Binary sequences derived from monomial permutation polynomials over GF(2^p)*

Qun-Xiong Zheng[1,2] Yupeng Jiang[3], Dongdai Lin[2], and Wen-Feng Qi[1]

[1] PLA Strategic Support Force Information Engineering University, Zhengzhou, 450001, China.
[2] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 100093, China.
[3] School of Cyber Science and Technology, Beihang University, Beijing 100191, China

Abstract. Let 2^p-1 be a Mersenne prime and e a primitive root modulo 2^p-1. Let $f=x^e$ be a monomial permutation polynomial over the finite field GF(2^p) and let $\underline{a}=(a,f(a),f^2(a),\ldots)$ be a sequence over GF(2^p) induced by f, where f^t is the t-fold composition of f for $t\geq 1$. Given a basis of GF(2^p) over GF(2), say $\{\alpha_0,\alpha_1,\ldots,\alpha_{p-1}\}$, if we write each $f^t(a)$, $t\geq 0$, in its unique representation as

$$f^t(a)=[f^t(a)]_0\cdot\alpha_0+[f^t(a)]_1\cdot\alpha_1+\cdots+[f^t(a)]_{p-1}\cdot\alpha_{p-1},$$

where $[f^t(a)]_i\in$ GF(2) for $0\leq i\leq p-1$, then we can simultaneously obtain p binary sequences $[\underline{a}]_0,[\underline{a}]_1,\ldots,[\underline{a}]_{p-1}$, where

$$[\underline{a}]_i=([a]_i,[f(a)]_i,[f^2(a)]_i,\ldots)\text{ for }0\leq i\leq p-1.$$

In this paper, the periodic property and the shift-equivalence of binary sequences described above are studied. Let $\{\beta_0,\beta_1,\ldots,\beta_{p-1}\}$ be the dual basis of $\{\alpha_0,\alpha_1,\ldots,\alpha_{p-1}\}$. It is shown that per $([\underline{a}]_i)=2^p-2$ if and only if $\beta_i\neq 1$; and per $([\underline{a}]_i)=(2^p-2)/p$ if and only if $\beta_i=1$, where per $([\underline{a}]_i)$ is the period of $[\underline{a}]_i$. Moreover, for $0\leq i<j\leq p-1$, it is shown that $[\underline{a}]_i=L^s[\underline{a}]_j$ for some positive integer s if and only if $\beta_j=\beta_i^{2^k}$ and $e^s\equiv 2^k \bmod 2^p-1$ for some $0\leq k\leq p-1$, where $L^s[\underline{a}]_j$ is the s-shift of $[\underline{a}]_j$. In addition, two special results are given if the basis of GF(2^p) over GF(2) is chosen to be a normal basis.

Keywords: Mersenne prime, Permutation polynomial, Pseudorandom sequence, Periodicity, Shift equivalence.

* This work was supported by NSF of China (Nos. 61872383). The work of Qun-Xiong Zheng was also supported by Young Elite Scientists Sponsorship Program by CAST (2016QNRC001) and by National Postdoctoral Program for Innovative Talents (BX201600188) and by China Postdoctoral Science Foundation funded project (2017M611035). Emails: qunxiong_zheng@163.com, jiangyupeng@amss.ac.cn, ddlin@iie.ac.cn, wenfeng.qi@263.net

1 Introduction

Pseudo-random number generators (PRNGs) are widely used in cryptography, communication, statistical sampling, Monte Carlo simulation, etc. Different applications have different requirements for PRNGs. For the application of stream ciphers, it is usually required that a PRNG should have a sufficiently large period, as well as a "good" nonlinear structure in order to effectively resist correlation attacks and algebraic attacks. Nonlinear feedback shift registers (NFSRs) are a most popular PRNGs for stream cipher design. However, some critical properties of NFSRs, such as the periodic properties, are still hard to be analyzed. In this paper, we propose a new PRNG based on permutation polynomials of finite fields. Our main idea is first to generate sequences with controllable periods by a suitable permutation polynomial over finite fields, and then to prove that the induced coordinate sequences also have sufficiently large periods. The nonlinear iterative approach naturally imply that the induced coordinate sequences are nonlinear. More importantly, since there are many choices of bases for a finite field, a variety of coordinate sequences can be derived.

Let $\mathrm{GF}(2^n)$ be a finite field with 2^n elements. A polynomial $f \in \mathrm{GF}(2^n)[x]$ is called a permutation polynomial of $\mathrm{GF}(2^n)$ if the associated mapping $x \mapsto f(x)$ from $\mathrm{GF}(2^n)$ into $\mathrm{GF}(2^n)$ is a permutation of $\mathrm{GF}(2^n)$. It is well-known that the monomial polynomial x^e is a permutation polynomial of $\mathrm{GF}(2^n)$ if and only if $\gcd(e, 2^n - 1) = 1$. Permutation polynomials have wide applications in many areas of mathematics and engineering such as coding theory, cryptography and combinatorial designs. We refer the reader to [1, Ch.7], [2, Ch.8], [3] and the references therein for a detailed exposition of permutation polynomials. We also refer the reader to [4,5,6] for some constructions of permutation polynomials. For some recent advances such as complete permutation polynomials over finite fields, [7,8,9] are recommended.

Let f be a permutation polynomial of $\mathrm{GF}(2^n)$. Given an initial value $a \in \mathrm{GF}(2^n)$, one can obtain a sequence $\underline{a} = (a, f(a), f^2(a), \ldots)$ over $\mathrm{GF}(2^n)$, where $f^t(a) = f(f^{t-1}(a))$ for any integer $t \geq 1$ and $f^0(a) = a$. For convenience, we say that $\underline{a}$ is a sequence induced by f with a being the initial value. If there exists a positive integer T such that $f^T(a) = a$, then $\underline{a}$ is called a **periodic sequence**. The minimum of such T is called the period of $\underline{a}$ and is denoted by $\mathrm{per}(\underline{a})$. Because of the fact that the associated mapping $x \mapsto f(x)$ from $\mathrm{GF}(2^n)$ into $\mathrm{GF}(2^n)$ is a bijection of $\mathrm{GF}(2^n)$, any sequence induced by f is periodic.

