On the period factor of quasigroups

Yonghua Tan, Yunqing Xu
Faculty of Science
Ningbo University
Ningbo 315211, China
xuyunqing@gmail.com

Abstract—**Quasigroups are algebraic structures closely related to Latin squares which have many different applications. Nonlinear pseudo random sequences based on quasigroups have important applications in cryptography. The quasigroups which generate nonlinear pseudo random sequences with large periods are only found by computer statistical search until now. In this paper, we discuss the probability distribution of periods factors of quasigroups by means of Frobenius groups theory.**

Keywords-pseudo random sequence; quasigroup; Latin square; period factor; Frobenius group

I. INTRODUCTION

Many scientific experiments require large amounts of random input data in order to simulate some process. Pseudo random sequences are inevitable in many fields like cryptography, communication, and automatic control etc. For this reason the field of pseudo random generators is widely exploited. Pseudo random sequence generators (PRSG) produce sequences of elements that imitate natural random behavior. However, widely available PRSGs have limited periods. But the PRSG designed using quasigroup processing is highly scalable and with arbitrary large period [1].

A quasigroup (Q, $*$) is a groupoid (i.e. algebra with one binary operation $*$ on the set Q) satisfying the law:

$$(\forall u,v\in Q)(\exists! x,y\in Q)(x*u=v\&u*y=v).$$

A Latin square on a set Q is an $|Q|\times|Q|$ array such that every symbol occurs in every row once, and also in every column once. It is fairly well known that (e.g., see [2]) the multiplication table of a quasigroup defines a Latin square; that is, a Latin square can be viewed as the multiplication table of a quasigroup with the headline and sideline removed.

It was noticed in [3] and [4] that quasigroups can be very useful for cryptographic purposes, mainly because there is a huge number of quasigroups operations on a given finite set, and it is easy to define the encoding and decoding functions by using the quasigroup operations as well.

Let Q be a set of elements ($|Q|\geq 2$). We denote by $Q^+ = \{x_1x_2\cdots x_k \mid x_i \in Q,\ k \geq 2\}$ the set of all finite sequences with elements of Q. Assuming that (Q,$*$) is a given quasigroup, for a fixed element $\alpha\in Q$, we define transformation $E_{\alpha,*}: Q^+\to Q^+$ as follows [5]:

$$E_{\alpha,*}(x_1x_2\cdots x_m)=y_1y_2\cdots y_m,$$

where

$$\begin{cases} y_1=\alpha*x_1, \\ y_{i+1}=y_i*x_{i+1}, \quad i=1,2,\cdots m-1. \end{cases}$$

Map $E_{\alpha,*}$ is called an *e-transformation* of Q^+ based on the quasigroup operation $*$ with leader α.

Edon80 was submitted to the eSTREAM project as a hardware stream cipher. It was designed by Gligoroski, Markovski, Kocarev, and Gusev and its original description is given in [6]. It has a unique design among known stream cipher designs: it concatenates 80 basic building blocks derived from four small quasigroups of order 4. Edon80 process e-transformation to the initial string consisting of letters “0 1 2 3 0 1 2 3 0···” in 80 steps and output every second letter that forms the key-stream of the stream cipher. There are 576 quasigroups of order 4, and for Edon80, by Gligoroski's experiments, 384 of them are suitable, 64 of them are very suitable [7]. All the data are obtained by experimental method using computer. It is reasonable to expect that not all quasigroups provide the same period of the PRSG and we can easily observe that the period growth of the PRSG designed using quasigroup processing is at least linear (see [8]). Quasigroups of arbitrary order can be used to generate pseudo random sequence algorithm of sequence cipher system. But for higher order of quasigroups, their statistical test are almost impossible. In this paper, we research probability distribution of period factors of quasigroups of high orders by using Frobenius groups theory.

II. DEFINITIONS AND THEOREMS ON THE PERIOD FACTOR DISTRIBUTION OF A QUASIGROUP

We say that a string $X = x_1x_2\cdots x_n \in Q^+$ where $x_i \in Q$ has a period p if p is the smallest positive integer such that $x_{i+1}x_{i+2}\cdots x_{i+p} = x_{i+p+1}x_{i+p+2}\cdots x_{i+2p}$ for each $i \geq 0$.

