Linnæus University
School of Computer Science, Physics and Mathematics

Degree Project

Factorization Algorithms for Polynomials over Finite Fields

Sajid Hanif, Muhammad Imran
2011-05-03
Subject: Mathematics
Level: Master
Course code: 4MA11E

Abstract

Integer factorization is a difficult task. Some cryptosystem such as RSA (which stands for Rivest, Shamir and Adleman) are in fact designed around the difficulty of integer factorization.
For factorization of polynomials in a given finite field $\mathbb{F}_p$ we can use Berlekamp's and Zassenhaus algorithms. In this project we will see how Berlekamp's and Zassenhaus algorithms work for factorization of polynomials in a finite field $\mathbb{F}_p$. This project is aimed toward those with interests in computational algebra, finite fields, and linear algebra.

Contents

1 Introduction

Any non constant polynomial over a field can be expressed as a product of irreducible polynomials. In finite fields, some algorithms work for the calculation of irreducible factors of a polynomial of positive degree. The factorization of polynomials over finite fields has great importance in coding theory. In this project we will present two algorithms which work for factorization of polynomials over finite field. We will use Berlekamp's algorithm for a small finite field and Zassenhaus algorithm for a large finite field.

2 Field

Definition 2.1. A **field** $(\mathbb{F}, +, \cdot)$ is a set $\mathbb{F}$, together with two binary operations, denoted by $+$ and $\cdot$ such that:

1. $\mathbb{F}$ is an abelian group with respect to both $(+)$ and $(\cdot)$

2. The distributive laws hold. That is, for all a,b,c $\in \mathbb{F}$, we have,

$$a.(b+c) = a.b + a.c \quad \text{and} \quad (b+c).a = b.a + c.a$$

Definition 2.2. A field $\mathbb{F}$ is said to be a **finite field** if number of elements of field $\mathbb{F}$ are finite. A finite field can also be defined as:
For a prime p, let $\mathbb{F}_p$ be the set $\{1, 2, ..., p-1\}$ of integers and let
$\phi : \mathbb{Z}/(p) \to \mathbb{F}_p$ be the mapping defined by $\phi([a]) = a$ for $a = 0, 1, 2, ..., p-1$.
Where $\mathbb{Z}/(p)$ is residue class ring and [a] denotes the residue class of integer a, and ϕ is isomorphism. Then $\mathbb{F}_p$, endowed with the field structure induced by ϕ, is a finite field, called the **Galois field** of order p.

Example 2.1. An even simpler and most important example is the finite field F_2. It has two elements 0 and 1 and operation table has the following form:

+	0	1
0	0	1
1	1	0

and

.	0	1
0	0	0
1	0	1

The elements 0 and 1 are called binary elements.

Definition 2.3. Let $\mathbb{F}$ be a field. Any expression of the form

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$$

is called a **polynomial** over the field $\mathbb{F}$. Where $a_n, a_{n-1}, ..., a_1, a_0 \in \mathbb{F}$ and n is a non negative integer.

If n is a largest non negative integer $a_n \neq 0$, then we say that the polynomial $f(x) = a_n x^n + + ... + a_0$ has the **degree** n, written as $\deg(f) = n$. The coefficient a_n is called the **leading coefficient** of f(x).

If a_0 is the leading coefficient, the f is called a **constant polynomial**. If the leading coefficient is 1, then f is said to be a **monic polynomial**.

Note that the set of all polynomials with coefficients in $\mathbb{F}$ is denoted by $\mathbb{F}[x]$.

Definition 2.4. A non constant polynomial p $\in \mathbb{F}[x]$ is said to be **irreducible over the field** $\mathbb{F}[x]$ if p has positive degree and p = bc with b,c $\in \mathbb{F}[x]$ implies that either b or c is a constant polynomial.

For example, the polynomial p $= x^2 - 2 \in \mathbb{Q}[x]$ is irreducible over the field $\mathbb{Q}[x]$ and reducible over the field of real numbers $\mathbb{R}[x]$.
Note that,

1. All polynomials of degree 1 are irreducible.
2. A polynomial of degree 2 or 3 is irreducible over the field $\mathbb{F}$ if and only if it has no roots in $\mathbb{F}$.

Theorem 2.1. Given a field $\mathbb{F}$, non zero polynomials $f_1, f_2, ..., f_k \in \mathbb{F}[x]$ that are pairwise relatively prime, and arbitrary polynomials $g_1, g_2, ..., g_k \in \mathbb{F}[x]$, then the simultaneous congruences

$$\begin{aligned} h &\equiv g_1 \mod f_1 \\ h &\equiv g_2 \mod f_2 \\ &\vdots \\ h &\equiv g_r \mod f_r \end{aligned}$$

has a unique solution modulo $f = f_1 f_2 ..... f_r$.