Let $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ be a basis of $\mathrm{GF}(2^n)$ over $\mathrm{GF}(2)$. Each element $a \in \mathrm{GF}(2^n)$ can be uniquely represented as

$$a = [a]_0 \cdot \alpha_0 + [a]_1 \cdot \alpha_1 + \cdots + [a]_{n-1} \cdot \alpha_{n-1} \text{ with } [a]_i \in \mathrm{GF}(2) \text{ for } 0 \leq i \leq n-1,$$

where $[a]_i$ is called the i-th coordinate of a w.r.t. $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$. Let

$$\underline{a} = (a, f(a), f^2(a), \ldots)$$

be a sequence over $\mathrm{GF}(2^n)$. If each $f^t(a)$, $t \geq 0$, is uniquely represented as

$$f^t(a) = [f^t(a)]_0 \cdot \alpha_0 + [f^t(a)]_1 \cdot \alpha_1 + \cdots + [f^t(a)]_{n-1} \cdot \alpha_{n-1},$$

where $[f^t(a)]_i \in \mathrm{GF}(2)$ for $0 \le i \le n-1$, then one can simultaneously obtain n binary sequences $[\underline{a}]_0, [\underline{a}]_1, \ldots, [\underline{a}]_{n-1}$, where

$$[\underline{a}]_i = ([a]_i, [f(a)]_i, [f^2(a)]_i, \ldots) \text{ for } 0 \le i \le n-1.$$

For convenience, $[\underline{a}]_i$ is called the **i-th coordinate sequence** of $\underline{a}$ w.r.t. $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$. The idea of using permutation polynomials to derive coordinate sequences can be traced back to Niederreiter [10], where pseudorandom vectors are generated by the inversive method. The method of using coordinate vectors to describe pseudorandom numbers is driven by paralleized simulation methods. For details of applications in paralleized simulation methods, Anderson [11], Bhavsar and Isaac [12], and Eddy [13] are recommended. It is worth noticing that the period of each coordinate sequence strictly divides the period of the original sequence. Then a natural problem has arisen—that is, if $\underline{a}$ is a sequence induced by a nonlinear permutation polynomial f with period large enough, do all of its coordinate sequences have period large enough? In particular, all have the same period as $\underline{a}$. If so, these coordinate sequences may be of potential interest to many applications, such as the design of stream ciphers, since it is a challenging work to design nonlinear sequences with controllable periods. However, the above problem is of independent interest in theory, regardless of its potential applications.

In this paper, we focus ourself on the monomial permutation polynomials over $\mathrm{GF}(2^n)$. Let $f = x^e$ be a monomial permutation polynomial over $\mathrm{GF}(2^n)$ and let $\underline{a} = (a, f(a), f^2(a), \ldots)$ be a sequence over $\mathrm{GF}(2^n)$ induced by f. It is easy to see that the maximum possible period for $\underline{a}$ is $2^n - 2$. If $\mathrm{per}\,(\underline{a}) = 2^n - 2$, then $\underline{a}$ is called an MLM-sequence (maximal length monomial sequence). Firstly, it is shown that $\underline{a}$ is an MLM-sequence if and only if $2^n - 1$ is a Mersenne prime and e is a primitive root modulo $2^n - 1$. Secondly, the periods of coordinate sequences of an MLM-sequence $\underline{a}$ are studied. Let $[\underline{a}]_0, [\underline{a}]_1, \ldots, [\underline{a}]_{n-1}$ be n binary coordinate sequences of $\underline{a}$ w.r.t. a given basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ of $\mathrm{GF}(2^n)$ over $\mathrm{GF}(2)$. It is shown that $\mathrm{per}\,([\underline{a}]_i) = 2^n - 2$ if and only if $\beta_i \ne 1$; and $\mathrm{per}\,([\underline{a}]_i) = (2^n - 2)/n$ if and only if $\beta_i = 1$, where $1 \le i \le n$ and $\{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$ is the dual basis of $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$. In particular, $\mathrm{per}\,([\underline{a}]_0) = \mathrm{per}\,([\underline{a}]_1) = \cdots = \mathrm{per}\,([\underline{a}]_{n-1}) = 2^n - 2$ if $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ is chosen to be a normal basis of $\mathrm{GF}(2^n)$ over $\mathrm{GF}(2)$. Finally, the shift-equivalence of $[\underline{a}]_0, [\underline{a}]_1, \ldots, [\underline{a}]_{n-1}$ is further studied. For $0 \le i < j \le n-1$, it is shown that $[\underline{a}]_i = L^s[\underline{a}]_j$ for some positive integer s if and only if $\beta_j = \beta_i^{2^k}$ and $e^s \equiv 2^k \bmod 2^n - 1$ for some $0 \le k \le n-1$, where $L^s[\underline{a}]_j$ is the s-shift of $[\underline{a}]_j$. Particularly, if $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ is chosen to be a normal basis of $\mathrm{GF}(2^n)$ over $\mathrm{GF}(2)$, then there always exists a positive integer $s_j = u_j(2^n - 2)/n$ with $1 \le u_j \le n-1$ such that $[\underline{a}]_0 = L^{s_j}[\underline{a}]_j$. Moreover, $s_1, s_s, \ldots, s_{n-1}$ run exactly through the set $\{(2^n - 2)/n, 2(2^n - 2)/n, \ldots, (n-1)(2^n - 2)/n\}$.

The rest of this paper is organized as follows. In Sect. 2, we first recall the definition of dual bases and their basic properties, and then we give a necessary and sufficient condition for MLM-sequences. In Sect. 3, we study the periodicity and the shift-equivalence of coordinate sequences derived from MLM-sequences. Finally, we conclude this paper in Sect. 4.

2 Preliminaries

2.1 Dual bases

Let $n > 1$ and let $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ and $\{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$ be two bases of $\mathrm{GF}(2^n)$ over $\mathrm{GF}(2)$. Then $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ and $\{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$ are said to be dual bases if for $0 \le i, j \le n-1$ we have

$$\mathrm{Tr}(\alpha_i \beta_j) = \begin{cases} 0 \text{ if } i \neq j, \\ 1 \text{ if } i = j, \end{cases}$$

where $\mathrm{Tr}(y) = y + y^2 + \cdots + y^{2^{n-1}}$ is the trace function from $\mathrm{GF}(2^n)$ to $\mathrm{GF}(2)$. It is known that given a basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ of $\mathrm{GF}(2^n)$ over $\mathrm{GF}(2)$, its dual basis $\{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$ always exists and is uniquely determined by $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$. Moreover, for $0 \le i \le n-1$, it is easy to check that

$$[y]_i = \mathrm{Tr}(\beta_i y) \text{ for all } y \in \mathrm{GF}(2^n), \tag{1}$$

where $[y]_i$ is the i-th coordinate of y w.r.t. $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$. For more details of dual bases, we refer to [1].

