Using Fermat to Solve Large Polynomial and Matrix Problems

Robert H. Lewis

Department of Mathematics
Fordham University, New York City
rlewis@fordham.edu

Software name: Fermat

Short description: *Fermat* is a computer algebra system in which the basic items being computed can be rational numbers, modular numbers, finite fields, multivariable polynomials, rational functions, or polynomials modulo other polynomials. The "ground ring" F may be $\boldsymbol{Q}$, the rational numbers, or $\boldsymbol{Z}/m$. On top of this may be attached any number of symbolic variables $t_1, t_2, \ldots, t_n$, thereby creating the polynomial ring $F[t_1, t_2, \ldots, t_n]$ and its quotient field, the field of rational functions. Further, polynomials $p, q, \ldots$ can be chosen to mod out with, creating the quotient ring $F(t_1, t_2, \ldots) \; / < p, q, \ldots >$.

Fermat has extensive built-in primitives for array and matrix manipulations, such as submatrix, sparse matrix, determinant, minors, normalize, column reduce, reduced row echelon, matrix inverse, Smith normal form, etc. It is consistently faster than some well known computer algebra systems. *Fermat* has a complete programming language and file system.

I will demonstrate the Dixon Resultant technique for systems of polynomial equations, in particular how I attack the *spurious factor problem.*

Public access: http://www.bway.net/~lewis

Abstract

Fermat is an interactive system for mathematical experimentation. It is a super calculator – computer algebra system, in which the basic items being computed can be rational numbers, modular numbers, finite fields, multivariable polynomials, rational functions, or polynomials modulo other polynomials.

In *Fermat* the default "ground ring" F is the field of rational numbers. One may choose to work modulo a specified integer m, thereby changing the ground ring F from $\boldsymbol{Q}$ to $\boldsymbol{Z}/m$. On top of this may be attached any number of symbolic variables $t_1, t_2, \ldots, t_n$, thereby creating the polynomial ring $F[t_1, t_2, \ldots, t_n]$ and its quotient field, the field of rational functions, whose elements are called *quolynomials*. Further, polynomials $p, q, \ldots$ can be chosen to mod out with, creating the quotient ring $F(t_1, t_2, \ldots)\ /\ < p, q, \ldots >$, whose elements are called *polymods*. If this is done correctly, finite fields result. Finally, it is possible to allow *Laurent polynomials*, those with negative as well as positive exponents. Once the computational ring is established in this way, all computations are of elements of this ring.

Fermat has extensive built-in primitives for array and matrix manipulations, such as submatrix, sparse matrix, determinant, minors, normalize, column reduce, reduced row echelon, matrix inverse, Smith normal form, and characteristic polynomial. It is consistently faster than some well known computer algebra systems – orders of magnitude faster in some cases.

Fermat is a complete programming language. Programs and data can be saved to an ordinary text file that can be read during a later session or read by some other software system.

Fermat has solved real problems that other computer algebra systems could not. It is more efficient in both time and space. These problems have come from algebraic topology, group theory, image processing, computational geometry, decision theory, and signal processing.

Most recent applications involve solving systems of polynomial equations with the **Dixon Resultant** technique. I will demonstrate this method at the conference, in particular how I attack the *spurious factor problem.*

Fermat is available for Windows95/98/NT/etc and Mac OS. Fermat for Linux is ready for beta testing.

Lewis, Robert H. and Stephen Bridgett, "Conic Tangency Equations and Apollonius Problems in Biochemistry and Pharmacology," Mathematics and Computers in Simulation **61(2)** (2003) p. 101-114.

Lewis, Robert H. and Peter F. Stiller, "Solving the recognition problem for six lines using the Dixon resultant," Mathematics and Computers in Simulation **49** (1999) p. 205-219.

Lewis, Robert H. and Michael Wester, "Comparison of Polynomial-Oriented Computer Algebra Systems," SIGSAM Bulletin **33(4)**, (1999) p. 5-13.