Proof. We have $f_i(x)$ is relatively prime to $f_j(x)$ for $i \neq j$. The polynomial $f_k(x)$ is relatively prime to

$$l_k(x) = \frac{f(x)}{f_k(x)} = f_1(x).f_2(x)....f_{k-1}(x).f_{k+1}(x)....f_r(x).$$

$(l_k(x).f_k(x)) = 1$, because $(f_j(x).f_k(x)) = 1$ when $j \neq k$. Hence we can find the inverse $m_k(x)$ of $l_k(x) \mod f_k(x)$, so that

$$l_k(x)m_k(x) \equiv 1 \mod f_k(x).$$

$$l_k(x)m_k(x) \equiv 0 \mod f_j(x).$$

Let

$$h(x) \equiv g_1l_1m_1 + g_2l_2m_2 + ... + g_rl_rm_r \mod f(x).$$

The polynomial $h(x)$ is the simultaneous solution of the r congruences.
To demonstrate this, we must show that $h(x) \equiv g_k(x) \mod f_k(x)$, where $k = 1, 2, ..., r$.
Since $f_k(x)$ divides $l_j(x)$, whenever $j \neq k$, we have

$$l_j(x) \equiv 0 \mod f_k(x).$$

Therefore in the sum for $h(x)$, all the terms except the kth term are congruent to $0 \mod f_k(x)$. Hence

$$h(x) \equiv g_k(x)l_k(x)m_k(x) \equiv g_k(x) \mod f_k(x).$$

because $l_k(x).m_k(x) \equiv 1 \mod f_k(x)$.
Now, we show that any two solutions are congruent modulo f(x). For this, we let $h_1(x)$ and $h_2(x)$ both be simultaneous solutions to the system of r congruences. Therefore, for each k

$$h_1(x) \equiv h_2(x) \equiv g_k(x) \mod f_k(x).$$

So that,

$$f_k \mid (h_1(x) - h_2(x)).$$

Also,

$$f \mid (h_1(x) - h_2(x)).$$

Therefore $h_1(x) \equiv h_2(x) \mod f(x)$. This shows that the simultaneous solution of the system of r congruences is unique modulo $f(x)$. □

Example 2.2. The system of congruences

$$h \equiv 3 \mod (x - 1)$$

$$h \equiv 2 \mod (x - 2)$$

$$h \equiv -1 \mod (x - 3)$$

has unique solution modulo $f(x) = (x - 1)(x - 2)(x - 3)$.

Solution:
Here we have,

$$f_1(x) = x - 1,\ f_2(x) = x - 2,\ f_3(x) = x - 3$$

and

$$g_1 = 3,\ g_2 = 2,\ g_3 = -1$$

$f(x) = (x-1)(x-2)(x-3)$
Now we divide f(x) with $f_1(x), f_2(x)$ and $f_3(x)$.
we will get

$$l_1 = \tfrac{f(x)}{f_1(x)} = (x-2)(x-3) = x^2 - 5x + 6$$

$$l_2 = \tfrac{f(x)}{f_2(x)} = (x-1)(x-3) = x^2 - 4x + 3$$

$$l_3 = \tfrac{f(x)}{f_3(x)} = (x-1)(x-2) = x^2 - 3x + 2$$

To find the inverse m_1 of l_1, m_2 of l_2 and m_3 of l_3, we solve

$$(x^2 - 5x + 6)m_1 \equiv 1 \mod (x-1).$$

$$(x^2 - 4x + 3)m_2 \equiv 1 \mod (x-2).$$

$$(x^2 - 3x + 2)m_3 \equiv 1 \mod (x-3).$$

So that, we get

$$m_1 = \frac{1}{2},\ m_2 = -1,\ m_3 = \frac{1}{2}$$

Hence,

$$\begin{aligned} h &\equiv g_1 l_1 m_1 + g_2 l_2 m_2 + g_3 l_3 m_3 \mod f(x). \\ &\equiv (\frac{1}{2})(x-2)(x-3)(3) + (-1)(x-1)(x-3)(2) + (\frac{1}{2})(x-1)(x-2)(-1) \mod f(x). \\ &\equiv -x^2 + 2x + 2 \mod f(x). \end{aligned}$$

Theorem 2.2. Any polynomial $f \in \mathbb{F}[x]$ of positive degree can be written in the form

$$f = a.p_1^{e_1}.p_2^{e_2} \dots p_k^{e_k}$$

Where, $a \in \mathbb{F}$, $p_1, p_2, \dots p_k$ are distinct monic irreducible polynomials in $\mathbb{F}[x]$ and $e_1, e_2, \dots, e_k$ are positive integers. Moreover, this factorization is unique apart from the order in which the factors occur.

