Galois Field Library for HP-50g/49g+/49g

(c) 2008 by Takashi Matsubara

1 Introduction

The Galois Field library is a collection of basic calculations of Galois field $GF(q)$ with $q = p^n$ where p is a prime number and n is a positive integer, that is, a finite field $\mathbb{F}_q = \mathbb{F}_{p^n}$. This library includes commands of multiplication and division on $GF(q)$, factorization of a polynomial over $GF(q)$, kernel of a matrix over $GF(q)$, the minimal polynomial of an element of $GF(q)$ over $GF(p)$, and more. The latest versions of the libraries FACTMOD and KERMOD are contained. The library ID is 767.

2 Files

`gfwhelp.hp`	The Galois field library file for the 49G (ROM 1.24, ROM 2.10-7), 49G+ (ROM 1.23, ROM 2.09) and 50g (ROM 2.09) with help for CAT.
`gfwohelp.hp`	The Galois field library file for the 49G (ROM 1.24, ROM 2.10-7), 49G+ (ROM 1.23, ROM 2.09) and 50g (ROM 2.09) without help.
`gfwhelp196.hp`	The Galois field library file for the 49G (ROM 1.19-6) with help for CAT.
`gfwohelp196.hp`	The Galois field library file for the 49G (ROM 1.19-6) without help.
`^GbENTER.hp`	The file βENTER for automatic simplification.
`^GbENTER.txt`	The source file of `^GbENTER.hp`.
`readme.pdf`	This file

3 Version

Ver1.00 :	2005.8.16	First release
Ver1.01 :	2005.9.5	Files for ROM 1.19-6 and ROM 1.18 are added.
Ver1.02 :	2005.11.17	Commands GFADD, GFSUB, GFMUL, GFPOW are added. The file βENTER for automatic simplification is added. GFSIMP now can be applied for quotient of polynomials over Galois field.
Ver1.03 :	2006.12.8	Some commands (help for CAT and SETGF) are compressed by debug4x (ver2.2 build104) and size of file is reduced.
Ver1.04 :	2007.8.7	A bug on FACTGF is fixed. Commands MINPOLY2, GFINVM, ISPPOLY?, NPPOLY, ISPEGF?, NPEGF etc. are added.
Ver1.05 :	2007.8.19	A bug on MINPOLY2 is fixed. Some commands can be used in an algebraic object like as 'MINPOLY2($\alpha+1, \alpha^2+\alpha$)'.
Ver1.06 :	2007.8.27	Commands GFLOG, GFLOG2 and GFA are added. The outputs of P→L and P→LL are changed. MINPOLY2 is slightly faster than previous versions.
Ver1.06a :	2008.5.01	A few typos in the help file for CAT are fixed.
Ver1.07 :	2008.5.23	Size of file is reduced.
Ver1.10 :	2008.12.25	A bug on FACTGF is fixed.

4 Installation

Before installation, delete the libraries FACTMOD and KERMOD if you use. Then, you can choose `gfwhelp.hp` or `gfwohelp.hp` to install. `gfwhelp.hp` includes help which can be shown in command catalog CAT. `gfwohelp.hp` does not include help. This is smaller than `gfwhelp.hp`. If ROM version is 1.19-6 or 1.18, choose `gfwhelp196.hp` (with help) or `gfwohelp196.hp` (without help).

Send one of the above file to the calculator from PC, and move the file to PORT1 or PORT2 by using filer of the calculator (PORT2 is recommended). After that, reboot the calculator by ON+C.

To use the library, set flag -105 (System flag 105 : exact mode on).

`^GbENTER.hp` is the program for automatic simplification by using trace mode of the 49G. If `^GbENTER.hp` is transfered to HP49G/G+ in some directory, βENTER appears in the directory. To turn on trace mode, set flag -62 and -63 (System flag 62 and 63). When the command `+`, `-`, `*`, `/`, `^` or `INV` is executed in the directory, the result is simplified automatically by the command GFSIMP of the library.

5 Usage

1. Press APPS and select "Galois Field".
2. Press SETGF in the menu. In this menu, define a polynomial ring $GF(q)[X]$ over $GF(q)$, where $GF(q) = \mathbb{Z}_p[\alpha]/(f(\alpha))$, $\mathbb{Z}_p = GF(p) = \{0, 1, \ldots, p-1\}$ with a prime number p.

   First, push CLEAR (right-shift + back-space), then following sample parameters are shown.

Indep.var :	'X'
Modulo p :	2
Irr poly f :	'α^3+α+1'
var. of poly :	'α'

This means $GF(q) = GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1) =$ { polynomials with degree less than 3 }. Multiplication is executed by taking modulo $\alpha^3 + \alpha + 1$. An element of $GF(q)$ is represented by a polynomial with variable α which is defined by "var. of poly".

