

# Formal Verification in Industry

John Harrison

Intel Corporation

- The cost of bugs
- Formal verification
- Machine-checked proof
- Automatic and interactive approaches
- HOL Light
- Floating point verification
- Tangent example
- Conclusions

## The human cost of bugs

Computers are often used in safety-critical systems where a failure could cause loss of life.

- Heart pacemakers
- Aircraft
- Nuclear reactor controllers
- Car engine management systems
- Radiation therapy machines
- Telephone exchanges (!)
- ...

## Financial cost of bugs

Even when not a matter of life and death, bugs can be financially serious if a faulty product has to be recalled or replaced.

- 1994 FDIV bug in the Intel®Pentium® processor: US \$500 million.
- Today, new products are ramped much faster...

So Intel is especially interested in all techniques to reduce errors.

## Complexity of designs

At the same time, market pressures are leading to more and more complex designs where bugs are more likely.

- A 4-fold increase in bugs in Intel processor designs per generation.
- Approximately 8000 bugs introduced during design of the Pentium 4.

Fortunately, pre-silicon detection rates are now very close to 100%.

Just enough to tread water...

## Limits of testing

Bugs are usually detected by extensive testing, including pre-silicon simulation.

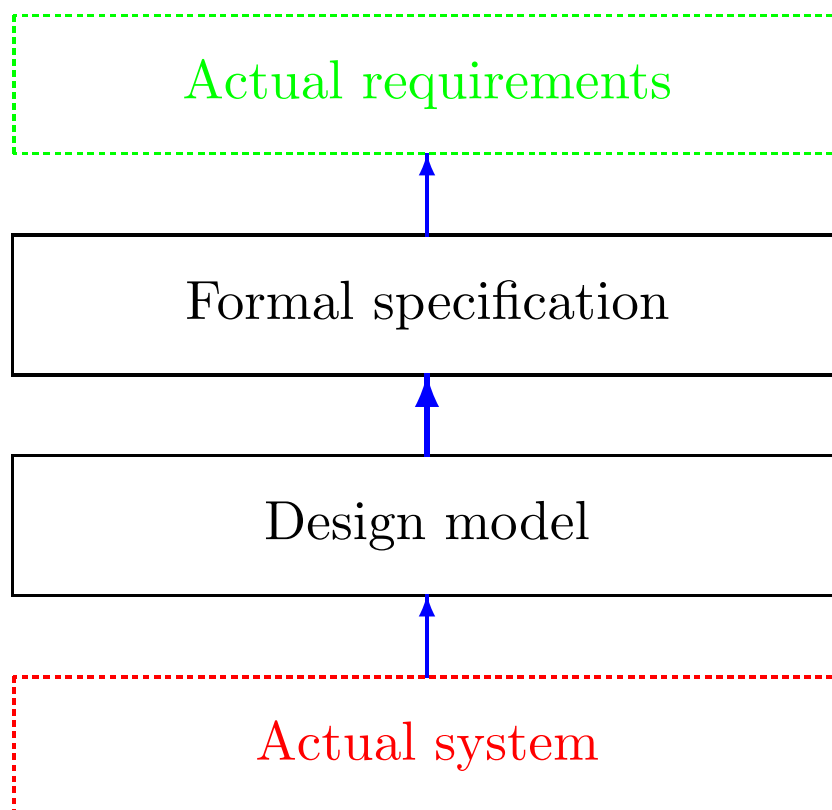
- Slow — especially pre-silicon
- Too many possibilities to test them all

For example:

- $2^{160}$  possible pairs of floating point numbers (possible inputs to an adder).
- Vastly higher number of possible states of a complex microarchitecture.

## Formal verification

Formal verification: mathematically prove the correctness of a *design* with respect to a mathematical *formal specification*.



## Verification vs. testing

Verification has some advantages over testing:

- Exhaustive.
- Improves our intellectual grasp of the system.

However:

- Difficult and time-consuming.
- Only as reliable as the formal models used.
- How can we be sure the proof is right?

## Analogy with mathematics

Sometimes even a huge weight of empirical evidence can be misleading.

- $\pi(n)$  = number of primes  $\leq n$
- $li(n) = \int_0^n du/\ln(u)$

Littlewood proved in 1914 that  $\pi(n) - li(n)$  changes sign infinitely often.

No change of sign at all had ever been found despite testing up to  $n = 10^{10}$  (in the days before computers).

Similarly, extensive testing of hardware or software may still miss errors that would be revealed by a formal proof.



## Formal verification is hard

Writing out a completely formal proof of correctness for real-world hardware and software is difficult.

