Two-Dimensional Sequences of Primitive Polynomials

Bongjoo Park[1], Taejoo Chang[1,2], Iickho Song[2] and Byung-Hwa Chang[1]
[1]Dept. 5-4-2, Agency for Defense Development (ADD)
P.O. Box 35, Yuseong, Daejeon 305-600
Korea

[2]Department of Electrial Engineering
Korea Advanced Institute of Science and Technology (KAIST)
373-1 Guseong Dong, Yuseong Gu, Daejeon 305-701
Korea
email: isong@Sejong.kaist.ac.kr

ABSTRACT. In this paper we consider the two-dimensional sequence of primitive polynomials, which is defined by two positive integers and a primitive polynomial. The concept of q^m *conjugate order* is used to describe the two-dimensional sequence. Using the two-dimensional sequences, we can find maximum period primitive polynomial sequences for more values of degrees than using the one-dimensional sequences. Examples of the applications of the two-dimensional sequence by computer search are shown.

1 Introduction

Primitive polynomials over $GF(q)$ are useful in many application areas including design of scramblers, error correcting coders and decoders, and cryptographic devices.

The searching algorithms for primitive polynomials [1] can be divided into two classes: the class of algorithms which test a given polynomial for primitivity and the class of algorithms which construct primitive polynomials. For example, a construction algorithm for finding primitive polynomials has been proposed in [2]. The algorithm generates a sequence of primitive polynomials from a known primitive polynomial and an integer. (Such a sequence will be called one-dimensional.) In [3] the concept of the "q^m order" to determine the period of a sequence has been introduced.

JCMCC 25 (1997), pp. 97-111

It is an interesting problem to search all of the primitive polynomials for a given degree: that is, to search a primitive polynomial sequence whose period is equal to the maximum number $\phi(q^m - 1)/m$ of primitive polynomials, where m is the degree.

We describe in this paper the two-dimensional sequences of primitive polynomials, which is defined by two positive integers and a primitive polynomial. The q^m conjugate order is introduced to describe the two-dimensional sequence. Some examples obtained from computer search are shown. It is shown that, using the two-dimensional sequences, we can find maximum period primitive polynomial sequences for more values of m than using the one-dimensional sequences.

2 Preliminaries

Let $f(x)$ be a primitive polynomial of degree m over $GF(q)$ with a root α. For an integer k such that $gcd(k, q^m - 1) = 1$, the minimal polynomial of α^k is a primitive polynomial and is said to be *generated from f with k.*

Let h and k be positive integers that are relatively prime to $q^m - 1$. If g is generated from f with k and y is generated from g with h, then the polynomial generated from f with kh is y as shown in Figure 1.

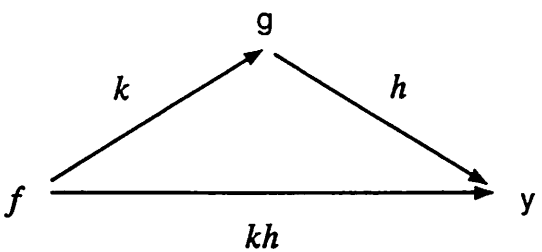

Figure 1. Generation of primitive polynomials

For an integer k, for which $gcd(k, q^m - 1) = 1$, let f_{k^i} be generated from $f_{k^{i-1}}$ with k, $i = 1, 2, \ldots$, where f_1 is given. Then the sequence $\{f_{k^i}\}, i = 0, 1, 2, \ldots$, is called the one-dimensional sequence of primitive polynomials: for example, the sequence can be obtained from the generation method of primitive polynomials considered in [2]. The same sequence of polynomials $\{f_{k^i}\}$ can also be generated from f with k^i, as shown in Figure 2. In [3] the periods of the one-dimensional sequences have been determined by introducing the concept of the q^m *order* with the latter generation method.

Definition 1 ([3]) *For a positive integer k such that $gcd(k, q^m - 1) = 1$, the q^m order of k, denoted by $o(k)$, is the least integer $e \geq 1$ such that*

$$k^e \equiv q^i \ (mod\ q^m - 1), \quad \textit{for some integer } i. \tag{1}$$

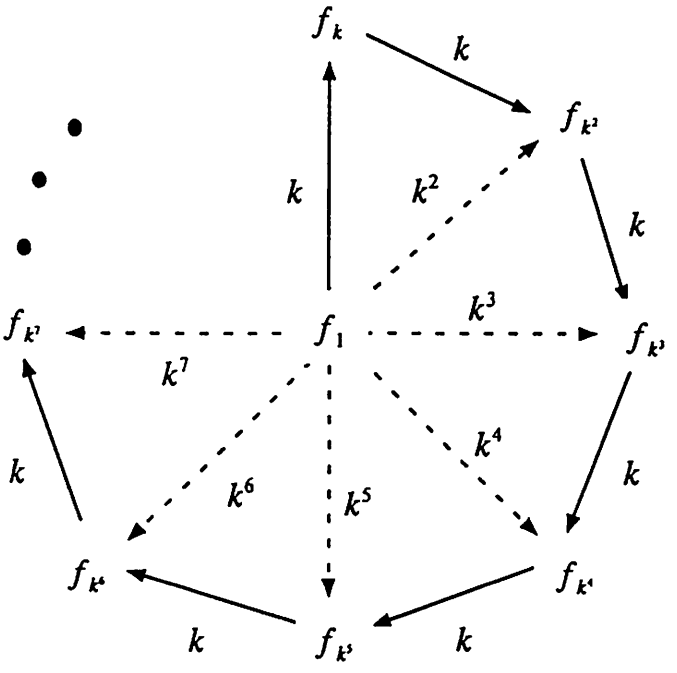

Figure 2.
Generation of the one-dimensional sequence of primitive polynomials

Theorem 1 ([3]) *If there exists an integer j such that $k^l \equiv q^j \pmod{q^m - 1}$, then l is divisible by $o(k)$.*