2.2 Maximal length monomial sequences

Let n be an integer greater than 1 and e a positive integer coprime with $2^n - 1$. Let $f = x^e$ be a monomial permutation polynomial over $\mathrm{GF}(2^n)$ and $\underline{a} = (a, f(a), f^2(a), \ldots)$ a sequence over $\mathrm{GF}(2^n)$ induced by f. It is clear that $\underline{a}$ is an all-zero sequence with $\mathrm{per}\,(\underline{a}) = 1$ if $a = 0$; and $\underline{a}$ is an all-one sequence with $\mathrm{per}\,(\underline{a}) = 1$ if $a = 1$; and $\underline{a}$ is a periodic sequence with $\mathrm{per}\,(\underline{a}) \le 2^n - 2$ if $a \in \mathrm{GF}(2^n) \backslash \{0, 1\}$.

Definition 1. *(MLM-sequences) Let $f = x^e$ be a monomial permutation polynomial over $\mathrm{GF}(2^n)$, where e is a positive integer coprime with $2^n - 1$. Let $\underline{a} = (a, f(a), f^2(a), \ldots)$ be a sequence over $\mathrm{GF}(2^n)$ induced by f. If $\mathrm{per}\,(\underline{a}) = 2^n - 2$, then $\underline{a}$ is called a maximal length monomial sequence (called MLM-sequence in short).*

Remark 1. If $a \notin \{0, 1\}$, then $f^t(a) = a^{e^t} \notin \{0, 1\}$ for any integer $t \ge 0$. Therefore, $a, f(a), f^2(a), \ldots f^{2^n-3}(a)$ run exactly through the set $\mathrm{GF}(2^n) \backslash \{0, 1\}$ if $\underline{a}$ is an MLM-sequence over $\mathrm{GF}(2^n)$.

We recall that a prime number of the form $2^n - 1$ is called a Mersenne prime. It is necessary that n is prime if $2^n - 1$ is a Mersenne prime. We also recall that a positive integer e coprime to $2^n - 1$ is called a **primitive root** modulo $2^n - 1$, if the multiplicative order of e modulo $2^n - 1$ (the smallest positive integer k with $e^k \equiv 1 \bmod 2^n - 1$) is equal to $\varphi(2^n - 1)$, where $\varphi(\cdot)$ is the Euler's totient function. There are totally $\varphi(\varphi(2^n - 1))$ primitive roots modulo $2^n - 1$ for $1 < e < 2^n - 1$.

Next we will give a necessary and sufficient condition for MLM-sequences.

Theorem 1. *Let $f = x^e$ be a monomial permutation polynomial over* $\mathrm{GF}(2^n)$*, where e is a positive integer coprime with $2^n - 1$. Let $a \in \mathrm{GF}(2^n)\backslash\{0,1\}$. Then $\underline{a} = (a, f(a), f^2(a), \ldots)$ is an MLM-sequence over* $\mathrm{GF}(2^n)$ *if and only if $2^n - 1$ is a Mersenne prime and e is a primitive root modulo $2^n - 1$.*

Proof. ($\Leftarrow$) We note that $f^t(a) = a^{e^t}$ for any integer $t \geq 0$. If there exists an integer $1 \leq t \leq 2^n - 3$ such that $f^t(a) = a$, then $a^{e^t} = a$, and so

$$a^{e^t - 1} = 1. \tag{2}$$

Since $2^n - 1$ is a Mersenne prime, every element belongs to $\mathrm{GF}(2^n)\backslash\{0,1\}$ is a primitive element of $\mathrm{GF}(2^n)$. It naturally follows that a is a primitive element of $\mathrm{GF}(2^n)$. Now (2) implies that $e^t \equiv 1 \bmod 2^n - 1$, which is a contradiction since by assumption e is a primitive root modulo $2^n - 1$. Therefore,

$$f^t(a) \neq a \text{ for } 1 \leq t \leq 2^n - 3,$$

and so $\mathrm{per}\,(\underline{a}) \geq 2^n - 2$. On the other hand, it is obvious that $\mathrm{per}\,(\underline{a}) \leq 2^n - 2$. Altogether, we have shown that $\mathrm{per}\,(\underline{a}) = 2^n - 2$, or equivalently, that $\underline{a}$ is an MLM-sequence over $\mathrm{GF}(2^n)$.

($\Rightarrow$) We recall that the nonzero elements of $\mathrm{GF}(2^n)$ form a cyclic group of order $2^n - 1$ under multiplication. Let $\mathrm{ord}(a)$ denote the order of a. Then $\mathrm{ord}(a) \mid 2^n - 1$. On the other hand, it follows from Remark 1 that $a, a^e, a^{e^2}, \ldots, a^{e^{2^n-3}}$ run exactly through the set $\mathrm{GF}(2^n)\backslash\{0,1\}$. This implies that $\mathrm{ord}(a) > 2^n - 2$. Now, together with $\mathrm{ord}(a) \mid 2^n - 1$, we get $\mathrm{ord}(a) = 2^n - 1$. Since

$$a^{e^{2^n-2}} = f^{2^n-2}(a) = a \text{ but } a^{e^t} = f^t(a) \neq a \text{ for } 1 \leq t \leq 2^n - 3, \tag{3}$$

by applying $\mathrm{ord}(a) = 2^n - 1$ to (3) we obtain

$$e^{2^n-2} \equiv 1 \bmod 2^n - 1 \text{ but } e^t \neq 1 \bmod 2^n - 1 \text{ for } 1 \leq t \leq 2^n - 3,$$

and hence the multiplicative order of e modulo $2^n - 1$ is equal to $2^n - 2$. This happens only if $2^n - 1$ is a Mersenne prime and e is a primitive root modulo $2^n - 1$.

3 Properties of coordinate sequences derived from MLM-sequences

Throughout this section, we always assume that $2^p - 1$ is a Mersenne prime (p is, of course, a prime number) and e is a primitive root modulo $2^p - 1$.

We will study two properties of coordinate sequences derived from MLM-sequences. Before proceeding, we first give two concrete examples.

