Article 3: Berlekamp's Algorithm for Factoring Polynomials

Debadatta Kar

June 17, 2025

1 Introduction

Polynomial rings described over finite fields contain irreducible polynomials. These polynomials cannot be factored further into a product of smaller-degree polynomials. This means that any polynomial that we pick from a polynomial ring can have factors, irreducible factor, and we can have a representation of any given polynomial as the product of their factors as:

$$f(x) = f_1(x) \times f_2(x) \times \cdots \times f_k(x)$$

This intuition is good to consider if we can find an algorithm that can deterministically factor out a polynomial $f(x)$ into its irreducible factors. For this, we need to know if the factorization is unique, some results from fields, and some help from linear algebra about solving systems of linear equations. This is the idea of Berlekamp's algorithm, which is the main highlight of this article.

Result 1.1. *If F_q is a finite field, then any $f(x) \in F[x]$ can be expressed as a product of distinct monic irreducible polynomials raised to some powers as*

$$f(x) = f_1^{e_1}(x) \times f_2^{e_2}(x) \times \cdots \times f_k^{e_k}(x)$$

where $f_i(x) \in F[x]$ and $e_i \in \mathbb{Z}^+$ for $1 \leq i \leq k$
Moreover, this factorization is unique apart from the order in which the factors occur.

2 Mathematical Background for Factoring Polynomials

Some of the important theorems used for Brelekemp's algorithms are noted in the results of this article.

Result 2.1. *Let F_q be a field then for any $a \in F$ the relation $a^q = a$*

Result 2.2. *Let F_q be a field and K be a subfield of F_q then $x^q - x$ in $K[x]$ factors linearly in $F_q[x]$ as:*

$$x^q - x = \prod_{a \in F_q} (x - a)$$

F_q is called the splitting field of $x^q - x$ over K

Result 2.3. *The element $b \in F$ is a multiple root of $f \in F[x]$ iff a root of both f and f'.*

Theorem 2.4. *Let F_q be a field and $f \in F_q[x]$ be a monic polynomila and $h \in F_q[x]$ is such that $h^q(x) \equiv h(x) \mod f(x)$ then*

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

Theorem 2.5. *Let $f_1, f_2, \cdots f_k \in F[x] \setminus \{0\}$ be relatively prime polynomials and $g_1, g_2, \cdots, g_k \in F[x]$ be arbitrary then the simultaneous congruence*

$$h(x) \equiv g_1(x) \mod f_1(x) \tag{1}$$
$$h(x) \equiv g_2(x) \mod f_2(x) \tag{2}$$
$$\vdots$$
$$h(x) \equiv g_k(x) \mod f_k(x) \tag{3}$$

has unique solution modulo $f = f_1 \cdot f_2 \cdots f_k$

Proof. Since $f_1, f_2, \cdots, f_k$ are relatively prime then $\gcd(f_i, f_j) = 1 \ \forall i \neq j$.
Construct

$$l_r = \frac{f(x)}{f_r(x)} = f_1 \cdot f_2 \cdots f_{r-1} \cdot f_{r+1} \cdots f_k$$

Now,

$$\gcd(l_r(x), f_r(x)) = 1$$

Consider the inverse of l_r to be m_r.

$$l_r(x)m_r(x) \equiv \mod f_r(x)$$

$$l_r(x)m_r(x) \equiv 0 \mod f_j(x)$$

Construct the $h(x)$ as:

$$h(x) = g_1 l_1 m_1 + g_2 l_2 m_2 + \cdots g_k l_k m_k \mod f(x)$$

$h(x)$ is the solution of the congruence. Since $f_r | l_j 4$ we have $l_j(x) \equiv mod f_r(x)$ or also $g_j l_j m_j \equiv \mod f_r(x)$ when $j \neq k$
Finally,

$$h(x) \equiv g_r(x) l_r(x) m_r(x) \mod f_k(x)$$

Now, we go for the uniqueness part,
Let there be two solutions namely $h_1(x)$ and $h_2(x)$, the we would have the relations,

