PERMUTATION POLYNOMIALS: ITERATION OF SHIFT AND INVERSION MAPS OVER FINITE FIELDS

ANNA CHLOPECKI, JULIANO LEVIER-GOMES, WAYNE PENG, ALEX SHEARER, AND ADAM TOWSLEY

ABSTRACT. We show that all permutations in $S_n$ can be generated by affine unicritical polynomials. We use the PGL group structure to compute the cycle structure of permutations with low Carlitz rank. The tree structure of the group generated by shift and inversion maps is used to study the randomness properties of permutation polynomials.

1. Introduction

Throughout this paper, let $p$ be an odd prime, and $1 \leq d < p-1$ be an integer coprime to $p-1$. A polynomial $f : \mathbb{F}_p \rightarrow \mathbb{F}_p$ is a permutation polynomial if $f$ is bijective i.e., every element in the image will only have one preimage. A permutation polynomial $f$ represents an element $\Sigma$ in the symmetric group $S_p$ on $p$ letters, but in general $f$ is not unique in representing $\Sigma$. For any permutation $\Sigma \in S_p$ of a finite field $\mathbb{F}_p$, we can always find a unique permutation polynomial $f$ with $\deg(f) < p$ to represent $\Sigma$. We then say that the correspondent permutation polynomial of $\Sigma$ is $f$, and say that $f$ represent a permutation $\Sigma$ if we have no restriction on the degree of $f$.

Given a monic polynomial $f_{d,c}(x) = x^d + c$ over a finite field $\mathbb{F}_p$, the polynomial is a permutation polynomial when $f_{d,c}$ is a bijection of $\mathbb{F}_p$. The map $f_{d,c} : \mathbb{F}_p \rightarrow \mathbb{F}_p$ is a bijection when $\gcd(d,p-1) = 1$. In this case $\mathbb{F}_p$ has no $d$-th root of unity and, thus, $f_{d,c}$ is injective on a finite set. In this paper, the authors study the structure of the group generated by the above monic permutation polynomials; it turns out that the group can be generated by only two polynomials, the shifting map $\sigma = x + 1$ and the inversion map $\delta = x^{p-2}$. We call $x^{p-2}$ the inversion map because $x^{p-1} \equiv x^{p-2} \cdot x \equiv 1 \mod p$ for all $x \neq 0$ by Fermat’s little theorem. Our main result is the following (see Theorem 3.5):

**Theorem 1.1.** Let $f_{d,c} = x^d + c$ over $\mathbb{F}_p$. Then

$$\langle \sigma, \delta \rangle \cong \langle f_{d,c} \rangle \cong \begin{cases} S_p & p \equiv 1 \mod 4 \\ A_p & p \equiv 3 \mod 4 \end{cases},$$

where $S_p$ is the symmetric group on $p$ letters, and $A_p$ is the alternating group on $p$ letters.

As a consequence (see Corollary 3.6) of the theorem, we revisit a well-known result of Carlitz [3], where he shows that the group generated by affine maps $ax + b$ and the inverse map $x^{p-2}$ for $a, b \in \mathbb{F}_p$ is $S_p$.

Since, for this paper, the inversion and the shifting maps serve as the only two generators, we are able to analyze and systematically compute permutation polynomials with a tree, which is almost isomorphic to a $(p-1)$-ary tree, see Figure 1. We are able to find a general form in terms of $\sigma$ and $\delta$ for the permutation polynomial that represents the permutation $(01)(23)$ for any prime $p$.

**Key words and phrases.** weak Carlitz rank, permutation polynomials over finite fields, randomness in permutation trees.
This result is slightly stronger than the ones given in [1] and [5]. They observed that any permutation over $\mathbb{F}_p$ can be rewritten as the polynomial of the form

$$P_n(x) = (\cdots ((a_0 x + a_1)^{p-2} + a_2)^{p-2} \cdots + a_n)^{p-2} + a_{n+1}, \quad \text{for some } n \geq 0.$$  

In regards to our work, any permutation over $\mathbb{F}_p$ can be represented by the polynomial $P_n(x)$ with $a_0 = 1$ or $\pm 1$ for $p \equiv 1$ or $3 \mod 4$ respectively. We let $Q_n(x)$ be the polynomial in the form (1) with $a_0 = 1$. We refer to $Q_n$ as the weak form of index $n$, and $P_n$ is a standard form of index $n$.

Note that the Carlitz rank of a permutation $\Sigma$ or its correspondent permutation polynomial $f$, denoted as $\text{Crk}(\Sigma)$ and $\text{Crk}(f)$ respectively, defined in [1], is the minimal number $n$ of inversions required in the form (1) to represent $\Sigma$. We define the weak Carlitz rank of a permutation $\Sigma$ or its correspondent permutation polynomial $f$, denoted as $\text{wCrk}(\Sigma)$ and $\text{wCrk}(f)$ respectively, as the minimal $n$ such that there is a permutation polynomial $Q_n$ representing $\Sigma$. An obvious relation between these two ranks is $\text{Crk}(\Sigma) \leq \text{wCrk}(\Sigma)$ for any $\Sigma \in S_p$. The key lemma of this paper implies $\text{Crk}((12)(34)) \leq \text{wCrk}((12)(34)) \leq 6$ for all $p$. These papers (see [2] and [20]) give a survey about the recent development on the Carlitz rank. In Section 4, we will provide an algebraic geometry point of view on low Carlitz rank, and use it to say certain permutations cannot appear when the Carlitz rank is low. Permutation polynomials are an active area of research due to their valuable applications across the fields of cryptography, engineering, coding theory, and other fields of math. These polynomials are valuable because they share properties with genuinely random mappings, while in special cases also having predictable underlying structures. One notable result is Polard’s rho algorithm for factoring large numbers, which operates on points of collision using pseudorandom functions [16]. Due to quadratic permutation polynomials having a number of periodic points equal to the expected amount for a random function, they are a clear choice for use in the rho algorithm [7]. In cryptography, permutation polynomials have been used to generate balanced binary words [12]. They also play a key role in the RC6 encryption algorithm [18].

Psuedorandom permutations have found applications in affecting the efficiency of turbo codes. Though random permutations seem to be standard practice, more research into semirandom and nonrandom permutations may produce wanted results in the future [6].

An interesting property of permutation polynomials is that they do not behave in a manner that is truly random. As shown in [9], the number of cycles of a given length of a permutation polynomial is bounded. Our result also provide an example of a specific compositions of functions that corresponds to the same element of $S_p$, for all $p$ greater than a given value. Hence, a natural question to ask is then what other nonrandom behaviors can be induced on families of permutation polynomials. See the Appendix for an example of this.

