Proyecciones (Antofagasta. On line) | vol. 39, n. 5 (2020) | pp. 1295-1313.

10.22199/issn.0717-6279-2020-05-0079

PROYECCIONES
Journal of Mathematics

ISSN 0717-6279 (On line)

Sequences of numbers via permutation polynomials over some finite rings

G. R. Vadiraja Bhatta[1] orcid.org/0000-0003-0631-0205
B. R. Shankar[2] orcid.org/0000-0001-5084-0567
Vishnu Narayan Mishra[3] orcid.org/0000-0002-2159-7710
Prasanna Poojary[4] orcid.org/0000-0002-0749-8994

[1]Manipal Academy of Higher Education, Dept. of Mathematics, Center for cryptography, Manipal, KA, India. vadiraja.bhatta@manipal.edu
[2]National Institute of Technology Karnataka, Dept. of Mathematical and Computational Sciences, Surathkal, KA, India. brs@nitk.ac.in
[3]Indira Gandhi National Tribal University, Dept. of Mathematics, Amarkantak, MP, India. vishnunarayanmishra@gmail.com
[4]Manipal Academy of Higher Education, Department of Mathematics, Manipal, KA, India. poojaryprasanna34@gmail.com

Received: January 2020 | Accepted: March 2020

Abstract:

A polynomial can represent every function from a finite field to itself. The functions which are also permutations of the field give rise to permutation polynomials, which have potential applications in cryptology and coding theory. Permutation polynomials over finite rings are studied with respect to the sequences they generate. The sequences obtained through some permutation polynomials are tested for randomness by carrying out known statistical tests. Random number generation plays a major role in cryptography and hence permutation polynomials may be used as random number generators.

Keywords: Permutation polynomial; Ring; Statistical tests; Cryptography.
MSC (2020): 05B15.

Cite this article as (IEEE citation style):

G. R. Vadiraja Bhatta, B. R. Shankar, V. N. Mishra, and P. Poojary, "Sequences of numbers via permutation polynomials over some finite rings", *Proyecciones (Antofagasta, On line)*, vol. 39, no. 5, pp. 1295-1313, Oct. 2020, doi: 10.22199/issn.0717-6279-2020-05-0079.

1. Introduction

Finite fields and finite rings are interesting algebraic concepts in modern mathematics. These algebraic structures are being studied for both theoretical and practical purposes. Because of their great algebraic properties and finiteness, they are considered widely in modern applications. Polynomials over these finite structures induce some more mathematical properties. Some practical questions arise when we try to find polynomials effecting permutations. Obviously, such questions lead to find their practical applications. Permutation polynomials have increasingly attracted the attention of various researchers in the past couple of decades. As an introduction to the subject the inspiring survey papers were given by Lidl and Mullen [12, 10].

Various cryptographic applications, including a key exchange protocol for public key cryptography based on permutation polynomials have been proposed. Permutations of finite fields have become of considerable interest in the construction of cryptographic systems for the secure transmission of data. Let M be a message (0r an element of a finite field F_q) which is to be sent securely from A to B. If $P(x)$ is a permutation polynomial of F_q, then A sends to B the field element $N = P(M)$. Since $P(x)$ is a bijection B can obtain the original message M by calculating $P^{-1}(N) = P^{-1}(P(M)) = M$. $P(x)$ should have a simple form so that if M is a message, then $N = P(M)$ which is sent from A to B can be easily computed. Also $P(x)$ must have the property that without some secrete information (the key) that only A and B know, $P^{-1}(x)$ will be hard or impossible to get, so that an unauthorized receiver can not calculate $P^{-1}(N)$. At the same time, with knowledge of the key, $P^{-1}(x)$ is easily obtained by B so that $P^{-1}(N) = M$ can be recovered by B.

Permutation functions have been studied since the last century. In recent years considerable attention has been given to their potential applications in public key cryptography. The importance of permutation functions lies in the fact that they connect two essential components of the theory of finite fields: combinatorics and algebra. The permutation property and the applications in cryptography are of combinatorial nature and the use of polynomials or rational functions for representing these combinatorial objects allows powerful algebraic methods to be employed. It is the same type of synthesis that has worked very successfully in the theory of error correcting codes. One can hope for more generalization of the permutation polynomial functions over finite rings and finite fields with the concept of

invexity assumptions as in [13] and over ring as in [18]. Moreover it may be interesting to study orthogonality properties of the permutation polynomials too in the line of Chebyshevs polynomials or pseudo-Chebyshevs polynomials in [7, 11, 21]. But here we restrict ourselves only to study the behavior of certain permutation polynomials with respect to the randomness of the sequences they generated.

