galois

2024年9月16日 星期一 11:03

galois

ANU COMP2700: Galois field by examples

Alwen Tiu (26/09/2022)

Concepts and notations

Recall that a Galois field $GF(2^n)$, for $n \geq 2$, is a finite field whose elements are polynomials of degree at most $n-1$ and whose coefficients are elements of $GF(2)$. $GF(2)$ is a finite field with two elements $\{0, 1\}$, with two operations: addition modulo 2, and multiplication modulo 2.

Some examples:

- The elements of $GF(2^2)$ consists of `polynomials` of degree at most 1:

$$\{0, 1, x, x+1\}.$$

- The elements of $GF(2^3)$ are polynomials of degree at most 2:

$$\{0,\ 1,\ x,\ x+1,\ x^2,\ x^2+1,\ x^2+x,\ x^2+x+1\}.$$

- The elements of $GF(2^4)$ are polynomials of degree at most 3:

$$\begin{Bmatrix} 0,\ 1,\ x,\ x+1,\ x^2,\ x^2+1,\ x^2+x,\ x^2+x+1 \\ x^3,\ x^3+1,\ x^3+x,\ x^3+x+1, \\ x^3+x^2,\ x^3+x^2+1,\ x^3+x^2+x,\ x^3+x^2+x+1 \end{Bmatrix}$$

Note that the x's in a polynomial in $GF(2^n)$ are not meant to be evaluated when performing computations over $GF(2^n)$.

Binary Representation of $GF(2^n)$

Given a polynominal in $GF(2^k)$

$$a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_2x^2 + a_1x + a_0$$

we can represent it as a vector of its coefficients:

$$(a_{k-1}, a_{k-2}, \ldots, a_2, a_1, a_0).$$

Since the coeeficients are drawn from $GF(2)$ (whose elements are 0 and 1), each element of $GF(2^k)$ can be represented as a bit vector of length k.

Note that in writing polynomials, terms that have 0 as their coefficients are not written explicitly. For example, in $GF(2^4)$, when we write x^2+x+1, we really mean the polynomial $0 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 1$. However, when representing a polynomial as a vector, we need to include the coefficients for those missing terms as well. So for this particular example, the bit vector representation is $(0, 1, 1, 1)$.

For brevity, when writing a bit vector, we will omit the parentheses and the commas, so for example, we will write 0111 to denote the bit vector $(0, 1, 1, 1)$.

Some more examples:

- The polynomial $x^3 + x^2 + 1 \in GF(2^4)$ can be rewritten as

  $$1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 1$$

  so it can be represented as the bit vector 1101.

- The same polynomial $x^3 + x^2 + 1$, when considered as an element of $GF(2^8)$ can be represented as the bit vector 00001101. This is because when considered as an element of $GF(2^8)$, $x^3 + x^2 + 1$ is the same as

  $$0 \cdot x^7 + 0 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 1.$$

  That is, we need to represent the coefficients of the omitted terms x^7, x^6, x^5 and x^4.

- The bit vector 10011 can be interpreted as the following polynomial in $GF(2^5)$:

  $$1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 1 = x^4 + x + 1.$$

HEX representation of $GF(2^8)$

Elements of $GF(2^8)$ can be represented as bit vectors of length 8, in other words, a byte. For AES (and many other operations in computer science), it is often convenient to use the hexadecimal notation (HEX) to represent bytes. Given a bit vector of length 8, its HEX representation consists of two HEX digits, representing the first four bits and the last four bits, respectively. So for example, the bit vector 00111101 can be represented as the HEX number 3D, where 3 represents the first 4 bits (0011) and D represents the last 4 bits (1101).

