Coset-wise affine functions and cycle types of complete mappings

Alexander Bors\textsuperscript{1} \hspace{1em} Qiang Wang\textsuperscript{1}

September 10, 2021

Abstract

Let $K$ be a finite field of characteristic $p$. We study a certain class of functions $K \rightarrow K$ that agree with an $\mathbb{F}_p$-affine function $K \rightarrow K$ on each coset of a given additive subgroup $W$ of $K$ – we call them $W$-coset-wise $\mathbb{F}_p$-affine functions of $K$. We show that these functions form a permutation group on $K$ with the structure of an imprimitive wreath product and characterize which of them are complete mappings of $K$. As a consequence, we are able to provide various new examples of cycle types of complete mappings of $K$, including that $K$ has a complete mapping moving all elements of $K$ in one cycle if $p > 2$.

1 Introduction

1.1 Background and main results

Let $(G, +)$ be an additive (but not necessarily abelian) group. A complete mapping of $G$ is a permutation $f$ of $G$ such that the function $f + \text{id} : G \rightarrow G, g \mapsto f(g) + g$, is also a permutation of $G$. A complete mapping of a field $K$ is just a complete mapping of the underlying additive group of $K$. See Evans’ book \cite{6} for a concise introduction to the theory of complete mappings.

The study of complete mappings has a long and rich history and has been spurred by their various applications. Originally, complete mappings were introduced by Mann in 1942 as a tool in constructing mutually orthogonal Latin squares \cite{10}. The question of which groups admit complete mappings, which comprises the celebrated

\textsuperscript{1}School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa ON K1S 5B6, Canada.

First author’s e-mail: alexanderbors@cunet.carleton.ca

Second author’s e-mail: wang@math.carleton.ca

The authors are supported by the Natural Sciences and Engineering Research Council of Canada (RGPIN-2017-06410).

2020 Mathematics Subject Classification: Primary: 12E20. Secondary: 11T06, 15A21, 20B05.

Keywords and phrases: Finite field, Complete mapping, Cycle type, Cycle structure, Wreath product.
**Hall-Paige Conjecture**, was heavily studied and finally answered completely by group theorists – in chronological order, this involved the work of Bateman [1], Hall-Paige [13], Wilcox [28], Evans [7], and Bray [3, Section 2]. A unified proof of this conjecture can be found in Evans’ book [8], an expansion of his other book [6] cited earlier.

An important and heavily studied special case are complete mappings of finite fields (or, equivalently, of finite elementary abelian groups), whose polynomial representations have been investigated extensively. An influential early work in this regard is Niederreiter-Robinson’s 1984 paper [20]. This paper came before the various practical applications of complete mappings were discovered, for example in check-digit systems [23, 24] and the construction of cryptographic functions [19, 25]. These applications spurred even greater interest in complete mappings, see e.g. [14, 26, 29, 30, 32, 33].

Recall that every permutation \( \sigma \) of a finite set \( \Omega \) decomposes into pairwise disjoint cycles. The **cycle type** of \( \sigma \), which we will denote by \( \text{CT}(\sigma) \) in this paper, is the unique monomial

\[
x_1^{k_1}x_2^{k_2} \cdots x_{|\Omega|}^{k_{|\Omega|}} \in \mathbb{Q}[x_n : n \geq 1]
\]

where \( k_\ell \) is the number of length \( \ell \) cycles of \( \sigma \) for \( \ell = 1, 2, \ldots, |\Omega| \). Hence, \( \text{CT}(\sigma) \) encodes the information how many cycles of each given length \( \sigma \) has.

Although complete mappings of finite fields have been heavily studied, it is still not well understood which cycle types can be achieved by them. The following two elementary facts are known:

1. A complete mapping \( f \) of an abelian group \( G \) cannot have a 2-cycle. Indeed, if \((x, f(x)) \) is a 2-cycle of \( f \), then \((f + \text{id})(x) = f(x) + x = x + f(x) = f(f(x)) + f(x) = (f + \text{id})(f(x))\), contradicting the injectivity of \( f + \text{id} \).

2. An orthomorphism of an additive group \( G \) is a permutation \( f \) of \( G \) such that \( f - \text{id} : G \to G, g \mapsto f(g) - g \), is also a permutation of \( G \). Because a fixed point of \( f \) is the same as a pre-image of the neutral element \( 0_G \) under \( f - \text{id} \), each orthomorphism of an arbitrary group has precisely one fixed point. Note that if \( G \) has exponent 2 (which happens precisely when \( G \) is the underlying additive group of a field of characteristic 2), then complete mappings of \( G \) are the same as orthomorphisms of \( G \), and so complete mappings of \( G \) must have precisely one fixed point then.

Note that these conditions allow one to refute certain cycle types as possible for complete mappings of a finite field \( \mathbb{F}_q \). On the other hand, we also have some knowledge of cycle types that are possible:

1. A complete mapping (or orthomorphism) of cycle type \( x_1^{k_1}x_2^{k_2} \cdots x_{|\Omega|}^{k_{|\Omega|}} \) is called \( \ell \)-regular (see [9], whence this terminology apparently originated). Because a scalar multiplication \( \mathbb{F}_q \to \mathbb{F}_q, x \mapsto ax \) for fixed \( a \in \mathbb{F}_q \), is a complete mapping of \( \mathbb{F}_q \) if and only if \( a \notin \{0, -1\} \), we see that \( \ell \)-regular complete mappings of \( \mathbb{F}_q \) exist for every divisor \( \ell \) of \( q - 1 \) such that

\[
\ell \neq \begin{cases} 2, & \text{if } 2 \nmid q, \\ 1, & \text{if } 2 \mid q. \end{cases}
\]
A. Bors and Q. Wang

Cosets and complete mappings

Other examples of ℓ-regular complete mappings have been studied by various authors, see [5, 12, 17, 18, 21, 31].

(2) In their earlier paper [2], the authors derived existence results for cycle types of complete mappings of \( F_q \) that are generalized cyclotomic mappings of \( F_q \) — functions which fix 0 and restrict to a monomial function \( x \mapsto a_i x^{r_i} \) on each coset \( C_i \) of a fixed subgroup \( C \) of \( F_q^* \).

(3) Over a finite field of characteristic \( p > 2 \), complete mappings need not have any fixed points. A trivial example for this are the functions \( \mathbb{F}_q \to \mathbb{F}_q, x \mapsto x + c \) with \( c \in \mathbb{F}_q^* \) fixed, which have cycle type \( x_p^{q/p} \). For a less trivial class of examples, see [19, Theorem 9].

Our goal in this paper is to study an additive analogue of the multiplicative approach of [2]. That is, we will consider the following notion of a function that is defined via additive cosets:

**Definition 1.1.** Let \( K \) be a field, let \( V \) be a \( K \)-vector space, and let \( W \) be a \( K \)-subspace of \( V \). A function \( f : V \to V \) is called \( W \)-coset-wise \( K \)-affine if for each coset \( C \) of \( W \) in \( V \), there is a vector \( v_C \in V \) and an endomorphism \( \varphi_C \in \text{End}(V) \) with \( \varphi_C(W) \subseteq W \) such that for all \( x \in C \), one has \( f(x) = \varphi_C(x) + v_C \).

In our application, we will have \( V = \mathbb{F}_q = \mathbb{F}_q^d \) and \( K = \mathbb{F}_q \), but it is more convenient to discuss the problem in terms of vector spaces (rather than fields). Our main result, Theorem 1.3 below, is a means of obtaining the existence of cycle types of complete mappings of finite-dimensional \( \mathbb{F}_q \)-vector spaces from known cycle types of complete mappings on \( \mathbb{F}_p \)-vector spaces of smaller dimension. Before we formulate it, we introduce a bit of notation:

**Notation 1.2.** We introduce the following pieces of notation:

(1) If \( X \) is a set of permutations of a given finite set \( \Omega \), then we set

\[
\text{CT}(X) := \{ \text{CT}(\sigma) : \sigma \in X \}.
\]

(2) Let \( \ell \) be a positive integer. The \( \ell \)-blow-up function is the unique \( \mathbb{Q} \)-algebra endomorphism \( \text{BU}_\ell \) of \( \mathbb{Q}[x_n : n \geq 1] \) such that \( \text{BU}_\ell(x_n) = x_{\ell n} \) for all \( n \in \mathbb{N}^+ \).

(3) Let \( d \) be a positive integer and \( q \) be a prime power.

(a) Recall that \( \text{GL}_d(q) \) denotes the group of invertible \((d \times d)\)-matrices over \( \mathbb{F}_q \).

(b) If \( M \) is a \((d \times d)\)-matrix over \( \mathbb{F}_q \) and \( v \in \mathbb{F}_q^d \) a row vector, then the function \( \lambda(M, v) : \mathbb{F}_q^d \to \mathbb{F}_q^d, x \mapsto xM + v \), is called an \( \mathbb{F}_q \)-affine map of \( \mathbb{F}_q^d \). An \( \mathbb{F}_q \)-affine map \( \lambda(M, v) \) is a permutation of \( \mathbb{F}_q^d \) if and only if \( M \) is invertible, and the \( \mathbb{F}_q \)-affine maps that are permutations form a permutation group on \( \mathbb{F}_q^d \) denoted by \( \text{AGL}_d(q) \).

(c) We denote by \( \text{CGL}_d(q) \) the set of all matrices \( A \in \text{GL}_d(q) \) that do not have \(-1\) as an eigenvalue (equivalently, that represent an \( \mathbb{F}_q \)-linear complete mapping of \( \mathbb{F}_q^d \)).

(d) We set \( \text{ACGL}_d(q) := \{ \lambda(A, v) : A \in \text{CGL}_d(q), v \in \mathbb{F}_q^d \} \subseteq \text{AGL}_d(q) \).

3
4. Let $p$ be a prime, and let $d$ and $\ell$ be positive integers. We set

$$
\Gamma(d, p, \ell) := \begin{cases} 
\text{CT}(\text{ACGL}_d(p)), & \text{if } \ell = 1, \\
\text{CT}(\text{AGL}_d(p)), & \text{if } \ell \geq 2 \text{ and } (d, p) \neq (1, 2), (1, 3), (2, 2), \\
\{x_1^3, x_3\}, & \text{if } \ell \geq 2 \text{ and } (d, p) = (1, 3), \\
\{x_1^4, x_2^2, x_1 x_3\}, & \text{if } \ell \geq 2 \text{ and } (d, p) = (2, 2).
\end{cases}
$$

Section 2 of this paper contains information on the cycle types of $\mathbb{F}_q$-affine permutations of $\mathbb{F}_q^d$. In principle, it is possible to compute the sets $\text{CT}(\text{AGL}_d(q))$ and $\text{CT}(\text{ACGL}_d(q))$ for each pair $(d, q)$ from this.

We are now ready to formulate the main result of this paper:

**Theorem 1.3.** Let $p$ be a prime, and let $d$ and $t$ be positive integers. Assume that $x_1^{k_1} x_2^{k_2} \cdots x_p^{k_t}$ is the cycle type of a complete mapping of $\mathbb{F}_p^t$. For $\ell = 1, 2, \ldots, p^t$ and $i = 1, 2, \ldots, k_\ell$, let $\gamma_{i, \ell} \in \Gamma(d, p, \ell)$. Then for every $d$-dimensional subspace $W$ of $\mathbb{F}_p^{d+t}$, the $\mathbb{F}_p$-vector space $\mathbb{F}_p^t$ admits a $W$-coset-wise $\mathbb{F}_p$-affine complete mapping of the cycle type

$$
\prod_{i=1}^{p^t} \prod_{\ell=1}^{k_\ell} \text{BU}_\ell(\gamma_{i, \ell}).
$$

In fact, Theorem 1.3 is a compact, inexplicit version of a more elaborate result, Theorem 1.5, which explicitly describes how to construct a $W$-coset-wise $\mathbb{F}_p$-affine complete mapping of $\mathbb{F}_p^t$ of the specified cycle type from a known complete mapping of $\mathbb{F}_p$ of cycle type $x_1^{k_1} \cdots x_p^{k_t}$. For readers that are only interested in constructing permutations (but not necessarily complete mappings) of $\mathbb{F}_q$ with a given cycle type, we note that there is a simpler analogue of Theorem 1.3 (or, rather, its explicit version), where each of the two occurrences of “complete mapping” is replaced by “permutation”, and the set $\Gamma(d, p, \ell)$ may be replaced by its superset $\text{CT}(\text{GL}_d(p))$. For more details, see the end of Section 4.