Proof. Let $f(x) \in \mathbb{F}[x]$ be a non constant polynomial. If $f(x)$ is reducible then at least

$$f(x) = a \cdot g(x) \cdot h(x)$$

Where $a \in \mathbb{F}$ and,

$$\deg(g(x)) < \deg(f(x))$$

$$\deg(h(x)) < \deg(f(x))$$

Further, If $g(x)$ and $h(x)$ are irreducible, then we stop here. If not, then at least one of them is reducible into lower degree polynomials. Continuing this process, we get

$$f(x) = a \cdot p_1(x) \cdot p_2(x) \dots p_r(x)$$

Where, $p_i(x)$ are irreducible polynomials in $\mathbb{F}[x]$ and $i = 1, 2, ..., r$.
To show the uniqueness,let

$$f(x) = a_1 \cdot p_1(x) \dots p_r(x) = a_2 \cdot q_1(x) \dots q_s(x) \tag{2.1}$$

be the two factorizations of f(x) into irreducible polynomials. Then by the theorem, $p(x)$ is an irreducible polynomial in $\mathbb{F}[x]$. If $p(x)$ divides $r(x) \cdot s(x)$ for $r(x), s(x) \in \mathbb{F}[x]$, then $p(x)$ divides either $r(x)$ or $s(x)$.
So $p_i(x)$ divides some $q_j(x)$.
Let we assume that $q_1(x)$ divides $p_1(x)$, then

$$q_1(x) = u_1.p_1(x) \text{ since } q_1(x) \text{ is irreducible}$$

By putting this value of $q_1(x)$ in (2.1), we will get

$$u_1.p_1(x).q_2(x).....q_s(x) = p_1(x).p_2(x).....p_r(x) \tag{2.2}$$

$$\Rightarrow \quad u_1.q_2(x).....q_s(x) = p_2(x).....p_r(x) \tag{2.3}$$

Now, by putting $q_2(x) = u_2.p_2(x)$ in the equation (2.3), we will get

$$u_1.u_2.q_3(x).....q_s(x) = p_3(x).....p_r(x) \tag{2.4}$$

Continuing this process and we get

$$1 = u_1.u_2.....u_r.q_{r+1}(x).....q_s(x) \tag{2.5}$$

This is only possible if $r = s$, so that the equation (2.5) has actually the form

$$1 = u_1.u_2.....u_r.$$

Therefore, irreducible factors $p_i(x)$ and $q_i(x)$ were the same. Hence the theorem. □

3 Factoring Over Small Finite Fields

Lemma 3.1. If $\mathbb{F}$ is a finite field with q elements,then every $a \in \mathbb{F}$ satisfies $a^q = a$.

Lemma 3.2. If $\mathbb{F}$ is a finite field with q elements and $\mathbb{K}$ is a sub field of $\mathbb{F}$, then the polynomial $x^q = x$ in $\mathbb{K}[x]$ factors in $\mathbb{F}[x]$ as

$$x^q - x = \prod_{a \in \mathbb{F}_q} (x - a).$$

and $\mathbb{F}$ is a splitting field of $x^q - x$ over $\mathbb{K}$.

Theorem 3.3. Let $\mathbb{F}_q$ be a field. If $f \in \mathbb{F}_q[x]$ is a monic polynomial and $h \in \mathbb{F}_q[x]$ is such that $h^q \equiv h \mod f$,then

$$f(x) = \prod_{c \in \mathbb{F}_q} \gcd(f(x), h(x) - c)). \tag{3.1}$$

Proof. From the above equation (3.1) we can see that each greatest common divisor on the right side divides $f(x)$. For $c \in \mathbb{F}_q$ and $h(x) \in \mathbb{F}_q[x]$, $h(x) - c$ are pairwise relatively prime polynomials.
i.e $h_2(x) = h_1(x) + c_1 - c_2$, where $c_1, c_2 \in \mathbb{F}_q$, $c_1 \neq c_2$.
So are the greatest common divisors with $f(x)$, and thus product of all these greatest common divisors divides $f(x)$. Since $h^q \equiv h \mod f$
$\Rightarrow f(x)$ divides $h(x)^q - h(x)$ and from (Lemma 3.2) we have

$$h(x)^q - h(x) = \prod_{c \in F_q} (h(x) - c). \tag{3.2}$$

Which shows that f(x) divides the right-hand side of (3.1).Thus both sides of equation (3.1) are monic polynomials which divides each other. Therefore must be equal. Hence the theorem. □

Particulars

1. Note that it is feasible to use (theorem 3.3) to obtain a factorization of polynomial $f(x)$ over a small finite field $\mathbb{F}_q$ since it requires the calculation of q gcd's.