Definition 2.1: Let Q be an n-set and σ be a permutation on Q. $\forall x \in Q$, the period of sequence x $\sigma(x)$ $\sigma^2(x)\cdots$ $\sigma^i(x)\cdots$ is called the period factor of σ on x and denoted by $f_\sigma(x)$.

Suppose Q is a set and σ is a permutation on Q, it is easy to see that if $x\in Q$ is in a cycle of σ of length k, then $f_\sigma(x) = k$.

Theorem 2.2: [9] Suppose Q is an n-set and σ is a permutation on Q. If the type of σ is $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$, i.e., σ has λ_i cycles of length i (i = 1, 2, $\cdots$,n), and the probability distribution on Q is uniform: $\{P(x) = 1/n : x \in Q\}$, then the probability distribution of f_σ is

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ P(f_\sigma = 1) & P(f_\sigma = 2) & \cdots & P(f_\sigma = n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ \frac{\lambda_1}{n} & \frac{2\lambda_2}{n} & \cdots & \frac{n\lambda_n}{n} \end{pmatrix}.$$

Definition 2.3: Let $Q = \{1, 2, \cdots, n\}$ and $(Q, *)$ be a quasigroup, $L = (l_{i,j})_{n\times n}$ be the Latin square of the multiplication table of $(Q, *)$. $\forall i \in Q$, the permutation

$$\sigma_i = \begin{pmatrix} 1 & 2 & \cdots & n \\ l_{1i} & l_{2i} & \cdots & l_{ni} \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1*i & 2*i & \cdots & n*i \end{pmatrix}.$$

is called the i-th column permutation of L (or $(Q, *)$).

Theorem 2.4: [9] Let $Q = \{1, 2, \cdots, n\}$, $(Q, *)$ be a quasigroup and $\sigma_1, \sigma_2, \cdots, \sigma_n$ be the column permutations of $(Q, *)$. Suppose $X = x_1x_2\cdots x_m \cdots \in Q^+$ is periodic with period p. $E_{\alpha_0,*}$ is the e-transformation function of Q^+ based on the operation $*$ with leader $\alpha_0 \in Q$ and

$$Y = y_1y_2\cdots y_m \cdots = E_{\alpha_0,*}(x_1x_2\cdots x_m\cdots).$$

If α_0 is in a cycle of length k of the permutation $\sigma = \sigma_{x_p}\sigma_{x_{p-1}}\cdots\sigma_{x_1}$, then Y is periodic and period of Y is $k \cdot p$.

Definition 2.5: Suppose Q is an n-set and $(Q, *)$ is a quasigroup, $\sigma_1, \sigma_2, \cdots \sigma_n$ are the column permutations of $(Q, *)$ and $S_* = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$. For any positive integer p, let $S_*^p = \{\sigma_{i_p}\sigma_{i_{p-1}}\ldots\sigma_{i_1} : 1 \le i_1, i_2, \ldots, i_p \le n\}$ be a multi-set. $\forall(\sigma, x) \in S_*^p \times Q$, the period of sequence $x\ \sigma(x)\cdots\ \sigma^p(x)\cdots$ is called the period factor of $(Q, *)$ of degree p with σ and x and denoted by $f_*^{(p)}(\sigma, x)$. The function $f_*^{(p)} = f_*^{(p)}(\sigma, x)$ with domain $S_*^p \times Q$ is a random variable with sample space $N = \{1, 2, \cdots, n\}$. $f_*^{(p)}$ is called the period factor of $(Q, *)$ of degree p.

Theorem 2.6: [9] Suppose Q is an n-set and $(Q, *)$ is a quasigroup, and $S_* = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ is the set of column permutations of $(Q, *)$. Let $\{\tau_1, \tau_2, \cdots, \tau_v\} = <S_*>$ be the permutation group generated by S_*, and suppose the type of τ_i is $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ (i =1, 2, $\cdots$, n). Suppose the probability distribution on Q is uniform: $\{P(x) = 1/n : x \in Q\}$. For any positive integer p, if the multi-set

$$S_*^p = \{\sigma_{i_p}\sigma_{i_{p-1}}\ldots\sigma_{i_1} : 1 \le i_1, i_2, \ldots, i_p \le n\} = \left\{n_1^{(p)}\cdot\tau_1, n_2^{(p)}\cdot\tau_2, \ldots, n_v^{(p)}\cdot\tau_v\right\},$$

then the probability distribution of $f_*^{(p)}$ is

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \frac{1}{n^{p+1}}\sum_{i=1}^{v} n_i^{(p)}\lambda_{i1} & \frac{2}{n^{p+1}}\sum_{i=1}^{v} n_i^{(p)}\lambda_{i2} & \ldots & \frac{n}{n^{p+1}}\sum_{i=1}^{v} n_i^{(p)}\lambda_{in} \end{pmatrix}.$$

Every application of an e-transformation in Edon80 can be seen as a random variable ξ that receives values from the set {1, 2, 3, 4}. Every ξ has the same probability distribution as the period factor distribution of the quasigroups.