### Example 1.2.

Let $p = 5$, then the valid choices for $d$ are 1 and 3.

| $x$  | $x+1$ | $x+2$ | $x+3$ | $x+4$ |
|------|-------|-------|-------|-------|
| $f(0)$ |  0  |  1  |  2  |  3  |  4  |
| $f(1)$ |  1  |  2  |  3  |  4  |  0  |
| $f(2)$ |  2  |  3  |  4  |  0  |  1  |
| $f(3)$ |  3  |  4  |  0  |  1  |  2  |
| $f(4)$ |  4  |  0  |  1  |  2  |  3  |
| $\sigma$ | id | (0 1 2 3 4) | (0 2 4 1 3) | (0 3 1 4 2) | (0 4 3 2 1) |
2. Some Permutation Polynomial Results

**Observation 2.1.** The function $x + 1$ over $\mathbb{F}_p$ corresponds to the even permutation 
$$ (0 \ 1 \ \cdots \ p - 1), $$
where $p$ is a prime greater than 2.

**Proof.** Clearly $f(x)$ maps $x$ to $x + 1$. Since the operation is done mod $p$, should $x + 1 = p$, then $x$ will be mapped to 0, which will eventually be mapped back to $x$. This shows that the function corresponds to a full cycle of the form $(0 \ 1 \ \cdots \ p - 1)$. Finally, since the cycle contains $p$ elements and $p$ is an odd prime, the cycle is an even permutation. □

**Observation 2.2.** The permutation associated to $f_{d,c}(x)$ over $\mathbb{F}_p$ is equal to $(0 \ 1 \ \cdots \ p - 1)^{c-i}\sigma_i$ for any $\sigma_i$, where $\sigma_i$ is a permutation corresponding to $f_{d,i}(x)$.

**Proof.** Consider the function $f_{d,c} = x^d + c = (x^d + i) + c - i$. Viewed as a composition of functions, this can be written as $f_{1,c-i} \circ f_{d,i}$. We have already established that $f_{d,i}$ is equivalent to a permutation, which we will refer to as $\sigma_i$, and from Observation 2.1, we know that $f_{1,c-i}$ corresponds to $c - i$ iterations of $(0 \ 1 \ \cdots \ p - 1)$. By translating $f_{1,c-i} \circ f_{d,i}$ to cycle notation, we arrive at $(0 \ 1 \ \cdots \ p - 1)^{c-i}\sigma_i$. □

**Proposition 2.3.** The number of left (or right) cosets of the cyclic group $\langle (0 \ 1 \ \cdots \ p - 1) \rangle$ in the group $\langle f_{d,c} \rangle$ over $\mathbb{F}_p$ is $\phi(p - 1)$, where $\phi$ is Euler’s totient function.

**Proof.** Let’s consider functions $f_{d,c}(x)$ over a finite field $\mathbb{F}_p$. Let $\tau_p$ be the set of cosets yielded. We know that the gcd($d$, $p - 1$) = 1, thus $|\tau_p|$ is at most $\phi(p - 1)$. We want to show that $|\tau_p| = \phi(p - 1)$.

This is equivalent to showing that $[\sigma_i] \neq [\sigma_j]$ for $d_i \neq d_j \mod (p - 1)$.

Assume that $d_i \neq d_j$ and, for a contradiction, assume that $[\sigma_i] = [\sigma_j]$. Then, $\sigma_i \in [\sigma_j]$. So, there exists $c$ such that $x^{d_i} + c \equiv x^{d_j} \mod (p - 1)$ for all $x \in \mathbb{F}_p$. Then, for every $x \in \mathbb{F}_p$ it follows that $x^{d_i} + c - x^{d_j} \equiv 0 \mod (p - 1)$. We can only have max($d_i$, $d_j$) roots, unless $d_i = d_j$ and $c = 0$. If our assumption is true, $x^{d_i} + c - x^{d_j}$ must have $p$ distinct roots in $\mathbb{F}_p$. However, max($d_i$, $d_j$) < $p$. Thus we have a contradiction. □

For a fixed $d$, as a consequence of Observation 2.2, there are $p$ distinct permutations given by a function $f_{d,c}(x)$ over $\mathbb{F}_p$. So, using Proposition 2.3, it is clear that the total number of permutations yielded by $f_{d,c}(x)$ for all $d$ is $p \cdot \phi(p - 1)$.

3. Generating $A_p$ or $S_p$ from Permutation Polynomials

Our overall goal for this section is to observe which groups are generated by the set of permutations corresponding to $f_{d,c}(x)$ over $\mathbb{F}_p$. For this investigation, we will focus on the functions $x + 1 \mod p$ and $x^{p-2} \mod p$, as both maps behave in a predictable manner across any choice of $p$. By Observation 2.1, the function $x + 1$ corresponds to the cycle $(0 \ 1 \ \cdots \ p - 1)$. Also, we notice that $x^{p-2}$ can be simplified via Fermat’s little theorem to $x^{-1}$. This shows that $x^{p-2}$ is its own inverse. Therefore, it is a permutation of order 2 and must be composed of disjoint two cycles.
From these two properties, our intent is to show that the functions $x + 1$ and $x^{p-2}$ can act as a minimal generating set for $\langle f_{d,c} \rangle$.

It is known from a result by Iradmusa and Taleb [11] that a permutation of the form $(a \ b)(c \ d)$ and a full cycle, that is a cycle of length $p$, are sufficient to generate all of the group $A_p$.\footnote{This statement is conditionally true, however all these conditions are satisfied when $p$ is prime} We have already established that $x + 1$ is a full cycle. We will now show that $(0 \ 1)(2 \ 3)$ can be generated as a composition of $x + 1$ and $x^{p-2}$ for all $p \geq 5$.

**Observation 3.1.** In $\mathbb{F}_p$, for $p \geq 5$, the function $x^{p-2}$ only has three fixed points, 0, 1, and $-1$.

**Proof.** Clearly 0 is fixed by $x^{p-2}$, so let $x \neq 0$. If $x^{p-2} = x$, then $x^{-1} = x$, so $1 = x^2$. Thus, $x^2 - 1 = (x - 1)(x + 1) = 0$, so the the only other fixed points are $\pm 1$. $\square$

In the following lemma, we will establish a weak form for the $(01)(23)$.

**Lemma 3.2.** Let $\delta$ and $\sigma$ be the permutations corresponding to $x^{p-2}$ and $x + 1$, respectively. Then, for $p \geq 5$,

$$(01)(23) = \sigma^3 \delta \cdot \sigma^{-1} \delta \cdot (\sigma \delta)^3 \cdot \sigma^{-1} \delta.$$  

In particular, we have $\Crk((01)(23)) = w\Crk((01)(23)) = 6$.