Some examples:

- The polynomial $x^3 + x^2 + 1 \in GF(2^8)$ can be represented as the bit vector 00001101, which in turn can be represented as the HEX number 0D.
- The HEX number AE represents the bit vector 10101110 (since 1010 is A and 1110 is E in HEX), which in turn represents the following polynomial in $GF(2^8)$:

  $$x^7 + x^5 + x^3 + x^2 + x.$$

Addition and subtraction in $GF(2^n)$

To add two polynomials in $GF(2^n)$, simply add up the coefficients for the same terms.

Addition and subtraction in $GF(2)$ are the same operation. This is because we have in GF(2):

$$-1 \equiv 1 \mod 2.$$

Therefore

$$a + b \equiv a + 1 \cdot b \equiv a + (-1) \cdot b \equiv a - b \mod 2.$$

Examples:

1. Let $A(x) = x^3 + x^2 + 1$ and $B(x) = x^2 + x$ be two polynomials in $GF(2^4)$. Compute $A(x) + B(x)$.

$$\begin{array}{rrcl} & A(x) & = & 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 1 \\ + & B(x) & = & 0 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 0 \\ \hline & A(x) + B(x) & = & (1+0 \mod 2) \cdot x^3 + (1+1 \mod 2) \cdot x^2 + (0+1 \mod 2) \cdot x + (1+0 \mod 2) \\ & & = & 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 1 \\ & & = & x^3 + x + 1. \end{array}$$

2. Let $x = 0\text{A}$ and $y = \text{B1}$ be two HEX numbers representing two polynomials in $GF(2^8)$. Compute the HEX value $(x + y)$ in $GF(2^8)$.

$$\begin{array}{rll} & 0\text{A} = 00001010 & \longrightarrow 0 \cdot x^7 + 0 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 0 \\ + & \text{B1} = 10110001 & \longrightarrow 1 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x + 1 \\ \hline & \text{BB} = 10111011 & \longleftarrow 1 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^3 + 1 \cdot x + 1 \end{array}$$

Observation 1: Addition and subtraction in $GF(2^n)$ can be computed by using bitwise XOR of the binary representations of the polynomials. So a shorter way to compute $(x + y)$ in the above example is to simply compute the following XOR on the binary representations:

$$00001010 \oplus 10110001 = 10111011 = \text{BB}$$

where $\oplus$ denotes the bitwise XOR operator.

Multiplication in $GF(2^n)$

Adding two polynomials in $GF(2^n)$ always results in another polynomial of degree at most $n - 1$, so the result is always in $GF(2^n)$. This is not the case with multiplication, as the result of multiplying two polynomials of degree at most k may result in another polynomial of degree higher than k. For example, we have x^6 and x^5 both in $GF(2^8)$, but their multiplication $x^6 \cdot x^5 = x^{11}$ is not in $GF(2^8)$, since its degree is higher than 7. In this case, we need to compute the remainder of x^{11} using a `modulus`, which is a (specifically) chosen *irreducible* polynomial of degree 8. For example, in AES, the irreducible polynomial chosen for the field $GF(2^8)$ is

$$P(x) = x^8 + x^4 + x^3 + x + 1.$$

Some examples:

1. Let $A(x) = x^3 + x + 1$ and $B(x) = x^5 + x^2$. Compute $A(x) \times B(x) \mod P(x)$ in $GF(2^8)$ with irreducible polynomial $P(x) = x^8 + x^4 + x^3 + x + 1$ as the modulus.

   We first compute the multiplication of $A(x)$ and $B(x)$, and then perform the remainder computation.

$$\begin{array}{rcl} A(x) \times B(x) & = & (x^3 + x + 1) \cdot (x^5 + x^2) \\ & = & x^3(x^5 + x^2) + x(x^5 + x^2) + (x^5 + x^2) \\ & = & x^8 + x^5 + x^6 + x^3 + x^5 + x^2 \\ & = & x^8 + x^6 + 2x^5 + x^3 + x^2 \\ & = & x^8 + x^6 + x^3 + x^2. \end{array}$$

   Recall that the coefficients of $GF(2^8)$ are in $GF(2)$, so $2x^5 = 0 \cdot x^5 = 0$ because $2 \equiv 0$ in $GF(2)$.