Polynomial f with variable α must be irreducible over $\mathbb{Z}_p = \{0, 1, ..., p-1\}$, where p is the current modulus which can be defined in the above menu. If f is not irreducible, a warning message is shown in the end of execution of SETGF. In this case, execute SETGF again to set correctly irreducible polynomial f. You can find a irreducible polynomial f by using NPPOLY after setting the current modulus p by SETGF, MODSTO or the CAS menu, since a primitive polynomial is irreducible. (eg. NPPOLY(X^3) returns a primitive polynomial with degree 3.)

The current variable "Indep.var" and the current modulus are the same in the CAS menu and stored in CASDIR. The irreducible polynomial f and variable of f are stored in the global name GFPAR.

3. After setting parameters correctly by SETGF, following commands can be used. Some commands work over $GF(p)$ or $GF(p)[X]$, and some commands work over $GF(q)$ or $GF(q)[X]$.

If you find any problems, please let me know in comp.sys.hp48 or by E-mail (qqvv6t89@io.ocn.ne.jp).

6 Commands

SETGF

Set the parameters for the library. Edit GFPAR. GFPAR is a list of a variable and a irreducible polynomial for this library. e.g. GFPAR={ α 'α^3+$\alpha+1$' }

Input	Level 1/Argument 1	none
Output	Level 1/Argument 1	none

DISPGF

Display the status of $GF(q) = \mathbb{Z}_p[\alpha]/(f(\alpha))$ defined by SETGF in the status area.

Input	Level 1/Argument 1	none
Output	Level 1/Argument 1	none

EGCDMOD

Extended GCD of two polynomials over $GF(p)$. (p : the current modulus)

Input	Level 2/Argument 1	a : a polynomial over $GF(p)$
	Level 1/Argument 2	b : a polynomial over $GF(p)$
Output	Level 1/Argument 1	$\{d, u, v\}$ $(d, u, v \in GF(p)[X].\ d = \gcd(a, b),\ d = au + bv\ )$

MODC

Modulo matrix, vector or polynomial with the current modulus.

Input	Level 1/Argument 1	a : a matrix, a vector or a polynomial in $GF(p)[X]$
Output	Level 1/Argument 1	$a \mod p$: same type object as input

GF

The list of all elements of $GF(p^n)$ represented by lists.

Input	Level 2/Argument 1	p : a positive integer
	Level 1/Argument 2	n : a positive integer
Output	Level 1/Argument 1	a list of lists

e.g.

Input	Level 2/Argument 1	2
	Level 1/Argument 2	3
Output	Level 1/Argument 1	$\{\{0,0,0\},\{0,0,1\},\ldots,\{1,1,1\}\}$

GFV

The list of all elements of $GF(p^n)$ represented by vectors.

Input	Level 2/Argument 1	p : a positive integer
	Level 1/Argument 2	n : a positive integer
Output	Level 1/Argument 1	a list of vectors

e.g.

Input	Level 2/Argument 1	2
	Level 1/Argument 2	3
Output	Level 1/Argument 1	$\{[0,0,0],[0,0,1],\ldots,[1,1,1]\}$

GFP

The list of all elements of $GF(p^n)$ represented by polynomials with the current variable defined.

Input	Level 2/Argument 1	p : a positive integer
	Level 1/Argument 2	n : a positive integer
Output	Level 1/Argument 1	a list of polynomials

e.g.

Input	Level 2/Argument 1	2
	Level 1/Argument 2	3
Output	Level 1/Argument 1	$\{0,1,X,\ldots,X^2+X+1\}$

GFM

The list of all elements of $GF(p^n)$ represented by matrices.

Input	Level 2/Argument 1	p : a positive integer
	Level 1/Argument 2	n : a positive integer
Output	Level 1/Argument 1	a list of matrices

e.g.

Input	Level 2/Argument 1	2
	Level 1/Argument 2	3
Output	Level 1/Argument 1	$\{[[0,0,0]],[[0,0,1]],\ldots,[[1,1,1]]\}$

L→P

Convert a list of coefficients to a polynomial the current independent variable.

Input	Level 1/Argument 1	a list of coefficients
Output	Level 1/Argument 1	a polynomial of the current independent variable

e.g.

Input	Level 1/Argument 1	$\{1,A,B+1,3\}$
Output	Level 1/Argument 1	$X^3+AX^2+(B+1)X+3$

P→L

Convert a polynomial of the current independent variable to a list of coefficients.

