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 Zasenhaus'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

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

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

$$Tr^{(i)}_{q^n/q}(\alpha) = \sum_{0 \le j_1 < \cdots < j_i \le n-1} \alpha^{q^{j_1}} \alpha^{q^{j_2}} \cdots \alpha^{q^{j_i}},$$

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

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

$$g_i = (-1)^{n-i} Tr^{(n-i)}_{q^n/q}(\alpha). \tag{1}$$

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 $F_q = F_{p^s}$ of degree n. Let $\delta \in F_q$ and $Tr_{q/p}(n\delta - a_{n-1}) = 0$. 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. $P(x) = \sum_{u=0}^{n} a_u x^u$ be an monic irreducible polynomial of degree n over F_q and $Tr_{q/p}(n\delta - a_{n-1}) = 0$. 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: $F(x) = G_0(x)G_1(x)\ldots G_{p-1}(x)$, where*

$$G_0(x) = x^n + g_{n-1}x^{n-1} + \cdots + g_1 x + g_0,$$

$$G_k(x) = x^n + g^{(k)}_{n-1}x^{n-1} + \cdots + g^{(k)}_1 x + g^{(k)}_0 \qquad k = 1, 2, \ldots, p-1$$

and $g^{(k)}_i = \sum_{v=0}^{n-i} (-1)^{n+v-i} k^{n-v-i} \binom{n-v}{i} g_{n-v} \qquad i = 0, 1, 2, \ldots, n.$

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

$$P(x) = \prod_{i=0}^{n-1} (x - \alpha^{q^i}) \tag{2}$$

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

$$F(x) = P(x^p - x - \delta) = \prod_{i=0}^{n-1} (x^p - x - \delta - \alpha^{q^i}) = \prod_{i=0}^{n-1} (x^p - x - (\delta + \alpha)^{q^i}) \tag{3}$$

Let us consider the polynomial $l(x) = x^p - x - (\delta + \alpha)$.
By proposition 2 $l(x)$ has a root in F_{q^n} if and only if $Tr_{q^n/p}(\delta + \alpha) = 0$.
Now we compute $Tr_{q^n/p}(\delta + \alpha)$.

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

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 γ 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, $\gamma^{q^i} + k, k \in F_p$ are all the roots of $x^p - x - (\delta + \alpha)^{q^i}$.

Hence from (3) we have

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

Denote

$$G_k(x) = \prod_{i=0}^{n-1}\left(x - \gamma^{q^i} - k\right).$$

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

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

From (1) we have

$$g_i^{(k)} = (-1)^{n-i}Tr_{q^n/q}^{(n-i)}(\gamma + k) = (-1)^{n-i}\sum_{0\le j_1<\ldots<j_{n-i}\le n-1}(\gamma+k)^{q^{j_1}}(\gamma+k)^{q^{j_2}}\ldots(\gamma+k)^{q^{j_{n-i}}}.$$

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

$$g_i^{(k)} = (-1)^{n-i}\sum_{0\le j_1<\ldots<j_{n-i}\le n-1}\left(k^{n-i} + k^{n-i-1}\sum_{\substack{j_1\le u_1\le j_{n-i}\\ u_1\in\{j_1\ldots j_{n-i}\}}}\gamma^{q^{u_1}}\right.$$
$$+k^{n-i-2}\sum_{\substack{j_1\le u_1<u_2\le j_{n-i}\\ u_1,u_2\in\{j_1\ldots j_{n-i}\}}}\gamma^{q^{u_1}}\gamma^{q^{u_2}} + \cdots + k\sum_{\substack{j_1\le u_1<\ldots<u_{n-i-1}\le j_{n-i-1}\\ u_1,\cdots,u_{n-i-1}\in\{j_1\ldots j_{n-i}\}}}\gamma^{q^{u_1}}\gamma^{q^{u_2}}\ldots\gamma^{q^{u_{n-i-1}}}$$
$$\left.+\gamma^{q^{j_1}}\gamma^{q^{j_2}}\ldots\gamma^{q^{j_{n-i}}}\right) \tag{4}$$

Now we compute the following double sum

$$\sum_{0\le j_1<\ldots<j_{n-i}\le n-1}\ \sum_{\substack{j_1\le u_1<\ldots<u_r\le j_{n-i}\\ u_1,\ldots,u_r\in\{j_1\ldots j_{n-i}\}}}\gamma^{q^{u_1}}\gamma^{q^{u_2}}\ldots\gamma^{q^{u_r}} \qquad r = 1,\cdots,n-i-1 \tag{5}$$

