

Using HOL to study *Sugar 2.0* semantics

Michael J. C. Gordon

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

2

Four contributions were initially

simplifications to the semantics occur if there is no non-trivial clocking, that different semantics of

6

$((M; w \models b$

3.3 CTL: Sugar Optional Branching Extension (OBE)

The syntax of the Sugar

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

- - - -

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

12

$((M; w \models^C b) \models$

$$\begin{aligned}
& ((M; \models^{C!} b) = \\
& \quad \text{9i 2 pl . FirstRise } M \quad c \ i \ ^\wedge \ (M; L_M(i) \models b)) \\
& \quad ^\wedge \\
& \quad ((M; \models^{C!} : f) = \\
& \quad \quad : (M; \models^C f)) \\
& \quad ^\wedge \\
& \quad ((M; \models^{C!}
\end{aligned}$$

$$\begin{aligned}
 & ((M; \quad \overset{C!}{j} \models \text{fr1g} \mid \rightarrow \text{fr2g}) = \\
 & (M; \quad \overset{C!}{j} \models \text{fr1g} \mid \rightarrow \text{fr2g!}) \\
 & \overline{((M; \quad \overset{C}{j} \models \text{fr1g} \mid \rightarrow \text{fr2g}) \wedge} \\
 & \quad \text{8j 2 pl . j 2 pl })
 \end{aligned}$$

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

$$((M; \models^C f@c1!) = (M; \models^{C1!} f))$$

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 $\mathcal{O_SEM}$ is defined so that $\mathcal{O_}$

$$\text{FirstRise } M \quad c \quad i \quad = \quad (M; \quad (L_M \quad ($$

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

$$(M; \models^C b) = \text{FirstRise } M \text{ } c \text{ } i \text{ }) \text{ } (M; L_M(i) \models b)$$

so that we get

$$(M; \models^{T!} b) = \text{9i. } (i=0) \wedge (M; L_M(i) \models b)$$

$$(M; \models^T b) = \text{8i. } (i=0) \text{ } (M; L_M(i) \models b)$$

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

Thus the semantics was modified so that all quantifications are suitably restricted. In addition,