Input	Level 1/Argument 1	a polynomial of the current independent variable
Output	Level 1/Argument 1	a list of coefficients

e.g.

Input	Level 1/Argument 1	$X^3 + AX^2 + (B+1)X + 3$
Output	Level 1/Argument 1	$\{1, A, B+1, 3\}$

FACTMOD

Factorizes a polynomial modulo the current modulus. The built-in command FACTORMOD cannot be executed for a polynomial with degree that can be divided by the current modulus. FACTMOD can be executed for such polynomials. First, this program makes the input polynomial square-free, after that, built-in SystemRPL command "BerlekampP" is applied. Prime factors are chosen as monic.

Input	Level 1/Argument 1	g : a polynomial over $GF(p)$
Output	Level 1/Argument 1	$ag_1^{e_1} \cdots g_n^{e_n}$: a polynomial over $GF(p)$ ($a \in GF(p)$, $g_i \in GF(p)[X]$: irreducible and monic polynomial, $e_i \in \mathbb{Z}$)

Input	Level 1/Argument 1	$\{g, h, \dots\}$: a list of polynomials over $GF(p)$
Output	Level 1/Argument 1	$\{ag_1^{e_1} \cdots g_n^{e_n}, bh_1^{l_1} \dots h_m^{l_m}, \cdots\}$: a list of polynomials over $GF(p)$

e.g. (current modulus=13)

Input	Level 1/Argument 1	$X^{13} - 1$
Output	Level 1/Argument 1	$(X-1)^{13}$

Input	Level 1/Argument 1	$\{X^{13} - 1, X^3 + 1\}$
Output	Level 1/Argument 1	$\{(X-1)^{13}, (X+1)(X+3)(X-4)\}$

FACTSMOD

Factorizes a polynomial modulo the current modulus.

Input	Level 1/Argument 1	g : a polynomial over $GF(p)$
Output	Level 1/Argument 1	$\{a, \{g_1, e_1\}, \{g_2, e_2\}, \dots, \{g_n, e_n\}\}$ ($a \in GF(p)$, $g_i \in GF(p)[X]$: irreducible monic polynomial, $e_i \in \mathbb{Z}$ such that $g = ag_1^{e_1} g_2^{e_2} \dots g_n^{e_n}$)

Input	Level 1/Argument 1	a list of polynomials over $GF(p)$
Output	Level 1/Argument 1	a list of lists

e.g. (current modulus=2)

Input	Level 1/Argument 1	$X^6 + X^4 + X + 1$
Output	Level 1/Argument 1	$\{1, \{X+1, 1\}, \{X^2+X+1, 1\}, \{X^3+X+1, 1\}\}$

Input	Level 1/Argument 1	$\{X^2 + 1, X^3 + 1\}$
Output	Level 1/Argument 1	$\{\{1, \{X+1, 2\}\}, \{1, \{X+1, 1\}, \{X^2+X+1, 1\}\}\}$

KERMOD

Kernel of a matrix with the current modulus.

Input	Level 1/Argument 1	a matrix over $GF(p)$
Output	Level 1/Argument 1	a list of vectors over $GF(p)$: the basis of the kernel of input matrix.

e.g. (current modulus=5)

Input	Level 1/Argument 1	$[[1, 2, 3], [1, 2, 3], [0, 0, 0]]$
Output	Level 1/Argument 1	$\{[3, 1, 0], [2, 0, 1]\}$

IMAGEMOD

Image of a matrix with the current modulus.

Input	Level 1/Argument 1	a matrix over $GF(p)$
Output	Level 1/Argument 1	a list of vectors over $GF(p)$: the basis of the image of input matrix.

e.g. (current modulus=5)

Input	Level 1/Argument 1	$[[1, 2, 3], [2, 4, 1]]$
Output	Level 1/Argument 1	$\{[1, 2]\}$

BASISMOD

Basis of a vector space with the current modulus.

Input	Level 1/Argument 1	a list of vectors over $GF(p)$
Output	Level 1/Argument 1	a list of vectors over $GF(p)$: the basis of the linear space spanned by vectors of input.

Input	Level 1/Argument 1	a matrix over $GF(p)$
Output	Level 1/Argument 1	a list of vectors over $GF(p)$: the basis of the linear space spanned by row vectors of input matrix.

e.g. (current modulus=5)

Input	Level 1/Argument 1	$\{[1, 2, 3], [2, 3, 4]\}$
Output	Level 1/Argument 1	$\{[0, 1, 2], [1, 0, -1]\}$

Input	Level 1/Argument 1	$[[1,2,3],[2,3,4]]$
Output	Level 1/Argument 1	$\{[0,1,2],[1,0,-1]\}$

IBASISMOD

Basis of the intersection of two vector spaces with the current modulus.

