Prime Decomposition of Ideals in Polynomial Rings

Steve Melczer srm9@sfu.ca
Michael Monagan mmonagan@cecm.sfu.ca
Roman Pearce rpearcea@cecm.sfu.ca

NSERC CRSNG

Introduction

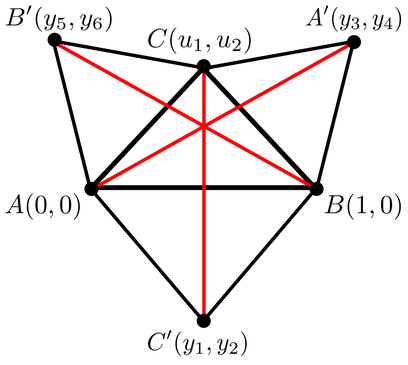
Given a natural number n, one of the most fundamental problems in algebra is representing n as a product of primes. Likewise, given an ideal I in a polynomial ring $k[x_1, \ldots, x_n]$, one of the most fundamental operations that can be performed on I is to represent the radical of I as the intersection of prime ideals,

$$\sqrt{I} = P_1 \cap P_2 \cap \cdots \cap P_r$$

This decomposition, which corresponds to writing the set of solutions of I as a union of irreducible solution sets, has applications solving polynomial systems and in Automatic Theorem Proving.

Example from Theorem Proving

Steiner's Triangle Theorem Let ABC', BCA', and CAB' be three equilateral triangles drawn all outward or all inward on the three sides of an arbitrary triangle ABC. Then the three lines AA', BB', and CC' are concurrent.



Example 1. The following six polynomials represent the hypotheses of Steiner's Triangle Theorem:

$$\begin{aligned}
h_1 &= 2y_1 - 1 = 0 && (AC' = BC') \\
h_2 &= y_1^2 + y_2^2 - 1 = 0 && (AC' = AB) \\
h_3 &= y_3^2 + y_4^2 - u_1^2 - u_2^2 = 0 && (AB' = AC) \\
h_4 &= y_3^2 + y_4^2 - (y_3 - u_1)^2 - (y_4 - u_2)^2 = 0 && (AB' = CB') \\
h_5 &= (y_5 - 1)^2 + y_6^2 - (u_1 - 1)^2 - u_2^2 = 0 && (BA' = BC) \\
h_6 &= (y_5 - 1)^2 + y_6^2 - (y_5 - u_1)^2 - (y_6 - u_2)^2 = 0 && (BA' = CA)
\end{aligned}$$

To prove Steiner's Triangle Theorem automatically, the ideal $<h1, h2, h3, h4, h5, h6>$ must be decomposed as the intersection of prime ideals. The algorithms for prime decomposition built into Maple 14 and Magma V2.16 – 10 failed to return after running for an hour on a machine with a 3GHz Intel Xeon processor and 20GB of memory.

Our Approach

There are well known algorithms for prime decomposition which are efficient for zero dimensional ideals (see chapter 8 of Becker [1]). Unfortunately, in the standard algorithms a positive dimensional ideal must be written in terms of zero dimensional ideals in parametrized polynomial rings, which is slow. Because of this, we decided to augment the standard algorithm for prime decomposition of positive dimensional ideals by splitting one large decomposition into several small ones.

Lemma (Splitting Lemma). Suppose that $I \subset k[x_1, \ldots, x_n]$ and there exist $f, g \in k[x_1, \ldots, x_n]$ such that $f \cdot g \in I$. Then

$$\sqrt{I} = \sqrt{<I, f>} \cap \sqrt{<I, g>}.$$

In addition to using this lemma, we also added several heuristic tests to identify prime ideals and speed up zero dimensional decomposition.

Example 2. Consider the positive dimensional ideal

$$I = <(x-2)(x^2+y^2-1), (y-3)(x^2+y^2-1)>$$

Applying the splitting lemma on the first generator gives

$$\sqrt{I} = \sqrt{<x-2, (y-3)(y^2+3)>} \cap \sqrt{<x^2+y^2-1>}$$

The first ideal in the above decomposition is zero dimensional and the second is clearly prime because it is a principal ideal with an irreducible generator. Furthermore, applying the splitting lemma again gives the prime decomposition

$$\sqrt{I} = <x-2, y^2+3> \cap <x-2, y-3> \cap <x^2+y^2-1>$$

Unfortunately, we may not always be able to split until we obtain prime (or even zero dimensional) ideals. In the worst case, we have to use a standard algorithm for prime decomposition on some of the split components.

Results

We implemented this improved algorithm in Maple 14, using Maple's PolynomialIdeals package to finish the prime decomposition if the splitting and heuristic tests failed. The improved algorithm was run on a set of 36 test ideals compiled from a variety of sources, most notably the POSSO test suite. Of these 36 ideals, Maple's built in algorithm could only decompose 12. In contrast, our improved algorithm decomposed 26 of the ideals with many of the decompositions occurring in seconds. It is notable that our improved algorithm split the 26 ideals into 397 components, only 21 of which did not pass the heuristic tests.

Timings

Below is a selection of the results comparing our improved algorithm to the algorithm built into Maple 14. These results were taken from a machine with a 3GHz Intel Xeon processor and 20GB of memory, and a dash means that the algorithm failed to terminate after 350 seconds. Any ideal whose name begins with a capital letter comes from the automatic proof of a geometric theorem.

Ideal	Variables	Components after Split	Maple Time	Improved Time
butcher	7	10	–	0.404
butcher8	8	8	–	0.452
circles	5	2	6.206	2.501
cyclic4	4	2	0.135	0.022
discriminant4	4	3	0.202	0.872
gerdt85	7	34	–	2.836
gonnet83	17	18	–	0.523
hairer1	8	1	0.966	0.339
Incenter Thm	6	34	–	2.130
krider	10	8	–	6.968
Orthocenter Thm	8	23	–	4.025
Parallelogram Thm	7	5	–	0.067
pavelle	8	1	0.548	0.026
Steiner Triangle	**8**	**11**	**–**	**3.532**
Steiner-Lehmus	6	12	–	50.696
symmetric5	5	42	52.368	119.404
vermeer	5	2	6.270	0.645
wang89	4	2	0.094	0.108
wang92a	7	1	–	0.074
wang92c	4	6	41.103	0.752
wang92f	17	44	–	5.341

Table 1: Timings in CPU seconds

References

[1] T. Becker and V. Weispfenning. *Gröbner Bases: A Computational Approach to Commutative Algebra.* New York: Springer-Verlag, 1993.

[2] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms.* Springer New York, 1992.