- Must specify intended behaviour formally
- Need to make many hidden assumptions explicit
- Requires long detailed proofs, difficult to review

The state of the art is quite limited.

Software verification has been around since the 60s, but there have been few major successes.

## Faulty hand proofs

“Synchronizing clocks in the presence of faults”  
(Lamport & Melliar-Smith, JACM 1985)

This introduced the Interactive Convergence Algorithm for clock synchronization, and presented a ‘proof’ of it.

- Presented five supporting lemmas and one main correctness theorem.
- Lemmas 1, 2, and 3 were all false.
- The proof of the main induction in the final theorem was wrong.
- The main result, however, was correct!

## Machine-checked proof

A more promising approach is to have the proof checked (or even generated) by a computer program.

- It can reduce the risk of mistakes.
- The computer can automate some parts of the proofs.

There are limits on the power of automation, so detailed human guidance is usually necessary.

## Automatic verification?

Many problems can be attacked using decision methods with (in principle!) limited human intervention, e.g.

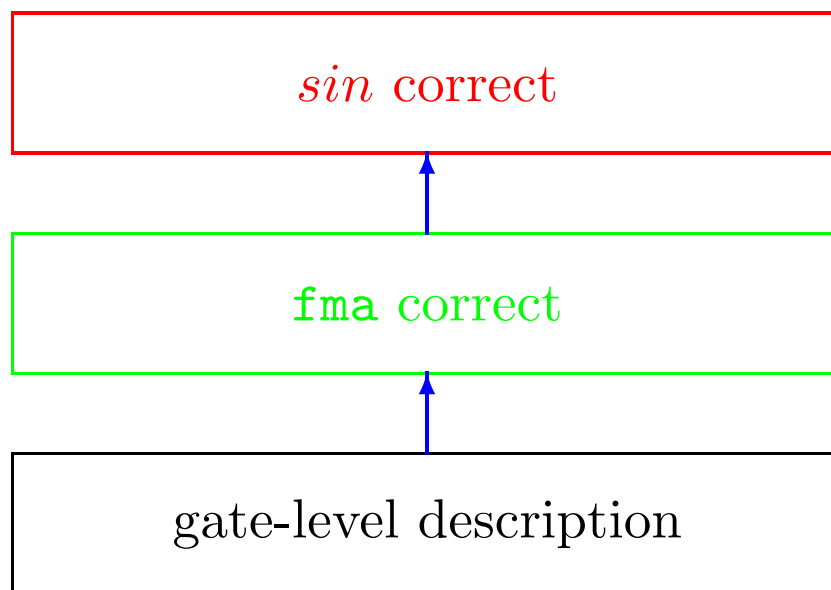
- Boolean equivalence checking
- Temporal logic model checking
- Symbolic trajectory evaluation

This probably accounts for the relative success of formal verification in hardware.

However, sometimes we need more general theorem proving, especially for the kinds of applications I'm interested in...

## Levels of verification

My job involves verifying higher-level floating-point algorithms based on assumed correct behavior of hardware primitives.



We will assume that all the operations used obey the underlying specifications as given in the Architecture Manual and the IEEE Standard for Binary Floating-Point Arithmetic.

This is a typical *specification* for lower-level verification (someone else's job).

## The spectrum of theorem provers

From interactive proof checkers to fully automatic theorem provers.

**AUTOMATH** (de Bruijn)

**Stanford LCF** (Milner)

**Mizar** (Trybulec)

...

...

**PVS** (Owre, Rushby, Shankar)

...

...

**ACL2** (Boyer, Kaufmann, Moore)

**Otter** (McCune)

## Automation vs. expressiveness

Tools like Boolean tautology checkers and symbolic model checkers are:

- Completely automatic
- Efficient enough for nontrivial problems
- Incapable even of expressing, let alone proving, many interesting properties.

On the other hand, proof checkers like Mizar:

- Can prove essentially any mathematical theorem in principle
- Require detailed and explicit human guidance even for relatively simple problems.

To verify interesting floating-point algorithms, we need automation *and* expressiveness.

## HOL Light

HOL Light is based on the approach to theorem proving pioneered in Edinburgh LCF in the 70s.

- All theorems created by low-level primitive rules.
- Guaranteed by using an abstract type of theorems; no need to store proofs.
- ML available for implementing derived rules by arbitrary programming.

The system can be extended reliably without making unsafe modifications

The user controls the means of production (of theorems).



## Other LCF theorem provers

There are many versions of HOL:

- HOL88
- hol90
- ProofPower
- HOL Light
- hol98
- HOL 4

and several other provers based on LCF:

- Coq
- Isabelle
- Nuprl

## Floating point verification

We've used HOL Light to verify the accuracy of floating point algorithms (used in hardware and software) for:

- Division and square root
- Transcendental function such as *sin*, *exp*, *atan*.