Definition 1.1. *Assume* $f(x) = a_n x^n + ... + a_1 x + a_0$ *is a polynomial of degree* $n \geq 1$ *modulo* m*, where* $a_n = 0 \ (mod\ m)$*. If* $f(x) = ((a_n x^n + ... + a_1 x + a_0) \ mod \ m)$ *forms a bijection* $F : \{0, 1, ..., m-1\} \to \{0, 1, ..., m-1\}$*, we say that* $f(x)$ *is a* **permutation polynomial modulo m**. *The bijection* F *is called the* **induced bijection** *of the polynomial* $f(x)$ *modulo* m*.*

Definition 1.2. *If two permutation polynomial are equivalent modulo* m*, we say they are* **equivalent** *permutation polynomial modulo* m*. It is obvious that equivalent permutation polynomials modulo* m *induce the same bijection over* $\{0,1,...,m\text{-}1\}$*.*

Pinaki [9] related the number of permutation polynomials in,$F_q[x]$ of degree $d \leq q-2$ to the solutions $(x_1, x_2, ..., x_q)$ of a system of linear equations over F_q, with the added restriction that $x_i = 0$ and $x_i = x_j$ whenever $i = j$. Using this he find an expression for the number of permutation polynomials of degree $p-2$ in $F_p[x]$ in terms of the permanent of a Vandermonde matrix whose entries are the primitive pth roots of unity. This leads to nontrivial bounds for the number of such permutation polynomials. Also he provided some numerical examples to illustrate his method and indicated how the results can be generalised to polynomials of other degrees.

Rivest [1], gave an exact characterization of permutation polynomials modulo $n = 2^w$, $w \geq 2$. He also characterized polynomials defining Latin squares modulo $n = 2^w$.

Theorem 1.3. *[1] Let* $P(x) = a_0 + a_1 x + ... + a_d x^d$ *be a polynomial with integral coefficients. Then* $P(x)$ *is a permutation polynomial modulo* $n = 2^w, w \geq 2$*, if and only if* a_1 *is odd,* $(a_2 + a_4 + a_6 + ...)$ *is even, and* $(a_3 + a_5 + a_7 + ...)$ *is even.*

Example 1.4. *The following are permutation polynomials modulo* $n = 2^w$*,* $w \geq 1$*;*
1. $x(a + bx)$ *where* a *is odd and* b *is even.*
2. $x + x^2 + x^4$*.*
3. $1 + x + x^2 + ... + x^d$*, where* $d = 1(mod\ 4)$*.*

Hollmann and Xiang [8] constructed a class of permutation polynomials of F_{2^m} that are closely related to Dickson polynomials. Muratović-Ribić [6] described some relations on the coefficients of a polynomial in terms of the map that induces and used them to characterize the coefficients of the inverse polynomials of some special classes of permutation polynomials. Zhou [5] gave an explicit representation of the class of linear permutation polynomials.

Cryptography requires the generation of keys for secured communication. One can think of generating secret keys using sequences of random numbers. Permutations of elements of a finite ring will give sequences of random numbers. Let $R[x]$ denote the set of all polynomials over the ring or field R. All the elements or polynomials of this ring cannot be permutation polynomials.

Let $P(x) = a_0 + a_1x + a_2x^2 + ... + a_mx^m$ be a polynomial of degree m over a ring R. There will be as many choices as the order of the ring for each coefficient a_i. So, in case of the rings Z_n, we see that there are n^{m+1} polynomials of degree m. Some of them will be permutation polynomials depending both on n and coefficients. The structures and various properties of permutation polynomials are explained in detail in [19, 3, 4, 20, 2, 14].

We may also consider the permuted values of $0, 1, ..., n-1$ got via a permutation polynomial $P(x)$ and define a sequence y_k by

$$y_k = P(k) \text{ mod n}, \ 0 \leq k \leq n-1$$
$$\text{and } y_k = P(k \text{ mod n}) \ \text{ mod n for } k \geq n.$$

For example, with $P(x) = x + x^2 + x^4$, we obtain the sequence (0, 3, 6, 13, 4, 15, 10, 9 ,8 ,11, 14, 5, 12, 7 ,2 ,1) over Z_{16}.

Sequences got this way have not been investigated much with respect to randomness. It seems reasonable to expect the sequences thus obtained to exhibit a good degree of randomness since values of $P(x)$ for any two consecutive integers in Z_n are highly independent of their prior positions. Here we make some preliminary studies in this direction and present some experimental and computational work, got by carrying out three among several well-known statistical tests on these sequences to decide whether any of them can be considered as good pseudorandom generators. The various properties of and statistical tests of random sequences are explained in detail in [16, 15].

2. Statistical tests

A sequence of numbers generated by some or the other way, can not be trusted to judge by ourselves whether it is random or not. Some unbiased mechanical tests must be applied. Every sequence that is to be used extensively should be tested carefully. If a sequence behaves randomly with respect to tests $T_1, T_2, ..., T_n$, we can not be sure in general that it will not be a failure when it is subjected to a further test T_{n+1}. Yet each test gives us more and more confidence in the randomness of the sequence. In practice, we apply different kinds of statistical tests to sequence.