III. The period factor of the quasigroups based on Frobenius groups

A Frobenius group is a transitive permutation group which is not regular, but in which only the identity has more than one fixed point. Historically, finite Frobenius groups have played an important role in many areas in finite group theory. The detailed definition of Frobenius groups is given in [10].

Theorem 3.1: [10, Example 3.4.1] Let U denote a subgroup of the group of a finite field F. Then the set G consisting of all permutations of F of the form

$$t_{\xi\beta} : \alpha \mapsto \xi\alpha + \beta \text{ with } \xi \in U, \beta \in F$$

is a Frobenius group.

Lemma 3.2: Let $Q = \{\beta_1, \beta_2, \cdots, \beta_n\}$ be the set of all elements from a finite field F, and let $*_\xi$ ($\xi \ne 0$) be a binary operation defined on Q:

$$*_\xi : \alpha *_\xi \beta = \alpha\xi + \beta, \forall \alpha, \beta \in Q.$$

Then the pair $(Q, *_\xi)$ is a quasigroup.

Proof : For every $\beta_i, \beta_j \in Q$, the equations

$$\beta_i *_\xi x_1 = \beta_j \text{ and } x_2 *_\xi \beta_i = \beta_j$$

have a unique solution $x_1 = \beta_j - \beta_i\xi \in Q$, $x_2 = (\beta_j - \beta_i) / \xi \in Q$. So $(Q, *)$ is a quasigroup.

Since $\xi \ne 0$, we have n–1quasigroups from Lemma 3.2. And if ξ is a primitive root of a finite field F, then the n–1 quasigroups are $(Q, *_1)$, $(Q, *_\xi)$, $\cdots$, $(Q, *_{\xi^{n-2}})$.

Definition 3.3: Let $Q = \{\beta_1, \beta_2, \cdots, \beta_n\}$ be the set of all elements from a finite field F and $(Q, *_\xi)$ be a quasigroup from Lemma 3.2. Let $L = (l_{\alpha\beta})_{n\times n}$ be the Latin square of the multiplication table of $(Q,*_\xi)$ (i.e. $l_{\alpha\beta} = \xi\alpha + \beta$), the permutation

$$\sigma_{\xi i} = \begin{pmatrix} \beta_1 & \beta_2 & \cdots & \beta_n \\ \beta_1\xi + \beta_i & \beta_2\xi + \beta_i & \cdots & \beta_n\xi + \beta_i \end{pmatrix}$$

is called the i-th column permutation of L (or $(Q, *_\xi)$).

Let $F = \{\beta_1, \beta_2, \cdots, \beta_n\}$ be a finite field of order n. 1 is the identity element and let $\beta_1 = 0$ be the zero element of F. Let $T_\xi = \{\sigma_{\xi i} : \alpha \mapsto \xi\alpha + \beta_i \mid \xi \ne 0, \alpha, \beta_i \in F\}$ be a set of permutations on F from G of Theorem 3.1, then we know that T_ξ is a Frobenius group.

Theorem 3.4: Let $F = \{\beta_1, \beta_2, \cdots, \beta_n\}$ be a finite field of order n, $T_\xi = \{\sigma_{\xi i} : \alpha \mapsto \xi\alpha + \beta_i \mid \xi \ne 0, \alpha, \beta_i \in F\}$ be a Frobenius group. $(Q, *_1)$ is a quasigroup from Lemma 3.2 when $\xi = 1$ is the identity element of F. Then the probability distribution of $f_{*_1}^{(p)}$ is

$$\begin{pmatrix} 1 & n \\ \frac{1}{n} & \frac{n-1}{n} \end{pmatrix}$$

for any positive integer p.

