The Construction and Determination of Irreducible Polynomials Over Finite Fields

Yun Song[1] and Zhihui Li[2(✉)]

[1] School of Computer Science, Shaanxi Normal University, Xi'an 710062, China
songyun09@163.com

[2] School of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710062, China
lizhihui@snnu.edu.cn

Abstract. The approach for constructing the irreducible polynomials of arbitrary degree n over finite fields which is based on the number of the roots over the extension field is presented. At the same time, this paper includes a sample to illustrate the specific construction procedures. Then in terms of the relationship between the order of a polynomial over finite fields and the order of the multiplicative group of the extension field, a method which can determine whether a polynomial over finite fields is irreducible or not is proposed. By applying the Euclidean Algorithm, this judgment can be verified easily.

Keywords: Irreducible polynomial · Finite field · Cyclotomic polynomial · Mersenne prime · Order

1 Introduction

Generating irreducible polynomials and determining their irreducibility is one of the challenging and important problems in the theory of finite fields and its applications, especially computer algebra [1], coding theory [2] and cryptography [3]. For instance, irreducible polynomials are often used as a basic unit in constructing stream ciphers for implementing linear feedback shift register. Since linear feedback shift registers are described by coefficients of polynomials, these polynomials should be treated as the key information. Due to their important role in various applications, recent advances in these areas have awakened an even more interest to the subject of such polynomials [4–9]. Let F_q be the finite field of order $q = p^k$, where p is a prime and k is a positive integer. According to the field structure of F_q, there exists an irreducible polynomial of degree n over finite field F_q [9]. Kyuregyan [10, 11] presented some results on the constructive theory of synthesis of irreducible polynomials over F_{2^s}. Abrahamyan et al. [12, 13] considered recursive constructions of irreducible polynomials over finite fields.

This paper proposes a method for constructing irreducible polynomials over F_q in terms of the number of the roots over the extension field. If $\varphi(q^n - 1) = q^n - q$, the irreducible polynomials of arbitrary degree n over finite fields can be obtained by factoring $Q_{q^n-1}(x)$, because the primitive polynomials over F_q of degree n are all the irreducible polynomials; If $\varphi(q^n - 1) \neq q^n - q$, the irreducible polynomials of arbitrary

Y. Tan et al. (Eds.): ICSI 2016, Part II, LNCS 9713, pp. 618–624, 2016.
DOI: 10.1007/978-3-319-41009-8_67

degree n over finite fields can be obtained by factoring $I(q,n;x)$. Furthermore, The correlation between the order of a polynomial over finite fields and the order of the multiplicative group of the extension field is analyzed, and a sufficient and necessary condition on judging whether a polynomial of arbitrary degree n over finite fields is irreducible or not is presented.

2 The Construction of Irreducible Polynomials Over F_q

In this section, we will construct the irreducible polynomials of arbitrary degree n over finite fields based on the number of the roots over the extension field. Only monic polynomials, i.e., the polynomials whose leading coefficient is equal to 1, are studied in this paper.

Definition 2.1 [14]. Let $f(x) \in F_q[x]$ be a nonzero polynomial. If $f(0) \neq 0$, then the least positive integer e for which $f(x)$ divides $x^e - 1$ is called the order of $f(x)$ and is denoted by $\mathrm{ord}(f(x))$. If $f(0) = 0$, then $f(x) = x^h g(x)$, where $h \in N$ and $g(x) \in F_q[x]$ with $g(0) \neq 0$ are uniquely determined; $\mathrm{ord}(f(x))$ is then defined to be $\mathrm{ord}(g(x))$.

Theorem 2.2 [12]. Let K be a field of characteristic p, n a positive integer not divisible by p, and ζ a primitive nth root of unity over K. Then the polynomial $Q_n(x) = \prod_{s=1,\gcd(s,n)=1}^{n} (x - \zeta^s)$ is called the nth cyclotomic polynomial over K.

By Definition 2.1, the order of any root of $Q_n(x)$ is n.

Theorem 2.3 [10]. Let $(q,n) = 1$. $Q_n(x)$ factors into $\frac{\phi_n(x)}{d}$ distinct monic irreducible polynomials in $F_q[x]$ of the same degree d, where d is the least positive integer such that $q^d \equiv 1 \bmod n$.

Theorem 2.4. Let T_q^n be the number of irreducible polynomials in $F_q[x]$ of degree n, then

$$\frac{\phi(q^n - 1)}{n} \leq T_q^n \leq \left[\frac{q^n - q}{n}\right].$$

In particular, for the case $\phi(q^n - 1) = q^n - q$, $T_q^n = \frac{q^n - q}{n}$.