Input	Level 2/Argument 1	a list of vectors over $GF(p)$
	Level 1/Argument 2	a list of vectors over $GF(p)$
Output	Level 1/Argument 1	a list of vectors over $GF(p)$: the basis of the intersection of two linear spaces spanned by input vectors.

e.g. (current modulus=2)

Input	Level 2/Argument 1	$\{[1,0,0],[0,1,0]\}$
	Level 1/Argument 2	$\{[1,1,0],[0,0,1]\}$
Output	Level 1/Argument 1	$\{[1,1,0]\}$

P→LL

Convert a polynomial over $GF(q)$ to a list of lists of coefficients.

Input	Level 1/Argument 1	an element g of $GF(q)[X,A,B,\dots]$ ($GF(q) = GF(p)[\alpha]/(f(\alpha))$, $g = \sum_{i=0}^{n} g_i(\alpha)X^i$, $g_i(\alpha) = \sum_{j=0}^{m_i} g_{ij}\alpha^j$, $g_{ij} \in GF(p)[A,B,\dots]$)
Output	Level 1/Argument 1	a list of lists of coefficients in $GF(p)[A,B,\dots]$. $\{\{g_{n,m_n}, g_{n,m_n-1},\dots,g_{n,0}\},\dots,\{g_{0,m_0}, g_{0,m_0-1},\dots,g_{0,0}\}\}$

e.g.

Input	Level 1/Argument 1	$X^3 + AX^2 + (B\alpha^2 + C\alpha + 1)X + (\alpha^2 + 1)$
Output	Level 1/Argument 1	$\{1,\{A\},\{B,C,1\},\{1,0,1\}\}$

LL→P

Convert a list of lists of coefficients to a polynomial over $GF(q)$.

Input	Level 1/Argument 1	a list of lists of coefficients in $GF(p)[A,B,\dots]$
Output	Level 1/Argument 1	an element g of $GF(q)[X,A,B,\dots]$

e.g.

Input	Level 1/Argument 1	$\{1,\{A\},\{B,C,1\},\{1,0,1\}\}$
Output	Level 1/Argument 1	$X^3 + AX^2 + (B\alpha^2 + C\alpha + 1)X + (\alpha^2 + 1)$

COLCVX

Collect a polynomial with respect to the current variable.

Input	Level 1/Argument 1	an element of $\mathbb{Q}[X, \alpha, Y, Z, A, \dots]$, where $\mathbb{Q}$ is the rational number field.
Output	Level 1/Argument 1	an element of $\mathbb{Q}[X, \alpha, Y, Z, A, \dots]$

e.g.

Input	Level 1/Argument 1	$\alpha^2X^2 + \alpha AX^2 + \alpha X^2 + A + 1$
Output	Level 1/Argument 1	$(\alpha^2 + (A+1)\alpha)X^2 + A + 1$

COLC

Collect a polynomial with respect to variables defined by level 1 input. When level 1 input is $\{X, \alpha\}$, the output is the same as that of COLCVX.

Input	Level 2/Argument 1	an element of $\mathbb{Q}[X, \alpha, Y, Z, A, \dots]$, where $\mathbb{Q}$ is the rational number field.
	Level 1/Argument 2	a list of variables
Output	Level 1/Argument 1	an element of $\mathbb{Q}[X, \alpha, Y, Z, A, \dots]$

e.g.

Input	Level 2/Argument 1	$\alpha^2X^2 + \alpha AX^2 + \alpha X^2 + A + 1$
	Level 1/Argument 2	$\{A, \alpha, X\}$
Output	Level 1/Argument 1	$(X^2\alpha + 1)A + X^2\alpha^2 + X^2\alpha + 1$

GFSIMP

Simplify an elements of $GF(q)[X, Y, Z, \dots]$ by taking $\mod f(\alpha)$, where $GF(q) = GF(p)[\alpha]/(f(\alpha))$.