Example 1. It can be verified that $2^5 - 1$ is a Mersenne prime and 11 is a primitive root modulo $2^5 - 1$. Let $\mathrm{GF}(2^5) = \mathrm{GF}(2)[x]/(x^5 + x^3 + 1)$, where $x^5 + x^3 + 1$ is an irreducible polynomial of degree 5 over $\mathrm{GF}(2)$. Let $\alpha \in \mathrm{GF}(2^5)$ be a root

of $x^5 + x^3 + 1$. Then $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$ is a polynomial basis of GF(2^5) over GF(2). Set $f = x^{11}$ and $a = \alpha$. By Theorem 1, $\underline{a} = (a, f(a), f^2(a), \ldots)$ is an MLM-sequence over GF(2^5) with $\mathrm{per}\,(\underline{a}) = 30$. In fact, it can be checked that

$$\begin{aligned}\underline{a} = (&\alpha, \alpha^3+\alpha^2+\alpha+1, \alpha^2+1, \alpha^3+\alpha, \alpha^4+\alpha^3+\alpha^2+1, \alpha^4+\alpha, \alpha^4,\\ &\alpha^4+\alpha^2+1, \alpha^4+\alpha^3+\alpha+1, \alpha^3+\alpha^2+\alpha, \alpha^3+1, \alpha^4+\alpha^3+\alpha^2,\\ &\alpha^3+\alpha^2, \alpha^4+\alpha^2+\alpha+1, \alpha+1, \alpha^4+\alpha^2, \alpha^4+\alpha^3+\alpha^2+\alpha+1, \alpha^3,\\ &\alpha^2, \alpha^2+\alpha+1, \alpha^4+1, \alpha^4+\alpha^2+\alpha, \alpha^4+\alpha^3+1, \alpha^4+\alpha^3+\alpha^2+\alpha,\\ &\alpha^4+\alpha^3+\alpha, \alpha^3+\alpha+1, \alpha^3+\alpha^2+1, \alpha^2+\alpha, \alpha^4+\alpha+1, \alpha^4+\alpha^3, \ldots),\end{aligned} \tag{4}$$

and so the 5 coordinate sequences of $\underline{a}$ w.r.t. $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$ are as follows:

$$[\underline{a}]_0 = (0,1,1,0,1,0,0,1,1,0,1,0,0,1,1,0,1,0,0,1,1,0,1,0,0,1,1,0,1,0,\ldots),$$

$$[\underline{a}]_1 = (1,1,0,1,0,1,0,0,1,1,0,0,0,1,1,0,1,0,0,1,0,1,0,1,1,1,0,1,1,0,\ldots),$$

$$[\underline{a}]_2 = (0,1,1,0,1,0,0,1,0,1,0,1,1,1,0,1,1,0,1,1,0,1,0,1,0,0,1,1,0,0,\ldots),$$

$$[\underline{a}]_3 = (0,1,0,1,1,0,0,0,1,1,1,1,1,0,0,0,1,1,0,0,0,0,1,1,1,1,1,0,0,1,\ldots),$$

$$[\underline{a}]_4 = (0,0,0,0,1,1,1,1,1,0,0,1,0,1,0,1,1,0,0,0,1,1,1,1,1,0,0,0,1,1,\ldots).$$

It can be seen that

$$\mathrm{per}\,([\underline{a}]_0) = 6, \mathrm{per}\,([\underline{a}]_1) = \mathrm{per}\,([\underline{a}]_2) = \mathrm{per}\,([\underline{a}]_3) = \mathrm{per}\,([\underline{a}]_4) = 30.$$

Consequently, among the 5 coordinate sequences, only 4 of them attain the maximum period. It also can be seen that

$$[\underline{a}]_1 = L^{18}[\underline{a}]_2 \text{ and } [\underline{a}]_3 = L^{12}[\underline{a}]_4,$$

where $L^k\underline{z}$ denotes the k-shift of $\underline{z}$ (i.e., $L^k\underline{z} = (z(t+k))_{t\geq 0}$ if $\underline{z} = (z(t))_{t\geq 0}$). This implies that $[\underline{a}]_1$ and $[\underline{a}]_2$ (or $[\underline{a}]_3$ and $[\underline{a}]_4$) are shift equivalent. However, it can be checked that $[\underline{a}]_1$ (or $[\underline{a}]_2$) and $[\underline{a}]_3$ (or $[\underline{a}]_4$) are shift distinct.

Example 2. Let GF(2^5) and α be as in Example 1. Let $\beta = \alpha^3 + 1$. Then

$$\beta^2 = \alpha^4+\alpha+1, \beta^4 = \alpha^4+\alpha^3+\alpha^2+\alpha+1, \beta^8 = \alpha^4+\alpha^3+\alpha^2+1, \beta^{16} = \alpha^4+\alpha^3+1,$$

and so $\{\beta, \beta^2, \beta^4, \beta^8, \beta^{16}\}$ is a normal basis of GF(2^5) over GF(2). Let $\underline{a}$ be as in (4). Then the 5 coordinate sequences of $\underline{a}$ w.r.t. $\{\beta, \beta^2, \beta^4, \beta^8, \beta^{16}\}$ are as follows:

$$[\underline{a}]_0 = (0,1,1,0,0,1,1,0,0,0,1,1,0,0,1,1,0,0,0,1,0,1,0,1,1,1,1,0,0,1,\ldots),$$

$$[\underline{a}]_1 = (0,0,1,1,0,0,0,1,0,1,0,1,1,1,1,0,0,1,0,1,1,0,0,1,1,0,0,0,1,1,\ldots),$$

$$[\underline{a}]_2 = (1,1,1,0,0,1,0,1,1,0,0,1,1,0,0,0,1,1,0,0,1,1,0,0,0,1,0,1,0,1,\ldots),$$

$$[\underline{a}]_3 = (1,0,0,0,1,1,0,0,1,1,0,0,0,1,0,1,0,1,1,1,1,0,0,1,0,1,1,0,0,1,\ldots),$$

$$[\underline{a}]_4 = (0,1,0,1,0,1,1,1,1,0,0,1,0,1,1,0,0,1,1,0,0,0,1,1,0,0,1,1,0,0,\ldots).$$

It can be seen that

$$\mathrm{per}\,([\underline{a}]_0) = \mathrm{per}\,([\underline{a}]_1) = \mathrm{per}\,([\underline{a}]_2) = \mathrm{per}\,([\underline{a}]_3) = \mathrm{per}\,([\underline{a}]_4) = 30.$$

Moreover, any two of $[\underline{a}]_0, [\underline{a}]_1, [\underline{a}]_2, [\underline{a}]_3, [\underline{a}]_4$ are shift equivalent. In fact, we have

$$[\underline{a}]_0 = L^{18}[\underline{a}]_1 = L^{6}[\underline{a}]_2 = L^{24}[\underline{a}]_3 = L^{12}[\underline{a}]_4.$$

Examples 1 and 2 above have shown that the properties of coordinate sequences are closely related to the choice of a basis. In the rest of this section, we will discuss more details. In Subsection 3.1, we will completely determine the periods of coordinate sequences of MLM-sequences. In particular, a necessary and sufficient condition is given for coordinate sequences whose periods attain the maximum. In Subsection 3.2, we will give a necessary and sufficient condition for coordinate sequences of MLM-sequences who are shift equivalent.

