Des. Codes Cryptogr. (2015) 76:257–267
DOI 10.1007/s10623-014-9945-5

# Monomial isomorphisms of cyclic codes

**Edward Dobson**

Received: 17 October 2013 / Revised: 29 January 2014 / Accepted: 14 February 2014 /
Published online: 8 March 2014

**Abstract** For codes, there are multiple notions of isomorphism. For example, we can consider isomorphisms that only permute the coordinates of codewords, or isomorphisms that not only permute the coordinates of codewords but also multiply each coordinate by a scalar (not necessarily the same scalar for each coordinate) as it permutes the coordinates. Isomorphisms of cyclic codes of the first kind have been studied in some circumstances—we will call them permutation isomorphisms—and our purpose is to begin the study of the second kind of isomorphism—which we call monomial isomorphisms—for cyclic codes. We give examples of cyclic codes that are monomially isomorphic but not permutationally isomorphic. We also show that the monomial isomorphism problem for cyclic codes of length $n$ over $\mathbb{F}_q$ reduces to the permutation isomorphism problem for cyclic codes of length $n$ over $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$. Applying known results, this solves the monomial isomorphism problem for cyclic codes satisfying $\gcd(n, q(q-1)) = 1$. Additionally, we solve the monomial isomorphism problem for cyclic codes of prime length over all finite fields. Finally, our results also hold for some codes that are not cyclic.

**Keywords** Cyclic code · Monomial · Permutation · Isomorphism · Equivalent

**Mathematical Subject Classification** 94B15

A **linear code** of length $n$ over the field of $q$ elements $\mathbb{F}_q$ is simply a subspace of $\mathbb{F}_q^n$, and an element of the subspace is called a **codeword**. There are two common ways of defining linear isomorphisms (usually called equivalence) between linear codes. In the first definition, one only considers possible isomorphisms which are simply permutations of letters

Communicated by C. E. Praeger.

E. Dobson (✉)
Department of Mathematics and Statistics, Mississipi State University, PO Drawer MA,
Mississipi, MS 39762, USA
e-mail: dobson@math.msstate.edu

E. Dobson
University of Primorska, IAM, Muzejeska trg 2, 6000 Koper, Slovenia

(or coordinates) in a code word. More specifically, if $C$ and $C'$ are linear codes of length $n$ over $\mathbb{F}_q$, then $C$ and $C'$ are isomorphic if there exists an $n \times n$ permutation matrix $P$ such that $Pc \in C'$ if and only if $c \in C$. As a permutation matrix simply permutes the coordinates, we can and sometimes will consider $P \in S_n$. This kind of isomorphism we will refer to as a **permutation isomorphism** for the rest of the paper. The second kind is more complicated. We still need an $n \times n$ permutation matrix $P$, but we will also allow multiplication of a component by a scalar in $\mathbb{F}_q$. This can be represented as $PD$, where $D$ is a diagonal matrix whose determinant is nonzero. We will call such an isomorphism a **monomial isomorphism**. We remark that monomial isomorphisms between codes is in some sense the most general form of linear isomorphism between codes, as Filip and Heise [7] have shown that any Hamming weight preserving linear bijection from one linear code to another is necessarily a monomial isomorphism between the two codes. We remark that there are *nonlinear* isomorphisms between linear codes—see [11]. We shall not consider such isomorphisms here. We point out that Sendrier and Simosit [22] have shown that the monomial isomorphism problem for codes reduces to the permutation isomorphism problem for codes, but that in the reduction the length of the code increases.

As there two notions of linear isomorphism for linear codes, there are two notions of linear automorphism for linear codes as well. By $\mathrm{PAut}(C)$, we denote the group of all permutation isomorphisms between a code $C$ and itself, called **permutation automorphisms**, and by $\mathrm{MAut}(C)$, the group of all monomial isomorphisms between a code $C$ and itself, **called monomial automorphisms**. A code $C$ is **cyclic**, if the map that shifts coordinates by 1 is a permutation automorphism of $C$. That is, the map $(c_1, \ldots, c_n) \mapsto (c_n, c_1, \ldots, c_{n-1})$ is a permutation automorphism of $C$. The permutation isomorphism problem for cyclic codes of length $n$ over any finite field has been solved by Huffman et al. [10] in the case where $n$ is a prime squared. Recently Muzychuk [17] showed that the permutation isomorphism problem for cyclic codes of length $n$ over $\mathbb{F}_q$ reduces to the isomorphism problem for circulant color digraphs provided that $\gcd(n, q) = 1$. In this paper, we begin the investigation of monomial isomorphisms of cyclic codes, and give an arithmetic condition for which the solution of the monomial isomorphism problem for cyclic codes reduces to the permutation isomorphism problem for cyclic codes (Corollary 2.2). Combining this with Muzychuk's results, we solve the monomial isomorphism problem for all values of $n$ and for all finite fields of certain characteristic depending on the length $n$ (Corollary 2.4). Additionally, we give an example of cyclic codes of prime length $p$ over $\mathbb{F}_q$, $q$ a prime, which are monomially isomorphic but not permutationally isomorphic (Example 1.1), and then completely solve the monomial isomorphism problem for cyclic codes of prime length over all finite fields (Theorem 3.1 and Theorem 3.2).

