A Survey of Algorithms Alternatives to Buchberger's Algorithm

Nitesh Mathur Ryan Kinser

February 12, 2021

Nitesh Mathur Ryan Kinser A Survey of Algorithms

Intro Buchberger's Algorithm Newer Algorithms Demonstrations Conclusion

Table of Contents

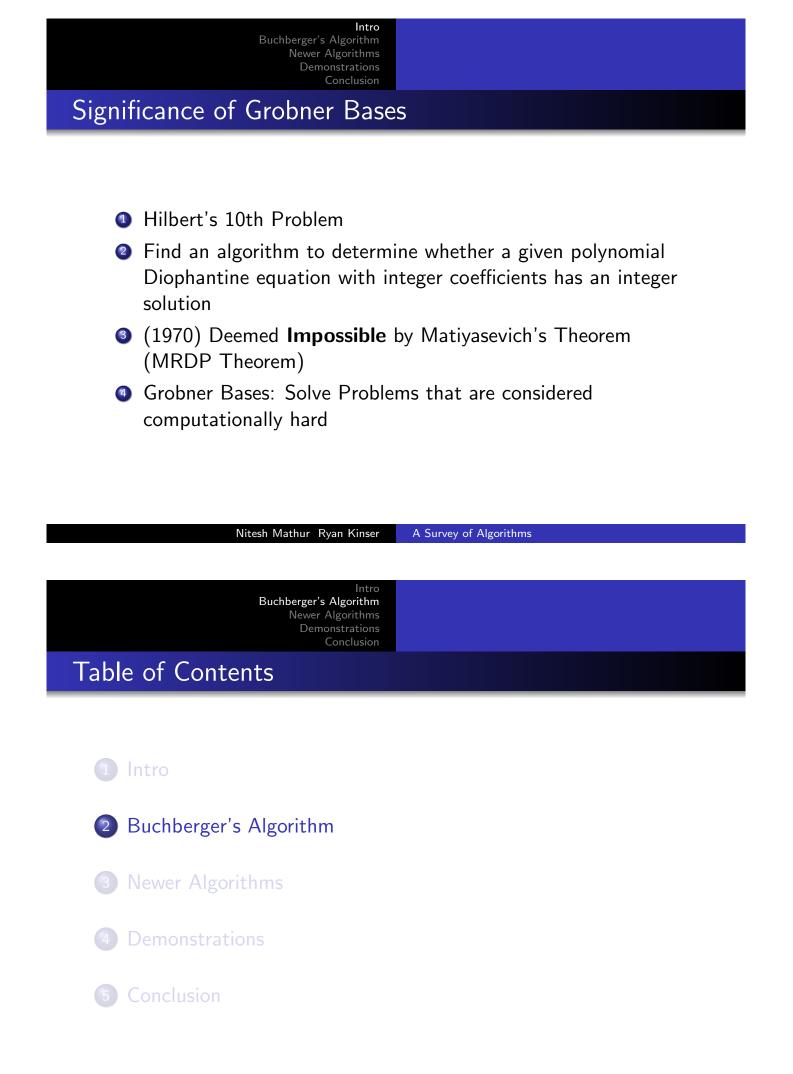


2 Buchberger's Algorithm

3 Newer Algorithms

4 Demonstrations

5 Conclusion





- The input is a finite set of polynomials, and output is a finite Grobner basis.
- Buchberger's Algorithm requires the use of S-polynomial and Division Algorithm
- 8 Recall

$$S(f_1, f_2) = \frac{M}{\mathsf{LT}(f_1)} f_1 - \frac{M}{\mathsf{LT}(f_2)} f_2$$