References

1. J. Beres, 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, 1999.

APPENDIX: Initial HOL semantics

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

$$((M; \bigwedge_{j=1}^{c!} \text{frg}(f)) =$$

9i. FirstRise M c i ^

8j. (M; (L₁
L₂
L₃
L₄
L₅
L₆
L₇
L₈
L₉
L₁₀
L₁₁
L₁₂
L₁₃
L₁₄
L₁₅
L₁₆
L₁₇
L₁₈
L₁₉
L₂₀
L₂₁
L₂₂
L₂₃
L₂₄
L₂₅
L₂₆
L₂₇
L₂₈
L₂₉
L₃₀
L₃₁
L₃₂
L₃₃
L₃₄
L₃₅
L₃₆
L₃₇
L₃₈
L₃₉
L₄₀
L₄₁
L₄₂
L₄₃
L₄₄
L₄₅
L₄₆
L₄₇
L₄₈
L₄₉
L₅₀
L₅₁
L₅₂
L₅₃
L₅₄
L₅₅
L₅₆
L₅₇
L₅₈
L₅₉
L₆₀
L₆₁
L₆₂
L₆₃
L₆₄
L₆₅
L₆₆
L₆₇
L₆₈
L₆₉
L₇₀
L₇₁
L₇₂
L₇₃
L₇₄
L₇₅
L₇₆
L₇₇
L₇₈
L₇₉
L₈₀
L₈₁
L₈₂
L₈₃
L₈₄
L₈₅
L₈₆
L₈₇
L₈₈
L₈₉
L₉₀
L₉₁
L₉₂
L₉₃
L₉₄
L₉₅
L₉₆
L₉₇
L₉₈
L₉₉
L₁₀₀
L₁₀₁
L₁₀₂
L₁₀₃
L₁₀₄
L₁₀₅
L₁₀₆
L₁₀₇
L₁₀₈
L₁₀₉
L₁₁₀
L₁₁₁
L₁₁₂
L₁₁₃
L₁₁₄
L₁₁₅
L₁₁₆
L₁₁₇
L₁₁₈
L₁₁₉
L₁₂₀
L₁₂₁
L₁₂₂
L₁₂₃
L₁₂₄
L₁₂₅
L₁₂₆
L₁₂₇
L₁₂₈
L₁₂₉
L₁₃₀
L₁₃₁
L₁₃₂
L₁₃₃
L₁₃₄
L₁₃₅
L₁₃₆
L₁₃₇
L₁₃₈
L₁₃₉
L₁₄₀
L₁₄₁
L₁₄₂
L₁₄₃
L₁₄₄
L₁₄₅
L₁₄₆
L₁₄₇
L₁₄₈
L₁₄₉
L₁₅₀
L₁₅₁
L₁₅₂
L₁₅₃
L₁₅₄
L₁₅₅
L₁₅₆
L₁₅₇
L₁₅₈
L₁₅₉
L₁₆₀
L₁₆₁
L₁₆₂
L₁₆₃
L₁₆₄
L₁₆₅
L₁₆₆
L₁₆₇
L₁₆₈
L₁₆₉
L₁₇₀
L₁₇₁
L₁₇₂
L₁₇₃
L₁₇₄
L₁₇₅
L₁₇₆
L₁₇₇
L₁₇₈
L₁₇₉
L₁₈₀
L₁₈₁
L₁₈₂
L₁₈₃
L₁₈₄
L₁₈₅
L₁₈₆
L₁₈₇
L₁₈₈
L₁₈₉
L₁₉₀
L₁₉₁
L₁₉₂
L₁₉₃
L₁₉₄
L₁₉₅
L₁₉₆
L₁₉₇
L₁₉₈
L₁₉₉
L₂₀₀
L₂₀₁
L₂₀₂
L₂₀₃
L₂₀₄
L₂₀₅
L₂₀₆
L₂₀₇
L₂₀₈
L₂₀₉
L₂₁₀
L₂₁₁
L₂₁₂
L₂₁₃
L₂₁₄
L₂₁₅
L₂₁₆
L₂₁₇
L₂₁₈
L₂₁₉
L₂₂₀
L₂₂₁
L₂₂₂
L₂₂₃
L₂₂₄
L₂₂₅
L₂₂₆
L₂₂₇
L₂₂₈
L₂₂₉
L₂₃₀
L₂₃₁
L₂₃₂
L₂₃₃
L₂₃₄
L₂₃₅
L₂₃₆
L₂₃₇