Proof : $(Q, *_1)$ is a quasigroup of order n and $\sigma_{11}, \sigma_{12}, \cdots, \sigma_{1n}$ are the column permutations of $(Q, *_1)$. σ_{11} from the set T_ξ is the identical permutation and the type is 1^n. Since T_ξ is a Frobenius group, σ_{1i} has no fixed point for $i \ge 2$. So the type of σ_{1i} is n^1 (i = 2, 3, $\cdots$, n).

Let $S = \{\sigma_{11}, \sigma_{12}, \cdots, \sigma_{1n}\}$, it is easy to see that $\langle\sigma_{11}, \sigma_{12}, \ldots, \sigma_{1n}\rangle = \{\sigma_{11}, \sigma_{12}, \cdots, \sigma_{1n}\}$, we have $\{\sigma_{11}, \sigma_{12}, \cdots, \sigma_{1n}\}^p = n^{p-1}\{\sigma_{11}, \sigma_{12}, \cdots, \sigma_{1n}\}$. Applying Theorem 2.6, we have

$$p(f_{*_1}^{(p)}=1)=\frac{1}{n^{p+1}}\sum_{i=1}^{n}n_i^{(p)}\lambda_{i1}=\frac{1}{n^{p+1}}\cdot n^{p-1}\cdot n=\frac{1}{n},$$

$$p(f_{*_1}^{(p)}=h)=\frac{h}{n^{p+1}}\sum_{i=1}^{n}n_i^{(p)}\lambda_{ih}=\frac{h}{n^{p+1}}\cdot n^{p-1}\cdot 0=0,$$

(h = 2, $\cdots$, n-1),

$$p(f_{*_1}^{(p)}=n)=\frac{n}{n^{p+1}}\sum_{i=1}^{n}n_i^{(p)}\lambda_{in}=\frac{n}{n^{p+1}}\cdot n^{p-1}\cdot(n-1)=\frac{n-1}{n}.$$

So the probability of $f_{*_1}^{(p)}$ is $\begin{pmatrix}1 & n\\ \frac{1}{n} & \frac{n-1}{n}\end{pmatrix}$ for all positive integer p.

According to Theorem 3.4, the possible value of $f_{*_1}^{(p)}$ is 1 or n. And the expected value of $f_{*_1}^{(p)}$ is E ($f_{*_1}^{(p)}$) = 1 × 1/n + n × (n–1)/n = (n^2–n+1)/n.

Theorem 3.5: Let F = {β_1, β_2, $\cdots$, β_n} be a finite field of order n, $T_\xi=\{\sigma_{\xi i}:\alpha\mapsto\xi\alpha+\beta_i \mid \xi\neq 0,\alpha,\beta_i\in F\}$ be a Frobenius group and (Q, $*_\xi$) be a quasigroup from Lemma 3.2. If ξ is a primitive root of the field F, then the probability distribution of $f_{*_\xi}^{(p)}$ is

$$\begin{cases}\begin{pmatrix}1 & n\\ \frac{1}{n} & \frac{n-1}{n}\end{pmatrix}, & when \quad p\equiv 0\ (\mathrm{mod}(n-1)),\\ \begin{pmatrix}1 & n-1\\ \frac{1}{n} & \frac{n-1}{n}\end{pmatrix}, & when \quad p\equiv k\ (\mathrm{mod}(n-1)), k\nmid(n-1),\\ \begin{pmatrix}1 & \frac{n-1}{k}\\ \frac{1}{n} & \frac{n-1}{n}\end{pmatrix}, & when \quad p\equiv k\ (\mathrm{mod}(n-1)), k\mid(n-1).\end{cases}$$

Proof: ξ is the primitive root of the field F, i.e. the multiplicative order of ξ is n–1. (Q, $*_\xi$) is a quasigroup of order n. $\sigma_{\xi1}$, $\sigma_{\xi2}$, $\cdots$, $\sigma_{\xi n}$ are the column permutations of (Q, $*_\xi$).

