Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

Languages
Add links

Faugère's F4 and F5 algorithms

From Wikipedia, the free encyclopedia
(Redirected from Faugère F4 algorithm)

In computer algebra, the **Faugère F4 algorithm**, by Jean-Charles Faugère, computes the Gröbner basis of an ideal of a multivariate polynomial ring. The algorithm uses the same mathematical principles as the Buchberger algorithm, but computes many normal forms in one go by forming a generally sparse matrix and using fast linear algebra to do the reductions in parallel.

The **Faugère F5 algorithm** first calculates the Gröbner basis of a pair of generator polynomials of the ideal. Then it uses this basis to reduce the size of the initial matrices of generators for the next larger basis:

> If G_{prev} is an already computed Gröbner basis $(f_2, \ldots, f_m)$ and we want to compute a Gröbner basis of $(f_1) + G_{\text{prev}}$ then we will construct matrices whose rows are $m\,f_1$ such that m is a monomial not divisible by the leading term of an element of G_{prev}.

This strategy allows the algorithm to apply two new criteria based on what Faugère calls *signatures* of polynomials. Thanks to these criteria, the algorithm can compute Gröbner bases for a large class of interesting polynomial systems, called *regular sequences*, without ever simplifying a single polynomial to zero—the most time-consuming operation in algorithms that compute Gröbner bases. It is also very effective for a large number of non-regular sequences.

Implementations [edit]

The Faugère F4 algorithm is implemented

- as a package FGb for the Maple computer algebra system. This package is included in Maple distribution as the option **method=fgb** of function **Groebner[gbasis]**;
- in the Magma computer algebra system.
- as a C library.

Study versions of the Faugère F5 algorithm is implemented in[*citation needed*]

- the SINGULAR computer algebra system;[1]
- the Sage computer algebra system.

Applications [edit]

The previously intractable "cyclic 10" problem was solved by F5, as were a number of systems related to cryptography; for example HFE and C*.

References [edit]

1. ^ Eder, Christian (2008). "On The Criteria Of The F5 Algorithm". arXiv:0804.2033 [math.AC].

- Faugère, J.-C. (June 1999). "A new efficient algorithm for computing Gröbner bases (F_4)" (PDF). *Journal of Pure and Applied Algebra* (Elsevier Science) **139** (1): 61–88. doi:10.1016/S0022-4049(99)00005-5. ISSN 0022-4049.
- Faugère, J.-C. (July 2002). "A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5)" (PDF). *Proceedings of the 2002 international symposium on Symbolic and algebraic computation (ISSAC)* (ACM Press): 75–83. doi:10.1145/780506.780516. ISBN 1-58113-484-3.
- Till Stegers Faugere's F5 Algorithm Revisited (alternative link). Diplom-Mathematiker Thesis, advisor Johannes Buchmann, Technische Universität Darmstadt, September 2005 (revised April 27, 2007). Many

references, including links to available implementations.

External links [edit]

- Faugère's home page (includes pdf reprints of additional papers)
- An introduction to the F4 algorithm.

This algorithms or data structures-related article is a stub. You can help Wikipedia by expanding it.

Categories: Computer algebra | Algorithms and data structures stubs | Computer science stubs