the formula :
  \( \text{Init} \implies \text{ALL}(\text{after } a \implies \text{POT enable } b) \)

- **Inevitably possible response** : if an action \( a \) is executed then necessarily \( b \) becomes
  executable. This is expressed by the formula :
  \( \text{Init} \implies \text{ALL}(\text{after } a \implies \text{INEV enable } b) \)
Some interesting properties of this family for the given example are:

* \( \text{Init} \implies \text{ALL} (\text{after} (\text{send,repeat}) \implies \text{POT enable receive}) \)
  
  i.e. the line from the \text{SENDER} to the \text{RECEIVER} is able to transmit messages.

* \( \text{Init} \implies \text{ALL} (\text{after} (\text{sendack,repeatack}) \implies \text{POT enable receivack}) \)
  
  i.e. the line from the \text{RECEIVER} to the \text{SENDER} is able to transmit acknowledgements.

* \( \text{Init} \implies \text{ALL} (\text{after} (\text{send,repeat}) \implies \text{INEV enable receivack}) \)
  
  i.e. after sending a message the \text{SENDER} waits for an acknowledgement.

* \( \text{Init} \implies \text{ALL} ( (\text{after} \text{accept} \implies \text{INEV(enable sendack)}) \land (\text{after} \text{sendack} \implies \text{AA.B=MM.B}) ) \)
  
  i.e. when the \text{RECEIVER} receives a new message, it will send the corresponding acknowledgement.

4. PROVING SPECIFICATIONS IN CESAR

4.1. The results used by the analyser

In this paragraph we present the basic theoretical results used by the analyser. The method consists in iteratively computing fixed points of predicate transformers obtained from the IPN under study. Fixed points are precisely the interpretations of temporal operators as it is shown by the following results proved in detail in [Sifakis 79].

Let \( S = (Q, \rightarrow) \) be a transition system. It is convenient to identify any unary predicate on \( Q \) with its characteristic set. \( (2^Q, \cup, \cap, \neg) \) represents the lattice of predicates and \( [2^Q \rightarrow 2^Q] \) the set of the internal mappings of \( 2^Q \) (predicate transformers). For \( f, g \in [2^Q \rightarrow 2^Q] \), \( f \circ g, f \circ g, \overline{f}, \overline{g} \) and \( \text{Id} \) denote the functions \( f \circ g = \lambda P. f(P)g(P), f \circ g = \lambda P. g(P)g(P), \overline{f} = \lambda P. \overline{f}(P), \overline{g} = \lambda P. \overline{g}(P), \text{Id} = \lambda P. P \).

We also introduce the notations:

\[
\begin{align*}
    f^* &= \text{Id} \cup f^* \cup \ldots \cup f^* \\
    f^\oplus &= \text{Id} \cap f^\oplus \cap \ldots \cap f^\oplus \\
    f^\alpha &= \text{Id} \circ f^\alpha \circ \ldots \circ f^\alpha \\
    f^\beta &= \text{Id} \circ f^\beta \circ \ldots \circ f^\beta
\end{align*}
\]

Definition 1: Given \( S = (Q, \rightarrow) \) a transition system, \( P \in 2^Q \) and \( q \in Q \), we define the predicate transformer \( \text{pre} : \text{pre} P(q) \equiv \neg \exists q'(q \rightarrow q' \text{ and } P(q')) \).

Proposition 1:

Let \( f \) be a formula of \( L \), \( S = (Q, \rightarrow) \) a transition system such that \( \rightarrow \) be image-finite and \( \models \) an interpretation of \( L \) in \( S \).

a) \( |\text{ALL}(f)| = \pre X f | \)

b) \( |\text{SOME}(f)| = (\text{Id} \circ (\text{preupte}))X f | \)

Proposition 2:

Let \( f \) be a formula of \( L \), \( S = (Q, \rightarrow) \) a transition system such that \( \rightarrow \) be image-finite and \( \models \) an interpretation of \( L \) in \( S \).
4.2 The principle of the verification method

According to the results of the preceding section, it is possible to compute iteratively the interpretation of the temporal operators. We present hereafter the principle of the verification method applied by the analyzer:

Let \( f \) be a formula to be verified on a given program PROG and \( N \) the IPN obtained by translation from PROG. Denote by \( F = \{f_1, \ldots, f_n\} \) the set of the propositional variables occurring in \( f \).