The formula above may seem like magic: it was found using a tree describing the possible nontrivial permutations generated by $\delta$ and $\sigma$. We first apply $\delta$ and then can apply any of $\sigma, \sigma^2, \ldots, \sigma^{p-1}$. We can then only apply $\delta$, see Figure 1, after which we can apply $\sigma, \sigma^2, \ldots, \sigma^{p-1}$. Exhausting this tree led us to a form which always gives the desired result.

**Proof.** Use $\delta$ and $\sigma$ as defined above, and let $c_1, c_2, \ldots < p$ be nonnegative integers. In the following argument, we use the following significant but simple fact:

**Fact 1.** For any integer $n$ coprime to $p$, we can find an integer $0 \leq c < p$ such that $\frac{1+cp}{n}$ is not only an integer, but also an inverse of $n$, by simply checking

$$n \cdot \frac{1+cp}{n} \equiv 1 \mod p.$$
We will demonstrate the process of the calculations by showing that

$$\sigma^3 \delta \cdot \sigma^{-1} \delta \cdot (\sigma \delta)^3 \cdot \sigma^{-1} \delta(n) = n$$

for $3 < n < p$.

By Fact 1, we have $c_1$ such that

$$\delta(n) \equiv \frac{1 + c_1 p}{n} \mod p$$

and

$$\sigma^{-1} \delta(n) \equiv \frac{1 + c_1 p}{n} - 1 \equiv \frac{1 - n + c_1 p}{n}.$$

Then, we apply $\delta$ to $\sigma^{-1} \delta$ which gives

$$\delta \sigma^{-1} \delta(n) \equiv \frac{1 + c_2 p}{(1 - n + c_1 p) / n} \equiv \frac{n + c_2 n p}{1 - n + c_1 p} \mod p$$

and

$$\sigma \delta \sigma^{-1} \delta(n) \equiv \frac{n + c_2 n p}{1 - n + c_1 p} + 1 \equiv \frac{1 + c_3 p}{1 - n + c_1 p} \mod p$$

where $c_3$ is chosen such that $c_3 \equiv c_1 + c_2 n \mod p$. We should note that all of these fractions are actually integers. This is important because it allows us to use Fact 1. Since the process repeats the above computations, we will only show a few more steps and leave it to the reader to check the rest:

$$\delta \sigma \delta \sigma^{-1} \delta(n) \equiv \frac{1 + c_4 p}{(1 + c_3 p) / (1 - n + c_1 p)}$$

$$\equiv \frac{1 - n + (1 - n) c_3 p + c_1 p + c_1 c_4 p^2}{1 + c_3 p}$$

$$\equiv \frac{1 - n + c_5 p}{1 + c_3 p} \mod p \quad \text{for } c_5 \equiv (1 - n) c_3 + c_1 + c_1 c)4p \mod p;$$

$$\sigma \delta \sigma \sigma^{-1} \delta(n) \equiv \frac{1 - n + c_5 p}{1 + c_3 p} + 1$$

$$\equiv \frac{2 - n + c_6 p}{1 + c_3 p} \mod p \quad \text{for } c_6 \equiv c_3 + c_5 \mod p$$

$$\delta \sigma \delta \sigma^{-1} \delta(n) \equiv \frac{1 + c_7}{(2 - n + c_6 p) / (1 + c_3 p)}$$

$$\equiv \frac{1 + c_8 p}{2 - n + c_6 p} \mod p \quad \text{for } c_8 \equiv c_6 + (2 - n) c_3 + c_3 c_6 p \mod p$$

$$\sigma \delta \sigma \sigma^{-1} \delta(n) \equiv \frac{1 + c_8 p}{2 - n + c_6 p} + 1$$

$$\equiv \frac{1 + c_8 p + 2 - n + c_6 p}{2 - n + c_6 p} \mod p \quad \text{for } c_9 \equiv c_6 + c_8 \mod p$$

$$\vdots$$
In summary, the following chart proves the lemma. For $3 < n < p$,

\[
\begin{array}{cccccccc}
0 & \delta & 0 & \sigma^{-1} & -1 & \delta & \cdots & \sigma^3 & 1 \\
1 & \delta & 1 & \sigma^{-1} & 0 & \delta & \cdots & \sigma^3 & 0 \\
2 & \delta & \frac{pc_{2,1}+1}{2} & \sigma^{-1} & \frac{pc_{2,2}-1}{2} & \delta & \cdots & \sigma^3 & 3 \\
3 & \delta & \frac{pc_{3,1}+1}{3} & \sigma^{-1} & \frac{pc_{3,2}-2}{3} & \delta & \cdots & \sigma^3 & 2 \\
n & \delta & \frac{pc_{n,1}+1}{n} & \sigma^{-1} & \frac{pc_{n,2}+1-n}{n} & \delta & \cdots & \sigma^3 & n \\
\end{array}
\]

where $1 \leq c_{i,j} < p$ are integers.

The $\text{Crk}(\Sigma) = 6$ follows directly from Lemma 2 in [2], which says that if $P_n$ represents $\Sigma$ with $n < (p-1)/2$, then $n = \text{Crk}(\Sigma)$.

\[\square\]

**Lemma 3.3.** We have the following:

1. The polynomial $x^{p-2}$ gives an odd permutation of $\mathbb{F}_p$ if and only if $p \equiv 1 \mod 4$.
2. The polynomial $-x$ gives an odd permutation of $\mathbb{F}_p$ if and only if $p \equiv 3 \mod 4$.

**Proof.** (1) Under the inverse map $x^{p-2}$, by Observation 3.1, we know that there are only 3 fixed points: 0, 1, and $-1$. Moreover, the permutation corresponding to $x^{p-2}$ can be written as disjoint 2-cycles. Therefore, the map $x^{p-2}$ must produce a permutation with $\frac{p-3}{2}$ transpositions.

If $p \equiv 1 \mod 4$ then $p = 4m + 1$ for some $m \in \mathbb{Z}$. Therefore, there are $2m - 1$ transpositions. So, there are an odd number of transpositions; therefore $x^{p-2}$ forms an odd permutation. Hence, there exists an odd permutation in the set given by $f_{d,c}(x)$ over $\mathbb{F}_p$ if $p \equiv 1 \mod 4$.

(2) The map $-x$ will have one fixed point, 0. Everything else will be sent to its additive inverse. This means that $-x$ yields a permutation made up of transpositions. There must be $\frac{4m+3-1}{2}$ transpositions within our permutation, or $2m-1$ transpositions. So $-x$ yields an odd permutation.

\[\square\]

**Lemma 3.4.** There exist no odd permutations in the set given by $f_{d,c}(x)$ over $\mathbb{F}_p$ if $p \equiv 3 \mod 4$.