2. In general (theorem 3.3) does not give a complete factorization of $f(x)$ since the $\gcd(f, h - c)$'s might be reducible.

Definition 3.1. If $h \in \mathbb{F}_q[x]$ be such that (theorem 3.3) yields a non trivial factorization of $f(x)$ is called **f-reducing** polynomials.

If $h \equiv c \mod f$ for some $c \in \mathbb{F}_q$, then (theorem 3.3) gives trivial factorization of f. And for any h with $h^q \equiv h \mod f$, when $0 < \deg h < \deg f$, is obviously f-reducing polynomial. Now we use Berlekamp's algorithm to find these f-reducing polynomials.

4 Berlekamp's Algorithm

Let us assume that f has no repeated factors, so that $f = f_1.f_2.....f_k$ are the distinct monic irreducible polynomials over $\mathbb{F}_q$. If $(c_1.c_2.....c_k)$ is any k-tuple of elements of $\mathbb{F}_q$.then by (theorem 2.1) there is a unique $h \in \mathbb{F}_q[x]$ with $h(x) \equiv c_i \mod f_i(x)$ for $1 \leqslant i \leq k$ and $\deg(h) < \deg(f)$.

The polynomial $h(x)$ satisfies the condition

$$h(x)^q \equiv c_i^q = c_i \equiv h(x) \mod f_i(x) \text{ for } 1 \leqslant i \leq k,$$

and therefore

$$h(x)^q \equiv h(x) \mod f(x), \ \deg(h) < \deg(f). \tag{4.1}$$

Also if h is is a solution of (4.1) then (3.2) implies that every irreducible factor of f divides one of the polynomials $h(x) - c$.
Thus, all solutions of (4.1) satisfy $h(x) \equiv c_i \mod f_i(x), 1 \leqslant i \leq k,$ for k-tuple $(c_1.c_2.....c_k)$ of elements of $\mathbb{F}_q$.

Consequently, we have exactly q^k solutions of (4.1). We find these solutions by reducing (4.1) to a system of linear equations. Let $\deg(f) = n$ then we construct n×n matrix $B = (b_{ij}), 0 \leq i, j \leq n-1$, by calculating the powers of $x^{iq} \mod f(x)$.

$$x^{iq} \equiv \sum_{j=0}^{n-1} b_{ij} x^j \mod f(x) \text{ for } 0 \leq i \leq n-1. \tag{4.2}$$

where $b_{ij} \in \mathbb{F}_q$. $h(x) = a_0 + a_1 x + ... + a_{n-1}x^{n-1} \in F_q[x]$ satisfies (4.1) if and only if

$$(a_0, ..., a_{n-1})B = (a_0, ..., a_{n-1}). \tag{4.3}$$

where $B = (b_{ij})$ and $0 \leq i, j \leq n-1$ (4.3) holds if and only if

$$\begin{aligned} h(x) &= \sum_{j=0}^{n-1} a_j x^j = \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} a_i b_{ij} x^j. \\ &\equiv \sum_{i=0}^{n-1} a_i x^{iq} \equiv h^q \mod f(x). \end{aligned}$$

The system (4.3) can be written as

$$(a_0, ..., a_{n-1})(B - I) = (0, 0, \ldots, 0), \tag{4.4}$$

By the considerations above system (4.4) has exact q^k solutions. Therefore dimensions of $B - I$ is k, the number of distinct monic irreducible factors of f. And rank of $B - I$ is $n - k$. Since the polynomial $h_1(x) = 1$ is trivial solution of (4.1), so the vector (1,0,...,0,) is solution of (4.4). There will exist the polynomials $h_2(x), \ldots h_k(x)$ with degree $\leq n-1$ such that the corresponding vectors to $h_2(x), \ldots h_k(x)$ form the basis of null space of $B - I$. So the polynomials $h_2(x), \ldots h_k(x)$ are f-reducing. Now once the rank r is found, we know the number of irreducible polynomials by $k = n - r$.
If $k = 1$ then $f(x)$ is irreducible and we will terminate the procedure. Also for $k = 1$, the solutions of $h^q \equiv h \mod f$ are the constant polynomials and the null

