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:

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 $R$ is given on the right.

**Strong Until.** The new proof rule is as follows:

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

This new rule, like RF, involves showing that $\mathcal{R}_{X}^{\mathcal{F}}$ 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 $\Phi_2$ holds at the frontier: $\mathcal{F} \models \Phi_2$. Finally, the proof rule, like RW, requires that along every path from $X$ through the chute $\mathcal{C}$, $\Phi_1$ holds (by requiring that the first projection of $\mathcal{R}_{X}^{\mathcal{F}}$ satisfies $\Phi_1$) unless the frontier $\mathcal{F}$ has been reached at which point $\Phi_2$ holds.