This involves background work in formalizing:

- Real analysis
- Basic floating point arithmetic

## Existing real analysis theory

- Definitional construction of real numbers
- Basic topology
- General limit operations
- Sequences and series
- Limits of real functions
- Differentiation
- Power series and Taylor expansions
- Transcendental functions
- Gauge integration

## Examples of useful theorems

$$\begin{aligned} &|- \sin(x + y) = \\ &\quad \sin(x) * \cos(y) + \cos(x) * \sin(y) \end{aligned}$$

$$|- \tan(n * \pi) = 0$$

$$\begin{aligned} &|- 0 < x \wedge 0 < y \\ &\quad ==> (\ln(x / y) = \ln(x) - \ln(y)) \end{aligned}$$

$$\begin{aligned} &|- f \text{ contl } x \wedge g \text{ contl } (f \ x) \\ &\quad ==> (g \circ f) \text{ contl } x \end{aligned}$$

$$\begin{aligned} &|- (!x. a \leq x \wedge x \leq b \\ &\quad ==> (f \text{ diff1 } (f' \ x)) \ x) \wedge \\ &\quad f(a) \leq K \wedge f(b) \leq K \wedge \\ &\quad (!x. a \leq x \wedge x \leq b \wedge (f'(x) = 0)) \\ &\quad ==> f(x) \leq K \\ &\quad ==> !x. a \leq x \wedge x \leq b ==> f(x) \leq K \end{aligned}$$

## HOL floating point theory

Generic floating point theory in HOL.

Can be applied to all the required formats, and others supported in software.

Precise specification of floating point rounding, floating point exceptions etc. Typical theorems include monotonicity of rounding:

$$\begin{aligned} &|- \sim(\text{precision fmt} = 0) \wedge x \leq y \\ &==> \text{round fmt rc } x \leq \text{round fmt rc } y \end{aligned}$$

and subtraction of nearby floating point numbers:

$$\begin{aligned} &|- a \text{ IN iformat fmt } \wedge b \text{ IN iformat fmt } \wedge \\ & a / \&2 \leq b \wedge b \leq \&2 * a \\ &==> (b - a) \text{ IN iformat fmt} \end{aligned}$$

## Example: tangent algorithm

Works essentially as follows.

- The input number  $X$  is first reduced to  $r$  with approximately  $|r| \leq \pi/4$  such that  $X = r + N\pi/2$  for some integer  $N$ . We now need to calculate  $\pm \tan(r)$  or  $\pm \cot(r)$  depending on  $N$  modulo 4.
- If the reduced argument  $r$  is still not small enough, it is separated into its leading few bits  $B$  and the trailing part  $x = r - B$ , and the overall result computed from  $\tan(x)$  and pre-stored functions of  $B$ , e.g.

$$\tan(B + x) = \tan(B) + \frac{\frac{1}{\sin(B)\cos(B)}\tan(x)}{\cot(B) - \tan(x)}$$

- Now a power series approximation is used for  $\tan(r)$ ,  $\cot(r)$  or  $\tan(x)$  as appropriate.

## Overview of the verification

To verify this algorithm, we need to prove:

- The range reduction to obtain  $r$  is done accurately.
- The mathematical facts used to reconstruct the result from components are applicable.
- The pre-stored constants such as  $\tan(B)$  are sufficiently accurate.
- The power series approximation does not introduce too much error in approximation.
- The rounding errors involved in computing with floating point arithmetic are within bounds.

Most of these parts are non-trivial. Moreover, some of them require more pure mathematics than might be expected.

## Why mathematics?

Controlling the error in range reduction becomes difficult when the reduced argument  $X - N\pi/2$  is small.

To check that the computation is accurate enough, we need to know:

How close can a floating point number be to an integer multiple of  $\pi/2$ ?

Even deriving the power series (for  $0 < |x| < \pi$ ):

$$\cot(x) = 1/x - \frac{1}{3}x - \frac{1}{45}x^3 - \frac{2}{945}x^5 - \dots$$

is much harder than you might expect.



## Conclusions

- Formal verification of mathematical algorithms is industrially important, and can be attacked with current theorem proving technology.
- A large part of the work involves building up general theories about both pure mathematics and special properties of floating point numbers.
- It is easy to underestimate the amount of pure mathematics needed for obtaining very practical results.
- The mathematics required is often the sort that is not found in current textbooks: very concrete results but with a proof!
- Using HOL Light, we can confidently integrate all the different aspects of the proof, using programmability to automate tedious parts.