Introduction to finite fields, II

Finite field of p^n elements

$\mathbb{F}_4$

Because we are interested in doing "computer things" it would be useful for us to construct fields having 2^n elements.

Let's construct a field of 4 elements; we will mimic the construction of the integers mod a prime p. We begin with the polynomials having coefficients from $\mathbb{F}_2$; i.e., each of the coefficients of our polynomials is either 0 or 1. Select a polynomial of degree 2 that is irreducible over $\mathbb{F}_2$ (i.e., it does not factor into polynomials of smaller degree having coefficients 0 and 1). This irreducible polynomial corresponds to the prime p. There are irreducibility tests for polynomials just as there are primality tests for integers. For example, $X^2 + X + 1$ is irreducible over $\mathbb{F}_2$. By polynomial long division, divide each polynomial having coefficients 0 and 1 by $X^2 + X + 1$ and take the remainder. What does the remainder look like? After division, the remainder is of degree less than 2; so, the remainder will look like $\square x + \square$ where each coefficient is either 0 or 1. So, there are 4 possible remainders: $0x + 0 = 0$, $0x + 1 = 1$, $1x + 0 = x$, and $1x + 1 = x + 1$. These 4 elements form a field.

Sometimes polynomials model "real world" situations, and X is treated as an unknown for which we want to solve. We want to look at polynomials in a slightly different way now – more of an abstract algebra way. We do not care about solving for the "value of X," we only care about the polynomial itself. Thinking this way, a polynomial is determined by its coefficients; the powers of X are just used to separate the coefficients. We could just as well think of a polynomial as a vector where the components are the coefficients; e.g., the four remainders that we obtained above could be written as (0, 0), (0, 1), (1, 0), and (1, 1). We will use these vectors as the elements of our field of 4 elements rather than the corresponding polynomials (but we will have to remember from time to time that they "really are polynomials" to make sense of multiplication).

We could carry this one more step. We are used to work with strings of bits; so, we might replace the 4 polynomials and their corresponding vectors by the 2-bit strings 00, 01, 10, 11.

So, we have the following correspondences:

polynomial	vector	bit string
$0X+0$	(0, 0)	00
$0X+1$	(0, 1)	01
$1X+0$	(1, 0)	10
$1X+1$	(1, 1)	11

We will be thinking about bit strings. We have always been able to add (XOR) strings of bits, but we want to come up with a way to multiply strings of bits. Then we can apply some of the mathematical ideas that we used with the classical ciphers to strings of bits.

Addition of vectors

To add (1, 0) and (1, 1), we can think of adding the corresponding polynomials mod 2:

$$\begin{array}{r} X+0 \\ X+1 \\ \hline 0X+1 \end{array}$$

Thinking of vectors, we just add the vectors mod 2:

$$\begin{array}{r} (1,\,0) \\ (1,\,1) \\ \hline (0,\,1) \end{array}$$

Or, in terms of 2-bit strings:

$$\begin{array}{r} 10 \\ 11 \\ \hline 01 \end{array}$$

which just corresponds to XORing bits.

Here is the addition table for our field of 4 elements:

+	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 0)	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 1)	(0, 1)	(0, 0)	(1, 1)	(1, 0)
(1, 0)	(1, 0)	(1, 1)	(0, 0)	(0, 1)
(1, 1)	(1, 1)	(1, 0)	(0, 1)	(0, 0)

Multiplication of vectors

To multiply, we must recall the polynomial origins of our operations.

To multiply $(1, 0)\times(1, 1)$, we must multiply

$$X\times(X+1)=X^2+X$$

and then go mod X^2+X+1. By polynomial long division mod 2, we obtain

$$X^2+X=1\left(X^2+X+1\right)+1$$

Mod X^2+X+1, this becomes (the remainder) 1. So, $(1, 0)\times(1, 1)=(0, 1)$.

Here is the multiplication table for our field of 4 elements.

×	(0, 1)	(1, 0)	(1, 1)
(0, 1)	(0, 1)	(1, 0)	(1, 1)
(1, 0)	(1, 0)	(1, 1)	(0, 1)
(1, 1)	(1, 1)	(0, 1)	(1, 0)

$\mathbb{F}_8$

To construct a field of $8 = 2^3$ elements, we would need to mod out by an irreducible polynomial of degree 3; the remainders would look like $\square X^2 + \square X + \square$ where each coefficient is either 0 or 1.

