A Survey of Algorithms

Alternatives to Buchberger's Algorithm

Nitesh Mathur
Ryan Kinser

February 12, 2021

Table of Contents

Significance of Grobner Bases

1. Hilbert's 10th Problem
2. Find an algorithm to determine whether a given polynomial Diophantine equation with integer coefficients has an integer solution
3. (1970) Deemed **Impossible** by Matiyasevich's Theorem (MRDP Theorem)
4. Grobner Bases: Solve Problems that are considered computationally hard

Table of Contents

Introduction

1. The **input** is a finite set of polynomials, and **output** is a finite Grobner basis.
2. Buchberger's Algorithm requires the use of **S-polynomial** and **Division Algorithm**
3. Recall
$$S(f_1, f_2) = \frac{M}{\text{LT}(f_1)} f_1 - \frac{M}{\text{LT}(f_2)} f_2$$
where $M = \text{LCM}\ ((\text{LT}(f_1), \text{LT}(f_2))$.

Problems With Buchberger's Algorithm

1. Simplicity, Efficiency, Memory Usage
2. Many "useless" $S-$polynomial computation (several divisions that reduce to 0)
3. Buchberger's product and chain criterion to reduce complexity (1979, 1985)

Table of Contents

Intro
Buchberger's Algorithm
Newer Algorithms
Demonstrations
Conclusion

Important Features of Other Algorithms

1. **Product Criterion**: If LCM $(\text{LT}(f), \text{LT}(g)) = \text{LT}(f)\text{LT}(g)$, then the pair (f, g) can be removed.
2. **Chain Criterion**: A pair (f, g) can be removed if there is some h such that $\text{LT}(h)|$ LCM(LT (f), LT(g)), and both pairs (f, h) and (h, g) have been removed before.
3. For a fixed polynomial $r-$tuples $\mathbf{f} = (f_1, .., f_r) \in P^r, (g_1, .., g_r) \in P^r$ is called a **syzygy** wrt **f** if $\sum g_i f_i = 0$.
4. Sparse matrices, "signature," and rewriting

Nitesh Mathur Ryan Kinser A Survey of Algorithms

Historical Progress

1. Moller, Mora, Traverso present an algorithm that uses full module of syzygies, but inefficient (1992)
2. Grobner Walk: Conversion between Grobner basis for different monomial orders
3. Faugere's F4 and F5 Algorithm
4. F4: Normal forms computed and makes use of sparse matrices (1999). Easy to understand, efficient, but memory usage grows quickly
5. F5 algorithm **detects all** useless S-polynomial reductions (2002) via signatures and rewriting rules. Efficient but difficult to understand
6. Last 15 years, G2V, GVW, and other variants

Table of Contents

Computer Programs

1. FGb, Maple
2. CoCoA, Macaulay2, Magma, Singular, Sage
3. Mathematica: Buchberger and Groebner walk
4. Maple: fgb, maplef4 (F4 algorithm), buchberger, fglm (Faugere, Gianni, Lazard, Mora), Groebner walk

Maple Demonstration

1.

Groebner base from tdeg order to plex order

Asked 2 years, 6 months ago Active 1 year, 4 months ago Viewed 90 times

2

I try to solve an equation by using Groebner bases. When I use Maple to find its Groebner basis with plex order, Maple take too long to calculate and the proceed does not terminate. Thus, I try to find with tdeg order and the proceed takes seconds.

Now, I have the Groebner basis with *tdeg order*. I want to use it to find the Groebner basis with *plex order*. Can I do it in Maple?

2

maple groebner-basis

Mathematica Demonstration

1. Consider $\{xy^4 + yz^4 - 2x^2y - 3, y^4 + xy^2z + x^2 - 2xy + y^2 + z^2, -x^3y^2 + xyz^3 + y^4 + xy^2z - 2xy\}$.
2.
```
GroebnerBasis[polys, {x, y, z}, Method → "GroebnerWalk"]; // Timing
{0.1875, Null}
```
3.
```
TimeConstrained[GroebnerBasis[polys, {x, y, z}, Method → "Buchberger"];, 60]
$Aborted
```


Maple Results

1. $\{x^2 - 2xz + 5, xy^2 + yz^3, 3y^2 - 8z^3\}$
2.
```
> Basis(F, lexdeg([x], [y,z]), method=walk);
-> Groebner Walk
 total time:         0.003 sec
```
$$\left[8z^3 - 3y^2, 9y^4 + 48y^3z + 320y^2, 8xy^2 + 3y^3, x^2 - 2xz + 5\right]$$
3.
```
> Basis(F, grlex(x,y,z));
-> F4 algorithm
 total time:         0.005 sec
```
$$\left[x^2 - 2xz + 5, 8z^3 - 3y^2, 8xy^2 + 3y^3, 9y^4 + 48y^3z + 320y^2\right]$$
```
total time:         0.013 sec
```
$$\left[x^2 - 2xz + 5, 8z^3 - 3y^2, 8xy^2 + 3y^3, 9y^4 + 48y^3z + 320y^2\right]$$
4.

Table of Contents

Applications

1. Faugere's F5 solved the first Hidden Field Equation (HFE) Cryptosystem Challenge (80 polynomial equations with 80 unknowns)
2. Cyclic 10 Problem solved by F5
3. Cryptography, robotics, celestial mechanics, signal theory, error correcting codes
4. Other related algorithms: Knuth-Bendix Completion, Robinson's resolution in automated theorem proving

The End

- Thank You!
- Questions?