Contemporary Mathematics
http://ojs.wiserpub.com/index.php/CM/

UNIVERSAL WISER PUBLISHER

Research Article

# Randomness of Sequences of Numbers Using Permutation Polynomials over Prime Finite Fields

**Mansi Harish**[*], **Sagar Vinayak**, **Shalini Gupta**

Department of Mathematics & Statistics, Himachal Pradesh University, Shimla, India
E-mail: mansihverma16@gmail.com

**Received:** 9 May 2023; **Revised:** 30 July 2023; **Accepted:** 3 August 2023

**Abstract:** The randomness of a sequence plays an important role in cryptography like deciding the key, encryption and decryption algorithms. The sequences obtained by permutation polynomials over the finite fields have different properties which are used as random number generators. In the present paper, we have checked the randomness of sequence of numbers obtained from permutation polynomials over prime finite fields using different non-parametric statistical tests.

***Keywords*:** permutation polynomials, prime finite fields, randomness

**MSC:** 11T06, 11T71, 62G10

## 1. Introduction

For $q = p^r$ a prime power, where $r \in \mathbb{Z}^+$, let $\mathbb{F}_q$ be the finite field with $q$ elements. Finite field is an important aspect of modern algebra which has extensive applications in different areas such as coding theory, cryptography, Monte carlo, Pseudo Monte Carlo methods and wireless communication. It's development is tremendous during the last few decades.

For any finite field $\mathbb{F}_q$, let $\mathbb{F}_q[y]$ denotes the ring of polynomials. The polynomials over these finite structures are widely used in various areas of mathematical as well as other sciences. A one-one onto polynomial $f \in \mathbb{F}_q[y]$ is a Permutation Polynomial (PP) from $\mathbb{F}_q$ to itself. The initial study of permutation polynomials was developed by Dickson and Hermite [1] with subsequent contribution by others. Lidl and Mullen [2] worked deeply to find out the necessary condition for a polynomial to be permutation polynomial over a field. Charpin and Kyureghyan [3] constructed different permutation polynomials using monomial functions. Later on Cao et al. [4] constructed permutation polynomials from piecewise permutations.

Permutation polynomials over $\mathbb{F}_q[y]$ are widely used in coding theory, combinatorial design theory, etc. Ding and Zhou [5] used permutation polynomials over $\mathbb{F}_{2^m}$ to construct binary cyclic codes. In Yann [6], permutation polynomials are used to derive the equivalent form of Helleseth conjucture. Permutation polynomials are also used to improve the efficiency of Substitution-Permutation Network (SPN), Feistel networks and Lai-Massey design strategies, see [7]. Moreover, these polynomials are helpful in constructing bent functions which reduces the attacks on stream ciphers and block ciphers, see [8-10]. Permutation polynomials are studied to construct circular costas array which is further used in direction finding algorithms, see [11-12]. In block ciphers, S-box is constructed using a permutation in encryption

DOI: https://doi.org/10.37256/cm.4320233011

algorithm and inverse of permutation in decryption alogorithm.

The security of cryptographic systems is strongly related to randomness. Randomness [13] refers to the outcome of a probabilistic process that produces independent, uniformly distributed and unpredictable values that cannot be reliably reproduced. Origin of different cryptographic methods started with the use of different random numbers as a key in the encryption and decryption algorithms. For instance, in different categories of substitution ciphers either a single random digit $k_1$ or a pair of random digits $(k_1, k_2)$ are used as keys. However, these systems can easily be broken by using different attacks. This led to the use of Pseudo Random Number Generators (PRNGs) [14] which builds a sequence of random numbers. But these PRNGs exhibit some artifacts like lack of uniformity for large numbers, correlation of successive values and poor dimensional distribution of the output sequence which causes them to fail the criteria of randomness in some statistical tests. To overcome this, the sequence of permutation polynomials may be used as a random number. Bhatta et al. [15] studied the sequence of permutation polynomials over finite rings.

In the present paper, we have discussed the randomness of sequences of numbers obtained from permutation polynomials over prime finite fields. We have used Run test, Sign test and Spearman's test to check the randomness of the sequence of numbers using permutation polynomials.

## 2. Preliminaries

Here, we recall some preliminary results which are useful for the subsequent section.

**Theorem 2.1** [16] For odd $q$, the polynomial $y^{(q+1)/2} + ay \in \mathbb{F}_q[y]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $\eta(a^2 - 1) = 1$.

Since all the primes $p > 2$ are odd, so we can apply this theorem on every prime finite field. But to satisfy the condition of the $\eta(a^2 - 1) = 1$, the following remark is used.

**Remark 2.2** [16] We have $\eta(a^2 - 1) = 1$ if and only

$$a = (c^2 + 1)(c^2 - 1)^{-1}, \tag{1}$$

for some $c \in \mathbb{F}_q^*$ with $c^2 \neq 1$.