Theorem 2 ([3]) *For a positive integer k such that $gcd(k, q^m - 1) = 1$ and a primitive polynomial f_1 of degree m over $GF(q)$, the period of the sequence $\{f_{k^i}\}$ of primitive polynomials is $o(k)$.*

3 The two-dimensional sequence

In Section 2 we discussed briefly the (one-dimensional) sequence of primitive polynomials generated from a polynomial f of degree m and an integer k such that $gcd(q^m - 1, k) = 1$. Let us describe in this section a method of generating the *two-dimensional sequence* of primitive polynomials as an extension of the one-dimensional sequence: A two-dimensional sequence is a sequence of primitive polynomials which is generated from a primitive polynomial f and two positive integers and has distinct primitive polynomials in a period.

In Table 1, we list all $\phi(2^8 - 1)/8 = 16$ primitive polynomials of degree 8: the table will be used as an example in the sequel.

primitive polynomials	Binary	Hexadecimal
$x^8+x^6+x^5+x+1$	1 0110 0011	163_H
$x^8+x^5+x^3+x+1$	1 0010 1011	$12b_H$
$x^8+x^7+x^6+x^5+x^4+x^2+x+1$	1 1111 0101	$1f5_H$
$x^8+x^6+x^5+x^4+1$	1 0111 0001	171_H
$x^8+x^5+x^3+x^2+1$	1 0010 1101	$12d_H$
$x^8+x^6+x^3+x^2+1$	1 0100 1101	$14d_H$
$x^8+x^7+x^6+x^3+x^2+x+1$	1 1100 1111	$1cf_H$
$x^8+x^7+x^6+x+1$	1 1100 0011	$1c3_H$
$x^8+x^7+x^6+x^5+x^2+x+1$	1 1110 0111	$1e7_H$
$x^8+x^7+x^2+x+1$	1 1000 0111	187_H
$x^8+x^7+x^3+x^2+x+1$	1 1000 1101	$18d_H$
$x^8+x^7+x^5+x^3+x+1$	1 1010 1001	$1a9_H$
$x^8+x^6+x^4+x^3+x^2+x+1$	1 0101 1111	$15f_H$
$x^8+x^4+x^3+x^2+1$	1 0001 1101	$11d_H$
$x^8+x^6+x^5+x^3+1$	1 0110 1001	169_H
$x^8+x^6+x^5+x^2+1$	1 0110 0101	165_H

Table 1. Primitive polynomials of degree 8

A. The two-dimensional sequence

Let $GF(q^m)$ be an extension of $GF(q)$ and let $\alpha \in GF(q^m)$. Then the elements $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ are called the *conjugates of α with respect to $GF(q)$* and have the same minimal polynomial [1].

Definition 2 *For two integers a and b, we say that b is the q^m conjugate of a or a and b are in the q^m conjugate relation, written $a \equiv_{q^m} b$, if*

$$a \equiv bq^i \pmod{q^m - 1}, \quad \text{for some integer } i. \tag{2}$$

Let β be an element of $GF(q^n)$, and a and b be two positive integers that are relatively prime to $q^m - 1$. If a and b are in the q^m conjugate relation, then β^a and β^b are conjugates with respect to $GF(q)$, and the polynomial generated from f with a and that from f with b are the same. Conversely, if the polynomial generated from f with a and that from f with b are the same, then a and b are in the q^m conjugate relation.

Theorem 3 ([3]) *For a positive integer k such that $gcd(k, q^m - 1) = 1$, let $K = \{k^i \mid 0 \le i < o(k)\}$. Then*

1) *An element in the set K is not in the q^m conjugate relation with any other element.*

2) *For any integer j, k^j is the q^m conjugate of $k^{j+o(k)n} \in K$ for some integer n.*

Lemma 1 *For integers a, b, c, d, and i, the following relations hold.*

1) *If $a \equiv_{q^m} b$, then $ac \equiv_{q^m} bc$.*

2) *If $a \equiv_{q^m} b$ and $b \equiv_{q^m} c$, then $a \equiv_{q^m} c$.*

3) *If $a \equiv_{q^m} b$ and $c \equiv_{q^m} d$, then $ac \equiv_{q^m} bd$.*

4) *If a and b are relatively prime to $q^m - 1$ and $a \equiv_{q^m} b$, then $a^i \equiv_{q^m} b^i$.*

5) *If $gcd(q^m - 1, k) = 1$, then $k^{o(k)} \equiv_{q^m} 1$.*

6) *If $gcd(q^m - 1, k) = 1$, and $k^a \equiv_{q^m} 1$, then $o(k)|a$.*

The proof of Lemma 1 is immediate from the definition of the q^m conjugate and Theorem 1.