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

$$\sum_{0\le u_1<u_2<\ldots<u_r\le n-1}\gamma^{q^{u_1}}\gamma^{q^{u_2}}\ldots\gamma^{q^{u_r}} \qquad r = 1,\cdots,n-i-1 \tag{6}$$

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

So, one may conclude that

$$\sum_{0\le j_1<\ldots<j_{n-i}\le n-1}\ \sum_{\substack{j_1\le u_1<\ldots<u_r\le j_{n-i}\\ u_1,\ldots,u_r\in\{j_1\ldots j_{n-i}\}}}\gamma^{q^{u_1}}\gamma^{q^{u_2}}\ldots\gamma^{q^{u_r}}$$
$$= \frac{\binom{n}{n-i}\cdot\binom{n-i}{r}}{\binom{n}{r}}\sum_{0\le u_1<\ldots<u_r\le n-1}\gamma^{q^{u_1}}\gamma^{q^{u_2}}\ldots\gamma^{q^{u_r}}$$

$$= (-1)^r \binom{n-r}{i} g_{n-r} \quad r = 1, \cdots, n-i-1 \tag{7}$$

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

$$g_i^{(k)} = \sum_{v=0}^{n-i} (-1)^{n+v-i} k^{n-v-i} \binom{n-v}{i} g_{n-v} \tag{8}$$

where $0 \le i \le n, 0 \le k \le p-1.$

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 $r \ge 2$ irreducible factors $f_1, \cdots, f_r$ each of degree d. Since $f_1, \dots, f_r$ are pairwise relatively prime, the Chinese Remainder Theorem provides the isomorphism:

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

$$h \mod f \longmapsto (h \mod f_1, \dots, h \mod f_r).$$

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

$$F_q \subseteq F_q[x]/(f_i) = R_i \cong F_{q^d} \qquad for \qquad 1 \le i \le r.$$

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 ith component of $\chi(h \mod f)$ is zero. Thus if $h \in F_q[x]$ is such that $(h \mod f_1, \dots, h \mod f_r)$ 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 characteristic 2 fields). We take $m = (q^d - 1)/2$ and an r-tuple $(h_1, \dots, h_r)$ with each $h_i \in R_i^\times = F_{q^d}^\times = F_{q^d}/\{0\}$. In $F_{q^d}^\times$, half of the values are quadratic residues and the other half are quadratic nonresidues. Thus, $h_i^m = \pm 1$, 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 $(h_1, \dots, h_r)$ of its image under the Chinese remainder isomorphism are independently and uniformly distributed random elements in $R_i^\times = F_{q^d}^\times$. 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 $(h_1^m - 1, \dots, h_r^m - 1)$ are equal , is $2 \cdot 2^{-r} = 2^{-r+1} \le \frac{1}{2}$. Running the algorithm l times ensures a probability of failure at most 2^{-l}. Producing factorization $f = g_1 g_2$ 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*** $g = h^{(q^n-1)/2} - 1(\mod F)$

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:*** $g_2 = \frac{F}{g}, \qquad g_1 = g;$

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

[Cantor, 1981] D. Cantor, H. Zassenhaus. A New Algorithm for Factoring Polynomials over Finite Fields. Mathematics of Computation, Vol. 36, No. 154, April, 1981, 587–592.

[Cao, 2012] X. Cao, L. Hu. On the reducibility of some composite polynomials over finite fields. Des. Codes Cryptogr, 64, 2012, pp. 229-239.

[Cohen, 1992] S.D. Cohen. The explicit construction of irreducible polynomials finite fields. Des. Codes Cryptogr, 2, 1992, pp. 169-174.

[Gathen, 2001] J. V. Z. Gathen, D. Panario. Factoring Polynomials over Finite Fields: A Survey, Academic Press, 2001.

[Kyuregh, 2011] M. Kyureghyan, G. Kyureghyan. Irreducible Compositions of Polynomials over Finite Fields. Des. Codes Cryptogr, 61(3), 2011, pp. 301-314.

[Lidl, 1987] R. Lidl, H. Niederreiter. Finite Fields, Cambridge University Press, 1987.

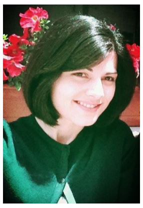
[Meyn, 1990] H.Meyn. On the construction of irreducible self-reciprocal polynomials over fnite fields. Appl. Algebrain Eng. Commun. Comput,1 1990, pp. 43-53.

[Varshamov, 1973] R. R. Varshamov, Operation substitution in a Galois field and their applications, Soviet Math. Dokl., 211, 1973, 768 – 771.

[Varshamov, 1984] R. R. Varshamov, A general method of synthesizing irreducible polynomials over Galois fields, Soviet Math. Dokl., 29, 1984, 334 – 336.

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