Permutations from an arithmetic setting

Lucas Reis[a,1,*], Sávio Ribas[b]

[a] *Universidade de São Paulo, Instituto de Ciências Matemáticas e de Computação, São Carlos, SP 13560-970, Brazil.*
[b] *Universidade Federal de Ouro Preto, Instituto de Ciências Exatas e Biológicas, Departamento de Matemática, Ouro Preto, MG 35400-000, Brazil.*

Abstract

Let m, n be positive integers such that $m > 1$ divides n. In this paper, we introduce a special class of piecewise-affine permutations of the finite set $[1, n] := \{1, \ldots, n\}$ with the property that the reduction (mod m) of m consecutive elements in any of its cycles is, up to a cyclic shift, a fixed permutation of $[1, m]$. Our main result provides the cycle decomposition of such permutations. We further show that such permutations give rise to permutations of finite fields. In particular, we explicitly obtain classes of permutation polynomials of finite fields whose cycle decomposition and its inverse are explicitly given.

Keywords: permutations; cycle decomposition; m-th residues; finite fields
2010 MSC: 05A05, 11B50, 11T22

1. Introduction

Let m, n be positive integers such that $m > 1$ divides n. For integers $1 \le k_1 < k_2$, set $[k_1, k_2] = \{t \in \mathbb{N} \mid k_1 \le t \le k_2\}$. In this paper, we introduce a special class of *piecewise-affine permutations* of the set $[1, n]$. These permutations are piecewisely defined by affine-like rules, according to classes modulo m, in a way that the reduction modulo m of m consecutive elements in any of its cycles is, up to a cyclic shift, a fixed permutation of $[1, m]$. In particular, every cycle of this kind of permutation has length divisible by m. One of our main results, Theorem 3.8, provides the explicit cycle decomposition of such permutations. We also provide complete results on the characterization and number of such permutations. In particular, we show that the inverses of such permutations are of the same type and can be easily computed.

We further use our piecewise-affine permutations in the construction of permutation polynomials over finite fields. Namely, let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements. A polynomial $f \in \mathbb{F}_q[x]$ is called a *permutation polynomial* if the evaluation map $c \mapsto f(c)$ is a permutation of $\mathbb{F}_q$. It is well known that $\mathbb{F}_q^*$ is a multiplicative cyclic group of order $q - 1$. Let θ_q be a generator of $\mathbb{F}_q^*$. It turns out that if $f : \mathbb{F}_q \to \mathbb{F}_q$ is the function given by

$$f(0) = 0 \quad \text{and} \quad f(\theta_q^i) = \theta_q^{\pi(i)} \quad \text{for all } 1 \le i \le q - 1,$$

where π is a piecewise-affine permutation of $[1, q-1]$, the polynomial representation of the permutation f as well as its cycle decomposition and inverse can be derived. The permutations like the previous one are piecewise defined by monomials, according to *cyclotomic cosets*. This kind of permutations was previously explored in full generality by Wang [15]. However, there is no study on their cycle decomposition. It is worth mentioning that, for only few families of permutation polynomials, we know the cycle decomposition without needing to describe the whole permutation; namely, *monomials* [1], *Mbius maps* [6], *Dickson polynomials* [10] and certain *linearized polynomials* [11, 13].

---

*Corresponding author
Email addresses: `lucasreismat@gmail.com` (Lucas Reis), `savio.ribas@ufop.edu.br` (Sávio Ribas)
[1]Permanent address: Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte, MG, 30123-970, Brazil.

The idea of bringing piecewise permutations to obtain permutation polynomials was earlier used by Fernando & Hou [7] and by Cao, Hu & Zha [5], who obtained families of permutation polynomials via certain powers of linearized polynomials and using a matrix approach, respectively. Some other algebraic-combinatorial methods to produce large classes of permutation polynomials include *linear translators* [9], *algebraic curves* [3], and, most notably, the *AGW criterion* [2]. See [12, §8] for more details on permutation polynomials over finite fields and [8] for a survey on recent advances.

The structure of the paper is given as follows. In Section 2, we introduce our class of piecewise-affine permutations of $[1, n]$ and present some fundamental results, including the inverses (which are also piecewise-affine); in particular, we explore a special subclass of these permutations that are defined by two rules. In Section 3, we obtain an explicit description on their cycle decomposition. In Section 4 we show how these permutations can be used in the construction of permutation polynomials over finite fields and their inverses, and discuss further issues on these permutation polynomials.

2. On piecewise-affine permutations of the set $[1, n]$

We start fixing some notation. The letters n, m always denote positive integers such that $m > 1$ divides n. In general, $\vec{a}$ denotes an m-tuple of integers in a fixed range (usually $[1, m]$ or $[1, n]$). Also, a_i denotes the i-th coordinate of $\vec{a}$. In addition, for a positive integer $N > 1$, let $\mathrm{rad}(N)$ denote the product of the distinct prime divisors of N, and let $\mathrm{rad}(1) = 1$. We also denote by φ the Euler's totient function, and by $\mathrm{ord}_k r$ the order of r modulo k.

Definition 2.1. *Let $\mathcal{C}(m)$ denote the subset of $[1, m]^m$ of the vectors $\vec{c}$ whose entries comprise a permutation of the set $[1, m]$.*

Definition 2.2. *For an integer $k > 1$, let $\Psi_k : \mathbb{N} \to [1, k]$ such that $\Psi_k(a) = a \pmod{k}$.*

Definition 2.3. *An (n, m)-piecewise affine permutation (or (n, m)-p.a.p.) is a permutation π of the set $[1, n]$ such that there exist $\vec{a}, \vec{b} \in [1, n]^m$ and $\vec{c} \in \mathcal{C}(m)$ with the property that*

$$\pi(x) = \Psi_n(a_i x + b_i) \quad and \quad \Psi_m(\pi(x)) = c_{i+1}, \tag{1}$$

for any $x \in [1, n]$ with $\Psi_m(x) = c_i$, where the indexes are taken modulo m. In this case, we say that the triple $(\vec{a}, \vec{b}, \vec{c})$ is (n, m)-admissible and π is the (n, m)-p.a.p. with parameters $(\vec{a}, \vec{b}, \vec{c})$. Furthermore, we say that two (n, m)-admissible triples $(\vec{a}, \vec{b}, \vec{c})$ and $(\vec{A}, \vec{B}, \vec{C})$ are (n, m)-equivalent if they induce the same permutation on $[1, n]$.

Example 2.4. *Let $n = 12$, $m = 3$ and let π be the $(12, 3)$-p.a.p. with parameters $(\vec{a}, \vec{b}, \vec{c})$, where $\vec{a} = (1, 3, 5)$, $\vec{b} = (4, 6, 1)$ and $\vec{c} = (1, 2, 3)$. In other words, for each $x \in [1, 12]$,*

$$\pi(x) = \begin{cases} \Psi_{12}(x + 4) & if\ x \equiv 1 \pmod{3}, \\ \Psi_{12}(3x + 6) & if\ x \equiv 2 \pmod{3}, \\ \Psi_{12}(5x + 1) & if\ x \equiv 0 \pmod{3}. \end{cases}$$

The cycle decomposition of π is given by $(1\ 5\ 9\ 10\ 2\ 12)\ (3\ 4\ 8\ 6\ 7\ 11)$.

In the following theorem we characterize, up to (n, m)-equivalence, all the (n, m)-admissible triples.

Theorem 2.5. *Let $m > 1$ be a divisor of n and write $n = n_1 n_2$, where $\mathrm{rad}(n_1)$ divides $\frac{n}{m}$ and $\gcd\left(n_2, \frac{n}{m}\right) = 1$. Let $\vec{a} \in [1, n]^m$ and $\vec{c} \in \mathcal{C}(m)$. Then there exists an element $\vec{b} \in [1, n]^m$ such that the triple $(\vec{a}, \vec{b}, \vec{c})$ is (n, m)-admissible if and only if the entries of $\vec{a}$ are relatively prime with n_1. In this case, there are $\left(\frac{n}{m}\right)^m$ choices for $\vec{b}$. Moreover, two (n, m)-admissible triples $(\vec{a}, \vec{b}, \vec{c})$ and $(\vec{A}, \vec{B}, \vec{C})$ are (n, m)-equivalent if and only if there exists $t \in [1, m]$ such that, for every $1 \le i \le m$, the following properties hold:*

(i) $c_i = C_{i+t}$;

(ii) $a_i \equiv A_{i+t} \pmod{n/m}$;

(iii) $B_{i+t} = \Psi_n(a_i c_i + b_i - A_{i+t}C_{i+t})$.