Proof. If $f(x)$ is an irreducible polynomial in $F_q[x]$ of degree n, then all roots of $f(x)$ are in $F_{q^n} - F_q$. Thus we have

$$T_q^n \leq \left[\frac{q^n - q}{n}\right].$$

The number of primitive polynomials in $F_{q^n}[x]$ of degree n is $\frac{\phi(q^n - 1)}{n}$. Since the primitive polynomial over finite fields is irreducible as well, it follows that

$$\frac{\phi(q^n-1)}{n} \leq T_q^n.$$

Therefore

$$\frac{\phi(q^n-1)}{n} \leq T_q^n \leq \left[\frac{q^n-q}{n}\right].$$

In particular, if $\phi(q^n-1) = q^n - q$, $T_q^n = \frac{q^n-q}{n}$.

Corollary 2.5. Let T_2^n be the number of irreducible polynomial in $F_2[x]$ of degree n. If $2^n - 1$ is Mersenne prime, then $T_2^n = \frac{2}{n}(2^{n-1}-1)$.

Note that all the irreducible polynomials over F_q of degree n are primitive if $\phi(q^n-1) = q^n - q$ by Theorem 2.4. Besides, the product of all primitive polynomials over F_q of degree n is equal to the cyclotomic polynomial $Q_e(x)$ with $e = q^n - 1$. Therefore, we will present a factorization method for $Q_e(x)$ over F_q.

Lemma 2.6 [14] (Berlekamp Algorithm). Let $f(x)$ be a polynomial over F_q of degree k, $h(x) \in F_q[x]$, and $h(x) = \sum_{l=0}^{m-1} h_l x^l$. Then we have

$$f(x) = \prod_{c\in F_q} \gcd(f(x), h(x)-c) h^q(x) \equiv h(x) \bmod (f(x)).$$

Note that the key to factoring the polynomial of degree k by applying Berlekamp algorithm is to find the polynomial $h(x)$ whose degree is at most $k-1$. Similarly, the first method of factoring $Q_{q^n-1}(x)$ over F_q is given by the following theorem.

Theorem 2.7. Let $h(x) \in F_q[x]$ and $h(x) = \sum_{l=0}^{m-1} h_l x^l$, where $(m, q) = 1$.

If $h_{lq \bmod m} = h_1 (l = 0, 1, \ldots, m-1)$, then $h(x)^q = h(x) \bmod Q_m(x)$ and we have $Q_m(x) = \prod_{c\in F_q} \gcd(Q_m(x), h(x)-c)$.

Proof. We first prove that $h(x)^q = h(x) \bmod (x^m - 1)$.

Let $s_l = lq (\bmod m)$ and $l = 0, 1, \ldots, m-1$. Since $(m, q) = 1$, then $s_1 \bmod m$ will go through all the elements in $0, 1, \ldots, m-1$. Thus we have

$$h(x)^q = \sum_{l=0}^{m-1} h_l x^{s_l} \bmod (x^m-1) = \sum_{l=0}^{m-1} h_{s_l} x^{s_l} = \sum_{l=0}^{m-1} h_l x^l = h(x),$$
$$h(x)^q = h(x) \bmod (x^m-1).$$

Note that

$$Q_m(x) | x^m - 1,$$

So

$$h(x)^q = h(x) \bmod Q_m(x).$$

The conclusion then follows from Lemma 2.6.

Example 2.8. We construct all irreducible polynomials in $F_2[x]$ of degree 3 in accordance with Theorem 2.7.

Since $2^3 - 1$ is a Mersenne prime, then all the irreducible polynomials over F_2 of degree 3 are primitive, which can be obtained by factoring $Q_7(x)$ over F_2, where $Q_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. By Theorem 2.7, $l \to 2l \bmod n$ is a permutation of $\{0, 1, \ldots, n-1\}$.

Let $U_7 = \{0, 1, 2, 3, 4, 5, 6\}$. The permutation of U_7 can be expressed as $\begin{pmatrix} 0123456 \\ 0246135 \end{pmatrix}$, which implies three cycle including $(0), (1, 2, 4)$ and $(3, 6, 5)$. Each of cycles can determine a polynomial satisfying Theorem 2.7, $h_1(x) = 1, h_2(x) = x^4 + x^2 + x, h_3(x) = x^6 + x^5 + x^3$.

By Theorem 2.7 and Euclidean algorithm, we have

$$(Q_7(x), h_2(x)) = x^3 + x + 1,$$

$$(Q_7(x), h_2(x) + 1) = x^3 + x^2 + 1.$$

Hence, $Q_7(x) = (x^3 + x^2 + 1)(x^3 + x + 1)$ and all irreducible polynomials in $F_2[x]$ of degree 3 are $x^3 + x^2 + 1$ and $x^3 + x + 1$.

