

Machine-code verification for multiple architectures

— decompilation into logic —

Magnus O. Myreen, Konrad Slind, Michael J. C. Gordon

Macau, Feb 2009

Motivation

Formal verification of machine code:

machine code

code

Motivation

Formal verification of machine code:

machine code

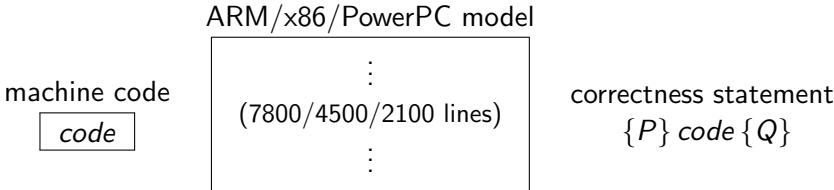
`code`

correctness statement

$\{P\} \text{code} \{Q\}$

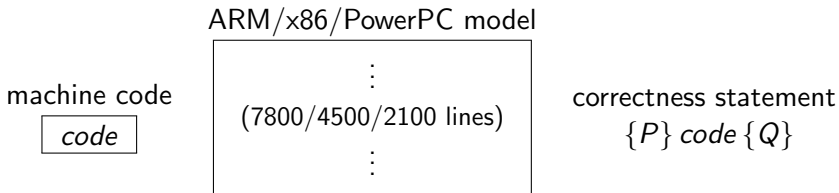
Motivation

Formal verification of machine code:



Motivation

Formal verification of machine code:

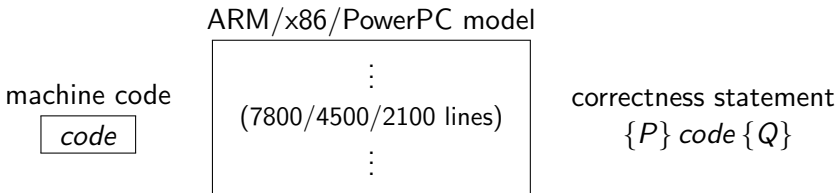


Contribution: a method/tool which

- ▶ exposes as little as possible of the big models to the user;
- ▶ makes non-automatic proofs independent of the models

Motivation

Formal verification of machine code:



Contribution: a method/tool which

- ▶ exposes as little as possible of the big models to the user;
- ▶ makes non-automatic proofs independent of the models

Decompiler — extracts (with proof in HOL4) a function describing the effect of the code on the model.

Talk outline

1. what is decompilation into logic?
2. how to implement decompilation?

Basic idea

Example: Given some hard-to-read (ARM) machine code,

```
0: E3A00000
4: E3510000
8: 12800001
12: 15911000
16: 1AFFFFFB
```

Basic idea

Example: Given some hard-to-read (ARM) machine code,

```
0: E3A00000      mov r0, #0
4: E3510000      L: cmp r1, #0
8: 12800001      addne r0, r0, #1
12: 15911000      ldrne r1, [r1]
16: 1AFFFFFB      bne L
```

Basic idea

Example: Given some hard-to-read (ARM) machine code,

```
0: E3A00000      mov r0, #0
4: E3510000      L: cmp r1, #0
8: 12800001      addne r0, r0, #1
12: 15911000      ldrne r1, [r1]
16: 1AFFFFFB      bne L
```

The decompiler produces a readable HOL4 function:

$$f(r_0, r_1, m) = \text{let } r_0 = 0 \text{ in } g(r_0, r_1, m)$$
$$g(r_0, r_1, m) = \text{if } r_1 = 0 \text{ then } (r_0, r_1, m) \text{ else}$$
$$\quad \text{let } r_0 = r_0 + 1 \text{ in}$$
$$\quad \text{let } r_1 = m(r_1) \text{ in}$$
$$\quad \quad g(r_0, r_1, m)$$

Decompilation, correct?