Proof. We observe that π is an (n,m)-p.a.p. with parameters $(\vec{a}, \vec{b}, \vec{c})$ if and only if π is of the form given by Eq. (1) and π is one to one. Suppose that $x, y \in [1, n]$ are such that $\pi(x) = \pi(y)$. Then $\pi(x) \equiv \pi(y) \equiv c_{i+1} \pmod{m}$ for some $i \in [1, m]$ and, by definition, $x \equiv y \equiv c_i \pmod{m}$, where i is taken modulo m. Therefore, the condition $\pi(x) = \Psi_n(a_i x + b_i) = \Psi_n(a_i y + b_i) = \pi(y)$ is equivalent to $a_i(x - y) \equiv 0 \pmod{n}$. Since n_2 divides n and $\gcd\left(n_2, \frac{n}{m}\right) = 1$, we have that n_2 divides m. Since $\gcd(n_1, n_2) = 1$, $x \equiv y \pmod{m}$ and n_2 divides m, the equation $a_i(x - y) \equiv 0 \pmod{n}$ is equivalent to

$$a_i(x - y) \equiv 0 \pmod{n_1},$$

which has the unique solution $x \equiv y \pmod{n_1}$ if and only if $\gcd(a_i, n_1) = 1$. In particular, π is one to one if and only if $\gcd(a_i, n_1) = 1$ for any $i \in [1, m]$. In this case, each b_i is uniquely determined modulo m by

$$b_i \equiv c_{i+1} - a_i c_i \pmod{m}.$$

Since the entries of $\vec{b}$ lie in $[1, n]$, there exist $\left(\frac{n}{m}\right)^m$ possibilities for $\vec{b}$.

Moreover, if the (n,m)-admissible triples $(\vec{a}, \vec{b}, \vec{c})$ and $(\vec{A}, \vec{B}, \vec{C})$ are (n,m)-equivalent, then, up to a cyclic shift, $\vec{c}$ and $\vec{C}$ are the same, so (i) holds. From this, we obtain $\Psi_n(a_i c_i + b_i) = \Psi_n(A_{i+t}C_{i+t} + B_{i+t})$, which implies (iii). Furthermore, for every $i \in [1, m]$ and every $j \in [1, \frac{n}{m}]$, we have that $a_i(c_i + jm) + b_i \equiv A_{i+t}(C_{i+t} + jm) + B_{i+t} \pmod{n}$, which implies that $(a_i - A_{i+t})j \equiv 0 \pmod{\frac{n}{m}}$, proving (ii). Conversely, if (i), (ii) and (iii) hold, then for every $i \in [1, m]$ and $j \in [1, \frac{n}{m}]$, the identities $a_i(c_i + jm) + b_i \equiv A_{i+t}(C_{i+t} + jm) + B_{i+t} \pmod{n}$ and $\Psi_m(a_i(c_i + jm) + b_i) = c_i = C_{i+t} = \Psi_m(A_{i+t}(C_{i+t} + jm) + B_{i+t})$ hold. Therefore, $(\vec{a}, \vec{b}, \vec{c})$ and $(\vec{A}, \vec{B}, \vec{C})$ are (n,m)-equivalent. $\square$

From the previous theorem, we obtain the exact number of permutations arising from (n,m)-p.a.p.'s.

Corollary 2.6. *Let $m > 1$ be a divisor of n and write $n = n_1 n_2$, where $\mathrm{rad}(n_1)$ divides $\frac{n}{m}$ and $\gcd\left(n_2, \frac{n}{m}\right) = 1$. Then the number of distinct (n,m)-p.a.p.'s equals*

$$(m - 1)! \cdot \left(\frac{n \cdot n_2 \cdot \varphi(n_1)}{m^2}\right)^m.$$

Proof. First, we compute the number of (n,m)-admissible triples. There are $m!$ choices for $\vec{c}$, and $n_2 \cdot \varphi(n_1)$ choices for each a_i, hence $[n_2 \cdot \varphi(n_1)]^m$ choices for $\vec{a}$. In addition, for fixed $\vec{a}$ and $\vec{c}$, there are $\left(\frac{n}{m}\right)^m$ choices for $\vec{b}$. Therefore, the number of (n,m)-admissible triples equals $m! \cdot \left(\frac{n \cdot n_2 \cdot \varphi(n_1)}{m}\right)^m$. For a fixed (n,m)-admissible triple $(\vec{a}, \vec{b}, \vec{c})$, Theorem 2.5 entails that such triple is (n,m)-equivalent to exactly $m \cdot \delta_m$ (n,m)-admissible triples, where δ_m is the number of ways of choosing vectors $(u_1, \ldots, u_m) \in [1, n]^m$ with $\gcd(u_i, n_1) = 1$ and $u_i \equiv a_i \pmod{n/m}$. From contruction, $\mathrm{rad}(n_1) = \mathrm{rad}(n/m)$ and so $u_i \equiv a_i \pmod{n/m}$ already implies that $\gcd(u_i, n_1) = 1$. Hence, $\delta_m = m^m$ and the result follows. $\square$

2.1. On the inverse of (n,m)-p.a.p.'s

We show that the inverse of an (n,m)-p.a.p. is another (n,m)-p.a.p. whose parameters can be explicitly computed (though not unique).

Theorem 2.7. *Let $m > 1$ be a divisor of n and write $n = n_1 n_2$, where $\mathrm{rad}(n_1)$ divides $\frac{n}{m}$ and $\gcd\left(n_2, \frac{n}{m}\right) = 1$. Let $(\vec{a}, \vec{b}, \vec{c})$ be an (n,m)-admissible triple and π be the (n,m)-p.a.p. with parameters $(\vec{a}, \vec{b}, \vec{c})$. For each $1 \leq i \leq m$, let $A_i \in [1, n_1]$ be such that $A_i \cdot a_{i-1} \equiv 1 \pmod{n_1}$. Then, for each $1 \leq i \leq m$, the system of congruences*

$$\begin{cases} x \equiv c_{i-1} - A_i c_i \pmod{m} \\ x \equiv -A_i b_{i-1} \pmod{n_1}, \end{cases} \tag{2}$$

3

admits a solution $B_i \in [1,n]$. *Also, if* $\vec{A} = (A_m, A_{m-1}, \ldots, A_1)$, $\vec{B} = (B_m, B_{m-1}, \ldots, B_1)$ *and* $\vec{C} = (c_m, c_{m-1}, \ldots, c_1)$, *then the triple* $(\vec{A}, \vec{B}, \vec{C})$ *is* (n,m)-*admissible and the permutation* π^{-1} *induced by such triple is the inverse of* π, *i.e.,*

$$\pi(\pi^{-1}(y)) = \pi^{-1}(\pi(y)) = y, \quad y \in [1,n].$$

Proof. From Theorem 2.5, we have that $\gcd(a_i, n_1) = 1$ for every $1 \leq i \leq m$, and so A_i is well defined. In order to prove that the system above has a solution $B_i \in [1,n]$, the Chinese Remainder Theorem entails that it suffices to show that

$$-A_i b_{i-1} \equiv c_{i-1} - A_i c_i \quad (\text{mod } \gcd(m, n_1)),$$

for every $1 \leq i \leq m$. This is true since the congruence $a_{i-1} c_{i-1} + b_{i-1} \equiv c_i \pmod{m}$ implies that $c_{i-1} + A_i b_{i-1} \equiv A_i c_i \pmod{\gcd(m, n_1)}$. From definition, $\gcd(A_i, n_1) = 1$ and

$$A_i c_i + B_i \equiv c_{i-1} \quad (\text{mod } m).$$

From Theorem 2.5, the triple $(\vec{A}, \vec{B}, \vec{C})$ is (n,m)-admissible. So it remains to prove that $\pi(\pi^{-1}(y)) = \pi^{-1}(\pi(y)) = y$ for $y \in [1,n]$. We only prove $\pi^{-1}(\pi(y)) = y$ since the equality $\pi(\pi^{-1}(y)) = y$ follows in a similar way. From definition, n_1 and n_2 are relatively prime and n_2 divides m. So it suffices to prove that $\pi^{-1}(\pi(y)) \equiv y \pmod{t}$ for $t \in \{n_1, m\}$. Suppose that $y \equiv c_i \pmod{m}$, hence $\pi(y) \equiv c_{i+1} \pmod{m}$ and so $\pi^{-1}(\pi(y)) \equiv c_i \equiv y \pmod{m}$. Moreover, $\pi^{-1}(\pi(y)) = \Psi_n(A_{i+1}(a_i y + b_i) + B_{i+1})$. Recall that n_1 is a divisor of n. From $A_{i+1} a_i \equiv 1 \pmod{n_1}$ and $B_{i+1} \equiv -A_{i+1} b_i \pmod{n_1}$, we conclude that

$$\Psi_n(A_{i+1}(a_i y + b_i) + B_{i+1}) \equiv y \quad (\text{mod } n_1).$$

$\square$

Example 2.8. *Let* π *the* $(12,3)$-*p.a.p. defined in Example 2.4. Then the inverse* π^{-1} *of* π *is the* $(12,3)$-*p.a.p. with parameters* $(\vec{A}, \vec{B}, \vec{C})$, *where* $\vec{A} = (3,1,1)$, $\vec{B} = (2,8,11)$ *and* $\vec{C} = (3,2,1)$ *so that, for each* $x \in [1,12]$,

$$\pi^{-1}(x) = \begin{cases} \Psi_{12}(x+11) & \text{if } x \equiv 1 \pmod 3, \\ \Psi_{12}(x+8) & \text{if } x \equiv 2 \pmod 3, \\ \Psi_{12}(3x+2) & \text{if } x \equiv 0 \pmod 3. \end{cases}$$

2.2. The class of p.a.p.'s defined by two rules

Here we introduce the special class of (n,m)-p.a.p.'s that can be defined by two affine-like rules, one for the multiples of m and one for the remaining integers in $[1,n]$. More specifically, we have the following definition.