**Theorem 2.2** [16] For $a \in \mathbb{F}_q$, $q$ odd and let $r \in \mathbb{N}$ with $gcd(r, q - 1) = 1$. Prove that $x^r(x^{\frac{q-1}{2}} - a)^2$ is a permutation polynomial of $\mathbb{F}_q$ if $a \neq \pm 1$.

Using above theorems and remark, we have obtained permutation polynomials for different prime fields which are used in the following sections.

## 3. Statistical tests and randomness of sequences of numbers from permutation polynomials

The sequence of numbers generated using permutation polynomials may or may not be random. To check the randomness, we have used three statistical tests. Some of the statistical tests require the data to be normally distributed. However, in some cases it is possible to convert the given data in normal distribution but not in all cases. As a result, it is essential to apply statistical tests that do not need the data in any specific type of distribution. Such kind of tests are known as distribution free or non parametric tests. Run test, Sign test and Spearman's test are examples of distribution free tests. In this section, we have discussed the three tests and used them to check the randomness of sequences of numbers obtained from permutation polynomials. Note that the inputs in each test is according to the original sequence of elements of the finite field $\mathbb{F}_q$ i.e. $x_i = 0, 1, 2, ..., p - 1$ and the corresponding output $f(x_i)$ obtained from permutation polynomials is taken as main data for further investigations.

### 3.1 *Run test*

The test of significance devised to test the randomness of a sample is the run test [17] which is based on the theory of runs. A run is an arrangement of symbols or phenomenons of one kind surrounded (followed or proceeded) by a sequence of symbols or occurrences of other kind or by none at all.

**For example** Consider a sequence containing data elements Males ($M$) and Females ($F$) described as $\underbrace{MM}_{1}\ \underbrace{FF}_{2}\ \underbrace{MMMM}_{3}\ \underbrace{FFF}_{4}\ \underbrace{M}_{5}\ \underbrace{F}_{6}\ \underbrace{MMM}_{7}$. Thus, the sequence has 7 runs. These runs are used for further investigations.

A run test uses the following notations for a sample consisting of two kinds only:

$$q_1 = \text{number of symbols of first kind,}$$

$$q_2 = \text{number of symbols of second kind,}$$

$$k = q_1 + q_2 \text{ (total sample size),}$$

$$r = \text{number of runs in the sequence.}$$

It is not always necessary that the sample data is given in the form of symbols. It may be given in the form of numbers. In such cases, we firstly convert numbers into symbols using the median value and then in to runs. For instance, suppose $\{x_1, x_2, x_3, ..., x_n\}$ is the set of observations in numbers. We obtain the Median value (say $Md$) of the given set of sample and replace the numbers into symbols by the following manner:

(i) $A$, if the observation is $> Md$.

(ii) $B$, if the observation is $< Md$.

(iii) Ignore the number if value $= Md$.

Now, the mean of the given sample can be calculated from

$$\mu_r = \frac{2q_1q_2}{q_1 + q_2} + 1$$

and the standard error of the $r$ statistic is given by the formula

$$\sigma_r = \sqrt{\frac{2q_1q_2(2q_1q_2 - q_1 - q_2)}{(q_1 + q_2)^2(q_1 + q_2 - 1)}}.$$

Further, the following equation is used to standardize $r$

$$z = \frac{r - \mu_r}{\sigma_r}.$$

Set $\alpha$ as the significance level which decides whether the sequence is accepted or rejected. Usually, there are distinct levels of significance like 0.01, 0.05, 0.10 depending upon the requirements of precision. Here, we set $\alpha = 0.05$, that is, 5% level of significance. According to this level of significance, the $z$ value must lie in between -1.96 to +1.96. If the $z$ value lies within this range, then the sequence is considered as random with 95% accuracy.

The sequence of sample observations is not considered to be random if we have the following two conditions:

(i) If the similar items cluster together, resulting in too few runs.

(ii) If the similar items alternatively mix, resulting in too many runs.

Now, we are applying the run test to check the randomness of sequence of numbers obtained from permutation polynomials over prime finite fields. The computed $z$ values of certain PPs over $\mathbb{F}_{11}$, $\mathbb{F}_{13}$, $\mathbb{F}_{17}$, $\mathbb{F}_{19}$, $\mathbb{F}_{23}$ and $\mathbb{F}_{29}$ are presented in Table 1, Table 2, Table 3, Table 4, Table 5 and Table 6, respectively.

**Table 1.** $z$ values of PPs over $\mathbb{F}_{11}$

| Permutation polynomial | Number of runs | $z$ |
|---|---|---|
| $y^6 + 9y$ | 5 | -0.671 |
| $y^6 + 4y$ | 8 | 1.342 |
| $y^6 + 7y$ | 8 | 1.342 |
| $y^6 + 2y$ | 4 | -1.342 |
| $y^{11} + 7y^6 + 4y$ | 5 | -0.671 |