3.1 Periodic properties of the coordinate sequences

Lemma 1. *Let $f = x^e \in \mathrm{GF}(2^p)[x]$, where e is a primitive root modulo $2^p - 1$. Let $\underline{a} = (a, f(a), f^2(a), \ldots)$ be an MLM-sequence over $\mathrm{GF}(2^p)$, and let $[\underline{a}]_i$, $0 \le i \le p-1$, be the i-th coordinate sequence of $[\underline{a}]$ w.r.t. $\{\alpha_0, \alpha_1, \ldots, \alpha_{p-1}\}$, where $\{\alpha_0, \alpha_1, \ldots, \alpha_{p-1}\}$ is a basis of $\mathrm{GF}(2^p)$ over $\mathrm{GF}(2)$. Suppose $\{\beta_0, \beta_1, \ldots, \beta_{p-1}\}$ is the dual basis of $\{\alpha_0, \alpha_1, \ldots, \alpha_{p-1}\}$. Then $\mathrm{per}\,([\underline{a}]_i) \mid T$ if and only if*

$$\mathrm{Tr}\left(\beta_i\left(y^{e^T} + y\right)\right) = 0 \text{ for all } y \in \mathrm{GF}(2^p), \tag{5}$$

where T is a positive integer.

Proof. It is clear that $\mathrm{per}\,([\underline{a}]_i) \mid T$ if and only if

$$\left[f^{t+T}(a)\right]_i = \left[f^t(a)\right]_i \text{ for any integer } t \ge 0,$$

that is, if and only if

$$\left[\left(a^{e^t}\right)^{e^T}\right]_i = \left[a^{e^t}\right]_i \text{ for any integer } t \ge 0. \tag{6}$$

Since $a, a^e, a^{e^2}, \ldots, a^{e^{2^p-3}}$ run exactly through the set $\mathrm{GF}(2^p)\backslash\{0,1\}$ by Remark 1, the equality (6) is equivalent to

$$\left[y^{e^T}\right]_i = [y]_i \text{ for all } y \in \mathrm{GF}(2^p)\backslash\{0,1\}.$$

Observe that $\left[y^{e^T}\right]_i = [y]_i$ naturally holds for $y \in \{0,1\}$, and so (6) is also equivalent to

$$\left[y^{e^T}\right]_i = [y]_i \text{ for all } y \in \mathrm{GF}(2^p),$$

or equivalently,

$$\left[y^{e^T}+y\right]_i = 0 \text{ for all } y \in \mathrm{GF}(2^p). \tag{7}$$

Combining (6) and (7), we get that $\mathrm{per}\left([\underline{a}]_i\right) \mid T$ if and only if

$$\left[y^{e^T}+y\right]_i = 0 \text{ for all } y \in \mathrm{GF}(2^p).$$

Now (1) already gives the desired result.

Remark 2. Lemma 1 implies that if $\mathrm{per}\left([\underline{a}]_i\right) = T$, then T is the least positive integer for which the equality (5) holds.

Lemma 2. *Let $0 \neq \beta \in \mathrm{GF}(2^p)$ and $1 \leq d \leq 2^p - 1$. Then $\mathrm{Tr}\left(\beta\left(y^d+y\right)\right) = 0$ for all $y \in \mathrm{GF}(2^p)$ if and only if either $d = 1$ or $\beta = 1$ and $d = 2^k$ for some $1 \leq k \leq p-1$.*

Proof. ($\Leftarrow$) The result is obvious since $\mathrm{Tr}\left(\beta\left(y+y\right)\right) = 0$ and $\mathrm{Tr}\left(y^{2^k}+y\right) = \mathrm{Tr}\left(y^{2^k}\right) + \mathrm{Tr}\left(y\right) = 0$.

($\Rightarrow$) Let us view y as a variable over $\mathrm{GF}(2^p)$. Let $g(y)$ be the (unique) remainder of $\mathrm{Tr}\left(\beta\left(y^d+y\right)\right)$ modulo $y^{2^p}+y$. It is clear that $g(y)$ is a zero polynomial by assumption. We claim that

$$d = 2^k \text{ for some } 0 \leq k \leq p-1. \tag{8}$$

Otherwise, $d = 2^{k_1} + \cdots + 2^{k_w}$ for some $2 \leq w \leq p-1$. For convenience, we say that y^d has weight w. Note that the remainder of $\mathrm{Tr}\left(\beta y^d\right)$ modulo $y^{2^p}+y$ is a polynomial consisting of p terms, each of which has weight w, while the remainder of $\mathrm{Tr}\left(\beta y\right)$ modulo $y^{2^p}+y$ is a polynomial consisting of p terms, each of which has weight 1. Thus the remainder of $\mathrm{Tr}\left(\beta\left(y^d+y\right)\right) = \mathrm{Tr}\left(\beta y^d\right) + \mathrm{Tr}\left(\beta y\right)$ modulo $y^{2^p}+y$ is a nonzero polynomial, a contradiction. Therefore, we have proven the claim. If $d \neq 1$, then $d = 2^k$ for some $1 \leq k \leq p-1$. Now

$$0 = \mathrm{Tr}\left(\beta\left(y^d+y\right)\right) = \mathrm{Tr}\left(\beta\left(y^{2^k}+y\right)\right) = \mathrm{Tr}\left(\left(\beta^{2^{p-k}}+\beta\right)y\right)$$

implies that $\beta^{2^{p-k}} + \beta = 0$ since $\mathrm{Tr}\left(\cdot\right)$ maps $\mathrm{GF}(2^p)$ onto $\mathrm{GF}(2)$, and so $\beta \in \mathrm{GF}(2^{p-k})$. Since by assumption $0 \neq \beta \in \mathrm{GF}(2^p)$, we have

$$0 \neq \beta \in \mathrm{GF}(2^p) \cap \mathrm{GF}(2^{p-k}) = \mathrm{GF}(2),$$

and hence $\beta = 1$. This completes the proof.

With the above two lemmas, we can now completely determine the periods of coordinate sequences of MLM-sequences. In particular, we can give a necessary and sufficient condition for coordinate sequences whose periods attain the maximum.