Definition 2.9. *An* (n,m)-*p.a.p.* π *is said to be* 2-reducible *if there exist integers* $a_0, a, b_0, b \in [1,n]$ *such that, for any* $x \in [1,n]$, *we have that*

$$\pi(x) = \begin{cases} \Psi_n(a_0 \cdot x + b_0) & \text{if } x \equiv 0 \pmod m, \\ \Psi_n(a \cdot x + b) & \text{if } x \not\equiv 0 \pmod m. \end{cases}$$

In this case, the quadruple (a_0, a, b_0, b) *is called the* 2-reduced parameters *of* π.

From definition, any (n,m)-p.a.p. is 2-reducible if $m = 2$. Our aim is to provide a complete characterization of the 2-reducible (n,m)-p.a.p.'s, where $m > 2$. We start with the following auxiliary lemmas.

Lemma 2.10 (Lifting the Exponent Lemma)**.** *Let* p *be a prime and* ν_p *be the* p-*valuation. The following hold:*

(1) *if* p *is an odd prime divisor of* $a - 1$, $\nu_p(a^k - 1) = \nu_p(a - 1) + \nu_p(k)$;

(2) if $p = 2$ and $a > 1$ is odd,

$$\nu_2(a^k - 1) = \begin{cases} \nu_2(a - 1) & \text{if } k \text{ is odd,} \\ \nu_2(a^2 - 1) + \nu_2(k) - 1 & \text{if } k \text{ is even.} \end{cases}$$

Lemma 2.11. *Let a, b, m be positive integers and set $\mathrm{rad}_2(m) = \mathrm{rad}(m) \cdot \gcd(m, 2)$. Then the reductions modulo m of the numbers*

$$b, \ b(a + 1), \ \ldots, \ b(a^{m-1} + \cdots + a + 1)$$

are all distinct if and only if $\gcd(b, m) = 1$ and $a \equiv 1 \pmod{\mathrm{rad}_2(m)}$.

Proof. Set $f_0 = b$ and, for $1 \le i \le m - 1$, set $f_i = b(a^i + \cdots + a + 1)$. It is clear that b (resp. a) must be relatively prime with m, since otherwise the reduction modulo m of the elements f_i would not contain the class 1 (resp. the class 0). In particular, for $0 \le i < j \le m - 1$, $f_i \equiv f_j \pmod{m}$ if and only if $f_{j-i} \equiv 0 \pmod{m}$. Therefore, it suffices to prove that $i = m - 1$ is the smallest index such that $f_i \equiv 0 \pmod{m}$ if and only if $a \equiv 1 \pmod{\mathrm{rad}_2(m)}$. Of course, this holds for $a = 1$. Suppose that $a > 1$ and write $m = m_0 m_1$, where $\mathrm{rad}(m_0)$ divides $a - 1$ and m_1 is relatively prime with $a - 1$. In other words, we want to prove that $\mathrm{ord}_{m(a-1)} a = m$ if and only if $m_0 = m$ and $a \equiv 1 \pmod 4$ if m is even. Since m_1 and $a - 1$ are relatively prime, we have that

$$\mathrm{ord}_{m(a-1)} a = \mathrm{lcm}(\mathrm{ord}_{m_0(a-1)} a, \mathrm{ord}_{m_1} a) \le \mathrm{ord}_{m_0(a-1)} a \cdot \mathrm{ord}_{m_1} a, \tag{3}$$

with equality if and only if $\mathrm{ord}_{m_0(a-1)} a$ and $\mathrm{ord}_{m_1} a$ are relatively prime. However, from Lemma 2.10, $\mathrm{ord}_{m_0(a-1)} a \le m_0$ with equality if and only if m_0 is odd or m_0 is even and $a \equiv 1 \pmod 4$. In addition, $\mathrm{ord}_{m_1} a \le \varphi(m_1) < m_1$ whenever $m_1 > 1$. Therefore, from Eq. (3), we have that $\mathrm{ord}_{m(a-1)} a = m$ if and only if $m_1 = 1$ (i.e., $m_0 = m$) and $a \equiv 1 \pmod 4$ if m is even. $\square$

In the following proposition we describe the 2-reducible (n, m)-p.a.p's.

Proposition 2.12. *Let $m > 2$ be a positive divisor of n and write $n = n_1 n_2$, where $\mathrm{rad}(n_1)$ divides $\frac{n}{m}$ and $\gcd\left(n_2, \frac{n}{m}\right) = 1$. For integers $a_0, a, b_0, b \in [1, n]$, the quadruple (a_0, a, b_0, b) provides the 2-reduced parameters of a 2-reducible (n, m)-p.a.p. π if and only if the following properties hold:*

(i) *b and b_0 are relatively prime with m, and $b \equiv b_0 \pmod m$;*
(ii) *$a \equiv 1 \pmod{\mathrm{rad}_2(m)}$;*
(iii) *a and a_0 are relatively prime with n_1.*

In this case, π is the (n, m)-p.a.p. with parameters $(\vec{a}, \vec{b}, \vec{c})$, where $\vec{a} = (a_0, a, \ldots a)$, $\vec{b} = (b_0, b, \ldots, b)$ and $\vec{c}$ is a cyclic permutation of the vector $(c_1, \ldots, c_m)$ with

$$c_i = \begin{cases} m & \text{if } i = 1, \\ \Psi_m(b \cdot (a^{i-2} + a^{i-3} + \ldots + a + 1)) & \text{if } 2 \le i \le m. \end{cases} \tag{4}$$

Moreover, the inverse π^{-1} of the 2-reducible (n, m)-p.a.p. π is defined by the following affine rules:

$$\pi^{-1}(x) = \begin{cases} \Psi_n(A_0 \cdot x + B_0) & \text{if } x \equiv b \pmod m \\ \Psi_n(A \cdot x + B) & \text{if } x \not\equiv b \pmod m \end{cases}$$

where $A_0 \equiv a_0^{-1} \pmod{n_1}$, $A \equiv a^{-1} \pmod{\mathrm{lcm}(m, n_1)}$, B_0 is a solution of the system (2) with $i = 2$ and $B = \Psi_n(-Ab)$.

Proof. For the first part, we just need to show that, if (a_0, a, b_0, b) are the 2-reduced parameters of the 2-reducible (n, m)-p.a.p. π, then we necessarily have that $b \equiv b_0 \pmod m$. The remainder 'if and only if' part follows from Theorem 2.5 and Lemma 2.11; the further identities for c_i follow directly by calculations.

5

We observe that, since π is an (n, m)-p.a.p., for any $t \in [1, m]$ such that $t \neq \Psi_m(b_0)$, there exists $y = y(t) \in [1, m-1]$ such that $ay + b \equiv t \pmod{m}$. In particular, if $b \not\equiv b_0 \pmod{m}$, there exists $y \in [1, m-1]$ such that $ay + b \equiv b \pmod{m}$ and so $ay \equiv 0 \pmod{m}$. This implies that $d := \gcd(a, m) > 1$. However, in this case, the set $\{\Psi_m(ay + b) \mid y \in [1, m-1]\}$ has at most $\frac{m}{d}$ elements. Since $m > 2$, we have that $\frac{m}{d} < m - 1$ and so we get a contradiction with the property of $y(t)$.