In Table 1, $f(x_i) - M$ (median) corresponding to polynomials $y^6 + 4y$ and $y^6 + 7y$ are

$$\underbrace{-5}_{1},\ \underbrace{11}_{2},\ \underbrace{-1}_{3},\ \underbrace{4}_{4},\ \underbrace{-2}_{5},\ \underbrace{2, 5}_{6},\ \underbrace{-3, -4}_{7},\ \underbrace{3}_{8}$$

and

$$\underbrace{-5}_{1},\ \underbrace{3}_{2},\ \underbrace{-4, -3}_{3},\ \underbrace{5, 2}_{4},\ \underbrace{-2}_{5},\ \underbrace{4}_{6},\ \underbrace{-1}_{7},\ \underbrace{1}_{8}$$

respectively. Here 0 is ignored, so sequence is categorized as positive and negative numbers of two kinds instead of symbols. Hence, both the sequences have 8 runs. The value of $z$ are lying in the range -1.96 to 1.96. Therefore, the sequence of numbers obtained by these permutation polynomials over $\mathbb{F}_{11}$ are random.

**Table 2.** $z$ values of PPs over $\mathbb{F}_{13}$

| Permutation polynomial | Number of runs | $z$ |
|---|---|---|
| $y^7 + 6y$ | 9 | 1.21 |
| $y^7 + 11y$ | 3 | -2.42 |
| $y^7$ | 8 | 0.60 |
| $y^7 + 7y$ | 7 | 0 |
| $y^{10} + y^7 + y^4 + 3y$ | 4 | -1.81 |

The values of $z$ obtained in Table 2 lies in the range -1.96 to 1.96 except in the case of permutation polynomial $y^7 + 11y$. So, the sequence of numbers obtained from all permutation polynomials over $\mathbb{F}_{13}$ are considered as random expect for $y^7 + 11y$.

**Table 3.** $z$ values of PPs over $\mathbb{F}_{17}$

| Permutation polynomial | Number of runs | $z$ |
|---|---|---|
| $y^9 + 13y$ | 9 | 0 |
| $y^9 + 14y$ | 9 | 0 |
| $y^9 + 11y$ | 11 | 1.035 |
| $y^9 + 6y$ | 8 | -0.517 |
| $y^9 + 3y$ | 4 | -2.58 |
| $y^{15} + y^{11} + y^7 + 8y^3$ | 11 | 1.034 |
| $y^{13} + y^9 + y^5 + 8y$ | 13 | 2.069 |

In Table 3, the value of $z$ corresponding to $y^9 + 3y$ does not lie in the given significant range, so the sequence of numbers of all the above permutation polynomials are random expect $y^9 + 3y$ and $y^{13} + y^9 + y^5 + 8y$.

**Table 4.** $z$ values of PPs over $\mathbb{F}_{19}$

| Permutation polynomial | Number of runs | $z$ |
|---|---|---|
| $y + 4$ | 3 | -3.401 |
| $y^{10} + 8y$ | 16 | 2.926 |
| $y^{10} + 6y$ | 10 | 0 |
| $y^{10} + 10y$ | 14 | 1.951 |
| $y^{10} + 9y$ | 14 | 1.951 |
| $y^{10} + 13y$ | 11 | 0.487 |
| $y^{10} + 5y$ | 10 | 0 |
| $y^{10} + 14y$ | 11 | 0.487 |
| $y^{10} + 11y$ | 16 | 2.926 |
| $y^{19} + 13y^{10} + 9y$ | 9 | -0.486 |
| $y^{19} + 11y^{10} + 16y$ | 12 | 0.972 |

Similarly, the sequences corresponding to $y + 4$, $y^{10} + 8y$ and $y^{10} + 11y$ are rejected to be considered as random in Table 4.

In this case as shown in Table 5, all the sequences corresponding to permutation polynomials except $y + 5$ over $\mathbb{F}_{23}$ are accepted to be considered as random.

**Table 5.** $z$ values of PPs over $\mathbb{F}_{23}$

| Permutation polynomial | Number of runs | $z$ |
|---|---|---|
| $y + 5$ | 3 | -3.933 |
| $y^{12} + 17y$ | 13 | 0.346 |
| $y^{12} + 7y$ | 11 | -0.346 |
| $y^{12} + 18y$ | 13 | 0.346 |
| $y^{12} + 3y$ | 10 | 0.874 |
| $y^{12} + 5y$ | 12 | 0 |
| $y^{12} + 2y$ | 10 | 0.874 |
| $y^{12} + 16y$ | 13 | 0.346 |
| $y^{12} + 20y$ | 11 | -0.346 |
| $y^{12} + 21y$ | 11 | -0.346 |
| $y^{12} + 6y$ | 12 | 0 |
| $y^{23} + 15y^{12} + 16y$ | 10 | 0.874 |
| $y^{23} + 17y^{12} + 9y$ | 13 | 0.346 |

