Simple method to find primitive polynomials of degree n over $GF(2)$ where $2^n - 1$ is a Mersenne prime

Jiantao Wang[1], Dong Zheng[2], and Qiang Li[2]
[1]School of Information Security Engineering, Shanghai Jiao Tong University,
Shanghai 200240, China
[2]National Engineering Laboratory for Wireless Security,
Xi'an University of Posts and Telecommunications,
Xi'an 710121, Shaanxi Province, China

Abstract— *The paper describes the group structure of cyclotomic cosets modula $2^n - 1$, the group is cyclic when $2^n - 1$ is a prime. The integers modula $2^n - 1$ can be regarded as the exponents of a primitive element $\alpha \in GF(p^n)$. The traces of α^i show the same structure as the cyclic group of the cyclotomic cosets modula $2^n - 1$. The coefficients of the minimal polynomial of a specific α^j consist of the sum of the traces of different α^i, which follow the cyclic group structure. We demonstrate that all the primitive polynomials can be calculated fast through the permutation of the traces of α^i.*

Keywords: Finite Fields, Cyclotomic Cosets, Primitive Polynomial

1. Introduction

The theory of finite fields has played important roles in code design and cryptography[1], [2]. The irreducible polynomials of degree n over $GF(p)$, where $p > 0$ is a prime, is of special interest[3], [4]. Many algorithms require the calculations of different irreducible polynomials of a fixed degree n.

There has been various methods for constructing irreducible polynomials of the same degree n[1], [2], [4] from a given primitive polynomial. And one direct way is to use the relations between the coefficients and the roots of the irreducible polynomials[1], [2], [5]. For a defining element α of a finite field $GF(p^n)$, the coefficients of the minimal polynomials of different α^k are the sum of different α^t. This means that one specific power α^t appears in different positions in the coefficients of minimal polynomials of different elements. In this paper, we show that the reason is the group structure of cyclomotic cosets. For a Mersenne prime, which is defined to be the primes of the form $2^n - 1$, the group structure of the cyclotomic cosets reduces the computing work to simple group permutations. The group structure can also explain why some former classical algorithms[2], [6] using the cubic root and permutation succeeded.

The paper are organized as follows. In Section 2 some preliminary results are given. Section 3 introduces our main theory. Experiment results are given in Section 4. Section 5 concludes our work.

2. Newton Formula and Cyclomotic Cosets

We first give some preliminaries that are useful for our theory. In a finite field $F = GF(p^n)$, where p is a prime and $n > 0$ is an integer, the trace function of an element $\alpha \in F$ is defined as:

$$tr(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{n-1}} \in GF(p) \quad (1)$$

Assume $f(x)$ to be an irreducible polynomial over $GF(p)$ of degree n whose roots are $x_1 = \alpha, x_2 = \alpha^p, \cdots, x_n = \alpha^{p^{n-1}}$. The elementary symmetric polynomials $\sigma_1, \sigma_2, \cdots, \sigma_n$ are the coefficients of $f(x)$:

$$\begin{aligned} f(x) &= (x - x_1)(x - x_2)\cdots(x - x_n) \\ &= x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} \\ &\quad - \cdots + (-1)^{n-1}\sigma_{n-1}x + (-1)^n\sigma_n \end{aligned} \quad (2)$$

Another kind of symmetric polynomial is defined as:

$$\begin{aligned} s_k &= s_k(x_1, x_2, \ldots, x_n) \\ &= x_1^k + x_2^k + \cdots + x_n^k \\ &= \sum_{1 \le t \le n} (\alpha^{p^{n-1}})^k, \end{aligned} \quad (3)$$

where $k \ge 1$ is an integer.

The Newton Formula is [7, p.12]:

$$\begin{aligned} &s_k - s_{k-1}\sigma_1 + \cdots + (-1)^i s_{k-i}\sigma_i \\ &\quad + \cdots + (-1)^{k-1} s_1 \sigma_{k-i} \\ &\quad + (-1)^k k\sigma_k = 0, \sigma_j = 0 \quad \text{for} \quad j > n. \end{aligned} \quad (4)$$

The trace of α^k equals to the symmetric polynomial s_k induced by the roots of $f(x)$. If $f(x)$ is primitive, then α^k can denote all the elements in the finite fields, and we can use the Newton Formula to compute the trace of any element of the finite field via linear iteration.

In the expansion of $f(x)$, σ_i is the sum of all powers of α having exponents which, when written as p-ary n-tubles,

have i ones and $n-i$ zeroes. The exponents of α in one trace function also have the same ones when written as p-ary n-tubles. So the coefficients σ_i could be decomposed into the sum of traces of some specific elements.