Let $A = \{a_1, a_2, \ldots, a_n\}$ be a set of integers whose elements are relatively prime to $q^m - 1$. Let us denote by f-A the set of primitive polynomials generated from the primitive polynomial f with the elements of A: that is, f-$A = \{f_{a_1}, f_{a_2}, \ldots, f_{a_n}\}$. For two positive integers k and h that are relatively prime to $q^m - 1$, let $K = \{k^i \mid 0 \leq i < o(k)\}$ *and* $H = \{h^i \mid 0 \leq i < o(h)\}$. Then the $o(k)$ elements of f-K are distinct from each other due to 1) of Theorem 3. From 2) of Theorem 3, for an arbitrary integer i, the primitive polynomial generated from f with k^i is an element of f-K. However, the primitive polynomials generated from the elements of f-K with the elements of H may not be distinct from each other in general, because an element of K may be in the q^m conjugate relation with an element in H. In other words, the number of distinct primitive polynomials generated from f-K and elements of H is less than $o(k)o(h)$, if k^j and h^i are in the q^m conjugate relation for some i and j.

Example 1 *Let $q = 2$ and $m = 8$. Choose $k = 7$, $h = 13$, and $f(x) = x^8 + x^6 + x^5 + x + 1$ (The hexadecimal representation of a primitive polynomial will be used for convenience. For example, 163_H is the hexadecimal representation of $f(x)$.) Then $o(k) = 8$ and $o(h) = 4$. We see that the primitive polynomial generated from $f(x)$ with h^2 and that with k^4 are both $12d_H$, since $h^2 = 169$ and $k^4 = 2401$ are in the q^m conjugate relation (that is, $169 \equiv 2^2 \cdot 2401 (mod\ 2^8 - 1)$).* □

Theorem 4 tells us a necessary condition for the two elements $h^i \in H$ and $k^j \in K$ to be in the q^m conjugate relation.

Theorem 4 *Let k and h be two positive integers that are relatively prime to $q^m - 1$, and $d = gcd(o(k), o(h))$. If*

$$k^i \equiv_{q^m} h^j, \tag{3}$$

then i is a multiple of $o(k)/d$ and j is a multiple of $o(h)/d$.

Proof: Since $d = gcd(o(k), o(h))$, we may write $o(k) = ud$ and $o(h) = vd$, where v and u are relatively prime. Exponentiating both sides of (3) by $o(k)$, we have $k^{o(k)i} \equiv_{q^m} h^{o(k)j}$. Since $k^{o(k)i} \equiv_{q^m} 1$ from Lemma 1, $h^{o(k)j} \equiv_{q^m} 1$. Thus from 6) of Lemma 1, $o(h)|o(k)j$ and $vd|udj$; that is, $v|uj$. Since $gcd(v, u) = 1$, we finally have $v|j$, or equivalently, j is a multiple of $o(h)/d$ as desired.

Exponentiating both sides of (3) by $o(h)$ and applying a similar procedure, we can prove that i is a multiple of $o(k)/d$. □

Figure 3 illustrates Theorem 4.