Decompiler automatically proves, in HOL, a certificate which states that f describes the effect of the ARM code:

$$f_{pre}(r_0, r_1, m) \Rightarrow$$

$$\{ (R0, R1, M) \text{ is } (r_0, r_1, m) * \text{PC } p * S \}$$

$$p : \text{E3A00000 E3510000 12800001 15911000 1AFFFFF B}$$

$$\{ (R0, R1, M) \text{ is } f(r_0, r_1, m) * \text{PC } (p + 20) * S \}$$

Read informally as:

if initially reg 0, reg 1 and memory described by (r_0, r_1, m) , then the code terminates with reg 0, reg 1 and memory as $f(r_0, r_1, m)$

Decompilation, example

Precondition f_{pre} keeps track of side-conditions:

$$f_pre(r_0, r_1, m) = \text{let } r_0 = 0 \text{ in } g_pre(r_0, r_1, m)$$

$$g_pre(r_0, r_1, m) = \text{if } r_1 = 0 \text{ then } \mathit{true} \text{ else}$$
$$\quad \text{let } r_0 = r_0 + 1 \text{ in}$$
$$\quad \text{let } \mathit{cond} = r_1 \in \text{domain } m \wedge \mathit{aligned}(r_1) \text{ in}$$
$$\quad \text{let } r_1 = m(r_1) \text{ in}$$
$$\quad g_pre(r_0, r_1, m) \wedge \mathit{cond}$$

Decompilation, verification example

Decompiler automatically produced: f , f_{pre} and certificate.

Decompilation, verification example

Decompiler automatically produced: f , f_{pre} and certificate.

To verify functional correctness, formalise “linked-list in memory”:

$$list(nil, a, m) = a = 0$$

$$list(cons\ x\ l, a, m) = \exists a'. m(a) = a' \wedge m(a+4) = x \wedge a \neq 0 \wedge list(l, a', m) \wedge aligned(a)$$

Decompilation, verification example

Decompiler automatically produced: f , f_{pre} and certificate.

To verify functional correctness, formalise “linked-list in memory”:

$$list(nil, a, m) = a = 0$$

$$list(cons\ x\ l, a, m) = \exists a'. m(a) = a' \wedge m(a+4) = x \wedge a \neq 0 \wedge \\ list(l, a', m) \wedge aligned(a)$$

Manual part of verification proof (14 lines in HOL4):

$$\forall x\ l\ a\ m. list(l, a, m) \Rightarrow f(x, a, m) = (length(l), 0, m)$$

$$\forall x\ l\ a\ m. list(l, a, m) \Rightarrow f_{pre}(x, a, m)$$

Decompilation, verification example, cont.

Using the automatically proved certificate:

$$f_{pre}(r_0, r_1, m) \Rightarrow$$

$$\{ (R0, R1, M) \text{ is } (r_0, r_1, m) * \text{PC } p * S \}$$

p : E3A00000 E3510000 12800001 15911000 1AFFFFFFB

$$\{ (R0, R1, M) \text{ is } f(r_0, r_1, m) * \text{PC } (p + 20) * S \}$$

Decompilation, verification example, cont.

Using the automatically proved certificate:

$list(l, r_1, m) \Rightarrow$

$f_{pre}(r_0, r_1, m) \Rightarrow$

$\{ (R0, R1, M) \text{ is } (r_0, r_1, m) * PC \ p * S \}$

$p : E3A00000 \ E3510000 \ 12800001 \ 15911000 \ 1AFFFFFFB$

$\{ (R0, R1, M) \text{ is } f(r_0, r_1, m) * PC \ (p + 20) * S \}$

Decompilation, verification example, cont.

Using the automatically proved certificate:

$list(l, r_1, m) \Rightarrow$

$\{ (R0, R1, M) \text{ is } (r_0, r_1, m) * PC\ p * S \}$

$p : E3A00000\ E3510000\ 12800001\ 15911000\ 1AFFFFFFB$

$\{ (R0, R1, M) \text{ is } f(r_0, r_1, m) * PC\ (p + 20) * S \}$

Decompilation, verification example, cont.

Using the automatically proved certificate:

$list(l, r_1, m) \Rightarrow$

$\{ (R0, R1, M) \text{ is } (r_0, r_1, m) * PC \ p * S \}$

$p : E3A00000 \ E3510000 \ 12800001 \ 15911000 \ 1AFFFFFFB$

$\{ (R0, R1, M) \text{ is } (length(l), 0, m) * PC \ (p + 20) * S \}$

Decompilation, proof reuse

x86	0:	31C0	xor eax, eax
	2:	85F6	L1: test esi, esi
	4:	7405	jz L2
	6:	40	inc eax
	7:	8B36	mov esi, [esi]
	9:	EBF7	jmp L1

L2:

PowerPC	0:	38A00000	addi 5,0,0
	4:	2C140000	L1: cmpwi 20,0
	8:	40820010	bc 4,2,L2
	12:	7E80A02E	lwzx 20,0(20)
	16:	38A50001	addi 5,5,1
	20:	4BFFFFFF0	b L1

L2:

Decompilation, proof reuse, cont.