Cyclomotic cosets[2, p.42] are a classification of the non-zero residues modula p^n-1. Each coset contains the numbers that are congruent to each other modula p^n-1 by multiplying a power of p, e.g. $\{1,2,4\},\{3,6,5\}$ are two cyclomotic cosets modula $2^3-1=7$. Every coset equals to a set of the exponents of the powers appeared in the trace function of a finite field element $\beta=\alpha^k, k$ is an integer. All α^i where i runs through a cyclomotic coset have the same minimal polynomial in the finite field[2].

3. Group Structure and Minimal Polynomials

We present our main theory in this section. According to number theory, the residues modula $q=p^n-1$ forms an Abelian group with respect to multiplication. The group is cyclic for $p=2$ and $q=2^n-1$ prime, and we denote the cyclic group as G. And all the cyclomotic cosets have the same length n as all the irreducible polynomials are primitive polynomials for q prime.

Considering cyclomotic coset modula q, $H=\{1,2,2^2,\ldots,2^{n-1}\}$. It is also a cyclic subgroup of G. We have the following relations between G and H.

Proposition 1: H is a normal subgroup of G. The quotient group G/H is a cyclic group. Multiplying any $1\le k<2^n-1$ to all the elements in G/H means a permutation of the quotient group.

Proof: Because G is commutative, the subgroups of G are all normal, so does H. Both G and H are cyclic, G/H is also cyclic by group theory.

Let $H_1\in G/H$, then $H_1=k_1H$, where $1\le k_1<2^n-1$, then $k\cdot H_1=k\cdot k_1H=kH\cdot k_1H=k_2H$ where $1\le k,k_2<2^n-1$. Consider kH as a group member of G/H, hence the theorem follows. ∎

Example 1: $p=2, n=5, q=31, G=\{1,2,\ldots,30\}, H=\{1,2,4,8,16\}$.
Then G/H is an cyclic group of order 6.

$$\begin{aligned}
H_1&=H=\{1,2,4,8,16\},\\
H_2&=3H=\{3,6,12,24,17\},\\
H_3&=5H=\{5,10,20,9,18\},\\
H_4&=7H=\{7,14,28,25,19\},\\
H_5&=11H=\{11,22,13,26,21\},\\
H_6&=15H=\{15,30,29,27,23\},\\
G/H&=\{H_1,H_2,\ldots,H_6\}.
\end{aligned}$$

H_2 is a generator of G/H. $H_2^2=9H=5H=H_3, H_2^3=15H=H_6, H_2^4=45H=14H=H_4, H_2^5=11H=H_5, H_2^6=2H=H_1$.

We want to find all the primitive polynomials from a given primitive polynomial of degree n over $GF(2)$. The coefficients of the primitive polynomials consists of the traces of α^k where k belongs to cyclomotic cosets leaders for a Mersenne prime q.

From finite field theory, q is the smallest integer such that $\alpha^q=1$. So any $\beta\in GF(q)$ can be written in the form α^k and has the same order q as α. This means the minimal polynomials of all α^k where k belongs to different cyclomotic cosets, are all the primitive polynomials of degree n.

From the general structure of minimal polynomials discussed in the former section, the exponents of powers of α contained in the coefficients of $f(x)$ cover all the cyclomotic cosets. Every exponent needs to be multiplied by k to compute the minimal polynomial of a specific element α^k. The numbers in the same cosets appear as a whole in the same coefficient of a primitive polynomial, as proved in Proposition 1. The coefficients of the minimal polynomial of α^k are the sum of permuted elements of the quotient group defined in Proposition 1.

For example, the minimal polynomial of a primitive element $\alpha\in GF(2^5)$ has the following form.

$$\begin{aligned}
f_\alpha(x)=x^5&+tr(\alpha)x^4+(tr(\alpha^3)+tr(\alpha^5))x^3\\
&+(tr(\alpha^7)+tr(\alpha^{11}))x^2+tr(\alpha^{15})x+1
\end{aligned}\tag{5}$$

The minimal polynomial of any element $\beta=\alpha^k\in GF(q)$ is a primitive polynomial of the same form shown in (5). The trace function has the exponent property $tr((\alpha^k)^t)=tr(\alpha^{kt})$, so the minimal polynomial of β can be represented by α. Continued from (5), let $k=3$, then:

$$\begin{aligned}
f_\beta(x)&=x^5+tr(\beta)x^4+(tr(\beta^3)+tr(\beta^5))x^3\\
&\quad+(tr(\beta^7)+tr(\beta^{11}))x^2+tr(\beta^{15})x+1\\
&=x^5+tr(\alpha^3)x^4+(tr(\alpha^9)+tr(\alpha^{15}))x^3\\
&\quad+(tr(\alpha^{21})+tr(\alpha^{33}))x^2+tr(\alpha^{45})x+1\\
&=x^5+tr(\alpha^3)x^4+(tr(\alpha^5)+tr(\alpha^{15}))x^3\\
&\quad+(tr(\alpha^{11})+tr(\alpha))x^2+tr(\alpha^7)x+1
\end{aligned}\tag{6}$$