Theorem 2. *Let $f = x^e \in \mathrm{GF}(2^p)[x]$, where e is a primitive root modulo $2^p - 1$. Let $\underline{a} = (a, f(a), f^2(a), \ldots)$ be an MLM-sequence over $\mathrm{GF}(2^p)$, and let $[\underline{a}]_i$, $0 \leq i \leq p-1$, be the i-th coordinate sequence of $[\underline{a}]$ w.r.t. $\{\alpha_0, \alpha_1, \ldots, \alpha_{p-1}\}$, where $\{\alpha_0, \alpha_1, \ldots, \alpha_{p-1}\}$ is a basis of $\mathrm{GF}(2^p)$ over $\mathrm{GF}(2)$. Suppose $\{\beta_0, \beta_1, \ldots, \beta_{p-1}\}$ is the dual basis of $\{\alpha_0, \alpha_1, \ldots, \alpha_{p-1}\}$. Then:*

(i) $\mathrm{per}\left([\underline{a}]_i\right) = 2^p - 2$ *if and only if* $\beta_i \neq 1$*; and*

(ii) $\mathrm{per}\left([\underline{a}]_i\right) = \left(2^p - 2\right)/p$ *if and only if* $\beta_i = 1$.

Proof. We note that $y^{2^p} = y$ for all $y \in \mathrm{GF}(2^p)$, and so for a given integer T we have $y^{e^T} = y^d$ for all $y \in \mathrm{GF}(2^p)$, where $e^T \equiv d \bmod 2^p - 1$ with $1 \leq d \leq 2^p - 2$. Then by applying Lemmas 1 and 2, we get $\mathrm{per}\left([\underline{a}]_i\right) \mid T$ if and only if

$$e^T \equiv 1 \bmod 2^p - 1 \text{ or } \beta_i = 1 \text{ and } e^T \equiv 2^k \bmod 2^p - 1 \tag{9}$$

for some $1 \leq k \leq p-1$. We also note that

$$e^{(2^p-2)/p} \equiv 2^k \bmod 2^p - 1 \text{ for some } 1 \leq k \leq p-1. \tag{10}$$

This is because $e^{2^p-2} \equiv 1 \bmod 2^p - 1$ and $\{2, 2^2, \ldots, 2^{p-1}\}$ is exactly the set of primitive p-th roots of unity (i.e. the roots of $x^p = 1$ except for 1) over $\mathrm{GF}(2^p-1)$, the prime field with $2^p - 1$ elements.

(i) To prove the necessity of *(i)*, suppose, on the contrary, that $\beta_i = 1$. If we set $T = \left(2^p - 2\right)/p$, then (10) implies that the latter condition of (9) is satisfied, and so $\mathrm{per}\left([\underline{a}]_i\right) \mid \left(2^p - 2\right)/p$, a contradiction. Therefore, we have $\beta_i \neq 1$. Conversely, set $T = \mathrm{per}\left([\underline{a}]_i\right)$. It is clear that $T \mid 2^p - 2$. Since by assumption $\beta_i \neq 1$, the latter condition of (9) is not satisfied, and so we get $e^T \equiv 1 \bmod 2^p - 1$. Then the desired result follows from the fact that e is a primitive root modulo $2^p - 1$.

(ii) The necessity of *(ii)* is an immediate consequence of *(i)*. If $\beta_i = 1$, we set $T = \left(2^p - 2\right)/p$. Then it has been shown in proving the necessity part of *(i)* that $\mathrm{per}\left([\underline{a}]_i\right) \mid \left(2^p - 2\right)/p$. The equality $\mathrm{per}\left([\underline{a}]_i\right) = \left(2^p - 2\right)/p$ holds simplely because $e^s \neq 2^k \bmod 2^p - 1$ for any $1 \leq k \leq p-1$ if $1 \leq s < \left(2^p - 2\right)/p$.

Remark 3. Theorem 2 has shown that the coordinate sequences of MLM-sequences have desirable periodic properties. In detail, since $\{\beta_0, \beta_1, \ldots, \beta_{p-1}\}$ is a basis of $\mathrm{GF}(2^p)$ over $\mathrm{GF}(2)$, there are at least $p-1$ elements among $\beta_0, \beta_1, \ldots, \beta_{p-1}$ who are not equal to 1. It follows immediately that, among $[\underline{a}]_0, [\underline{a}]_1, \ldots, [\underline{a}]_{p-1}$, there are at least $p-1$ coordinate sequences whose periods attain the maximum $2^p - 2$. Although the period of the remaining one may not attain the maximum, it still not less than $\left(2^p - 2\right)/p$.

In the rest of this subsetion, we will give two further results for two special types of bases. The first one is for polynomial bases, and the second one is for normal bases.

Corollary 1. *Let f and $\underline{a}$ be as in Theorem 2. Let $[\underline{a}]_i$, $0 \leq i \leq p-1$, be the i-th coordinate sequence of $[\underline{a}]$ w.r.t. $\{1, \alpha, \alpha^2, \ldots, \alpha^{p-1}\}$, where $\{1, \alpha, \alpha^2, \ldots, \alpha^{p-1}\}$*

is a polynomial basis of $\mathrm{GF}(2^p)$ *over* $\mathrm{GF}(2)$*. Then* $\mathrm{per}\,([\underline{a}]_i) = 2^p - 2$ *for* $1 \le i \le p-1$*; and*

$$\mathrm{per}\,([\underline{a}]_0) = \begin{cases} (2^p-2)/p & \text{if } \mathrm{Tr}(\alpha^j) = 0 \text{ for } 1 \le j \le p-1, \\ 2^p - 2 & \text{otherwise.} \end{cases}$$

Proof. Let $\{\beta_0, \beta_1, \ldots, \beta_{p-1}\}$ be the dual basis of $\{1, \alpha, \alpha^2, \ldots, \alpha^{p-1}\}$. It is clear that $\beta_i \neq 1$ for $1 \le i \le p-1$, since otherwise there is an integer $j \in \{1, 2, \ldots, p-1\}$ such that $\beta_j = 1$, and then $\mathrm{Tr}\,(\beta_j \cdot 1) = \mathrm{Tr}\,(1) = 1 \neq 0$, a contradiction to the fact that $\{\beta_0, \beta_1, \ldots, \beta_{p-1}\}$ is the dual basis of $\{1, \alpha, \alpha^2, \ldots, \alpha^{p-1}\}$. Therefore, the first result immediately follows from Theorem 2. To prove the second result, it suffices to show that

$$\beta_0 = 1 \text{ if and only if } \mathrm{Tr}(\alpha^j) = 0 \text{ for } 1 \le j \le p-1. \tag{11}$$

The necessity of (11) is obvious from the definition of the dual basis.

