1 Factoring polynomials over finite fields

In this section we describe Berlekamp's algorithm for computing the factorization of a polynomial in $\mathbb{F}_q[x]$ into irreducible factors. First we briefly recall some facts on polynomial rings.

In the sequel F will be a field, and $F[x]$ the polynomial ring over F in one indeterminate x.

Lemma 1 *Let $f, g \in F[x]$. Then there are unique $q, r \in F[x]$ such that $f = qg + r$ and $\deg r < \deg g$.*

There is a standard algorithm for computing the q, r from the previous lemma, called the *division algorithm*.

Lemma 2 *Let $I \subset F[x]$ be an ideal. Then there is a $g \in F[x]$ such that I is generated by g.*

Proof. For g choose a polynomial in I of minimal degree. Then using Lemma 1 it is straightforward to see that g generates I. $\square$

Proposition 3 *Let $f_1, f_2 \in F[x]$. Then there is a unique monic $g \in F[x]$ such that*

$$g \text{ divides } f_1 \text{ and } f_2 \tag{1}$$

$$\text{if } h \text{ divides } f_1, f_2 \text{ then } h \text{ divides } g. \tag{2}$$

Proof. Let g be a monic generator of the ideal I of $F[x]$ generated by f_1, f_2. Then (1) is trivial, and for (2) we note that, since $g \in I$, there are $g_1, g_2 \in F[x]$ such that $g = g_1 f_1 + g_2 f_2$.

Now supppose that there is a monic g' with (1) and (2). Then it follows that g' divides g, and g divides g'. Hence $g = g'$. $\square$

The polynomial g of the previous theorem is called the *greatest common divisor* of f_1 and f_2; it is denoted by $\gcd(f_1, f_2)$. We have that $\gcd(f_1, f_2)$ is the monic polynomial of maximal degree that divides both f_1 and f_2. (Indeed, consider the set D of all monic polynomials dividing both f_1 and f_2. Then $\gcd(f_1, f_2) \in D$, and it is the element of maximal degree in D by (2).)

Lemma 4 *Let $f, g \in F[x]$, and write $f = qg + r$. Then $\gcd(g, f) = \gcd(g, r)$.*

Proof. Let D_1 be the set of all polynomials dividing both g, f. Let D_2 be the set of all polynomials dividing both g, r. Then it is straightforward to prove that $D_1 = D_2$. $\square$

By Lemma 4 we have the following algorithm for calculating $\gcd(f, g)$. Set $r_0 = f$, $r_1 = g$. And for $n \geq 1$ let r_{n+1} be the unique element of $F[x]$ such that $\deg r_{n+1} < \deg r_n$ and $r_{n-1} = q_n r_n + r_{n+1}$. Since the degree of r_n decreases by every step, there is a $k > 0$ such that $r_{k+1} = 0$. In that case $r_k = \gcd(f, g)$. (Indeed, by Lemma 4 it follows that $\gcd(f, g) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_k, k_{k+1}) = r_k$.)

Example 5 Consider the polynomials $f = x^7 + 1$ and $g = x^4 + x^2 + x$ in $\mathbb{F}_2[x]$. We set $r_0 = f$, and $r_1 = g$. Furthermore, $r_0 = (x^3 + x + 1)r_1 + x^3 + x + 1$, so $r_2 = x^3 + x + 1$. Now $r_1 = xr_2 + 0$, and $r_3 = 0$. Therefore, $\gcd(f, g) = x^3 + x + 1$.

An element $f \in F[x]$ is said to be *irreducible* if $f = gh$ with $g, h \in F[x]$ implies that $g \in F$ or $h \in F$.

Theorem 6 *Let $f \in F[x]$. Then f can be written $f = cf_1^{e_1} \cdots f_r^{e_r}$, where $c \in F$, the f_i are monic and irreducible, and $f_i \neq f_j$ for $i \neq j$. Furthermore, upto rearrangement, the f_i, e_i and c are unique.*

Proof. First we reduce to the case where f is monic, by dividing by a nonzero element of F. If f is not irreducible, then $f = gh$, where $g, h \in F[x]$ are monic and $\deg g, h > 0$. Now we continue by induction.