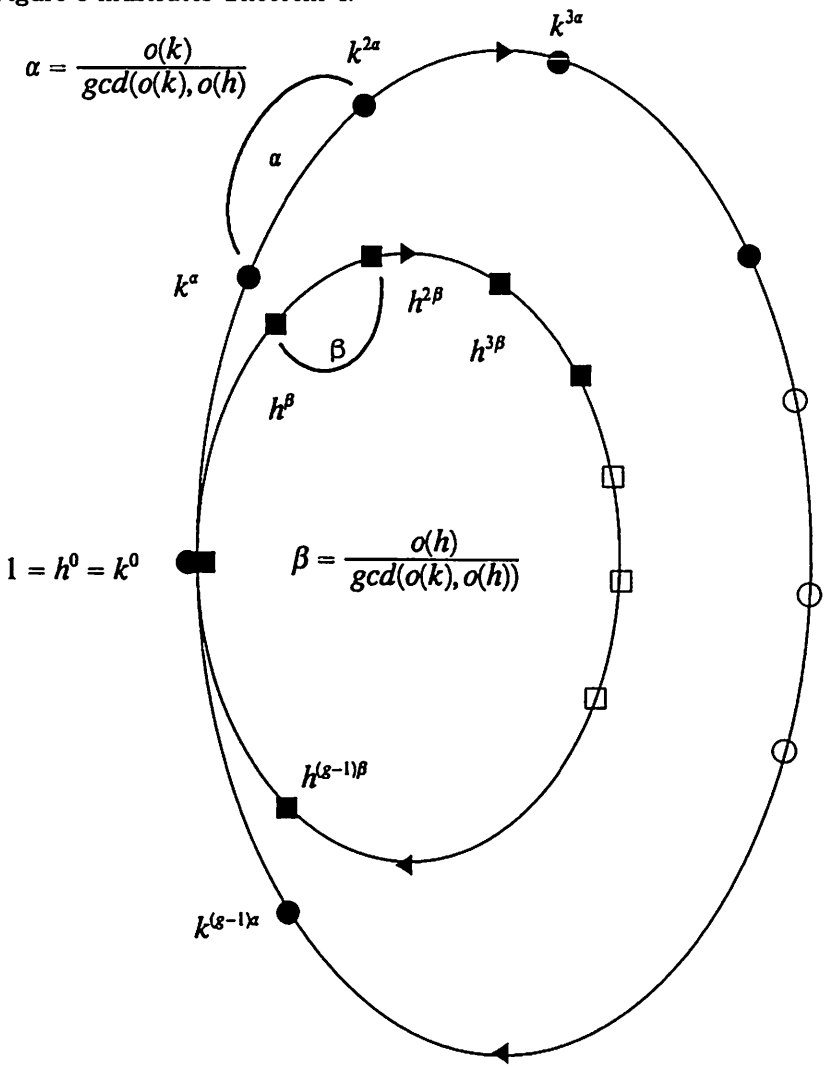

Figure 3. Possible i and j such that $k^i \equiv_{q^m} h^j$

Let us next find the distribution of h^j which is in the q^m conjugate relation with k^i.

Theorem 5 *For two positive integers k and h that are relatively prime to $q^m - 1$, let*

$$K = \{k^i \mid 0 \leq i < o(k)\} \tag{4}$$

and

$$H_K = \{h^i \mid 0 \leq i < o(h), \textit{the } q^m \textit{ conjugate of } h^i \textit{ must be in } K\}. \tag{5}$$

Then there exists a divisor a of $o(h)$ such that

$$H_K = \{h^{ai} \mid 0 \leq ai < o(h), i \textit{ is a nonnegative integer}\}. \tag{6}$$

Proof: Let b be the smallest nonzero exponent of the elements in H_K. We define

$$A = \{h^{bi} \mid 0 \leq bi < o(h),\ i \textit{ is a nonnegative integer}\}. \tag{7}$$

Then it is sufficient to show that b is a divisor of $o(h)$ and A is equal to H_K.

Let $o(h) = bQ + r$ for two integers Q and r, where $0 \leq r < b$. Then we have $h^r \equiv_{q^m} h^{-bQ}$, since $h^{o(h)} = h^{bQ+r} = h^{bQ}h^r$ and $h^{o(h)} \equiv_{q^m} 1$. Next, since h^b is an element of H_K, we have $h^b \equiv_{q^m} k^j$ for some integer j, from which we get $h^{-bQ} \equiv_{q^m} k^{-jQ}$. Thus h^r is an element of H_K, since k^{-jQ} is the q^m conjugate of an element in K from Theorem 3. Therefore, it follows that $r = 0$ from the minimality of b. This means b is a divisor of $o(h)$.

Let us next show that $A = H_K$ by showing $A \subseteq H_K$ and $A \supseteq H_K$. Since h^b is an element of H_K, so is h^{bi} for an integer i; that is, A is a subset of H_K. Let $c = bR + s, 0 \leq s < b$. Then we have $h^s = h^c h^{-bR}$, since $h^c = h^{bR+s} = h^{bR}h^s$. Next, since h^b is an element of H_K, $h^b \equiv_{q^m} k^j$ for some integer j, or $h^{-bR} \equiv_{q^m} k^{-jR}$. Since h^c and $h^{-bR} \equiv_{q^m} k^{-jR}$ are the q^m conjugates of some elements in K, so is h^s. Thus we must have $s = 0$, or $s = bR$, from the minimality of b. This concludes $h^c \in A$. □

Definition 3 *For two positive integers h and k that are relatively prime to $q^m - 1$, the q^m conjugate order of h with respect to k, denoted by $o(h)_k$, is the least positive integer z such that*

$$h^z \equiv q^i k^j \ (mod\ q^m - 1), \quad \textit{for some integers } i, j. \tag{8}$$

It is easily found from the proof of Theorem 5 that $o(h)_k$ is the number a described in Theorem 5. Therefore we know from Theorem 4 that $o(h)_k$ is a multiple of $o(h)/d$ and a divisor of $o(h)$, where $d = gcd(o(k), o(h))$.

Theorem 6 *For two positive integers h and k that are relatively prime to $q^m - 1$, let $G(h,k) = \{h^i k^j \mid 0 \le i < o(h)_k,\ 0 \le j < o(k)\}$. Then no two elements in the set $G(h,k)$ are in the q^m conjugate relation.*

Proof: Let $a = h^i k^j$ and $b = h^u k^v$ be two elements of $G(h,k)$. Suppose that a and b are distinct and in the q^m conjugate relation, or equivalently

$$h^i k^j \equiv_{q^m} h^u k^v. \tag{9}$$

Case 1: $i = u$. By rewriting (9), we have $k^{j-v} \equiv_{q^m} 1$, and $-o(k) < j - v < o(k)$. Since $o(k) | (j - v)$ from 6) of Lemma 1, $j = v$, and $a = b$, which is a contradiction.

Case 2: $i > u$. We have $0 < i - u < o(h)_k$, and (9) becomes $h^{i-u} \equiv_{q^m} k^{v-j}$. This contradicts the definition of $o(h)_k$.

