AN ALGORITHM FOR FACTORING COMPOSITE POLYNOMIAL $P(x^p - x - \delta)$

Sergey Abrahamyan, Knarik Kyuregyan

Abstract: Let $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be an irreducible polynomial over $F_q$. In [Cao, 2012, Varshamov, 1973, Lidl, 1987] the factorization of the composite polynomial $P(x^p - ax - \delta)$, when $a = 1$ and $Tr_{F_q/F_p}(nb - a_n - 1) = 0$ is considered. The result of factorization of polynomial $P(x^p - x - \delta)$ is a $p$ irreducible polynomials of degree $n$ over $F_q$. In this paper we propose an algorithm for factoring composite polynomial $P(x^p - x - \delta)$ over $F_q$ and give a explicit view of each factor.

Keywords: finite field, polynomial factorization, polynomial composition

ACM Classification Keywords: I.1.2. Algorithms

Introduction

Construction of irreducible polynomials from given irreducible polynomial is a classic problem of finite field theory and computer algebra. One of methods to construct irreducible polynomials is the polynomial composition method. Such methods have been studied by several authors including Varshamov [Varshamov, 1984], Cohen [Cohen, 1992], Meyn [Meyn, 1990], Kyureghyan [Kyuregh, 2011].

Let $F_q$ be the Galois field of order $q = p^s$, where $p$ is a prime and $s$ is a natural number and $F_q^*$ be its multiplicative group. Let $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be an irreducible polynomial over $F_q$. Varshamov proved that for $a = 1$ the composite polynomial $P(x^p - ax - \delta)$ is irreducible over $F_q$ if and only if $Tr_{F_q/F_p}(n\delta - a_n - 1) \neq 0$. In [Lidl, 1987, Varshamov, 1973] the problem of factorization of the composite polynomial $P(x^p - x - \delta)$, when $Tr_{F_q/F_p}(n\delta - a_n - 1) = 0$ is considered. Also, in [Cao, 2012] a short proof of above-mentioned problem is given.

For constructing $p$ irreducible polynomials from the given irreducible polynomial we need compute the composition $P(x^p - x - \delta)$, and then factorize $P(x^p - x - \delta)$. In this paper we show how factors of polynomial $P(x^p - x - b)$ are connected each other. Also, we propose a probabilistic algorithm based on Cantor Zassenhaus's algorithm for finding one of factors of polynomial $P(x^p - x - \delta)$.

Factorization of composite polynomial $P(x^p - x - \delta)$

Recall that the trace function of $F_q^n$ over $F_q$ is

$$Tr_{q^n/q}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i}, \quad \alpha \in F_q^n.$$ 

Define $Tr_{q^n/q}^{(i)}(\alpha)$ the following way

$$Tr_{q^n/q}^{(i)}(\alpha) = \sum_{0 \leq j_1 < \cdots < j_i \leq n-1} \alpha^{q^{j_1} \cdot q^{j_2} \cdots q^{j_i}},$$

here $Tr_{q^n/q}^{(1)}(\alpha) = Tr_{q^n/q}(\alpha)$.

Let $f(x) = \sum_{i=0}^{n-1} g_i x^i$ be a minimal polynomial of $\alpha$. It is easy to see that
\[ g_i = (-1)^{n-i} TP_{q^n/q}^{(n-i)}(\alpha). \]  

In this section based on Proposition 1 (introduced below) we show how connected factors of polynomial \( P(x^p - x - \delta) \) over \( F_q \).

**Proposition 1.** (Theorem 2.1 [Cao, 2012]) Let \( g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \) be an irreducible polynomial over \( F_q = F_{p^n} \) of degree \( n \). Let \( \delta \in F_q \) and \( TP_{q^n/p}(n\delta - a_{n-1}) = 0 \). Then \( g(x^p - x - \delta) \) decomposes as a product of \( p \) irreducible polynomials over \( F_q \) of degree \( n \). Let \( g(x^p - x - \delta) = u_0(x)u_1(x) \cdots u_{p-1}(x) \). Then via a suitable assignment of the indexes of the factors, \( u_k(x) = u_0(x + k) \) for \( k = 0, 1, \cdots p - 1, \ldots \)

In our proof we will need the following proposition.

**Proposition 2.** (Theorem 2.25 [Lidl, 1987]) Let \( F \) be a finite extension of \( K \). Then for \( \alpha \in F \) we have \( Tr_{F/K}(\alpha) = 0 \) if and only if \( \alpha = \beta^q - \beta \) for some \( \beta \in F \).