The uniqueness of the decomposition is shown by using the following result. "Suppose that $a \in F[x]$ is irreducible, and that a divides bc, for certain $b, c \in F[x]$. Then a divides b, or a divides c." From this it follows that if $f = f_1^{e_1} \cdots f_r^{e_r} = g_1^{d_1} \cdots g_t^{d_t}$ are two decompositions of f into a product of irreducibles, then f_1 must be equal to one of the g_i. We cancel these factors, and finish the proof by induction. □

Now we turn our attention to the main topic of this section: finding the factorization promised by Theorem 6, when $F = \mathbb{F}_q$ is a finite field, and $q = p^n$ for some prime p, $n \geq 1$. Let $f \in \mathbb{F}_q[x]$ be a monic polynomial, and write $f = f_1^{e_1} \cdots f_r^{e_r}$, where the f_i are irreducible, monic, and $f_i \neq f_j$ for $i \neq j$. The factors $f_i^{e_i}$ are called the *primary factors* of f. We first describe an algorithm to find those. It is based on the following result.

Lemma 7 *Let $f \in \mathbb{F}_q[x]$, and let $v \in \mathbb{F}_q[x]$ be such that $v^q \equiv v \bmod f$. Then*

$$f = \prod_{a \in \mathbb{F}_q} \gcd(f, v - a).$$

Proof. Note that $Y^q - Y = \prod_{a \in \mathbb{F}_q}(Y - a)$. So by specializing Y to v we have $v^q - v = \prod_{a \in \mathbb{F}_q}(v - a)$. Now f divides $v^q - v$, so that $\gcd(f, v^q - v) = f$. Therefore,

$$f = \gcd(f, \prod_{a \in \mathbb{F}_q}(v - a)) = \prod_{a \in \mathbb{F}_q} \gcd(f, v - a).$$

Where the last equality follows from the following fact: "If a, b, c are polynomials with $\gcd(b, c) = 1$, then $\gcd(a, bc) = \gcd(a, b)\gcd(a, c)$." (Which can be proved using Theorem 6.) Note that $\gcd(v - a, v - b) = 1$ if $a \neq b$. □

By this lemma we may be able to find factors of f using the algorithm to compute gcd's, provided we have solutions v of $v^q \equiv v \bmod f$. The next lemma helps with finding such solutions.

Lemma 8 *Let $f \in \mathbb{F}_q[x]$, and let $f = f_1^{e_1} \cdots f_r^{e_r}$ be its decomposition into primary factors. Let V be the set of all $v \in \mathbb{F}_q[x]$ such that $v^q \equiv v \bmod f$. Then V is an r-dimensional vector space over $\mathbb{F}_q$.*

Proof. For $\alpha \in \mathbb{F}_q$, and $v, w \in V$ we have $(\alpha v)^q = \alpha^q v^q = \alpha v \bmod f$, and $(v+w)^q = v^q + w^q = v + w \bmod f$. So we see that αv and $v + w$ both belong to V. Therefore V is a vector space over $\mathbb{F}_q$. By the Chinese Remainder Theorem we have an isomorphism of rings

$$\varphi : \mathbb{F}_q[x]/(f) \to \bigoplus_{i=1}^{r} \mathbb{F}_q[x]/(f_i^{e_i}).$$

For $v \in V$ we write $\varphi(v) = (v_1, \ldots, v_r)$. Now $v^q \equiv v \bmod f$ is equivalent to $v_i^q \equiv v_i \bmod f_i^{e_i}$ for $1 \leq i \leq r$. So Lemma 7 implies that $f_i^{e_i} = \prod_{a \in \mathbb{F}_q} \gcd(f_i^{e_i}, v_i - a)$. But f_i is irreducible, and the $v_i - a$ are pairwise relatively prime. Therefore there is exactly one $a \in \mathbb{F}_q$ such that $\gcd(f_i^{e_i}, v_i - a) \neq 1$. This means that $f_i^{e_i} = v_i - a$, and $v_i \equiv a \bmod f_i^{e_i}$. We conclude that $\varphi(V) \subset \oplus_{i=1}^{r} \mathbb{F}_q$. Since $a^q = a$ for all $a \in \mathbb{F}_q$ we also get the other inclusion. Hence $\varphi(V) = \oplus_{i=1}^{r} \mathbb{F}_q$. □

On the basis of the previous two lemmas we formulate the following algorithm, which is called *Berlekamp's algorithm*.

Algorithm Berlekamp
Input: a monic polynomial $f \in \mathbb{F}_q[x]$.
Output: the primary factors of f.