**Proof.** In order to show that no odd permutations are generated, we need only consider $f_{d,0}$, as a shift is an even permutation by Observation 2.1. We will show that each permutation is a product of an even number of cycles. We claim that for each cycle $(a_1 \cdots a_k)$ in a given permutation, there exists the cycle $(-a_1 \cdots -a_k)$ in the same permutation.

We first want to show that if $a_i \neq 0$ is in cycle $(a_1 \cdots a_k)$, then $-a_i$ is not in this cycle. In other words, for all $d$, $a_i^d \neq a_i$. Let’s consider a permutation $\sigma$. Suppose, for the sake of contradiction, $a_i^d = a_i$ for arbitrary $a_i \in \mathbb{F}_p$. Then, $a_i(a_i^{d-1} + 1) = 0$. Since we are considering nonzero $a_i$, we have $a_i^{d-1} + 1 = 0$. Hence, $(a_i^{(d^{p-1})/2})^2 \equiv -1 \mod p$. However, because $p \equiv 3 \mod 4$, by quadratic reciprocity (see, for example, [17, Chapter 21]), there is no solution to this equation.

Because $d$ is odd, it follows that if $a_i^d = a_i + 1$, then $-a_i^d = -a_i + 1$. Thus, for each cycle $(a_1 \cdots a_k)$, we have a matching cycle $(-a_1 \cdots -a_k)$ in the same permutation. Thus, every permutation generated is even.

\[\square\]

**Theorem 3.5** (Theorem 1.1). Let $f_{d,c} = x^d + c$ over $\mathbb{F}_p$. Then

$$\langle \sigma, \delta \rangle \cong \langle f_{d,c} \rangle \cong \begin{cases} S_p & p \equiv 1 \mod 4 \\ A_p & p \equiv 3 \mod 4 \end{cases},$$

where $S_p$ is the symmetric group on $p$ letters, and $A_p$ is the alternating group on $p$ letters.
Proof. For \( p \geq 5 \) it follows from Lemma 3.2, and for \( p = 3 \) it follows from a direct computation in sage, that the set of permutations generated by \( f_{d,c}(x) \) over \( \mathbb{F}_p \) must contain \((01)(23)\) and \((01 \ldots p-1)\). Thus, by [11], the permutations yielded by \( f_{d,c}(x) \) over \( \mathbb{F}_p \) must generate at least \( A_p \), as the cycles \((01)(23)\) and \((01 \ldots p-1)\) generate \( A_p \). We know by Lagrange’s theorem that \( A_p \) and an odd permutation generate \( S_p \). By Lemma 3.3(1), we know that we can find an odd permutation in our generating set when \( p \equiv 1 \) mod 4. Hence, when \( p \equiv 1 \) mod 4, we can generate \( S_p \). By Lemma 3.4, we know that no odd permutations exist within our generating set when \( p \equiv 3 \) mod 4. So, when \( p \equiv 3 \) mod 4, we generate \( A_p \). \( \square \)

The following corollary removes the monic condition on our generating polynomials \( f_{d,c} \). It recovers a result of Carlitz [3] with an elementary proof.

**Corollary 3.6.** Let \( f_{a,d,c} = ax^d + c \) over \( \mathbb{F}_p \) where \( a = 1 \) if \( p \equiv 1 \) mod 4 and \( a = \pm 1 \) if \( p \equiv 3 \) mod 4. Then \( \langle f_{a,d,c} \rangle \cong S_p \) for all \( p \) prime.

**Proof.** By Theorem 3.5, we know this is true when \( p \equiv 1 \) mod 4. So, we must only consider the case when \( p \equiv 3 \) mod 4. In this case, by Lemma 3.3(2), we know that \(-x\) gives an odd permutation. So, we generate all of \( S_p \). \( \square \)

### 4. Carlitz rank and weak Carlitz rank

From Corollary 3.6, we know that any permutation polynomial can be represented by the form \( P_n \) with \( a_0 = \pm 1 \); see (1). We will say \( P_n(x) \) is a weak form if \( a_0 = \pm 1 \), and denote as \( Q_n \). One can define a rank of a permutation \( \Sigma \) or a permutation polynomial over \( \mathbb{F}_p \) with degree \( < p \) similar to the Carlitz rank, called the weak Carlitz rank, as the minimal number \( n \) such that \( Q_n \) represents \( \Sigma \). We should keep in mind that the definition of weak form is not redundant since we naturally have

\[
0 = \text{Crk}(ax + b) < \text{wCrk}(ax + b) \quad \text{for} \quad a \neq \pm 1.
\]

Moreover, if we find \( 0 \neq \text{wCrk}(ax + b) \leq (p - 1)/2 \), then we have \( \text{Crk}(ax + b) \neq 0 \) from a result in [2]. Hence, we conclude that \( \text{wCrk}(ax + b) > (p - 1)/2 \).

In cryptography, there are several different measures for the complexity of a permutation polynomial. Let us introduce some of these:

We follow the definition given in [10]. The **linearity** \( \mathcal{L}(f) \) (or \( \mathcal{L}(\Sigma) \)) of a permutation polynomial \( f \) (or a permutation \( \Sigma \)) over a finite field \( \mathbb{F}_p \) with \( f(0) = 0 \) is

\[
\mathcal{L}(f) := \max_{a \in \mathbb{F}_p^*} |\{c \mid f(c) = ac\}|.
\]

We say an element \( c \in \mathbb{F}_p \) is \( a \)-**linear** if \( f(c) = ac \). From this point of view, any \( x \in \mathbb{F}_p \) is \( a \)-linear for some \( a \), so \( \mathcal{L}(f) \geq 1 \).

Another canonical measurement is called weight \( \omega(f) \) of a permutation polynomial \( f \) with \( \text{deg}(f) < p \) which is the number of nonzero coefficient of \( f \).

It is worth mentioning that there is another measurement, namely the index of a permutation polynomial. It was first introduced in [14], defined in [21], and further studied in [13], [21], and [22]. For application of cryptography, one would like to have a permutation polynomial \( f \) that has small linearity and large Carlitz rank, degree, and weight.

Using Lemma 3.2 we can measure the complexity of the form (12)(34).