## 1 Definitions, terminology, and known and preliminary results

We begin with notation and terminology regarding monomial maps. A matrix of the form $PD$, where $P$ is a permutation matrix and $D$ is a diagonal matrix with nonzero determinant, is a **monomial matrix**, and the group $\mathcal{MM}_n(q)$ of all $n \times n$ monomial matrices with entries in $\mathbb{F}_q$ is isomorphic to $S_n \ltimes (\mathbb{F}_q^*)^n$. For convenience, we let $\mathcal{P}_n(q)$ be the group of all $n \times n$ permutation matrices, $\mathcal{D}_n(q)$ the group of all $n \times n$ diagonal matrices with entries in the field $\mathbb{F}_q$ with nonzero determinant, and $\mathcal{S}_n(q)$ the set of all $n \times n$ scalar matrices in $\mathcal{D}_n(q)$, where a scalar matrix is a matrix of the form $\alpha I_n$, $\alpha \in \mathbb{F}_q^*$. Now let $S_n \wr \mathbb{F}_q^*$ act on $\mathbb{Z}_n \times \mathbb{F}_q$ in the natural fashion. That is, $S_n \wr \mathbb{F}_q^* = \{(i, j) \mapsto (\sigma(x), \alpha_i j) : \sigma \in S_n, \alpha_i \in \mathbb{F}_q^*\}$. Then $S_n \wr \mathbb{F}_q^* \cong S_n \ltimes (\mathbb{F}_q^*)^n$, and so $\mathcal{MM}_n(q) \cong S_n \wr \mathbb{F}_q^*$. Thus any subgroup of $\mathcal{MM}_n(q)$ is isomorphic to a subgroup of $S_n \wr \mathbb{F}_q^*$ by the map, say, $\xi$. Clearly under $\xi$ the group of permutation matrices maps to the subgroup $\{(i, j) \mapsto (\sigma(i), j) : \sigma \in S_n\}$. Also, there is a canonical isomorphism between the group of all $n \times n$ permutation matrices and $S_n$, which we denote by $\psi$.

Let $G$ be a group and define $g_L : G \to G$ by $g_L(x) = gx$. Let $G_L = \{g_L : g \in G\}$. Then $G_L$ is the **left-regular representation of** $G$. For $g \in G$, we define $\hat{g}_L = \psi^{-1}(g_L)$ and let $\hat{G}_L = \psi^{-1}(G_L)$. Then $\hat{g}_L : G \times \mathbb{F}_q \to G \times \mathbb{F}_q$ by $\hat{g}_L(x, i) = (gx, i)$. Of course $\hat{G}_L$ is a group isomorphic to $G$. We say that a code $C$ is $\hat{G}_L$-invariant if $\hat{G}_L \le \text{MAut}(C)$. Note that this is equivalent to requiring that the group of codeword preserving permutations of the components of codewords contains $G_L$, or equivalently, that $G_L \le \psi(\text{PAut}(C))$. A cyclic code of length $n$ in this language is just a $\hat{\mathbb{Z}}_n$-invariant code.

Note that as $\hat{G}_L \le \text{MAut}(C)$, the coordinates of a codeword can indexed with elements of $G$. We may then consider $\psi(\text{PAut}(C)) \le S_G$, where $S_G$ is the symmetric group on $G$. We may also identify $S_G$ with the $n \times n$ (or $|G| \times |G|$) permutation matrices, in which case $\text{PAut}(C)$ consists of those permutation matrices which stabilize $C$.

We begin with an example showing that there are cyclic codes that are monomially isomorphic but not permutation isomorphic. For coding theory terms used in the following result that are not defined here, see [11].

*Example 1.1* Let $n$ be a positive integer, $p|n$ be prime, and $q$ a prime-power such that $p|(q-1)$. Then there exists monomially isomorphic cyclic codes of length $n$ over $\mathbb{F}_q$ of dimension 1 that are not permutationally isomorphic.