**Theorem 1.** Let \( q = p^s \) where \( p \) is a prime. \( P(x) = \sum_{i=0}^{n} a_i x^i \) be an monic irreducible polynomial of degree \( n \) over \( F_q \) and \( TP_{q^n/p}(n\delta - a_{n-1}) = 0 \). Then the polynomial \( F(x) = P(x^p - x - \delta), \delta \in F_q \) factors to \( p \) irreducible polynomials of degree \( n \) over \( F_q \) as follows: \( F(x) = G_0(x)G_1(x) \cdots G_{p-1}(x) \), where

\[
G_0(x) = x^n + g_{n-1}x^{n-1} + \cdots + g_1x + g_0, \\
G_k(x) = x^n + g_{n-1}^{(k)}x^{n-1} + \cdots + g_1^{(k)}x + g_0^{(k)} \\
\text{for } k = 1, 2, \ldots, p - 1 \\
\text{and } g_i^{(k)} = \sum_{v=0}^{n-i}(-1)^{n-v+i}g_{n-v-i}^{(n-v)}g_{n-v}^{(n-v)} \text{ for } i = 0, 1, 2, \ldots, n.
\]

**Proof 1.** Let \( \alpha \in F_{p^n} \) be a root of \( P(x) \). Then we have

\[ P(x) = \prod_{i=0}^{n-1} (x - \alpha^q) \]  

Substituting \( x^p - x - \delta \) for \( x \) in (2), we will derive

\[ F(x) = P(x^p - x - \delta) = \prod_{i=0}^{n-1} (x^p - x - \delta - \alpha^q) = \prod_{i=0}^{n-1} (x^p - x - (\delta + \alpha)^q) \]  

Let us consider the polynomial \( l(x) = x^p - x - (\delta + \alpha) \).

By proposition 2 \( l(x) \) has a root in \( F_{p^n} \) if and only if \( Tr_{q^n/p}(\delta + \alpha) = 0 \).

Now we compute \( Tr_{q^n/p}(\delta + \alpha) \).

\[
Tr_{q^n/p}(\delta + \alpha) = Tr_{q^n/p}(Tr_{q^n/q}(\delta + \alpha)) = Tr_{q^n/q}(n\delta + Tr_{q^n/q}(\alpha)) = Tr_{q^n/p}(n\delta - a_{n-1})
\]

which is equal to 0 by condition of theorem. So we have that \( l(x) \) has a root in \( F_{q^n} \).

Let \( \gamma \in F_{q^n} \) be a root of \( l(x) \), that is

\[
\gamma^p - \gamma - (\delta + \alpha) = 0.
\]

Considering that \( \alpha = \gamma^p - \gamma - \delta \) one can see that \( F_q(\gamma) \supseteq F_q(\alpha) = F_{q^n} \), therefore \( \gamma \) is proper element of \( F_{q^n} \). It is easy to see that \( p \) roots of \( x^p - x - (\delta + \alpha) \) are \( \gamma + k, k = 0, 1, \ldots, p - 1 \). Clearly, \( \gamma^q + k, k \in F_p \) are all the roots of \( x^p - x - (\delta + \alpha)^q \).
Hence from (3) we have

\[
F(x) = \prod_{i=0}^{n-1} \prod_{k=0}^{p-1} (x - \gamma^q^i - k) = \prod_{k=0}^{p-1} \left( \prod_{i=0}^{n-1} (x - \gamma^q^i - k) \right).
\]

Denote

\[
G_k(x) = \prod_{i=0}^{n-1} (x - \gamma^q^i - k).
\]

It is obvious \(G_k(x)\) is the minimal polynomial of \(\gamma + k\), where \(k = 0, 1, \ldots, p - 1\) and \(G_k(x) = G_0(x - k)\). Thus \(G_k(x)\) is a irreducible polynomial over \(F_q\).

Let \(G_0(x) = x^n + g_{n-1}x^{n-1} + \cdots + g_1x + g_0\) and \(G_k(x) = x^n + g_{n-1}^kx^{n-1} + \cdots + g_1^kx + g_0^k\).