Case 3: $i < u$. A contradiction can be established as in Case 2.

Therefore, no two elements in $G(h,k)$ are in the q^m conjugate relation. □

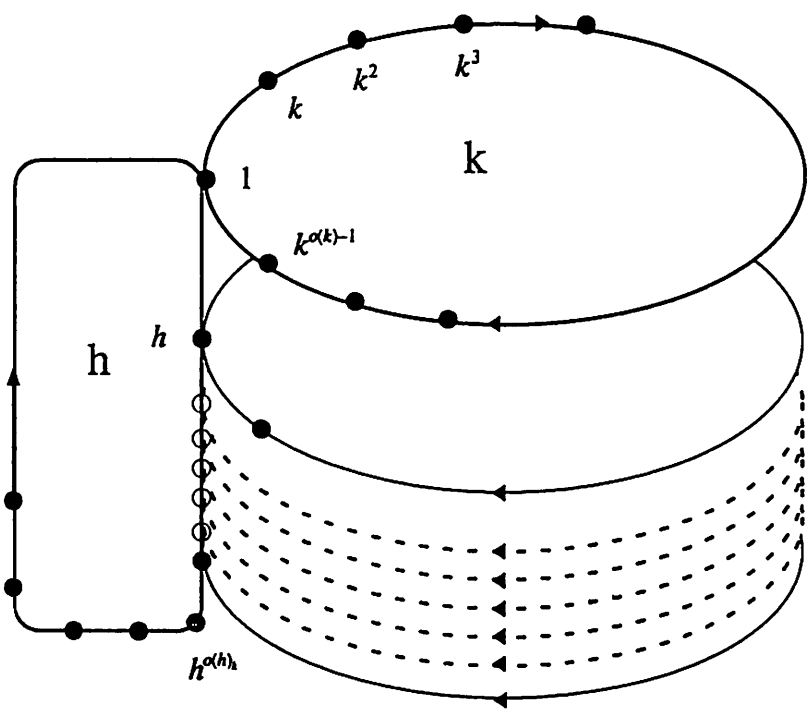

Figure 4.
The two-dimensional sequence of $o(k)o(h)_k$ primitive polynomials

The number of elements in $G(h,k)$ is $o(h)_k o(k)$. Since no two elements are in the q^m conjugate relation in $G(h,k)$ by Theorem 6, a primitive polynomial sequence of length $o(h)_k o(k)$ will be generated from an arbitrary primitive polynomial and the elements in $G(h,k)$. This sequence of primitive polynomials constitutes the two-dimensional sequence as shown in Figure 4, where the points on the $o(h)_k$ circles represent the elements in $G(h,k)$. Figure 4 also shows a practical way to obtain the two-dimensional sequence: for $h^i, i = 0, 1, \ldots, o(h)_k - 1$, we get $o(k)$ primitive polynomials from a primitive polynomial f with $k^0, k^1, \ldots, k^{o(h)-1}$.

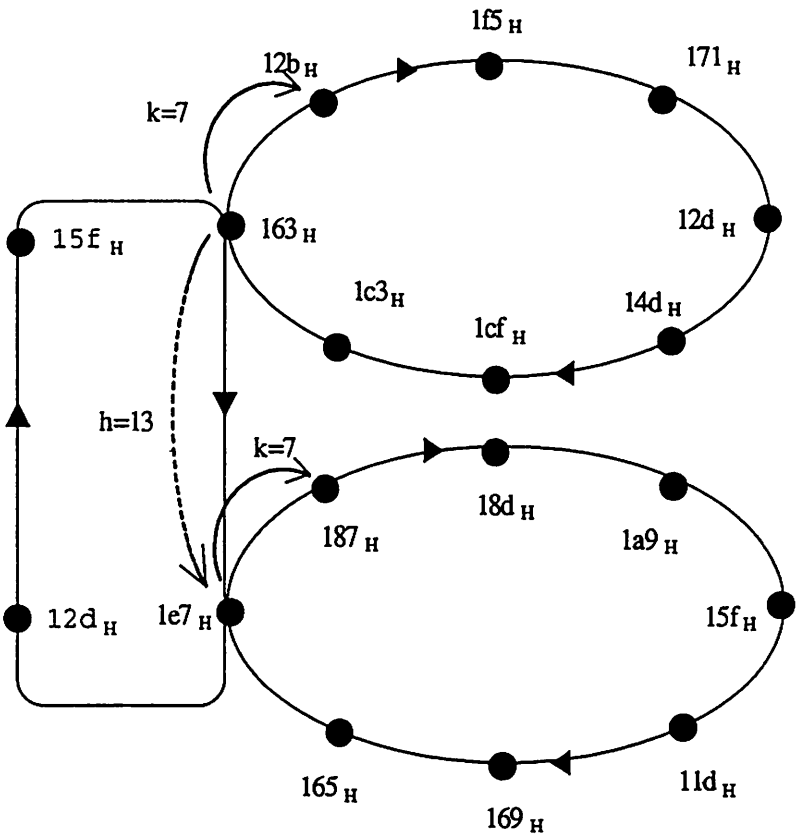

Figure 5. An example of the two-dimensional sequence of 8×2 primitive polynomials of degree 8 over GF(2) for $k = 7$ and $h = 13$