Decompilation of x86 and PowerPC code:

$$f'(eax, esi, m) = \text{let } eax = eax \otimes eax \text{ in } g'(eax, esi, m)$$

$$g'(eax, esi, m) = \text{if } esi \& esi = 0 \text{ then } (eax, esi, m) \text{ else} \\ \text{let } eax = eax + 1 \text{ in} \\ \text{let } esi = m(es_i) \text{ in} \\ g'(eax, esi, m)$$

$$f''(r_5, r_{20}, m) = \text{let } r_5 = 0 \text{ in } g''(r_5, r_{20}, m)$$

$$g''(r_5, r_{20}, m) = \text{if } r_{20} = 0 \text{ then } (r_5, r_{20}, m) \text{ else} \\ \text{let } r_{20} = m(r_{20}) \text{ in} \\ \text{let } r_5 = r_5 + 1 \text{ in} \\ g''(r_5, r_{20}, m)$$

But in this case, easy to prove $f = f' = f''$ (3 lines in HOL4).

Decompilation, in a nut shell

Proof-producing decompilation:

- ▶ takes machine code, returns function and certificate
- ▶ keeps manual proofs independent of underlying model
(possible proof reuse)

Talk outline

1. what is decompilation into logic?
2. how to implement decompilation?

Talk outline

1. what is decompilation into logic?
2. how to implement decompilation?
 - ▶ processor models
 - ▶ machine-code specifications: “{...} *code* {...}”
 - ▶ tail-recursive functions

ISA models

Underlying ISA specifications:

ARM – developed by Anthony Fox, verified against a register-transfer level model of an ARM processor;

x86 – developed together with Susmit Sarkar, Peter Sewell, Scott Owens, etc, heavily tested against a real processor;

PowerPC – a HOL4 translation of Xavier Leroy's PowerPC model, used in his proof of an optimising C compiler.

Large detailed models...

Machine code, x86

Even 'simple' instructions get complex definition.

Sequential op.sem. evaluated for instruction "40" (i.e. `inc eax`):

```
x86_read_reg EAX state = eax ∧
x86_read_eip state = eip ∧
x86_read_mem eip state = some 0x40 ⇒
x86_next state =
  some (x86_write_reg EAX (eax + 1)
        (x86_write_eip (eip + 1)
          (x86_write_eflag AF none
            (x86_write_eflag SF (some (sign_of (eax + 1))))
            (x86_write_eflag ZF (some (eax + 1 = 0)))
            (x86_write_eflag PF (some (parity_of (eax + 1))))
            (x86_write_eflag OF none state))))))
```

Here some/none types used for modelled/non-modelled values.

Machine code, specifications

A machine-code specifications:

$$\{ R \text{ EAX } a * \text{ EIP } p * S \}$$

$$p : 40$$

$$\{ R \text{ EAX } (a+1) * \text{ EIP } (p+1) * S \}$$

where S existentially quantifies the status flags:

$$S = \exists a s z p o. \text{ eflag AF } a * \text{ eflag SF } s * \text{ eflag ZF } z * \dots$$

Machine code, specifications

A machine-code specifications:

$$\forall P. \{ R \text{ EAX } a * \text{ EIP } p * S * P \}$$
$$p : 40$$
$$\{ R \text{ EAX } (a+1) * \text{ EIP } (p+1) * S * P \}$$

where S existentially quantifies the status flags:

$$S = \exists a s z p o. \text{ eflag AF } a * \text{ eflag SF } s * \text{ eflag ZF } z * \dots$$

Machine code, specifications

A machine-code specifications:

$$\{ R \text{ EAX } a * \text{ EIP } p * S * R \text{ EBX } b \}$$

$$p : 40$$

$$\{ R \text{ EAX } (a+1) * \text{ EIP } (p+1) * S * R \text{ EBX } b \}$$

where S existentially quantifies the status flags:

$$S = \exists a s z p o. \text{ eflag AF } a * \text{ eflag SF } s * \text{ eflag ZF } z * \dots$$

