Polynomial Representation

The elements of F_2^m are polynomials of degree less than m, with coefficients in F_2; that is,

$$\{a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \ldots + a_2x^2 + a_1x + a_0 \mid a_i = 0 \text{ or } 1\}.$$

These elements can be written in vector form as $(a_{m-1} \ldots a_1\ a_0)$.

F_2^m has 2^m elements.

The main operations in F_2^m are addition and multiplication.

Some computations involve a polynomial

$$f(x) = x^m + f_{m-1}x^{m-1} + f_{m-2}x^{m-2} + \ldots + f_2x^2 + f_1x + f_0,$$

where each f_i is in F_2. The polynomial $f(x)$ must be irreducible; that is, it cannot be factored into two polynomials over F_2, each of degree less than m.

Addition

$$(a_{m-1} \ldots a_1\ a_0) + (b_{m-1} \ldots b_1\ b_0) = (c_{m-1} \ldots c_1\ c_0)$$

where each $c_i = a_i + b_i$ over F_2. Addition is just the componentwise XOR of $(a_{m-1} \ldots a_1\ a_0)$ and $(b_{m-1} \ldots b_1\ b_0)$.

Subtraction

In the field F_2^m, each element $(a_{m-1} \ldots a_1\ a_0)$ is its own additive inverse, since $(a_{m-1} \ldots a_1\ a_0) + (a_{m-1} \ldots a_1\ a_0) = (0 \ldots 0\ 0)$, the additive identity. Thus addition and subtraction are equivalent operations in F_2^m.

Multiplication

$$(a_{m-1} \ldots a_1\ a_0)\ (b_{m-1} \ldots b_1\ b_0) = (r_{m-1} \ldots r_1\ r_0)$$

where $r_{m-1}x^{m-1} + \ldots + r_1x + r_0$ is the remainder when the polynomial $(a_{m-1}x^{m-1} + \ldots + a_1x + a_0)\ (b_{m-1}x^{m-1} + \ldots + b_1x + b_0)$ is divided by the polynomial $f(x)$ over F_2. (Note that all polynomial coefficients are reduced modulo 2.)

Exponentiation

The exponentiation $(a_{m-1} \ldots a_1\ a_0)^e$ is performed by multiplying together e copies of $(a_{m-1} \ldots a_1\ a_0)$.

Multiplicative Inversion

There exists at least one element g in F_2^m such that all non-zero elements in F_2^m can be expressed as a power of g. Such an

element $\boldsymbol{g}$ is called a *generator* of $F_2{}^m$. The multiplicative inverse of an element $a = g^i$ is $a^{-1} = g^{(-i) \bmod (2^m - 1)}$.

$F_2{}^4$ with Polynomial Representation

The elements of $F_2{}^4$ are the 16 vectors:

(0000) (0001) (0010) (0011) (0100) (0101) (0110) (0111)

(1000) (1001) (1010) (1011) (1100) (1101) (1110) (1111).

The irreducible polynomial used will be $\boldsymbol{f(x) = x^4 + x + 1}$. The following are sample calculations.

Addition

(0110) + (0101) = (0011).

Multiplication

(1101) (1001)

$= (x^3 + x^2 + 1)\,(x^3 + 1) \bmod f(x)$

$= x^6 + x^5 + 2x^3 + x^2 + 1 \bmod f(x)$

$= x^6 + x^5 + x^2 + 1 \bmod f(x)$ (coefficients are reduced modulo 2)

$= (x^4 + x + 1)(x^2 + x) + (x^3 + x^2 + x + 1) \bmod f(x)$

$= x^3 + x^2 + x + 1$

$= (1111).$

Exponentiation

To compute $(0010)^5$, first finds
$(0010)^2$
$= (0010)\ (0010)$
$= x\ x \bmod f(x)$
$= (x^4 + x + 1)(0) + (x^2) \bmod f(x)$
$= x^2$
$= (0100).$
Then
$(0010)^4$
$= (0010)^2\ (0010)^2$
$= (0100)\ (0100)$
$= x^2\ x^2 \bmod f(x)$
$= (x^4 + x + 1)(1) + (x + 1) \bmod f(x)$
$= x + 1$
$= (0011).$
Finally, $(0010)^5$
$= (0010)^4\ (0010)$
$= (0011)\ (0010)$
$= (x + 1)\ (x) \bmod f(x)$
$= (x^2 + x) \bmod f(x)$
$= (x^4 + x + 1)(0) + (x^2 + x) \bmod f(x)$
$= x^2 + x$
$= (0110).$

Multiplicative Inversion

The element $\boldsymbol{g} = (0010)$ is a generator for the field. The powers of $\boldsymbol{g}$ are:

$g^0 = (0001)$	$g^1 = (0010)$	$g^2 = (0100)$	$g^3 = (1000)$
$g^4 = (0011)$	$g^5 = (0110)$	$g^6 = (1100)$	$g^7 = (1011)$
$g^8 = (0101)$	$g^9 = (1010)$	$g^{10} = (0111)$	$g^{11} = (1110)$
$g^{12} = (1111)$	$g^{13} = (1101)$	$g^{14} = (1001)$	$g^{15} = (0001)$

The multiplicative identity for the field is $g^0 = (0001)$.

The multiplicative inverse of $g^7 = (1011)$ is

$g^{-7 \bmod 15} = g^{8 \bmod 15} = (0101)$.

To verify this, see that

$(1011)\ (0101)$

$= (x^3 + x + 1)\ (x^2 + 1) \bmod f(x)$

$= x^5 + x^2 + x + 1 \bmod f(x)$

$= (\ x^4 + x + 1)(x) + (1) \bmod f(x)$

$= 1$

$= (0001)$,

which is the multiplicative identity.