Example 2 *Let $q = 2, m = 8, k = 7, h = 13$, and $f(x) = x^8 + x^6 + x^5 + x + 1$ $(=163_H)$. Then $o(k) = 8$ and $o(h)_k = 2$. The one-dimensional sequence generated from 163_H with k is $\{163_H, 12b_H, 1f5_H, 171_H, 12d_H, 14d_H, 1cf_H, 1c3_H\}$ and the two-dimensional sequence generated from 163_H with*

$k = 7$ and $h = 13$ is $\{163_H, 12b_H, 1f5_H, 171_H, 12d_H, 14d_H, 1cf_H, 1c3_H, 1e7_H, 187_H, 18d_H, 1a9_H, 15f_H, 11d_H, 169_H, 165_H\}$ as shown in Figure 5. Because we have all the primitive polynomials of degree 8, we need not generate further primitive polynomials from $12d_H$ or $15f_H$. □

Now let us show that a two-dimensional sequence can be obtained by exchanging h and k.

Theorem 7 *Given a primitive polynomial f and two positive integers h and k that are relatively prime to $q^m - 1$, let*

$$G'(h,k) = \{h^i k^j \mid 0 \le i < o(h),\ 0 \le j < o(k)\}, \tag{10}$$

and

$$G(h,k) = \{h^i k^j \mid 0 \le i < o(h)_k,\ 0 \le j < o(k)\}. \tag{11}$$

Then f-$G(h,k)$ and f-$G'(h,k)$ are the same set.

Proof: All we have to show is that the primitive polynomials generated from f with an element of $G'(h,k)$ for $o(h)_k \le i < o(h)$ are redundant ones. For $a \ge o(h)_k$, we may write $a = o(h)_k Q + r$ with $0 \le r < o(h)_k$. Then we have $h^a \equiv_{q^m} k^{jQ} h^r$, since $h^a = h^{o(h)_k Q + r}$ and $h^{o(h)_k} \equiv_{q^m} k^j$ by the definition of $o(h)_k$. Thus h^a is the q^m conjugate of an element in $G(h,k)$, and the primitive polynomial generated from f with h^a is an element of f-$G(h,k)$.

Note that we have f-$G(h,k) = f$-$G(k,h)$, since f-$G(h,k) = f$-$G'(h,k)$ and f-$G'(h,k) = f$-$G(k,h)$ from Theorem 7.

Corollary 1 *For two positive integers h and k that are relatively prime to $q^m - 1$,*

$$o(h)_k o(k) = o(k)_h o(h). \tag{12}$$

Eq. (12) is the period of a two-dimensional sequence of primitive polynomials. Figures 4 and 6 show the relation (12). Figure 7 is an example of the two-dimensional sequence generated from the primitive polynomial 163_H as in Figure 5 with k and h exchanged.

