Small Model Theory

As previously stated, we would like to separate the two main activities (and challenges) associated with deductive verification:

- The invention of auxiliary constructs.
- Establishing the validity of the premises of the relevant rule.

In this lecture, we will present one of the simplest methods for deciding validity of the premises – the small model theory.

Non-Mathematical Induction

Of course, we can check separately $S(2) \models \psi$, $S(3) \models \psi$, $S(4) \models \psi$, etc. Suppose they all come out valid. What can we conclude?

To the extent that formal verification is viewed as a debugging tool, then this would usually uncover most of the existing bugs. However, if we wish to establish the absolute correctness of the system, this is insufficient.

Much research has been expended in trying to identify a cutoff value $N_0$ such that

$$\forall N : S(N) \models \psi \iff S(N_0) \models \psi.$$

So far, only partial results have been obtained by Emerson, Ip, and Namjoshi.

Parameterized Systems

In its simplest form, a parameterized system is a parallel composition, such as

$$S(N) = P[1] \parallel \cdots \parallel P[N] \quad \text{or} \quad S(N) = C \parallel P[1] \parallel \cdots \parallel P[N]$$

where $N > 1$ is a parameter and $P[1], \ldots, P[N]$ are finite-state processes.

Uniform Verification: Establish in one verification effort that all instances of the system satisfy a property $\psi$. That is, $S(N) \models \psi$, for every $N > 1$.

Example: MUTEX

$$\text{MUTEX}[N] :: \begin{cases} \text{in } N : \text{natural where } N > 1 \\ \text{local } x : \text{boolean where } x = 1 \\ \text{loop forever do} \\ \begin{cases} \ell_0 : \text{Non-Critical} \\ \ell_1 : \text{request } x \\ \ell_2 : \text{Critical} \\ \ell_3 : \text{release } x \end{cases} \end{cases}$$

The semaphore instructions “request $x$” and “release $x$” appearing in the program stand, respectively, for (when $x = 1$ do $x := 0$) and $x := 1$.

Suppose we wish to establish the invariance of the assertion $p : \text{at}_{\ell_2}[1] \rightarrow (x = 0)$. This assertion is not inductive by itself. We need to strengthen it into the inductive assertion:

$$\forall i \neq j : (\text{at}_{\ell_2,3}[i] + \text{at}_{\ell_2,3}[j] + x) \leq 1$$

It only remains to check the validity of the premises of rule INV.
Checking the Premises for MUX-SEM[5]

We can check the validity of the premises by using BDD techniques, e.g. using TLV. In file mux5.pf we write:

To calc-phi;
Let phi := 1;
For (i in 1...N)
  For (j in i+1...N)
    Let phi := phi &
      (((P[i].loc in 2..3) + (P[j].loc in 2..3) + x) <= 1);
End -- For (j in i+1...N)
End -- For (i in 1...N)
End -- To calc-phi;

Premise Checking for MUX-SEM[5] Continued

Let p := ((P[1].loc=2) -> (x=0));
calc-phi;
Let counter := Theta & !phi; -- Check Premise 1
If (counter)
  Print ``n Premise 1 invalid: ",counter,"n"; Quit;
End -- If (counter)
Let counter := phi & rho & !next(phi); -- Check Premise 2
If (counter)
  Print ``n Premise 2 invalid: ",counter,"n"; Quit;
End -- If (counter)
Let counter := phi & !p; -- Check Premise 3
If (counter)
  Print ``n Premise 3 invalid: ",counter,"n"; Quit;
End -- If (counter)

R-Assertions

Consider the following signature:

- Boolean variables — $x_1, \ldots, x_a : \text{boolean}$.
- Index variables — $i_1, \ldots, i_b : [1..N]$. 1 and $N$ are considered to be \textit{constants} of type index.
- Boolean arrays — $y_1, \ldots, y_c : \text{array}[1..N] \text{ of boolean}$.