where $M = \text{LCM} ((\text{LT}(f_1), \text{LT}(f_2))).$

Nitesh Mathur Ryan Kinser A Survey of Algorithms

Intro Buchberger's Algorithm Newer Algorithms Demonstrations Conclusion

Problems With Buchberger's Algorithm

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

Buchberger's Algorithm Newer Algorithms Demonstrations Conclusion

Table of Contents



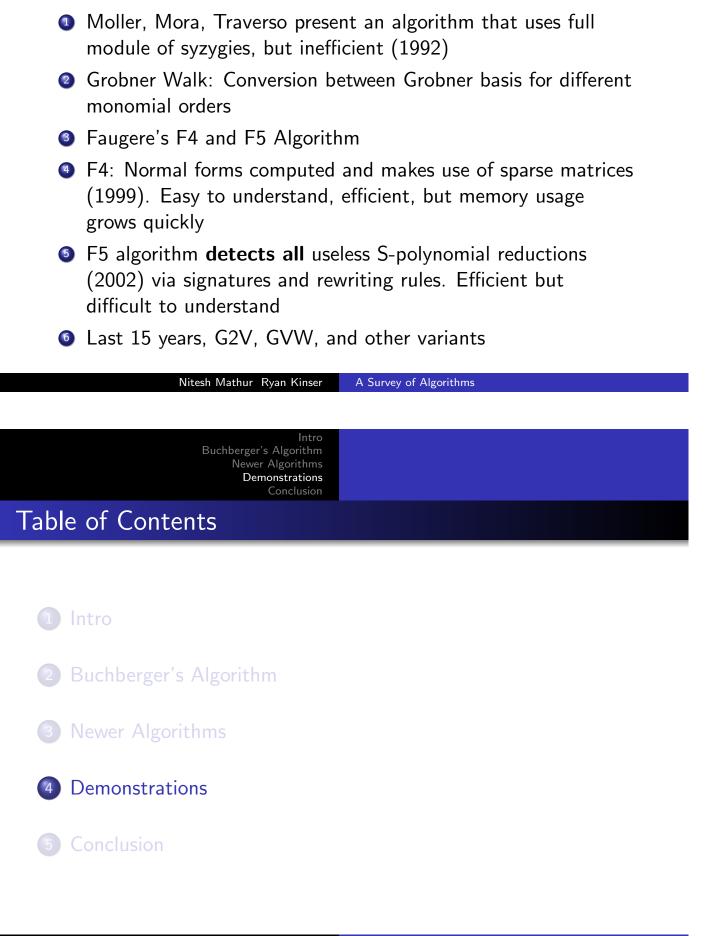


- Product Criterion: If LCM (LT(f), LT(g)) = LT(f)LT(g), then the pair (f,g) can be removed.
- Chain Criterion: A pair (f,g) can be removed if there is some h such that LT(h) LCM(LT (f), LT(g), and both pairs (f, h) and (h,g) have been removed before.
- So For a fixed polynomial r-tuples $\mathbf{f}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

Buchberger's Algorithm Newer Algorithms Demonstrations

Conclusion

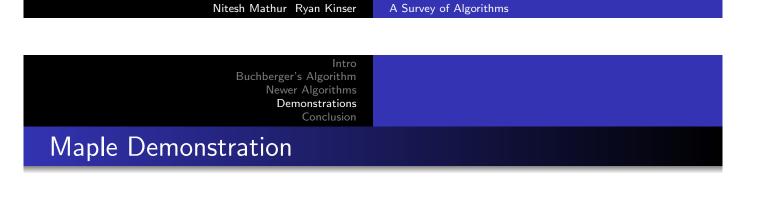
Historical Progress

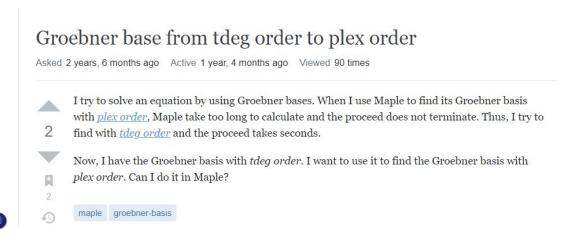


Buchberger's Algorithm Newer Algorithms Demonstrations Conclusion

Computer Programs

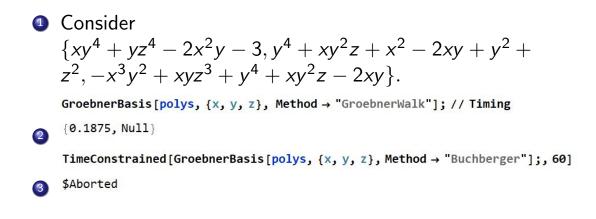
- FGb, Maple
- CoCoA, Macaulay2, Magma, Singular, Sage
- Mathematica: Buchberger and Groebner walk
- Maple: fgb, maplef4 (F4 algorithm), buchberger, fglm (Faugere, Gianni, Lazard, Mora), Groebner walk





Buchberger's Algorithm Newer Algorithms Demonstrations Conclusion

Mathematica Demonstration

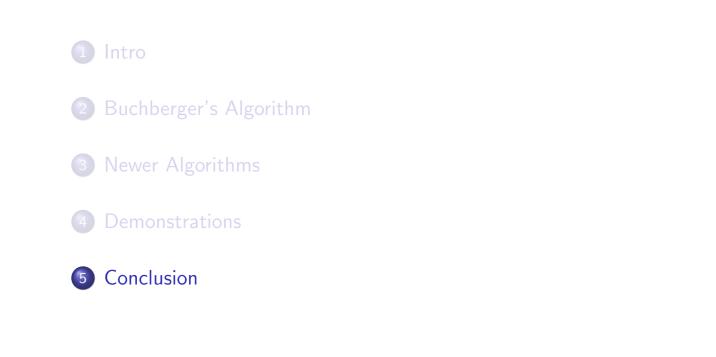


Nitesh Mathur Ryan Kinser

A Survey of Algorithms

Intro Buchberger's Algorithm Newer Algorithms Demonstrations Conclusion Maple Results $\{x^2 - 2xz + 5, xy^2 + yz^3, 3y^2 - 8z^3\}$ > Basis(F, lexdeg([x], [y,z]), method=walk); -> Groebner Walk 0.003 sec total time: $\left[8z^3-3y^2,
ight.$ $9y^4 + 48y^3z + 320y^2, 8xy^2 + 3y^3, x^2 - 2xz + 5$ 2 > Basis(F, grlex(x,y,z)); -> F4 algorithm total time: 0.005 sec $|x^2|$ $-2xz+5,\,8z^3-3y^2,\,8xy^2+3y^3,\,9y^4+48y^3z+320y^2\Big]$ 3 0.013 sec total time: x^2 $-2xz+5, 8z^3-3y^2, 8xy^2+3y^3, 9y^4+48y^3z+320y^2$ 4

Table of Contents



Intro Buchberger's Algorithm Newer Algorithms Demonstrations Conclusion

A Survey of Algorithms

- 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

Nitesh Mathur Ryan Kinser

- Cryptography, robotics, celestial mechanics, signal theory, error correcting codes
- Other related algorithms: Knuth-Bendix Completion, Robinson's resolution in automated theorem proving

Intro Buchberger's Algorithm Newer Algorithms Demonstrations **Conclusion**

The End

- Thank You!
- Questions?

Nitesh Mathur Ryan Kinser A Sur

A Survey of Algorithms