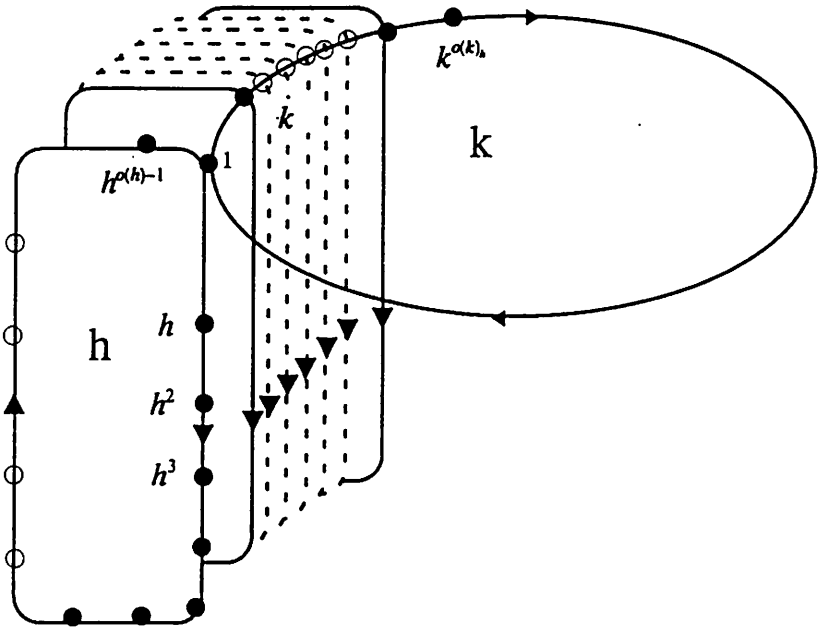

Figure 6.
The two-dimensional sequence of $o(h)o(k)_h$ primitive polynomials

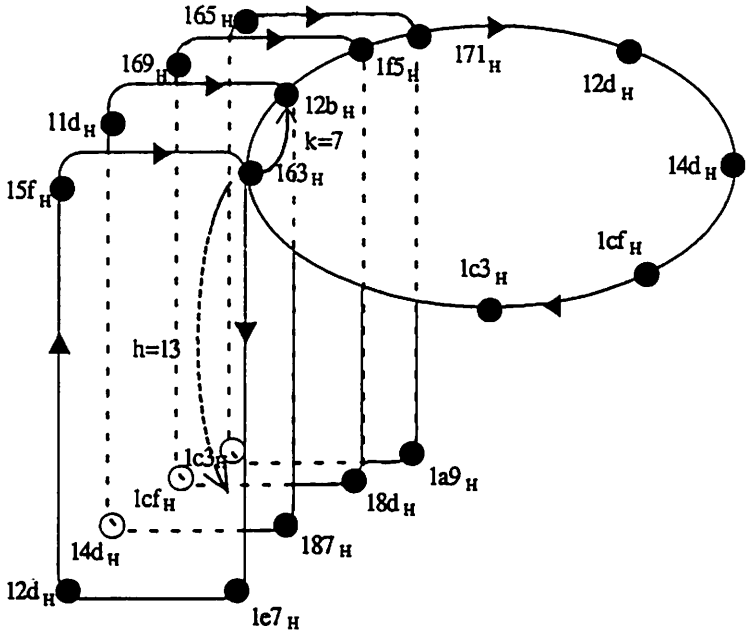

Figure 7. An example of the two-dimensional sequence of 4×4 primitive polynomials of degree 8 over $GF(2)$ for $h = 13$ and $k = 7$.

B. Computing the period

It is well-known that the number of primitive polynomials of degree m is $\phi(q^m-1)/m$ [1]. From Theorem 6 the number of primitive polynomials in f-$G(h,k)$ is $o(h)_k o(k)$. Thus we can determine all the primitive polynomials of degree m, if we find two positive integers h and k such that

$$o(h)_k o(k) = \phi(q^m-1)/m. \tag{13}$$

Let us describe a method for finding h and k satisfying (13). Factorization of q^m-1 required to compute $\phi(q^m-1)$ can be accomplished as in [4], and $o(k)$ can be found using the algorithm considered in [3]. Here we obtain an explicit method for computing $o(h)_k$.

Theorem 8 *For two positive integers h and k that are relatively prime to q^m-1, if*

$$h^i \equiv_{q^m} k^j, \tag{14}$$

then

$$gcd(id/o(h), d) = gcd(jd/o(k), d), \tag{15}$$

where $d = gcd(o(h), o(k))$.

Proof: From $d = gcd(o(h), o(k))$ we have $o(h) = ud$ and $o(k) = vd$ for two integers u and v that are relatively prime. From Theorem 4 we may write $i = su$ and $j = tv$ for some integers s and t. Thus we have to show $gcd(s,d) = gcd(t,d)$.

1) Let $w = gcd(s,d)$. Then we have $s = wa$ and $d = wb$ for two integers a and b. Exponentiating both sides of (14) by b, we obtain $h^{aud} \equiv_{q^m} k^{tvb}$, or $h^{o(h)a} \equiv_{q^m} k^{tvb}$ so that $k^{tvb} \equiv_{q^m} 1$ from 5) of Lemma 1. Thus we have $o(k)|tvb$, $vd|tvb$, $vwb|tvb$, or $w|t$ from 6) of Lemma 1. Since $w|t$ and $w|d$, we have $w|gcd(t,d)$, or $gcd(s,d)|gcd(t,d)$.

2) Letting $z = gcd(t,d)$ and applying a similar procedure as above, we can easily show $gcd(t,d)|gcd(s,d)$.

The results 1) and 2) imply $gcd(s,d) = gcd(t,d)$ as desired. □

Example 3 *Let $q = 2$, $m = 8$, $k = 7$, and $h = 13$. Then $o(k) = 8$, $o(h) = 4$, and $g = gcd(o(h), o(k)) = 4$. Let $i = 2$ and $j = 4$. Then we have $gcd(2 \cdot 4/8) = gcd(4 \cdot 4/8)$, noting that $169 \equiv 2^2 \cdot 2401 (mod\ 2^8-1)$. Now we take $j = 3$. Then $gcd(2 \cdot 4/8) \neq gcd(3 \cdot 4/8)$. This shows that for given i and j we can easily check if $h^i \equiv_{q^m} k^j$. (More precisely, in order to show i and j do not satisfy (14), it is easier to show that (15) is not satisfied for the same i and j.)* □

For two positive integers h and k that are relatively prime, let $d = gcd(o(h), o(k))$, then $o(h) = ud$ and $o(k) = vd$. Then $o(h)_k$ is a multiple of u from Theorem 4, and is a divisor of $o(h)$ from Theorem 5. Let $o(h)_k = nu$ for an integer n, then $n|d$, since $o(h)_k|o(h)$. From Theorem 8, $gcd(i/u, d) = gcd(j/v, d)$, or $n = gcd(j/v, d)$. Thus we have the following Corollary.