We define an index \textit{term} to be an index variable $i_j$ or one of the constants 1, $N$. An \textit{atomic formula} is a boolean variable $x_k$, a boolean term $a[t]$, where $a$ is an array and $t$ is an index term, or a comparison $t_1 < t_2$, where $t_1$ and $t_2$ are index terms.

A \textit{boolean R-assertion} is a boolean combination of atomic formulas.

An \textit{R-assertion} is built out of boolean \textit{R} assertions to which we apply further boolean operations and quantification over index variables. For example:

\[
\forall i : \exists j \geq i : y[j] \neq y[i]
\]
\[
\forall i : (1 \leq i \leq N) \rightarrow \exists j : i \leq j \land j \leq N \land y[j] \neq y[i]
\]

Note that the first formula can be viewed as an abbreviation of the second formula. An \textit{R-assertion} of the form $\forall i_1, \ldots, i_b : \exists j_1, \ldots, j_m : \varphi$, where $\varphi$ is a boolean \textit{R-assertion} is called an \textit{AER-assertion}.

$n$-Models

Let $\psi$ be an \textit{R}-assertion. An $n$-model $M(n)$ over the vocabulary of $\psi$ provides the following interpretation to the elements appearing in $\psi$:

- Each boolean variable $x_j$ is assigned a value from $\{0, 1\}$.
- Each index variable $i_j$ is assigned a value from $[1..n]$. The constants 1 and $N$ are assigned the values 1 and $n$.
- Each array variable $a_j$ is assigned a boolean array of size $n$.

In general, it is not necessary to assign values to index variables which appear bounded in $\psi$. Thus, an adequate model over the vocabulary of the \textit{AER}-assertion $\forall i : \exists j \geq i : y[j] \neq y[i]$ should only interpret the constant $N$ (as $n$) and the array $y$.

For example a 3-model for this formula can be specified by the assignment:

$N = 3$, \quad $y = (0, 1, 1)$

Given an \textit{R}-assertion $\psi$ and a model $M(n)$, we can evaluate $\psi$ over $M(n)$, and find out whether $M(n)$ satisfies $\psi$. \textit{R-assertion $\psi$ is said to be valid} if it is satisfied by every model.
A Small Model Theorem

Let \( \psi : \forall i_1, \ldots, i_k : \exists j_1, \ldots, j_m : \varphi \) be a closed AER-assertion.

Claim 15. [Small Model Theorem]

Assertion \( \psi \) is valid iff it is satisfied by all models \( M(n) \) for \( n \leq k + 2 \).

Proof Sketch:

In order to prove the claim, it is sufficient to show that if the negation
\( \chi = \neg \psi = \exists i_1, \ldots, i_k : \forall j_1, \ldots, j_m : \neg \varphi \)
has a satisfying model \( M(n) \) of size \( n > k + 2 \) then it also has a satisfying model of size \( \leq k + 2 \). We establish this by showing that every satisfying model of size \( n > k + 2 \) can be reduced to a satisfying model of size \( n - 1 \).

Let \( M \) be a satisfying model of size \( n > k + 2 \). Model \( M \) assigns to \( 1, i_1, \ldots, i_k, N \) values ranging in the set \( 1..n \). This set of values can contain at most \( k + 2 < n \) distinct values. Thus, there must exist some value \( r \in 1..n \) which is not the interpretation of any index term. Note that \( 1 < r < n \). We construct a new model \( M' \) of size \( n - 1 \) as follows:

- \( M'(N) = n - 1 \).
- For each index term \( t \), we let
  \[
  M'(t) = \text{if } M(t) < r \text{ then } M(t) \text{ else } M(t) - 1
  \]

Example

Consider the formula \( \psi = \forall i : \exists j \geq i : y[j] \neq y[i] \). In this case, \( k = 1 \) so the cutoff value is \( N_0 = 3 \). The negation is given by \( \chi = \exists i : \forall j \geq i : y[j] = y[i] \). Assertion \( \chi \) has a satisfying model of size \( 5 \) given by

\[
M(5) : (N : 5, i : 3, y : (0, 0, 1, 1, 1))
\]