Many statistical tests require that our data follow a normal distribution. Some times this is not the case. In some instances, it is possible to transform the data to make them follow a normal distribution. Sometimes it is not possible or the sample size might be so small that it is difficult to ascertain whether or not the data a normally distributed. In such cases, it is necessary to use a statistical test that does not require the data to follow a particular distribution. Such a test is called a **non-parametric** or **distribution free** test. The runs test and sign test are examples of such a test.

The runs test counts the number of runs that formed due to the appearance of the numbers less than or greater than the mean of the sequence. Originally tests are made on runs up and down at once; A run up would be followed by a run down, then another run up, and so on.It is noted that the run test does not depend on the uniform distribution of the x_i's but only on the fact that $x_i = x_j$ occurs with probability zero when $i = j$. Therefore this test can be applied to many types of random sequences.

The sign test is used to test the null hypothesis that the median of a distribution is equal to some value. It can be used for ordered categorial data where a numerical scale is inappropriate but where it is possible to rank the observations.

Several statistical tests are available to determine the extent to which a given sequence exhibits randomness. Indeed, a given sequence may pass some tests very well whereas failing some other tests. We tested the sequences using three tests.

2.1. Runs test

A **run** is a sequence of identical occurrences preceded and followed by different occurrences or by none at all. In general, a random process lists the elements involved in some sequence. The runs test will consider them in two different types of occurrences. As we move along the sequence, we

observe the groups of two types of occurrences alternatively. Each group of the same occurrence in a continued pattern is called a **run**. The test counts the number of such runs and the number of occurrences of each type.

A test of runs would use the following symbols if it contained just two kinds of occurrences.

$$\begin{gathered} n_1 = \text{number of occurrences of type1.} \\ n_2 = \text{number of occurrences of type 2.} \\ r = \text{number of runs.} \end{gathered}$$

If there are too many types of occurrences in a sequence, we classify them into just two kinds (by using some criteria), say A and B. In the tests done, we put all numbers less than the mean as type A and those that are greater than or equal to the mean as type B.

$$\begin{gathered} \text{Let } n_1 = \text{number of } A\text{'s} \\ n_2 = \text{number of } B\text{'s} \\ r = \text{number of runs.} \end{gathered}$$

The number of runs, r is a statistic with its own special sampling distribution and its own test. Obviously, runs may be of differing lengths, and various numbers of runs can occur in one sample. In general, too few or too many runs in a sample indicate that something other than chance was at work when the elements are selected. A one-sample runs test, then, is based on the idea that too few or too many runs show that the elements are not chosen randomly.

The mean of the sampling distribution of the r statistic, μ_r, is given by

$$\mu_r = \frac{2n_1n_2}{n_1+n_2} + 1$$

The standard error of the r statistic can be calculated using the formula,

$$\sigma_r = \sqrt{\frac{2n_1n_2(2n_1n_2-n_1-n_2)}{(n_1+n_2)^2(n_1+n_2-1)}}$$

In the one-sample runs test, the sampling distribution of r can be closely approximated by the normal distribution if either n_1 or n_2 is larger than 20. So we can use the normal approximation in such cases.

Next, we use the following equation to standardize the sample r statistic

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

The purpose of testing is not to question the computed value of the sample statistic but to make a judgment about the difference between that sample statistic and a hypothesized population parameter. We set a significance level α for the testing hypothesis. This α is the confidence level with which we accept or reject the random sequence as a truly random one. Here, we set $\alpha = 0.05$. i.e., we use the 5 percent level of significance. In this case, whenever a random number sequence passes the test, we accept it with 95 percent probability that it is truly random. The higher the significance level we use for testing randomness, the higher is the probability of rejecting the sequence, when it is true. Almost all runs tests are two-tailed because the question to be answered is whether there are too many or too few runs. The critical values for z, in this case, are ± 1.96. That is, the $z-$values must lie between -1.96 and $+1.96$ for the sequence to be considered random with 95 percent confidence. Since $n_1 = n_2 = m/2$, depending on the permutation polynomial we use, and the ring we consider, the fluctuation of positions of the values of the polynomial as we move from 0 to $m-1$ will give us the number of runs, r. Here we consider a few permutation polynomials over some rings Z_m, where $m = 2^w$. We observe that the number of runs r is sufficiently close to $m/2$ in almost all cases. i.e., the number of runs is approximately 50 percent of m, which is neither too few nor too many.

Also, we look at the lengths of the runs and the number of derangements of ring elements due to the permutations. The maximum run length indicates the maximum length of the sequence carried over, without fluctuating about the mean.

Here, the same set of permutation polynomials are chosen for different Z_n's with $n = 2^w$.