$\sigma_{\xi1}:\alpha\mapsto\xi\alpha\ (\alpha\in F)$ is a permutation from T_ξ and 0 is the fixed point of $\sigma_{\xi1}$. Let 1 is the identity element of F, then we have $\sigma_{\xi1}$ = (1 ξ ξ^2 $\cdots$ ξ^{n-2}) since ξ is the primitive root of the field F, and the type of $\sigma_{\xi1}$ is $1^1(n-1)^1$. For i ≥ 1, $\sigma_{\xi i}:\alpha\mapsto\xi\alpha+\beta_i$, and we have $\sigma_{\xi i}$ = (1 ξ+β_i ξ^2+$\xi\beta_i$+ β_i $\cdots$ ξ^{n-2}+$\xi^{n-3}\beta_i$+β_i)(β_i/(1–ξ)) since ξ^{n-1}+$\xi^{n-2}\beta_i$+$\xi^{n-3}\beta_i$+ $\cdots$ +β_i = 1+(ξ^{n-2}+ξ^{n-3}+$\cdots$+1) β_i = 1+0×β_i = 1. And α = β_i /(1–ξ) is the fixed point of $\sigma_{\xi i}$. So the type of $\sigma_{\xi i}$ is $1^1(n-1)^1$. $\sigma_{\xi2}$, $\cdots$, $\sigma_{\xi n}$ have the same type with $\sigma_{\xi1}$. In the similar way, when $\xi\neq 0$ is not the primitive root of the field F, $\sigma_{\xi2}$, $\cdots$, $\sigma_{\xi n}$ have the same type with $\sigma_{\xi1}$.

Let S = {$\sigma_{\xi1}$, $\sigma_{\xi2}$, $\cdots$, $\sigma_{\xi\mathrm{n}}$ }, $\sigma_{\xi i}\cdot\sigma_{\xi j}:\alpha\mapsto\xi^2\alpha+\xi\beta_i+\beta_j$ is the product of the two permutations (i, j = 1, 2, $\cdots$, n). And we know that $\xi\beta_i$+ β_j ∈ F. $\sigma_{\xi^2 t}:\alpha\mapsto\xi^2\alpha+\beta_t$ is the permutation from T_ξ. So $\sigma_{\xi i}\cdot\sigma_{\xi j}=\sigma_{\xi^2 t}$ when β_t = $\xi\beta_i$+ β_j. Then it is easy to get $S^2=n\{\sigma_{\xi^2 1},\sigma_{\xi^2 2},\cdots,\sigma_{\xi^2 n}\}$ and $\sigma_{\xi^2 i}:\alpha\mapsto\xi^2\alpha+\beta_i$. In the similar way, we have

$$\begin{cases}S^3=n^2\{\sigma_{\xi^3 1},\sigma_{\xi^3 2},\cdots,\sigma_{\xi^3 n}\},\ \ \sigma_{\xi^3 i}:\alpha\mapsto\xi^3\alpha+\beta_i,\\ \cdots\\ S^{n-1}=n^{n-2}\{\sigma_{11},\sigma_{12},\cdots,\sigma_{1n}\},\ \ \sigma_{1i}:\alpha\mapsto\alpha+\beta_i,\\ S^n=n^{n-1}\{\sigma_{\xi1},\sigma_{\xi2},\cdots,\sigma_{\xi n}\},\ \ \sigma_{\xi i}:\alpha\mapsto\xi\alpha+\beta_i,\\ \cdots\end{cases}$$

We know that the type of $\sigma_{\xi i}$ is $1^1(n-1)^1$. Applying the property of Frobenius groups and the theory of permutation group, when p ≡ k (mod (n–1)) and k | (n–1), $\sigma_{\xi^k i}$ has a fixed point $\alpha=\frac{\beta_i}{1-\xi^k}$ and has k cycles of length $\frac{n-1}{k}$. So the type of $\sigma_{\xi^k i}$ is $1^1(\frac{n-1}{k})^k$. When p ≡ k (mod (n–1)) and $k\nmid$ (n–1), we know that the type of $\sigma_{\xi^k i}$ is $1^1(n-1)^1$. The type of σ_{11} is 1^n and the type of σ_{1i} is n^1 (i = 2, 3, $\cdots$, n).

From the above discussion we know that when p ≡ 0 (mod (n–1)),

$$p(f_{*_\xi}^{(p)}=1)=\frac{1}{n^{p+1}}\sum_{i=1}^{n}n_i^{(p)}\lambda_{i1}=\frac{1}{n^{p+1}}\cdot n^{p-1}\cdot n=\frac{1}{n},$$

$$p(f_{*_\xi}^{(p)}=h)=\frac{h}{n^{p+1}}\sum_{i=1}^{n}n_i^{(p)}\lambda_{ih}=\frac{h}{n^{p+1}}\cdot n^{p-1}\cdot 0=0$$

$$(h=2,\cdots,n-1),$$

$$p(f_{*_\xi}^{(p)}=n)=\frac{n}{n^{p+1}}\sum_{i=1}^{n}n_i^{(p)}\lambda_{in}=\frac{n}{n^{p+1}}\cdot n^{p-1}\cdot(n-1)=\frac{n-1}{n},$$

and the probability distribution of $f_{*_\xi}^{(p)}$ is $\begin{pmatrix}1 & n\\ \frac{1}{n} & \frac{n-1}{n}\end{pmatrix}$.