space of $B-I$ will have the vectors $(c,0,0,....0)$ where $c \in \mathbb{F}_q$. If $k \geq 2$, we will get the polynomial $h_2(x)$ which is f-reducing. Then we find $\gcd(f(x), h_2(x)-c)$, for all $c \in \mathbb{F}_q$, the result will be a non trivial factorization of f(x) by (theorem 3.3). If we do not get k factors of f by using $h_2(x)$, we will find the $\gcd(g(x), h_3(x)-c)$, for all $c \in \mathbb{F}_q$, and the process will continue until we get k factors of $f(x)$.

Example 4.1. Factor $f(x) = x^4+x^2+x+1$ over F_2 by Berlekamp's algorithm.

Solution: To factor the polynomial $f(x)$ we will do following steps.

1. Note that, $f'(x) = 4x^3 + 2x + 1 = 1$.
   so, $\gcd(f(x), f'(x)) = 1$ and f(x) has no repeated factors.

2. We must compute the powers $x^{2i} \mod f(x)$ for $0 \leq i \leq 3$.This yields the following congruences:

$$\begin{aligned} x^0 &\equiv 1 \mod f. \\ x^2 &\equiv x^2 \mod f. \\ x^4 &\equiv 1+x+x^2 \mod f. \\ x^6 &\equiv 1+x+x^3 \mod f. \end{aligned}$$

3. So, the matrix B of order 4×4 is given as

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

   and the matrix B-I is

$$B - I = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

4. Now rank of $B-I$ is $r = 2$, therefore f(x) has $k = 4-2 = 2$ distinct monic irreducible factors.

5. Two vectors (1, 0, 0, 0) and (0, 0, 1, 1) form the basis of the null space of $B-I$.

6. The polynomials corresponding to the basis vectors are:

$$h_1(x) = 1 \quad \text{and} \quad h_2(x) = x^2 + x^3$$

7. Now, by using the (theorem 3.3) we calculate

$$\begin{aligned} &\gcd(f(x), h_2(x) - 0) = x + 1. \\ &\gcd(f(x), h_2(x) - 1) = x^3 + x^2 + 1. \end{aligned}$$

8. f has two distinct monic irreducible factors. Therefore, our desired factorization is
$$f(x) = (x+1)(x^3+x^2+1).$$

Example 4.2. Factor $f(x) = x^8+x^7+x^4+x^3+x+1$ over F_3 by Berlekamp's algorithm.

Solution: Since, $\gcd(f(x), f'(x)) = 1$, $f(x)$ has no repeated factors.
Now we will compute $x^{iq} \mod f(x)$ for $q = 3$ and $0 \leq i \leq 7$. We have the congruences

$$\begin{aligned}
x^0 &\equiv 1 \mod f.\\
x^3 &\equiv x^3 \mod f.\\
x^6 &\equiv x^6 \mod f.\\
x^9 &\equiv 1+2x^2+x^3+2x^5+x^7 \mod f.\\
x^{12} &\equiv x+x^4+2x^5 \mod f.\\
x^{15} &\equiv 1+x+x^3+2x^4+2x^7 \mod f.\\
x^{18} &\equiv 1+x^4+2x^6 \mod f.\\
x^{21} &\equiv 2+x^2+x^5 \mod f.
\end{aligned}$$

So, the matrix B of order 8×8 is given as

$$B = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\
1 & 0 & 2 & 1 & 0 & 2 & 0 & 1\\
0 & 1 & 0 & 0 & 1 & 2 & 0 & 0\\
1 & 1 & 0 & 1 & 2 & 0 & 0 & 2\\
1 & 0 & 0 & 0 & 1 & 0 & 2 & 0\\
2 & 0 & 1 & 0 & 0 & 1 & 0 & 0
\end{pmatrix}$$

and the matrix B-I is

$$B - I = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 2 & 0 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 2 & 0 & 0 & 0 & 1 & 0\\
1 & 0 & 2 & 0 & 0 & 2 & 0 & 1\\
0 & 1 & 0 & 0 & 0 & 2 & 0 & 0\\
1 & 1 & 0 & 1 & 2 & 2 & 0 & 2\\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 0\\
2 & 0 & 1 & 0 & 0 & 1 & 0 & 2
\end{pmatrix}$$

