Using HOL to study *Sugar 2.0* semantics

Michael J. C. Gordon

University of Cambridge Computer Laboratory
William Gates Building, JJ Thomson Aven

Four contributions were initially

simpli cations to the semantics occur if there is no non-trivial clocking, that di erent semantics of

4

The semantic embadding of

((M; w ⊨ b

3.3 CTL: Sugar Optional Branching Extension (OBE)

The syntax of the Sugar

Ftidfunctions B
of the Sugar Foundation Language (FL) and formulas of the Optional Branching
Extension (OBE), respectively. Fdocumentation we have de ned
seman
Corresponding to Appendix A.2 of the

SEM. that interpret boolean ex-

The official semantics uses a different approach in which the currently active clock is an argument of the semantic function used to interpret SEREs and formulas. Proving this approach equivalent to compiling away clocks, followed by a simpler unclocked semantics, is one of the formal challenges to which we hope to submit the semantics.

4.2 Finite paths

Sugar 2.0 gives a semantics to formulas

((M; w ⊨ b) ⇔

$$
\begin{array}{l}
((M; \overset{c!}{\models} b) = \\
\quad \mathbf{9} i \mathbf{2} pl \ . \ \mathrm{FirstRise}\ M \quad c\ i \ \mathbf{\wedge}\ (M; L_M(\ _i) \overset{}{\models} b)) \\
\mathbf{\wedge} \\
((M; \overset{c!}{\models} \mathbf{:} f) = \\
\quad \mathbf{:}(M; \overset{c}{\models} f)) \\
\mathbf{\wedge} \\
((M; \overset{c!}{\models}
\end{array}
$$

```
((M;    j=c!  fr1g|->fr2g) =
 (M;    j=c!  fr1g|->fr2g!)
 ((M;    j=c  fr1g|->fr2g) ^
   8j 2 pl .j 2 pl )
```

((M; $\models^{C}$ [f1 U f2]) =
  (M; $\models^{C!}$ [f1

$$((M; \models^{c} f@c1!) = (M; \models^{c1!} f))$$

This semantics of FL formulas differs from the one we originally transcribed from the Accellera submission document [6]. See the Appendix for the original semantics and Section 5 for a discussion of the differences between it and the current semantics in Section 4.5.

4.6 Optional Branching Extension

The semantic function `O_SEM` **is defined so that** `O_`

FirstRise M c i = (M; (Ĺ$_M$ ((

With this, clearly ($M; \models^{T} b$**) is not equal to (**$M; \models^{T!} b$**)). The solution, suggested by Cindy Eisner, is to replace the weak semantics by**

$$(M; \models^{C} b) = \forall i.\ \mathrm{FirstRise}\ M\ c\ i \Rightarrow (M; L_M(\__i) \models b)$$

so that we get

$$(M; \models^{T!} b) = \exists i.\ (i=0) \wedge (M; L_M(\__i) \models b)$$

$$(M; \models^{T} b) = \forall i.\ (i=0) \Rightarrow (M; L_M(\__i) \models b)$$

which makes ($M; \models^{T} b$**)**

Thus the semadtics was modi ed so that all quadti cations are suitably restricted. In addition,

References

1. I. Beer, S. Ben-David, C. Eisner, D. Fisman, A. Gringauze, and Y. Rodeh. The temporal logic Sugar. In G. Berry, H. Comon, and A. Finkel, editors, Proc. 13th International Conference on Computer Aided Verification

APPENDIX: Initial HOL semantics

This appendix consists of a typeset version of our initial transcription in

$$((M; \quad \models^{c!} \quad \mathbf{f}r\mathbf{g}(f)) = \mathbf{9}i.\ \mathrm{FirstRise}\ M \left(\begin{array}{l} c\ i \ \hat{} \\ \mathbf{8}j.\ (M;\ (\hat{L}_M \end{array} \right.$$

^
((M; $\models^C$ f1 ^ f2) =
  9i. FirstRise M c i
)
  ((M; $\models^i$ f1)
  ^
  (M; $\models^i$ f2)))
^
((M; $\models^C$ X! f) =
  9i. (FirstRise M c i
  ^
  (nite) i < length - 1))
)
  (M; $\models^{i+1}$ f))
^
((M; $\models^C$ [f1 U f2]) =

((M; $\overset{c}{\models}$ **f**r1**g**|->**f**r2**g**) =
9i. FirstRise M c i **)**

```
   ^
((M, s ⊨ [f1 U f2]) =
  9 . Path M                    ^
```