**Table 6.** $z$ values of PPs over $\mathbb{F}_{29}$

| Permutation polynomial | Number of runs | $z$ |
|---|---|---|
| $y^{15} + 21y$ | 15 | 0 |
| $y^{15} + 23y$ | 15 | 0 |
| $y^{15} + 18y$ | 15 | 0 |
| $y^{15} + 11y$ | 20 | 1.926 |
| $y^{15} + 24y$ | 9 | -2.3112 |
| $y^{15} + 13y$ | 20 | 1.926 |
| $y^{15} + 6y$ | 14 | -0.385 |
| $y^{15} + 16y$ | 21 | 2.311 |
| $y^{15} + 20y$ | 17 | 0.346 |
| $y^{15} + 8y$ | 12 | -1.155 |
| $y^{15} + 9y$ | 12 | -1.155 |
| $y^{15} + 13y$ | 12 | -1.155 |
| $y^{22} + y^{15} + y^{8} + 9y$ | 16 | -3.709 |
| $y^{22} + y^{15} + y^{8} + 17y$ | 22 | -2.11 |

Here in Table 6, the sequences corresponding to $y^{15} + 24y$, $y^{15} + 16y$, $y^{22} + y^{15} + y^{8} + 9y$ and $y^{22} + y^{15} + y^{8} + 17y$ are rejected to be considered as random.

## 3.2 *Sign test*

The sign test [17] is based on the signs that is, it uses only positive and negative signs to perform the test. It can be applied on a single median data as well as median of paired differences for two dependent population data.

In this test, if the sample size is 25 or less, then it is considered as small sample. In case the sample size is > 25, then it is said to be large sample and we can use the normal probability distribution. However, normal distribution may not provide correct observations because the sequence generated by elements of finite field is finite but we need infinite elements for normal distribution, so binomial distribution is used for the same.

Let $n$ be the number of entries in the data, $M$ be the median of the data and $p$ be the probability value. In our null hypothesis, we consider half observations below the median and half above the median. The general step by step procedure for sign test is shown below:

**Step 1:** Calculate the number of entries in the data which are greater than $M$ and call it $r^+$. Similarly, calculate the number of entries in the data which are less than $M$ and call it $r^-$. Ignore the entries which are equal to the median $M$ of the given data.

**Step 2:** Now, calculate the sum of $r^+$ and $r^-$, that is, $(r^+ + r^-)$ and call it $n'$.

**Step 3:** Select $r = \min(r^-, r^+)$.

**Step 4:** The $p$ value is calculated using the Table IV given in [18].

Under null hypothesis, both $r^+$ and $r^-$ will satisfy binomial distribution with $p = 0.5$ and $n = n'$. If the test is one sided, then the probability value obtained from binomial distribution table is the $p$ value. If the test is paired sided, then two times of the probability value given by binomial distribution table is the required $p$ value. Hence, if the $p$ value is obtained less than 0.05, then we will reject the null hypothesis otherwise, we will fail to reject the null hypothesis.

Now, we are applying sign test to check the randomness of sequence of numbers obtained from permutation polynomials. To apply sign test in paired data, we consider two sequences one of which is the original sequence $x_i = 0, 1, 2, ..., p - 1$ of the elements of finite field and other is output of the first sequence (say $y_i$) over permutation polynomials. The difference $x_i - y_i$ is calculated and same process is followed from the step 2 to calculate the corresponding $p$ value. The computed $p$ values of certain PPs over $\mathbb{F}_{11}$, $\mathbb{F}_{13}$, $\mathbb{F}_{19}$ and $\mathbb{F}_{23}$ are presented in Table 7, Table 8, Table 9 and Table 10, respectively.

**Table 7.** $p$ values of PPs over $\mathbb{F}_{11}$

| Permutation polynomial | Positive difference | Negative difference | Ties | $p$ |
|---|---|---|---|---|
| $y + 2$ | 9 | 2 | 0 | 0.065 |
| $y^6 + 9y$ | 6 | 4 | 1 | 0.754 |
| $y^6 + 4y$ | 6 | 4 | 1 | 0.754 |
| $y^6 + 7y$ | 4 | 6 | 1 | 0.754 |
| $y^6 + 2y$ | 2 | 3 | 6 | 1 |

**Table 8.** $p$ values of PPs over $\mathbb{F}_{13}$

| Permutation polynomial | Positive difference | Negative difference | Ties | $p$ |
|---|---|---|---|---|
| $y + 3$ | 10 | 3 | 0 | 0.092 |
| $y^7$ | 3 | 3 | 7 | 1 |
| $y^7 + 6y$ | 6 | 6 | 1 | 1 |
| $y^7 + 2y$ | 3 | 3 | 7 | 1 |
| $y^7 + 7y$ | 6 | 6 | 1 | 1 |
| $y^7 + 11y$ | 6 | 6 | 1 | 1 |

**Table 9.** $p$ values of PPs over $\mathbb{F}_{19}$

| Permutation polynomial | Positive difference | Negative difference | Ties | $p$ |
|---|---|---|---|---|
| $y + 4$ | 15 | 4 | 0 | 0.019 |
| $y^{10} + 6y$ | 9 | 9 | 1 | 1 |
| $y^{10} + 9y$ | 9 | 9 | 1 | 1 |
| $y^{10} + 5y$ | 10 | 8 | 1 | 0.815 |
| $y^{10} + 14y$ | 9 | 9 | 1 | 1 |
| $y^{10} + 11y$ | 9 | 9 | 1 | 1 |
| $y^{10} + 13y$ | 8 | 10 | 1 | 0.815 |