L₂₃₈
L₂₃₉
L₂₄₀
L₂₄₁
L₂₄₂
L₂₄₃
L₂₄₄
L₂₄₅
L₂₄₆
L₂₄₇
L₂₄₈
L₂₄₉
L₂₅₀
L₂₅₁
L₂₅₂
L₂₅₃
L₂₅₄
L₂₅₅
L₂₅₆
L₂₅₇
L₂₅₈
L₂₅₉
L₂₆₀
L₂₆₁
L₂₆₂
L₂₆₃
L₂₆₄
L₂₆₅
L₂₆₆
L₂₆₇
L₂₆₈
L₂₆₉
L₂₇₀
L₂₇₁
L₂₇₂
L₂₇₃
L₂₇₄
L₂₇₅
L₂₇₆
L₂₇₇
L₂₇₈
L₂₇₉
L₂₈₀
L₂₈₁
L₂₈₂
L₂₈₃
L₂₈₄
L₂₈₅
L₂₈₆
L₂₈₇
L₂₈₈
L₂₈₉
L₂₉₀
L₂₉₁
L₂₉₂
L₂₉₃
L₂₉₄
L₂₉₅
L₂₉₆
L₂₉₇
L₂₉₈
L₂₉₉
L₃₀₀
L₃₀₁
L₃₀₂
L₃₀₃
L₃₀₄
L₃₀₅
L₃₀₆
L₃₀₇
L₃₀₈
L₃₀₉
L₃₁₀
L₃₁₁
L₃₁₂
L₃₁₃
L₃₁₄
L₃₁₅
L₃₁₆
L₃₁₇
L₃₁₈
L₃₁₉
L₃₂₀
L₃₂₁
L₃₂₂
L₃₂₃
L₃₂₄
L₃₂₅
L₃₂₆
L₃₂₇
L₃₂₈
L₃₂₉
L₃₃₀
L₃₃₁
L₃₃₂
L₃₃₃
L₃₃₄
L₃₃₅
L₃₃₆
L₃₃₇
L₃₃₈
L₃₃₉
L₃₄₀
L₃₄₁
L₃₄₂
L₃₄₃
L₃₄₄
L₃₄₅
L₃₄₆
L₃₄₇
L₃₄₈
L₃₄₉
L₃₅₀
L₃₅₁
L₃₅₂
L₃₅₃
L₃₅₄
L₃₅₅
L₃₅₆
L₃₅₇
L₃₅₈
L₃₅₉
L₃₆₀
L₃₆₁
L₃₆₂
L₃₆₃
L₃₆₄
L₃₆₅
L₃₆₆
L₃₆₇
L₃₆₈
L₃₆₉
L₃₇₀
L₃₇₁
L₃₇₂
L₃₇₃
L₃₇₄
L₃₇₅
L₃₇₆
L₃₇₇
L₃₇₈
L₃₇₉
L₃₈₀
L₃₈₁
L₃₈₂
L₃₈₃
L₃₈₄
L₃₈₅
L₃₈₆
L₃₈₇
L₃₈₈
L₃₈₉
L₃₉₀
L₃₉₁
L₃₉₂
L₃₉₃
L₃₉₄
L₃₉₅
L₃₉₆
L₃₉₇
L₃₉₈
L₃₉₉
L₄₀₀
L₄₀₁
L₄₀₂
L₄₀₃
L₄₀₄
L₄₀₅
L₄₀₆
L₄₀₇
L₄₀₈
L₄₀₉
L₄₁₀
L₄₁₁
L₄₁₂
L₄₁₃
L₄₁₄
L₄₁₅
L₄₁₆
L₄₁₇
L₄₁₈
L₄₁₉
L₄₂₀
L₄₂₁
L₄₂₂
L₄₂₃
L₄₂₄
L₄₂₅
L₄₂₆
L₄₂₇
L₄₂₈
L₄₂₉
L₄₃₀
L₄₃₁
L₄₃₂
L₄₃₃
L₄₃₄
L₄₃₅
L₄₃₆
L₄₃₇
L₄₃₈
L₄₃₉
L₄₄₀
L₄₄₁
L₄₄₂
L₄₄₃
L₄₄₄
L₄₄₅
L₄₄₆
L₄₄₇
L₄₄₈
L₄₄₉
L₄₅₀
L₄₅₁
L₄₅₂
L₄₅₃
L₄₅₄
L₄₅₅
L₄₅₆
L₄₅₇
L₄₅₈
L₄₅₉
L₄₆₀
L₄₆₁
L₄₆₂
L₄₆₃
L₄₆₄
L₄₆₅
L₄₆₆
L₄₆₇
L₄₆₈
L₄₆₉
L₄₇₀
L₄₇₁
L₄₇₂
L₄₇₃
L₄₇₄
L₄₇₅
L₄₇₆
L₄₇₇
L₄₇₈
L₄₇₉
L₄₈₀
L₄₈₁
L₄₈₂
L₄₈₃
L₄₈₄
L₄₈₅
L₄₈₆
L₄₈₇
L₄₈₈
L₄₈₉
L₄₉₀
L₄₉₁
L₄₉₂
L₄₉₃
L₄₉₄
L₄₉₅
L₄₉₆
L₄₉₇
L₄₉₈
L₄₉₉
L₅₀₀
L₅₀₁
L₅₀₂
L₅₀₃
L₅₀₄
