H-0265 (H0901-022) January 26, 2009
Electrical Engineering

IBM Research Report

An Example of a Δ-extendible Proof with a Spurious Interpolant

Oded Fuhrmann, Shlomo Hoory
IBM Research Division
Haifa Research Laboratory
Mt. Carmel 31905
Haifa, Israel

Research Division
Almaden - Austin - Beijing - Cambridge - Haifa - India - T. J. Watson - Tokyo - Zurich

An Example of a Δ-extendible Proof with a Spurious Interpolant

Oded Fuhrmann and Shlomo Hoory

IBM Haifa Research Lab

Abstract. We give an example of a model and a Δ-extendible refutation that a given property hold for all cycles up to $k = 5$. We show that a classical partition of the axioms into initial and final sets A, B where the common variables reside in cycle 2 leads to a 'spurious' interpolant. The interpolant is spurious in the sense that there exists a legeal path from the states conforming to it and a state that violates the specified property.

Keywords:
Craigs Interpolant, Proof Extension

Note: This document was written as a brief footnote to On Extending Bounded Proofs to Inductive Proofs, see [FH09]. As such we assume equiantence with the above and will freely adopt all defenitions and notations.

1 The Example

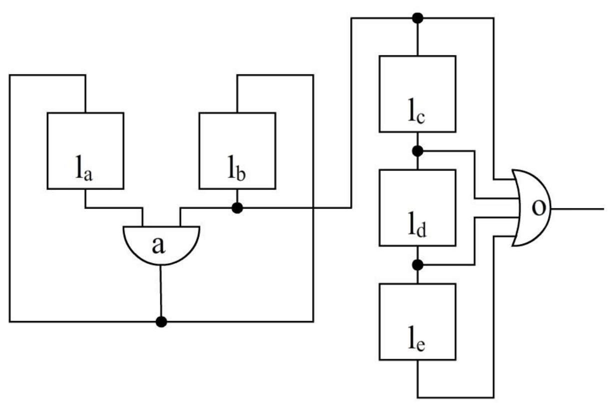


Fig. 1. The model

Consider the model described in Figure 1 in which each box is anottated with the name of the corresponding output net. We examine the case with init constraints $I = \left\{ \left(l_a^0\right), \left(l_b^0\right) \right\}$ and the desired property that net o is true for all cycles. It is easily observed that this specification holds for all cycles. In Figure 2a we give a refutation for the BMC formula, proving that no bug exists up to cycle k=5 for the axioms:

$$I\left(W_0\right) \wedge \bigwedge_{i=1}^{k-1} T\left(W_i, W_{i+1}\right) \wedge \bigvee_{i=1}^{k} P\left(\neg W_i\right),$$

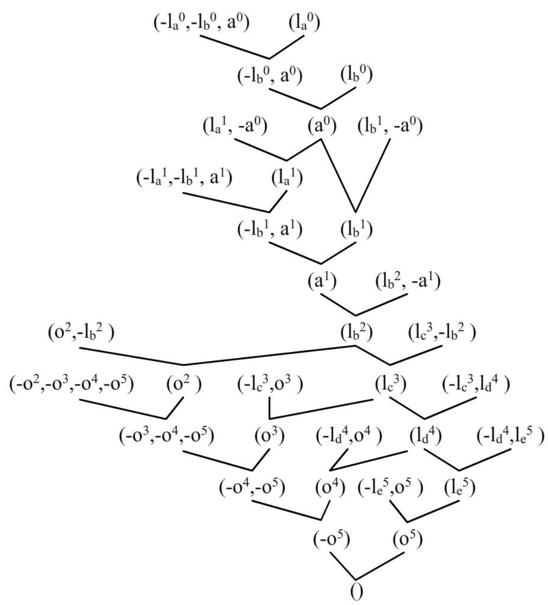
where W_i stands for the set of problem variables at cycle i.

The given proof is 1-extendible since every path from an init axiom in I to the root passes through $u = (a^1)$, and $v = (a^0)$. Therefore, the property holds ad infinitum.

We partition the leaf axioms of the refutation into two sets A,B where A contains all axioms with at least one lit in the $[0 \ldots 2]$ range, and B contains all other axioms. It is easy to verify that the resulting interpolat, Int, computed as described in interpolation [McM03], is $l_b^2 \wedge o^2$. Yet the formula:

$$Int(W_1) \wedge \bigwedge_{i=1}^{k} T(W_i, W_{i+1}) \wedge \bigvee_{i=2}^{k+1} \neg P(W_i),$$

is satisfies for the assignment in Figure 2b, implying that it is a spurious counter example for the interpolant.



(a)

cycle	l_a	l_b	a	l_c	l_d	l_e	o
2	0	1	0	1	1	1	1
3	0	0	0	0	1	1	1
4	0	0	0	0	0	1	1
5	0	0	0	0	0	0	1
6	0	0	0	0	0	0	0

(b)

Fig. 2. (a) A refutation showing that no bug in the first five cycles, (b) An assignment where the interpolant holds, yet the property does not

References

[FH09] Oded Fuhrman and Shlomo Hoory. On extending bounded proofs to inductive proofs. Submitted, 2009.

[McM03] Kenneth L. McMillan. Interpolation and sat-based model checking. In *CAV*, pages 1–13, 2003.