- Associate a boolean variable with each place of \( N \).
- For each \( \text{after} \ a \in F \), express \( \text{after} \ a \) as a predicate on these variables (if necessary, \( N \) is transformed by adding new places).
- For each \( \text{enable} \ a \in F \), express \( \text{enable} \ a \) as a predicate on the boolean control variables and program variables.
- Express \( \text{Init} \) as a predicate representing the set of all possible initial states (knowing the initial marking of the net and the initial values of program variables).
- Reduce \( N \) without transforming the places which are involved in the expression of the predicates of \( \{\text{If}_{1}, \ldots, \text{If}_{n}\} \). Reducing \( N \) consists in applying transformation rules preserving the property expressed by \( f \) in order to obtain an IPN of less complexity.
- Compute the predicate transformer \( \text{pre} \) associated to the reduced IPN and then, the interpretation of temporal operators following the evaluation order imposed by the formula \( f \). During these computations simplification rules are applied, taking advantage of the fact that sequential processes correspond to state graphs. Given that there is no criterion on the speed of the convergence of these iterations, the user can impose a maximum number of iterations.
- If some iterative computation yields no result within the acceptable number of iterations then the analyzer fails to give an answer. If not, it evaluates \( |f| (q) = \text{tt} \) for every state \( q \).

4.3 Example

For the AB-protocol, the liveness property \( \text{Init} \Rightarrow \text{ALL \ POT \ enable} \ (\text{SENDER}) \) is verified by computing successively:

1) \( \text{Init} = s_m \wedge a_i \wedge r_i \). Intersection operators are omitted. The boolean variables \( s_i, m_i, a_i, r_i \), represent the fact that the places with the same name have a token (see figure 2).
2) \( \text{enable} \ (\text{SENDER}) = s_m \wedge u_s a_2 u_s a_2 u_s \)
3) the interpretation of \( \text{POT \ enable} \ (\text{SENDER}) \) as the limit of \( P_{k+1} = P_k \cup \text{pre}(P_k) \) with
\( P_0 = \text{enable (SENDER)}. \)

The following relations are invariants generated by the translator expressing the fact that each process is a safe state graph and they are used to simplify the boolean expressions computed by the analyzer:

\[
\begin{align*}
s_1 s_2 s_3 u s_1 s_2 s_3 s_2 s_3 &= \top \quad (\top \text{ is the always true predicate}) \\
r_1 r_2 r_3 u r_1 r_2 r_3 r_1 r_2 r_3 &= \top \\
m_1 m_2 u m_1 m_2 &= \top \\
a_1 a_2 u a_1 a_2 &= \top
\end{align*}
\]

The first step of the computation gives, \( \text{pre}(P_0) = s_3 u r_2 u r_3 u a_2 u m_2. \) Thus, \( P_1 = P_0 u \text{pre}(P_0) = \top \) and \( \text{POT enable (SENDER)} = \top. \)

4) \( \text{ALL POT enable (SENDER)} = \top \)

5) \( [\text{Init} \implies \text{ALL POT enable (SENDER)}] = \top \) (the property is verified).

5. CONCLUSION

We have tried to illustrate with an example, the AB-protocol, the analysis method applied in CESAR.

This method is based on the idea of translating the description of a system, given in some high-level formalism, into a model for which there exists a verification theory. This approach presents the advantage, on the one hand of abstracting from all the details which are not relevant to the verification of the behaviour (for example, data represented by variables of non-specified types), on the other hand, of displaying the control structure (invariants, for instance). In particular, the translation into a Petri net gives the possibility of naming control points which makes the expression of the properties easier.

The language of the formulas allows the expression of a great number of foundamental properties (invariant properties, liveness properties, properties of response to an action). The use of such a language is interesting from a methodological point of view as it provides the possibility of classification and comparison of the properties according to various criteria. Also, the representation of properties by formulas using temporal operators leads to mechanizable proofs provided that a method for obtaining from a given description the associated predicate transformer \( \text{pre} \) be given.

Computing fixed points of monotonic functions is, from a practical point of view, a central problem and it determines the limitations of our approach. Apart from the limitations of theoretical nature (non-decidability of the "interesting" system properties) serious problems appear when applying iterative methods which require the manipulation, simplification and comparison of predicates on many variables. For this reason, the current version of CESAR can verify formulas with variables of type boolean, enumerated and integer with known bounds, only. In order to simplify computations, the analyzer...
encodes the enumerated and bounded integer variables so that it manipulates only boolean variables; this coding is completely transparent to the user.

However, in spite of these simplifications the problems due to the complexity of the analyzed system remain crucial. We intend to increase the efficiency of the applied method by working in the following directions:

- Use of methods for approximating fixed points of monotonic operators in a lattice [Cousot 78] [Clarke 80],

- Reduction of the complexity of the iterative computations by decomposing global assertions into a set of local assertions,

- Study of a methodology of description since the possibility of proving a property greatly depends on the way the description is built.

REFERENCES