Input	Level 1/Argument 1	an element of $GF(q)(X, Y, Z, A, \dots)$
Output	Level 1/Argument 1	an element of $GF(q)(X, Y, Z, A, \dots)$

Input	Level 1/Argument 1	a list of elements in $GF(q)(X, Y, Z, A, \dots)$
Output	Level 1/Argument 1	a list of elements in $GF(q)(X, Y, Z, A, \dots)$

Input	Level 1/Argument 1	a vector of elements in $GF(q)(X, Y, Z, A, \dots)$
Output	Level 1/Argument 1	a vector of elements in $GF(q)(X, Y, Z, A, \dots)$

Input	Level 1/Argument 1	a matrix of elements in $GF(q)(X, Y, Z, A, \dots)$
Output	Level 1/Argument 1	a matrix of elements in $GF(q)(X, Y, Z, A, \dots)$

e.g. ($GF(q) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$)

Input	Level 1/Argument 1	$\alpha^5 + 1$
Output	Level 1/Argument 1	$\alpha^2 + \alpha$

Input	Level 1/Argument 1	α^{-2}
Output	Level 1/Argument 1	$\alpha^2 + \alpha + 1$

Input	Level 1/Argument 1	$\alpha^5 X^3 + 1$
Output	Level 1/Argument 1	$(\alpha^2 + \alpha + 1)X^3 + 1$

Input	Level 1/Argument 1	$(\alpha^{-2}X^2 + 1)/(X + \alpha/X)$
Output	Level 1/Argument 1	$(X^3 + \alpha^2 X)/(\alpha^2 X^2 + \alpha + 1)$

Input	Level 1/Argument 1	$[[\alpha^5 X^3 + 1, \alpha^3], [2, \alpha^4 A]]$
Output	Level 1/Argument 1	$[[(\alpha^2 + \alpha + 1)X^3 + 1, \alpha + 1], [0, A\alpha^2 + A\alpha]]$

GFADD

Addition of two elements of $GF(q)[X]$ or matrices over $GF(q)[X]$. This is simply taking '+' after that applying GFSIMP. GFSIMP is not fast, so if there are many addition, subtraction, multiplication, power, then using GFADD, GFSUB, GFMUL, GFPOW is not recommended. Recommended is that using '+', '−', '∗', '^' and applying GFSIMP once.

Input	Level 2/Argument 1	a
	Level 1/Argument 2	b
Output	Level 1/Argument 1	$a + b \mod f(\alpha)$

GFSUB

Subtraction of two elements of $GF(q)[X]$ or matrices over $GF(q)[X]$ This is simply taking '−' after that applying GFSIMP. GFSIMP is not fast, so if there are many addition, subtraction, multiplication, power, then using GFADD, GFSUB, GFMUL, GFPOW is not recommended. Recommended is that using '+', '−', '∗', '^' and applying GFSIMP once.

Input	Level 2/Argument 1	a
	Level 1/Argument 2	b
Output	Level 1/Argument 1	$a - b \mod f(\alpha)$

GFMUL

Multiplication of two elements of $GF(q)[X]$ or matrices over $GF(q)[X]$ This is simply taking '∗' after that applying GFSIMP. GFSIMP is not fast, so if there are many addition, subtraction, multiplication, power, then using GFADD, GFSUB, GFMUL, GFPOW is not recommended. Recommended is that using '+', '−', '∗', '^' and applying GFSIMP once.

Input	Level 2/Argument 1	a
	Level 1/Argument 2	b
Output	Level 1/Argument 1	$ab \mod f(\alpha)$

GFPOW

Power of an element of $GF(q)[X]$ or a matrix over $GF(q)[X]$ by an integer This is simply taking '^' after that applying GFSIMP. GFSIMP is not fast, so if there are many addition, subtraction, multiplication, power, then using GFADD, GFSUB, GFMUL, GFPOW is not recommended. Recommended is that using '+', '−', '∗', '^' and applying GFSIMP once.

Input	Level 2/Argument 1	a
	Level 1/Argument 2	n : an integer (n can be negative)
Output	Level 1/Argument 1	$a^n \mod f(\alpha)$

GFINV

Inverse of an element of $GF(q)$

Input	Level 1/Argument 1	a : an element of $GF(q)$
Output	Level 1/Argument 1	a^{-1} : an element of $GF(q)$

e.g. ($GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$)

Input	Level 1/Argument 1	α
Output	Level 1/Argument 1	$\alpha^2 + 1$

GFDIV

Division of two elements of $GF(q)$

Input	Level 2/Argument 1	a : an element of $GF(q)$
	Level 1/Argument 2	b : an element of $GF(q)$
Output	Level 1/Argument 1	a/b

e.g. ($GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$)

Input	Level 2/Argument 1	α
	Level 1/Argument 2	$\alpha^2 + 1$
Output	Level 1/Argument 1	α^2

GFPDIV

Division of two polynomials in $GF(q)[X]$

Input	Level 2/Argument 1	f_1: a polynomial in $GF(q)[X]$
	Level 1/Argument 2	f_2: a polynomial in $GF(q)[X]$
Output	Level 2/Argument 1	q : quotient
	Level 1/Argument 2	r : remainder ($f_1 = f_2 q + r$, $\deg r < \deg f_2$)

e.g. ($GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$)