Noting that the range of interpretation consists of \( \{1, 3, 5\} \), we can remove from the model the index values 2 and 4. This yields the following smaller satisfying model:

\[
M(3) : (N : 3, i : 2, y : (0, 1, 1))
\]

The Systems we Consider: BDS

A bounded-data discrete system (BDS) is an FDS whose system variables have the form:

- \( N : \text{integer where } N > 0 \) — aka the system’s parameter.
- \( x_1, \ldots, x_n : \text{boolean} \) — Any finite-domain type can be encoded by booleans.
- \( i_1, \ldots, i_k : [1..N] \) — The index variables.
- \( y_1, \ldots, y_c : \text{array } [1..N] \text{ of boolean} \)

The initial condition is a boolean combination of formulas of the form \( \forall \vec{i} : \Theta_k \), where \( \Theta_k \) are boolean \( R \)-assertions.

The transition relation is required to have the form:

\[
\exists \vec{h} \forall \vec{i} : R(\vec{h}, \vec{i}),
\]

where \( \vec{h}, \vec{i} \) are index variables, and \( R(\vec{h}, \vec{i}) \) is a boolean \( R \)-assertion. We denote by \( H = |\vec{h}| \) the number of existentially quantified variables in \( \rho \).

Typically, a bounded-data parameterized system is a parallel composition

\[
P[1] \parallel \cdots \parallel P[N].
\]
Deciding the Verification Conditions

Consider the case that property $p$ and the auxiliary assertion $\varphi$ both have the form

$$\varphi = \forall i, j : \psi(i, j)$$

where $\psi(i, j)$ is a boolean $R$-assertion.

The most complex verification condition, $I2$, is then:

$$(\forall u, v : \psi(u, v)) \land (\exists h : R(h, t)) \rightarrow \forall i, j : \psi'(i, j)$$

Moving quantifiers to the front, this can be rewritten as

$$\forall i, j, h : \exists u, v, t : (\psi(u, v) \land R(h, t)) \rightarrow \psi'(i, j)$$

Thus, this premise has 3 universally quantified variables. According to Claim 15, it is sufficient to check the validity of all premises on models of size $n \leq 5$.

For BDS’s, this solves the 2nd task associated with deductive verification — Establishing the validity of the premises.

Example: Program Arbiter

Consider the following program $\text{ARBITER}$:

$$r, g : \text{array}[1..N] \text{ of boolean where } \forall i : [1..N] : r[i] = g[i] = 0$$

$$A :: \begin{array}{c}
\text{loop forever do}

k : [1..N] \text{ where } k = 1

\begin{cases}
  m_0 : & \text{if } r[k] \text{ then } \begin{cases}
  m_1 : & g[k] := 1 \\
  m_2 : & \text{await } r[k] \\
  m_3 : & g[k] := 0
  \end{cases} \\
  m_4 : & k := k \oplus N 1
\end{cases}

\end{array}$$

$C[i] :: \begin{array}{c}
\text{loop forever do}

l_0 : \text{Non-Critical}

l_1 : r[i] := 1

l_2 : \text{await } g[i]

l_3 : \text{Critical}

l_4 : r[i] := 0

l_5 : \text{await } \neg g[i]

\end{array}$$

for which we wish to prove

$$p : \forall i \neq j : \neg (\text{at}_l \ell_3[i] \land \text{at}_l \ell_3[j])$$

BDS's usually contain the system array variable $\pi[1..N]$ which represents the program counter in each of the processes.
Progressing to Richer Signatures

Up to now, we only considered systems with array signatures $[1..N] \mapsto \text{bool}$. The method can be extended to signatures $\langle [1..N_1] \mapsto \text{bool}, [1..N_1] \mapsto [1..N_2] \rangle$.