**Proposition 4.1.** For any permutation \( \Sigma \) of the form \((a a + 1)(a + 2 a + 3)\), we have

\[
\text{Crk}(\Sigma) = \text{wCrk}(\Sigma) = 6, \quad \text{deg}(\Sigma) \geq p - 7, \quad \text{and} \quad \omega(\Sigma) > \frac{p - 14}{7}.
\]
Proof. The proof of this proposition is just a direct consequence of results in [10], [4] and [8]. More precisely, we have the following inequalities:

\begin{align*}
(2) \quad \text{Crk}(\Sigma) & \geq p - \mathcal{L}(\Sigma); \\
(3) \quad \text{Crk}(\Sigma) & \geq p - \deg(f) - 1; \\
(4) \quad \text{Crk}(\Sigma) & \geq \frac{p}{\omega(\Sigma) - 2} + 1.
\end{align*}

Since \((a + 1)(a + 2a + 3)\) is conjugate to \((01)(23)\) two by an iteration of the shifting map \(\sigma\), the weak Carlitz rank is the same. Thus, we get our inequality by direct computation. \(\Box\)

It has been observed that \(\sigma^k \delta\) is equal to

\[ R(x) = k + \frac{1}{x} = \frac{kx + 1}{x} \]

for all \(x \in \mathbb{F}_p \setminus \{0\}\) where 0 is the pole of the mobius transformation. Thus, we can let \(P_0(x) = R_0(x) = a_1 x + a_0\), and define the following recursive relation

\[ R_m(x) = a_{m+1} + \frac{1}{R_{m-1}(x)} \]

to have \(P_n(x) = R_n(x)\) for \(x \in \mathbb{F}_p \setminus \{0\}\) where \(0\) is the pole of \(R_m\) for all \(m = 1, 2, \ldots, n\). We denote \(\mathcal{O}_{(a_0, \ldots, a_{n+1})} = \{\rho_m \mid \rho_m \text{ is the pole of } R_m \forall m = 1, 2, \ldots, n\}\), and omit the subindex \((a_0, \ldots, a_{n+1})\) if it is clear in the context. This alternating expression explains why one needs a permutation polynomial with large Carlitz rank for application of cryptography.

Proposition 4.2. Given a permutation polynomial \(f\) over \(\mathbb{F}_p\), let \(n = \text{Crk}(f)\). Then, there are at least \(p - n\) many elements \(c \in \mathbb{F}_p\) satisfying \(f(c) = R_n(c)\) where \(R_n\) is the correspondent mobius transformation. If \(n = \text{Crk}(f) < (1 - (1/2)^{1/3})p \approx 0.21p\), then the probability of solving the correspondent \(R_n\) by randomly choosing 3 points, is greater than 1/2.

Proof. First of all, \(|\mathcal{O}^n| \leq n\) since there are \(n\) many inversions, so there are at least \(p - n\) many \(c\) satisfying \(f(c) = R_n(c)\). Thus, \(p - n \geq p - (1 - (1/2)^{1/3})p = (1/2)^{1/3}p\). Hence, we know the ratio of \(c \in \mathbb{F}_p\) satisfying \(f(c) = R_n(c)\) is \((1/2)^{1/3}\). Hence, the conclusion is directly followed. \(\Box\)

We furthermore have the following canonical isomorphism

\[ \left\{ \frac{ax + b}{cx + d} \mid a, b, c, d \in \mathbb{F}_p \right\} \cong \text{PGL}_2(\mathbb{F}_p) \]

where the operations are functional composition and matrix multiplication respectively.

From these two observations, we have the following correspondence between the form \(P_n(x)\) over a finite field \(\mathbb{F}_p\) and matrix in \(\text{PGL}_2(\mathbb{F}_p)\)

\[ P_n(x) \leftrightarrow \begin{bmatrix} a_{n+1} & 1 & 0 \\ 1 & a_n & 1 \\ 0 & 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_2 & 1 & 0 \\ 1 & a_1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \mod p. \]

To find all \(a\)-linear elements of \(P_n(x)\) over \(\mathbb{F}_p\), we need to solve \(P_n(x) = ax\) over \(\mathbb{F}_p\). Correspondingly, we will solve an equation of matrices,

\[ \begin{bmatrix} a_{n+1} & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_1 & 0 \\ 0 & 1 \end{bmatrix} \mod p = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \]

where we treat all \(a_i\) as variables. The solution of the equation of matrix is a variety \(V \in \mathbb{F}_p^{n+2}\) with dimension \(\dim(V) \geq n - 2\). Therefore, \(V\) is not empty for \(n \geq 3\). If \((a_0, a_1, \ldots, a_{n+1})\) is on \(V\), then the correspondent permutation polynomial \(P_n(x)\) is \(ax\) for \(x \in \mathbb{F}_p \setminus \mathcal{O}^n\). This is definitely not
a good way to approach this problem for large $n$, but we can still say something for small $n$ with fixed $a_1$ and $a_0$. We should remind readers that $a_1 = 1$ is correspondent to the weak form $Q_n$.

**Theorem 4.3.** For $p \geq 13$, the only permutation polynomial $P_n$ with $n \leq 4$ and $a_1 = \alpha$ that has $p - 4$ many $\alpha$-linear points is the polynomial $\alpha x$. In particular, we conclude $\text{wCrk}(\Sigma) > 4$ if $\Sigma$ permutes at most 4 elements.

**Proof.** If there are 4 elements not in $O^4$ on $y = R_4(x)$, then $R_4(x)$ is completely determined by these points. Therefore, if we have more than $4 + |O^4|$ $\alpha$-linear elements, then $R_4(x) = ax$. Since we assumed $f$ has at least $p - 4$ $\alpha$-linear elements, we have the inequality

$$p - 4 \geq 4 + 4 \geq 4 + |O^4|,$$

and we get that $p$ is a prime at greater than 12.

Thus, our condition implies the following matrix equation

$$\begin{bmatrix} a_5 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_4 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_3 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha & a_0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix}$$

which yields the following system of equations:

$$\alpha a_2 a_3 a_4 a_5 + \alpha a_2 a_3 + \alpha \alpha a_2 a_5 + \alpha a_4 a_5 = 0$$
$$a_0 a_2 a_3 a_4 a_5 + a_0 a_2 a_3 + a_0 a_2 a_5 + a_0 a_4 a_5 + a_3 a_4 a_5 + a_0 + a_3 + a_5 = 0$$
$$a_2 a_3 a_4 + a_4 + a_2 = 0$$
$$a_0 a_2 a_3 a_4 + a_3 a_4 + a_0 a_4 + a_0 a_2 = 0$$

The first equation and the third equation together imply $\alpha a_2 a_3 = 0$, which means $a_2 = 0$ or $a_3 = 0$. Therefore, the form $P_4$ with $a_1 = \alpha$ will be reduced to the form $P_2$ with $a_1 = \alpha$. We then set up a matrix equation regarding $P_2$ with $a_1 = \alpha$, and find it will reduce again to $P_0$ with $a_1 = \alpha$. Hence, the only form $P_n$ with $a_1 = \alpha$ and $n \leq 4$ which has at least $p - 4$ many $\alpha$-linear elements is $\alpha x$.