Since, the rank of $B-I$ is $r = 5$, therefore $f(x)$ has $k = 8-5 = 3$ distinct monic irreducible factors. The null space of the matrix $B-I$ is (1,0,0,0,0,0,0,0),

(0,0,0,1,0,0,0,1) and (0,2,2,1,1,1,1,0). And the polynomials corresponding to these basis vectors are

$$h_1(x) = 1.$$
$$h_2(x) = x^3 + x^7.$$
$$h_3(x) = 2x + 2x^2 + x^3 + x^4 + x^5 + x^6.$$

First, we take $h_2(x)$ and we find that

$$\gcd(f(x), h_2(x) - 0) = 1.$$
$$\gcd(f(x), h_2(x) - 1) = 1 + x.$$
$$\gcd(f(x), h_2(x) - 2) = 1 + x^3 + x^7.$$

Since $f(x)$ has three distinct monic irreducible factors but we have

$$f(x) = (1 + x)(1 + x^3 + x^7).$$

To obtain f-reducing polynomial, we take the polynomial $1 + x^3 + x^7$ and by repeating the same procedure as above, we will get

$$1 + x^3 + x^7 = (2 + 2x + 2x^2 + x^3 + x^4 + x^5 + x^6)(2 + x).$$

So that

$$f(x) = (1 + x)(2 + 2x + 2x^2 + x^3 + x^4 + x^5 + x^6)(2 + x).$$

Now for $2 + 2x + 2x^2 + x^3 + x^4 + x^5 + x^6$ we see that $k = 1$, so it is irreducible and we terminate here.
Secondly, for $h_3(x)$ we will have

$$\gcd(f(x), h_3(x) - 0) = 1 + x.$$
$$\gcd(f(x), h_3(x) - 1) = 2 + 2x + 2x^2 + x^3 + x^4 + x^5 + x^6.$$
$$\gcd(f(x), h_3(x) - 2) = 2 + x.$$

then f has the factorization as

$$f(x) = (1 + x)(2 + 2x + 2x^2 + x^3 + x^4 + x^5 + x^6)(2 + x).$$

5 Factoring Over Large Finite Fields

A finite field, $\mathbb{F}_q$ is considered large if q is substantially bigger than the degree of the polynomial to be factored. In that case, the factorization of the given polynomial by the method in the previous section become more difficult. However, we may still be able to find an f-reducing polynomial with a reasonable effort but a direct application of the basic formula (3.1) become difficult because it requires the calculation of q greatest common divisors.

Let f be a monic polynomial in $\mathbb{F}[x]$ with no repeated factors. We can find an f-reducing polynomial $h(x)$ by the use of Berlekamp's algorithm. Since the various greatest common divisors in (3.1) are pairwise relatively prime, it is clear that at most k of these greatest common divisors will be $\neq 1$. We will then use the Zassenhaus algorithm to characterize the elements $c \in \mathbb{F}_q$ for which $\gcd(f(x), h(x) - c) \neq 1$.

5.1 Zassenhaus Algorithm

To characterize the elements $c \in \mathbb{F}_q$ for which the greatest common divisors in (3.1) need to be calculated is based on the following considerations
Let $C = \{c \in \mathbb{F}_q : \gcd(f(x), h(x) - 1) \neq 1\}$, (3.1) implies

$$f(x) = \prod_{c \in C} \gcd(f(x), h(x) - c)). \tag{5.1}$$

and so $f(x)$ divides $\prod_{c \in C}(h(x) - c)$.
Also consider the polynomial $G(y) = \prod_{c \in \mathbb{F}_q}(y - c)$, then $f(x)$ divides $G(h(x))$. To characterize the polynomial $G(y)$, we take a look at the following theorems.

Theorem 5.1. $\mathbb{F}[x]$ is principal ideal domain. In fact, for every ideal $J \neq (0)$ of $\mathbb{F}[x]$ there exist a uniquely determined monic polynomial $g \in \mathbb{F}[x]$ with $J = (g)$

Theorem 5.2. Among all the polynomials $g \in \mathbb{F}_q[y]$ such that $f(x)$ divides $g(h(x))$, the polynomial $G(y)$ is the unique monic polynomial of least degree.