Remark. If $\phi(q^n - 1) \neq q^n - q$, all irreducible polynomials in $F_q[x]$ can be determined by factoring $I(q, n; x)$ which is the product of all irreducible polynomials in $F_q[x]$ of degree n [14].

3 The Determination of Irreducible Polynomials Over F_q

According to the relationship between the order of a polynomial over finite fields and the order of the multiplicative group of the extension field, and the construction of irreducible polynomials above, we will present a sufficient and necessary condition on judging whether a polynomial of arbitrary degree n over finite fields is irreducible or not.

For irreducible polynomials in $F_q[x]$ of degree n, which satisfy $\phi(q^n - 1) = q^n - q$, we can get the following theorem by the discussion in Sect. 2.

Theorem 3.1. Let $f(x) \in F_q[x]$ be a polynomial over F_q of degree n and $\phi(q^n - 1) = q^n - q$. $f(x)$ is irreducible if and only if $\mathrm{ord}(f(x)) = q^n - 1$.

Lemma 3.2 [12]. For every finite field F_q and every $n \in N$, the product of all irreducible polynomials over F_q whose degree divides n is equal to $x^{q^n} - x$.

Lemma 3.3 [12]. Let c be a positive integer. Then the polynomial $f(x) \in F_q[x]$ with $f(0) \neq 0$ divides $x^c - 1$ if and only if $\mathrm{ord}(f(x))|c$.

Let $f(x)$ be a polynomials in $F_q[x]$ of degree n, and $n = p_1^{t_1} p_2^{t_2} \ldots p_s^{t_s}$ is the prime factor decomposition of n. Let $n_i = n/p_i$.

Theorem 3.4. Let $f(x)$ be a polynomial over F_q of degree n. If $f(x)$ satisfies the following properties:

(1) $\mathrm{ord}(f(x))|q^n - 1$;
(2) For every $c \in F_q, f(c) \neq 0$;
(3) $\gcd(\mathrm{ord}(f(x)), q^{n_i} - 1) = 1, \ (i = 1, 2, \ldots, s)$

then $f(x)$ is an irreducible polynomial over F_q.

Proof. Since $\mathrm{ord}(f(x))|q^n - 1$, we have $f(x)|x^{q^n - 1} - 1$.

According to Lemma 3.3, $f(x)$ has no repeated factor. Suppose $f(x)$ were reducible over F_q. Then we have a factorization $f(x) = f_1(x) f_2(x) \ldots f_t(x)$, where each $f_j(x) (j = 1, 2, \ldots, t)$ are pairwise relatively prime. Since $f_j(x)|x^{q^n - 1} - 1$, then

$$\deg(f_j(x))|n \quad (j = 1, 2, \ldots, t).$$

we claim that

$$\deg(f_j(x)) \nmid n_i \ (i = 1, 2 \ldots, s).$$

Suppose $\deg(f_j(x))|n_k$ for some $1 \leq k \leq s$. Then

$$f_j(x)|x^{q^{n_k}} - x \quad \text{and} \quad f_j(x)|x^{q^{n_k} - 1} - 1.$$

By Lemma 3.2, since

$$\mathrm{ord}\big(f_j(x)\big)|\mathrm{q}^{n_k} - 1 \text{ and } \mathrm{ord}\, f_j(x)|\mathrm{ord}\, f(x),$$

by Lemma 3.3, we have

$$\gcd(\mathrm{ord}(f(x)), q^{n_k} - 1) \neq 1.$$

a contradiction to (3). Therefore, $\deg(f_j(x)) = n$ and $f_j(x) = f(x)$. Hence, $f(x)$ is an irreducible polynomial over F_q.

Theorem 3.5. If $f(x)$ is an irreducible polynomial over F_q, then

(1) $\mathrm{ord}(f(x))|q^n - 1$;
(2) For every $c \in F_q$,$f(c) \neq 0$;
(3) $\mathrm{ord}(f(x)) \nmid q^{n_i} - 1$.

Proof. Since $f(x)$ is an irreducible polynomial over F_q of degree n, then $f(c) \neq 0$ for every $c \in F_q$, and $\mathrm{ord}(f(x))|q^n - 1$.

Suppose

$$\mathrm{ord}(f(x))|\ q^{n_k} - 1 \ \text{ for some } \ 1 \leq k \leq s.$$

According to Lemma 3.3,

$$f(x)|x^{q^{n_k}-1} - 1.$$

Then

$$f(x)|x^{q^{n_k}} - x.$$

Hence, $\deg(f(x))|n_k$, a contradiction to $\deg(f(x)) = n$ by Lemma 3.2. Therefore, $\mathrm{ord}(f(x)) \nmid q^{n_i} - 1 \quad (i = 1, 2, \ldots, s)$.