Next we will prove the sufficiency part of (11). Since by the definition of the dual basis, we have

$$\mathrm{Tr}(\alpha^j \beta_0) = \begin{cases} 1 \text{ for } j = 0, \\ 0 \text{ for } 1 \le j \le p-1. \end{cases}$$

Combining it with the condition that $\mathrm{Tr}(\alpha^j) = 0$ for $1 \le j \le p-1$, we get

$$\mathrm{Tr}(\alpha^j\,(\beta_0 - 1)) = 0 \text{ for } 0 \le j \le p-1.$$

Note that $\{1, \alpha, \alpha^2, \ldots, \alpha^{p-1}\}$ is a basis of $\mathrm{GF}(2^p)$ over $\mathrm{GF}(2)$, and so we obtain the desired result that $\beta_0 = 1$. This completes the proof.

Corollary 2. *Let* f *and* $\underline{a}$ *be as in Theorem 2. Let* $[\underline{a}]_i$*,* $0 \le i \le p-1$*, be the* i*-th coordinate sequence of* $[\underline{a}]$ *w.r.t.* $\{\alpha, \alpha^2, \ldots, \alpha^{2^{p-1}}\}$*, where* $\{\alpha, \alpha^2, \ldots, \alpha^{2^{p-1}}\}$ *is a normal basis of* $\mathrm{GF}(2^p)$ *over* $\mathrm{GF}(2)$*. Then*

$$\mathrm{per}\,([\underline{a}]_i) = 2^p - 2 \text{ for } 0 \le i \le p-1.$$

Proof. Let $\{\beta_0, \beta_1, \ldots, \beta_{p-1}\}$ be the dual basis of $\{\alpha, \alpha^2, \ldots, \alpha^{2^{p-1}}\}$. By Theorem 2, it suffices to show that $\beta_i \neq 1$ for $0 \le i \le p-1$. This result follows from the fact that $\{\beta_0, \beta_1, \ldots, \beta_{p-1}\}$ is also a normal basis of $\mathrm{GF}(2^p)$ over $\mathrm{GF}(2)$ (see, for example, [14]) and that any element of a normal basis is not equal to 1.

3.2 Shift-equivalence of the coordinate sequences

We recall that two periodic sequences $\underline{a}$ and $\underline{b}$ are called shift equivalent if $\underline{a} = L^s\underline{b}$ for some nonnegative integer s, where $L^s\underline{b}$ is the s-shift of $\underline{b}$. Otherwise, $\underline{a}$ and $\underline{b}$ are called shift distinct.

Lemma 3. *With the notation of Theorem 2, let* $0 \le i < j \le p-1$*. Then* $[\underline{a}]_i = L^s[\underline{a}]_j$ *for some positive integer* s *if and only if* $\mathrm{Tr}\left(\beta_i y + \beta_j y^{e^s}\right) = 0$ *for all* $y \in \mathrm{GF}(2^p)$*.*

Proof. Firstly, we show that $[\underline{a}]_i = L^s[\underline{a}]_j$ if and only if

$$\mathrm{Tr}\left(\beta_i y\right) = \mathrm{Tr}\left(\beta_j y^{e^s}\right) \text{ for all } y \in \mathrm{GF}(2^p)\backslash\{0,1\}. \tag{12}$$

We note that $\underline{a} = (a, f(a), f^2(a), \ldots)$, where $f^t(a) = a^{e^t}$ for any integer $t \geq 0$, and so by (1) we have

$$[f^t(a)]_i = \mathrm{Tr}\left(\beta_i a^{e^t}\right) \text{ and } [f^{t+s}(a)]_j = \mathrm{Tr}\left(\beta_j \left(a^{e^t}\right)^{e^s}\right) \text{ for any integer } t \geq 0.$$

Therefore, $[\underline{a}]_i = L^s[\underline{a}]_j$ if and only if

$$\mathrm{Tr}\left(\beta_i a^{e^t}\right) = \mathrm{Tr}\left(\beta_j \left(a^{e^t}\right)^{e^s}\right) \text{ for any integer } t \geq 0,$$

if and only if

$$\mathrm{Tr}\left(\beta_i y\right) = \mathrm{Tr}\left(\beta_j y^{e^s}\right) \text{ for all } y \in \mathrm{GF}(2^p)\backslash\{0,1\}.$$

The last equality follows from the fact that $a, a^e, a^{e^2}, \ldots, a^{e^{2^p-3}}$ run exactly through the set $\mathrm{GF}(2^p)\backslash\{0,1\}$ and $a^{e^{2^p-2}} = a$.

For $y = 0$, the equality holds obviously. Since the trace functions are balanced, the equality must hold for $y = 1$ too. This completes the proof.

The main result of this subsection can be described explicitly in the following Theorem.

Theorem 3. *With the notation of Theorem 2, let* $0 \leq i < j \leq p-1$. *Then* $[\underline{a}]_i = L^s[\underline{a}]_j$ *for some positive integer* s *if and only if* $\beta_j = \beta_i^{2^k}$ *and* $e^s \equiv 2^k \bmod 2^p - 1$ *for some* $0 \leq k \leq p-1$.

Proof. By Lemma 3, it suffices to show that $\mathrm{Tr}\left(\beta_i y + \beta_j y^{e^s}\right) = 0$ for all $y \in \mathrm{GF}(2^p)$ if and only if

$$\beta_j = \beta_i^{2^k} \text{ and } e^s \equiv 2^k \bmod 2^p - 1 \text{ for some } 0 \leq k \leq p-1.$$

If $\beta_j = \beta_i^{2^k}$ and $e^s \equiv 2^k \bmod 2^p - 1$ for some $0 \leq k \leq p-1$, then it is clear that

$$\mathrm{Tr}\left(\beta_i y + \beta_j y^{e^s}\right) = \mathrm{Tr}\left(\beta_i y + \beta_i^{2^k} y^{2^k}\right) = \mathrm{Tr}\left(\beta_i y + (\beta_i y)^{2^k}\right) = 0$$

holds for all $y \in \mathrm{GF}(2^p)$.

