Complex Quantifier Elimination in HOL

John Harrison

Intel Corporation

- What is quantifier elimination?
- Why over the complex numbers?
- Geometry theorem proving

Quantifier elimination

Given a formula in some particular class, return one with no quantifiers that is equivalent. For example over the natural numbers:

$$(\forall z.\, x < z \Longrightarrow y < z) \equiv y \leq x$$

or over the real numbers:

$$(\exists x.\, ax^2 + bx + c = 0) \equiv$$
$$a \neq 0 \wedge b^2 \geq 4ac \vee a = 0 \wedge (b \neq 0 \vee c = 0)$$

A convenient way of getting a decision procedure for closed formulas: eliminate quantifiers and then just 'evaluate' the quantifier-free equivalent.

Why over the complex numbers

Over the reals, quantifier elimination is possible (Tarski,...). This has actually been implemented in HOL. But it's too inefficient for interesting problems.

Over the naturals or integers, we can only eliminate quantifiers from 'linear' formulas, so we can't make interesting use of multiplication.

Over the complex numbers, we can use multiplication, but the algorithm is efficient enough to manage some non-trivial examples, e.g:

```
|- !x a.
       (a pow 2 = Cx (&2)) /\
       (x pow 2 + a * x + Cx (&1) = Cx (&0))
       ==> (x pow 4 + Cx (&1) = Cx (&0))
```

Universal problems like this are solved more efficiently using *Gröbner bases* than the general procedure.

Geometry theorem proving

We can prove virtually any Euclidean geometry theorem by reducing it to real coordinates and using Tarski's procedure. In practice it's hopeless.

However, as noted by Wu, many theorems remain true if we allow complex 'coordinates'. Then we can use Gröbner bases etc. For example:

```
|- collinear x a0 a3 /\
   collinear x a1 a2 /\
   collinear y a2 a3 /\
   collinear y a1 a0 /\
   is_midpoint m1 (a1,a3) /\
   is_midpoint m2 (a0,a2) /\
   is_midpoint m3 (x,y)
   ==> collinear m1 m2 m3
```

This is a result known as *Gauss's theorem*. Proved automatically in 17 second on my laptop using HOL Light.