L₅₀₅
L₅₀₆
L₅₀₇
L₅₀₈
L₅₀₉
L₅₁₀
L₅₁₁
L₅₁₂
L₅₁₃
L₅₁₄
L₅₁₅
L₅₁₆
L₅₁₇
L₅₁₈
L₅₁₉
L₅₂₀
L₅₂₁
L₅₂₂
L₅₂₃
L₅₂₄
L₅₂₅
L₅₂₆
L₅₂₇
L₅₂₈
L₅₂₉
L₅₃₀
L₅₃₁
L₅₃₂
L₅₃₃
L₅₃₄
L₅₃₅
L₅₃₆
L₅₃₇
L₅₃₈
L₅₃₉
L₅₄₀
L₅₄₁
L₅₄₂
L₅₄₃
L₅₄₄
L₅₄₅
L₅₄₆
L₅₄₇
L₅₄₈
L₅₄₉
L₅₅₀
L₅₅₁
L₅₅₂
L₅₅₃
L₅₅₄
L₅₅₅
L₅₅₆
L₅₅₇
L₅₅₈
L₅₅₉
L₅₆₀
L₅₆₁
L₅₆₂
L₅₆₃
L₅₆₄
L₅₆₅
L₅₆₆
L₅₆₇
L₅₆₈
L₅₆₉
L₅₇₀
L₅₇₁
L₅₇₂
L₅₇₃
L₅₇₄
L₅₇₅
L₅₇₆
L₅₇₇
L₅₇₈
L₅₇₉
L₅₈₀
L₅₈₁
L₅₈₂
L₅₈₃
L₅₈₄
L₅₈₅
L₅₈₆
L₅₈₇
L₅₈₈
L₅₈₉
L₅₉₀
L₅₉₁
L₅₉₂
L₅₉₃
L₅₉₄
L₅₉₅
L₅₉₆
L₅₉₇
L₅₉₈
L₅₉₉
L₆₀₀
L₆₀₁
L₆₀₂
L₆₀₃
L₆₀₄
L₆₀₅
L₆₀₆
L₆₀₇
L₆₀₈
L₆₀₉
L₆₁₀
L₆₁₁
L₆₁₂
L₆₁₃
L₆₁₄
L₆₁₅
L₆₁₆
L₆₁₇
L₆₁₈
L₆₁₉
L₆₂₀
L₆₂₁
L₆₂₂
L₆₂₃
L₆₂₄
L₆₂₅
L₆₂₆
L₆₂₇
L₆₂₈
L₆₂₉
L₆₃₀
L₆₃₁
L₆₃₂
L₆₃₃
L₆₃₄
L₆₃₅
L₆₃₆
L₆₃₇
L₆₃₈
L₆₃₉
L₆₄₀
L₆₄₁
L₆₄₂
L₆₄₃
L₆₄₄
L₆₄₅
L₆₄₆
L₆₄₇
L₆₄₈
L₆₄₉
L₆₅₀
L₆₅₁
L₆₅₂
L₆₅₃
L₆₅₄
L₆₅₅
L₆₅₆
L₆₅₇
L₆₅₈
L₆₅₉
L₆₆₀
L₆₆₁
L₆₆₂
L₆₆₃
L₆₆₄
L₆₆₅
L₆₆₆
L₆₆₇
L₆₆₈
L₆₆₉
L₆₇₀
L₆₇₁
L₆₇₂
L₆₇₃
L₆₇₄
L₆₇₅
L₆₇₆
L₆₇₇
L₆₇₈
L₆₇₉
L₆₈₀
L₆₈₁
L₆₈₂
L₆₈₃
L₆₈₄
L₆₈₅
L₆₈₆
L₆₈₇
L₆₈₈
L₆₈₉
L₆₉₀
L₆₉₁
L₆₉₂
L₆₉₃
L₆₉₄
L₆₉₅
L₆₉₆
L₆₉₇
L₆₉₈
L₆₉₉
L₇₀₀
L₇₀₁
L₇₀₂
L₇₀₃
L₇₀₄
L₇₀₅
L₇₀₆
L₇₀₇
L₇₀₈
L₇₀₉
L₇₁₀
L₇₁₁
L₇₁₂
L₇₁₃
L₇₁₄
L₇₁₅
L₇₁₆
L₇₁₇
L₇₁₈
L₇₁₉
L₇₂₀
L₇₂₁
L₇₂₂
L₇₂₃
L₇₂₄
L₇₂₅
L₇₂₆
L₇₂₇
L₇₂₈
L₇₂₉
L₇₃₀
L₇₃₁
L₇₃₂
L₇₃₃
L₇₃₄
L₇₃₅
L₇₃₆
L₇₃₇
L₇₃₈
L₇₃₉
L₇₄₀
L₇₄₁
L₇₄₂
L₇₄₃
L₇₄₄
L₇₄₅
L₇₄₆
L₇₄₇
L₇₄₈
L₇₄₉
L₇₅₀
L₇₅₁
L₇₅₂
L₇₅₃
L₇₅₄
L₇₅₅
L₇₅₆
L₇₅₇
L₇₅₈
L₇₅₉
L₇₆₀
L₇₆₁
L₇₆₂
L₇₆₃
L₇₆₄
L₇₆₅
L₇₆₆
L₇₆₇
L₇₆₈
L₇₆₉
L₇₇₀
L₇₇₁
