Reasoning about Nondeterminism in Programs

[Extension to Support the Strong Until U]

Eric Koskinen
Stevens Institute of Technology

In this short discussion, we present a small extension to our prior work (PLDI 2013). Previously, we presented CTL proof rules, but did not include support for the the strong until operator U. We assume that the reader is already familiar with the prior work, particularly Section 3. As a reminder, the existing proof rules are as follows:

$$\frac{X \subseteq [\![p]\!]}{X \vdash \kappa, p}\;\textsc{RAp} \qquad \frac{X \vdash \mathsf{L}\kappa, \Phi_1 \quad X \vdash \mathsf{R}\kappa, \Phi_2}{X \vdash \kappa, \Phi_1 \wedge \Phi_2}\;\textsc{RAnd}$$

$$\frac{X = X_1 \cup X_2 \quad X_1 \vdash \mathsf{L}\kappa, \Phi_1 \quad X_2 \vdash \mathsf{R}\kappa, \Phi_2}{X \vdash \kappa, \Phi_1 \vee \Phi_2}\;\textsc{ROr}$$

$$\frac{X, S, \mathcal{F}^{\kappa} \Vdash \kappa, \gamma}{X \vdash \kappa, \mathsf{A}\gamma}\;\textsc{RA} \qquad \frac{(X, \mathcal{C}^{\kappa}, \mathcal{F}^{\kappa}) \text{ is rcr} \quad X, \mathcal{C}^{\kappa}, \mathcal{F}^{\kappa} \Vdash \kappa, \gamma}{X \vdash \kappa, \mathsf{E}\gamma}\;\textsc{RE}$$

$$\frac{\mathcal{R}\underset{X}{\overset{\mathcal{F}^{\kappa}}{\mathcal{C}^{\kappa}}} \text{ is w.f.} \quad \mathcal{F}^{\kappa} \vdash \mathsf{L}\kappa, \Phi}{X, \mathcal{C}^{\kappa}, \mathcal{F}^{\kappa} \Vdash \kappa, \mathsf{F}\Phi}\;\textsc{RF} \qquad \frac{\mathcal{R}\underset{X}{\overset{\mathcal{F}^{\kappa}}{\mathcal{C}^{\kappa}}}|_1 \vdash \mathsf{L}\kappa, \Phi_1 \quad \mathcal{F}^{\kappa} \vdash \mathsf{R}\kappa, \Phi_2}{X, \mathcal{C}^{\kappa}, \mathcal{F}^{\kappa} \Vdash \kappa, [\Phi_1 \;\mathsf{W}\; \Phi_2]}\;\textsc{RW}$$

$$\frac{(s,t) \in R \quad s \in X \quad s \notin \mathcal{F} \quad s,t \in \mathcal{C}}{\mathcal{R}\underset{X}{\overset{\mathcal{F}}{\mathcal{C}}}\;(s,t)}$$

$$\frac{\mathcal{R}\underset{X}{\overset{\mathcal{F}}{\mathcal{C}}}\;(s,t) \quad (t,u) \in R \quad t \notin \mathcal{F} \quad u \in \mathcal{C}}{\mathcal{R}\underset{X}{\overset{\mathcal{F}}{\mathcal{C}}}\;(t,u)}$$

On the left is a proof system for CTL that unifies the temporal treatment of universal A and existential E. There is a side condition on the existential rule that the relevant states form a recurrent set. The definition of $\mathcal{R}$ is given on the right.

Strong Until. The new proof rule is as follows:

$$\frac{\mathcal{R}\underset{X}{\overset{\mathcal{F}^{\kappa}}{\mathcal{C}^{\kappa}}} \text{ is w.f.} \quad \mathcal{F}^{\kappa} \vdash \mathsf{R}\kappa, \Phi_2 \quad \mathcal{R}\underset{X}{\overset{\mathcal{F}^{\kappa}}{\mathcal{C}^{\kappa}}}|_1 \vdash \mathsf{L}\kappa, \Phi_1}{X, \mathcal{C}^{\kappa}, \mathcal{F}^{\kappa} \Vdash \kappa, [\Phi_1 \;\mathsf{U}\; \Phi_2]}\;\textsc{RU}$$

When used with RA and RE, this additional proof rule adds support for strong until temporal properties $\mathsf{A}[\phi \mathsf{U} \psi]$ and $\mathsf{E}[\phi \mathsf{U} \psi]$, respectively.

This new rule, like RF, involves showing that $\mathcal{R}\underset{X}{\overset{\mathcal{F}}{\mathcal{C}}}$ is well-founded. This well-foundedness condition ensures that all traces through $X, \mathcal{C}, \mathcal{F}$ reach the frontier $\mathcal{F}$ after finitely many steps. Moreover, the RU rule requires that subproperty Φ_2 holds at the frontier: $\mathcal{F} \vdash \Phi_2$. Finally, the proof rule, like RW, requires that along every path from X through the chute $\mathcal{C}$, Φ_1 holds (by requiring that the first projection of $\mathcal{R}\underset{X}{\overset{\mathcal{F}}{\mathcal{C}}}$ satisfies Φ_1) unless the frontier $\mathcal{F}$ has been reached at which point Φ_2 holds.