Conversely, suppose $\mathrm{Tr}\left(\beta_i y + \beta_j y^{e^s}\right) = 0$ for all $y \in \mathrm{GF}(2^p)$. An argument similar to that leading to (8) shows that

$$e^s \equiv 2^k \bmod 2^p - 1 \text{ for some } 0 \leq k \leq p-1.$$

Consequently,

$$\begin{aligned} 0 &= \mathrm{Tr}\left(\beta_i y + \beta_j y^{e^s}\right) \\ &= \mathrm{Tr}\left(\beta_i y + \beta_j y^{2^k}\right) \\ &= \mathrm{Tr}\left(\beta_i y + \left(\beta_j y^{2^k}\right)^{2^{p-k}}\right) \\ &= \mathrm{Tr}\left(\left(\beta_i + \beta_j^{2^{p-k}}\right) y\right) \end{aligned}$$

holds for all $y \in \mathrm{GF}(2^p)$, which immediately implies that $\beta_i = \beta_j^{2^{p-k}}$, or, equivalently, that $\beta_j = \beta_i^{2^k}$.

For normal bases, we have a more concrete result, which is stated in the following Corollary.

Corollary 3. *Let f and $\underline{a}$ be as in Theorem 2. Let $[\underline{a}]_j$, $0 \le j \le p-1$, be the i-th coordinate sequence of $[\underline{a}]$ w.r.t. $\{\alpha, \alpha^2, \ldots, \alpha^{2^{p-1}}\}$, where $\{\alpha, \alpha^2, \ldots, \alpha^{2^{p-1}}\}$ is a normal basis of $\mathrm{GF}(2^p)$ over $\mathrm{GF}(2)$. Then for $1 \le j \le p-1$, there exists an integer $s_j = u_j(2^p-2)/p$ with $1 \le u_j \le p-1$ such that $[\underline{a}]_0 = L^{s_j}[\underline{a}]_j$. Moreover, $s_1, s_2, \ldots, s_{p-1}$ run exactly through the set*

$$\{\,(2^p-2)\,/p, 2\,(2^p-2)\,/p, \ldots, (p-1)\,(2^p-2)\,/p\}.$$

Proof. Let $\{\beta_0, \beta_1, \ldots, \beta_{p-1}\}$ be the dual basis of $\{\alpha, \alpha^2, \ldots, \alpha^{2^{p-1}}\}$. Since the dual basis of a normal base is also a normal base, it immediately follows that $\beta_j = \beta_0^{2^j}$ for $0 \le j \le p-1$. Furthermore,

$$e^{(2^p-2)/p} \equiv 2^k \bmod 2^p - 1 \text{ for some } 1 \le k \le p-1 \tag{13}$$

by (10). Let u_j be the least nonnegative residue of $k^{-1}j$ modulo p for $1 \le j \le p-1$, that is $u_j = k^{-1}j \bmod p$, where k^{-1} is the inverse of k modulo p. Then (13) yields

$$e^{u_j(2^p-2)/p} \equiv 2^{u_j k} \equiv 2^j \bmod 2^p - 1. \tag{14}$$

By setting $i = 0$ and applying (13) and (14) to Theorem 3, the first desired result immediately follows. The second desired result follows from the fact that $u_j = k^{-1}j \pmod p$ runs through the set $\{1, 2, \ldots, p-1\}$ if j runs through $\{1, 2, \ldots, p-1\}$.

4 Conclusions

Binary sequences with desirable properties have important applications in cryptography, communication, Monte Carlo simulation and so on. In this paper, a class of binary sequences induced by monomial permutation polynomials over $\mathrm{GF}(2^n)$ is proposed, and the periodic property and the shift-equivalence of these

binary sequences are studied. In particularly, a necessary and sufficient condition is given such that they have the maximum possible period. Moreover, a necessary and sufficient condition is also given for two sequences who are shift equivalent. The results of this paper imply that these binary sequences should be potential interested for several applications such as stream ciphers.

How to generate a pseudo-random sequence with desirable properties is a classical problem. Although our new proposed PRNG can be viewed as a Galois NFSR, it should be pointed out that its actual performance cannot be compared with NFSR since the power operations over finite fields are usually resource-consuming. How to improve the performance of the proposed PRNG or how to design other type of PRNGs with desirable properties and performance deserves further study.

References

1. Lidl, R., Niederreiter, H.: Finite Fields. Encyclopedia of Mathematics and Its Applications, vol. 20. Cambridge University Press, Cambridge, (1997)
2. Mullen, G.L., Panario, D.: Handbook of Finite Fields. CRC Press, Boca Raton, (2013)
3. Hou, X.D.: Permutation polynomials over finite fields – A survey of recent advances. Finite Fields Appl. **32**, 82-119 (2015)
4. Tu, Z.R., Zeng, X.Y.: A class of permutation trinomials over finite fields of odd characteristic. Cryptogr. Commun. **11**(4), 563–583 (2019)
5. Tu, Z.R., Zeng, X.Y., Jiang, Y.P.: Two classes of permutation polynomials having the form $(x^{2^m}+x+\delta)^s+x$. Finite Fields Appl. **53**, 99-112 (2018)
6. Wang, L.B., Wu, B.F.: General constructions of permutation polynomials of the form $(x^{2^m}+x+\delta)^{i(2m-1)+1}+x$ over $F_{2^{2m}}$. Finite Fields Appl. **52**, 137-155 (2018)
7. Feng, X.T., Lin, D.D., Wang, L.P., Wang, Q.: Further results on complete permutation monomials over finite fields. Finite Fields Appl. **57**, 47-59 (2019)
8. Xu, X.F, Feng, X.T., Zeng, X.Y.: Complete permutation polynomials with the form $(x^{p^m}-x+\delta)^s+ax^{p^m}+bx$ over F_{p^n}. Finite Fields Appl. **57**, 309-343 (2019)
9. Wu, B.F., Lin, D.D.: On constructing complete permutation polynomials over finite fields of even characteristic. Discret. Appl. Math. **184**, 213-222 (2015)
10. Niederreiter, H.: Pseudorandom vector generation by the inversive method. ACM Trans. Model. Comput. Simul. **4**(2), 191-212 (1994)
11. Anderson, S.L.: Random number generators on vector supercomputers and other advanced architectures. SIAM Rev. **32**, 221-251 (1990) .
12. Bhavsar, V.C., Isaac, J.R.: Design and analysis of parallel Monte Carlo algorithms. SIAM J. Sci. Stat. Comput. **8**, s73-s95 (1987)
13. Eddy, W.F.: Random number generators for parallel processors. J. Comput. Appl. Math. **31**, 63-71 (1986)
14. Menezes, A.J., Blake, I.F., et al: Applications of Finite Fields. Kluwer Academic Publishers, Massachusetts, (1993)