Computing Parameterized Helpful Assertions and Ranking Functions

In this lecture we will present some algorithms for the computation of helpful assertions and ranking for the case of parameterized systems. As in the case of algorithms for computing invariants, these algorithms are based on the analysis of small instances of the parameterized systems.

First, we consider the deductive analysis of finite-state systems, where most of the examples are instances of parameterized systems.

We start by presenting a version of rule WELL which is based on the justice requirements rather than on transitions.
**Justice-Based Rule WELL**

**Rule WELL**
For a well-founded domain \((\mathcal{A}, \triangleright)\)

Justice requirements \(J_1, \ldots, J_m\),

assertions \(p, q = h_0, h_1, \ldots, h_m\),

and ranking functions \(\delta_1, \ldots, \delta_m : \Sigma \mapsto \mathcal{A}\)

W1. \(p \Rightarrow \bigvee_{j=0}^{m} h_j\)

For \(i = 1, \ldots, m\)

W2. \(h_i \land \rho \Rightarrow (h'_i \land \delta_i = \delta'_i) \lor \bigvee_{j=0}^{m} (h'_j \land \delta_i \succ \delta'_j)\)

W3. \(h_i \Rightarrow \neg J_i\)

\[ p \Rightarrow \Diamond q \]

Note that the justice requirements \(J_1, \ldots, J_m\) need not be disjoint. Nor do they have to include all the justice requirements of the verified system.
Identifying the Requirement with Minimal Rank

Assume that $J_{\text{min}}$ is the requirement with minimal positive ranking.

Examining the premises of rule \textit{WELL} for the case of $J_{\text{min}}$, we find that assertion $h_{\text{min}}$ should satisfy:

\begin{align*}
\text{W2.} & \quad h_{\text{min}} \land \rho \implies h'_{\text{min}} \lor q' \\
\text{W3.} & \quad h_{\text{min}} \implies \neg J_{\text{min}}
\end{align*}

Namely, we should pick a requirement $J_{\text{min}}$ whose associated transition can lead in one step to the goal $q$. We should then determine an assertion $h_{\text{min}}$ such that $J_{\text{min}}$ is false on all $h_{\text{min}}$-states (W3), and all $\rho$-successors of $h_{\text{min}}$-states satisfy $h_{\text{min}} \lor q$.

Furthermore, $h_{\text{min}}$ should consist of pending states. These are the states which can be reached from a reachable $(p \land \neg q)$-state by a $q$-free path. These states can be computed symbolically by the expression:

$$
\text{pend} : \quad (\text{reachable}_D \land p \land \neg q) \Diamond (\rho \land \neg q')^*
$$
A Fix-point Computation

Recall that the condition $f \land \rho \rightarrow g$ can be rewritten as $f \rightarrow \text{pre} (\rho, g)$, where $\text{pre} (\rho, g) = \forall V'. (\rho \rightarrow g')$. Using this notation, premises W2–W3 for the case $J_{\min}$ can be rewritten as the single implication

$$\text{Imp} (h_{\min}) : \ h_{\min} \rightarrow \text{pend} \land \neg J_{\min} \land \text{pre} (\rho, h_{\min} \lor \neg \text{pend})$$

Note that we have rewritten $q$ as $\neg \text{pend}$. This is because all $(\neg \text{pend})$-successors of $\text{pend}$-states must satisfy $q$.

$\text{Imp} (h_{\min})$ can be viewed as an inequality with the unknown $h_{\min}$. Given $J_{\min}$ and $\text{pend}$, the maximal solution of this implication can be found by the iterations associated with the fix-point expression

$$\nu h : \text{pend} \land \neg J_{\min} \land \text{pre} (\rho, h \lor \neg \text{pend})$$
An Algorithm for Computing Auxiliary \textsc{WELL} Constructs