L₇₇₂
L₇₇₃
L₇₇₄
L₇₇₅
L₇₇₆
L₇₇₇
L₇₇₈
L₇₇₉
L₇₈₀
L₇₈₁
L₇₈₂
L₇₈₃
L₇₈₄
L₇₈₅
L₇₈₆
L₇₈₇
L₇₈₈
L₇₈₉
L₇₉₀
L₇₉₁
L₇₉₂
L₇₉₃
L₇₉₄
L₇₉₅
L₇₉₆
L₇₉₇
L₇₉₈
L₇₉₉
L₈₀₀
L₈₀₁
L₈₀₂
L₈₀₃
L₈₀₄
L₈₀₅
L₈₀₆
L₈₀₇
L₈₀₈
L₈₀₉
L₈₁₀
L₈₁₁
L₈₁₂
L₈₁₃
L₈₁₄
L₈₁₅
L₈₁₆
L₈₁₇
L₈₁₈
L₈₁₉
L₈₂₀
L₈₂₁
L₈₂₂
L₈₂₃
L₈₂₄
L₈₂₅
L₈₂₆
L₈₂₇
L₈₂₈
L₈₂₉
L₈₃₀
L₈₃₁
L₈₃₂
L₈₃₃
L₈₃₄
L₈₃₅
L₈₃₆
L₈₃₇
L₈₃₈
L₈₃₉
L₈₄₀
L₈₄₁
L₈₄₂
L₈₄₃
L₈₄₄
L₈₄₅
L₈₄₆
L₈₄₇
L₈₄₈
L₈₄₉
L₈₅₀
L₈₅₁
L₈₅₂
L₈₅₃
L₈₅₄
L₈₅₅
L₈₅₆
L₈₅₇
L₈₅₈
L₈₅₉
L₈₆₀
L₈₆₁
L₈₆₂
L₈₆₃
L₈₆₄
L₈₆₅
L₈₆₆
L₈₆₇
L₈₆₈
L₈₆₉
L₈₇₀
L₈₇₁
L₈₇₂
L₈₇₃
L₈₇₄
L₈₇₅
L₈₇₆
L₈₇₇
L₈₇₈
L₈₇₉
L₈₈₀
L₈₈₁
L₈₈₂
L₈₈₃
L₈₈₄
L₈₈₅
L₈₈₆
L₈₈₇
L₈₈₈
L₈₈₉
L₈₉₀
L₈₉₁
L₈₉₂
L₈₉₃
L₈₉₄
L₈₉₅
L₈₉₆
L₈₉₇
L₈₉₈
L₈₉₉
L₉₀₀
L₉₀₁
L₉₀₂
L₉₀₃
L₉₀₄
L₉₀₅
L₉₀₆
L₉₀₇
L₉₀₈
L₉₀₉
L₉₁₀
L₉₁₁
L₉₁₂
L₉₁₃
L₉₁₄
L₉₁₅
L₉₁₆
L₉₁₇
L₉₁₈
L₉₁₉
L₉₂₀
L₉₂₁
L₉₂₂
L₉₂₃
L₉₂₄
L₉₂₅
L₉₂₆
L₉₂₇
L₉₂₈
L₉₂₉
L₉₃₀
L₉₃₁
L₉₃₂
L₉₃₃
L₉₃₄
L₉₃₅
L₉₃₆
L₉₃₇
L₉₃₈
L₉₃₉
L₉₄₀
L₉₄₁
L₉₄₂
L₉₄₃
L₉₄₄
L₉₄₅
L₉₄₆
L₉₄₇
L₉₄₈
L₉₄₉
L₉₅₀
L₉₅₁
L₉₅₂
L₉₅₃
L₉₅₄
L₉₅₅
L₉₅₆
L₉₅₇
L₉₅₈
L₉₅₉
L₉₆₀
L₉₆₁
L₉₆₂
L₉₆₃
L₉₆₄
L₉₆₅
L₉₆₆
L₉₆₇
L₉₆₈
L₉₆₉
L₉₇₀
L₉₇₁
L₉₇₂
L₉₇₃
L₉₇₄
L₉₇₅
L₉₇₆
L₉₇₇
L₉₇₈
L₉₇₉
L₉₈₀
L₉₈₁
L₉₈₂
L₉₈₃
L₉₈₄
L₉₈₅
L₉₈₆
L₉₈₇
L₉₈₈
L₉₈₉
L₉₉₀
L₉₉₁
L₉₉₂
L₉₉₃
L₉₉₄
L₉₉₅
L₉₉₆
L₉₉₇
L₉₉₈
L₉₉₉
L₁₀₀₀
L₁₀₀₁
L₁₀₀₂
L₁₀₀₃
L₁₀₀₄
L₁₀₀₅
L₁₀₀₆
L₁₀₀₇
L₁₀₀₈
L₁₀₀₉
L₁₀₁₀
L₁₀₁₁
L₁₀₁₂
L₁₀₁₃
L₁₀₁₄
L₁₀₁₅
L₁₀₁₆
L₁₀₁₇
L₁₀₁₈
L₁₀₁₉
L₁₀₂₀
L₁₀₂₁
L₁₀₂₂
L₁₀₂₃
L₁₀₂₄
L₁₀₂₅
L₁₀₂₆
L₁₀₂₇
L₁₀₂₈
L₁₀₂₉
L₁₀₃₀
L₁₀₃₁<