The expression for the parameters $A_0, A \in [1, n_1]$ and $B_0 \in [1, \mathrm{lcm}(m, n_1)]$ of π^{-1} follows directly from Theorem 2.7. Furthermore, we can extend $A \in [1, \mathrm{lcm}(m, n_1)]$ to be also the inverse of a modulo m so that $A \equiv a^{-1} \pmod{\mathrm{lcm}(m, n_1)}$, since $\gcd(a, m) = 1$ by item (ii). Let $B = \Psi_n(-Ab)$. We are going to show that B is a solution of the system (2) for every $i \in [1, m] \backslash \{2\}$. The second equation of system (2) is trivial. If $i \in [3, m]$ then the first one is equivalent to $B \equiv b(a^{i-3} + \cdots + a + 1) - Ab(a^{i-2} + \cdots + a + 1)$ $\pmod{m}$, which is true since $A \equiv a^{-1} \pmod{m}$. If $i = 1$ then the first equation of (2) is equivalent to $-Ab \equiv b(a^{m-2} + \cdots + a + 1) \pmod{m}$, which follows from Lemma 2.11. $\qquad\square$

From the previous proposition, a lower bound for the number of 2-reducible (n, m)-p.a.p.'s is derived.

Corollary 2.13. *The number of non-equivalent 2-reducible (n, m)-p.a.p.'s is at least*

$$\varphi\left(\frac{n}{m}\right) \cdot \frac{\varphi(m) \cdot n^2}{m^2}.$$

Proof. We provide a class of non-equivalent (n, m)-p.a.p.'s with 2-reduced parameters of the form $(a_0, 1, b_0, b)$ which proves the claim. Let C be the set of quadruples $(a_0, 1, b_0, b)$ such that $1 \leq a_0 \leq \frac{n}{m}$, $\gcd\left(a_0, \frac{n}{m}\right) = 1$ (hence $\gcd(a_0, n_1) = 1$), $1 \leq b_0 \leq n$, $\gcd(b, m) = 1$ and $b_0 \equiv b \pmod{m}$. Proposition 2.12 entails that any element of C yields a 2-reducible (n, m)-p.a.p. and it is clear that C has exactly $\varphi\left(\frac{n}{m}\right) \cdot \frac{\varphi(m) \cdot n^2}{m^2}$ elements. We just need to verify that any two of them yield non-equivalent permutations of $[1, n]$. Suppose that two elements $(a_0, 1, b_0, b)$ and $(a_0', 1, b_0', b')$ of C yield the same permutation of $[1, n]$. Since $a_0, a_0' \leq \frac{n}{m}$, Theorem 2.5 entails that $a_0 = a_0'$. Also, taking $x = n$ in Definition 2.9, we have that $b_0 = b_0'$ and the same definition readily implies that $b = b'$. $\qquad\square$

3. Cycle decomposition

We fix $(\vec{a}, \vec{b}, \vec{c})$ an (n, m)-admissible triple and $\pi = \pi(\vec{a}, \vec{b}, \vec{c})$ the (n, m)-p.a.p. with parameters $(\vec{a}, \vec{b}, \vec{c})$. The following proposition provides basic properties of the cycle decomposition of π.

Proposition 3.1. *For any $y \in [1, n]$, the following properties hold:*

(i) *the cycle of π containing y has length divisible by m;*

(ii) *there exists an element $z \in [1, n]$ such that z is divisible by m and lies in the same cycle of π containing y.*

In addition, if a cycle of π has length mt, then for each $i \in [1, m]$, such a cycle contains exactly t elements congruent to i modulo m.

Proof. (i) From Definition 2.3, $\Psi_m(\pi(x)) = c_{i+1}$ whenever $\Psi_m(x) = c_i$. This guarantees that the sequence

$$\Psi_m(y), \ \Psi_m(\pi(y)), \ \Psi_m(\pi^{(2)}(y)), \ \ldots$$

can only return to $\Psi_m(y)$ after cyclically running through the entries of $\vec{c} \in \mathcal{C}(m)$. In particular, the sequence

$$y, \ \pi(y), \ \pi^{(2)}(y), \ \ldots$$

has minimal period divisible by m.

(ii) In fact, there is an entry of $\vec{c}$ equals to m, and its correspondent in the above sequence is divisible by m.

We observe that, in a cycle of length mt of π, $\vec{c}$ is traversed t times if we consider the reduction modulo m of its elements. Therefore, each $i \in [1, m]$ appears exactly t times.

$\square$

In particular, in order to compute the cycle decomposition of π, Proposition 3.1 entails that it suffices to compute the minimal period of the multiples of m in the set $[1, n]$. In this context, the following definition is useful.

Definition 3.2. 1. *The* principal product *of* $\pi = \pi(\vec{a}, \vec{b}, \vec{c})$ *is* $P_\pi = \prod_{i=1}^{m} a_i$.

2. *The* principal sum *of* $\pi = \pi(\vec{a}, \vec{b}, \vec{c})$ *is the unique positive integer* $S_\pi \in [1, n]$ *with the property that* $\pi^{(m)}(x) = \Psi_n(P_\pi \cdot x + S_\pi)$, *for any* $x \in [1, n]$ *such that* $x \equiv 0 \pmod{m}$.

Example 3.3. *The principal product and principal sum of the 2-reducible (n, m)-p.a.p. π with parameters (a_0, a, b_0, b) are $P_\pi = a_0 a^{m-1}$ and $S_\pi = \Psi_n\left(b_0 a^{m-1} + b(a^{m-2} + \ldots + a + 1)\right)$ respectively.*

The following lemma provides a way of obtaining the mk-th iterates of π at elements $x \in [1, n]$ that are divisible by m.

Lemma 3.4. *The principal sum S_π of $\pi(\vec{a}, \vec{b}, \vec{c})$ is well defined and, for any positive integers k, x such that $x \in [1, n]$ is divisible by m, we have that*

$$\pi^{(mk)}(x) = \Psi_n\left(P_\pi^k \cdot x + \frac{P_\pi^k - 1}{P_\pi - 1} \cdot S_\pi\right),$$

whenever $P_\pi \neq 1$. For $P_\pi \equiv 1 \pmod{n}$, we have that $\pi^{(mk)}(x) = \Psi_n(x + k \cdot S_\pi)$ and, for $P_\pi = 1$, we have that $\pi^{(mk)}(x) = \Psi_n\left(x + k \cdot \sum_{1 \leq i \leq m} b_i\right)$.

Proof. The composition of affine functions is also affine. Since $\pi^{(m)}(x)$ is the reduction modulo n of the composition of m affine functions given by Definition 2.3, each of which has slope a_i, $\pi^{(m)}(x)$ is affine as well, with slope P_π. Therefore, the linear coefficient S_π is well-defined. In fact, by reindexing $\vec{c}$ under a cyclic shift if needed, S_π is given by

$$S_\pi = \Psi_n\left(\sum_{i=1}^{m} a_m a_{m-1} \ldots a_{i+2} a_{i+1} b_i\right). \tag{5}$$

For the remainder, we proceed by induction on k. The case $k = 1$ follows from the definition of principal sum. Suppose that

$$\pi^{(mk)}(x) = \Psi_n\left(P_\pi^k \cdot x + (P_\pi^{k-1} + \cdots + P_\pi + 1) \cdot S_\pi\right)$$

for some $k \geq 1$. Then

$$\pi^{(m(k+1))}(x) = \pi^{(mk)}(\pi^{(m)}(x)) = \pi^{(mk)}(\Psi_n(P_\pi \cdot x + S_\pi))$$
$$= \Psi_n\left(P_\pi^k \cdot (P_\pi \cdot x + S_\pi) + (P_\pi^{k-1} + \cdots + P_\pi + 1) \cdot S_\pi\right)$$
$$= \Psi_n\left(P_\pi^{k+1} \cdot x + (P_\pi^k + P_\pi^{k-1} + \cdots + P_\pi + 1) \cdot S_\pi\right),$$

from where we obtain directly the cases $P_\pi \neq 1$ and $P_\pi \equiv 1 \pmod{n}$. If $P_\pi = 1$ then $a_i = 1$ for all $1 \leq i \leq m$, which implies $S_\pi = \Psi_n\left(\sum_{1 \leq i \leq m} b_i\right)$.

$\square$

Since $\pi^{(m)}(x) \equiv x \pmod{m}$, it holds $S_\pi \equiv 0 \pmod{m}$. The previous lemma implies the following result.