When p ≡ k (mod (n–1)), k | (n–1),

$$p(f_{*_\xi}^{(p)}=1)=\frac{1}{n^{p+1}}\sum_{i=1}^{n}n_i^{(p)}\lambda_{i1}=\frac{1}{n^{p+1}}\cdot n^{p-1}\cdot n=\frac{1}{n},$$

$$p(f_{*_\xi}^{(p)}=\frac{n-1}{k})=\frac{\frac{n-1}{k}}{n^{p+1}}\sum_{i=1}^{n}n_i^{(p)}\lambda_{i\frac{n-1}{k}}=\frac{\frac{n-1}{k}}{n^{p+1}}\cdot n^{p-1}\cdot k\cdot n=\frac{n-1}{n},$$

and the probability distribution of $f_{*_\xi}^{(p)}$ is $\begin{pmatrix}1 & \frac{n-1}{k}\\ \frac{1}{n} & \frac{n-1}{n}\end{pmatrix}$.

When p ≡ k (mod (n–1)), $k\nmid$ (n–1),

$$p(f_{*_\xi}^{(p)}=1)=\frac{1}{n^{p+1}}\sum_{i=1}^{n}n_i^{(p)}\lambda_{i1}=\frac{1}{n^{p+1}}\cdot n^{p-1}\cdot n=\frac{1}{n},$$

$$p(f_{*_\xi}^{(p)} = n-1) = \frac{n-1}{n^{p+1}} \sum_{i=1}^{n} n_i^{(p)} \lambda_{i\ \ n-1} = \frac{n-1}{n^{p+1}} \cdot n^{p-1} \cdot 1 \cdot n = \frac{n-1}{n}$$

and the probability distribution of $f_{*_\xi}^{(p)}$ is $\begin{pmatrix} 1 & n-1 \\ \frac{1}{n} & \frac{n-1}{n} \end{pmatrix}$.

This completes the proof.

According to the Theorem 3.5, we know that the possible value of $f_{*_\xi}^{(p)}$ is 1, n–1, n, or $\frac{n-1}{k}$. The expected value of $f_{*_\xi}^{(p)}$ is

$$E(f_{*_\xi}^{(p)}) = \begin{cases} \frac{n^2-n+1}{n}, & when \quad p \equiv 0 \ (\bmod n-1), \\ \frac{n^2-2n+2}{n}, & when \quad p \equiv k \ (\bmod n-1), k \nmid n-1, \\ \frac{n^2-2n+k+1}{nk}, & when \quad p \equiv k \ (\bmod n-1), k \mid n-1. \end{cases}$$

When ξ is not the primitive root of the field F, for example $\xi^m = 1$ ($m \neq n$–1), we may calculate the period factor distribution and the expected value in the similar way. We know that it is convenient to use quasigroup of order 2^m in computers. So, in the following, we consider the finite fields of order 2^m. In Frobenius group G, only the identity has more than one fixed point. So if $2^m – 1$ is a prime number, we have the following corollary.

Corollary 3.6: Let $F = \{\beta_1, \beta_2, \cdots, \beta_n\}$ be a finite field of order 2^m, $T_\xi = \{\sigma_{\xi i} : \alpha \mapsto \xi\alpha + \beta_i \mid \xi \neq 0, \alpha, \beta_i \in F\}$ be a Frobenius group and $(Q, *_\xi)$ be a quasigroup from Lemma 3.2. When $2^m – 1$ is a prime number, the period factor distribution of $(Q, *_\xi)$ is

$$\begin{cases} \begin{pmatrix} 1 & 2^m-1 \\ \frac{1}{2^m} & \frac{2^m-1}{2^m} \end{pmatrix}, & when \quad p \not\equiv 0 \ (\bmod(2^m-1)), \\ \begin{pmatrix} 1 & 2^m \\ \frac{1}{2^m} & \frac{2^m-1}{2^m} \end{pmatrix}, & when \quad p \not\equiv 0 \ (\bmod(2^m-1)). \end{cases}$$