\textbf{Algorithm} compute-help — Compute Auxiliary Constructs for Rule \textsc{WELL}. The non-disjoint case

\begin{align*}
\text{pend} & := (\text{reachable}_{D} \land p \land \neg q) \diamond (\rho \land \neg q')^* \\
r & := 0 \\
nj & := nJ(1) \\
\text{Fix } (\text{pend}) \\
\text{for } i = 1, \ldots, nj \text{ do} \\
& \quad h_{\text{min}} := \nu h : \text{pend} \land \neg J[i] \land \text{pre}(\rho, h \lor \neg \text{pend}) \\
& \quad \text{If } h_{\text{min}} \neq 0 \text{ then} \\
& \quad \quad r := r + 1 \quad \text{— — Increment rank} \\
& \quad \quad h[r] := h_{\text{min}} \quad \text{— — Set helpful assertion} \\
& \quad \quad d[r] := r \quad \text{— — Set rank} \\
& \quad \quad \text{ind}J[r] := i \quad \text{— — index of justice requirement} \\
& \quad \quad \text{pend} := \text{pend} \land \neg h_{\text{min}} \\
& \quad \quad \text{— — Remove } h_{\text{min}}\text{-states from } \text{pend}
\end{align*}

The algorithm places in $h[1], h[2], \ldots, d[1], d[2], \ldots,$ and $\text{ind}J[1], \text{ind}J[2], \ldots$ the helpful assertions, ranks, and indices of justice requirements, respectively.
An Example in TLV

To apply this process to program \textsc{Token-Ring}(5), we place in file \texttt{tokenr-help.pf} the following script:

To compute\_inv;
Let inv := 1;
For (i in 1...N)
Let inv := inv & (P[i].loc in \{1,4,5\} -> k=i);
End -- For (i in 1...N)
End -- To compute\_inv;
compute\_inv;
Call binv(inv);
Load "compute-constructs.pf";
Print "\n Compute Constructs for tring\n";
compute\_help P[N].loc=3, P[N].loc=4;
Call wellx\_nond(P[N].loc=3, P[N].loc=4, inv, rank, h, d, indJ);

where \texttt{wellx-nond} is the procedure that checks the premises of rule \texttt{WELL} for the case of non-disjoint justice requirements.
The Case of Disjoint Justice Requirements

In many cases, it is possible to find lists \( J_1, \ldots, J_m \) and corresponding \( h_1, \ldots, h_m \), such that the \( J_i \)’s are pairwise disjoint. To find the \( h_i \)’s for such a case we start by employing an algorithm similar to compute-help except that its innermost block is replaced by

\[
\text{If } h_{\text{min}} \neq 0 \text{ then}
\begin{align*}
&h[i] := h[i] \lor h_{\text{min}} \quad \text{— — Add helpful assertion} \\
&p\text{end} := p\text{end} \land \neg h_{\text{min}} \\
&\text{— — Remove } h_{\text{min}}\text{-states from } p\text{end}
\end{align*}
\]

where, \( h[1], \ldots, h[n_j] \) are initially set to 0. Thus, it is assumed that, while computing a new candidate for \( h_{\text{min}} \), we may encounter a candidate corresponding to \( J[i] \) more than once. This version takes as \( h[i] \) the disjunction of all candidates corresponding to \( J[i] \).

This part of the modified algorithm does not compute the ranks, which are no longer given by the index of the assertion/justice requirement.

In order to compute the ranks we employ an additional algorithm which performs topological sort on the assertions. The lowest rank is assigned to an \( h[i] \) which has no successor in any \( h[j], j \neq i \). Once such an assertion is identified, it is removed from the list, and the process is repeated.
Computing the Ranks by Topological Sort

\[
\text{for } i = 1, \ldots, nj \text{ do}
\begin{align*}
\text{for } j = 1, \ldots, nj \text{ do } & \quad \text{prec}[i, j] := (i \neq j) \land (h[i] \land \rho \land h[j]') \neq 0 \\
\quad \quad \quad \quad \quad \quad \text{— — Set } \text{prec}[i, j] \text{ to } 1 \text{ iff } i \neq j \text{ and } h[i] \text{ has a successor in } h[j] \\
\text{nsuc}[i] := \sum_{j=1}^{nj} \text{prec}[i, j] & \quad \quad \quad \quad \quad \text{— — Number of successors of } h[i] \\
\text{d}[i] := 0
\end{align*}
\]

\[r := 0\]