To construct a field of $16 = 2^4$ elements, we would need to mod out by an irreducible polynomial of degree 4; the remainders would look like $\square X^3 + \square X^2 + \square X + \square$.

To construct a field of bytes, we would need to mod out by an irreducible polynomial of degree 8.

Let's construct a field of 8 elements.

We will use the polynomial $X^3 + X^2 + 1$, which is irreducible over $\mathbb{F}_2$.

The remainders after division by $X^3 + X^2 + 1$ look like $\{ax^2 + bx + c : a, b, c \in \mathbb{F}_2\}$; i.e., the remainders look like 3-dimensional vectors where each component is 0 or 1. Or, we could think of the remainders as being 3-bit strings.

Addition is XORing bits.

Addition

	(0,0,0)	(0,0,1)	(0,1,0)	(1,0,0)	(1,0,1)	(1,1,1)	(0,1,1)	(1,1,0)
(0,0,0)	(0,0,0)	(0,0,1)	(0,1,0)	(1,0,0)	(1,0,1)	(1,1,1)	(0,1,1)	(1,1,0)
(0,0,1)	(0,0,1)	(0,0,0)	(0,1,1)	(1,0,1)	(1,0,0)	(1,1,0)	(0,1,0)	(1,1,1)
(0,1,0)	(0,1,0)	(0,1,1)	(0,0,0)	(1,1,0)	(1,1,1)	(1,0,1)	(0,0,1)	(1,0,0)
(1,0,0)	(1,0,0)	(1,0,1)	(1,1,0)	(0,0,0)	(0,0,1)	(0,1,1)	(1,1,1)	(0,1,0)
(1,0,1)	(1,0,1)	(1,0,0)	(1,1,1)	(0,0,1)	(0,0,0)	(0,1,0)	(1,1,0)	(0,1,1)
(1,1,1)	(1,1,1)	(1,1,0)	(1,0,1)	(0,1,1)	(0,1,0)	(0,0,0)	(1,0,0)	(0,0,1)
(0,1,1)	(0,1,1)	(0,1,0)	(0,0,1)	(1,1,1)	(1,1,0)	(1,0,0)	(0,0,0)	(1,0,1)
(1,1,0)	(1,1,0)	(1,1,1)	(1,0,0)	(0,1,0)	(0,1,1)	(0,0,1)	(1,0,1)	(0,0,0)

Multiplication is polynomial multiplication modulo $X^3 + X^2 + 1$.

Multiplication

	(0,0,1)	(0,1,0)	(1,0,0)	(1,0,1)	(1,1,1)	(0,1,1)	(1,1,0)
(0,0,1)	(0,0,1)	(0,1,0)	(1,0,0)	(1,0,1)	(1,1,1)	(0,1,1)	(1,1,0)
(0,1,0)	(0,1,0)	(1,0,0)	(1,0,1)	(1,1,1)	(0,1,1)	(1,1,0)	(0,0,1)
(1,0,0)	(1,0,0)	(1,0,1)	(1,1,1)	(0,1,1)	(1,1,0)	(0,0,1)	(0,1,0)
(1,0,1)	(1,0,1)	(1,1,1)	(0,1,1)	(1,1,0)	(0,0,1)	(0,1,0)	(1,0,0)
(1,1,1)	(1,1,1)	(0,1,1)	(1,1,0)	(0,0,1)	(0,1,0)	(1,0,0)	(1,0,1)
(0,1,1)	(0,1,1)	(1,1,0)	(0,0,1)	(0,1,0)	(1,0,0)	(1,0,1)	(1,1,1)
(1,1,0)	(1,1,0)	(0,0,1)	(0,1,0)	(1,0,0)	(1,0,1)	(1,1,1)	(0,1,1)

$\mathbb{F}_{16}$

The simplified AES we considered uses a field of 16 elements obtained by going modulo the irreducible polynomial $X^4 + X + 1$. For example,

$$(1, 0, 1, 1) + (0, 1, 1, 0) = (1, 1, 0, 1)$$

and

$$(1, 0, 1, 1) \times (1, 1, 0, 1) = (0, 1, 1, 0)$$

Although E.H. Moore proved that for each p^n, p prime, there is an unique finite field of p^n elements, the uniqueness is "up to isomorphism" – an algebraic term. Addition is the same for all finite fields of p^n elements; it is just addition modulo p^n. But, multiplication of two elements of the field depends on the irreducible polynomial that is used as the modulus.