Input	Level 2/Argument 1	$\alpha^2 X^3 + 1$
	Level 1/Argument 2	$\alpha X + 1$
Output	Level 2/Argument 1	$\alpha X^2 + X + \alpha^2 + 1$
	Level 1/Argument 2	α^2

GFPEGCD

Extended GCD of two polynomials in $GF(q)[X]$

Input	Level 2/Argument 1	f_1: a polynomial in $GF(q)[X]$
	Level 1/Argument 2	f_2: a polynomial in $GF(q)[X]$
Output	Level 1/Argument 1	$\{d, u, v\}$ $(d, u, v \in GF(q)[X].\ d = \gcd(f_1, f_2), d = f_1u + f_2v)$

GFPGCD

GCD of two polynomials in $GF(q)[X]$

Input	Level 2/Argument 1	f_1: a polynomial in $GF(q)[X]$
	Level 1/Argument 2	f_2: a polynomial in $GF(q)[X]$
Output	Level 1/Argument 1	$\gcd(f_1, f_2)$

FACTGF

Factorizes a polynomial in $GF(q)[X]$ where $GF(q) = \mathbb{Z}_p[x]/(f(x))$ defined by SETGF.

Input	Level 1/Argument 1	g : a polynomial over $GF(q)$
Output	Level 1/Argument 1	$ag_1^{e_1} \cdots g_n^{e_n}$: a polynomial over $GF(q)$ $(a \in GF(q),\ g_i \in GF(q)[X]$: irreducible, $e_i \in \mathbb{Z})$

Input	Level 1/Argument 1	$\{g, h, \dots\}$: a list of polynomials over $GF(q)$
Output	Level 1/Argument 1	$\{ag_1^{e_1} \cdots g_n^{e_n}, bh_1^{l_1} \dots h_m^{l_m}, \cdots\}$: a list of polynomials over $GF(q)$

e.g. ($GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$)

Input	Level 1/Argument 1	$X^3 + X + 1$
Output	Level 1/Argument 1	$(X + \alpha)(X + \alpha^2)(X + \alpha^2 + \alpha)$

Input	Level 1/Argument 1	$\{X^2 + \alpha, X^2 + \alpha^3 X + \alpha\}$
Output	Level 1/Argument 1	$\{(X + \alpha^2 + \alpha)^2, (X + 1)(X + \alpha)\}$

FACTSGF

Factorizes a polynomial in $GF(q)[X]$ where $GF(q) = \mathbb{Z}_p[x]/(f(x))$ defined by SETGF.

Input	Level 1/Argument 1	g : a polynomial over $GF(q)$
Output	Level 1/Argument 1	$\{a, \{g_1, e_1\}, \{g_2, e_2\}, \dots, \{g_n, e_n\}\}$ $(a \in GF(q),\ g_i \in GF(q)[X]$: irreducible polynomial, $e_i \in \mathbb{Z}$ such that $g = ag_1^{e_1} g_2^{e_2} \dots g_n^{e_n})$

Input	Level 1/Argument 1	a list of polynomials over $GF(q)$
Output	Level 1/Argument 1	a list of lists

e.g. ($GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$)

Input	Level 1/Argument 1	$X^3 + X + 1$
Output	Level 1/Argument 1	$\{1, \{X + \alpha, 1\}, \{X + \alpha^2, 1\}, \{X + \alpha^2 + \alpha, 1\}\}$

Input	Level 1/Argument 1	$\{X^2 + \alpha, X^2 + \alpha^3 X + \alpha\}$
Output	Level 1/Argument 1	$\{\{1, \{X+\alpha^2+\alpha, 2\}\}, \{1, \{X+1, 1\}, \{X+\alpha, 1\}\}\}$

RREFGF

Row-reduced Echelon form of a matrix over $GF(q)$

Input	Level 1/Argument 1	a matrix over $GF(q)$
Output	Level 1/Argument 1	a matrix over $GF(q)$

e.g. ($GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$)

Input	Level 1/Argument 1	$[[1, \alpha, \alpha^2], [\alpha^2, \alpha, 1]]$
Output	Level 1/Argument 1	$[[1, 0, 1], [0, 1, \alpha^2 + \alpha + 1]]$

IMAGEGF

Image of a matrix over $GF(q)$.

Input	Level 1/Argument 1	a matrix over $GF(q)$
Output	Level 1/Argument 1	a list of vectors over $GF(q)$: the basis of the image of input matrix.

e.g. ($GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$)

Input	Level 1/Argument 1	$[[1, \alpha], [\alpha^2, \alpha + 1]]$
Output	Level 1/Argument 1	$\{[1, \alpha^2]\}$

BASISGF

Basis of a vector space over $GF(q)$.