As the formulation of Theorem 1.3 is rather technical, it may be hard to gauge its power at a first glance. To demonstrate its usefulness, we derive the following interesting consequence:

**Corollary 1.4.** Let $q = p^k$ be an odd prime power, and let $S$ be a Sylow $p$-subgroup of the symmetric group $\text{Sym}(q)$. Then every cycle type of an element of $S$ is also the cycle type of a suitable complete mapping of $\mathbb{F}_q$.

**Proof of Corollary 1.4 using Theorem 1.3.** We proceed by induction on $k$. For $k = 1$, we have that $S$ is cyclic, generated by a $p$-cycle. Hence the only cycle types of elements of $S$ are $x_1^p$ and $x_p$. Since $\text{id}_{x_1^p}$ and the function $\mathbb{F}_p \to \mathbb{F}_p, x \mapsto x + 1$, are complete mappings of $\mathbb{F}_p$ of cycle type $x_1^p$ and $x_p$, respectively, the claim is true in this case.

Now assume that $k > 1$, and that the claim holds for $p^{k-1}$. Let $x_1^{a_0} x_p^{a_1} x_p^{a_2} \cdots x_p^{a_k}$ be the cycle type of an element of $S$. Then

$$
a_0 \equiv \sum_{i=0}^{k} a_i p^{i} = p^k \equiv 0 \pmod{p}.
$$
The following is the cycle type of an element of a Sylow $p$-subgroup of $\text{Sym}(p^k-1)$:

$$x_1^{a_0} x_p^{a_1} x_p^2 x_p^3 \cdots x_p^{a_k}.$$  \hfill (1)

By the induction hypothesis, there is a complete mapping of $\mathbb{F}_{p^k-1}$ of cycle type (1). We will apply Theorem 1.3 with $d = 1$, $t = k - 1$, $x_1^{b_1} \cdots x_p^{b_t}$ equal to (1) and

$$\gamma_{\ell,i} = \begin{cases} x_p^\ell, & \text{if } \ell = 1 \text{ and } i \in \{1, 2, \ldots, \frac{a_\ell}{p}\}, \\ x_p, & \text{otherwise}; \end{cases}$$

note that it is possible to choose the $\gamma_{\ell,i}$ like this because $\{x_1^p, x_p\} \subseteq \text{CT}(\text{ACGL}_1(p)) \subseteq \Gamma(1, p, \ell)$ for all $\ell \geq 1$. Our application of Theorem 1.3 shows that

$$\text{BU}_1(x_1^{p\ell})^{a_0} \cdot \text{BU}_1(x_1^{p\ell})^{a_1} \cdot \text{BU}_p(x_1^{p\ell})^{a_2} \cdots \text{BU}_{p^{k-1}}(x_1^{p\ell})^{a_k} = x_1^{a_0} x_p^{a_1} x_p^2 \cdots x_p^{a_k}$$

is the cycle type of a suitable complete mapping of $\mathbb{F}_{p^k}$, as required. \hfill $\Box$

We note that Corollary 1.4 is false for even $q$. In fact, if $q$ is even, then none of the cycle types of elements of a Sylow 2-subgroup $S$ of $\text{Sym}(q)$ can be the cycle type of a complete mapping of $\mathbb{F}_q$. This is because all elements of $S$ have an even number of fixed points, whereas complete mappings of $\mathbb{F}_q$ have precisely one fixed point (see the discussion before Definition 1.1). Of course, this does not mean that Theorem 1.3 is useless in characteristic 2 – one can still apply it to exhibit various cycle types of complete mappings. However, the situation is more complicated, because one cannot choose $d = 1$ in Theorem 1.3 if $p = 2$ (as $\Gamma(1, 2, \ell) = \emptyset$ for all $\ell \geq 1$).

Corollary 1.4 has the following interesting consequence, with which we conclude this introductory subsection:

**Corollary 1.5.** Let $q$ be a prime power. The following are equivalent:

(1) $\mathbb{F}_q$ admits a complete mapping of cycle type $x_q$ (i.e., that permutes the elements of $\mathbb{F}_q$ in one cycle).

(2) $q$ is odd.

**Proof.** Every Sylow $q$-subgroup of $\text{Sym}(q)$ contains a $q$-cycle. Therefore, Corollary 1.4 implies that $\mathbb{F}_q$ has a complete mapping of cycle type $x_q$ if $q$ is odd. On the other hand, if $q$ is even, then as mentioned in the discussion before Definition 1.1, a complete mapping of $\mathbb{F}_q$ is also an orthomorphism of $\mathbb{F}_q$ and thus has precisely one fixed point. In particular, the said complete mapping cannot be a $q$-cycle. \hfill $\Box$

In Section 5, we will explicitly construct, for each prime power $q$, a permutation of $\mathbb{F}_q$ that is a $q$-cycle and, if $q$ is odd, is a complete mapping of $\mathbb{F}_q$. This is an application of Theorem 4.5, the explicit version of Theorem 1.3 mentioned above.
1.2 Some notation used in this paper

We denote by \( \mathbb{N}^+ \) the set of positive integers. The symmetric group on a set \( X \) is denoted by \( \text{Sym}(X) \). As is customary in group theory, all group actions in this paper are on the right, and we use the notations \( f(x) \) and \( x^f \) to denote the value of \( x \) under the function \( f \) interchangeably. In particular, we consider \( \text{GL}_d(q) \) as a group of matrices acting on row vectors from \( \mathbb{F}_q^d \) through multiplication on the right (\( v^M := v \cdot M \) for \( v \in \mathbb{F}_q^d \) and \( M \in \text{GL}_d(q) \)). As a consequence, our companion matrix forms (see formula (2)) are the transposes of the companion matrices used by Fripertinger [10] (who worked with the left action of \( \text{GL}_d(q) \) on column vectors instead).

1.3 Overview of this paper

In Section 2, we recall the computation of cycle types of affine permutations of finite vector spaces, a problem studied and solved by Fripertinger in [10]. This is useful for readers who want to use the theorem to construct explicit examples of complete mappings with a prescribed cycle type, as we do in Section 5.

Section 3 is concerned with the problem of determining the product sets

\[ C_{\text{GL}_d(q)}(\ell) = \{ A_1 \cdots A_\ell : A_i \in C_{\text{GL}_d(q)} \} \]

for each triple \((d, q, \ell)\), see Proposition 3.1. For us, this is an auxiliary problem for proving Theorem 1.3, but it is also interesting in its own right and has some connections with a group-theoretic problem recently studied by Larsen, Shalev and Tiep in [15], see the end of Section 3.

In Section 4 we formulate and prove Theorem 4.5, the above-mentioned stronger (explicit) version of Theorem 1.3, and in Section 5 we explicitly construct one-cycle complete mappings of finite fields of odd characteristic as an application. Section 6 concludes the paper with a discussion of a related, but harder problem which we aim to tackle in a follow-up paper.

2 Cycle types of affine permutations of finite vector spaces

Let \( q \) be a prime power, and let \( V \) be a finite-dimensional \( \mathbb{F}_q \)-vector space. Our goal in this section is to discuss how to compute the cycle type of a given affine permutation \( \lambda(\alpha, v) \) of \( V \), following Fripertinger [10], though we will use a slightly different presentation.

For this, we need the so-called primary rational canonical form of finite-dimensional vector space automorphisms, which we now briefly recall. For every field \( K \), each endomorphism \( \varphi \) of a finite-dimensional \( K \)-vector space \( V \) induces a direct decomposition \( V = \bigoplus_{i=1}^s W_i \) of \( V \) into \( \varphi \)-invariant \( K \)-subspaces \( W_i \) such that for \( i = 1, 2, \ldots, s \), the restriction \( \varphi|_{W_i} \) can be represented, with respect to a suitable basis of \( W_i \), by \( \text{Comp}(Q_i^{e_i}) \) where \( Q_i \in K[X] \) is a monic irreducible polynomial, \( e_i \) is a positive
integer, and \( \text{Comp}(P) \) denotes the so-called companion matrix of the polynomial
\[
P = X^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0 \in K[X],
\]
which is the following \((d \times d)\)-matrix over \(K\):
\[
\begin{pmatrix}
0 & 1 & 0 & \cdots & 0 & 0 \\
0 & 0 & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1 & 0 \\
0 & 0 & 0 & \cdots & 0 & 1 \\
-a_0 & -a_1 & -a_2 & \cdots & -a_{d-2} & -a_{d-1}
\end{pmatrix}.
\]
(2)

A direct decomposition \( V = \bigoplus_{i=1}^s W_i \) of \( V \) as described in the last sentence will be referred to as a \( \varphi \)-block subspace decomposition of \( V \). Observe that \( \text{Comp}(P) \) is the matrix representing the multiplication
\[
R + (P) \mapsto RX + (P)
\]
by \( X \) on the quotient algebra \( K[X]/(P) \) with respect to the basis \((1 + (P), X + (P), X^2 + (P), \ldots, X^{d-1} + (P))\). While the \( \varphi \)-block subspace decomposition \( V = \bigoplus_{i=1}^s W_i \) is not necessarily unique, the multiset \( \{Q_i^e : i = 1, 2, \ldots, s\} \) of powers of monic irreducible polynomials associated with the decomposition is uniquely determined by \( \varphi \). The corresponding companion matrices \( \text{Comp}(Q_i^e) \) are called the primary rational canonical blocks of \( \varphi \), and any block diagonal matrix that has these companion matrices as its diagonal blocks is called a primary rational canonical form of \( \varphi \). Observing that for each monic polynomial \( P \in K[X] \), both the characteristic and the minimal polynomial of \( \text{Comp}(P) \) is \( P \) itself, we conclude that the characteristic polynomial of \( \varphi \) is \( \prod_{i=1}^s Q_i^e \), whereas its minimal polynomial is \( \text{lcm}(Q_i^e : i = 1, 2, \ldots, s) \).

It follows that \( \varphi \) is an automorphism of \( V \) if and only if \( Q_i \neq X \) for all \( i \), and that \( \varphi \) is a complete automorphism of \( V \) if and only if \( Q_i \neq X, X + 1 \) for all \( i \). Assume henceforth that \( \varphi = \alpha \) is an automorphism of \( V \). Moreover, let \( v = \sum_{i=1}^s v_i \in V \), with \( v_i \in W_i \) for all \( i \). Using that
\[
\text{CT}(\lambda(\alpha, v)) = \bigotimes_{i=1}^s \text{CT}(\lambda(\alpha|W_i, v_i)),
\]
where \( \otimes \) is as in [27, Definition 2.2], we see that in order to understand the cycle types of (complete) affine permutations of \( V \), it suffices to understand the cycle types of affine permutations \( \lambda(\gamma, w) \) whose automorphism part \( \gamma \) can be represented by a companion matrix of the form \( \text{Comp}(Q^e) \) for some positive integer \( e \) and some monic irreducible polynomial \( Q \in K[X] \) such that \( Q \neq X \) (and \( Q \neq X + 1 \) for the complete case). This is also what Fripertinger did in [10], though in case \( e > 1 \), he replaced \( \text{Comp}(Q^e) \) by a certain similar, so-called hypercompanion matrix. He obtained essentially the following result, formulated in terms of polynomial quotient algebras:

**Proposition 2.1.** Let \( q > 1 \) be a power of a prime \( p \), let \( Q, U \in \mathbb{F}_q[X] \) with \( Q \neq X \) monic irreducible, and let \( e \) be a positive integer. Consider the affine permutation
\[
\lambda(X, U) : R + (Q^e) \mapsto RX + U + (Q^e)
\]
of \( \mathbb{F}_q[X]/(Q^e) \).
A. Bors and Q. Wang

Cosets and complete mappings

We now make a case distinction according to the four statements we need to prove:

1. If \( Q \neq X - 1 \), then \( \lambda(X, U) \) has the following cycle count (independently of \( U \)):
   - 1 fixed point;
   - \( \frac{q^\deg Q - 1}{\ord(Q)} \) cycles of length \( \ord(Q) \);
   - for each \( a = 1, 2, \ldots, \lceil \log_p(e) \rceil - 1 \):
     - \( \frac{q^{a-1} \deg Q (q^{\deg Q - 1} (p^a - 1))}{p^a \ord(Q)} \) cycles of length \( \ord(Q) p^a \); and
     - \( \frac{q^{\lceil \log_p(e) \rceil}}{p^\lceil \log_p(e) \rceil \ord(Q)} \) cycles of length \( \ord(Q) p^\lceil \log_p(e) \rceil \).