Proof. We have already shown above that the monic polynomial $G(y)$ is such that $f(x)$ divides $G(h(x))$. It is easily seen that the polynomials $g \in \mathbb{F}_q[y]$ with $f(x)$ dividing $g(h(x))$ form a non zero ideal of $\mathbb{F}_q[y]$. By (theorem 5.1) $F_q[y]$ is a principal ideal domain, so this ideal is generated by a uniquely determined monic $G_o \in \mathbb{F}_q[y]$. It follows that $G_o(y)$ divides $G(y)$ and so

$$G_o(y) = \prod_{c \in C_1} (y - c).$$

where $C_1 \subseteq C$. Furthermore, $f(x)$ divides
$G_o(h(x)) = \prod_{c \in C_1} (h(x) - c)$, so

$$f(x) = \prod_{c \in C_1} \gcd(f(x), h(x) - c)).$$

A comparison with (5.1) shows that $C = C_1$, so $G_o(y) = G(y)$, and hence the theorem. □

This result is applied in following method. Let m be the number of elements of the set C. then

$$G(y) = \prod_{c \in C} (y - c) = \sum_{j=0}^{m} b_j y^j \in F_q[y].$$

where $b_m = 1$. Since $f(x)$ divides $G(h(x))$, so that $\sum_{j=0}^{m} b_j y^j \equiv 0 \mod f$.
Since $b_m = 1$, this may be given a non trivial linearly dependent relation over $\mathbb{F}_q$ of residues $1, h(x), h(x)^2, \ldots, h(x)^m \mod f(x)$. (theorem 5.2) says with the normalization $b_m = 1$ this linearly dependent relation is unique and residue classes $1, h(x), h(x)^2, \ldots, h(x)^m \mod f(x)$ are linearly independent.
We can find the polynomial G by calculating the residues
$\mod f(x)$ of $1, h(x), h(x)^2, \ldots,$ until we find the smallest powers of $h(x)$ that is linearly dependent over $\mathbb{F}_q$ on its predecessors. The scalars in this linear dependence relation are the coefficients of G. The elements of the set C are the roots of the polynomial G. This method of reducing the problem of finding the elements of C to that of calculating the roots of a polynomial in $\mathbb{F}_q$ is called the Zassenhaus algorithm.

Example 5.1. Factor $f = x^5 + 4x^2 + 3x + 1$ over $\mathbb{F}_{17}$.

Solution: Using Berlekamp's algorithm, we can determine that $k = 3$ and find an f-reducing polynomial $h = x^3 - 8x^2 - 5x$. We now compute the powers of $h \mod f$ until we find a non trivial linear dependence.

$$h^2 \equiv 3x^4 + 8x^3 + x^2 - 4x - 1 \mod f.$$
$$h^3 \equiv 4x^4 - 4x^3 - 6x^2 + 10 \mod f.$$

So linearly dependent relation is $h^3 = 7h^2 + 8h$. Thus $G = y^3 - 7y^2 - 8y$. Now by using Remainder theorem we can see that
$G(0) = 0^3 - 7 \cdot 0^2 - 8 \cdot 0 = 0 \mod 17$.
$G(8) = 8^3 - 7 \cdot 8^2 - 8 \cdot 8 = 0 \mod 17$.
$G(16) = 16^3 - 7 \cdot 16^2 - 8 \cdot 16 = 0 \mod 17$.
Therefore roots of G are 0,8 and 16, so we only need to compute

$$\gcd(f, h - 0) = x + 11.$$
$$\gcd(f, h - 8) = x + 14.$$
$$\gcd(f, h - 16) = x^3 + 9x^2 + 12x + 1.$$

So we get
$f = (x + 11)(x + 14)(x^3 + 9x^2 + 12x + 1)$.
where $x + 11, x + 14$ are monic and so irreducible, also on checking further $x^3 + 9x^2 + 12x + 1$ is irreducible
Hence
$f = (x + 11)(x + 14)(x^3 + 9x^2 + 12x + 1)$. is factorization of f.

