Factoring Polynomials in Finite Fields

Paul Stankovski

Factoring polynomials in finite fields is generally a hard problem. However, the examples that we encounter throughout this course are quite easy.

1 Basics

When we say "a polynomial $p(x)$ over $\mathbb{F}_q$", it means that the coefficients of the polynomial are elements of $\mathbb{F}_q$.

How to show that a polynomial $p(x)$ is reducible? Find a factor. That is, writing $p(x)$ as a product of two or more factors proves your point.

How to determine if a polynomial $p(x)$ is irreducible? If it is not reducible, it is irreducible. You need to convincingly show that $p(x)$ *cannot* be written as a product of two (or more) factors. If $p(x)$ is a polynomial of degree n, then it is sufficient to show that factors of degree $\lfloor \frac{n}{2} \rfloor$ or less cannot exist (why?).

Let's see how we can actually find these (irreducible) factors.

2 Finding linear factors

The smallest factors, linear ones. You know how to do this already, by looking for zeros. An element $a \in \mathbb{F}_q$ is a root of $p(x)$ if $p(a) = 0$. This means that $p(x)$ has a factor $x - a$ and can be written as

$$p(x) = (x - a)p'(x) \tag{1}$$

for some polynomial $p'(x)$ of smaller degree. Using $p(x)$ and the linear factor $x - a$, you can easily determine $p'(x)$ by polynomial division.

You are now left with a problem that is smaller, factoring $p'(x)$. Repeat the above, look for linear factors in $p'(x)$. Make sure that you understand how to spot multiple zeros.

When working in $\mathbb{F}_q$, there are q possible zeros for you to examine, don't forget to try all of them.

When q is prime, you can think of $\mathbb{F}_q$ as $\mathbb{Z}/q\mathbb{Z}$ (integers modulo q), so you may need to try all of $p(0), p(1), \ldots, p(q-1)$ to obtain a complete factorization. Also, if you want to avoid the minus sign in the linear factor $(x - a)$ in Eq. (1), you can write it as $(x + (q - a))$.

3 Finding quadratic factors

If there are no linear factors, you need to step up and search for quadratic factors. Use the definition. For example, consider

$$p(x) = x^5 + x + 1,$$

which has no linear factors over $\mathbb{F}_2$. For $p(x)$ to be reducible, it must be possible to write

$$p(x) = (x^2 + ax + b)(x^3 + cx^2 + dx + e) \tag{2}$$

for some constants $a, b, c, d, e \in \mathbb{F}_2$. Now simply carry out the multiplication in Eq. (2) and identify coefficients.

$$\begin{aligned} p(x) &= (x^2 + ax + b)(x^3 + cx^2 + dx + e) \\ &= x^5 + (a + c)x^4 + (b + d + ac)x^3 + \\ &\quad (e + ad + bc)x^2 + (ae + bd)x + be \\ &= x^5 + x + 1, \end{aligned}$$

which gives us the equation system

$$\begin{cases} a + c &= 0, \\ b + d + ac &= 0, \\ e + ad + bc &= 0, \\ ae + bd &= 1, \\ be &= 1, \end{cases}$$

in $\mathbb{F}_2$. If the resulting equation system has a solution (in this case it does, $a = b = c = e = 1$ and $d = 0$), then you have found a factorization. If the system has no solutions, then there are no factors of degree two.

This approach generalizes to factors of higher degree as well, of course, but there is a limit to what is practical to do by hand.

A simple shortcut that can be applied above is to realize that we must have $b = e = 1$ in Eq. (2).