Proposition 3.5. *Let π be an (n,m)-p.a.p. with principal product P_π and principal sum S_π. For any positive integer $x \in [1,n]$ divisible by m with $x = mx_0$, the length of the cycle of π containing x is given as follows:*

(i) $m \cdot \frac{n}{\gcd(n,S_\pi)}$ *if $P_\pi \equiv 1 \pmod{n}$;*

(ii) *if $P_\pi \neq 1$, this length is given by $m \cdot \mathrm{ord}_{\kappa(x)} P_\pi$, where*

$$\kappa(x) = \frac{n \cdot (P_\pi - 1)}{\gcd(n \cdot (P_\pi - 1), x \cdot (P_\pi - 1) + S_\pi)} = \frac{\frac{n}{m} \cdot (P_\pi - 1)}{g_\pi \cdot \gcd\left(\frac{n}{m} \cdot \frac{P_\pi - 1}{g_\pi}, x_0 \cdot \frac{P_\pi - 1}{g_\pi} + \frac{S_\pi}{m \cdot g_\pi}\right)}, \tag{6}$$

$$g_\pi = \gcd\left(\frac{S_\pi}{m}, P_\pi - 1\right). \tag{7}$$

Proof. (i) In this case, the cycle has length mk if and only if k is minimal such that $\pi^{(mk)}(x) = \Psi_n(x + k \cdot S_\pi) = x$, i.e., $kS_\pi \equiv 0 \pmod{n}$. It is clear that the minimal k satisfying the latter equals $\frac{n}{\gcd(n,S_\pi)}$.

(ii) In this case, $\pi^{(mk)}(x) = \Psi_n\left(P_\pi^k \cdot x + \frac{P_\pi^k - 1}{P_\pi - 1} \cdot S_\pi\right) = x$, and so we have the following equivalent conditions:

$$(P_\pi^k - 1) \cdot x + \frac{P_\pi^k - 1}{P_\pi - 1} \cdot S_\pi \equiv 0 \pmod{n},$$
$$(P_\pi^k - 1) \cdot [x \cdot (P_\pi - 1) + S_\pi] \equiv 0 \pmod{n(P_\pi - 1)},$$
$$P_\pi^k - 1 \equiv 0 \pmod{\kappa(x)}.$$

Therefore, the smallest possible $k > 0$ is $k = \mathrm{ord}_{\kappa(x)} P_\pi$ and the cycle of π containing x has length equals $m \cdot \mathrm{ord}_{\kappa(x)} P_\pi$. $\square$

The next lemma displays all the possible values of

$$N_0 = N_0(x_0) := \gcd\left(\frac{n}{m} \cdot \frac{P_\pi - 1}{g_\pi}, \; \frac{P_\pi - 1}{g_\pi} \cdot x_0 + \frac{S_\pi}{m \cdot g_\pi}\right), \tag{8}$$

and the number of solutions in each case. By Eqs. (6) and (8), we observe that

$$\kappa(x) = \frac{\frac{n}{m} \cdot (P_\pi - 1)}{g_\pi \cdot N_0}. \tag{9}$$

Lemma 3.6. *Let α, β, γ be positive integers such that $\gcd(\alpha, \beta) = 1$ and α divides γ. Write $\gamma = \gamma_1 \gamma_2$, where $\mathrm{rad}(\gamma_1)$ divides α and $\gcd(\gamma_2, \alpha) = 1$. Then the following properties hold:*

(i) *as y runs over $[1, \gamma/\alpha]$, $\gcd(\alpha y + \beta, \gamma)$ runs over all the divisors of γ_2;*

(ii) *for each divisor d of γ_2, the number of solutions $y \in [1, \gamma/\alpha]$ of the equation*

$$\gcd(\alpha y + \beta, \gamma) = \gamma_2 / d$$

is $\varphi(d) \cdot \gamma_1$.

Proof. (i) We have that α divides γ_1. Since $\gcd(\gamma_1, \gamma_2) = \gcd(\alpha, \beta) = 1$, we obtain the following equalities

$$\gcd(\alpha y + \beta, \gamma) = \gcd(\alpha y + \beta, \gamma_1 \gamma_2) = \gcd(\alpha y + \beta, \gamma_2).$$

In particular, $\gcd(\alpha y + \beta, \gamma)$ divides γ_2. Let d be a positive divisor of γ_2. In the following, we show that there exists $y \in [1, \gamma/\alpha]$ such that

$$\begin{cases} \alpha y + \beta \equiv \beta \pmod{\gamma_1} \\ \alpha y + \beta \equiv d \pmod{\gamma_2} \end{cases}$$

and this implies that $\gcd(\alpha y + \beta, \gamma_2) = d$. The first congruence is equivalent to $y = t\gamma_1/\alpha$ for some $t \in \mathbb{Z}$, and the second one is equivalent to $t\gamma_1 \equiv d - \beta \pmod{\gamma_2}$, which has a solution for $t \in [1, \gamma_2]$, so that $y \in [1, \gamma/\alpha]$.

(ii) Let $\omega \in [1, \gamma/\alpha]$ be the smallest solution of $\gcd(\alpha y + \beta, \gamma) = \gamma_2/d$. All the other solutions are of the form $\omega + j\frac{\gamma_2}{d}$ with $0 \le j < \gamma_1 d$. Since $\gcd(\alpha, \gamma_2) = \gcd(\gamma_1, \gamma_2) = 1$, the number $\omega + j\frac{\gamma_2}{d}$ is a solution as well if and only if

$$\gcd\left(\frac{\alpha\omega + \beta}{\gamma_2/d} + \alpha j, d\right) = 1 \quad \text{and} \quad 0 \le j < \gamma_1 d.$$

Therefore, the number of solutions $x_0 + j \cdot \frac{\gamma_2}{d} \in [1, \gamma/\alpha]$ of this equation is $\varphi(d) \cdot \gamma_1$. $\qquad\square$

Suppose that $P_\pi > 1$ and let $\alpha = \frac{P_\pi - 1}{g_\pi}$, $\beta = \frac{S_\pi}{m \cdot g_\pi}$ and $\gamma = \frac{n}{m} \cdot \frac{P_\pi - 1}{g_\pi} = \frac{n}{m}\alpha$ be as in Lemma 3.6. Write $\frac{n}{m} = N_1 N_2$, where $\mathrm{rad}(N_1)$ divides α and $\gcd(N_2, \alpha) = 1$. Hence the number N_0 defined by Eq. (8) can be any divisor of N_2, that is, N_0 can be any divisor of n/m that is relatively prime with $\frac{P_\pi - 1}{g_\pi}$ when x_0 runs over $[1, n/m]$. This observation and Eq. (9) easily imply the following result.

Corollary 3.7. *Fix $x = mx_0 \in [1, n]$. Let $\kappa(x)$ and N_0 be defined as in Eqs. (6) and (8), respectively. We write $\frac{n}{m} = N_1 N_2$ where $\mathrm{rad}(N_1)$ divides $\frac{P_\pi - 1}{g_\pi}$ and $\gcd\left(N_2, \frac{P_\pi - 1}{g_\pi}\right) = 1$, as above. For a divisor d of N_2 such that $N_0 = N_2/d$, we have that $\kappa(x) = N_1 \cdot \frac{P_\pi - 1}{g_\pi} \cdot d$. In addition, the equation $N_0 = N_2/d$ has exactly $\varphi(d) \cdot N_1$ solutions x with $x_0 \in [1, n/m]$.*

Finally, we exhibit the cycle decomposition of an arbitrary (n, m)-p.a.p. π with principal product $P_\pi \ne 1$ (the case $P_\pi \equiv 1 \pmod{n}$ follows trivially by item (i) of Proposition 3.5). In what follows, $\mathrm{Cyc}(r)$ denotes a cycle of length r. Moreover, $G_1 \oplus G_2$ denotes the disjoint union of the graphs G_1 and G_2, $\bigoplus_{\ell \in \Lambda} G_\ell$ denotes the disjoint union of the graphs G_ℓ for $\ell \in \Lambda$ and, for a positive integer k, $k \times G = \bigoplus_{1 \le i \le k} G$.