**Table 10.** $p$ values of PPs over $\mathbb{F}_{23}$

| Permutation polynomial | Positive difference | Negative difference | Ties | $p$ |
|---|---|---|---|---|
| $y + 5$ | 18 | 5 | 0 | 0.011 |
| $y^{12} + 17y$ | 11 | 11 | 1 | 1 |
| $y^{12} + 7y$ | 11 | 11 | 1 | 1 |
| $y^{12} + 18y$ | 11 | 11 | 1 | 1 |
| $y^{12} + 3y$ | 11 | 11 | 1 | 1 |
| $y^{12} + 5y$ | 8 | 14 | 1 | 0.286 |
| $y^{12} + 2y$ | 7 | 4 | 11 | 0.549 |
| $y^{12} + 16y$ | 14 | 8 | 1 | 0.286 |
| $y^{12} + 20y$ | 8 | 14 | 1 | 0.286 |
| $y^{12} + 21y$ | 11 | 11 | 1 | 1 |
| $y^{12} + 6y$ | 11 | 11 | 1 | 1 |

In the above tables, according to the significance level of 5%, the sequences of numbers corresponding to permutation polynomials $y + 4$ over $\mathbb{F}_{19}$ and $y + 5$ over $\mathbb{F}_{23}$ have $p$ value less than 0.05. Hence, considered as random whereas all the other sequences corresponding to other permutation polynomials are rejected to be considered as random.

### 3.3 *The Spearman's rho rank correlation coefficient test*

The Spearman's rho rank correlation coefficient test [17] decides the class of relationship between data from populations with unknown distributions. This test is used to identify and test the strength of relationship between two sets of data. Here, $r_s$ is the Spearman's rho rank correlation coefficient for sample data. $r_s$ is simply the linear correlation coefficient between the ranks of the data on variables $a$ and $b$. However, by previous arguments sequence $x_i$ and its output over permutation polynomial $y_i$ will work as data variables $a$ and $b$ respectively. We do not need to make any assumptions about the sequences $x_i$ and $y_i$ to construct a test of the hypothesis about $r_s$.

The ranks of the sequences are considered as given in the following Table 11. Here $x_1$ and $y_2$ are two given sequences. The elements are ranked in increasing order and denoted the corresponding ranks by $r_1$ and $r_2$. However, the elements can also be ranked in decreasing order as per convenience.

**Table 11.** Ranks of sequences $x_1$ and $y_2$

| $x_1$ | $r_1$ | $y_2$ | $r_2$ |
|---|---|---|---|
| 12 | 1 | 113 | 2 |
| 17 | 2 | 110 | 1 |
| 27 | 5 | 121 | 5 |
| 22 | 4 | 115 | 3 |
| 15 | 3 | 117 | 4 |

Following procedure is carried out to calculate the value of $r_s$:

**Step 1:** Rank the given elements corresponding to sequences $x_i$ and $y_i$ separately.

**Step 2:** Denote the ranks by $r_1$ and $r_2$ respectively.

**Step 3:** Take the difference between each pair of ranks and denote it by $d$. Thus, $d = r_1 - r_2$.

**Step 4:** Square each difference $d$ and find $\sum d^2$.

**Step 5:** Finally, calculate the value of $r_s$ using the formula

$$r_s = 1 - \frac{6\sum d^2}{n(n^2 - 1)}.$$

The $t$ value is calculated using the formula

$$t = r_s\sqrt{\frac{n-2}{1-r_s^2}}$$

and D o F denotes the degrees of freedom which in this case is $n - 2$ and finally, the $p$ value is calculated using bionomial distribution table.

Now, we are applying Spearman's test rho rank correlation coefficient to check the randomness of the sequence of the numbers obtained using permutation polynomials. The computed $p$ values of some PPs over $\mathbb{F}_{11}$, $\mathbb{F}_{13}$, $\mathbb{F}_{17}$, $\mathbb{F}_{19}$, $\mathbb{F}_{23}$, $\mathbb{F}_{29}$ and $\mathbb{F}_{31}$ are presented in Table 12, Table 13, Table 14, Table 15, Table 16, Table 17 and Table 18, respectively.

