Polynomial arithmetic

Irreducible polynomial

The Galois field $GF(2)$ has two elements, 0 and 1, the binary numbers.

The set of polynomials *over* $GF(2)$ forms a ring, called the polynomial ring.

These are polynomials where the cofactors are either 0 or 1. Some examples:

$$x + 1$$

$$x^2 + x$$

$$x^2 + x + 1$$

but also 1 and x.

Remember that the way to get a finite field with integers is to do arithmetic mod some number.

If the set consists of polynomials, we do arithmetic mod some polynomial. (And it bears repeating that addition will be XOR, not the usual addition).

An irreducible or prime polynomial is one without factors. To say that a given polynomial $p(x)$ is irreducible means that there do not exist:

$$f(x) \times g(x) = p(x)$$

There are only two irreducible polynomials of degree 3 in $GF(2)$ and they are:

$$x^3 + x + 1$$

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

It is claimed that you cannot find $f(x)$ and $g(x)$ such that $f(x) \times g(x)$ is equal to either of these, and these are the only polynomials in $GF(2)$ (of degree 3) with that property.

That's a challenge.

Suppose we build up possible factors of these expressions, starting with $x^0 = 1$ and continuing with polynomials with greatest term x^1.

Degree $0 = x^0 = 1$ is a special kind of polynomial.

There are two polynomials of degree 1.

$$x$$

$$x + 1$$

Now consider all the polynomials with greatest term x^2 (degree 2) formed by multiplying these last two together:

$$x(x) = x^2$$

$$x(x + 1) = x^2 + x$$

$$(x + 1)(x + 1) = x^2 + 1$$

That's three, but there's one missing. The other one is

$$x^2 + x + 1$$

Since it can't be generated as a product of either of the degree 2 polynomials, it is irreducible.

It may help to think of these as binary numbers: all of those with three digits and the first digit a 1 are

$$100, 101, 110, 111$$

Those are the four we looked at above, and the last is in the irreducible class.

Now consider all products with greatest term x^3. These *must* arise as products of a degree 2 with a degree 1. Thus:

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

Recall that we said we'd use XOR for addition, that has been used for two cases. Six of these are unique:

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

$$x^3 + 1$$

It's easier to see if we write the binary numbers (there should be 8 altogether with four places and the first digit equal to 1):

1000 1010 1100 1110 1111 1001

The two missing ones are: 1011 and 1101, corresponding to

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

Since they do not appear in our results, there is no way to factor either one of them.

Proving something similar for higher degrees might seem to be a challenge, but we'll see Kak's proof later.

Modulo an irreducible polynomial

So the trick, apparently, is that if we define the field $GF(2^n)$ to be polynomials mod some irreducible polynomial, we get a field with good properties. I can't really understand the wikipedia article, but that's reading between the lines.

So, let's consider all polynomials defined over $GF(2)$ modulo the irreducible polynomial $x^3 + x + 1$.

When multiplication results in a polynomial whose degree equals or exceeds that of the irreducible polynomial, take the remainder modulo that polynomial.

One way to get the remainder is to do polynomial division:

Example:

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

Since there is a term with x^4, we must solve

$$\frac{x^4 + x^3 + x + 1}{x^3 + x + 1}$$

Let's see:

$$x(x^3 + x + 1) = x^4 + x^2 + x$$

which when subtracted from the numerator leaves $x^3 - x^2 + 1$ so we have

$$\frac{x^3 - x^2 + 1}{x^3 + x + 1}$$

Now the quotient is 1 with a remainder of $-x^2 - x$.

Recall that $-1 = 1$, because 1 is its own additive inverse: $1 + 1 = 0$ so $1 = 0 - 1$. We have then $x^2 + x$.

Restate the result:

$$\frac{x^4 + x^3 + x + 1}{x^3 + x + 1}$$
$$= x + 1 + \frac{x^2 + x}{x^3 + x + 1}$$
$$= x^2 + x \mod x^3 + x + 1$$

Let's check. The whole part was $x + 1$ so multiplying the irreducible polynomial by that gives:

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

$$= x^4 + x^3 + x^2 + 1$$

which falls short of the original numerator $x^4 + x^3 + x + 1$ by exactly $x^2 + x$:

$$(x^4 + x^3 + x^2 + 1) + (x^2 + x)$$
$$= x^4 + x^3 + x + 1$$

There is a less error-prone way to do this kind of modulo operation and we will see it at the end.

Summary

Polynomials defined over $GF(2)$ modulo the irreducible polynomial $x^3 + x + 1$ consist of the finite set:

$$0$$
$$1$$
$$x$$
$$x + 1$$
$$x^2$$
$$x^2 + 1$$
$$x^2 + x$$
$$x^2 + x + 1$$

We checked that $(x^2 + x + 1) \times (x^2 + 1) = x^2 + x$ using this modulus.

We assert without proof that all pairwise multiplications have this property.

It's starting to look familiar. In binary format:

000

001

010

011

100

101

110

111

There are only eight of them.

We refer to this set as $GF(2^3)$. 3 is the degree of the modulus polynomial, it is something like $x^3+b_2x^2+b_1x^1+b_0$. This arithmetic generates a field of polynomials of the form $b_2x^2 + b_1x^1 + b_0$, which corresponds in turn to the $2^3 = 8$ binary numbers shown above.

Polynomial arithmetic provides a way to *map* these binary values to a finite field.

Easy division

We need to solve:

$$\frac{x^4 + x^3 + x + 1}{x^3 + x + 1}$$

Left-shift $x^3 + x + 1$.

$$= x^4 + x^2 + x$$

Then XOR it with the numerator:

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

Now XOR this result with $x^3 + x + 1$:

$$= x^2 + x$$

And that's the same result.

Using binary numbers:

```
11011
1011
-----
 1101
 1011
  ----
  110
```

which is $x^2 + x$.

looking ahead

It's easy to be confused because, to take the example we've been working with, $2^3 = 8$ and the group Z_8 (integers mod 8) is not a field. That's because some elements of Z_8, namely, those that are not co-prime to 8 like $2, 4, 6$ do not have multiplicative inverses.

By using this definition of addition as XOR and polynomial arithmetic mod an irreducible polynomial of degree 3 is to **generate a field with 2^3 elements**. Each of the 8 elements will turn out to have a multiplicative inverse. And we can map the integers $0 - 7$ to this field.

We can do exactly the same thing with 2^8, generating $GF(2^8)$.