Over the ring Z_{64}:

Permutation Polynomials	Number of runs	z	Maximum of run lengths	Number of displacements
$x(2x+1)$	31	-0.504	8	56
$x+x^2+x^4$	27	-1.512	11	56
$1+x+x^2+x^4$	27	-1.512	11	64
$1+x+x^2+x^3+x^4+x^5$	35	0.504	3	64
$1+x+2x^2+x^3+x^5$	35	0.504	6	64
$x+3x^2+x^3+x^4+x^5$	39	1.512	5	56
$1+x+x^2++x^9$	35	0.504	4	64
$1+x+x^2++x^{13}$	39	1.512	3	64

Here, all the polynomials pass the runs test with 95 percent confidence with z values lying between ± 1.96. Polynomials $x+x^2+x^4$ and $1+x+x^2+x^4$ give sequences with lesser number of runs and larger values for a maximum of run lengths than other polynomials. Polynomials are having no constant term fix all multiples of 8 and move the other 56 numbers. Polynomials with a constant term derange all the numbers.

Over the ring Z_{128}:

Permutation Polynomials	Number of runs	z	Maximum of run lengths	Number of displacements
$x(2x+1)$	63	-0.355	11	112
$x+x^2+x^4$	51	-2.485	7	120
$1+x+x^2+x^4$	47	-3.195	7	128
$1+x+x^2+x^3+x^4+x^5$	59	-1.065	5	128
$1+x+2x^2+x^3+x^5$	71	1.065	5	128
$x+3x^2+x^3+x^4+x^5$	59	-1.065	7	120
$1+x+x^2++x^9$	55	-1.775	9	128
$1+x+x^2++x^{13}$	63	-0.355	6	128

In this ring, polynomials $x+x^2+x^4$ and $1+x+x^2+x^4$ fail to pass the test with our level of confidence. The polynomial $x(2x+1)$ has 63 runs, which is comparatively more than some other polynomials, but it has a run of length 11(maximum in the list). Whereas, $1+x+2x^2+x^3+x^5$ has 71 runs but the maximum run length is just 5.

Over the ring Z_{2048}:

Permutation Polynomials	Number of runs	z	Maximum of run lengths	Number of displacements
$x(2x+1)$	1023	-0.088	45	1984
$x+x^2+x^4$	1011	-0.597	13	2016
$1+x+x^2+x^4$	1007	-0.796	13	2048
$1+x+x^2+x^3+x^4+x^5$	1011	-0.619	10	2048
$1+x+2x^2+x^3+x^5$	975	-2.210	13	2048
$x+3x^2+x^3+x^4+x^5$	1063	1.68	9	2016
$1+x+x^2++x^9$	1039	0.619	9	2048
$1+x+x^2++x^{13}$	1043	0.796	17	2048

When $m = 2048$, the polynomial $1+x+2x^2+x^3+x^5$ gives the z value outside the region of acceptance. The polynomial $x(2x+1)$ has z value much closer to 0, and it has the maximum run length 45, which is much greater than the other values in the list. Also, this polynomial fixes more number of points than the other polynomials.

Over the ring Z_{8192}:

Permutation Polynomials	Number of runs	z	Maximum of run lengths	Number of displacements
$x(2x+1)$	4095	-0.044	91	8064
$x+x^2+x^4$	4035	-1.359	16	8128
$1+x+x^2+x^4$	4039	-1.282	16	8192
$1+x+x^2+x^3+x^4+x^5$	4039	-1.282	11	8192
$1+x+2x^2+x^3+x^5$	4091	-0.133	10	8192
$x+3x^2+x^3+x^4+x^5$	4099	0.044	13	8128
$1+x+x^2++x^9$	4079	-0.398	18	8192
$1+x+x^2++x^{13}$	4107	0.221	12	8192

In this ring, all polynomials pass the test. Here again the maximum run length is much more in case of $x(2x+1)$ than that of other polynomials.

Since $n_1 = n_2 = m/2$, depending on the permutation polynomial we use, and the ring we consider, the fluctuation of positions of the values of the polynomial as we move from 0 to $m-1$ will give us the number of runs, r. We observe that the number of runs r is sufficiently close to $m/2$

in almost all cases. i.e., the number of runs is approximately 50 percent of m, which is neither too few nor too many. Also, the maximum run lengths are very small compared to n in case of all the polynomials in all the rings.

Remark 2.1. *From the last* 4 *tables, we observe that some points of the rings are fixed only if the permutation polynomials have no constant term. i.e., if* 0 *is shifted due to the action of a permutation polynomial, then all other elements of the ring are displaced from their positions. Also, the displaced numbers are multiples of* 8 *(may not be all multiples of* 8*), as we consider the rings of order* $m = 2^w$ *in our examples. For the permutation polynomial* $x(2x + 1)$ *the* z *value gets closer to* 0*, as we increase* m*. This is a remarkable polynomial and is used in the RC6 block cipher. It seems to steadily improve in being more random as* m *increases.*

A binomial $f(x) = a_2x^2 + a_1x$ is a permutation polynomial modulo p^d, whenever $a_2 \equiv 0(mod\ p)$ and $a_1 = 0(mod\ p)$, where p is a prime and $d \geq 1$.

Example 2.2. $14x^2+5x$ *modulo* $343(= 7^3)$ *and* $33x^2+15x$ *modulo* $121(= 11^2)$.