**Table 12.** $p$ values of PPs over $\mathbb{F}_{11}$

| Permutation polynomial | $n$ | $r_s$ | $t$ value | D o F | $p$ |
|---|---|---|---|---|---|
| $y^6 + 9y$ | 10 | -0.6 | -2.121 | 8 | 0.0688 |
| $\mathrm{y}^6 + 4y$ | 10 | 0.06 | 0.189 | 8 | 0.854 |
| $\mathrm{y}^6 + 2y$ | 10 | 0.6 | 2.12 | 8 | 0.0688 |
| $y^{11} + 7y^6 + 4y$ | 10 | 0.33 | 0.989 | 8 | 0.351 |

**Table 13.** $p$ values of PPs over $\mathbb{F}_{13}$

| Permutation polynomial | $n$ | $r_s$ | $t$ value | D o F | $p$ |
|---|---|---|---|---|---|
| $y^7$ | 12 | 0.364 | 1.23 | 10 | 0.2452 |
| $y^7 + 6y$ | 12 | -0.2727 | -0.89 | 10 | 0.39 |
| $y^7 + 2y$ | 12 | 0.2727 | 0.896 | 10 | 0.391 |
| $y^7 + 7y$ | 12 | -0.636 | -2.608 | 10 | 0.02609 |
| $y^7 + 11y$ | 12 | -0.818 | -4.5 | 10 | 0.0011 |
| $y^{10} + y^7 + y^4 + 3y$ | 12 | 0.181 | 0.5819 | 10 | 0.5735 |

**Table 14.** $p$ values of PPs over $\mathbb{F}_{17}$

| Permutation polynomial | $n$ | $r_s$ | $t$ value | D o F | $p$ |
|---|---|---|---|---|---|
| $y^9$ | 16 | 0.4 | 1.633 | 14 | 0.1247 |
| $y^9 + 13y$ | 16 | -0.05 | -0.187 | 14 | 0.854 |
| $y^9 + 14y$ | 16 | -0.45 | -1.885 | 14 | 0.0802 |
| $y^9 + 11y$ | 16 | -0.5 | -2.1602 | 14 | 0.04858 |
| $y^9 + 6y$ | 16 | -0.4 | -0.1633 | 14 | 0.124 |
| $y^{15} + y^{11} + y^7 + 8y^3$ | 16 | 0.197 | 0.7518 | 14 | 0.464 |
| $y^{13} + y^9 + y^5 + 8y$ | 16 | 0.297 | 1.1642 | 14 | 0.2638 |

**Table 15.** $p$ values of PPs over $\mathbb{F}_{19}$

| Permutation polynomial | $n$ | $r_s$ | $t$ value | D o F | $p$ |
|---|---|---|---|---|---|
| $y^{10} + 6y$ | 18 | 0.137 | 0.554 | 16 | 0.587 |
| $y^{10} + 9y$ | 18 | 0.176 | 0.717 | 16 | 0.483 |
| $y^{10} + 5y$ | 18 | 0.0196 | 0.0784 | 16 | 0.9384 |
| $y^{10} + 14y$ | 18 | -0.0196 | -0.0784 | 16 | 0.93844 |
| $y^{10} + 11y$ | 18 | 0.176 | 0.717 | 16 | 0.483 |
| $y^{10}+ 13y$ | 18 | -0.137 | -0.5542 | 16 | 0.587 |
| $y^{19} + 13y^{10} + 9y$ | 18 | 0.019 | 0.076 | 16 | 0.94 |
| $y^{19} + 11y^{10} + 16y$ | 18 | -0.29 | 1.1213 | 16 | 0.24 |

**Table 16.** $p$ values of PPs over $\mathbb{F}_{23}$

| Permutation polynomial | $n$ | $r_s$ | $t$ value | D o F | $p$ |
|---|---|---|---|---|---|
| $y^{12} + 17y$ | 22 | -0.0389 | 0.1743 | 20 | 0.8633 |
| $y^{12} + 7y$ | 22 | 0.246 | 1.138 | 20 | 0.268 |
| $y^{12} + 18y$ | 22 | -0.22 | -1.1023 | 20 | 0.3234 |
| $y^{12} + 3y$ | 22 | 0.3246 | 1.5351 | 20 | 0.1404 |
| $y^{12} + 5y$ | 22 | 0.2207 | 1.012 | 20 | 0.323 |
| $y^{12} + 2y$ | 22 | 0.6363 | 3.689 | 20 | 0.00145 |
| $y^{12} + 16y$ | 22 | -0.2467 | -1.1387 | 20 | 0.2682 |
| $y^{12} + 20y$ | 22 | -0.3246 | -1.5351 | 20 | 0.1404 |
| $y^{12} + 21y$ | 22 | -0.6363 | -3.689 | 20 | 0.00145 |
| $y^{12} + 6y$ | 22 | 0.03896 | 0.1743 | 20 | 0.8633 |
| $y^{23} + 15y^{12} + 16y$ | 22 | 0.1689 | 4.5371 | 20 | 0.452 |
| $y^{23} + 17y^{12} + 9y$ | 22 | 0.1168 | 0.526 | 20 | 0.6 |