Declarations for such systems will have the form:

\[
\begin{align*}
type_1 &= [1..N_1] \\
type_2 &= [1..N_2] \\
x_1, \ldots, x_a &= \text{boolean} \\
y_1, \ldots, y_b &= [1..N_1] \\
z_1, \ldots, z_c &= \text{array}[1..N_1] \text{ of } \text{boolean} \\
w_1, \ldots, w_d &= [1..N_2] \\
v_1, \ldots, v_e &= \text{array}[1..N_1] \text{ of } [1..N_2]
\end{align*}
\]

In the assertions, we allow comparisons ($<, \leq$) between $type_1$ values and between $type_2$ values, but never between a $type_1$ and a $type_2$ value.

We consider invariants of the form $\forall \vec{h}_1, \vec{h}_2 \forall \vec{t}_1, \vec{t}_2 : R(\vec{h}_1, \vec{h}_2, \vec{t}_1, \vec{t}_2)$ and transition relations of the form $\exists \vec{h}_1, \vec{h}_2 \forall \vec{t}_1, \vec{t}_2 : R(\vec{h}_1, \vec{h}_2, \vec{t}_1, \vec{t}_2)$.

Further Extensions

It is possible to extend the approach to any stratified signature, allowing $type_1, \ldots, type_k$ and array types $type_i \mapsto type_j$ as long as $i < j$. This leads to:

**Claim 16.** The premises of rule INV are valid over $S(N_1, N_2)$ for all $(N_1, N_2) \geq (2, 2)$ iff they are valid over $S(N_1, N_2)$ for all $(N_1, N_2) \leq (N_1^0, N_2^0)$ where $N_1^0 = b + I_1 + H_1$ and $N_2^0 = d + I_2 + H_2 + c(b + I_1 + H_1)$.

Additional extensions are introduced by allowing

- $h_2 = h_1 + 1$  
  Can be rewritten as $\forall h : (h \leq h_1) \lor (h \geq h_2)$

- $h_0 = 0$  
  Can be rewritten as $\forall h : h \geq h_0$

Similarly, for $h = N$.
Unstratified Systems

In some cases, we have to move to unstratified systems. This is the case of program \textsc{Peterson}(N).

\begin{verbatim}
in N : integer where N > 1

type Pr_id : [1..N]
Level : [0..N]

local y : array Pr_id of Level where y = 0
s : array Level of Pr_id

loop forever do
    \(\begin{array}{l}
    \ell_0 : \text{NonCritical} \\
    \ell_1 : (y[i], s[1]) := (1, i) \\
    \ell_2 : \text{while } y[i] < N \text{ do} \\
    \ell_3 : \text{await } s[y[i]] \neq i \lor \forall j \neq i : y[j] < y[i] \\
    \ell_4 : (y[i], s[y[i] + 1]) := (y[i] + 1, i) \\
    \ell_5 : \text{Critical} \\
    \ell_6 : y[i] := 0
    \end{array}\)\end{verbatim}

Summary of Results

\begin{tabular}{|c|c|c|c|c|}
\hline
System & \(N_0\) & \(\tau_1\) & \(\tau_2\) & \(\tau_3\) \\
\hline
MUX-SEM & 5 & .01 & .01 & .01 \\
S. German's Cache & 4 & 10.21 & 10.72 & 133.04 \\
Illinois's Cache & 4 & 1.47 & .04 & .58 \\
3-stages Pipeline & 6 & 20.66 & .27 & 29.59 \\
SZYMANSKI & 4 & < .01 & .06 & .06 \\
TOKEN-RING & 5 & < .01 & < .01 & < .01 \\
BAKERY & 5 & .41 & .16 & .25 \\
\textsc{Peterson}(N) & (6,7) & 79 & 1211 & 240 \\
\hline
\end{tabular}

Here

\(\tau_1 : \text{Time to compute reach}\)
\(\tau_2 : \text{Time to compute candidate assertion}\)
\(\tau_3 : \text{Time to check premises over } S(N_0)\)