The above two binomials pass the runs test with $z = -0.162$ and $z = -0.091$ respectively. $14x^2 + 5x$ gives a sequence modulo 343, with 171 runs and maximum run length being 7, whereas $33x^2 + 15x$ gives a sequence modulo 121, with 61 runs and maximum run length 7. Also, both these polynomials fix only 0.

2.2. The sign test

Many statistical tests require that our data follow a normal distribution. Sometimes that is not the case. In some instances it is possible to transform the data to make them follow a normal distribution; in others, this is not possible, or the sample size might be so small that it is difficult to ascertain whether or not the data is normally distributed. In such cases, it is necessary to use a statistical test that does not require the data to follow a particular distribution. Such a test is called a non-parametric or distribution-free test. The sign test is an example of one of these.[17]

The sign test is used to test the null hypothesis that the median of a distribution is equal to some value. It can be used
a) in place of a one-sample t-test
b) in place of a paired t-test

c) for ordered categorial data where a numerical scale is inappropriate but where it is possible to rank the observations.

Let the observations in a sample of size n be $\{x_1, x_2, ..., x_n\}$. Suppose that r^+ of the observations are greater than M and r^- are smaller than M. Values of x which are exactly equal to M are ignored; the sum $r^+ + r^-$ may, therefore, be less than n and we will denote it by n'. Under the null hypothesis, we would expect half the x's to be above the median and half below. Therefore, under the null hypothesis both r^+ and r^- follow a binomial distribution with $p = \frac{1}{2}$ and $n = n'$.

The test procedure is as follows:
1. Choose $r = max(r^-, r^+)$.
2. Use tables of the binomial distribution to find the probability of observing a value of r or higher assuming $p = \frac{1}{2}$ and $n = n'$. If the test is one-sided, this is the p-value.
3. If the test is a two-sided test, double the probability obtained in (2) to obtain the p-value.

Example 2.3. *The table below shows the hours of relief provided by analgesic drugs in 12 patients suffering from arthritis.*

Case	*Drug A*	*Drug B*
1	*2.0*	*3.5*
2	*3.6*	*5.7*
3	*2.6*	*2.9*
4	*2.6*	*2.4*
5	*7.3*	*9.9*
6	*3.4*	*3.3*
7	*14.9*	*16.7*
8	*6.6*	*6.0*
9	*2.3*	*3.8*
10	*2.0*	*4.0*
11	*6.8*	*9.1*
12	*8.5*	*20.9*

In this case our null hypothesis is that the median difference is zero. Our actual differences (Drug B-Drug A) are:
+1.5, +2.1, +0.3, -0.2, +2.6, -0.1, +1.8, -0.6, +1.5, +2.0, +2.3, +12.4
Our actual median difference is 1.65 hours. We have $r^+ = 9$, $r^- = 3$, $n = 12$, $r = max(r^-, r^+) = 9$. Therefore our two-sided p-value (from binomial tables) is $p = 0.146$.

2.3. Wilcoxon Signed Rank Sum Test

The Wilcoxon signed rank sum test is another example of a non-parametric or distribution free test, which is used to test the null hypothesis that the median of a distribution is equal to some value. [17]

Case 1: Paired data

1. State the null hypothesis - in this case, it is that the median difference, M, is equal to zero.
2. Calculate each paired difference, $d_i = x_i - y_i$, where x_i, y_i are the pairs of observations.
3. Rank the d_is, ignoring the signs (i.e. assign rank 1 to the smallest $|d_i|$, rank 2 to the next etc.)
4. Label each rank with its sign, according to the sign of d_i.
5. Calculate W^+, the sum of the ranks of the positive d_is, and W^-, the sum of the ranks of the negative d_is. (As a check the total, $W^+ + W^-$, should be equal to $\frac{n(n+1)}{2}$, where n is the number of pairs of observations in the sample).

Case 2: Single set of observations

1. State the null hypothesis - the median value is equal to some value M.
2. Calculate the difference between each observation and the hypothesised median, $d_i = x_i - M$.
3. Apply Steps 3-5 as above in Case 1.

Under the null hypothesis, we would expect the distribution of the differences to be approximately symmetric around zero and the distribution of positives and negatives to be distributed at random among the ranks. Under this assumption, it is possible to work out the exact probability of every possible outcome for W.

To carry out the test, we proceed as follows:
Choose $W = min(W^-, W^+)$.
Use tables of critical values for the Wilcoxon signed rank sum test to find the probability of observing a value of W. Most tables give both one-sided and two-sided p-values. If not, double the one-sided p-value to obtain the two-sided p-value.

If the number of observations/pairs is such that $\frac{n(n+1)}{2}$ is large enough (> 20), a normal approximation can be used with $\mu_W = \frac{n(n+1)}{2}$, $\sigma_W = \sqrt{\frac{n(n+1)(2n+1)}{24}}$.

There are two types of tied observations that may arise when using the Wilcoxon signed rank test:

1. Observations in the sample may be exactly equal to M (i.e. 0 in the case of paired differences). Ignore such observations and adjust n accordingly.