**Table 17.** $p$ values of PPs over $\mathbb{F}_{29}$

| Permutation polynomial | $n$ | $r_s$ | $t$ value | D o F | $p$ |
|---|---|---|---|---|---|
| $y^{15} + 21y$ | 28 | 0.0634 | 0.3244 | 26 | 0.7482 |
| $y^{15} + 23y$ | 28 | 0.0317 | 0.1619 | 26 | 0.8725 |
| $y^{15} + 2y$ | 28 | 0.36 | 1.99 | 26 | 0.056 |
| $y^{15} + 18y$ | 28 | -0.263 | -1.39 | 26 | 0.1758 |
| $y^{15} + 11y$ | 28 | 0.0317 | 0.1619 | 26 | 0.8725 |
| $y^{15} + 24y$ | 28 | 0.0476 | 0.243 | 26 | 0.8098 |
| $y^{15} + 13y$ | 28 | -0.1428 | -0.7359 | 26 | 0.4683 |
| $y^{15} + 6y$ | 28 | 0.0391 | 0.199 | 26 | 0.8433 |
| $y^{15} + 16y$ | 28 | 0.262 | 1.384 | 26 | 0.178 |
| $y^{15} + 20y$ | 28 | -0.168 | -0.8719 | 26 | 0.3912 |
| $y^{15} + 8y$ | 28 | -0.16077 | -0.8305 | 26 | 0.413 |
| $y^{15} + 9y$ | 28 | 0.133 | 0.6865 | 26 | 0.4984 |
| $y^{15} + 13y$ | 28 | -0.154 | -0.799 | 26 | 0.4311 |
| $y^{22} + y^{15} + y^{8} + 10y$ | 28 | -0.047 | -4.008 | 26 | 0.00069 |
| $y^{22} + y^{15} + y^{8} + 17y$ | 28 | 0.047 | 4.008 | 26 | 0.00069 |

**Table 18.** $p$ values of PPs over $\mathbb{F}_{31}$

| Permutation polynomial | $n$ | $r_s$ | $t$ value | D o F | $p$ |
|---|---|---|---|---|---|
| $y^{16} + 12y$ | 30 | 0.0482 | 0.255 | 28 | 0.800 |
| $y^{16} + 9y$ | 30 | -0.0069 | -0.0364 | 28 | 0.9711 |
| $y^{16} + 28y$ | 30 | -0.338 | -1.89 | 28 | 0.0677 |
| $y^{16} + 14y$ | 30 | -0.227 | -1.23 | 28 | 0.226 |
| $y^{16} + 17y$ | 30 | 0.227 | 1.23 | 28 | 0.226 |
| $y^{16} + 23y$ | 30 | -0.0896 | -0.476 | 28 | 0.637 |
| $y^{16} + 3y$ | 30 | 0.338 | 1.899 | 28 | 0.0677 |
| $y^{16} + 8y$ | 30 | 0.0896 | 0.476 | 28 | 0.637 |
| $y^{16} + 22y$ | 30 | 0.00689 | 0.0364 | 28 | 0.971 |
| $y^{16} + 16y$ | 30 | -0.1724 | -0.926 | 28 | 0.3622 |
| $y^{16} + 6y$ | 30 | 0.0620 | 0.329 | 28 | 0.7445 |
| $y^{16} + 25y$ | 30 | -0.062 | -0.329 | 28 | 0.7445 |
| $y^{16} + 15y$ | 30 | 0.40 | 0.2119 | 28 | 0.8337 |
| $y^{16} + 19y$ | 30 | -0.048 | -0.2557 | 28 | 0.8 |
| $y^{31} + 25y^{16} + 9y$ | 30 | 0.338 | 1.9 | 28 | 0.067 |
| $y^{31} + 27y^{16} + 4y$ | 30 | 0.5448 | 3.438 | 28 | 0.0018 |

In the above tables, according to the 5% significance level, the sequence of numbers corresponding to polynomials $y^7 + 7y$, $y^7 + 11y$ over $\mathbb{F}_{13}$, $y^9 + 11y$ over $\mathbb{F}_{17}$, $y^{12} + 2y$, $y^{12} + 21y$ over $\mathbb{F}_{23}$, $y^{22} + y^{10} + y^8 + 10y$, $y^{22} + y^{10} + y^8 + 17y$ over $\mathbb{F}_{29}$ and $y^{31} + 25y^{16} + 9y$, $y^{31} + 27y^{16} + 4y$ over $\mathbb{F}_{31}$ have value of $p$ less than 0.05. Hence, sequence of numbers of these permutations polynomials are considered as random.

## 4. Comparative analysis

Here, the comparison of run test, sign test and Spearman's rank test is shown in the following Table 19:

**Table 19.** Comparative analysis

| Permutation polynomial | Field | Run test<br>($z$) | Sign test<br>($p$) | Spearman's test<br>($p$) |
|---|---|---|---|---|
| $y^7 + 7y$ | $\mathbb{F}_{13}$ | 0 | 1 | 0.02609 |
| $y^7 + 11y$ | $\mathbb{F}_{13}$ | 2.42 | 1 | 0.0011 |
| $y + 4$ | $\mathbb{F}_{19}$ | -3.401 | 0.019 | 0.4838 |
| $y^9 + 11y$ | $\mathbb{F}_{17}$ | 1.035 | - | 0.04858 |
| $y^{10} + 13y$ | $\mathbb{F}_{19}$ | 0.487 | 0.815 | 0.587 |
| $y^{12} + 2y$ | $\mathbb{F}_{23}$ | 0.874 | 0.549 | 0.00145 |
| $y^{12} + 21y$ | $\mathbb{F}_{23}$ | -0.346 | 1 | 0.00145 |
| $y + 5$ | $\mathbb{F}_{23}$ | -3.93 | 0.011 | 0.0001 |
| $y^{22} + y^{15} + y^8 + 17y$ | $\mathbb{F}_{29}$ | -2.11 | - | 0.00069 |