Step 1 Compute a basis $\{v_1 = 1, v_2, \ldots, v_r\}$ of the vector space V, consisting of all $v \in \mathbb{F}_q[x]$ such that $v^q \equiv v \bmod f$.

Step 2 Set $P = \{f\}$ and for $2 \leq j \leq r$ do the following:

Step 2a Replace each $h \in P$ by the nontrivial elements of the set $\{\gcd(h, v_j - a) \mid a \in \mathbb{F}_q\}$.

Step 3 Return P.

Proposition 9 *The algorithm* Berlekamp *returns the set of primary factors of f.*

Proof. We note that throughout the algorithm f is equal to the product of all elements of P; this follows immediately from Lemma 7. Also the elements of P are pairwise relatively prime, as $v_j - a$ and $v_j - b$ are relatively prime for $a \neq b$. So the only thing that can be wrong with the output is that it contains an element which is divided by at least two primary factors.

Let h be an element of the set returned by the algorithm. Then for each j with $1 \leq j \leq r$ there is an $a_j \in \mathbb{F}_q$ such that $v_j \equiv a_j \bmod h$. (For a fixed j, this is certainly true after the execution of Step 2a where j is treated. Furthermore, it remains true, as in subsequent steps a polynomial is replaced by factors of it.) Let $v \in V$, then there are $\beta_j \in \mathbb{F}_q$ such that $v = \sum_{j=1}^{r} \beta_j v_j$. Hence if we set $a_v = \sum_{j=1}^{r} \beta_j a_j$ we have that $v \equiv a_v \bmod h$. Now suppose that h contains two primary factors of f, say $f_1^{e_1}$ and $f_2^{e_2}$. Then for $v \in V$ we have $\varphi(v) = (a_v, a_v, \ldots)$, where φ is as in the proof of Lemma 8. But this means that $\varphi(V) \neq \oplus_{i=1}^{r} \mathbb{F}_q$, which contradicts the last statement in the proof of Lemma 8. □

The remaining problem is to find the factorization of a primary factor. Suppose that $f = g^e$, and let $f' = eg'g^{e-1}$ be the derivative of f. Then there are two cases to be considered. Firstly, supppose that $f' = 0$. Then p divides e, or $g' = 0$. In the first case we have that f is a polynomial in x^p, i.e., $f = h(x^p) = h(x)^p$. If $g' = 0$ then g is a polynomial in x^p, but then the same holds for f. It follows that $f = h(x)^p$. We compute h, and find its factorization, from which the factorization of f is easily derived.

The second case occurs when $f' \neq 0$. But then $g = f/\gcd(f, f')$, so it is straightforward to find g.

Example 10 Consider the polynomial $f = x^7 + x^4 + x^2 + x + 1$ in $\mathbb{F}_2[x]$. Set $v = a_0 + a_1x + a_2x^2 + \cdots + a_6x^6$. Then $v^2 \bmod f = a_0 + a_5 + a_6 + (a_4 + a_5 + a_6)x + (a_1 + a_4 + a_5)x^2 + (a_4 + a_5 + a_6)x^3 + a_2x^4 + (a_4 + a_5 + a_6)x^5 + a_3x^6$. Now the requirement $v^2 \equiv v \bmod f$ leads to a set of linear equations for the a_i. After some rewriting we see that they amount to $a_1 = a_2 = a_3 = a_4 = a_5 = a_6$. So a basis of V is formed by the elements $v_1 = 1$ and $v_2 = x^6 + x^5 + x^4 + x^3 + x^2 + x$.

Now in Step 2a we replace f by the two polynomials $\gcd(f, v_2)$ and $\gcd(f, v_2 + 1)$. We have that $\gcd(f, v_2) = x^4+x^2+1$, and $\gcd(f, v_2+1) = x^3+x+1$. It follows that these are the primary factors of f. Now we look at these factors. The derivative of $g_1 = x^4+x^2+1$ is zero, which means that $g_1 = h(x^2) = h(x)^2$, with in this case $h = x^2+x+1$. Now $\gcd(h, h') = 1$ so that h is irreducible. It follows that $g_1 = (x^2 + x + 1)^2$. Setting $g_2 = x^3 + x + 1$, we have $g_2' = x^2 + 1$, and $\gcd(g_2, g_2') = 1$, so that also g_2 is irreducible. It follows that $f = (x^2 + x + 1)^2(x^3 + x + 1)$ is the factorization of f.