2. Two or more observations/differences may be equal. If so, average the ranks across the tied observations and reduce the variance by $\frac{t^3-t}{48}$ for each group of t tied ranks.

Example 2.4. *Consider the example 2.3.*
In this case the null hypothesis is that the median difference is zero.
The actual differences (Drug B - Drug A) are:
+1.5, +2.1, +0.3, -0.2, +2.6, -0.1, +1.8, -0.6, +1.5, +2.0, +2.3, +12.4
The actual median difference is 1.65 hours.

Ranking the differences and affixing a sign to each rank (steps 3 and 4 above):

Difference	*0.1*	*0.2*	*0.3*	*0.6*	*1.5*	*1.5*	*1.8*	*2.0*	*2.1*	*2.3*	*2.6*	*12.4*
Rank	*1*	*2*	*3*	*4*	*5.5*	*5.5*	*7*	*8*	*9*	*10*	*11*	*12*
Sign	-	-	+	-	+	+	+	+	+	+	+	+

Calculating W^+ and W^- gives:

$$W^- = 1 + 2 + 4 = 7$$
$$W^+ = 3 + 5.5 + 7 + 8 + 9 + 10 + 11 + 12 = 71$$
$$\text{We have } \frac{n(n+1)}{2} = \frac{12\times13}{2} = 78 = W^- + W^+$$
$$W = max(W^-, W^+) = 71.$$

We can use a normal approximation in this case. We have one group of 2 tied ranks, so we must reduce the variance by $\frac{8-2}{48} = 0.125$. We get

$$z = \frac{71 - \frac{12\times13}{4}}{\sqrt{\frac{12\times13\times25}{24} - 0.125}}$$

$$= \frac{71 - 39}{\sqrt{126.5 - 0.125}} = 2.511$$

This gives a two-sided p-value of $p = 0.012$. There is a strong evidence that Drug B provides more relief than Drug A.

Test of Random sequences: To apply the sign test in SPSS, we took two sequences together: one is the original sequence of the elements of Z_n, in the natural order, and the other is the sequence of the permuted values. i.e., we consider the first sequence to be (x_i), where $x_i = i$, for $i = 0, 1, 2, ..., n-1$ and the second sequence being $(y_i = P(x_i))$, for $i = 0, 1, 2, ..., n-1$, where P is a permutation polynomial over the ring Z_n.

It can be observed from the tables of the test that all polynomials have a sufficiently good number of both positive and negative differences $(y_i - x_i)$. Under the null hypothesis, we expect half the x's to be above the median and half below.

From the tables, we can also observe that the distribution of the differences is approximately symmetric around zero, and the distribution of positives and negatives is random among the ranks, in all the cases.

The tests are tabulated for different rings as follows:

The Sign test:

1. Over the Ring Z_{64}:

Polynomails	Negative Differences	Positive Differences	Ties	Z	Asymptotic significance
$x + x^2 + x^4$	26	30	8	-0.401	0.688
$x + 3x^2 + x^3 + x^4 + x^5$	29	27	8	-0.134	0.894
$x(2x + 1)$	19	37	8	-2.272	0.023
$1 + x + x^2 + x^4$	27	37	0	-1.125	0.261
$1 + x + x^2 + x^3 + x^4 + x^5$	31	33	0	-0.125	0.901
$1 + x + x^2 + ... + x^9$	30	34	0	-0.375	0.708
$1 + x + x^2 + ... + x^{13}$	31	33	0	-0.125	0.901
$1 + x + 2x^2 + x^3 + x^5$	20	44	0	-2.875	0.004

2. Over the Ring Z_{128}:

Polynomails	Negative Differences	Positive Differences	Ties	Z	Asymptotic significance
$x + x^2 + x^4$	54	66	8	-1.004	0.315
$x + 3x^2 + x^3 + x^4 + x^5$	69	51	8	-1.552	0.121
$x(2x + 1)$	43	69	16	-2.362	0.018
$1 + x + x^2 + x^4$	55	73	0	-1.503	0.133
$1 + x + x^2 + x^3 + x^4 + x^5$	71	57	0	-1.149	0.251
$1 + x + x^2 + ... + x^9$	62	62	0	-0.265	0.791
$1 + x + x^2 + ... + x^{13}$	62	66	0	-0.265	0.791
$1 + x + 2x^2 + x^3 + x^5$	71	57	0	-1.149	0.251

3. Over the Ring Z_{2048}:

Polynomails	Negative Differences	Positive Differences	Ties	Z	Asymptotic significance
$x + x^2 + x^4$	966	1050	32	-1.849	0.065
$x + 3x^2 + x^3 + x^4 + x^5$	1021	995	32	-0.557	0.578
$x(2x + 1)$	931	1053	64	-2.717	0.007
$1 + x + x^2 + x^4$	967	1081	0	-2.497	0.013
$1 + x + x^2 + x^3 + x^4 + x^5$	1007	1041	0	-0.729	0.466