2. If \( Q = X - 1 \) and \( U + \langle Q \rangle \) is a non-unit in \( \mathbb{F}_q[X]/\langle Q \rangle \), then \( \lambda(X, U) \) has the following cycle count:
   - \( q \) fixed points;
   - for each \( a = 1, 2, \ldots, \lceil \log_p(e) \rceil - 1 \):
     - \( \frac{q^{a-1} (q^{a-1} (p^a - 1))}{p^a} \) cycles of length \( p^a \); and
     - \( \frac{q^{\lceil \log_p(e) \rceil} - 1 (q^{\lceil \log_p(e) \rceil} - 1)}{p^{\lceil \log_p(e) \rceil}} \) cycles of length \( p^{\lceil \log_p(e) \rceil} \).

3. If \( Q = X - 1 \), if \( U + \langle Q \rangle \) is a unit in \( \mathbb{F}_q[X]/\langle Q \rangle \), and if \( e > 1 \) is not a power of \( p \), then \( \lambda(X, U) \) has all of length \( p^{\lceil \log_p(e) \rceil} \) cycles, all of length \( p^{\lceil \log_p(e) \rceil} \).

4. If \( Q = X - 1 \), if \( U + \langle Q \rangle \) is a unit in \( \mathbb{F}_q[X]/\langle Q \rangle \), and if \( e \) is a power of \( p \) (including the case \( e = 1 \)), then \( \lambda(X, U) \) has \( \frac{q}{p^e} \) cycles, all of length \( p^e \).

Because our presentation differs slightly from the one of Fripertinger (we chose to avoid using hypercompanion matrices for greater uniformity), we give a self-contained proof of Proposition 2.1 for the reader’s convenience:

**Proof of Proposition 2.1.** For each positive integer \( \ell \), we have

\[
\lambda(X, U)^\ell (R + \langle Q \rangle) = RX^\ell + U(1 + X + X^2 + \cdots + X^{\ell - 1}) + \langle Q \rangle
\]

for all \( R \in \mathbb{F}_q[X] \). Therefore, the number of solutions \( R \) modulo \( Q^e \) of the congruence

\[
RX^\ell + U(1 + X + X^2 + \cdots + X^{\ell - 1}) \equiv X \pmod{Q^e}
\]

equals the number of points in \( \mathbb{F}_q[X]/\langle Q^e \rangle \) that lie on a cycle of \( \lambda(X, U) \) whose length divides \( \ell \). This congruence is equivalent to

\[
R(X - 1)(1 + X + \cdots + X^{\ell - 1}) = R(X^{\ell - 1}) \equiv -U(1 + X + \cdots + X^{\ell - 1}) \pmod{Q^e}.
\]

We now make a case distinction according to the four statements we need to prove:

1. Case: \( Q \neq X - 1 \). Since \( X - 1 \) is a unit modulo \( Q^e \), we conclude that the precise number of solutions modulo \( Q^e \) of congruence \( 3 \) is

\[
q^{\deg Q \min(e, \nu_Q(X^{\ell - 1}))}.
\]

Observing that

\[
\nu_Q(X^k - 1) = \begin{cases} 
0, & \text{if } \ord(Q) \nmid k, \\
p^k \min(1, \frac{\ord(Q)}{\ord(Q)}), & \text{if } \ord(Q) \mid k
\end{cases}
\]

we have

\[

8
we see that the cycle lengths of $\lambda(X,U)$ are 1 and the numbers of the form
$\text{ord}(Q)p^a$ for some $a = 0, 1, \ldots, \lfloor \log_p(e) \rfloor$ (those are the values of $\ell$ for which
the number of solutions of congruence [3] is strictly larger than the number of
solutions for any proper divisor of $\ell$). Moreover, the number of fixed points of
$\lambda(X,U)$ is precisely
$$q^{\deg Q - \min(e, \nu_Q(X-1))} = q^{\deg Q - \min(e, 0)} = q^0 = 1,$$
whereas for $a = 0, 1, \ldots, \lfloor \log_p(e) \rfloor$, the number of solutions of congruence [3]
for $\ell = \text{ord}(Q)p^a$ is precisely
$$q^{\deg Q - \min(e, p^a)}.$$

An inclusion-exclusion counting argument now confirms the asserted cycle count
of $\lambda(X,U)$.

(2) Case: $Q = X - 1$, and $U + (Q^\ell)$ is a non-unit in $\mathbb{F}_q[X]/(Q^\ell)$ (i.e., $Q \mid U$). Then
the $Q$-adic valuation of the right-hand side $-U(1 + X + X^2 + \cdots + X^{\ell - 1})$ of
congruence [3] is at least $1 + \nu_Q(1 + X + X^2 + \cdots + X^{\ell - 1})$, which is the precise $Q$-
adic valuation of the coefficient $X^{\ell - 1}$ of the left-hand side of that congruence.
It follows that congruence [3] is solvable for all $\ell$ and, more precisely, its number
of solutions modulo $Q^e$ is
$$q^{\min(e, \nu_Q(X^{\ell - 1}))}.$$ Since $Q = X - 1$, we have that
$$\nu_Q(X^k - 1) = p^\nu_p(k)$$
and conclude that the cycle lengths of $\lambda(X,U)$ are just the numbers of the form
$p^a$ with $a = 0, 1, \ldots, \lfloor \log_p(e) \rfloor$, with precisely $q^{\min(e, p^a)}$ points lying on a
cycle whose length divides $p^a$. As in Case (1), an inclusion-exclusion counting
argument now yields the asserted cycle count of $\lambda(X,U)$.

(3) Case: $Q = X - 1$, $U + (Q^\ell)$ is a unit in $\mathbb{F}_q[X]/(Q^\ell)$ (i.e., $Q \nmid U$), and $\ell > 1$
is not a power of $p$. For $\ell = p^{\lfloor \log_p(e) \rfloor}$, congruence [3] becomes the universally
solvable
$$0 \equiv R(X-1)^{p^{\lfloor \log_p(e) \rfloor}} \equiv -U(X-1)^{p^{\lfloor \log_p(e) \rfloor} - 1} \equiv 0 \pmod{(X - 1)^e},$$
so all cycles of $\lambda(X,U)$ have length dividing $p^{\lfloor \log_p(e) \rfloor}$. On the other hand, if
$a \in \{0, 1, \ldots, \lfloor \log_p(e) \rfloor \} - 1$ and $\ell = p^a$, then congruence [3] has no solutions,
because the $Q$-adic valuation $p^a$ of the left-hand side coefficient $(T^p - 1) =
(T - 1)^p$ is strictly larger than $p^a - 1$, the $Q$-adic valuation of the right-hand
side $-U(T - 1)^{p^a - 1}$. It follows that all cycles of $\lambda(X,U)$ have the length $p^{\lfloor \log_p(e) \rfloor}$,
as required.

(4) Case: $Q = X - 1$, $U + (Q^\ell)$ is a unit in $\mathbb{F}_q[X]/(Q^\ell)$ (i.e., $Q \nmid U$), and $e$ is a
power of $p$ (possibly $e = 1$). Then an argument analogous to the one of Case
(3) shows that all cycles of $\lambda(X,U)$ have length $p^{\lfloor \log_p(e) \rfloor + 1} = pe$. □
The following notation will come in handy in the next example:

**Notation 2.2.** Let $q$ be a prime power, and let $M$ be an invertible $(n \times n)$-matrix over $\mathbb{F}_q$.

1. We denote by $\Gamma(M) = \Gamma_{\mathbb{F}_q}(M)$ the set of all cycle types of affine permutations of $\mathbb{F}_n^d$ of the form $\lambda(M,v)$, with $v \in \mathbb{F}_q^n$.
2. For a non-constant monic polynomial $P \in \mathbb{F}_q[X]$ with $P(0) \neq 0$, we set $\Gamma(P) := \Gamma(\text{Comp}(P))$.

**Example 2.3.** Let $q = 3$ and $V = \mathbb{F}_q^3$. Consider the $\mathbb{F}_3$-endomorphism $\alpha$ of $V$ whose standard matrix is the block diagonal matrix with blocks

$$\text{Comp}((X - 1)^2), \text{Comp}((X - 1)^3), \text{and } \text{Comp}(X^2 + X + 2).$$

This diagonal matrix is a primary rational canonical form of $\alpha$. We list the possible cycle types of (complete) affine permutations of $V$ of the form $\lambda(\alpha, v)$ for some $v \in V$.

By Proposition 2.1 we have

$$\Gamma((X - 1)^2) = \{x_1^3 x_2^2, x_3^3\}, \Gamma((X - 1)^3) = \{x_1^3 x_3^3, x_9^3\}, \text{and } \Gamma(X^2 + X + 2) = \{x_1 x_8\}.$$  

This yields the following possibilities for $\text{CT}(\lambda(\alpha, v))$ (note that the second and fourth of them are equal), which we computed via an implementation of Wei-Xu’s product $\ast$ in GAP [11]:

- $(x_1^3 x_3^2) \ast (x_1^2 x_3^3) \ast (x_1 x_8) = x_1^9 x_3^{78} x_9^2 x_2^{78},$
- $(x_1^3 x_3^2) \ast x_9^3 \ast (x_1 x_8) = x_9^{27} x_2^{72},$
- $x_3^3 \ast (x_1^3 x_3^3) \ast (x_1 x_8) = x_3^{81} x_9^{24},$
- $x_3^3 \ast x_9^3 \ast (x_1 x_8) = x_9^{27} x_2^{72}.$

### 3 Products of complete vector space automorphisms

In order to prove Theorem 1.3 we will need to understand which elements of $\text{GL}_d(q)$ can be written as products of matrices in $\text{CGL}_d(q)$ with a given number $\ell$ of factors. The following proposition solves this problem:

**Proposition 3.1.** Let $d$ and $\ell$ be positive integers, and let $q$ be a prime power. Set

$$\text{CGL}_d(q)^{(\ell)} := \{A_1 \cdots A_\ell : A_i \in \text{CGL}_d(q) \text{ for } i = 1, 2, \ldots, \ell\} \subseteq \text{GL}_d(q).$$

Then

$$\text{CGL}_d(q)^{(\ell)} = \begin{cases} 
\text{CGL}_d(q), & \text{if } \ell = 1, \\
\text{GL}_d(q), & \text{if } \ell \geq 2 \text{ and } (d,q) \neq (1,2), (1,3), (2,2), \\
\emptyset, & \text{if } \ell \geq 2 \text{ and } (d,q) = (1,2), \\
\{(1)\}, & \text{if } \ell \geq 2 \text{ and } (d,q) = (1,3), \\
\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}, & \text{if } \ell \geq 2 \text{ and } (d,q) = (2,2). 
\end{cases}$$
Proof. It is clear by definition that $\text{CGL}_d(q)^{(1)} = \text{CGL}_d(q)$, so we may assume that $\ell \geq 2$. First, we discuss the three exceptional cases $(d, q) = (1, 2), (1, 3), (2, 2)$. For $(d, q) = (1, 2)$, we have $\text{CGL}_d(q) = \text{CGL}_1(2) = \emptyset$, because $F_2$ has no complete mappings. This implies $\text{CGL}_1(2)^{(\ell)} = \emptyset$ for all $\ell \in \mathbb{N}^+$, in particular for $\ell \geq 2$. For $(d, q) = (1, 3), (2, 2)$, one can easily check the asserted equalities for $\ell = 2$. In particular, we find that in those cases, $\text{CGL}_d(q)^{(2)}$ is a subgroup of $\text{GL}_d(q)$ containing $\text{CGL}_d(q)$, which implies that $\text{CGL}_d(q)^{(\ell)} = \text{CGL}_d(q)^{(2)}$ for all $\ell \geq 2$, as required.

Now we assume in addition to $\ell \geq 2$ that $(d, q) \neq (1, 2), (1, 3), (2, 2)$. Under these assumptions, we need to show that $\text{CGL}_d(q)^{(\ell)} = \text{GL}_d(q)$. As in the last paragraph, if we can only show this assertion for $\ell = 2$, it is clear that it holds for all $\ell \geq 2$. So we will focus on proving that $\text{CGL}_d(q)^{(2)} = \text{GL}_d(q)$. We distinguish a few cases.