\text{Fix } (r) \text{ do}

\[
\begin{align*}
\text{for } i = 1, \ldots, nj \text{ do } & \quad \text{if } \text{nsuc}[i] = 0 \land \text{d}[i] = 0 \land (h[i] \neq 0) \text{ then} \\
\quad \quad \quad \quad \quad \quad \text{— — Node } i \text{ has no successors. Rank it} \\
\quad \quad \quad \quad \quad \quad r := r + 1 \\
\quad \quad \quad \quad \quad \quad \text{d}[i] := r \\
\quad \quad \quad \quad \quad \quad \text{— — Remove node } i \text{ from the graph} \\
\text{for } j = 1, \ldots, nj \text{ do } & \quad \text{nsuc}[j] := \text{nsuc}[j] - \text{prec}[j, i] \\
\quad \quad \quad \quad \quad \quad \text{— — For each } j, \text{ subtract } 1 \text{ from } \text{nsuc}[j] \\
\quad \quad \quad \quad \quad \quad \text{— — if } i \text{ is a successor of } j
\end{align*}
\]
Example in TLV

To apply the method of disjoint justice requirements, we place in file `tring-nond.pf` the following script:

To compute-inv;
    Let inv := 1;
    For (i in 1...N)
        Let inv := inv & (P[i].loc in {1,4,5} -> k=i);
    End -- For (i in 1...N)
End -- To compute-inv;
compute-inv;
Call binv(inv);
Load "compute-constructs.pf";
Print "\n Compute Constructs for tring\n";
compute-construct P[N].loc=3, P[N].loc=4; rank-by-sort;
Call wellx(P[N].loc=3,P[N].loc=4,inv,rank,h,d);

where `compute-construct` is the procedure that produces helpful assertions with unique associated justice requirements, `rank-by-sort` computes ranks by topological sorting, and `wellx` is a procedure that checks the premises of rule `WELL` for the disjoint-requirements case.
Often, we may wish to use rule \textsc{DISTR-RANK} for proving a response property. Recall that a good insight for designing the distributed ranks $\delta[i]$ is to take them as assertions (i.e. functions ranking over $\{0, 1\}$), where state $s$ satisfies $\delta[i]$ iff there exists a pending path from $s$ to a state $\tilde{s}$ that satisfies $h[i]$. Consequently, we use the following algorithm for computing distributed ranks:

\begin{algorithm}
\textbf{Algorithm} compute-distr \quad \text{Compute distributed ranks}
\begin{algorithmic}
\State \textbf{for} $i = 1, \ldots, nj$ \textbf{do} $\delta[i] := (\text{pend} \land \rho)^\ast \diamond h[i]$
\end{algorithmic}
\end{algorithm}
Example in TLV

We apply rule **DISTR-RANK** in order to prove accessibility for an instance of **BAKERY**. To do so, we place in file **bakery-distr.pf** the following script:

To compute-inv;
   Let inv := 1;
   For (i in 1...N)
      Let inv := inv & ((C[i].loc>1) <-> (y[i]>0))
      & (C[i].loc in 3..4 -> C[i].cond2)
      & (& for (j=i+1;j<=N;j=j+1){y[i]=0 | y[i] != y[j]});
   End -- For (i in 1...N)
End -- To compute-inv;
compute-inv;   Call binv(inv);
Load "compute-constructs.pf";
Print "\nCompute Constructs for Bakery\n";
compute-constructs C[1].loc=1, C[1].loc=3; compute-distr;
Call distr(C[1].loc=1, C[1].loc=3, inv, h, del);
Uniform Verification of Parameterized Systems

All the examples shown above were of individual instances of parameterized systems. We will now consider methods for uniform verification of progress properties of parameterized systems. These methods establish in one application that $S(N) \models p \Rightarrow \Diamond q$, for every $N$.

The method is based on the project & generalize approach which consists of the following steps, where we assume that we intend to apply rule DISTR-RANK with helpful assertions and boolean rankings of the form $h_j[i]$ and $\delta_j[i]$, where $i \in [1..N]$ and $j$ ranges over a fixed domain $j \in [1..k]$, independent of $N$:

- Choose an appropriate cutoff value $N_0$.
- Apply algorithms compute-constructs and compute-distr to $S(N_0)$. As a sanity check, establish that $S(N_0) \models p \Rightarrow \Diamond q$.
- Choose a generic index, say $i = 3$. Generalize $h_j[3]$ and $\delta_j[3]$ to $h_j[i]$ and $\delta_j[i]$, respectively, for all $i \in [1..N_0]$ and $j \in [1..k]$.
- Invoke rule DISTR-RANK with the generalized versions of $h_j[i]$ and $\delta_j[i]$.