4. Over the Ring Z_{8192}:

Polynomails	Negative Differences	Positive Differences	Ties	Z	Asymptotic significance
$x + x^2 + x^4$	4158	4032	2	-1.381	0.167
$x + 3x^2 + x^3 + x^4 + x^5$	4133	4056	3	-0.840	0.401
$x(2x + 1)$	4113	4077	2	-0.387	0.699
$1 + x + x^2 + x^4$	4160	4032	0	-1.403	0.161
$1 + x + x^2 + x^3 + x^4 + x^5$	4088	4104	0	-0.166	0.868

The Signed Rank Sum test:
1. Over the Ring Z_{64}:

Polynomails	Negative ranks Sum/Mean	Positive Ranks Sum/Mean	Z	Asymptotic significance
$x + x^2 + x^4$	750/28.85	846/28.20	-0.392	0.695
$x + 3x^2 + x^3 + x^4 + x^5$	843/29.07	753/27.89	-0.367	0.713
$x(2x + 1)$	721/37.95	875/23.65	-0.630	0.529
$1 + x + x^2 + x^4$	986/36.52	1094/29.57	-0.361	0.718
$1 + x + x^2 + x^3 + x^4 + x^5$	1073/34.61	1007/30.52	-0.221	0.825
$1 + x + x^2 + ... + x^9$	1071/35.70	1009/29.68	-0.208	0.836
$1 + x + x^2 + ... + x^{13}$	1080/34.84	1000/30.30	-0.268	0.789
$1 + x + 2x^2 + x^3 + x^5$	825/41.25	1255/28.52	-1.444	0.149

2. Over the Ring Z_{128}:

Polynomails	Negative ranks Sum/Mean	Positive Ranks Sum/Mean	Z	Asymptotic significance
$x + x^2 + x^4$	3482/64.48	3778/57.24	-0.388	0.698
$x + 3x^2 + x^3 + x^4 + x^5$	3677/53.29	3583/70.25	-0.123	0.902
$x(2x + 1)$	2976/69.21	3352/48.58	-0.546	0.585
$1 + x + x^2 + x^4$	3950/71.82	4306/58.99	-0.423	0.672
$1 + x + x^2 + x^3 + x^4 + x^5$	4315/60.77	3941/69.14	-0.445	0.656
$1 + x + x^2 + ... + x^9$	4190/67.58	4066/61.61	-0.147	0.883
$1 + x + x^2 + ... + x^{13}$	4190/67.58	4066/61.61	-0.147	0.883
$1 + x + 2x^2 + x^3 + x^5$	4315/60.77	3941/69.14	-0.445	0.656

3. Over the Ring Z_{2084}:

Polynomails	Negative ranks Sum/Mean	Positive Ranks Sum/Mean	Z	Asymptotic significance
$x + x^2 + x^4$	1008359/1043.85	1024777/975.98	-0.314	0.753
$x + 3x^2 + x^3 + x^4 + x^5$	1016028/995.3	1017108/1022.22	-0.021	0.984
$x(2x + 1)$	973313/1045.45	995807/945.69	-0.441	0.659
$1 + x + x^2 + x^4$	1039829/1075.31	1058347/979.04	-0.346	0.729
$1 + x + x^2 + x^3 + x^4 + x^5$	1043123/1035.87	1055053/1013.50	-0.223	0.824

4. Over the Ring Z_{8192}:

Polynomails	Negative ranks Sum/Mean	Positive Ranks Sum/Mean	Z	Asymptotic significance
$x + x^2 + x^4$	17028928/4095.46	16513231/4095.54	-1.205	0.228
$x + 3x^2 + x^3 + x^4 + x^5$	16924632/4095.00	16609302/4095.00	-0.737	0.461
$x(2x + 1)$	16898594/4108.58	16643539/4082.30	-0.596	0.551
$1 + x + x^2 + x^4$	17042236/4096.69	16516327/4096.31	-1.228	0.219
$1 + x + x^2 + x^3 + x^4 + x^5$	16858284/4123.85	16700258/4069.26	-0.369	0.712

Conclusion

The sequences of numbers obtained by permutation polynomials over some small finite rings are tested for randomness. The run test, sign test and Wilcoxon Signed Rank test show significant results in case of all polynomials, which we tested. These type of random sequences may be considered for key generation applicable in ccryptography. In future, the permutation polynomials over finite fields may be suitably used for key generation to achieve high security.

Acknowledgement

The authors would like to thank the Editor-in-chief and the anonymous referees for their valuable comments and suggestions, which helped us to improve the quality of this manuscript. The first author and fourth author acknowledges Manipal Institute of Technology (MIT), Manipal Academy of Higher Education, India for their kind encouragement. The second author acknowledges National Institute of Technology, Surathkal, Karnataka, India for their kind encouragement.