First, assume that $d = 1$ and $q > 3$. Then $\text{CGL}_d(q) = \text{CGL}_1(q) = \{(a) : a \in F_q^*, a \neq -1\}$. Because $q > 3$, we have $|F_q^*| = q - 1 \geq 3$. Hence, for each $a \in F_q^*$, we can choose an element $b \in F_q^* \setminus \{-1, -a\}$. Then $a = b \cdot \frac{a}{b}$ is a representation of $a$ as a product of two elements of $F_q$ that are distinct from $-1$. This shows that $\text{CGL}_1(q)^{(2)} = \text{GL}_1(q)$, as required.

Next, assume that $d > 1$ and $q > 2$. For each one-dimensional $F_q$-subspace $L$ of $F_q^d$, set

$$G_L := \{A \in \text{GL}_d(q) : L \text{ is contained in the } (-1)\text{-eigenspace of } A\}.$$ Observe that for each $L$, we have $|G_L| = \prod_{i=1}^{d-1} (q^d - q^i)$, that $\text{GL}_d(q) \setminus \text{CGL}_d(q) \subseteq \bigcup_L G_L$, and that $-I_d \in G_L$ for all $L$. Since $F_q^d$ has precisely $\frac{q^d - 1}{q - 1}$ one-dimensional $F_q$-subspaces $L$, this implies that

$$|\text{GL}_d(q) \setminus \text{CGL}_d(q)| \leq \frac{q^d - 1}{q - 1} \prod_{i=1}^{d-1} (q^d - q^i) - \left(\frac{q^d - 1}{q - 1} - 1\right) = \frac{1}{q - 1} |\text{GL}_d(q)| - \left(\frac{q^d - 1}{q - 1} - 1\right) < \frac{1}{q - 1} |\text{GL}_d(q)| \leq \frac{1}{2} |\text{GL}_d(q)|.$$

Hence, for each given $A \in \text{GL}_d(q)$, each of the two sets $\text{CGL}_d(q)$ and $A \cdot \text{CGL}_d(q)^{-1}$ has size larger than $\frac{1}{2} |\text{GL}_d(q)|$, whence $|\text{CGL}_d(q) \cap (A \cdot \text{CGL}_d(q)^{-1})| > 0$. That is, there are $C_1, C_2 \in \text{CGL}_d(q)$ such that $C_1 = A \cdot C_2$ or, equivalently, $A = C_1 C_2 \in \text{CGL}_d(q)^{(2)}$. This shows that $\text{CGL}_d(q)^{(2)} = \text{GL}_d(q)$, as required.

This leaves us with the assumptions $d > 1$ and $q = 2$. Since $q$ is even, we have $-1 = 1$ in $F_q$, whence $\text{CGL}_d(q) = \text{CGL}_d(2)$ consists of exactly those matrices $A \in \text{GL}_d(2)$ that are fixed-point-free (henceforth abbreviated to f.p.f.), which is defined to mean that those matrices have no nonzero fixed points. We use this to rewrite the assertion that $\text{CGL}_d(2)^{(2)} = \text{GL}_d(2)$ into an easier to handle equivalent form as follows: For a given matrix $A \in \text{GL}_d(2)$, there exist f.p.f. matrices $C_1, C_2 \in \text{GL}_d(2)$ such that $A = C_1 C_2$ if and only if there exists an f.p.f. matrix $C \in \text{GL}_d(2)$ such that $AC^{-1}$ is f.p.f. as well. Now, $AC^{-1}$ is f.p.f. if and only if for each vector $v \in F_2^d$, the condition $v \cdot AC^{-1} = v$, which is equivalent to $vA = vC$, implies $v = \bar{0}$. That is, $AC^{-1}$ is f.p.f. if and only if $\ker(A - C) = \ker(A + C) = \{0\}$, i.e., if and only if $A + C \in \text{GL}_d(2)$. 

11
In view of this, we are done once we have shown the following claim:

For each \( A \in \text{GL}_d(2) \), there is an f.p.f. \( C \in \text{GL}_d(2) \) such that \( A + C \in \text{GL}_d(2) \). (4)

Observe that since the set \( \text{CGL}_d(2) \) of f.p.f. invertible \((d \times d)\)-matrices over \( \mathbb{F}_2 \) is closed under conjugation by matrices in \( \text{GL}_d(2) \), if claim (4) holds for a given \( A \in \text{GL}_d(2) \), it also holds for every matrix in the conjugacy class \( A^{\text{GL}_d(2)} \). Therefore, it suffices to prove claim (4) for only one matrix \( A \) per \( \text{GL}_d(2) \)-conjugacy class.

We prove claim (4) by induction on \( d \geq 3 \). One can check with GAP [11] that the claim holds for \( 3 \leq d \leq 6 \). We may thus assume that \( d \geq 7 \) and that the claim holds in dimensions \( 3, 4, \ldots, d - 1 \). Let \( A \in \text{GL}_d(2) \) be arbitrary but fixed, and let \( \mathbb{F}_2^d = \bigoplus_{i=1}^s V_i \) be an \( A \)-block subspace decomposition of \( \mathbb{F}_2^d \), with blocks \( \text{Comp}(Q_i^A) \).

If it is possible to partition the multiset of primary rational canonical blocks of \( A \) into two submultisets such that the sum of the block dimensions of each submultiset lies in \( \{3, 4, \ldots, d - 3\} \), then we are done by the induction hypothesis. Indeed, we then have that \( A \) can be written as a block diagonal matrix

\[
\begin{pmatrix}
A_1 & 0 \\
0 & A_2
\end{pmatrix}
\]

such that each diagonal block \( A_i \) has dimension \( d_i \in \{3, 4, \ldots, d - 3\} \). The induction hypothesis yields that there exist matrices \( C_i \in \text{CGL}_{d_i}(2) \) for \( i = 1, 2 \) such that \( A_i + C_i \in \text{GL}_{d_i}(2) \). Setting

\[
C := \begin{pmatrix} C_1 & 0 \\ 0 & C_2 \end{pmatrix},
\]

we find that \( C \in \text{CGL}_d(2) \) and \( A + C \in \text{GL}_d(2) \), as required.

Therefore, we may assume that a partition of the multiset \( M \) of primary rational canonical blocks of \( A \) as described above is not possible. This leaves the following possibilities for the multiset \( M' \) of the dimensions of the primary rational canonical blocks of \( A \): \( \{d\} \), \( \{1, d - 1\} \), \( \{1, 1, d - 2\} \), and \( \{2, d - 2\} \). Indeed, \( A \) cannot have any primary rational canonical block of a dimension in \( \{3, 4, \ldots, d - 3\} \) – otherwise, consider the bipartition of \( M \) where one partition class is just the singleton consisting of a block of \( A \) with dimension in \( \{3, 4, \ldots, d - 3\} \). Therefore, the possible elements of \( M' \) are 1, 2, \( d - 2 \), \( d - 1 \) and \( d \). Since \( \sum M' = d \), we find that \( M' = \{d\} \) if \( d \in M' \).

Now assume that \( d \notin M' \). Since \( d \geq 7 \), we have \( d - 1 > d - 2 > \frac{1}{2} d \), so \( M' \) can only contain one of \( d - 1 \) and \( d - 2 \), and only with multiplicity 1. In particular, \( M' \) must contain at least one of the numbers 1 and 2. But since \( 3 \leq d - 3 \), we have that \( M' \) cannot contain both 1 and 2 – otherwise, consider the bipartition of \( M \) where one partition class consists of precisely one block each of dimensions 1 and 2. Similarly, using that \( 3 \leq d - 3 \) resp. \( 4 \leq d - 3 \), we see that the multiplicity of 1 resp. 2 in \( M' \) is at most 2 resp. 1. Hence, \( M' \) must contain precisely one of \( d - 1 \) or \( d - 2 \), and it does so with multiplicity 1. Since all other elements of \( M' \) are equal to 1 or 2, it now follows that \( M' \) is one of the remaining three multisets listed at the beginning of this paragraph.

We now go through the four possibilities for \( M' \) in a case distinction.
(1) Case: $M' = \{d\}$. Let Comp$(Q^e)$ be the unique primary rational canonical block of $A$. First, assume that $Q \neq X + 1$. Then ord$(Q)$ is an odd number greater than 1, and since $A$ is f.p.f. and has no 2-cycles according to Proposition 2.1 we find that both $A^{-1}$ and $A^2$ are f.p.f., whence $C := A^{-1}$ is an f.p.f. invertible matrix such that $A + C = A + A^{-1} = A^{-1}(A^2 + I_d) \in \text{GL}_d(2)$, as required.

Now assume that $Q = X + 1$. Then we may assume without loss of generality that $A$ is the hypercompanion matrix

$$
\begin{pmatrix}
1 & 1 & 0 & 0 & \cdots & 0 & 0 \\
0 & 1 & 1 & 0 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 1 & 1 \\
0 & 0 & 0 & 0 & \cdots & 0 & 1
\end{pmatrix}
$$

For $C$, we make the ansatz of choosing it as a companion matrix

$$(5) \quad C = \text{Comp}(X^d + b_{d-1}X^{d-1} + \cdots + b_1X + b_0) = 
\begin{pmatrix}
0 & 1 & 0 & 0 & \cdots & 0 & 0 \\
0 & 0 & 1 & 0 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 0 & 1 \\
b_0 & b_1 & b_2 & b_3 & \cdots & b_{d-2} & b_{d-1}
\end{pmatrix}.$$

Note that $C \in \text{CGL}_d(2)$ if and only if $b_0 = 1$ and $b_1 + \cdots + b_{d-1} = 1$. Indeed, $C \in \text{GL}_d(2) = \text{SL}_d(2)$ if and only if $b_0 = \det C = 1$, and under this assumption, $C$ is f.p.f. if and only if the characteristic polynomial $\chi_C = 1 + b_1X + b_2X^2 + \cdots + b_{d-1}X^{d-1} + X^d$ is not divisible by $X + 1$ (i.e., does not have 1 as a root), which is equivalent to $b_1 + b_2 + \cdots + b_{d-1} = 1$.

Now, observe that

$$
A + C = 
\begin{pmatrix}
1 & 0 & 0 & \cdots & 0 & 0 \\
0 & 1 & 0 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1 & 0 \\
b_0 & b_1 & b_2 & \cdots & b_{d-2} & b_{d-1} + 1
\end{pmatrix},
$$

and $A + C \in \text{GL}_d(2)$ if and only if the rows of $A + C$ span $F^d_2$, which is the case if and only if $b_{d-1} = 0$. Hence, if we choose $b_0 := b_1 := 1$ and $b_2 := b_3 := \cdots := b_{d-1} := 0$ in formula (5), the resulting matrix $C$ will be invertible and f.p.f. and satisfy $A + C \in \text{GL}_d(2)$, as required.

(2) Case: $M' = \{1, d - 1\}$. Let Comp$(Q^e)$ be the primary rational canonical block of $A$ of dimension $d - 1$. First, assume that $Q \neq X + 1$. Then we assume without loss of generality that $A$ is its own primary rational canonical form,
where $Q^e = a_0 + a_1 X + a_2 X^2 + \cdots + a_{d-2} X^{d-2} + X^{d-1}$. Note that since $X+1 \not| Q^e$, the sum of all coefficients of $Q^e$ is 1, i.e., $a_0 + a_1 + \cdots + a_{d-2} = 0$.