Input	Level 1/Argument 1	a list of vectors over $GF(q)$
Output	Level 1/Argument 1	a list of vectors over $GF(q)$: the basis of the linear space spanned by vectors of input.

e.g. ($GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$)

Input	Level 1/Argument 1	$\{[1, \alpha^2], [\alpha, \alpha + 1]\}$
Output	Level 1/Argument 1	$\{[1, \alpha^2]\}$

KERGF

Kernel of a matrix over $GF(q)$.

Input	Level 1/Argument 1	a matrix over $GF(q)$
Output	Level 1/Argument 1	a list of vectors over $GF(q)$: the basis of the kernel of input matrix.

e.g. ($GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$)

Input	Level 1/Argument 1	$[[1, \alpha], [\alpha^2, \alpha + 1]]$
Output	Level 1/Argument 1	$\{[\alpha, 1]\}$

IBASISGF

Basis of the intersection of two vector spaces over $GF(q)$.

Input	Level 2/Argument 1	a list of vectors over $GF(q)$
	Level 1/Argument 2	a list of vectors over $GF(q)$
Output	Level 1/Argument 1	a list of vectors over $GF(q)$: the basis of the intersection of two linear spaces spanned by input vectors.

e.g. ($GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$)

Input	Level 2/Argument 1	$\{[1, \alpha, 1], [1, 1, \alpha]\}$
	Level 1/Argument 2	$\{[1, \alpha, 0], [0, 0, 1]\}$
Output	Level 1/Argument 1	$\{[1, \alpha, 1]\}$

MINPOLY

Calculates the minimal polynomial for an element of $GF(q)$ over $GF(p)$

Input	Level 1/Argument 1	a : an element of $GF(q)$
Output	Level 1/Argument 1	g : the minimal polynomial of a in $GF(p)[X]$

Input	Level 1/Argument 1	$\{a_1, \ldots, a_m\}$: a list of elements of $GF(q)$
Output	Level 1/Argument 1	$\{g_1, \ldots, g_m\}$: list of the minimal polynomial of a_i in $GF(p)[X]$

e.g. ($GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$)

Input	Level 1/Argument 1	$\alpha + 1$
Output	Level 1/Argument 1	$X^3 + X^2 + 1$

Input	Level 1/Argument 1	$\{\alpha + 1, \alpha^2\}$
Output	Level 1/Argument 1	$\{X^3 + X^2 + 1, X^3 + X + 1\}$

MINPOLY2

Calculates the minimal polynomial for an element a over $GF(p)(b)$, where a and b are elements of $GF(q)$ and $GF(p)(b)$ is the minimum field containing $GF(p)$ and b.

Input	Level 2/Argument 2	a : an element of $GF(q)$
	Level 1/Argument 1	b : an element of $GF(q)$
Output	Level 1/Argument 1	g : the minimal polynomial of a in $GF(p)(b)[X]$

e.g. ($GF(q) = GF(2^6) = \mathbb{Z}_2[\alpha]/(\alpha^6+\alpha+1)$. The minimal polynomial of $b = \alpha^9$ is X^3+X^2+1 (by MINPOLY) and $GF(p)(b) = GF(2)(\alpha^9) = \mathbb{Z}_2[x]/(x^3+x^2+1) = GF(2^3)$.)

Input	Level 2/Argument 2	$\alpha + 1$
	Level 1/Argument 1	α^9
Output	Level 1/Argument 1	$X^2 + ((\alpha^9)^2 + 1)X + (\alpha^9)^2 + \alpha^9$

ISPEZ?

If the input is a primitive element in $GF(p)$, ISPEZ? returns 1, else returns 0.

Input	Level 1/Argument 1	a : an element of $GF(p)$
Output	Level 1/Argument 1	1/0 : primitive/non-primitive.

e.g. ($p = 13$)

Input	Level 1/Argument 1	2
Output	Level 1/Argument 1	1.

ISPEGF?

If the input is a primitive element in $GF(q)$, ISPEGF? returns 1, else returns 0.

Input	Level 1/Argument 1	a : an element of $GF(q)$
Output	Level 1/Argument 1	1/0 : primitive/non-primitive.

e.g. ($GF(q) = GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$)

Input	Level 1/Argument 1	$\alpha^2 + 1$
Output	Level 1/Argument 1	1.

ISPPOLY?

If the input is a primitive polynomial over $GF(p)$, ISPPOLY? returns 1, else returns 0.