References

[1] R. L. Rivest, "Permutation polynomials modulo 2w", *Finite fields and their applications*, vol. 7, no. 2, pp. 287–292, Apr. 2001, doi: 10.1006/ffta.2000.0282

[2] G. R. V.Bhatta and B. R. Shankar, "Variations of orthogonality of latin squares", *International journal of mathematical combinatorics*, vol. 3, pp. 55-61, 2015. [On line]. Available: https://bit.ly/307xpPg

[3] G. R. V. Bhatta and B. R. Shankar, "A study of permutation polynomials as latin squares", in *Nearrings, nearfields and related topics*, K. S. P. Syam Prasad, K. Babushri Srinivas, P. Harikrishnan, and S. Satyanarayana, Eds. World Scientific, 2017, pp. 270–281, doi: 10.1142/9789813207363_0025

[4] M. K. Singh and R. P. Singh, "On a conjecture concerning Kloosterman polynomials", *The journal of analysis*, vol. 27, no. 2, pp. 515–523, 2018, doi: 10.1007/s41478-018-0090-9

[5] K. Zhou, "A remark on linear permutation polynomials", *Finite fields theorem applications*, vol. 14, no. 2, pp. 532-536, Apr. 2008, doi: 10.1016/j.ffa.2007.07.002

[6] A. Muratović-Ribić, "A note on the coefficients of inverse polynomials", *Finite fields theorem applications*, vol. 13, no. 4, pp. 977-980, Nov. 2007, 10.1016/j.ffa.2006.11.003

[7] C. Cesarano and P. Ricci, "Orthogonality properties of the pseudo-Chebyshev Functions (Variations on a Chebyshev's theme)", *Mathematics*, vol. 7, no. 2, pp. Art ID. 180, Feb. 2019, doi: 10.3390/math7020180

[8] H., D. L. Hollman and Q. Xiang, "A class of permutation polynomials of F2m related to Dickson polynomials", *Finite fields theorem application*, vol. 11, no. 1, pp. 111-122, Jan. 2005, doi: 10.1016/j.ffa.2004.06.005

[9] P. Das, "The number of permutation polynomials of a given degree over a finite field", *Finite fields theorems applications*, vol. 8, no. 4, pp. 478-490, Oct. 2002, doi: 10.1006/ffta.2002.0355

[10] R. Lidl and G. L. Mullen, "When does a polynomial over a finite field permute the elements of the field?, II", *The American mathematical monthly*, vol. 100, no. 1, pp. 71-74, Jan. 1993, doi: 10.2307/2324822

[11] C. Cesarano, S Pinelas, and P. Ricci, "The third and fourth kind pseudo-Chebyshev polynomials of half-integer degree", *Symmetry*, vol. 11, no. 2, Art ID. 274, Feb. 2019, doi: 10.3390/sym11020274

[12] R. Lidl and G. L. Mullen, “When does a polynomial over a finite field permute the elements of the field?”, *The American mathematical monthly*, vol. 95, no. 3, pp. 243-246, Mar. 1988, doi: 10.2307/2323626

[13] R. Dubey, L. N. Mishra, and C. Cesarano, “Multiobjective fractional symmetric duality in mathematical programming with (C, Gf)-invexity assumptions”, *Axioms*, vol. 8, no. 3, Art ID. 97, Aug. 2019, doi: 10.3390/axioms8030097

[14] L. N. Mishra, "On existence and behavior of solutions to some nonlinear integral equations with applications", Ph.D. Thesis, National Institute of Technology, Silchar, Assam, India, 2017.

[15] A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. R. Dray , and S. C. Vo, “A statistical test suite for random and pseudorandom number generators for cryptographic applications”, Special Publication (NIST SP) - 800-22, 2001. [On line]. Available: https://bit.ly/3j2kiGw

[16] W. B. Nelson, *Accelerated testing: statistical models, test plans, and data analysis*, Hoboken, NJ: Wiley-Interscience, 2009.

[17] R. Shier, “Statistics: 2.3 The Mann-Whitney U Test”, Loughborough: Loughborough University, Mathematics Learning Support Centre, 2004. [On line]. Available: https://bit.ly/3kJGvtm

[18] Deepmala and L. N. Mishra, “Differential operators over modules and rings as a path to the generalized differential geometry”, *Facta universitatis. Series: mathematics and informatics (Online)*, vol. 30, no. 5, pp. 753-764, 2015. [On line]. Available: https://bit.ly/365DwHG

[19] J. H. van Lint and R. M. Wilson, *A course in combinatorics*, 2nd ed. Cambridge: Cambridge University Press, 2001.

[20] R. Lidl and H. Niederreiter, *Finite fields*, 2nd ed. Cambridge: Cambridge University Press, 1997, doi: 10.1017/CBO9780511525926

[21] R. Dubey, Deepmala, and V. N. Mishra, “Higher-order symmetric duality in nondifferentiable multiobjective fractional programming problem over cone constraints”, *Statistics, optimization & information computing*, vol. 8, no. 1, pp 187-205, 2020, doi: 10.19139/soic-2310-5070-601