1 Complex quantifier elimination

There is a general procedure for transforming every formula involving complex addition and multiplication into a quantifier-free equivalent, e.g.

$$
\begin{aligned}
&(\exists x\ y.\ ax^2 + bx + c = 0 \wedge ay^2 + by + c = 0 \wedge \neg(x = y)) \\
&\equiv a = 0 \wedge b = 0 \wedge c = 0 \vee \neg(a = 0) \wedge \neg(b^2 = 4ac)
\end{aligned}
$$

Although there are similar procedures for the reals, they are sufficiently inefficient that they're not useful for many practical cases.

There are procedures for naturals and integers, but only for the linear case — no non-trivial use of multiplication.

2 Constructing the complex numbers

We construct $\mathbb{C}$ as isomorphic to $\mathbb{R} \times \mathbb{R}$. The type bijections are `complex` : $\mathbb{R} \times \mathbb{R} \to \mathbb{C}$ and `coords` : $\mathbb{C} \to \mathbb{R} \times \mathbb{R}$. Using the auxiliary functions:

```
|- Re(z) = FST(coords(z))

|- Im(z) = SND(coords(z))
```

we define the operations on complex numbers in terms of the real operations, e.g.

```
|- w + z = complex(Re(w) + Re(z),Im(w) + Im(z))

|- w * z = complex(Re(w) * Re(z) - Im(w) * Im(z),
                   Re(w) * Im(z) + Im(w) * Re(z))
```

It's easy to prove all the basic properties of the operations. We also define the 'modulus' function `mod` : $\mathbb{C} \to \mathbb{R}$ and the square root function `csqrt` : $\mathbb{C} \to \mathbb{C}$ and prove basic properties.

3 Fundamental theorem of algebra

The basic theorem underlying quantifier elimination is the Fundamental Theorem of Algebra: every nonconstant polynomial has a root. Our proof is a formalization of a fairly standard one:

- For any nonconstant polynomial p and bound M, there's a radius R outside which the modulus of the polynomial exceeds M, i.e. $|z| > R \Longrightarrow |p(z)| > M$.
- Within any closed disc $|z| \leq R$, a polynomial attains its minimum modulus somewhere
- If the modulus $|p(z)| = m$ is nonzero at any point, it is possible to find arbitrarily close points z' with $|p(z')| < m$.

Putting these pieces together, we get the final result.

4 Quantifier elimination

Because of the Fundamental Theorem of Algebra

$$\forall x.\, p(x) = 0 \Longrightarrow q(x) = 0$$

is equivalent to $p \mid q^{\partial(p)}$ where $\partial(p)$ denotes the degree of p and '|' the divisibility relation on polynomials. For if we imagine the two polynomials split into linear factors, the assertion becomes:

$$\forall x. (x - a_1) \cdots (x - a_n) = 0 \Longrightarrow (x - b_1) \cdots (x - b_m) = 0$$

That is, each a_i must also be among the b_j and hence each $x - a_i$ must occur among the $x - b_j$. However it may occur up to n times.

It's sufficient to consider only this special case, because we can transform formulas in various ways including using $p(x) = 0 \lor q(x) = 0 \equiv p(x)q(x) = 0$ and cancelling between multiple equations.

5 Examples

Note that this implies that over the reals $x^2 + \sqrt{2}x + 1 \neq 0$.

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

A simple existential assertion:

```
|- !a b. ~(a = b)
         ==> ?x y. (y * x pow 2 = a) /\ (y * x pow 2 + x = b)
```

The following can be considered as asserting that two non-parallel lines have an intersection.

```
|- !a1 b1 c1 a2 b2 c2.
       ~(a1 * b2 = a2 * b1)
       ==> ?x y. (a1 * x + b1 * y = c1) /\ (a2 * x + b2 * y = c2)
```

6 Gröbner bases

For proving purely *universal* assumptions, we can use a more efficient procedure based on Gröbner bases. By negating and transforming to DNF, it suffices to prove that certain polynomial families have no common solution:

$$\begin{aligned}\neg(\exists x_1, \ldots, x_n.\ & p_1(x_1, \ldots, x_n) = 0 \wedge \cdots \wedge \\ & p_k(x_1, \ldots, x_n) = 0)\end{aligned}$$

If this is indeed true, the Gröbner basis algorithm can be “logged” to give us polynomials q_i such that (as a polynomial identity):

$$\begin{aligned}& q_1(x_1, \ldots, x_n) \cdot p_1(x_1, \ldots, x_n) + \cdots + \\ & q_n(x_1, \ldots, x_n) \cdot p_n(x_1, \ldots, x_n) = 1\end{aligned}$$

We can easily use this in HOL to refute the existential assertion and hence verify universal assumptions. For the limited subset, generally much faster, e.g. the following in 1.8 seconds instead of 203.2:

```
|- !a b c x y.
        (a * x pow 2 + b * x + c = Cx(&0)) /\
        (a * y pow 2 + b * y + c = Cx(&0)) /\
        ~(x = y)
        ==> (a * (x + y) + b = Cx(&0))
```

7 Geometry theorem proving

We can encode geometric assertions using coordinate translations over the reals, e.g.

```
|- collinear a b c =
        ((FST a - FST b) * (SND b - SND c) =
         (SND a - SND b) * (FST b - FST c))

|- is_midpoint b (a,c) =
       (&2 * FST b = FST a + FST c) /\
       (&2 * SND b = SND a + SND c)

|- is_intersection p (a,b) (c,d) =
      collinear a p b /\ collinear c p d
```

Many theorems that are universal assertions remain true if we generalize the “coordinates” to complex numbers, when we can use our relatively efficient decision procedures. For example Gauss’s theorem is proved in 17.01 seconds:

```
|- 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
```