Machine code, specifications

A machine-code specifications:

$$\{ R \text{ EAX } a * \text{ EIP } p * S * R \text{ EBX } b \}$$

$$p : 40$$

$$\{ R \text{ EAX } (a+1) * \text{ EIP } (p+1) * S * R \text{ EBX } b \}$$

$$\{ R \text{ EAX } a * \text{ EIP } p * S * R \text{ EBX } b \}$$

$$p : 01D8$$

$$\{ R \text{ EAX } (a+b) * \text{ EIP } (p+2) * S * R \text{ EBX } b \}$$

where S existentially quantifies the status flags:

$$S = \exists a s z p o. \text{ eflag AF } a * \text{ eflag SF } s * \text{ eflag ZF } z * \dots$$

Machine code, specifications

A machine-code specifications:

$$\{ R \text{ EAX } a * \text{ EIP } p * S * R \text{ EBX } b \}$$

$$p : 40$$

$$\{ R \text{ EAX } (a+1) * \text{ EIP } (p+1) * S * R \text{ EBX } b \}$$

$$\{ R \text{ EAX } (a+1) * \text{ EIP } (p+1) * S * R \text{ EBX } b \}$$

$$p+1 : 01D8$$

$$\{ R \text{ EAX } (a+1+b) * \text{ EIP } (p+3) * S * R \text{ EBX } b \}$$

where S existentially quantifies the status flags:

$$S = \exists a s z p o. \text{ eflag AF } a * \text{ eflag SF } s * \text{ eflag ZF } z * \dots$$

Machine code, specifications

A machine-code specifications:

$$\{ R \text{ EAX } a * \text{ EIP } p * S * R \text{ EBX } b \}$$
$$p : 4001D8$$
$$\{ R \text{ EAX } (a+1+b) * \text{ EIP } (p+3) * S * R \text{ EBX } b \}$$

where S existentially quantifies the status flags:

$$S = \exists a s z p o. \text{ eflag AF } a * \text{ eflag SF } s * \text{ eflag ZF } z * \dots$$

Tail-recursive functions

How to implement the proof-producing translation?

Key ideas:

1. define functions as instances of

$$\mathit{tailrec}(x) = \text{if } G(x) \text{ then } \mathit{tailrec}(F(x)) \text{ else } D(x)$$

Tail-recursive functions

How to implement the proof-producing translation?

Key ideas:

1. define functions as instances of

$$\textit{tailrec}(x) = \text{if } G(x) \text{ then } \textit{tailrec}(F(x)) \text{ else } D(x)$$

2. specify termination for value x as

$$\textit{pre}(x) = \exists n. \neg(G(F^n(x)))$$

Tail-recursive functions

How to implement the proof-producing translation?

Key ideas:

1. define functions as instances of

$$tailrec(x) = \text{if } G(x) \text{ then } tailrec(F(x)) \text{ else } D(x)$$

2. specify termination for value x as

$$pre(x) = \exists n. \neg(G(F^n(x)))$$

3. but give the user

$$pre(x) = \text{if } G(x) \text{ then } pre(F(x)) \text{ else true}$$

Tail-recursive functions

How to implement the proof-producing translation?

Key ideas:

1. define functions as instances of

$$tailrec(x) = \text{if } G(x) \text{ then } tailrec(F(x)) \text{ else } D(x)$$

2. specify termination for value x as

$$pre(x) = \exists n. \neg(G(F^n(x))) \wedge (\forall x. \dots \Rightarrow H(x))$$

3. but give the user

$$pre(x) = (\text{if } G(x) \text{ then } pre(F(x)) \text{ else true}) \wedge H(x)$$

4. actually also insert side-condition $H(x)$

Tail-recursive functions, cont.

5. use the following loop rule, one loop at a time:

$\forall P Q F D G H$ code.

$$(\forall x. H(x) \wedge G(x) \Rightarrow \{P(x)\} \text{ code } \{P(F(x))\}) \Rightarrow$$

$$(\forall x. H(x) \wedge \neg G(x) \Rightarrow \{P(x)\} \text{ code } \{Q(D(x))\}) \Rightarrow$$

$$(\forall x. \text{pre}(x) \Rightarrow \{P(x)\} \text{ code } \{Q(\text{tailrec}(x))\})$$

Decompilation algorithm

Algorithm:

1. derive specifications for individual instructions;
2. find control flow;
3. compose specifications;
4. apply loop rule;
5. exit or go to step 3.

Details in paper at FMCAD 2008.