For $C$, we choose the ansatz

$$
C = \begin{pmatrix}
0 & 0 & \cdots & 0 & 1 \\
0 & 0 & \cdots & 1 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 1 & \cdots & 0 & 0 \\
1 & 0 & \cdots & 0 & 0 \\
\end{pmatrix}
\begin{pmatrix}
b_{d-1} & b_{d-2} & \cdots & b_1 & 1 \\
1 & 0 & \cdots & 0 & 0 \\
0 & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & 0 \\
\end{pmatrix}
\begin{pmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1 \\
1 & b_1 & b_2 & \cdots & b_{d-1} \\
\end{pmatrix}
\begin{pmatrix}
0 & 0 & \cdots & 0 & 1 \\
0 & 0 & \cdots & 1 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 1 & \cdots & 1 & 0 \\
1 & 0 & \cdots & 0 & 0 \\
\end{pmatrix}
$$

with $b_1 + \cdots + b_{d-1} = 1$ (see the discussion after formula (5) in the previous case). Then

$$
A+C = \begin{pmatrix}
b_{d-1} & b_{d-2} + 1 & b_{d-3} & b_{d-4} & \cdots & b_3 & b_2 & b_1 & 1 \\
1 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 1 & 0 & 1 & 0 \\
a_0 & a_1 & a_2 & a_3 & a_4 & \cdots & a_{d-4} & a_{d-3} + 1 & a_{d-2} & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 1 \\
\end{pmatrix}
$$

For $i = 1,2,\ldots,d-1$, set

$$
b_i := \begin{cases}
    a_{d-1-i}, & \text{if } i \neq d-2, \\
    a_1 + 1, & \text{if } i = d-2.
\end{cases}
$$

Note that with this choice of $b_i$, we have $b_1 + \cdots + b_{d-1} = a_0 + \cdots + a_{d-2} + 1 = 1$, so $C \in \text{CGL}_d(2)$. Moreover, the difference between the first and penultimate rows of $A+C$ is the vector

$$
(0 \quad \cdots \quad 0 \quad 1 \quad 0 \quad 1).
$$
It follows that
\[
\text{RowSpace}_{\mathbb{F}_q} \begin{pmatrix} 1 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 \end{pmatrix} \subseteq \text{im}(A + C). \tag{6}
\]

We claim that the row space in formula (6) equals the hyperplane \(H\) of \(\mathbb{F}^d_2\) that consists of those vectors whose entry sum is 0. Indeed, a vector

\[
v = (x_0 \ x_1 \ \cdots \ x_{d-1}) \in \mathbb{F}^d_2
\]

lies in this row space if and only if there are scalars \(\lambda_0, \lambda_1, \ldots, \lambda_{d-2} \in \mathbb{F}_2\) such that

\[
\begin{align*}
(x_0 & \ x_1 \ \cdots \ x_{d-1}) = \\
\lambda_0 (1 & \ 0 & 1 & 0 & \cdots & 0 & 0 & 0) + \\
\lambda_1 (0 & \ 1 & 0 & 1 & \cdots & 0 & 0 & 0) + \\
\ & \vdots + \\
\lambda_{d-3} (0 & \ 0 & 0 & 0 & \cdots & 1 & 0 & 1) + \\
\lambda_{d-2} (0 & \ 0 & 0 & 0 & \cdots & 0 & 1 & 1),
\end{align*}
\]

which translates to the equation system

\[
\begin{align*}
\lambda_0 &= x_0 \\
\lambda_1 &= x_1 \\
\lambda_0 + \lambda_2 &= x_2 \\
\lambda_1 + \lambda_3 &= x_3 \\
\ & \vdots \\
\lambda_{d-5} + \lambda_{d-3} &= x_{d-3} \\
\lambda_{d-4} + \lambda_{d-2} &= x_{d-2} \\
\lambda_{d-3} + \lambda_{d-2} &= x_{d-1} \tag{7}
\end{align*}
\]

It is not hard to check that the equation system obtained from the system (7) by deleting the last equation, \(\lambda_{d-3} + \lambda_{d-2} = x_{d-1}\), has a unique solution for every choice of \(x_0, \ldots, x_{d-2}\), namely the one where for \(i = 0, 1, \ldots, d - 2\), one has

\[
\lambda_i = \sum_{j \leq 2|1-i-j} x_j;
\]

that is, \(\lambda_0 = x_0, \lambda_1 = x_1, \lambda_2 = x_0 + x_2, \lambda_3 = x_1 + x_3, \lambda_4 = x_0 + x_2 + x_4\), and so on. Therefore, the whole system (7) is solvable if and only if

\[
\sum_{j \leq d-3, 2|d-3-j} x_j + \sum_{j \leq d-2, 2|d-2-j} x_j = x_{d-1},
\]

15
which is equivalent to

\[ x_0 + x_1 + \cdots + x_{d-1} = 0, \]

i.e., to \( v \in H \). Hence, the row space in formula (1) is indeed equal to \( H \), as asserted. Now, since \( \text{im}(A + C) \) contains both \( H \) and the vector

\[
\begin{pmatrix}
 a_0 & a_1 & \cdots & a_{d-4} & a_{d-3} + 1 & a_{d-2} & 0
\end{pmatrix} \notin H,
\]

we conclude that \( \text{im}(A + C) = \mathbb{F}_2^d \), i.e., that \( A + C \in \text{GL}_d(2) \), as required.

Having dealt with the assumption \( Q \neq X+1 \), let us now assume that \( Q = X+1 \). Replacing the nontrivial primary Frobenius block \( \text{Comp}((X+1)^{d-1}) \) of \( A \) by its similar hypercompanion matrix, we may assume without loss of generality that

\[
A = \begin{pmatrix}
 1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\
 0 & 1 & 1 & 0 & \cdots & 0 & 0 & 0 \\
 \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
 0 & 0 & 0 & 0 & \cdots & 1 & 1 & 0 \\
 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\
 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1
\end{pmatrix}.
\]

We make the ansatz

\[
C = \text{Comp}(1 + b_1 X + b_2 X^2 + \cdots + b_{d-1} X^{d-1} + X^d) = \begin{pmatrix}
 0 & 1 & 0 & \cdots & 0 \\
 0 & 0 & 1 & \cdots & 0 \\
 \vdots & \vdots & \vdots & \ddots & \vdots \\
 0 & 0 & 0 & \cdots & 1 \\
 1 & b_1 & b_2 & \cdots & b_{d-1}
\end{pmatrix}
\]

with \( b_1 + \cdots + b_{d-1} = 1 \). Then

\[
A + C = \begin{pmatrix}
 1 & 0 & \cdots & 0 & 0 & 0 \\
 0 & 1 & \cdots & 0 & 0 & 0 \\
 \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
 0 & 0 & \cdots & 1 & 0 & 0 \\
 0 & 0 & \cdots & 0 & 1 & 1 \\
 1 & b_1 & \cdots & b_{d-3} & b_{d-2} & b_{d-1} + 1
\end{pmatrix}.
\]

If we choose \( b_1 := 1 \) and \( b_2 := b_3 := \cdots := b_{d-1} := 0 \), then the rows of \( A + C \) span \( \mathbb{F}_2^d \), whence \( A + C \in \text{GL}_d(2) \), as required.

(3) Case: \( M' = \{1,1,d-2\} \). Let \( \text{Comp}(Q^e) \) be the unique primary Frobenius block of \( A \) of dimension \( d-2 \). Without loss of generality, we may assume that \( A \) is its own primary rational canonical form. Hence, \( A \) can be viewed as a block diagonal matrix with diagonal blocks \( \text{Comp}(Q^e) \) and \( I_2 \). By the induction hypothesis and the statement for \( (d,q) = (2,2) \), we find that there are matrices \( C_1 \in \text{CGL}_{d-2}(2) \) and \( C_2 \in \text{CGL}_2(2) \) such that \( \text{Comp}(Q^e) + C_1 \in \text{GL}_{d-2}(2) \) and \( I_2 + C_2 \in \text{GL}_2(2) \). The block diagonal matrix \( C \) with diagonal blocks \( C_1 \) and \( C_2 \) lies in \( \text{CGL}_d(2) \) and satisfies \( A + C \in \text{GL}_d(2) \), as required.
(4) Case: \( M' = \{2, d - 2\} \). The unique primary Frobenius block \( B \) of \( A \) with dimension 2 can be either \( \text{Comp}(X + 1)^2 = \text{Comp}(X^2 + 1) \) or \( \text{Comp}(X^2 + X + 1) \). If \( B = \text{Comp}(X^2 + X + 1) \), then \( B \in \text{CGL}_2(2) \subseteq \text{CGL}_2(2)^{(2)} \), and we are done by an argument analogous to the one in the previous case. We may thus assume that

\[
B = \text{Comp}(X^2 + 1) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} =: B'.
\]

Write the unique primary Frobenius block of \( A \) of dimension \( d - 2 \) as \( \text{Comp}(Q^r) \). First, assume that \( Q \neq X + 1 \). We may assume without loss of generality that \( A \) is the block diagonal matrix with diagonal blocks \( \text{Comp}(Q^r) \) and \( B' \), i.e., that

\[
A = \begin{pmatrix}
0 & 1 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 1 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1 & 0 & 0 \\
a_0 & a_1 & a_2 & \cdots & a_{d-3} & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 1 & 1
\end{pmatrix}
\]

where \( Q^r = a_0 + a_1 X + \cdots + a_{d-3} X^{d-3} + X^{d-2} \), and we know that \( a_0 + \cdots + a_{d-3} = 0 \). As in the case “\( M' = \{1, d - 1\}\)”, we make the ansatz

\[
C = \begin{pmatrix}
b_d-1 & b_{d-2} & \cdots & b_1 & 1 \\
1 & 0 & \cdots & 0 & 0 \\
0 & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & 0
\end{pmatrix}
\]

with \( b_1 + \cdots + b_{d-1} = 1 \). Then

\[
A + C = \begin{pmatrix}
b_{d-1} & b_{d-2} + 1 & b_{d-3} & b_{d-4} & \cdots & b_4 & b_3 & b_2 & b_1 & 1 \\
1 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & \cdots & 0 & 0 & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 1 & 0 & 1 & 0 & 0 \\
a_0 & a_1 & a_2 & a_3 & \cdots & a_{d-5} & a_{d-4} + 1 & a_{d-3} & 0 & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 1
\end{pmatrix}.
\]

Note that since the last row of \( A + C \) is the last standard unit vector in \( \mathbb{F}_2^d \), we have that \( A + C \) lies in \( \text{GL}_d(2) \) if and only if the \( ((d - 1) \times (d - 1)) \)-matrix \( D \) obtained from \( A + C \) by deleting the entries from the last column and row lies in \( \text{GL}_{d-1}(2) \). Now, we can choose the \( b_i \) such that the first row of \( D \) is the vector

\[
(0 \ \cdots \ 0 \ 1 \ 0) \in \mathbb{F}_2^{d-1},
\]

17
and then as in the case \( M' = \{1, d - 1\} \), we see that \( \text{im}(D) = \mathbb{F}_2^{d-1} \), i.e., that \( D \in \text{GL}_{d-1}(2) \), as required.

Finally, assume that \( Q = X + 1 \). Then without loss of generality, we have

\[
A = \begin{pmatrix}
1 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & \cdots & 0 & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 1 & 1
\end{pmatrix}
\]

Make the ansatz

\[
C = \text{Comp}(1 + b_1 X + b_2 X^2 + \cdots + b_{d-1} X^{d-1} + X^d) = \begin{pmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 1 \\
1 & b_1 & b_2 & \cdots & b_{d-1}
\end{pmatrix}
\]

with \( b_1 + \cdots + b_{d-1} = 1 \). Then

\[
A + C = \begin{pmatrix}
1 & 0 & \cdots & 0 & 0 & 0 & 0 \\
0 & 1 & \cdots & 0 & 0 & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & 0 & 0 & 0 \\
0 & 0 & \cdots & 0 & 1 & 1 & 0 \\
0 & 0 & \cdots & 0 & 0 & 1 & 1 \\
1 & b_1 & \cdots & b_{d-4} & b_{d-3} & b_{d-2} + 1 & b_{d-1} + 1
\end{pmatrix}
\]

If we choose \( b_i := 0 \) for \( i = 1, 2, \ldots, d - 2 \), and \( b_{d-1} := 1 \), then \( A + C \in \text{GL}_d(2) \), as required.

There is an interesting connection between the theory developed in this section and the recent group-theoretic paper [13] by Larsen, Shalev and Tiep. More precisely, in [13, Section 10], the following question is studied: “Which transitive permutation groups \( S \) that are nonabelian simple as abstract groups have the property that every element of \( S \) is a product of two derangements in \( S \)?”. Using tools from algebraic geometry and character theory, it is shown that \( S \) has this property as long as \( |S| \) is large enough, see [13, Theorem 10.2]. Since \( \text{GL}_d(2) = \text{SL}_d(2) = \text{PSL}_d(2) \) is nonabelian simple for \( d \geq 3 \), and since the elements of \( \text{CGL}_d(2) \) are the derangements of the natural transitive action of \( \text{GL}_d(2) \) on \( \mathbb{F}_2^d \setminus \{0\} \), the result [13, Theorem 10.2] implies that \( \text{CGL}_d(2) = \text{GL}_d(2) \) if \( d \) is large enough. However, no explicit lower bound on \( |S| \) is given in [13, Theorem 10.2], whence it is not clear whether [13, Theorem 10.2] could be used to give a shorter proof of the fact that \( \text{CGL}_d(2) = \text{GL}_d(2) \) for all \( d \geq 3 \) than our elementary argument above.