This framework can also give us insight with regards to the iteration of the permutation polynomial $f_{p-2,a}(x) = x^{p-2} + a$. The matrix correspondent to $f_{p-2,a}$ is

$$M = \begin{bmatrix} a & 1 \\ 1 & 0 \end{bmatrix},$$

so the matrix correspondent to the $n^{th}$ iterate of $f_{p-2,a}$, denote by $f_{p-2,a}^n$, is simply $M^n$. It should be noticed that

$$M^n = \begin{bmatrix} F_{n+1}(a) & F_n(a) \\ F_n(a) & F_{n-1}(a) \end{bmatrix}$$

where $F_n(a)$ is the $n$-th Fibonacci polynomial. One of the many identities of Fibonacci polynomials that are going to help us here is the following

$$F_{n+m} = F_{n+1}F_m + F_nF_{m-1}.$$  \hspace{1cm} (5)

The other fact which will be used is the closed form of the sequence $\{F_n(\alpha)\}$ for $\alpha \in \mathbb{N}$ is

$$F_n = Az_+^n + Bz_-^n$$

where we let

$$z_+ = \frac{-\alpha + \sqrt{\alpha^2 + 4}}{2} \quad \text{and} \quad z_- = \frac{-\alpha - \sqrt{\alpha^2 + 4}}{2},$$
and let $A = 1/(z_+ - z_-)$ and $B = -1/(z_+ - z_-)$. We say the sequence is not ramified at a prime $p$ if $\alpha^2 + 4 \neq 0$. If we let $F_n \equiv 0 \mod p$, it is equivalent to say

$$
(6) \quad \left(\frac{z_+}{z_-}\right)^n \equiv -\frac{B}{A} \equiv 1 \pmod{p}.
$$

The $n$ is the multiplicative order of the element $(z_+/z_1)$ in the finite field $\mathbb{F}_p(\sqrt{\alpha^2 + 4})$, and so $n$ divides $p^2 - 1$. One can find more details about the order in [15].

**Lemma 4.4.** Let $p$ be an unramified prime for the sequence $\{F_n(\alpha)\}$, and assume $n, m \in \mathbb{N}$ where $n > m$. If $F_n(\alpha)F_{m-1}(\alpha) \equiv F_{n-1}(\alpha)F_m(\alpha) \pmod{p}$, and $n$ is the first integer after $m$ satisfying the equation, then $n - m$ is the multiplication order of $(z_+/z_-)$ in the ring $\mathbb{F}_p$ or $\mathbb{F}_p^2$.

**Proof.** Using the closed form of $F_n(\alpha)$, we have

$$(Az_+^n + Bz_-^n)(Az_+^{m-1} + Bz_-^{m-1}) \equiv (Az_+^{n-1} + Bz_-^{n-1})(Az_+^m + Bz_-^m) \pmod{p}.
$$

The equation then will simplify to

$$
\left(\frac{z_+}{z_-}\right)^{n-m} \equiv 1 \pmod{p}.
$$

Since we assumed $n$ is the first integer after $m$ satisfying the equation, $n - m$ should be the multiplication order of $(z_+/z_-)$.

**Theorem 4.5.** If $n < p$ is the minimal integer such that $F_n(\alpha) \equiv 0 \pmod{p}$, then the permutation polynomial $f_{p-2,\alpha}^n$ represents

$$
\left( -\frac{F_{n-1}}{F_{n-2}} \cdots -\frac{F_3}{F_2} - \frac{F_2}{F_1} 0 \right).
$$

Where $F_i$ is evaluated at $\alpha$. Moreover, we have $n$ dividing $p^2 - 1$. Conversely, if $f_{p-2,\alpha}^n$ fixes at least $n + 4$ elements in $\mathbb{F}_p$, and $2n + 4 \leq p$, then $F_n(\alpha) \equiv 0 \pmod{p}$.

**Proof.** We have to show $|\mathcal{O}_{(\alpha,\ldots,\alpha)}^n| = n$. It is equivalent to show that

$$
\frac{F_{k+1}}{F_k} \neq \frac{F_{l+1}}{F_l}
$$

for all $0 \leq l \neq k \leq n$.

By (5), we have

$$
F_{n+1} = F_nF_2 + F_{n-1}F_1.
$$

Since we assume $F_n(\alpha) = 0$, $F_{n+1}(\alpha) = F_{n-1}(\alpha)$. Therefore, $M^n$ is equivalent to the identity matrix, which is correspondent to the identity map. Thus, $R_n(x) = x = f_{p-2,\alpha}^n(x)$ for $x \in \mathbb{F}_p \setminus \mathcal{O}_{(\alpha,\ldots,\alpha)}^n$.

We have to show $\#\mathcal{O}_{(\alpha,\ldots,\alpha)}^n = n$. It is equivalent to show that if

$$
\frac{F_l}{F_{l+1}} = \frac{F_k}{F_{k+1}}
$$

for some $0 \leq l, k \leq n$, then $l = k$. Without lose of generality, we can assume $k \geq l$. By Lemma 4.4, we know $k - l$ is the multiplicative order of $z_+/z_-$. However, $n - 1$ should be less than or equal to the order by (6) and our assumption on $n$, so we get $n \leq k - l$. By $0 \leq l, k \leq n$, the consequence has to be $l = k$. 


Let $R(x) = R_1(x)$. The pole of $R(x)$ is 0, and we have $R_i(x) = R^i(x)$ for all $i$. Given $c \in \mathcal{O}_{\alpha_1,\ldots,\alpha_n}$, $f_{p-2,\alpha}(f_{p-2,\alpha}'(c)) = R(R_i(c)) = R_{i+1}(c)$ if and only if $R_{p-2}^i(\alpha)(c) \neq 0$. $R(x)$ is equal to $x'/x''$ where $x'$ and $x''$ is given by

$$\begin{bmatrix} a & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x \\ 1 \end{bmatrix} = \begin{bmatrix} x' \\ x'' \end{bmatrix}.$$ 

A pole $c$ is $-\frac{F_{i-1}}{F_i}$ or $R^i$, and the above computation shows

$$\begin{bmatrix} \alpha & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -F_{i-1}(\alpha) \\ F_i(\alpha) \end{bmatrix} = \begin{bmatrix} -\alpha F_{i-1}(\alpha) + F_i(\alpha) \\ -F_{i-1}(\alpha) \end{bmatrix} = \begin{bmatrix} -\alpha F_{i-1}(\alpha) + \alpha F_{i-1}(\alpha) + F_{i-2} \\ F_{i-1} \end{bmatrix} = \begin{bmatrix} F_{i-2} \\ -F_{i-1} \end{bmatrix}.$$ 

Thus, we have $f_{p-2,\alpha}^{-1}(-F_{i-1}/F_i) = 0$. It implies that $f_{p-2,\alpha}^n$ represents the permutation

$$\left( -\frac{F_{n-1}}{F_{n-2}} \ldots -\frac{F_3}{F_2} -\frac{F_2}{F_1} 0 \right).$$

Conversely, if $f_{p-2,\alpha}^n$ fixes at least $n + 4$ elements in $\mathbb{F}_p$, then it implies at least 4 elements are 1-linear and not a pole of $R_i(x)$ for all $i \leq n$. Therefore, $R_n(x) = x$, which implies $F_n(\alpha) \equiv 0 \pmod{p}$. \hfill \square

### Appendix A. Randomness in the $n$-th depth

**Appendix by Wayne Peng and Ching-Hua Shih**

While preparing the paper, the authors were asked by Shih-Han Hung what we could say about the permutation which appear in the $n$-th depth of the inverse tree used in the proof of Lemma 3.2, see Figure 1.