Theorem 3.8. *Let π be an (n, m)-p.a.p. with principal product $P_\pi > 1$ and principal sum S_π. Let g_π be defined as in Eq. (7) and write $n/m = N_1 N_2$, where $\mathrm{rad}(N_1)$ divides $\frac{P_\pi - 1}{g_\pi}$ and $\gcd\left(\frac{P_\pi - 1}{g_\pi}, N_2\right) = 1$. For each divisor d of N_2, set $\eta(d) = N_1 \cdot \frac{P_\pi - 1}{g_\pi} \cdot d$. Then the cycle decomposition of π is given by*

$$\bigoplus_{d | N_2} \frac{\varphi(d) \cdot N_1}{\mathrm{ord}_{\eta(d)} P_\pi} \times \mathrm{Cyc}\left(m \cdot \mathrm{ord}_{\eta(d)} P_\pi\right),$$

Proof. For each divisor d of N_2, let n_d be the number of cycles of π containing an element $x = mx_0 \in [1, n]$ such that the number $N_0 = N_0(x_0)$ defined by Eq. (8) satisfies

$$N_0 = N_2/d.$$

Since every element of $[1, n]$ belongs to a unique cycle, Proposition 3.5 and Corollary 3.7 yield

$$\sum_{d | N_2} n_d \cdot m \cdot \mathrm{ord}_{\eta(d)} P_\pi = n.$$

We claim that $n_d \cdot \mathrm{ord}_{\eta(d)} P_\pi \ge \varphi(d) \cdot N_1$. In fact, by Corollary 3.7, for $x = mx_0$ the equality $N_0(x_0) = N_2/d$ implies that

$$\kappa(x) = N_1 \cdot \frac{P_\pi - 1}{g_\pi} \cdot d = \eta(d),$$

where $\kappa(x)$ is given by Eq. (6). From the same corollary, the latter has exactly $\varphi(d)N_1$ solutions $x = mx_0 \in [1, n]$. Since there exist at most $\mathrm{ord}_{\eta(d)} P_\pi$ of such $x = mx_0$ in a same cycle of length $m \cdot \mathrm{ord}_{\eta(d)} P_\pi$ of π, it follows that $n_d \ge \frac{\varphi(d)N_1}{\mathrm{ord}_{\eta(d)} P_\pi}$, proving the claim. Therefore, we obtain the following inequalities

$$\frac{n}{m} = \sum_{d | N_2} n_d \cdot \mathrm{ord}_{\eta(d)} P_\pi \ge \sum_{d | N_2} \varphi(d) \cdot N_1 = N_1 \sum_{d | N_2} \varphi(d) = N_1 N_2 = \frac{n}{m},$$

9

forcing that $n_d = \dfrac{\varphi(d)N_1}{\operatorname{ord}_{\eta(d)} P_\pi}$.

$\square$

Example 3.9. *Let π be the $(12,3)$-p.a.p. given in Example 2.4. We have that $P_\pi = 15$ and $S_\pi = 9$, and in the notation of Theorem 3.8, $g_\pi = 1$ and $N_1 = 4$, $N_2 = 1$. From Theorem 3.8, the cycle decomposition of π is given by*

$$\frac{4}{\operatorname{ord}_{56}15} \times \operatorname{Cyc}(3 \cdot \operatorname{ord}_{56}15) = 2 \times \operatorname{Cyc}(6),$$

as confirmed by Example 2.4.

4. Application: permutation polynomials over finite fields

Throughout this section, we fix q a prime power and let $\mathbb{F}_q$ denote the finite field with q elements. We observe that, for a divisor $m > 1$ of $q - 1$, we may construct many $(q - 1, m)$-p.a.p.'s. It turns out that such permutations extend to permutations of the finite field $\mathbb{F}_q$. Let $\theta_q \in \mathbb{F}_q$ be a *primitive element*, i.e. a generator of the multiplicative group $\mathbb{F}_q^*$. If $m > 1$ divides $q - 1$ and π is any $(q - 1, m)$-p.a.p., we define its θ_q-*lift* as the permutation $F_{\pi,\theta_q} : \mathbb{F}_q \to \mathbb{F}_q$ given by

$$\begin{cases} F_{\pi,\theta_q}(0) &= 0 \qquad \text{and} \\ F_{\pi,\theta_q}(\theta_q^i) &= \theta_q^{\pi(i)} \qquad \text{for any } 1 \le i \le q - 1. \end{cases}$$

Of course, F_{π,θ_q} is a permutation of the finite field $\mathbb{F}_q$. We observe that, by construction, such permutation defines a piecewise monomial function on m-*cyclotomic cosets* of $\mathbb{F}_q^*$. In other words, if $\mathcal{D}_m \subset \mathbb{F}_q^*$ denotes the subgroup of perfect m-th powers, the restriction of $F_{\pi,\theta_q}(x)$ to each coset of $\mathbb{F}_q^*/\mathcal{D}_m$ is ruled by a monomial map αx^β.

Remark 4.1. *We emphasize that functions defined by different monomials on cyclotomic cosets of $\mathbb{F}_q^*$ were previously studied in full generality: see Theorem 2 of [15]. Our aim here is to apply our $(q-1, m)$-p.a.p.'s in the construction of permutation polynomials where the cycle decomposition and the inverse can be obtained.*

We want to find a polynomial representation for F_{π,θ_q}. Let $(\vec{a}, \vec{b}, \vec{c})$ be the parameters of π with $\vec{a} = (a_1, \ldots, a_m)$, $\vec{b} = (b_1, \ldots, b_m)$ and $\vec{c} = (c_1, \ldots, c_m)$. In particular, if $x = \theta_q^j$ with $j \equiv c_i \pmod{m}$, then

$$F_{\pi,\theta_q}(x) = \theta_q^{b_i} \cdot x^{a_i}.$$

Therefore, we only need to find a characteristic function for the elements $x = \theta_q^j$ with $j \equiv c_i \pmod{m}$. We have the following definition.

Definition 4.2. *For each divisor m of $q - 1$, set $E_m(x) = \displaystyle\sum_{j=0}^{m-1} x^{\frac{(q-1)j}{m}} \in \mathbb{F}_q[x]$.*

We observe that if $z \in \mathbb{F}_q^*$ then

$$E_m(z) = \begin{cases} m & \text{if } z^{\frac{q-1}{m}} = 1, \\ 0 & \text{otherwise.} \end{cases}$$

In particular, for each $j \in [1, m]$ we have that

$$E_m(z \cdot \theta_q^{-j}) = \begin{cases} m & \text{if } z = \theta_q^i \text{ with } i \equiv j \pmod{m}, \\ 0 & \text{otherwise.} \end{cases} \tag{10}$$

The following theorem provides a polynomial representation for F_{π,θ_q} and its inverse.

10

Theorem 4.3. *Let q be a prime power, $\theta_q \in \mathbb{F}_q$ be a primitive element and $m > 1$ be a divisor of $q-1$. If π is a $(q-1, m)$-p.a.p. with parameters $(\vec{a}, \vec{b}, \vec{c})$, then the θ_q-lift F_{π, θ_q} of π admits the following polynomial representation*

$$F_{\pi, \theta_q}(x) = \frac{1}{m} \sum_{i=1}^{m} \theta_q^{b_i} \cdot x^{a_i} E_m(x \cdot \theta_q^{-c_i}) \in \mathbb{F}_q[x].$$

In particular, this polynomial representation has at most m^2 nonzero coefficients. Moreover, if the $(q-1, m)$-p.a.p. π^{-1} is the inverse of π with parameters $(\vec{A}, \vec{B}, \vec{C})$ as in Theorem 2.7, then the inverse of F_{π, θ_q} over $\mathbb{F}_q$ is the following permutation polynomial

$$F_{\pi^{-1}, \theta_q}(x) = \frac{1}{m} \sum_{i=1}^{m} \theta_q^{B_i} \cdot x^{A_i} E_m(x \cdot \theta_q^{-C_i}) \in \mathbb{F}_q[x].$$

Proof. Since π is a $(q-1, m)$-p.a.p. with parameters $(\vec{a}, \vec{b}, \vec{c})$, we have that the function given by $F_{\pi, \theta_q}(0) = 0$ and $F_{\pi, \theta_q}(y) = \theta_q^{a_i j + b_i} = \theta_q^{b_i} y^{a_i}$ if $y = \theta_q^j$ with $j \equiv c_i \pmod{m}$, permutes $\mathbb{F}_q$. Since $E_m(x)/m$ acts as the characteristic function for the set of perfect m-th powers in $\mathbb{F}_q^*$, Eq. (10) entails that if $y = \theta_q^j$ with $j \equiv c_i \pmod{m}$, then

$$F_{\pi, \theta_q}(y) = \frac{1}{m} \sum_{i=1}^{m} \theta_q^{a_i j + b_i} E_m(y \cdot \theta_q^{-c_i}),$$

from where the polynomial expression for F_{π, θ_q} follows. The polynomial expression for the inverse of F_{π, θ_q} follows directly from the fact that the inverse π^{-1} of π is again a $(q-1, m)$-p.a.p. and that F_{π, θ_q} fixes $0 \in \mathbb{F}_q$. ∎

Remark 4.4. *We observe that if π and π_0 are two $(q-1, m)$-p.a.p.'s coming from $(q-1, m)$-equivalent $(q-1, m)$-admissible triples, their θ_q-lift coincide as permutations of $\mathbb{F}_q$. However, the polynomials F_{π, θ_q} and F_{π_0, θ_q} may not coincide and we can only guarantee that*

$$F_{\pi, \theta_q}(x) \equiv F_{\pi_0, \theta_q}(x) \pmod{x^q - x}.$$

When π is 2-reduced, the following corollary entails that the polynomial representation of F_{π, θ_q} and its inverse are quite simple. Its proof is a direct application of the previous theorem so we omit details.