Proof: Since the order of the field F is 2^m, there are $2^m(2^m–1)$ permutations in the Frobenius group. When $2^m – 1$ is a prime number, we know that the type of $\sigma_{\xi i}$ ($\xi \neq 1$, i = 1, 2, $\cdots$, 2^m) is $1^1(2^m–1)^1$. When $\xi = 1$, the type of σ_{11} is 1^{2^m} and the type of σ_{1i} (i = 2, 3, $\cdots$, 2^m) is $(2^m)^1$. From the proof of Theorem 3.5, we can get that the period factor distribution of $(Q, *_\xi)$.

Applying Corollary 3.6, we know that the possible value of $f_{*_\xi}^{(p)}$ is 1, 2^m–1, or 2^m. The expected value of $f_{*_\xi}^{(p)}$ is

$$E(f_{*_\xi}^{(p)}) = \begin{cases} \frac{2^{2m-1}-2^m+1}{2^{m-1}}, when \quad p \not\equiv 0 \ (\bmod 2^m-1), \\ \frac{2^{2m}-2^m+1}{2^m}, when \quad p \equiv 0 \ (\bmod 2^m-1). \end{cases} \qquad (1)$$

When the order of the field F is q^m ($q > 2$ is a prime), and $q^m – 1$ is a prime, then we can get a similar conclusion.

IV. Concluding Remarks

We have used the Frobenius group theory to discuss quasigroups with large period factors expected values. If the order of the quasigroup n is a prime power, the expected value of the period factors of the quasigroup based on operation $\alpha *_\xi \beta = \alpha\xi + \beta$ is

$$E(f_{*_\xi}^{(p)}) = \begin{cases} \frac{n^2-n+1}{n}, & when \quad p \equiv 0 \ (\bmod n-1), \\ \frac{n^2-2n+2}{n}, & when \quad p \equiv k \ (\bmod n-1), k \nmid n-1, \\ \frac{n^2-2n+k+1}{nk}, & when \quad p \equiv k \ (\bmod n-1), k \mid n-1. \end{cases}$$

If $n = 2^m$, and n–1is a prime number, then we have the best case as shown in Formula (1), and the best case is always obtained when n, the order of a quasigroup, is a prime power, and n–1 is a prime.

Acknowledgment

The authors would like to acknowledge the support of the National Natural Science Foundation of China under Grant No. 61373007 and Zhejiang Provincial Natural Science Foundation of China under Grant No. LY13F020039.

References

[1] V. Dimitrova, J. Markovski, On quasigroup pseudo random sequence generator, Proc. of the 1-st Balkan Conference in Informatics, Manolopoulos, Y. and Spirakis, P. eds., Thessaloniki, 21-13 Nov. 2004: 393--401.

[2] J. Dénes, A.D. Keedwell, Latin squares and Their Applications. Academic Press, New York and London, 1974.

[3] C. Kościelny, A methed of constructing quasigroup-based stream cipher. Appl. Math. and Comp. Sci. 6(1996) 109-121.

[4] S. Markovski, D. Gligoroski, S. Andova, Using quasigroups for one-one secure encoding. Proc. VIII Conf. Logic and Computer Science ``LIRA'97", Novi Sad, (1997) 157-162.

[5] S. Markovski, D. Gligoroski, V. Bakeva, Quasigroup string Processing-Part1, Contributions, Sec. math. Tech. Sci., MANU, XX, 1-2(1999) 13-28.

[6] D. Gligoroski, S. Markovski, L. Kocarev, M. Gusev, Edon80, eSTREAM, Report 2005/007 (2005).

[7] D. Gligoroski, S. Garkovski, S.J. Knapskog, The Stream Cipher Edon80, Lecture Notes in Computer Science 4986, 2008: 152-169.

[8] S. Markovski, Quasigroup string Processing and Applications in Cryptography, Proceedings 1st Conference of Mathematics and Informatics for Industry, Thessaloniki, Greece, (2003) 278-290.

[9] Y. Xu, On the Key-stream Periods Probability of Edon80 (preprint).

[10] D.D. John, B. Mortimer, Permutation Groups, Beijing World Publishing Corporation, 1997, pp. 85-91.