We further define the followings. On each level of the inverse tree, we say a permutation is of the **first type** if the last polynomial used in the composition is the inversion $\sigma$. Otherwise, we say the permutation is of the **second type**.

Our belief is that the permutations that appear in the $n$-th level should be random. If the permutations in the $n$-th level of the tree do appear randomly, then the probability that two elements, say $a = 1$ and $b = 2$, appear in the same cycle of a randomly selected permutation at that level is $\frac{1}{2}$. If we claim the behavior of permutations of the first type, $p$, with the correspondent permutation $p\delta$ of the second type, is independent, then the probability that $a$ and $b$ appear in the same cycle for $p$ and $p\delta$ together is $\frac{1}{4}$.

Using this fact, we used Sage [10] to find the frequency of $b$ in the orbit of $a$ under a permutation. We go through all primes from 547 (the 101-st prime) to 1229 (the 201-st prime) with depth from 1 to 10. However, it is computationally difficult to go through all branches on the inverse trees due to the exponentially growth of the tree, so for each prime and each depth, we generate 500 many random paths to the $n$-th level of the tree and tested whether 2 was in the orbit of 1.

The complete data can be found here. We demonstrate our result by providing the histograms for the first type, the second type, and both occurring. These histogram support our hypothesis that the random permutations appear on the $n$-th depth of the inverse tree, and it also support that $p$ and $p\delta$ are independent events.
We can do a more detailed analysis by applying $p$-test to small primes and depths. In those cases, we can run through all branches on the inverse trees by a defined pattern, and get a string of 0’s and 1’s where 0 means $a = 1$ and $b = 2$ are not on the same cycle of the permutation, and 1 means $a$ and $b$ are on the same cycle. For a given prime $p$, the branches at depth $d$ can be indexed by $\{1, 2, \ldots, p-1\}^d$ with lexicographic order. Let $(i_1, i_2, \ldots, i_d)$ be an index. The $k$-th coordinate $i_k$ indicates the path, compose with $\sigma^{i_k}$, from the depth $k - 1$ to the depth $k$. The result of the test is shown below, see Figures 3 and 4. The test shows that a string is likely to consists only of 0’s or only of 1’s when the depth becomes large.

**Acknowledgements**

This material is based upon work supported by the National Science Foundation under Grant No. DMS-1439786 while the author was in residence at the Institute for Computational and Experimental Research in Mathematics in Providence, RI, during the Summer@ICERM 2019 program on Computational Arithmetic Dynamics.

Towsley would like to thank John Doyle, Ben Hutz and Bianca Thompson for their collaboration organizing Summer@ICERM 2019 where this work was done.

**References**

[1] Esen Aksoy, Ayça Çeşmelioğlu, Wilfried Meidl, and Alev Topuzoğlu. On the Carlitz rank of permutation polynomials. *Finite Fields Appl.*, 15(4):428–440, 2009.

[2] Nurdagül Anbar, Almasa Odžak, Vandita Patel, Luciane Quoos, Anna Somoza, and Alev Topuzoğlu. On the Carlitz rank of permutation polynomials over finite fields: recent developments. In *Women in numbers Europe II*, volume 11 of *Assoc. Women Math. Ser.*, pages 39–55. Springer, Cham, 2018.

[3] L. Carlitz. Permutations in a finite field. *Proc. Amer. Math. Soc.*, 4:538, 1953.

[4] Ayça Çeşmelioğlu, Wilfried Meidl, and Alev Topuzoğlu. On the cycle structure of permutation polynomials. *Finite Fields Appl.*, 14(3):593–614, 2008.

[5] Ayça Çeşmelioğlu, Wilfried Meidl, and Alev Topuzoğlu. Permutations of finite fields with prescribed properties. *J. Comput. Appl. Math.*, 259(part B):536–545, 2014.

[6] S. Dolinar and D. Divsalar. Weight distributions for turbo codes using random and nonrandom permutations. 1995.

[7] Ryan Flynn and Derek Garton. Graph components and dynamics over finite fields. *Int. J. Number Theory*, 10(3):779–792, 2014.

[8] Domingo Gómez-Pérez, Alina Ostafe, and Alev Topuzoğlu. On the Carlitz rank of permutations of $\mathbb{F}_q$ and pseudorandom sequences. *J. Complexity*, 30(3):279–289, 2014.

[9] V. Gončarov. On the field of combinatorial analysis. *Amer. Math. Soc. Transl. (2)*, 19:1–46, 1962.
| Prime | Depth | Two sided p-value | Less p-value | Greater p-value |
|-------|-------|------------------|--------------|-----------------|
| 3     | 2     | 0.82809          | 0.14004      | 0.85996         |
|       | 3     | 0.78151          | 0.60924      | 0.39076         |
|       | 5     | 0.91628          | 0.54186      | 0.45814         |
| 5     | 2     | 0.26335          | 0.86833      | 0.13167         |
|       | 3     | 0.45392          | 0.22696      | 0.77304         |
|       | 4     | 0.59871          | 0.70064      | 0.29936         |
|       | 5     | 0.03095          | 0.98452      | 0.01547         |
| 7     | 2     | 0.16883          | 0.91558      | 0.08442         |
|       | 3     | 0.45259          | 0.86271      | 0.13729         |
|       | 4     | 0.00042          | 0.99979      | 0.00021         |
|       | 5     | 4.42e-05         | 0.99998      | 2.21e-05        |
| 11    | 2     | 0.68766          | 0.34383      | 0.65617         |
|       | 3     | 0.96205          | 0.48103      | 0.51897         |
|       | 4     | 0.00677          | 0.00339      | 0.99661         |
|       | 5     | 1.13e-05         | 5.65e-06     | 1.00000         |
| 13    | 2     | 0.73800          | 0.63100      | 0.36700         |
|       | 3     | 0.99996          | 0.50002      | 0.49998         |
|       | 4     | 0.95143          | 0.47572      | 0.52428         |
|       | 5     | 0.56364          | 0.71818      | 0.28182         |
| 17    | 2     | 0.98750          | 0.50625      | 0.49375         |
|       | 3     | 0.31958          | 0.15979      | 0.84021         |
|       | 4     | 0.66922          | 0.66539      | 0.33461         |
|       | 5     | 0.00416          | 0.00208      | 0.99792         |
| 19    | 2     | 0.37178          | 0.81411      | 0.18589         |
|       | 3     | 0.60601          | 0.30301      | 0.69699         |
|       | 4     | 0.83950          | 0.58025      | 0.41975         |
|       | 5     | 2.72e-17         | 1.36e-17     | 1.00000         |
| 23    | 2     | 0.52573          | 0.26286      | 0.73714         |
|       | 3     | 0.93955          | 0.46978      | 0.53022         |
|       | 4     | 0.34180          | 0.82910      | 0.17090         |
|       | 5     | 0.00016          | 7.90e-05     | 0.99992         |