Corollary 4.5. *Let q be a prime power, $\theta_q \in \mathbb{F}_q$ be a primitive element and $m > 1$ be a divisor of $q - 1$. If π is a 2-reducible $(q-1, m)$-p.a.p. with reduced parameters (a_0, a, b_0, b) and π^{-1} is its inverse, then the θ_q-lift F_{π, θ_q} of π admits the following polynomial representation*

$$F_{\pi, \theta_q}(x) = x^a \theta_q^b + \left(\frac{x^{a_0} \theta_q^{b_0} - x^a \theta_q^b}{m} \right) E_m(x) \in \mathbb{F}_q[x],$$

whose inverse F_{π^{-1}, θ_q} is given by

$$F_{\pi^{-1}, \theta_q}(x) = x^A \theta_q^B + \left(\frac{x^{A_0} \theta_q^{B_0} - x^A \theta_q^B}{m} \right) E_m(x \cdot \theta_q^{-b}) \in \mathbb{F}_q[x],$$

where A_0, A, B_0, B are defined in Proposition 2.12. In particular, these polynomial representations have at most $2m$ nonzero coefficients.

4.1. On the cycle decomposition

We observe that the cycle decomposition of the permutation polynomials given in Theorem 4.3 can be explicitly computed. In fact, for a given $(q-1, m)$-p.a.p. π with parameters $(\vec{a}, \vec{b}, \vec{c})$, we can compute its principal sum and product. In particular, the cycle decomposition of π is explicitly obtained from

Theorem 3.8. Moreover, for a fixed primitive element $\theta_q \in \mathbb{F}_q$, the cycle decomposition of the θ_q-lift permutation F_{π,θ_q} is obtained by the one of π, adding a loop that corresponds to the fixed point $0 \in \mathbb{F}_q$. Furthermore, F_{π,θ_q} and its inverse F_{π^{-1},θ_q} have the same cycle decomposition. We provide two examples of these facts.

Example 4.6. *Let $q = 13$ and let π be the $(12,3)$-p.a.p. given in Example 2.4. Applying Theorem 4.3 with $\theta_{13} = 2$, we obtain the permutation polynomial*

$$F_{\pi,2}(x) = 10x^{11} + 8x^9 + 12x^7 + x^5 + 4x^3 + 6x \in \mathbb{F}_{13}[x].$$

The inverse π^{-1} of π is given in Example 2.8, whence we obtain the polynomial representation for the inverse of $F_{\pi,2}$:

$$F_{\pi^{-1},2}(x) = 10x^{11} + 8x^9 + 10x^7 + 4x^5 + 10x^3 + x.$$

The cycle decomposition of $F_{\pi,2}$ (and of $F_{\pi^{-1},2}$) is given by $\mathrm{Cyc}(1) \oplus (2 \times \mathrm{Cyc}(6))$ (see also Example 3.9).

Example 4.7. *Let $q = 25$ and let π be the 2-reducible $(24,3)$-p.a.p. with reduced parameters $(5,7,2,8)$ so that*

$$\pi(x) = \begin{cases} \Psi_{24}(5x + 2) & if \quad x \equiv 0 \pmod 3, \\ \Psi_{24}(7x + 8) & otherwise. \end{cases}$$

Its inverse π^{-1} is given by

$$\pi^{-1}(x) = \begin{cases} \Psi_{25}(5x + 14) & if \quad x \equiv 2 \pmod 3, \\ \Psi_{25}(7x + 16) & otherwise. \end{cases}$$

The principal product of π equals $P_\pi = 245$ and its principal sum equals $S_\pi = 18$. In the notation of Theorem 3.8, we have that $g_\pi = 2$ and $N_1 = 8$, $N_2 = 1$. From Theorem 3.8, the cycle decomposition of π is given by

$$\frac{8}{\mathrm{ord}_{122.8}245} \times \mathrm{Cyc}(3 \cdot \mathrm{ord}_{122.8}245) = 2 \times \mathrm{Cyc}(12).$$

Let $\mathbb{F}_{25} = \mathbb{F}_5(\alpha)$, where $\alpha^2 - \alpha - 3 = 0$, so that α is a primitive element. In particular, the α-lift of π is

$$F_{\pi,\alpha}(x) = x^7\alpha^8 + \left(\frac{x^5\alpha^2 - x^7\alpha^8}{3}\right)E_3(x)$$
$$= (\alpha + 3)(x^{23} + x^{15}) + (2\alpha + 1)(x^{21} + x^{13} - x^7 + x^5),$$

over $\mathbb{F}_{25}$, whose inverse is

$$F_{\pi^{-1},\alpha}(x) = x^7\alpha^{16} + \left(\frac{x^5\alpha^{14} - x^7\alpha^{16}}{3}\right)E_3(x \cdot \alpha^{-8})$$
$$= (\alpha + 3)x^{23} + 4x^{21} + 3x^{15} + (2\alpha + 2)(x^{13} + x^7) + (3\alpha + 4)x^5.$$

The cycle decomposition of $F_{\pi,\alpha}$ (and of $F_{\pi^{-1},\alpha}$) is $\mathrm{Cyc}(1) \oplus (2 \times \mathrm{Cyc}(12))$.

4.1.1. Permutations yielding cycles of the same length
Here we characterize the $(q-1,m)$-p.a.p.'s π with the property that its cycles are of the same length ℓ, a prime number. This is a nice application of Theorem 3.8 and is stated as follows.

Proposition 4.8. *Let ℓ be a prime number, q be a prime power, $\theta_q \in \mathbb{F}_q$ be a primitive element and m be a divisor of $q - 1$. If π is a $(q-1,m)$-p.a.p. with principal product P_π and principal sum S_π, then the θ_q-lift F_{π,θ_q} of π decomposes into cycles of length ℓ if and only if the following properties hold:*

  (i) *$\ell = m$;*
  (ii) *$P_\pi \equiv 1 \pmod{\frac{q-1}{m}}$;*

(iii) $S_\pi \equiv 0 \pmod{q - 1}$.

In this case, if π^{-1} denotes the inverse π, F_{π, θ_q} and F_{π^{-1}, θ_q} have polynomial representations given by Theorem 4.3, and the cycle decomposition of F_{π, θ_q} (and of F_{π^{-1}, θ_q}) over $\mathbb{F}_q$ equals

$$\mathrm{Cyc}(1) \oplus \left(\frac{q - 1}{m} \times \mathrm{Cyc}(m) \right).$$

Proof. From construction, any $(q - 1, m)$-p.a.p. decomposes into cycles of length divisible by m, forcing that $m = \ell$. Since $\mathrm{ord}_b a$ divides $\mathrm{ord}_c a$ whenever $\gcd(bc, a) = 1$ and b divides c, Theorem 3.8 entails that π has only cycles of length m if and only if $P_\pi - 1$ is divisible by

$$\frac{(q - 1)(P_\pi - 1)}{m g_\pi},$$

where $g_\pi = \gcd\left(\frac{S_\pi}{m}, P_\pi - 1 \right)$. The latter is equivalent to $g_\pi \equiv 0 \pmod{\frac{q-1}{m}}$, i.e., $S_\pi \equiv 0 \pmod{q - 1}$ and $P_\pi \equiv 1 \pmod{\frac{q-1}{m}}$. $\qquad\square$

In particular, it is possible to obtain involutions from $(q - 1, 2)$-p.a.p.'s. Involutions over finite fields are frequently used in cryptographic applications. More specifically, they are used as S-boxes, a basic component in key-algorithms used to cover the relation between the key and the encrypted message. We observe that if P is an involution over $\mathbb{F}_q$, then any element $a \in \mathbb{F}_q$ either belongs to a cycle of length two or is a fixed point, i.e., $P(a) = a$. There are some cryptographic attacks that explore the number of fixed points of a permutation and according to [4], for secure implementations, involutions should have few fixed points. In the particular case $m = 2$ of Proposition 4.8, the θ_q-lift $F_{\theta_q, \pi}$ recover a family of involutions that were previously obtained in [14]. This is presented in the following corollary, which is just a straightforward application of the previous proposition. We omit details.