   Notice that the degree of $A(x) \times B(x)$ is 8, which is greater than 7 (which is the highest degree allowed in $GF(2^8)$). To compute the remainder of $A(x) \times B(x) \mod P(x)$, let us first compute the remainder of

$x^8 \mod P(x)$.

Since $P(x) = x^8 + x^4 + x^3 + x + 1$, subtracting both sides with $x^4 + x^3 + x + 1$, we get:

$$\begin{aligned} x^8 &= P(x) - (x^4 + x^3 + x + 1) && (1)\\ &= P(x) + (x^4 + x^3 + x + 1) && (2)\\ &\equiv x^4 + x^3 + x + 1 \mod P(x). && (3) \end{aligned}$$

Going from step (1) to (2), we use the fact that addition and subtraction are the same operation in $GF(2^8)$. Going from step (2) to (3), we use the definition of modulus: that is,

$$F(x) \equiv G(x) \mod P(x)$$

holds if and only if there is $H(x)$ such that

$$F(x) = H(x) \cdot P(x) + G(x).$$

Applying this to the equation (2), let $H(x) = 1$, $G(x) = x^4 + x^3 + 1$, and $F(x) = P(x) + (x^4 + x^3 + 1)$. Then we indeed have $F(x) = H(x) \cdot P(x) + G(x)$, and therefore $G(x) = x^4 + x^3 + x + 1$ is indeed our remainder.

Having obtained $x^8 \equiv x^4 + x^3 + x + 1 \mod P(x)$, we can substitute this to the equation for $A(x) \times B(x)$:

$$\begin{aligned} A(x) \times B(x) &\equiv x^8 + x^6 + x^3 + x^2 \\ &\equiv (x^4 + x^3 + x + 1) + x^6 + x^3 + x^2 \\ &\equiv x^6 + x^4 + x^2 + x + 1. \end{aligned}$$

2. Let $A(x) = x^3 + x^2$ and $B(x) = x^4 + x^2 + 1$. Compute $A(x) \times B(x) \mod P(x)$ in $GF(2^5)$ with $P(x) = x^5 + x^2 + 1$.

$$\begin{aligned} A(x) \times B(x) &= (x^3 + x^2) \cdot (x^4 + x^2 + 1) \\ &= x^7 + x^5 + x^3 + x^6 + x^4 + x^2 \\ &= x^7 + x^6 + x^5 + x^4 + x^3 + x^2 \end{aligned}$$

From $P(x) = x^5 + x^2 + 1$, using a similar reasoning as in the previous example, we get:

$$(*) \qquad x^5 = P(x) - (x^2 + 1) \equiv (x^2 + 1) \mod P(x).$$

From this, we derive:

$$\begin{aligned} x^6 &= x \cdot x^5 \\ &= x \cdot (x^2 + 1) \qquad \text{by } (*) \\ &\equiv x^3 + x \mod P(x) \\ x^7 &= x^2 \cdot x^5 \\ &= x^2 \cdot (x^2 + 1) \qquad \text{by } (*) \\ &\equiv x^4 + x^2 \mod P(x) \end{aligned}$$

We can now substitute the values of x^5, x^6 and x^7 to $A(x) \times B(x)$:

$$\begin{aligned} A(x) \times B(x) &= x^7 + x^6 + x^5 + x^4 + x^3 + x^2 \\ &= (x^4 + x^2) + (x^3 + x) + (x^2 + 1) + x^4 + x^3 + x^2 \\ &= 2x^4 + 2x^3 + 3x^2 + 1 \\ &\equiv x^2 + 1 \mod P(x) \end{aligned}$$

noting that the coefficients of the polynomial are in $GF(2)$ (so $2 \equiv 0 \mod 2$ and $3 \equiv 1 \mod 2$ in the last equation).