Input	Level 1/Argument 1	$f(X)$: a polynomial over $GF(p)$
Output	Level 1/Argument 1	1/0 : primitive/non-primitive.

e.g. ($p = 2$)

Input	Level 1/Argument 1	$X^3 + X + 1$
Output	Level 1/Argument 1	1.

PEZ

Finds a primitive element in $GF(p)$.

Input	None	None
Output	Level 1/Argument 1	a primitive element in $GF(p)$

e.g. ($p = 13$)

Input	None	None
Output	Level 1/Argument 1	2

NPEZ

Finds the next primitive element in $GF(p)$.

Input	Level 1/Argument 1	an element of $GF(p)$
Output	Level 1/Argument 1	a primitive element in $GF(p)$

e.g. ($p = 13$)

Input	Level 1/Argument 1	2
Output	Level 1/Argument 1	6

PEGF

Finds a primitive element in $GF(q)$.

Input	None	None
Output	Level 1/Argument 1	a primitive element in $GF(q)$

e.g. ($GF(q) = GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$)

Input	None	None
Output	Level 1/Argument 1	α

NPEGF

Finds the next primitive element in $GF(q)$.

Input	Level 1/Argument 1	an element of $GF(q)$
Output	Level 1/Argument 1	a primitive element in $GF(q)$

e.g. ($GF(q) = GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$)

Input	Level 1/Argument 1	α
Output	Level 1/Argument 1	$\alpha + 1$

NPPOLY

Finds the next primitive polynomial over $GF(p)$.

Input	Level 1/Argument 1	a polynomial over $GF(p)$
Output	Level 1/Argument 1	a primitive polynomial over $GF(p)$

e.g. ($p = 2$)

Input	Level 1/Argument 1	X^3
Output	Level 1/Argument 1	$X^3 + X + 1$

GFINVM

Inverse matrix over $GF(q)$.

Input	Level 1/Argument 1	a matrix over $GF(q)$
Output	Level 1/Argument 1	the inverse matrix over $GF(q)$

e.g. ($GF(q) = GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$)

Input	Level 1/Argument 1	$[[\alpha, \alpha^2], [1, 0]]$
Output	Level 1/Argument 1	$[[0, 1], [\alpha^2 + \alpha + 1, \alpha^2 + 1]]$

GFLOG

GFLOG(b) returns a non-negative integer n such that $\alpha^n = b$ for $b \in GF(q)$. If there is no integer with $\alpha^n = b$, GFLOG returns ∞. GFLOG searches n from 0 to $q - 2$ simply, so GFLOG is not fast.

Input	Level 1/Argument 1	b : an element of $GF(q)$
Output	Level 1/Argument 1	a non-negative integer n such that $\alpha^n = b$

Input	Level 1/Argument 1	$\{b_1, \ldots, b_m\}$: a list of elements of $GF(q)$
Output	Level 1/Argument 1	$\{n_1, \ldots, n_m\}$: a list of non-negative integers n_i such that $\alpha^{n_i} = b_i$

e.g. ($GF(q) = GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$)

Input	Level 1/Argument 1	$\alpha^2 + 1$
Output	Level 1/Argument 1	6

Input	Level 1/Argument 1	$\{\alpha^2 + \alpha, \alpha^2 + 1\}$
Output	Level 1/Argument 1	$\{4, 6\}$

e.g. ($GF(q) = GF(2^4) = \mathbb{Z}_2[\alpha]/(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1)$. The polynomial $X^4 + X^3 + X^2 + X + 1$ is not primitive.)

Input	Level 1/Argument 1	$\alpha + 1$
Output	Level 1/Argument 1	∞

GFLOG2

GFLOG2(b,a) returns a non-negative integer n such that $a^n = b$ for $a, b \in GF(q)$. If there is no integer with $a^n = b$, GFLOG2 returns ∞. GFLOG2 searches n from 0 to $q-2$ simply, so GFLOG2 is not fast.

Input	Level 2/Argument 1	b : an element of $GF(q)$
	Level 1/Argument 2	a : an element of $GF(q)$
Output	Level 1/Argument 1	a non-negative integer n such that $a^n = b$

e.g. ($GF(q) = GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$)

Input	Level 2/Argument 1	α^2
	Level 1/Argument 2	$\alpha + 1$
Output	Level 1/Argument 1	3

GFA

The list of all elements of $GF(q)$.

Input	Level 1/Argument 1	None
Output	Level 1/Argument 1	The list of all elements of $GF(q)$

e.g. ($GF(q) = GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$)

Input	Level 1/Argument 1	None
Output	Level 1/Argument 1	$\{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$

Takashi Matsubara (qqvv6t89@io.ocn.ne.jp)