We can easily observe that $y^7$+ $7y$ over $\mathbb{F}_{13}$, $y^9$+ $11y$ over $\mathbb{F}_{17}$ and $y^{12}$+ $2y$, $y^{12}$+$21y$ over $\mathbb{F}_{23}$ are accepted as random in run test and Speraman's test but rejected by sign test. However, the polynomials $y^7 + 11y$ over $\mathbb{F}_{13}$ and $y^{22} + y^{15} + y^8 + 17y$ over $\mathbb{F}_{29}$ is accepted by Spearman's test but rejected by both sign test and run test. Moreover, $y + 4$ over $\mathbb{F}_{19}$ and $y + 5$ over $\mathbb{F}_{23}$ are accepted by sign test. Since sign test works only upon the negative and positive signs without considering the amount of variation from median, it is little weaker as compared to run test and Spearman's test. So, the confirmation of randomness corresponding to a particular sequence of permutation polynomial can be decided either by satisfying all three tests or atleast two stronger tests.

## 5. Conclusion

In the present paper, we used statistical tests on the permutation polynomials over the prime finite fields to obtain the value of parameter $p$ in different cases which decides the randomness in a particular sequence of numbers corresponding to permutation polynomial. These permutation polynomials may be used to improve the key generation process which helps in security and time components of different cryptographic algorithms. In future, the randomness of sequences corresponding to permutation polynomials over extension fields may be considered as a major scope in this area.

## Acknowledgements

The second author thankfully acknowledge the financial assistance of CSIR. The authors would like to thank the anonymous reviewers for their valuable comments and helpful suggestions which improved both the quality and presentation of this paper.

## Conflict of interest

The authors declare no conflict of interest.

## References

[1] Dickson LE. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *The Annals of Mathematics*. 1896; 11(1/6): 65-120.

[2] Lidl R, Mullen GL. When does a polynomial over a finite field permute the elements of the field? *The American Mathematical Monthly*. 1988; 95(3): 243-246.

[3] Charpin P, Kyureghyan G. Monomial functions with linear structure and permutation polynomials. *Finite Fields: Theory and Applications*. 2010; 518: 99-111.

[4] Cao X, Hu L, Zha Z. Constructing permutation polynomials from piecewise permutation. *Finite Fields and Their Applications*. 2014; 26: 162-174.

[5] Ding C, Zhou Z. Binary cyclic codes from explicit polynomials over GF($2^m$). *Discrete Mathematics*. 2014; 321: 76-89.

[6] Laigle-Chapuy Y. Permutation polynomials and applications to coding theory. *Finite Fields and Their Applications*. 2007; 13(1): 58-70.

[7] Roy A, Steiner M. *An algebraic system for constructing cryptographic per-mutations over finite fields*. arXiv. Available from: doi: 10.48550/arXiv.2204.01802.

[8] Coulter RS, Mesnager S. Bent functions from involutions over $\mathbb{F}_{2^n}$. *IEEE Transactions on Information Theory*. 2017; 64(4): 2979-2986.

[9] Mesnager S. Further constructions of infinite families of bent functions from new permutations and their duals. *Cryptography and Communications*. 2016; 8(2): 229-246.

[10] Mesnager S. On constructions of bent functions from involutions. *IEEE International Symposium on Information Theory*. 2016; 110-114. Available from: doi: 10.1109/ISIT.2016.7541271.

[11] Golomb SW, Moreno O. On periodicity properties of costas arrays and a conjecture on permutation polynomials. *IEEE Transactions on Information Theory*. 1996; 42(6): 2252-2253.

[12] Tan CM, Fletcher P, Beach MA, Nix AR, Landmann M, Thoma RS. On the application of circular arrays in direction finding part I: Investigation into the estimation algorithms. *1st Annual COST*. 2002; 273: 29-30.

[13] Schneier B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New Jersey: John Wiley & Sons; 2007.

[14] James F. A review of pseudorandom number generators. *Computer Physics Communications*. 1990; 60(3): 329-344.

[15] Vadiraja Bhatta GR, Shankar BR, Mishra VN, Poojary P. Sequences of numbers via permutation polynomials over some finite rings. *Proyecciones (Antofagasta)*. 2020; 39(5): 1295-1313.

[16] Lidl R, Niederreiter H. *Finite Fields*. No. 20. United Kingdom: Cambridge University Press; 1997.

[17] Mann PS. *Introductory Statistics*. New Jersey: John Wiley & Sons; 2007.

[18] Walker HM, Lev J. *Statistical Inference*. New York: Henry Holt and Company. Inc.; 1953. Available from: doi: 10.1037/11773-000.