From (1) we have

\[
g_i^k = (-1)^{n-i} T_{r^{(n-i)}}^{q(x)/q} (\gamma + k) = (-1)^{n-i} \sum_{0 \leq j_1 < \cdots < j_{n-i} \leq n-1} (\gamma + k)^{q_j^1} (\gamma + k)^{q_2} \cdots (\gamma + k)^{q_{n-i}}.
\]

Let us compute \(g_i^k = (-1)^{n-i} T_{r^{(n-i)}}^{q(x)/q} (\gamma + k)\).

\[
g_i^k = (-1)^{n-i} \sum_{0 \leq j_1 < \cdots < j_{n-i} \leq n-1} \left( k^{n-i} + k^{n-i-1} \sum_{j_1 \leq u_1 \leq j_{n-i}} \gamma^{q_{u_1}} \right)
\]

\[
+ k^{n-i-2} \sum_{j_1 \leq u_1 < u_2 \leq j_{n-i}} \gamma^{q_{u_1}} \gamma^{q_{u_2}} + \cdots + k \sum_{j_1 \leq u_1 < \cdots < u_{n-i-1} \leq j_{n-i}} \gamma^{q_{u_1}} \gamma^{q_{u_2}} \cdots \gamma^{q_{u_{n-i-1}}}
\]

\[
+ \gamma^{q_{j_1}} \gamma^{q_{j_2}} \cdots \gamma^{q_{j_{n-i}}}
\]

(4)

Now we compute the following double sum

\[
\sum_{0 \leq j_1 < \cdots < j_{n-i} \leq n-1} \gamma^{q_{j_1}} \gamma^{q_{j_2}} \cdots \gamma^{q_{j_{r}}} \quad r = 1, \cdots, n - i - 1
\]

(5)

In the first and the second sums we have correspondingly \(\binom{n}{n-i}\) and \(\binom{n-i}{r}\) terms, and totally \(\binom{n}{n-i} \cdot \binom{n-i}{r}\) terms. It is easy to see that in (5) each term is repeated equal times. On the other hand the sum

\[
\sum_{0 \leq u_1 < u_2 < \cdots < u_r \leq n-1} \gamma^{q_{u_1}} \gamma^{q_{u_2}} \cdots \gamma^{q_{u_r}} \quad r = 1, \cdots, n - i - 1
\]

(6)

contains the same terms found in (5) without any repetition, whereas in (6) contains \(\binom{n}{r}\) terms.

So, one may conclude that

\[
\sum_{0 \leq j_1 < \cdots < j_{n-i} \leq n-1} \gamma^{q_{j_1}} \gamma^{q_{j_2}} \cdots \gamma^{q_{j_{r}}} = \binom{n}{n-i} \cdot \binom{n-i}{r} \sum_{0 \leq u_1 < u_2 < \cdots < u_r \leq n-1} \gamma^{q_{u_1}} \gamma^{q_{u_2}} \cdots \gamma^{q_{u_r}}
\]

(7)
\[ = (-1)^r \binom{n-r}{i} g_{n-r} \quad r = 1, \ldots, n - i - 1 \quad (7) \]

Opening brackets in (4) and substituting (7) in (4) we get

\[ g^{(k)}_i = \sum_{v=0}^{n-i} (-1)^{n-v-i} \binom{n-v}{i} g_{n-v} \quad (8) \]

where \( 0 \leq i \leq n, 0 \leq k \leq p - 1. \)

So, for obtaining the polynomial \( P(x^p - x - \delta) \) factors we need a single factor only. Rest factors may be computed by (8).

---

**An algorithm for factoring polynomial** \( P(x^p - x - \delta) \)

As seen from the proof of Theorem 1 a polynomial \( P(x^p - x - \delta) \) has no repeated factors. Below we propose an equal degree factorization algorithm based on Cantor and Zassenhaus's algorithm [Cantor, 1981].

Let \( f \) be a monic square-free univariate polynomial over a finite field \( F_q \) of degree \( n \) with \( r \geq 2 \) irreducible factors \( f_1, \ldots, f_r \), each of degree \( d \). Since \( f_1, \ldots, f_r \) are pairwise relatively prime, the Chinese Remainder Theorem provides the isomorphism:

\[ \chi : F_q[x]/(f) \to F_q[x]/(f_1) \times \cdots \times F_q[x]/(f_r), \]

\[ h \mod f \mapsto (h \mod f_1, \ldots, h \mod f_r). \]

Let us write \( R = F_q[x]/(f) \), and \( R_i = F_q[x]/(f_i) \) for \( 1 \leq i \leq r \). Then \( R_i \) is a field with \( q^d \) elements and so contains \( F_q \)

\[ F_q \subseteq F_q[x]/(f_i) = R_i \cong F_q^d \quad \text{for} \quad 1 \leq i \leq r. \]

Now \( f_i \) divides \( h \in F_q[x] \) if and only if \( h \equiv 0 \mod f_i \), that is, if and only if the \( i \)th component of \( \chi(h \mod f) \) is zero. Thus if \( h \in F_q[x] \) is such that \( h \mod f_1, \ldots, h \mod f_r \) has some zero components and some nonzero components, i.e. \( h \mod f \) is a nonzero zerodivisor in \( R \), then \( \gcd(h, f) \) is a nontrivial factor of \( f \), and we call \( h \) a “splitting polynomial”. Therefore, we look for polynomials with this property.