In this context, we also note that our proof of Proposition 3.1 yields the following:
Proposition 3.2. Let \( d \) be a positive integer, and let \( q \) be a prime power. If \((d,q) \neq (1,2),(1,3),(2,2)\), then every element of \( \text{GL}_d(q) \) is a product of two fixed-point-free elements of \( \text{GL}_d(q) \) (i.e., derangements in the natural transitive action of \( \text{GL}_d(q) \) on \( \mathbb{F}_q^d \setminus \{0\} \)).

Proof. If \( q > 2 \), then our proof of Proposition 3.1 shows that \( |\text{CGL}_d(q)| > \frac{1}{2} |\text{GL}_d(q)| \) (note that this also applies in case \( d = 1 \), although this was not noted explicitly in the proof of Proposition 3.1). But \( \text{CGL}_d(q) \) is in bijection with the set \( \text{OGL}_d(q) \) of all fixed-point-free invertible \((d \times d)\)-matrices of \( \mathbb{F}_q \) via the function \( M \mapsto M + I_d \). Therefore, \( |\text{OGL}_d(q)| > \frac{1}{2} |\text{GL}_d(q)| \), and an argument analogous to the one for “\( d > 1 \) and \( q > 2 \)” in the proof of Proposition 3.1 shows that every element in \( \text{GL}_d(q) \) is a product of two elements of \( \text{OGL}_d(q) \), as required.

Now assume that \( q = 2 \). Then \( \text{OGL}_d(q) = \text{CGL}_d(q) \), and the result follows from Proposition 3.1. \( \square \)

Recall the cycle type sets \( \Gamma(d,p,\ell) \) from Notation 1.2(4). The following consequence of Proposition 3.1 exhibits its connection with Theorem 1.3.

Corollary 3.3. Let \( p \) be a prime, and let \( d \) and \( \ell \) be positive integers. Then

\[
\Gamma(d,p,\ell) = \{ \text{CT}(\lambda(M,w)) : M \in \text{CGL}_d(p) )^{(\ell)} \text{ and } w \in \mathbb{F}_p^d \}. \tag{8}
\]

Proof. This is clear for \( \ell = 1 \) by the definitions of \( \Gamma(d,p,\ell) \) and \( A\text{CGL}_d(p) \). If \( \ell \geq 2 \) and \((d,p) \neq (1,2),(1,3),(2,2)\), then the set on the right-hand side of formula (8) is equal to \( \text{CT}(A\text{GL}_d(p)) = \Gamma(d,p,\ell) \) by Proposition 3.1. Likewise, for \( \ell \geq 2 \) and \((d,p) \in \{(1,2),(1,3),(2,2)\} \), one can check that the equality holds using the information on the set \( \text{CGL}_d(p) )^{(\ell)} \) from Proposition 3.1 and Proposition 2.1. \( \square \)

4 Proof of Theorem 1.3

In this section, we develop the necessary theory for the proof of Theorem 1.3 (a stronger version of Theorem 1.3), with which this section will be concluded. First, we discuss some generalities concerning coset-wise affine functions.

Let \( K \) be a field, let \( V \) be a finite-dimensional \( K \)-vector space, and let \( W \) be a \( K \)-subspace of \( V \). Throughout the rest of this discussion, we fix a complement \( U \) of \( W \) in \( V \), so that \( V = W \oplus U \). For \( u \in U \), we set \( W_u := W + u \). Then the sets \( W_u \) for the various \( u \in U \) are the cosets of \( W \) in \( V \). For \( U \)-indexed families \( \vec{v} = (v_u)_{u \in U} \) and \( \vec{\varphi} = (\varphi_u)_{u \in U} \), of vectors in \( V \) and \( K \)-endomorphisms of \( V \) stabilizing \( W \) respectively, we denote by \( f_{\vec{\varphi},\vec{v}} \) the \( W \)-coset-wise \( K \)-affine function of \( V \) such that for each \( u \in U \), one has \( f(x) \) = \( x^{\varphi_u} + v_u \) for all \( x \) in \( W_u \). Moreover, we denote by \( g_{\vec{\varphi},\vec{v}} \) the unique function \( U \rightarrow U \) such that for each \( u \in U \), one has

\[
f(W_u) \subseteq W_{g_{\vec{\varphi},\vec{v}}(u)}.
\]

Proposition 4.1. With notation as fixed above, the following hold:

1. \( f_{\vec{\varphi},\vec{v}} \) is a permutation of \( V \) if and only if \( \varphi_u \) restricts to an automorphism of \( W \) for all \( u \in U \) and \( g_{\vec{\varphi},\vec{v}} \) is a permutation of \( U \).
A. Bors and Q. Wang

Cosets and complete mappings

(2) \( f_{\bar{\varphi},\bar{v}} \) is a complete mapping of \( V \) if and only if \( \varphi_u \) restricts to a complete automorphism of \( W \) for all \( u \in U \) and \( g_{\bar{\varphi},\bar{v}} \) is a complete mapping of \( U \).

Proof. For statement (1): If \( f_{\bar{\varphi},\bar{v}} \) is a permutation of \( V \), then the following must hold:

- \( f_{\bar{\varphi},\bar{v}} \) must map each coset of \( W \) onto a coset of \( W \). For a fixed \( u \in U \), the elements of \( W_u \) are of the form \( w + u \) where \( w \) ranges over \( W \), and their images under \( f_{\bar{\varphi},\bar{v}} \) are of the form \((w + u)^{\varphi_u} + v_u = w^{\varphi_u} + u^{\varphi_u} + v_u\).

If this is to assume all values in the coset \( W_u^{\varphi_u} + v_u \), then \( w^{\varphi_u} \) must assume all values in \( W \). In other words, \( \varphi_u \) must be a surjective \( K \)-endomorphism of \( W \), i.e., a \( K \)-automorphism by the finiteness of \( \dim_K(W) \).

- \( f_{\bar{\varphi},\bar{v}} \) must permute the cosets of \( W \) in \( V \). In other words, \( g_{\bar{\varphi},\bar{v}} \) must be a permutation of \( U \), as required.

Conversely, assume that each \( \varphi_u \) restricts to an automorphism of \( W \) and that \( g_{\bar{\varphi},\bar{v}} \) is a permutation of \( U \). The latter implies that every coset of \( W \) in \( V \) intersects \( \mathrm{im}(f_{\bar{\varphi},\bar{v}}) \), and the former that every coset of \( W \) intersecting \( \mathrm{im}(f_{\bar{\varphi},\bar{v}}) \) is fully contained in \( \mathrm{im}(f_{\bar{\varphi},\bar{v}}) \). Together, this yields that \( f_{\bar{\varphi},\bar{v}} \) is surjective and thus a permutation of \( V \).

The proof of statement (2) is similar, and we omit it.

The coset-wise \( K \)-affine functions \( f_{\bar{\varphi},\bar{v}} \) of \( V \) that are permutations of \( V \) form a permutation group \( \text{CWAff}_W(V) \) on \( V \), and we want to understand the structure of this permutation group. First, we make a simplification with regard to the involved endomorphisms \( \varphi_u \).

Recall from above that for each \( u \in U \) and each \( w \in W \), we have

\[ f_{\bar{\varphi},\bar{v}}(w + u) = w^{\varphi_u} + u^{\varphi_u} + v_u. \]

Assume that \( \varphi' = (\varphi'_u)_{u \in U} \) is a different family of \( K \)-endomorphisms of \( V \) that stabilize \( W \), and assume that for each \( u \in U \), the restrictions of \( \varphi_u \) and \( \varphi'_u \) to \( W \) are equal. If we set

\[ v'_u := u^{\varphi'_u} + v_u - u^{\varphi_u} \]

for each \( u \in U \), and we set \( \bar{v}' := (v'_u)_{u \in U} \), then we find that

\[ f_{\bar{\varphi'},\bar{v}'}(w + u) = w^{\varphi'_u} + u^{\varphi'_u} + v'_u = w^{\varphi_u} + u^{\varphi_u} + v_u = f_{\bar{\varphi},\bar{v}}(w + u). \]

This shows that we still get the full group \( \text{CWAff}_W(V) \) if we restrict to only such coset-wise \( K \)-affine permutations \( f_{\bar{\varphi},\bar{v}} \) of \( V \) where each \( \varphi_u \) is an automorphism \( \gamma_u \) of \( V = W \oplus U \) of the form \( \alpha_u \oplus \text{id}_U \) for some \( \alpha_u \in \text{Aut}(W) \). We will henceforth assume that \( \bar{\varphi} = \bar{\gamma} \) is chosen of this form.

For the formulation of the next theorem, we briefly recall the notion of an imprimitive permutational wreath product:

**Definition 4.2.** Let \( G \) be an abstract group, and let \( P \leq \text{Sym}(\Lambda) \) be a permutation group.
(1) The (abstract) wreath product of $G$ and $P$, written $G \wr P$, is the abstract group that can be defined as the external semidirect product $P \rtimes G^\Lambda$ where $P$ acts on $G^\Lambda$, whose elements are $\Lambda$-indexed families $(g_\lambda)_{\lambda \in \Lambda}$ of elements of $G$, by “coordinate permutations”. More explicitly, the elements of $G \wr P$ are ordered pairs of the form $(\sigma, \bar{g})$ with $\sigma \in P$ and $\bar{g} = (g_\lambda)_{\lambda \in \Lambda} \in G^\Lambda$, and these elements are multiplied as follows:

$$(\sigma, (g_\lambda)_{\lambda \in \Lambda}) \cdot (\psi, (h_\lambda)_{\lambda \in \Lambda}) := (\sigma \psi, (g_{\psi^{-1}(\lambda)}h_\lambda)_{\lambda \in \Lambda}).$$

(2) If $G \leq \text{Sym}(\Omega)$ is a permutation group, then the abstract group $G \wr P$ is isomorphic to a certain permutation group on $\Omega \times \Lambda$ that is called the imprimitive (permutational) wreath product of $G$ and $P$ and will be denoted by $G \wr_{\text{imp}} P$. More explicitly, the function $G \wr P \to \text{Sym}(\Omega \times \Lambda)$ that maps $(\sigma, (g_\lambda)_{\lambda \in \Lambda}) \in G \wr P$ to the permutation

$$(\omega, \lambda) \mapsto (g_{\sigma(\lambda)}(\omega), \sigma(\lambda))$$

is an isomorphism of abstract groups between $G \wr P$ and $G \wr_{\text{imp}} P$.

Moreover, we remind the reader that an isomorphism of permutation groups $G \leq \text{Sym}(\Omega)$ and $H \leq \text{Sym}(\Lambda)$ is a bijection $\beta : \Omega \to \Lambda$ such that $\beta^{-1}G\beta = H$. In this case, the function $G \to H$, $g \mapsto \beta^{-1}g\beta$, is an isomorphism of abstract groups, and we say that $g \in G$ corresponds to $\beta^{-1}g\beta \in H$ under $\beta$.