The last step in the deduction is due to $tr(\alpha^{31})=1$ and the trace is the same for the exponents of powers of α in the same cyclomotic coset. Comparing (5) with (6), the coefficients of the minimal polynomials of α and $\beta=\alpha^3$ are permutations of the traces $tr(\alpha),tr(\alpha^3),tr(\alpha^5),tr(\alpha^7),tr(\alpha^{11}),tr(\alpha^{15})$.

A generator of the cyclic cyclomotic cosets group is needed to get all the primitive polynomials of degree n, . Multiplying the generator gives a permutation chain among all the cyclic group elements. Then all the primitive polynomials can be calculated by iteration.

Example 2 (continued from Example 1): $p=2, n=5, q=31$. Then $f_1(x)=x^5+x^3+1$ is a primitive

polynomial over GF(2) with a root α. So $\sigma_1 = \sigma_3 = \sigma_4 = 0, \sigma_2 = \sigma_5 = 1, s_1 = \sigma_1 = 0$.

By Newton Formula, $s_2 - \sigma_1 s_1 + 2\sigma_2 = 0, s_2 = 0$, then $s_3 = tr(\alpha^3) = 0, s_4 = 0, s_5 = tr(\alpha^5) = 1$. For $k > 5$, we have $s_k = s_{k-2} + s_{k-5}$. We get $s_7 = tr(\alpha^7) = 1$, $s_{11} = tr(\alpha^{11}) = 1$, $s_{15} = tr(\alpha^{15}) = 0$.

The basic structure of the minimal polynomial of degree 5 over $GF(2)$ is shown in (5). We use the form $(\gamma_1\ \gamma_2\ \ldots\ \gamma_m)$ to show a permutation σ over some elements $\{\gamma_1, \gamma_2, \gamma_3, \ldots, \gamma_m\}$ of a group where $\sigma(\gamma_i) = \gamma_{i+1}, for\ 1 \le i \le m-1, \sigma(\gamma_m) = \gamma_1$.

Example 1 shows that $H_2 = 3H$ is a generator of the cyclic group G/H. The cyclic relation can be written in a permutation form.

$$
\begin{aligned}
&(H \quad 3H \quad 5H \quad 15H \quad 7H \quad 11H)\\
&= (1 \quad 3 \quad 5 \quad 15 \quad 7 \quad 11)\\
&= (tr(\alpha) \quad tr(\alpha^3) \quad tr(\alpha^5) \quad tr(\alpha^{15}) \quad tr(\alpha^7) \quad tr(\alpha^{11}))
\end{aligned}
$$

This leads to the conversion from (5) to (6) . So the other primitive polynomials of degree 5 over $GF(2)$ can be computed by the permutation sequently.

$$
\begin{aligned}
f_{\alpha^5}(x) &= x^5 + tr(\alpha^5)x^4 + (tr(\alpha^{15}) + tr(\alpha^7))x^3\\
&\quad + (tr(\alpha) + tr(\alpha^3))x^2 + tr(\alpha^{11})x + 1\\
f_{\alpha^{15}}(x) &= x^5 + tr(\alpha^{15})x^4 + (tr(\alpha^7) + tr(\alpha^{11}))x^3\\
&\quad + (tr(\alpha^3) + tr(\alpha^5))x^2 + tr(\alpha)x + 1\\
f_{\alpha^7}(x) &= x^5 + tr(\alpha^7)x^4 + (tr(\alpha^{11}) + tr(\alpha))x^3\\
&\quad + (tr(\alpha^5) + tr(\alpha^{15}))x^2 + tr(\alpha^3)x + 1\\
f_{\alpha^{11}}(x) &= x^5 + tr(\alpha^{11})x^4 + (tr(\alpha) + tr(\alpha^3))x^3\\
&\quad + (tr(\alpha^{15}) + tr(\alpha^7))x^2 + tr(\alpha^5)x + 1
\end{aligned}
$$

Combining with the traces computed by Newton Formula, it follows:

$$
\begin{aligned}
&f_\alpha(x) = x^5 + x^3 + 1,\\
&f_{\alpha^3}(x) = x^5 + x^3 + x^2 + x + 1,\\
&f_{\alpha^5}(x) = x^5 + x^4 + x^3 + x + 1,\\
&f_{\alpha^{15}}(x) = x^5 + x^2 + 1,\\
&f_{\alpha^7}(x) = x^5 + x^4 + x^3 + x^2 + 1,\\
&f_{\alpha^{11}}(x) = x^5 + x^4 + x^2 + x + 1.
\end{aligned}
$$

4. Experiments

We give some numerical experiments to show the efficiency of our algorithm.