Now assume \( q \) to be odd (the algorithm can be generalized to characterize 2 fields). We take \( m = (q^d - 1)/2 \) and an \( r \)-tuple \( (h_1, \ldots, h_r) \) with each \( h_i \in R_i^\times = F_q^{d_i} \). In \( F_q^{d_i} \), half of the values are quadratic residues and the other half are quadratic nonresidues. Thus, \( h_i^{m \pm 1} = \pm 1 \), with the same probability for both values when \( h_i \) is chosen randomly. Now, choose at random (uniformly) a polynomial \( h \in F_q[x] \), with \( \deg h < n \), and let us assume that \( \gcd(h, f) = 1 \) (otherwise we have already found a partial factorization). The components \( (h_1, \ldots, h_r) \) of its image under the Chinese remainder isomorphism are independently and uniformly distributed random elements in \( R_i^\times = F_q^{d_i} \). Since \( h_i^{m} = 1 \) with probability \( \frac{1}{2} \), the probability that \( \gcd(h^{m - 1}, f) \) is not a proper factor of \( f \), i.e. all the components in \( (h_1^{m - 1}, \ldots, h_r^{m - 1}) \) are equal, is \( 2 \cdot 2^{-r} = 2^{-r+1} \leq \frac{1}{2} \). Running the algorithm \( l \) times ensures a probability of failure at most \( 2^{-l} \). Producing factorization \( f = g_1g_2 \) we can repeat it for \( g_1 \) (or for \( g_2 \) if \( \deg(g_2) < \deg(g_1) \)). The process is interrupted when \( \deg(g) \) is equal to \( n \).

**ALGORITHM:**

**Input:** Polynomial \( F(x) = P(x^p - x - \delta) \in F_q[x] \) of degree \( m = np \).

**Output:** Monic irreducible factor of \( F(x) \) of degree \( n \).
1: while $\deg(F) \neq n$, do
2: Choose $h \in F_q[x]$ with $\deg(h) < \deg(F)$ at random;
3: $g = \gcd(h, F)$
4: if $g = 1$, then $g = h^{(q^n-1)/2} - 1 \pmod{F}$
5: if $\gcd(g, F) \neq 1$, then $g_1 = \gcd(g, F), g_2 = \frac{F}{\gcd(g, F)}$
6: $F = \min_{\deg} \{g_1, g_2\}$
7: endif;
8: else: $g_2 = \frac{F}{g}, g_1 = g$
9: $F = \min_{\deg} \{g_1, g_2\}$
10: endif;
11: endwhile

For making the proposed algorithm more understandable, we will compare between ours and that of Cantor-Zassenhaus algorithm. Using Cantor-Zassenhaus algorithm we can split the polynomial into two proper factors. The remaining thing to do is to recursively call the algorithm on every splitting polynomial unless it is already irreducible. Using our algorithm we will also be able to split the polynomial into two proper factors. After that we are recursively call our algorithm only for one spitted polynomial, unless find one polynomial of degree $n$.

Theoretical computations show that the cost of the proposed algorithm for factoring polynomial $P(x^p - ax - \delta)$ of degree $np$, where $n$ is a degree of factors, is $O((n \log q + \log n))M(n) \log p$ operations in $F_q$.

Acknowledgements

This study was supported by the grant (‘YSSP-13-22’) of the National Foundation of Science and Advanced Technologies (RA) and Young Science Support Program(RA).

Bibliography


**Authors' Information**

**Sergey Abrahamyan** P.O. Box: 0014, P. Sevak street 1, Yerevan 0014, Armenia; e-mail: serj.abrahamyan@gmail.com
Major Fields of Scientific Research: Cryptography, Coding Theory

**Knarik Kyuregyan** P.O. Box: 0014, P. Sevak street 1, Yerevan 0014, Armenia; e-mail: knarikyuregyan@gmail.com
Major Fields of Scientific Research: Cryptography, Coding Theory