**Theorem 4.3.** Consider the bijection

$$\iota : V = W \oplus U \to W \times U, \; w + u \mapsto (w, u).$$

This bijection is a permutation group isomorphism between $\text{CWAff}_W(V)$ and the imprimitive permutational wreath product $\text{Aff}(W) \wr_{\text{imp}} \text{Sym}(U)$. In fact, if, as above, $\gamma = (\gamma_u)_{u \in U} = (\alpha_u \oplus \text{id}_U)_{u \in U}$ and $\nu = (\nu_u)_{u \in U}$, and if we write $\nu_u = \omega_u + \nu_u$ with $\omega_u \in W$ and $\nu_u \in U$, then we have that under this isomorphism, the element $f_{\gamma, \nu}$ of $\text{CWAff}_W(V)$, permuting the cosets $W_u = W + u$ of $W$ in $V$ according to $g_{\gamma, \nu} \in \text{Sym}(U)$, corresponds to the wreath product element

$$f_{\gamma, \nu}(\lambda(\alpha_u, \omega_u))_{u \in U}).$$

**Proof.** For all $w \in W$ and all $u \in U$, we have

$$f_{\gamma, \nu}(\iota^{-1}((w, u))) = f_{\gamma, \nu}(w + u) = w^{\alpha_u} + u + \nu_u = (w^{\alpha_u} + \omega_u) + (u + \nu_u)$$

$$= (w^{\alpha_u} + \omega_u) + g_{\gamma, \nu}(u) = \iota^{-1}((w^{\alpha_u} + \omega_u, g_{\gamma, \nu}(u)))$$

$$= \iota^{-1}((w, u)(g_{\lambda, \psi}(\lambda(\alpha_u, \omega_u))_{u \in U})),
$$

which shows that the diagram

$$\begin{array}{ccc}
V & \xrightarrow{\iota} & V \\
\downarrow f_{\gamma, \nu} & & \downarrow \iota \\
W \times U & \xrightarrow{f_{\gamma, \nu}} & W \times U \\
(g_{\gamma, \nu}, (\lambda(\alpha_u, \omega_u))_{u \in U}) & & 
\end{array}$$

remains commutative.
A. Bors and Q. Wang

Cosets and complete mappings

is commutative. This shows that the group isomorphism \( \text{Sym}(V) = \text{Sym}(W \oplus U) \to \text{Sym}(W \times U) \), \( \sigma \mapsto \ell^{-1}\sigma\ell \), restricts to an injective group homomorphism \( \text{CWAff}_W(V) \to \text{Aff}(W) \), and it remains to show that this homomorphism is also surjective. Let \( (\psi, (\lambda(\alpha_u, \omega_u))_{u \in U}) \in \text{Aff}(W) \). Set \( \vec{\gamma} := (\alpha_u \oplus \text{id}_U)_{u \in U} \) and \( \vec{\omega} := (\omega_u + u^p - u)_{u \in U} \). The calculations from the beginning of this proof show that

\[
\ell \circ f_{\vec{\gamma}, \vec{\omega}} \circ \ell^{-1} = \ell^{-1} f_{\vec{\gamma}, \vec{\omega}} = (\psi, (\lambda(\alpha_u, \omega_u))_{u \in U}),
\]
as required. \( \square \)

The following result concerning cycle types in imprimitive permutational wreath products will be useful in view of Theorem 4.3.

**Lemma 4.4.** Let \( \Omega \) and \( \Lambda \) be finite sets, let \( G \leq \text{Sym}(\Omega) \) and \( H \leq \text{Sym}(\Lambda) \), and let \( P := G \wr H \leq \text{Sym}(\Omega \times \Lambda) \). Consider an element \( \sigma = (\psi, (g_\lambda))_{\lambda \in \Lambda} \in P \). For each cycle \( \zeta = (\lambda_0, \lambda_1, \ldots, \lambda_{d-1}) \) of \( \sigma \) on \( \Lambda \), call an element of \( G \) of the form \( g_{\lambda_0}g_{\lambda_1} \cdots g_{\lambda_{d-1}} \) a forward cycle product of \( \sigma \) with respect to \( \zeta \). Since all forward cycle products of \( \sigma \) with respect to \( \zeta \) are \( G \)-conjugate to each other, the cycle type \( \gamma_{\zeta}(\sigma) := \text{CT}(g_{\lambda_0} \cdots g_{\lambda_{d-1}}) \) is uniquely determined by \( \sigma \) and \( \zeta \). Moreover,

\[
\text{CT}(\sigma) = \prod_{\zeta} \text{BU}_{\ell(\zeta)}(\gamma_{\zeta}(\sigma)),
\]

where \( \zeta \) ranges over the cycles of \( \psi \) on \( \Lambda \), and \( \ell(\zeta) \) denotes the length of \( \zeta \).

**Proof.** This is a slightly more general version of [2, Lemma 3.5], a “local” version of Pólya’s celebrated formula for the cycle index of an imprimitive permutational wreath product [22, table at the bottom of p. 180]. The proof is analogous to the one of [2, Lemma 3.5]. Note that we used the notation \( \text{CT}^{\ell}(\alpha) \) for \( \text{BU}_\ell(\text{CT}(\alpha)) \) in [2, Lemma 3.5]. \( \square \)

We now specialize to \( K = \mathbb{F}_p \) for some prime \( p \). Using the theory developed thus far, we can formulate and prove Theorem 4.3 below. To make the formulation of the theorem itself more concise, we introduce some notation used in it.

Let \( p \) be a prime, and let \( d \) and \( t \) be positive integers. Assume that \( g \) is a complete mapping of \( \mathbb{F}_p^t =: U \) of cycle type \( x_1^{k_1} \cdots x_p^{k_p} \). For \( \ell = 1, 2, \ldots, p^t \), enumerate the length \( \ell \) cycles of \( g \) on \( U \) as

\[
\zeta_{\ell,i} = (u_{\ell,i,0}, u_{\ell,i,1}, \ldots, u_{\ell,i,\ell}) \text{ for } i = 1, 2, \ldots, k_{\ell}.
\]

Moreover, for \( \ell = 1, 2, \ldots, p^t \) and \( i = 1, 2, \ldots, k_{\ell} \), choose a cycle type \( \gamma_{\ell,i} \in \Gamma(d, p, \ell) \). By Corollary 3.3, we can write

\[
\gamma_{\ell,i} = \text{CT}(\Lambda(M_{\ell,i,0} \cdots M_{\ell,i,\ell-1}, w_{\ell,i})) \in \text{CT}(\text{AGL}_d(p))
\]

for suitable \( M_{\ell,i,0}, \ldots, M_{\ell,i,\ell-1} \in \text{CGL}_d(p) \) and \( w_{\ell,i} \in \mathbb{F}_p \).
For \(\ell = 1, 2, \ldots, p^t\), \(i = 1, 2, \ldots, k_\ell\) and \(j = 0, 1, \ldots, \ell - 1\), set
\[
\alpha_{u,i,j} := (w \mapsto wM_{\ell,i,j}) \in \text{Aut}_F(W),
\]
set
\[
\omega_{u,i,j} := \begin{cases} 
\bar{0} \in \mathbb{F}_p^d, & \text{if } j < \ell - 1, \\
\omega_{u,i}, & \text{if } j = \ell - 1,
\end{cases}
\]
and set
\[
\nu_{u,i,j} := u_{i,(j+1) \mod \ell - u_{\ell,i,j}}.
\]
Observe that this defines the notations \(\alpha_u\), \(\omega_u\) and \(\nu_u\) uniquely for each \(u \in U\).

Consider the \(\mathbb{F}_p^t\)-vector space \(V = \mathbb{F}_p^{d+t} = \mathbb{F}_p^d \oplus \mathbb{F}_p^t = W \oplus U\). Set
\[
\bar{\gamma} := (\alpha_u \oplus \text{id}_U)_{u \in U} \in \text{Aut}_{\mathbb{F}_p}(V)^U
\]
and \(\bar{\nu} := (\omega_u + \nu_u)_{u \in U} \in V^U\).

**Theorem 4.5.** With notation as fixed above, we have that the \(W\)-coset-wise \(K\)-affine function
\[
f_{\bar{\gamma},\bar{\nu}} : V \to V, v = w + u \mapsto w^{\alpha_u} + u + \omega_u + \nu_u,
\]
is a complete mapping of \(V\) of cycle type
\[
\prod_{\ell=1}^{p^t} \prod_{i=1}^{k_\ell} BU_{\ell}(\gamma_{\ell,i}).
\]

**Proof.** By Theorem 4.3, \(f_{\bar{\gamma},\bar{\nu}}\) corresponds under a suitable isomorphism of permutation groups \(\text{CWAff}_{W}(V) \rightarrow \text{Aff}(W) \sim \text{Sym}(U)\) to the wreath product element \((\psi, (\lambda(\alpha_u, \omega_u))_{u \in U})\) where \(w^\psi = u + \nu_u\) for all \(u \in U\). By definition of \(\nu_u\), we have \(u + \nu_u = u^\varphi\), and so \(f_{\bar{\gamma},\bar{\nu}}\) corresponds to \(\sigma := (g, (\lambda(\alpha_u, \omega_u))_{u \in U})\). By Lemma 4.4, it suffices to show that for all \(\ell = 1, 2, \ldots, p^t\) and \(i = 1, 2, \ldots, k_\ell\), the cycle type of any forward cycle product of \(\sigma\) with respect to \(\zeta_{\ell,i}\) is equal to \(\gamma_{\ell,i}\). But by definition, the following is such a forward cycle product:
\[
\lambda(\alpha_{u_{\ell,i,0},\ell-1,0}) \cdot \lambda(\alpha_{u_{\ell,i,1},\ell-1,1}) \cdots \lambda(\alpha_{u_{\ell,i,\ell-1-1},\ell-1}) = \lambda(M_{\ell,i,0} M_{\ell,i,1} \cdots M_{\ell,i,\ell-1-1}, w_{\ell,i}),
\]
and this has the cycle type \(\gamma_{\ell,i}\) by construction. \(\square\)

We remark that an analogous proof shows that if each \(\gamma_{\ell,i}\) lies in \(\text{CT}(\text{AGL}_d(p))\), but not necessarily in \(\Gamma(d,p,\ell)\), then one obtains a permutation (but not necessarily a complete mapping) \(f_{\bar{\gamma},\bar{\nu}}\) of \(V\) of cycle type
\[
\prod_{\ell=1}^{p^t} \prod_{i=1}^{k_\ell} BU_{\ell}(\gamma_{\ell,i}).
\]
by choosing matrices \(M_{\ell,i,j} \in \text{GL}_d(p)\) and vectors \(w_{\ell,i} \in \mathbb{F}_p^d\) such that
\[
\gamma_{\ell,i} = \lambda(M_{\ell,i,0} M_{\ell,i,1} \cdots M_{\ell,i,\ell-1}, w_{\ell,i}).
\]
5 Construction of one-cycle complete mappings

In this section, we discuss an exemplary application of Theorem 4.5 – constructing, for each odd prime power $q$, a permutation $f_q$ of $\mathbb{F}_q$ of cycle type $x_q$ such that $f_q$ is a complete mapping of $\mathbb{F}_q$. We remark that the construction also makes sense if $q$ is even and yields a permutation of $\mathbb{F}_q$ of cycle type $x_q$ which is not a complete mapping of $\mathbb{F}_q$.

Write $q = p^k$ with $k \geq 1$. For fixed $p$, we recursively construct a complete mapping $h_k$ of the $\mathbb{F}_p$-vector space $\mathbb{F}_p^k$ of cycle type $x_p^k$ as follows:

- For $k = 1$, let $h_1 : \mathbb{F}_p \to \mathbb{F}_p$, $x \mapsto x + 1$. Observe that $h_1$ is of cycle type $x_p$ and is a complete mapping of $\mathbb{F}_p$ if $p > 2$.

- Now assume that $k > 1$ and that we already defined a permutation $h_{k-1}$ of $\mathbb{F}_p^{k-1} =: U$ such that $h_{k-1}$ is of cycle type $x_{p^{k-1}}$ and is a complete mapping of $U$ if $p > 2$. We can write $h_{k-1}$ in cycle notation as

\[(v_0, v_1, \ldots, v_{p^{k-1}-2}, v_{p^{k-1}-1} = \vec{0}).\]

Moreover, we write

\[h_1 = \lambda(1, 1) = \lambda(1, 0)\lambda(1, 0) \cdots \lambda(1, 0)\lambda(1, 1)\]

as a product with $\ell$ factors in $\text{AGL}_1(p)$, each of which is a complete mapping of $\mathbb{F}_p =: W$ if $p > 2$. Following the proof of Theorem 4.5, if we set

\[\vec{v} := (v_u)_{u \in U} \text{ and } \vec{v} := (v_u)_{u \in U},\]

then the function $h_k : \mathbb{F}_p^k = W \oplus U \to \mathbb{F}_p^k$,

\[w + u \mapsto w + u + v_u = \begin{cases} (w + 1) + u^{h_{k-1}}, & \text{if } u = \vec{0}, \\ w + u^{h_{k-1}}, & \text{if } u \neq \vec{0}, \end{cases}\]

has cycle type $x_{p^k}$ and is a complete mapping of $\mathbb{F}_p^k$ if $p > 2$.