Corollary 2 *For two positive integers h and k that are relatively prime to $q^m - 1$, let $d = gcd(o(h), o(k))$. If $h^{o(h)_k} \equiv_{q^m} k^j$ then $n = gcd(jd/o(k), d)$, where $o(h)_k = n \cdot o(h)/d$.*

Theorem 9 *For two positive integers h and k that are relatively prime to $q^m - 1$, let $d = gcd(o(h), o(k))$, $o(h) = du$, $o(k) = dv$, and $o(h)_k = nu$. Then for a factor a of d and some integer j, there exist an integer l, $0 \leq l < g$, and a prime factor p of a such that $h^{au/p} \equiv_{q^m} k^{lv}$, if $h^{au} \equiv_{q^m} k^{jv}$ and $au \neq o(h)_k$.*

Proof: Since $h^{au} \equiv_{q^m} k^{jv}$, we have from Theorem 5 $o(h)_k|au$, $nu|au$, or $n|a$. Since $au \neq o(h)_k$, we get $a/n \neq 1$, so that a/n must have a prime factor p, $p \neq 1$.

Let $c = a/(np)$. Then $a/p = nc$, $au/p = ncu$, or $au/p = o(h)_k c$. Therefore from Theorem 5 there exists an integer l such that $h^{au/p} \equiv_{q^m} k^{lv} (0 \leq l < g)$. □

Taking the contraposition of Theorem 9, we reach the final result for computing $o(h)_k$ as follows.

Corollary 3 *For two positive integers h and k that are relatively prime to $q^m - 1$, let $d = gcd(o(h), o(k))$, $o(h) = du$, $o(k) = dv$, and $o(h)_k = nu$. Suppose there exist an integer j and a factor a of d such that $h^{au} \equiv_{q^m} k^{jv}$. If $h^{au/p} \not\equiv_{q^m} k^{lv}$, for any prime factor p of a and any integer l, then $au = o(h)_k$.*

So far we have shown that we can obtain the two-dimensional sequences of primitive polynomials by computing $o(h)_k$. For three integers h, k, and t that are relatively prime to $q^m - 1$, we can similarly generate the 3-dimensional sequences if we first find the smallest t^i which is the q^m conjugate of an element of $G(h, k)$ defined in Theorem 7. (Of course, higher dimensional sequences may similarly be generated.)

C. Examples

We have computed the longest period of the one-dimensional sequence for each pair (q, m) by allowing k to change from 3 to 99: when $q = 2$ the

number of pairs (q, m) is 119 since $3 \leq m \leq 121$, and when $q = 3$ the number is 23 since $3 \leq m \leq 25$. We used Algorithm-P [3] to compute the periods. In Table 2, we listed the values of k, for which the longest periods of the one-dimensional sequences are equal to $\phi(q^m - 1)/m$. In the table, a missing value set $\{q, m,$ period, $k\}$ means that there does not exist a value of $k \in [3, 99]$ for which the sequence period is maximum.

q	m	Period	k
2	4	2	7
2	5	6	3
2	6	6	5
2	7	18	3
2	13	630	17
2	17	7710	3
2	19	26594	3
2	31	69273666	7
2	61	37800705069076950	37
3	7	156	5
3	13	61320	17
3	17	379610	7

Table 2. Some values of k for which the period of the one-dimensional sequence is maximum.

Some values of h and k for which the period of the two-dimensional sequence equals to $\phi(q^m - 1)/m$ are shown in Table 3, which are obtained for the same ranges of q, m, and k as above and $3 \leq h \leq 51$. The values of k are taken from the result of the one-dimensional sequence: that is, we choose the value k for which the one-dimensional sequence has the longest period for given (q, m). Theorem 9 is used to calculate the periods.

q	m	k	h	$o(k)$	$o(h)_k$	$o(k) \times o(h)_k$
2	10	5	13	30	2	60
2	11	3	5	88	2	176
2	14	7	5	126	6	756
2	23	3	5	178480	2	356960
2	25	11	7	1800	120	129600
2	26	7	5	8190	210	171900
2	34	5	13	131070	2570	336849900
2	38	5	11	524268	9198	4822382628
3	11	5	7	3850	2	7700
3	17	7	23	379610	10	3796100
3	19	13	5	36388	84	30566592

Table 3. Some values of h and k for which the period of the two-dimensional sequence is maximum.

4 Conclusion

The two-dimensional sequence of primitive polynomials has been described by introducing the concept of the q^m conjugate order: the two-dimensional sequence can be extended to higher dimensional case. Using the two-dimensional sequences, we can find maximum period primitive polynomial sequences for more values of degrees than using the one-dimensional sequences.

The distribution of the number of terms of primitive polynomials in the sequence and a new method to test the primitivity of a primitive polynomial based on the result of this paper are under consideration.

Acknowledgements

This research was supported in part by the Ministry of Information and Communications under a Grant from the University Basic Research Fund, for which the authors would like to express their thanks.

References

[1] R. Lidi and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge: Cambridge University Press, 1986.

[2] A. Di Porto, F. Guida, and E. Montolivo, Fast algorithm for finding primitive polynomials over $GF(q)$, *Electron. Lett.*, **Vol. 28**, Jan. 1992, pp. 118–120.

[3] B. Park, H. Choi, T. Chang, and K. Kang, Period of sequences of primitive polynomials, *Electron. Lett.*, **Vol. 29**, Feb. 1993, pp. 390–391.

[4] J. Brillhart, D.H. Selfdidge, J.L. Tuckerman, and S.S.J. Wagstaff, *Contemporary Mathematics, Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 7, 11, 13$ *up to High Powers*, Providence: American Mathematical Society Press, 1983.