The next Mersenne prime after 31 is $2^7 - 1 = 127$, and we know its primitive root is 3. Starting from a given primitive polynomial of degree 7, $f(x) = x^7 + x + 1$, the next table shows the cosets $3^k mod 127$ and their binary representative, from low digits to high digits, and their s_k computed by Newton Formula.

Table 1: The Coset Leaders And Their s_k

k	$3^k mod 127$	binary form	s_k
1	3	1 1 0 0 0 0 0	0
2	9	1 0 0 1 0 0 0	0
3	27	1 1 0 1 1 0 0	1
4	81	1 0 0 0 1 0 1	1
5	116	0 0 1 0 1 1 1	0
6	94	0 1 1 1 1 0 1	1
7	28	0 0 1 1 1 0 0	1
8	84	0 0 1 0 1 0 1	1
9	125	1 0 1 1 1 1 1	1
10	121	1 0 0 1 1 1 1	1
11	109	1 0 1 1 0 1 1	0
12	73	1 0 0 1 0 0 1	1
13	92	0 0 1 1 1 0 1	0
14	22	0 1 1 0 1 0 0	0
15	66	0 1 0 0 0 0 1	0
16	71	1 1 1 0 0 0 1	0
17	86	0 1 1 0 1 0 1	1

The number of ones in the binary form in the table shows the position the coset belongs in $f(x)$. The order of Table 1 shows the permutation structure. For a fixed permutation, one coset is replaced by a coset whose place has a fixed distance from the former one in Table 1. We compute all the other primitive polynomial according to the sum of the permuted s_k in Table 2. The polynomial is written in a short form, where 10101011 stands for $x^7 + x^5 + x^3 + x + 1$.

We have also tested the Mersenne prime $2^{13} - 1, 2^{17} - 1, 2^{19} - 1$, the result is too long for our paper, but we get all the polynomials in this simple way.

Table 2: The Primitive Polynomials Of Degree 7 Over GF(2)

k	minimal polynomial of α^k
3	1 0 1 0 1 0 1 1
9	1 0 1 1 1 0 0 1
27	1 1 1 1 0 1 1 1
81	1 1 1 0 0 1 0 1
116	1 0 0 1 0 0 0 1
94	1 1 1 1 0 0 0 1
28	1 1 1 1 1 1 0 1
84	1 1 0 0 1 0 1 1
125	1 1 0 0 0 0 0 1
121	1 1 0 1 0 1 0 1
109	1 0 0 1 1 1 0 1
73	1 1 1 0 1 1 1 1
92	1 0 1 0 0 1 1 1
22	1 0 0 0 1 0 0 1
66	1 0 0 0 1 1 1 1
71	1 0 1 1 1 1 1 1
86	1 1 0 1 0 0 1 1

5. Conclusion

This paper associates the computation of minimal polynomial with the group structure of cyclotomic cosets modula $2^n - 1$ for $2^n - 1$ is a Mersenne prime. From the examples and experiments, we see the computation of the primitive polynomials is simple and efficient due to the cyclic group

structure of the cyclomotic cosets, and the usual knowledge of the tables of the sums and products in the finite field is not required. This cyclic group structure is also the reason for the "rational algorithm" in [2, p.48] and for the valid assignments yielded by permutation in [6].

Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grant No 61272037, Key Program of Natural Science Foundation of Shaanxi Province(Grant No.2013JZ020) and "New Generation of Broadband Wireless Communications Network" Ministry of Industry and Information Technology major projects (Project No.2013ZX03002004).

References

[1] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications* , Cambridge University Press, 1986.

[2] S. W. Golomb and G. Gong, *Signal design for good correlation*, Cambridge University Press, 2005.

[3] J. A. Gordon, "Very simple method to find the minimum polynomial of an arbitrary nonzero element of a finite field," *Electronic Letters*, vol. 12, pp. 663–664, 1976.

[4] V. C. da Rocha Jr. and G. Markarian, "Simple Method to Find Trace of Arbitrary Element of a Finite Field," *Electronic Letters*, vol. 2, No. 7, Mar, 2006.

[5] O. Ahmadi and A. Menezes, "On the number of trace-one elements in polynomial bases for $GF(2^m)$," *Designs, Codes and Cryptography*, vol. 37, pp. 493–507, 2005.

[6] S. W. Golomb, "Obtaining specified irreducible polynomials over finite fields," *SIAM J. ALG. DISC. MATH*. vol. 1, No. 4, December, 1980.

[7] H. M. Edwards, *Galois Theory*. Springer, 1997.