Decompilation, restrictions

Restrictions:

1. **heuristics used for control-flow discovery**, cannot handle code-pointers (except subroutine call/return).
2. **underlying ISA model must be deterministic** (at least for the code which is decompiled).

Robust: heuristics only used for control-flow discovery.

Applications

Verification case studies done:

- ▶ copying garbage collectors
- ▶ LISP primitives: car, cdr, cons, equal, ...
- ▶ parser and printer for LISP s-expressions

Applications

Verification case studies done:

- ▶ copying garbage collectors
- ▶ LISP primitives: car, cdr, cons, equal, ...
- ▶ parser and printer for LISP s-expressions

Used for proof-producing compiler, to compile function f :

1. generate code for f ;
2. decompile code to produce f' ;
3. automatically prove $f = f'$.

Applications

Verification case studies done:

- ▶ copying garbage collectors
- ▶ LISP primitives: car, cdr, cons, equal, ...
- ▶ parser and printer for LISP s-expressions

Used for proof-producing compiler, to compile function f :

1. generate code for f ;
2. decompile code to produce f' ;
3. automatically prove $f = f'$.

$$(F = F' \wedge G = G' \wedge D = D' \implies \text{tailrec}_{F,G,D} = \text{tailrec}_{F',G',D'})$$

Applications

Verification case studies done:

- ▶ copying garbage collectors
- ▶ LISP primitives: car, cdr, cons, equal, ...
- ▶ parser and printer for LISP s-expressions

Used for proof-producing compiler, to compile function f :

1. generate code for f ;
2. decompile code to produce f' ;
3. automatically prove $f = f'$.

$$(F = F' \wedge G = G' \wedge D = D' \implies \text{tailrec}_{F,G,D} = \text{tailrec}_{F',G',D'})$$

- ▶ Compiler used to produce verified LISP evaluators.

Further work

Decompile to more abstract functions:

Connect decompiler to other tools:

Further work

Decompile to more abstract functions:

- ▶ e.g. machine code for list reverse should produce:

$$\begin{aligned}f(xs) &= g(xs, []) \\g(xs, ys) &= \text{if } xs = [] \text{ then } ys \\ &\quad \text{else } g(\text{tail}(xs), \text{cons}(\text{head}(xs), ys))\end{aligned}$$

- ▶ a few heauristics could implement this...

Connect decompiler to other tools:

Further work

Decompile to more abstract functions:

- ▶ e.g. machine code for list reverse should produce:

$$\begin{aligned}f(xs) &= g(xs, []) \\g(xs, ys) &= \text{if } xs = [] \text{ then } ys \\ &\quad \text{else } g(\text{tail}(xs), \text{cons}(\text{head}(xs), ys))\end{aligned}$$

- ▶ a few heauristics could implement this...

Connect decompiler to other tools:

- ▶ Import annotations from tools by Peter O'Hearn's group;

Further work

Decompile to more abstract functions:

- ▶ e.g. machine code for list reverse should produce:

$$\begin{aligned}f(xs) &= g(xs, []) \\g(xs, ys) &= \text{if } xs = [] \text{ then } ys \\ &\quad \text{else } g(\text{tail}(xs), \text{cons}(\text{head}(xs), ys))\end{aligned}$$

- ▶ a few heauristics could implement this...

Connect decompiler to other tools:

- ▶ Import annotations from tools by Peter O'Hearn's group;
- ▶ Link to automatic crypto prover by Eric W. Smith.

Summary

1. decompilation: given code, produces function and certificate;

Summary

1. decompilation: given code, produces function and certificate;
2. allows users to only deal with tail-recursive functions, instead of machine code;

Summary

1. decompilation: given code, produces function and certificate;
2. allows users to only deal with tail-recursive functions, instead of machine code;
3. separates manual proofs from definitions of processor state (thus scope for some proof-reuse);

Summary

1. decompilation: given code, produces function and certificate;
2. allows users to only deal with tail-recursive functions, instead of machine code;
3. separates manual proofs from definitions of processor state (thus scope for some proof-reuse);
4. 'easy' to implement (only 2500 lines of ML on top of HOL4).

Summary

1. decompilation: given code, produces function and certificate;
2. allows users to only deal with tail-recursive functions, instead of machine code;
3. separates manual proofs from definitions of processor state (thus scope for some proof-reuse);
4. 'easy' to implement (only 2500 lines of ML on top of HOL4).

Questions?