6 Mathematica code

6.1 Berlekamp

```
   Implementation of Berlekemp algorithm for
 factorizing polynomials modulo a prime field p.
Sajid Hanif, Muhammad Imran, Marcus Nilsson 2011.

f[x] = x^8+x^6+x^4+x^3+1;
p = 2;
deg = Exponent[f[x], x];

First we check that the polynomial has no
repeated factors.

PolynomialGCD[f[x], D[f[x], x], Modulus -> p]
1

Now we have to compute x^iq mod f(x)
for q (field) and 0<=i<=n-1, where n is degree
of polynomial and we will get coefficient matrix
B from our computation of x^iq. And then we
have to find B-I.
where I is identity matrix of order n*n.

B = {};
Do[pol = CoefficientList[PolynomialMod[x^(p i),
f[x], Modulus -> p], x];
pol = PadRight[pol, deg]; AppendTo[B, pol],
{i, 0, deg - 1}];
b = Transpose[Mod[B - IdentityMatrix[deg], p]];
b // MatrixForm

It will give us B-I marix.
Now we will find the rank of matrix B-I.

MatrixRank[b, Modulus -> p]
6

Since rank r and degree n, so k=n-r. Therefore
we will get  factors.of polynomial f(x).
Now we will find bases of null space of matrix
B-I and our h (x) f-reducing polynomial. At the
end we will compute gcd (f(x),h(x)-c)
where c belongs to F(x) .
```

```
nullbase = Mod[NullSpace[b, Modulus -> p], p];
pollist =
Table[FromDigits[Reverse[nullbase[[i]]], x], {i, 1,
Length[nullbase]}];
maybefactors =
Table[PolynomialGCD[f[x], pollist[[i]] - j,
 Modulus -> p], {i, 1,
Length[pollist]}, {j, 0, p - 1}]

{{1 + x + x^4 + x^5 + x^6, 1 + x + x^2}, {1,
  1 + x^3 + x^4 + x^6 + x^8}}

This will give the required factorization of any given
polynomial.
Here f (x)=(1+x+x^4+x^5+x^6)(1+x+x^2). On checking
further on 1+x+x^4+x^5+x^6 and 1+x+x^2 we will see
f(x)=(1+x+x^4+x^5+x^6)(1+x+x^2) is the factorization
of f (x).
```

6.2 Zassenhaus

```
Implementation of Zassenhaus algorithm for
 factorizing polynomials modulo a prime p.
Sajid Hanif, Muhammad Imran, Marcus Nilsson  2011.

f[x] = x^6-3x^5+5x^4-9x^3-5x^2+6x+7;
p = 47;
deg = Exponent[f[x], x];

First we check that the polynomial has no
repeated factors.

PolynomialGCD[f[x], D[f[x], x], Modulus -> p]
1

Now we have to compute x^iq mod f(x)
for q (field) and 0<=i<=n-1, where n is degree
of polynomial and we will get coefficient matrix
B from our computation of x^iq. And then we
have to find B-I.
where I is identity matrix of order n*n.

B = {};
Do[pol = CoefficientList[PolynomialMod[x^(p i),
f[x], Modulus -> p], x];
```

```
pol = PadRight[pol, deg]; AppendTo[B, pol],
{i, 0, deg - 1}];
b = Transpose[Mod[B - IdentityMatrix[deg], p]];
b // MatrixForm

Now we have to check number of facotrs of f (x).
And then we will find bases of null space of matrix
B-I and h(x) f-reducing polynomial.

NumberOfFactors = MatrixRank[b, Modulus -> p];
nullbase = Mod[NullSpace[b, Modulus -> p], p];
onepoly = Prepend[Table[0, {deg - 1}], 1];
If[nullbase[[1]] == onepoly, i = 2, i = 1];
h[x] = Expand[FromDigits[Reverse[nullbase[[i]]],
 x]];zlist = {};
AppendTo[zlist, Reverse[PadRight[CoefficientList
[h[x],x], deg]]];nullsp = {}; i = 2;
While[Length[nullsp] == 0,

Now  after finding h(x) we will compute h(x)^i
until we get a linearly dependent relation between
all h(x)^i.

zpol = Reverse[
   PadRight[
   CoefficientList[PolynomialMod[h[x]^i, f[x],
   Modulus -> p], x],
      deg]];
  AppendTo[zlist, zpol];
  nullsp = NullSpace[Transpose[zlist],
   Modulus -> p]; i++];
base = NullSpace[Transpose[zlist], Modulus -> p];
 base =  Append[Reverse[base[[1]]], 0];

In linearly dependent relation just replace h(x)
by y, so will get a polynomial G(y).

factorization = 1;
Do[factorization =
   factorization*
    PolynomialGCD[f[x], h[x] - roots[[i]],
    Modulus -> p], {i, 1,
   Length[roots]}];
    factorization

(28+x)(31+4x+x^2)(11+42x+12x^2+x^3)
```

```
This will give our required factorization of
any given polynomial.
In above example we get
f(x)=(28+x)(31+4x+x^2)(11+42x+12x^2+x^3).
```

7 Bibiliography

References

[1] RUDOLF LIDL and HARALD NIEDERREITER. Introduction to finite fields and their applications. *Cambridge university press*,2000.

Linnæus University
School of Computer Science, Physics and Mathematics

SE-351 95 Växjö / SE-391 82 Kalmar
Tel +46-772-28 80 00
dfm@lnu.se
Lnu.se/dfm