**Figure 3.** $p$-values of the for the randomness of the sequence of zeros and ones created by testing if 2 is in the orbit of 1 modulo $p$ for polynomials of the first type.

[10] Leyla Işık and Arne Winterhof. Carlitz rank and index of permutation polynomials. *Finite Fields Appl.*, 49:156–165, 2018.

[11] Moharram Iradmusa and Reza Taleb. On minimal generating sets for symmetric and alternating groups. *Bulletin of the Iranian Mathematical Society*, 44, 06 2018.

[12] Y. Laigle-Ghapuy. Permutation polynomials and applications to coding theory. *Finite Fields and Their Applications*, 13(1):58 – 70, 2007.

[13] Gary L. Mullen, Daqing Wan, and Qiang Wang. Index bounds for value sets of polynomials over finite fields. In *Applied algebra and number theory*, pages 280–296. Cambridge Univ. Press, Cambridge, 2014.

[14] Harald Niederreiter and Arne Winterhof. Cyclotomic $R$-orthomorphisms of finite fields. *Discrete Math.*, 295(1-3):161–171, 2005.

[15] Wayne Peng. Abc implies there are infinitely many non-fibonacci–wieferich primes - an application of abc conjecture over number fields, 2015.
| Prime | Depth | Two sided p-value | Less p-value | Greater p-value |
|-------|-------|-------------------|--------------|----------------|
| 3     | 2     | 0.28009           | 0.14004      | 0.85996        |
|       | 3     | 0.00000           | 0.99970      | 0.00030        |
|       | 4     | 0.00516           | 0.99742      | 0.00258        |
|       | 5     | 7.67729           | 1.00000      | 3.84e-09       |
| 5     | 2     | 0.05686           | 0.97157      | 0.02843        |
|       | 3     | 0.00000           | 0.99970      | 0.00030        |
|       | 4     | 0.00516           | 0.99742      | 0.00258        |
|       | 5     | 7.67729           | 1.00000      | 3.84e-09       |
| 7     | 2     | 0.01835           | 0.99083      | 0.00917        |
|       | 3     | 0.00852           | 0.99574      | 0.00426        |
|       | 4     | 7.79e-17          | 1            | 3.90e-17       |
|       | 5     | 1.30e-79          | 1            | 6.50e-80       |
| 11    | 2     | 0.11040           | 0.94480      | 0.05520        |
|       | 3     | 9.85e-09          | 1.00000      | 4.93e-09       |
|       | 4     | 2.25e-39          | 1            | 1.13e-39       |
|       | 5     | 0                | 1            | 0              |
| 13    | 2     | 0.44849           | 0.77576      | 0.22424        |
|       | 3     | 2.40e-09          | 1.00000      | 1.20e-09       |
|       | 4     | 1.31e-45          | 1            | 6.54e-46       |
|       | 5     | 0                | 1            | 0              |
| 17    | 2     | 0.05296           | 0.97351      | 0.0264815215218201 |
|       | 3     | 7.79e-13          | 1.00000      | 3.89725348505465e-13 |
|       | 4     | 1.77e-127         | 1            | 8.85e-128      |
|       | 5     | 0                | 1            | 0              |
| 19    | 2     | 4.19e-13          | 1.00000      | 2.10e-13       |
|       | 3     | 8.41e-24          | 1            | 4.20e-24       |
|       | 4     | 8.29e-157         | 1            | 4.15e-157      |
|       | 5     | 0                | 1            | 0              |
| 23    | 2     | 4.34e-09          | 1.00000      | 2.17e-09       |
|       | 3     | 7.59e-28          | 1            | 3.79e-28       |
|       | 4     | 1.71e-256         | 1            | 8.53e-257      |
|       | 5     | 0                | 1            | 0              |

Figure 4. $p$-values of the for the randomnness of the sequence of zeros and ones created by testing if 2 is in the orbit of 1 modulo $p$ for polynomials of the second type.

[16] J. M. Pollard. A Monte Carlo method for factorization. *Nordisk Tidsskr. Informationsbehandling (BIT)*, 15(3):331–334, 1975.
[17] Joseph H. Silverman. *A friendly introduction to number theory*. Upper Saddle River, NJ: Prentice Hall, 1997.
[18] R. Singh and S. Maity. Permutation polynomials modulo $p^n$. Cryptology ePrint Archive, Report 2009/393, 2009. https://eprint.iacr.org/.
[19] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.0)*. Sage Development Team, 2016.
[20] Alev Topuzoğlu. The Carlitz rank of permutations of finite fields: a survey. *J. Symbolic Comput.*, 64:53–66, 2014.
[21] Daqing Wan and Qiang Wang. Index bounds for character sums of polynomials over finite fields. *Des. Codes Cryptogr.*, 81(3):459–468, 2016.
[22] Qiang Wang. Cyclotomy and permutation polynomials of large indices. Finite Fields Appl., 22:57–69, 2013.
E-mail address: annanc2@illinois.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, CHAMPAIGN, ILLINOIS, USA

E-mail address: j10128@westminstercollege.edu

DEPARTMENT OF MATHEMATICS, WESTMINSTER COLLEGE, SALT LAKE CITY, UT, USA

E-mail address: junwen.wayne.peng@gmail.com

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ROCHESTER, ROCHESTER, NY, USA

E-mail address: sheareaj@plu.edu

PACIFIC LUTHERAN UNIVERSITY, TACOMA, WA, USA

E-mail address: adtsma@rit.edu

SCHOOL OF MATHEMATICAL SCIENCES, ROCHESTER INSTITUTE OF TECHNOLOGY, ROCHESTER, NY, USA