

# PCC: proof carrying code

Alexander Krivutsenko

December 14, 2009

## Introduction to First Order Logic

Idea of PCC

Example



## Introduction to FOL: 2

Given the arbitrary formula in FOL:

$: ((a \wedge \text{Pred1}(b) \rightarrow c)$

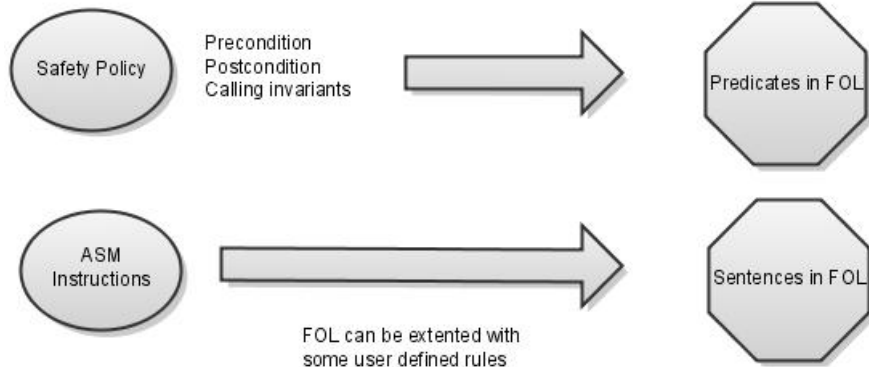
The power of FOL is:

- ▶ *Logical entailment* (inference)
- ▶ Automated theorem proving

The problem of FOL is:

- ▶ Semidecidable: the prover may never halt for some cases
- ▶ NP-COMplete (proving and entailment:  $O(e^n)$ )
- ▶ No arithmetic rules supported... need extension for representing low level code

# Idea of PCC: application for FOL



# Idea of PCC: algorithm

## Code producer

## Code consumer

1. Go through each instruction
2. Map to predicate or sentence in FOL if it is defined for this instruction.
3. Plug all predicates, sentences, pre/post conditions into one FOL formula

---

4. Serialize the formula to binary format using some FOL mapping scheme

5. Use theorem prover to find the formal proof that formula is truth.  
(NPEXP or may be semi-decidable)

6. Serialize the proof

7. Append proof to binary code

4. Get proof from binary

5. Verify that proof is valid for formula.  $O(n)$  at worse

1	ADDQ	r0, 8, r1	%Address of tag in r0
2	LDQ	r0, 8(r0)	%Address of data in r1
3	LDQ	r2, -8(r1)	%Data in r0
4	ADDQ	r0, 1, r0	%Tag in r2
5	BEQ	r2, L1	%Increment Data in r0
6	STQ	r0, 0(r1)	%Skip if tag == 0
L1	RET		%Write back data
			%Done

Safety policy:

- ▶ LDQ with address R within  $2^{64}$  range
- ▶ SDQ with address R within  $2^{64}$  range AND when  $R(8) \neq 0$

Also precondition is: valid address of tag in r0

$$\begin{aligned} SP_r &= \forall r_0. \forall r_m. Pre_r \Rightarrow rd(r_0 \oplus 8) \wedge rd(r_0 \oplus 8 \ominus 8) \\ &\quad \wedge sel(r_m, r_0 \oplus 8 \ominus 8) = 0 \Rightarrow \mathbf{true} \\ &\quad \wedge sel(r_m, r_0 \oplus 8 \ominus 8) \neq 0 \Rightarrow \mathbf{wr}(r_0 \oplus 8) \end{aligned}$$