$$\begin{aligned}
& \wedge \\
& ((M; \quad \overset{C}{j} \models f1 \wedge f2) = \\
& \quad 9i. \text{FirstRise } M \quad c \ i \\
& \quad) \\
& \quad ((M; \quad i \quad \overset{C}{j} \models f1) \\
& \quad \quad \wedge \\
& \quad \quad (M; \quad i \quad \overset{C}{j} \models f2))) \\
& \wedge \\
& ((M; \quad \overset{C}{j} \models X! f) = \\
& \quad 9i. (\text{FirstRise } M \quad c \ i \\
& \quad \quad \wedge \\
& \quad \quad (\text{nite} \quad) \ i < \text{length} \quad - 1)) \\
& \quad) \\
& \quad (M; \quad i+1 \quad \overset{C}{j} \models f)) \\
& \wedge \\
& ((M; \quad \overset{C}{j} \models [f1 \cup f2]) =
\end{aligned}$$

$$((M; \models^c \text{fr1g} \mid \rightarrow \text{fr2g}) = \\ 9i. \text{FirstRise } M \quad c \ i)$$

$$\begin{array}{l} \wedge \\ ((M; s \models [f1 \text{ U } f2]) = \\ \mathbf{9} . \text{Path } M \end{array} \quad \wedge$$