$$h_1(x) \equiv g_r(x) \mod f_r(x)$$

$$h_2(x) \equiv g_r(x) \mod f_r(x)$$

From above, we can deduce, $f_r(x) | h_1(x) - h_2(x)$ and,

$$f(x) | h_1(x) h_2(x)$$

Thus, $h_1(x) \equiv h_2(x) \mod f(x)$ □

3 Berlekemp's Algorithm

Assume that $f \in F_q[x]$ is the product of distinct monic irreducible polynomials, has no repeated roots

$$f = f_1 \times f_2 \times \cdots \times f_k$$

Let $(c_1, c_2, \ldots, c_k)$ be any k-tuple of F_q.
Now using Theorem 2.5 we can say that $\exists$ unique solution $h \in F_q[x]$ such that

$$h(x) \equiv c_1 \pmod{f_1(x)}$$
$$h(x) \equiv c_2 \pmod{f_2(x)}$$
$$\vdots$$
$$h(x) \equiv c_k \pmod{f_k(x)}$$

and,

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

Also,

$$h^q(x) \equiv c_i^q \equiv c_i \equiv h(x) \pmod{f_i(x)}$$

Thus,

$$h^q(x) \equiv c_i \pmod{f_i(x)} \quad f_i(x), \quad 1 \leq i \leq k \tag{4}$$

Since $h(x)$ is a solution to above equation so $h(x) - c_i | h^q(x) - h(x)$ for all $c_i \in F_q$

We have q^n solution to $h(x)^q = h(x) \mod f(x)$. We will find a solution by solving a system of linear equations.
Let $\deg(f) = n$, then construct,

$$B_{n\times n} = [b_{ij}], \quad 0 \leq i, j \leq n-1$$

by calculating the powers of $x^{iq} \mod f(x)$ Moreover,

$$x^{iq} = \sum_{j=0}^{n-1} b_{ij} x^j \mod f(x)$$

where $b_{ij} \in F_q$ and,
$h(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in F_q[x]$ satisfies (equation 4) iff

$$(a_0, \ldots, a_{n-1})B = (a_0, \ldots, a_{n-1})$$

The above equation can be written as

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

Above equation holds iff

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

The designed system has q^k solutions exactly.
Thus, the dimension of the matrix $B - I$ is k.
k = number of distinct monic irreducible factors of 'f'
case I
when $h(x) = 1$, this is the trivial solution as $1^q \equiv 1$
case II
$\exists\, h_2, h_3, \cdots, h_k$ with degree $\leq n-1$ such that the corresponding vectors to $h_2, h_3, \cdots, h_k$ forms basis of the null space of $B - I$.
So, polynomials are f-reducing once the rank r is found. We can then compute $k = n - r$
Then Compute $\gcd(f(x), h_2(x) - c)$ tahing all c from F_q.
The result will be a non-trivial factorization as,

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

If we do not get $k-$ factors of f using h_2, then we find $\gcd(f(x), h_3(x) - c)$ for all $c \in F_q$ and continue till we get all the $k-$factors.

Algorithm 1 Algorithm for Factoring Polynomials

1: Check if f has repeated roots or not.
2: Compute Berlekamp's Matrix
3: Solve Linear System of Equations
4: find $\gcd(f(x), h(x) - c)$ which is factor of $f(x)$

4 Conclusion

Berlekamp's algorithm efficiently factors polynomials over finite fields by converting the problem into a linear algebra task over the base field. The nullspace of a particular matrix determines all polynomials h satisfying $h^q \equiv h \pmod{f}$. Nontrivial elements from this nullspace can be used to find nontrivial factors of f.

References

[1] Elwyn R. Berlekamp, *Factoring Polynomials over Finite Fields*, Bell System Technical Journal, 1967.

[2] Lidl R, Niederreiter H, *Finite Fields*, 2nd ed. Cambridge University Press; 1996