*Proof* Let $\alpha \in \mathbb{F}_q^*$ be of order $p$. Then $\alpha$ is a root of the polynomial $x^n - 1$ (viewed as a polynomial with coefficients in $\mathbb{F}_q$). Let $C$ be the cyclic code of length $n$ over $\mathbb{F}_q$ with generating polynomial $(x^n - 1)/(x - \alpha)$. As $\alpha$ has order $p$ in $\mathbb{F}_q^*$, $(x^n - 1)/(x - \alpha)$ is not a multiple of $\sum_{i=0}^{n-1} x^i$. Then the code $C$ is monomially isomorphic to the repetition code of length $n$ over $\mathbb{F}_q$ (as they are both subspaces of $\mathbb{F}_q^*$ of dimension 1), but $C$ is clearly not permutation isomorphic to the repetition code of length $n$ over $\mathbb{F}_q$ as its generating polynomial is not a multiple of $\sum_{i=0}^{n-1} x^i$. Thus there are monomially isomorphic cyclic codes of length $n$ over $\mathbb{F}_q$ that are not permutationally isomorphic cyclic codes. □

The problem of permutation isomorphism between cyclic codes is usually discussed in terms of the Cayley isomorphism problem. We now define the appropriate terms for discussion of this problem not only in our context of permutation and monomial isomorphisms of codes, but also Cayley color digraphs and in the more general context of Cayley objects.

**Definition 1.2** Let $C$ be a $\hat{G}_L$-invariant linear code over $\mathbb{F}_q$. We say that $C$ is a **PCI-code of** $G$ if whenever $C'$ is a $\hat{G}_L$-invariant code over $\mathbb{F}_q$, then $C$ and $C'$ are permutation isomorphic if and only if they are permutation isomorphic by an automorphism of $G$ (by "isomorphic by a group automorphism of $G$" we mean $C$ and $C'$ are isomorphic by a permutation matrix $P$ such that $\psi(P)$ is an automorphism of $G$). We say that $C$ is an **MCI-code of** $G$ provided that $C$ and $C'$ are isomorphic by a monomial isomorphism if and only if they are isomorphic by a permutation matrix $P$, where again $\psi(P)$ is an automorphism of $G$.

**Definition 1.3** We define a **Cayley object of** $G$ to be a combinatorial object $X$ (e.g. digraph, graph, design, code) such that $G_L \le \text{Aut}(X)$, where $\text{Aut}(X)$ is the **automorphism group of** $X$ (note that this implies that the vertex set of $X$ is in fact $G$). If $X$ is a Cayley object of $G$ in some class $\mathcal{K}$ of combinatorial objects with the property that whenever $Y$ is another Cayley object of $G$ in $\mathcal{K}$, then $X$ and $Y$ are isomorphic if and only if they are isomorphic by a group automorphism of $G$, then we say that $X$ is a **CI-object of** $G$ **in** $\mathcal{K}$. If every Cayley object of

$G$ in $\mathcal{K}$ is a CI-object of $G$ in $\mathcal{K}$, then we say that $G$ is a **CI-group with respect to** $\mathcal{K}$. If $G$ is a CI-group with respect to every class of combinatorial objects, then $G$ is a **CI-group**.

Several equivalent precise definitions of the notion of a combinatorial object can be found in [20]. It is worth mentioning the following remarkable theorem of Pálfy [21].

**Theorem 1.4** *A group $G$ of order $n$ is a CI-group if and only if $n = 4$ or $\gcd(n, \varphi(n)) = 1$, where $\varphi$ is Euler's phi function.*

In our context, the above result says that if $n = 4$ or $\gcd(n, \varphi(n)) = 1$, then every $\hat{G}$-invariant code is a PCI-code. Note that this also explains why Huffman, Job, and Pless [10] began by considering the permutation isomorphism problem for cyclic codes of length a prime-squared as the simpler case of prime length is handled by Pálfy's Theorem above.

As for a $\hat{G}_L$-invariant code $C$ we have that $\psi(\mathrm{PAut}(C))$ is isomorphic to a subgroup of $S_G$ (here $S_G$ is the symmetric group on $G$) and $\psi(\hat{G}_L) = G_L$, the question of determining whether or not a group $G$ has the property every $\hat{G}_L$-invariant code over $\mathbb{F}_q$ is a PCI-code can be phrased in the context and language of the CI-problem. That is, a $\hat{G}$-invariant code would be called a "Cayley code" over $\mathbb{F}_q$, and that $G$ is a CI-group with respect to codes over $\mathbb{F}_q$ instead of that every $\hat{G}$-invariant code over $\mathbb{F}_q$ is a PCI-code. We remark that the term "Cayley code" is not used in coding theory, and such a code is called a **group code**. Finally, as mentioned earlier, we may identify the coordinates of a codeword canonically with elements of $G$. Then

Babai [1] characterized the CI-property in the following manner, and this tool is used in almost every positive result concerning the Cayley isomorphism problem.