Corollary 4.9. *Let $q \equiv 3 \pmod 4$ be a prime power and let $\theta_q \in \mathbb{F}_q$ be a primitive element. If π is a $(q-1, 2)$-p.a.p. with parameters $\vec{a} = (a_0, a)$, $\vec{b} = (b_0, b)$ and $\vec{c} = (2, 1)$, then its θ_q-lift $F_{\theta_q, \pi}$ is an involution if and only if $a_0 a \equiv 1 \pmod{\frac{q-1}{2}}$ and $b_0 a + b \equiv 1 \pmod{q - 1}$. In this case, the cycle decomposition of F_{π, θ_q} over $\mathbb{F}_q$ is given by $\mathrm{Cyc}(1) \oplus \left(\frac{q-1}{2} \times \mathrm{Cyc}(2) \right)$, and so it has only one fixed point. Moreover, in this case, F_{π, θ_q} has the following polynomial representation*

$$F_{\pi, \theta_q}(x) = \theta_q^{b_0} \cdot \frac{x^{\frac{q-1}{2} + a_0} + x^{a_0}}{2} + \theta_q^b \cdot \frac{x^a - x^{\frac{q-1}{2} + a}}{2}.$$

Example 4.10. *Let $q = 27$ and let π be the 2-reducible $(26, 2)$-p.a.p. with reduced parameters $(5, 8, 3, 2)$ so that*

$$\pi(x) = \begin{cases} \Psi_{26}(5x + 3) & \text{if } x \text{ is even,} \\ \Psi_{26}(8x + 2) & \text{if } x \text{ is odd.} \end{cases}$$

Let $\mathbb{F}_{27} = \mathbb{F}_3(\alpha)$ where $\alpha^3 - \alpha - 2 = 0$, so α is a primitive element. In particular, the α-lift of π yields the involution

$$F_{\pi, \alpha}(x) = \alpha^3 \left(\frac{x^{18} + x^5}{2} \right) + \alpha^2 \left(\frac{x^8 - x^{21}}{2} \right)$$
$$= \alpha^2 (x^{21} - x^8) - (\alpha + 2)(x^{18} + x^5),$$

over $\mathbb{F}_{27}$, whose cycle decomposition is $\mathrm{Cyc}(1) \oplus (13 \times \mathrm{Cyc}(2))$.

4.2. More explicit results

We observe that Theorem 4.3 provides classes of permutation polynomials over $\mathbb{F}_q$, that depend on a primitive element $\theta_q \in \mathbb{F}_q$. If q is large, it can be hard to find such a θ_q. Here we consider special cases where such permutation polynomials can be obtained without going through a primitive element of $\mathbb{F}_q$. Instead, we only need certain primitive roots of unity in the base field $\mathbb{F}_p$ of $\mathbb{F}_q$. This is done in the following proposition.

Proposition 4.11. *Let p be a prime and m, k be positive integers such that m divides $p - 1$. Write $p^k - 1 = n_1 n_2$, where $\mathrm{rad}(n_1)$ divides $\frac{p^k-1}{m}$ and $\gcd\left(n_2, \frac{p^k-1}{m}\right) = 1$. Let $\theta \in \mathbb{F}_p$ be any primitive m-th root of unity, write $q = p^k$ and let a, a_0 be positive integers such that $\gcd(aa_0, n_1) = 1$ and $a \equiv 1 \pmod{\mathrm{rad}_2(m)}$. Then, for any positive integer $b < m$ such that $\gcd(b, m) = 1$,*

$$F_{a_0,a,b}(x) = \theta^b \left(\frac{1}{m} E_m(x) \cdot x^{a_0} + \left(1 - \frac{1}{m} E_m(x)\right) \cdot x^a \right)$$

is a permutation polynomial over $\mathbb{F}_q$. Set $g = \gcd\left(\frac{q-1}{m}, a_0 a^{m-1} - 1\right)$ and write $\frac{q-1}{m} = N_1 N_2$, where $\mathrm{rad}(N_1)$ divides $\frac{a_0 a^{m-1}-1}{g}$ and $\gcd\left(\frac{a_0 a^{m-1}-1}{g}, N_2\right) = 1$. Then the cycle decomposition of the permutation polynomial $F_{a_0,a,b}$ over $\mathbb{F}_q$ is given by

$$\mathrm{Cyc}(1) \oplus \left(\bigoplus_{d \mid N_2} \frac{\varphi(d) \cdot N_1}{\mathrm{ord}_{\eta(d)}(a_0 a^{m-1})} \times \mathrm{Cyc}\left(m \cdot \mathrm{ord}_{\eta(d)}(a_0 a^{m-1})\right) \right), \tag{11}$$

where $\eta(d) = N_1 \cdot \frac{a_0 a^{m-1}-1}{g} \cdot d$.

Proof. From construction and Proposition 2.12, (a_0, a, B, B) are the reduced parameters of a $(q - 1, m)$-p.a.p., where $B = \frac{b(q-1)}{m}$. Therefore, as θ_q runs over the primitive elements of $\mathbb{F}_q$, $\theta_q^{\frac{q-1}{m}}$ runs over the primitive m-th roots of unity in $\mathbb{F}_p$. In particular, the fact that $F_{a_0,a,b}(x)$ permutes $\mathbb{F}_q$ follows from Theorem 4.3. Let π be the $(q - 1, m)$-p.a.p. with reduced parameters (a_0, a, B, B) where B is as before. Therefore, π has principal product $P_\pi = a_0 a^{m-1}$ and principal sum $S_\pi = q - 1$. In particular, Eq. (11) follows from Theorem 3.8. $\qquad\square$

Some cases of the previous proposition readily yield explicit results.

Corollary 4.12. *Let q be a prime power such that $q \equiv 3 \pmod 4$ and let a, a_0 be positive integers such that $\gcd\left(aa_0, \frac{q-1}{2}\right) = 1$ and $a \equiv 1 \pmod 4$. Then*

$$P_{a_0,a}(x) = -\frac{x^{\frac{q-1}{2}} + 1}{2} \cdot x^{a_0} + \frac{x^{\frac{q-1}{2}} - 1}{2} \cdot x^a,$$

is a permutation polynomial over $\mathbb{F}_q$ with cycle decomposition given by Eq. (11).

Corollary 4.13. *Let $q = 7^k$ with $\gcd(k, 3) = 1$ and let a, a_0 be positive integers such that $\gcd\left(aa_0, \frac{q-1}{3}\right) = 1$ and $a \equiv 1 \pmod 3$. Then for $j = 1, 2$,*

$$P_{a_0,a,j}(x) = 2^j \left(\frac{1 + x^{\frac{q-1}{3}} + x^{\frac{2(q-1)}{3}}}{3} \cdot x^{a_0} + \left(1 - \frac{1 + x^{\frac{q-1}{3}} + x^{\frac{2(q-1)}{3}}}{3}\right) \cdot x^a \right),$$

is a permutation polynomial over $\mathbb{F}_q$ with cycle decomposition given by Eq. (11).

References

[1] S. Ahmad, Cycle structure of automorphisms of finite cyclic groups, *J. Comb. Theory* **6** (1969), 370-374.

[2] A. Akbary, D. Ghioca, Q. Wang, On constructing permutations of finite fields, *Finite Fields Appl.* **17** (2011), 51-67.

[3] D. Bartoli, M. Giulietti, L. Quoos, G. Zini, Complete permutation polynomials from exceptional polynomials, *J. Number Theory* **176** (2017), 46-66.

[4] C. Boura, A. Canteaut, L.R. Knudsen et al., Reflection Ciphers, *Des. Codes Cryptogr.* **82** (2017), 3-25.

[5] X. Cao, L. Hu, Z. Zha, Constructing permutation polynomials from piecewise permutations, *Finite Fields Appl.* **26** (2014), 162-174.

[6] A. Çeşmelioğlu, W. Meidl, A. Topuzoğlu, On the cycle structure of permutation polynomials, *Finite Fields Appl.* **14** (2008), 593-614.

[7] N. Fernando, X.-d. Hou, A piecewise construction of permutation polynomials over finite fields, *Finite Fields Appl.* **18** (2012), 1184-1194.

[8] X.-d. Hou, Permutation polynomials over finite fields - A survey of recent advances, *Finite Fields Appl.* **32** (2015), 82-119.

[9] G.M. Kyureghyan, Constructing permutations of finite fields via linear translators, *J. Comb. Theory Ser. A* **118** (2011), 1052-1061.

[10] R. Lidl, G.L. Mullen, Cycle structure of Dickson permutation polynomials, *Math. J. Okayama Univ.* **33** (1991), 1-11.

[11] G.L. Mullen, T.P. Vaughan, Cycles of linear permutations over a finite field, *Linear Algebra Appl.* **108** (1988), 63-82.

[12] G.L. Mullen, D. Panario, Handbook of Finite Fields, *Boca Raton: Taylor and Francis* (2013).

[13] D. Panario, L. Reis, The functional graph of linear maps over finite fields and applications *Des. Codes Cryptogr.* **87** (2019), 437-453.

[14] Q. Wang, A note on inverses of cyclotomic mapping permutation polynomials over finite fields, *Finite Fields Appl.* **45** (2017), 422-427.

[15] Q. Wang, Cyclotomy and permutation polynomials of large indices, *Finite Fields Appl.* **22** (2013), 57-69.