Errata: Assume-Guarantee Reasoning for Safe Component Behaviours

Chris Chilton, Bengt Jonsson, and Marta Kwiatkowska

Last updated: November 12, 2012

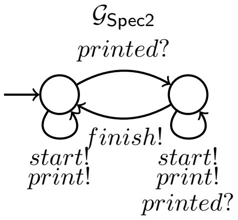
This document contains a list of errata for the official paper available at `www.springerlink.com`. The authors' personal copies contain the relevant amendments.

1. The definition of $\mathsf{violations}(X)$ on page 99 is ambiguous. It should instead read $\mathsf{violations}(X) \triangleq \{t \in \mathcal{A}_X^* : \exists t' \in (\mathcal{A}_X^I)^* \cdot tt' \in \mathcal{R}_X \cap \overline{\mathcal{G}_X}\}\mathcal{A}_X^*$.

2. The figure for $\mathcal{G}_{\mathsf{Spec1}\wedge\mathsf{Spec2}}$ is incorrect. The easiest correction without affecting the subsequent development of the paper is to redefine Spec2 as follows:

   - Spec2: If the number of jobs sent to $print$ is equal to or one greater than the number of jobs $printed$, then a job must be $printed$ before it can be $finished$, and no two jobs can be consecutively $finished$ without a document being $printed$ in between.

   To account for this change, $\mathcal{G}_{\mathsf{Spec2}}$ should add the $printed?$ action to the right-hand self-loop, thus obtaining the following guarantee:

   Based on this modification to Spec2, the figure for $\mathcal{G}_{\mathsf{Spec1}\wedge\mathsf{Spec2}}$ is correct.