Computer-Aided Formal Verification (Sheet #1)

Marius Gavrilescu

1. This piece of pseudocode computes $Reach(TS)$ as R. The ++ operator is set union, {} is the empty set, and $|X|$ is the number of elements in set X.

```
R <- I
loop:
  N <- {}
  for s in R do:
    N <- N ++ Post(s)
  if |N| == |R|:
    finish loop
  R <- N
```

2. Recall $pref(P) = \bigcup_{\sigma \in P} pref(\sigma)$ and $closure(P) = \{\sigma \in 2^{AP} | pref(\sigma) \subseteq pref(P)$.

   Note that $\forall \sigma \in P$, $pref(\sigma) \subseteq pref(P)$ and so $\sigma \in closure(P)$. Thus $P \subseteq closure(P)$, which leads to $pref(P) \subseteq pref(closure(P))$.

   Now take $x \in closure(P)$. By the definition of the closure, $pref(x) \subseteq pref(P)$. But $pref(closure(P)) = \bigcup_{\sigma \in closure(P)} pref(\sigma)$, and so $pref(closure(P)) \subseteq pref(P)$.

   Therefore $pref(closure(P)) = pref(P)$.

3. TS_2 can produce traces which contain bbb. TS_1 and TS_2 can only produce traces with at most two consecutive b.

   TS_2 cannot produce traces with an even number of consecutive b's, while TS_1 can produce a trace starting $abba$ and TS_3 can also produce a trace starting $abba$.

   As such $Traces(TS_2)$ is neither included nor includes nor is equal to $Traces(TS_1)$ or $Traces(TS_3)$.

   We still need to compare TS_1 and TS_3.

   TS_3 can produce the trace $aaaaa(abab)^*$ (by staying in u_5 in the beginning then going in the square). However TS_1 cannot obtain more than 2 a's in the beginning without going to state s_5, after which it cannot produce any more b's. So $Traces(TS_3)$ is not a subset of $Traces(TS_1)$.

   Finally note that TS_1 can produce the trace $abbaa$ whereas TS_3 can only produce two consecutive a's in the beginning.

   Thus none of the subset/equality relations we are checking is true.

4. A liveness property is one that can't be invalidated by finite traces, i.e. $pref(P) = (2^{AP})^*$

   We have $pref(P \cup P') = pref(P) \cup pref(P') = (2^{AP})^*$, so liveness properties are closed under set union.

   Liveness properties are not closed under set intersection due to some topological argument I do not understand (there is a natural topology of $(2^{AP})^\omega$ where safety properties are the closed sets and liveness properties are the dense sets. Since dense sets are not closed under intersection, neither are liveness properties).

   A safety property is one where $closure(P) = P$.

   We have $closure(P) = P$ and $closure(P') = P'$.

   Therefore $closure(P \cup P') =$
   $\{\sigma \in (2^{AP})^\omega | pref(\sigma) \subseteq pref(P \cup P')\} =$
   $\{\sigma \in (2^{AP})^\omega | pref(\sigma) \subseteq pref(P) \vee pref(\sigma) \subseteq pref(P'))\} =$
   $\{\sigma \in (2^{AP})^\omega | pref(\sigma) \subseteq pref(P)\} \cup \{\sigma \in (2^{AP})^\omega | pref(\sigma) \subseteq pref(P')\} =$
   $closure(P) \cup closure(P') =$
   $P \cup P'$

   Again, we have $closure(P) = P$ and $closure(P') = P'$.

   Therefore $closure(P \cap P') =$
   $\{\sigma \in (2^{AP})^\omega | pref(\sigma) \subseteq pref(P \cap P')\} =$
   $\{\sigma \in (2^{AP})^\omega | pref(\sigma) \subseteq pref(P) \wedge pref(\sigma) \subseteq pref(P'))\} =$
   $\{\sigma \in (2^{AP})^\omega | pref(\sigma) \subseteq pref(P)\} \cap \{\sigma \in (2^{AP})^\omega | pref(\sigma) \subseteq pref(P')\} =$
   $closure(P) \cap closure(P') =$
   $P \cap P'$

   Thus safety properties are closed under both set union and set intersection.