The following results can be implied by above two theorems.

Corollary 3.6. Let $f(x)$ be a polynomial over F_q of degree p, where p is a prime. Then $f(x)$ is irreducible if and only if:

(1) $\mathrm{ord}(f(x))|q^p - 1$;
(2) For every $c \in F_q$, $f(c) \neq 0$.

Corollary 3.7. Let $f(x)$ be a polynomial over F_q of degree $n = p_1 p_2$, where p_1 and p_2 are prime numbers. Then $f(x)$ is irreducible if and only if:

(1) $\mathrm{ord}(f(x))|q^n - 1$;
(2) For every $c \in F_q$, $f(c) \neq 0$;
(3) $\mathrm{ord}(f(x)) \nmid q^{p_1} - 1$ and $\mathrm{ord}(f(x)) \nmid q^{p_2} - 1$.

4 Conclusion

Irreducible polynomials over finite fields play an important role in computer algebra, coding theory and cryptography. This paper constructed the irreducible polynomials of arbitrary degree n over finite fields based on the number of the roots over the extension field and determined whether a polynomial over finite fields is irreducible or not in terms of the relationship between the order of a polynomial over finite fields and the order of the multiplicative group of the extension field. Furthermore, a relevant example was analyzed to show the specific construction procedures.

Acknowledgments. This work was supported by the National Natural Science Foundation of China (61373150, 11501343), the Key Technologies R&D Program of Shaanxi Province (2013k0611), and the Fundamental Research Funds for the Central Universities (GK201603087).

References

1. Garefalakis, T., Kapetanakis, G.: A note on the Hansen-Mullen conjecture for self-reciprocal irreducible polynomials. Finite Fields Appl. **35**(4), 61–63 (2015)
2. Magamba, K., Ryan, J.A.: Counting irreducible polynomials of degree r over F_{q^n} and generating Goppa Codes using the lattice of subfields of $F_{q^{nr}}$. J. Discrete Math. **2014**, 1–4 (2014)
3. Ugolini, S.: Sequences of irreducible polynomials over odd prime fields via elliptic curve endomorphisms. J. Number Theor. **152**, 21–37 (2015)
4. Ri, W.H., Myong, G.C., Kim, R., et al.: The number of irreducible polynomials over finite fields of characteristic 2 with given trace and subtrace. Finite Fields Appl. **29**, 118–131 (2014)
5. Kaminski, M., Xing, C.: An upper bound on the complexity of multiplication of polynomials modulo a power of an irreducible polynomial. IEEE Trans. Inf. Theor. **59**(10), 6845–6850 (2013)
6. Fan, H.: A Chinese remainder theorem approach to bit-parallel GF(2^n) polynomial basis multipliers for irreducible trinomials. IEEE Trans. Comput. **65**(2), 1 (2016)
7. Kopparty, S., Kumar, M., Saks, M.: Efficient indexing of necklaces and irreducible polynomials over finite fields. In: Esparza, J., Fraigniaud, P., Husfeldt, T., Koutsoupias, E. (eds.) ICALP 2014. LNCS, vol. 8572, pp. 726–737. Springer, Heidelberg (2014)
8. Nechae, A.A., Popov, V.O.: A generalization of Ore's theorem on irreducible polynomials over a finite field. Discrete Math. Appl. **25**(4), 241–243 (2015)
9. Pollack, P.: Irreducible polynomials with several prescribed coefficients. Finite Fields Appl. **22**(7), 70–78 (2013)
10. Kyuregyan, M.K.: Recurrent methods for constructing irreducible polynomials over F q of odd characteristics. Finite Fields Appl. **12**(3), 357–378 (2006)
11. Kyuregyan, M.K., Kyureghyan, G.M.: Irreducible compositions of polynomials over finite fields. Des. Codes Cryptogr. **61**(3), 301–314 (2011)
12. Abrahamyan, S., Kyureghyan, M.: A recurrent method for constructing irreducible polynomials over finite fields. In: Gerdt, V.P., Koepf, W., Mayr, E.W., Vorozhtsov, E.V. (eds.) CASC 2011. LNCS, vol. 6885, pp. 1–9. Springer, Heidelberg (2011)
13. Abrahamyan, S., Alizadeh, M., Kyureghyan, M.K.: Recursive constructions of irreducible polynomials over finite fields. Finite Fields Appl. **18**(4), 738–745 (2012)
14. Kaliski, B.: Irreducible Polynomial. Springer, New York (2011)