Using the recursive formula (10), it is not hard to show by induction on $k$ that $h_k$ has the explicit form

\[(x_1, \ldots, x_k)^{h_k} = (x_1, \ldots, x_{k-1}, x_k + 1, \ldots, x_k + 1) \text{ if } x_k = x_{k-1} = \cdots = x_{k+1} = 0. \] (11)

For example,

\[(x, y)^{h_2} = \begin{cases} (x, y + 1), & \text{if } y \neq 0, \\ (x + 1, y + 1), & \text{if } y = 0. \end{cases}\]
A. Bors and Q. Wang

Cosets and complete mappings

It is not hard to show by induction on $g$

We recursively define functions $f$ as follows:

We can also give a polynomial formula for a function $F_q \to F_q$ which, with regard to a suitable $F_p$-basis of $F_q$, has the form (11) and thus is a permutation of $F_q$ of cycle type $x_q$ and a complete mapping of $F_q$ if $q$ is odd. This uses the following well-known elementary lemma:

**Lemma 5.1.** Let $q = p^k$ be a prime power, and let $\omega \in F_q$ be of algebraic degree $k$

with respect to the $F_p$-basis $\mathcal{B}$ of $F_q$. For $i = 0, 1, \ldots, k - 1$, denote by $\pi_i$ the function $F_q \to F_p \subseteq F_q$ which maps $x = \sum_{j=0}^{k-1} x_j \omega^j \in F_q$ to its $i$-th $\mathcal{B}$-coordinate $x_i$. Then for all $x \in F_q$, we have

Note that formula (12) expresses each coordinate function $\pi_i$ as an $F_p$-linearized polynomial function. Now, the function $f_{p^k} : F_{p^k} \to F_{p^k}$ which with respect to the $F_p$-basis $\mathcal{B}$ of $F_q$ has the form (11) can be written as

We recursively define functions $g_j : F_{p^k} \to F_{p^k}$ for $j = 1, 2, \ldots, k - 1$ as follows:

It is not hard to show by induction on $j$ that

$$
g_j(x) = \begin{cases} 
0, & \text{if } \pi_j(x) \neq 0, \\
\omega^j, & \text{if } \pi_j(x) = 0 \text{ and } \pi_{j-1}(x) \neq 0, \\
\omega^j \omega^j, & \text{if } \pi_j(x) = \pi_{j-1}(x) = 0 \text{ and } \pi_{j-2}(x) \neq 0, \\
\vdots & \\
\omega^j + \omega^j + \cdots + \omega + 1, & \text{if } \pi_j(x) = \pi_{j-1}(x) = \cdots = \pi_1(x) = 0.
\end{cases}
$$
Hence

\[ f_{p^k}(x) = x + \omega^{k-1} + g_{k-1}(x) \text{ for all } x \in \mathbb{F}_{p^k}. \]

Since we know the reduced polynomial forms of the coordinate functions \( \pi_i \) by formula (12), we can recursively work out the reduced polynomial forms of the functions \( g_j \), allowing us to compute the reduced polynomial form of \( f_{p^k} \).

**Example 5.2.** We compute a reduced polynomial over \( \mathbb{F}_{27} \) that represents a complete mapping of \( \mathbb{F}_{27} \) of cycle type \( x_{27} \). The computations in this example were carried out using GAP [11]. Let \( \omega \in \mathbb{F}_{27} \) be a root of the Conway polynomial \( X^3 - X + 1 \in \mathbb{F}_3[X] \). In particular, \( \omega \) is a primitive root of \( \mathbb{F}_{27} \). By Lemma 5.1 we have for all \( x \in \mathbb{F}_{27} \) that

\[
\begin{pmatrix}
\pi_0(x) & \pi_1(x) & \pi_2(x)
\end{pmatrix} = 
\begin{pmatrix}
x & x^3 & x^9
\end{pmatrix} \cdot \begin{pmatrix}
1 & 1 & 1 \\
\omega & \omega^3 & \omega^9 \\
\omega^2 & \omega^6 & \omega^{18}
\end{pmatrix}^{-1} = 
\begin{pmatrix}
\omega^{25} & \omega^{14} & -1 \\
\omega^{23} & \omega^{16} & -1 \\
\omega^{17} & \omega^{22} & -1
\end{pmatrix}.
\]

Hence

\[
\pi_0(x) = \omega^{25}x + \omega^{23}x^3 + \omega^{17}x^9,
\pi_1(x) = \omega^{14}x + \omega^{16}x^3 + \omega^{22}x^9,
\pi_2(x) = -x - x^3 - x^9.
\]

Observe that

\[
g_1(x) = 1 - \pi_1(x)^2 = \\
\omega^5x^{18} + \omega^{12}x^{12} + \omega^{10}x^{10} + \omega^{19}x^6 + \omega^4x^4 + \omega^{15}x^2 + 1
\]

and

\[
g_2(x) = (1 - \pi_2(x)^2) \cdot (\omega + g_1(x)) = \\
\omega^{18}x^{36} + \omega^{10}x^{30} + \omega^{12}x^{28} + x^{24} + x^{22} + x^{20} + \omega^{16}x^{18} + x^{16} + x^{14} + \omega^9x^{12} + \omega^{23}x^{10} + \\
x^8 + \omega^{16}x^6 + \omega^{25}x^4 + \omega^{19}x^2 + \omega^9 = \\
x^{24} + x^{22} + x^{20} + \omega^{16}x^{18} + x^{16} + x^{14} + \omega^9x^{12} + \omega^9x^{10} + x^8 + \omega^{16}x^6 + \omega^9x^4 + \\
\omega^{16}x^2 + \omega^9.
\]

Therefore, we have

\[
f_{27}(x) = x + \omega^2 + g_2(x) = \\
x^{24} + x^{22} + x^{20} + \omega^{16}x^{18} + x^{16} + x^{14} + \omega^9x^{12} + \omega^9x^{10} + x^8 + \omega^{16}x^6 + \omega^9x^4 + \\
\omega^{16}x^2 + x + \omega^6.
\]
6 Concluding remarks

In this paper, we were concerned with producing examples of cycle types of complete mappings of finite fields. That is, we exhibited elements of the set

\[ \{ \text{CT}(f) : f \text{ is a complete mapping of } \mathbb{F}_q \} \].

There is also a related, harder problem, which asks for simultaneous control over the cycle types of a complete mapping \( f \) and its associated orthomorphism \( f + \text{id} \). In other words, this problem is concerned with the set

\[ \{(\text{CT}(f), \text{CT}(f + \text{id})) : f \text{ is a complete mapping of } \mathbb{F}_q \} \]

of cycle type pairs. For the most basic examples of complete mappings, scalar multiplications \( f_a : x \mapsto ax \) for a fixed \( a \in \mathbb{F}_q^* \setminus \{-1\} \), controlling the cycle types of \( f_a \) and \( f_a + \text{id} = f_{a+1} \) simultaneously is tantamount to controlling the multiplicative orders of \( a \) and \( a + 1 \) simultaneously, for which a theorem of Carlitz, [4, Theorem 1], is an important tool.

However, with \( f_a \) and \( f_a + \text{id} \) both being scalar multiplications, the range of possibilities for \( (\text{CT}(f_a), \text{CT}(f_a + \text{id})) \) is rather limited, and in order to obtain more interesting examples of such cycle type pairs, one needs to study a larger class of complete mappings \( f \) such that simultaneous control over \( \text{CT}(f) \) and \( \text{CT}(f + \text{id}) \) can be gained. In a follow-up paper, the authors intend to do so for a certain subclass of the class of complete, coset-wise \( \mathbb{F}_p \)-affine mappings of \( \mathbb{F}_{p^k} \).

References

[1] P.T. Bateman, A remark on infinite groups, *Amer. Math. Monthly* 57: 623–624, 1950.

[2] A. Bors and Q. Wang, Cycle types of complete mappings of finite fields, preprint (2021), [https://arxiv.org/abs/2105.00140](https://arxiv.org/abs/2105.00140).

[3] J.N. Bray, Q. Cai, P.J. Cameron, P. Spiga and H. Zhang, The Hall–Paige conjecture, and synchronization for affine and diagonal groups, *J. Algebra* 545: 27–42, 2020.

[4] L. Carlitz, Sets of primitive roots, *Compositio Math.* 13: 65–70, 1956.

[5] Y. Chen, L. Wang and S. Zhu, On the constructions of \( n \)-cycle permutations, *Finite Fields Appl.* 73: 101847, 2017.

[6] A.B. Evans, *Orthomorphism Graphs of Groups*, Springer (Lecture Notes in Mathematics, 1535), Berlin, 1992.

[7] A.B. Evans, The admissibility of sporadic simple groups, *J. Algebra* 321: 105–116, 2009.
[8] A.B. Evans, *Orthogonal Latin Squares Based on Groups*, Springer (Developments in Mathematics, 57), Cham, 2018.

[9] R.J. Friedlander, B. Gordon and P. Tannenbaum, Partitions of groups and complete mappings, *Pacific J. Math.* 92(2): 283–293, 1981.

[10] H. Fripertinger, Cycle indices of linear, affine and projective groups, *Linear Algebra Appl.* 263:133–156, 1997.

[11] The GAP Group, *GAP – Groups, Algorithms, and Programming*, Version 4.11.0 (2020) [http://www.gap-system.org](http://www.gap-system.org).

[12] S.W. Golomb, G. Gong and L. Mittenthal, Constructions of orthomorphisms of \( \mathbb{Z}_n^2 \), in: D. Jungnickel and H. Niederreiter (eds.), *Finite Fields and Applications. Proceedings of the Fifth International Conference on Finite Fields and Applications Fq5*, held at the University of Augsburg, Germany, August 2–6, 1999, Springer (Berlin, Heidelberg), 2001, pp. 178–195.

[13] M. Hall and L.J. Paige, Complete mappings on finite groups, *Pacific J. Math.* 5: 541–549, 1955.

[14] L. Işık, A. Topuzoğlu and A. Winterhof, Complete mappings and Carlitz rank, *Des. Codes Cryptogr.* 85: 121–128, 2017.

[15] M. Larsen, A. Shalev and P.H. Tiep, Products of normal subsets and derangements, preprint (2020), [https://arxiv.org/abs/2003.12882](https://arxiv.org/abs/2003.12882).

[16] H.B. Mann, The construction of orthogonal Latin squares, *Ann. Math. Statistics* 13: 418–423, 1942.

[17] L. Mittenthal, Block substitutions using orthomorphic mappings, *Adv. Appl. Math.* 16(10): 59–71, 1995.

[18] L. Mittenthal, Nonlinear dynamic substitution devices and methods for block substitutions employing coset decompositions and direct geometric generation, US Patent 5647001, 1997.

[19] A. Muratović-Ribić and E. Pasalic, A note on complete polynomials over finite fields and their applications in cryptography, *Finite Fields Appl.* 25: 306–315, 2014.

[20] H. Niederreiter and K.H. Robinson, Complete mappings of finite fields, *J. Austral. Math. Soc. Ser. A* 33(2):197–212, 1984.

[21] T. Niu, K. Li, L. Qu and Q. Wang, New constructions of involutions over finite fields, *Cryptogr. Commun.* 12: 165–185, 2020.

[22] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, *Acta Math.* 68(1): 145–254, 1937.
[23] R.-H. Schulz, On check digit systems using anti-symmetric mappings, in: I. Althöfer et al. (eds.), *Numbers, information and complexity*, Kluwer, Boston, 2000, pp. 295–310.

[24] R. Shaheen and A. Winterhof, Permutations of finite fields for check digit systems, *Des. Codes Cryptogr.* 57: 361–371, 2010.

[25] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A.K. Gangopadhyay and S. Maitra, Investigations on bent and negabent functions via the nega-Hadamard transform, *IEEE Trans. Inf. Theory* 58: 4064–4072, 2012.

[26] Z. Tu, X. Zeng and L. Hu, Several classes of complete permutation polynomials, *Finite Fields Appl.* 25: 182–193, 2014.

[27] W.-D. Wei and J.-Y. Xu, Cycle index of direct product of permutation groups and number of equivalence classes of subsets of $Z_v$, *Discrete Math.* 123: 179–188, 1993.

[28] S. Wilcox, Reduction of the Hall–Paige conjecture to sporadic simple groups, *J. Algebra* 321: 1407–1428, 2009.

[29] A. Winterhof, Generalizations of complete mappings of finite fields and some applications, *J. Symbolic Comput.* 64: 42–52, 2014.

[30] G. Wu, N. Li, T. Helleseth and Y. Zhang, Some classes of monomial complete permutation polynomials over finite fields of characteristic two, *Finite Fields Appl.* 28: 148–165, 2014.

[31] M. Wu, C. Li and Z. Wang, Characterizations and constructions of triple-cycle permutations of the form $x^r h(x^s)$, *Des. Codes Cryptogr.* 88(10): 2119–2132, 2020.

[32] G. Xu and X. Cao, Complete permutation polynomials over finite fields of odd characteristic, *Finite Fields Appl.* 31: 228–240, 2015.

[33] Z. Zha, L. Hu and X. Cao, Constructing permutations and complete permutations over finite fields via subfield-valued polynomials, *Finite Fields Appl.* 31: 162–177, 2015.