**Lemma 1.5** *For a Cayley object $X$ of $G$ in $\mathcal{K}$ the following are equivalent:*

*(1) $X$ is a CI-object,*
*(2) given a permutation $\delta \in S_G$ such that $\delta^{-1} G_L \delta \leq \mathrm{Aut}(X)$, $G_L$ and $\delta^{-1} G_L \delta$ are conjugate in $\mathrm{Aut}(X)$.*

If $X$ is not a CI-object of $G$, the solution to the isomorphism problem is usually expressed in terms of **solving sets**. Let $G$ be a finite group. We say that $S \subseteq S_G$ is a **solving set** for a Cayley object $X$ in a class of Cayley objects $\mathcal{K}$ if for every $X' \in \mathcal{K}$ such that $X \cong X'$, there exists $s \in S$ such that $s(X) = X'$. Observe that solving sets are not unique, as if $S$ is a solving set, then $\{sg_L : s \in S\}$ is a solving set for every $g \in G$. Also, $X$ is a CI-object of $G$ if and only if a solving set for $X$ consists of automorphisms of $G$. Solving sets for Cayley objects of abelian groups were characterized in [6, Lemma 13].

**Lemma 1.6** *Let $G$ be a finite abelian group, and $S \subseteq S_G$ set of permutations. Then the following conditions are equivalent:*

*(1) $S$ is a solving set for a Cayley object $X$ in a class $\mathcal{K}$ of Cayley objects of $G$,*
*(2) whenever $\delta \in S_G$ such that $\delta^{-1} G_L \delta \leq \mathrm{Aut}(X)$, then there exists $s \in S$ and $v \in \mathrm{Aut}(X)$ such that $v^{-1}\delta^{-1} g_L \delta v = s^{-1} g_L s$ for every $g \in G$.*

Let $C$ be a cyclic code of length $n$ over $\mathbb{F}_q$. We say that $S \subset \mathcal{P}_n(q)$ is a **permutation solving set** for $C$ if and only if any cyclic code $C'$ permutationally isomorphic to $C$ is permutationally isomorphic to $C$ by an element of $S$. Similarly, we say that $S \subset \mathcal{MM}_n(q)$ is a **monomial solving set** for $C$ if and only if any cyclic code $C'$ monomially isomorphic to $C$ is monomially isomorphic to $C$ by an element of $S$.

The isomorphism problem for Cayley objects has been most thoroughly studied when the object is a digraph or a graph (see [14] for a relatively recent survey). Usually, such results hold for **color** Cayley digraphs, where a color Cayley digraph of $G$ is a digraph whose edges have been colored (and so $G_L$ not only preserves edges, but also maps all edges of a given color to edges of the same color). A **circulant color digraph of order** $n$ is a Cayley color digraph of the group $\mathbb{Z}_n$. Recently, Muzyhcuk [17] discovered a relationship between the isomorphism problem for color Cayley digraphs and the isomorphism problem for group codes. The following result is a combination of [17, Theorems 1, 2 and 3], and contains the results of [17] that we will have need of. We need one additional term before proceeding. A $\hat{G}$-invariant code $C$ over $\mathbb{F}_q$ is called **semisimple** if $\gcd(|G|, q) = 1$.

**Theorem 1.7** *If G is either cyclic or a p-group, then a permutation solving set for color Cayley digaphs of G is a solving set for semisimple group codes of G. If in addition, G is a CI-group with respect to color digraphs, then G is a CI-group with respect to semisimple codes.*

The monomial isomorphism problem for $\hat{G}$-invariant codes over $\mathbb{F}_q$, $q$ odd, though cannot be rephrased in terms of the CI-problem, as it is never the case that $\mathrm{MAut}(C)$ is canonically isomorphic to a subgroup of $S_n$, where $n$ is the length of a codeword of $C$ (as the maps $\alpha I_n$, $\alpha \in \mathbb{F}_q^*$, are always monomial isomorphisms of a linear code over $\mathbb{F}_q$, and so are always in $\mathrm{MAut}(C)$). Nevertheless, these problems are clearly related, and after proving a preliminary lemma we prove an analog of Lemma 1.6 for monomial isomorphisms of $\hat{G}$-invariant linear codes. Before proceeding, we will need some additional terminology.

For groups $H \leq G$, we denote the centralizer of $H$ in $G$ by $Z_G(H)$. Let $C$ a $\hat{G}_L$-invariant code over $\mathbb{F}_q$. For $\sigma = PD \in \mathrm{MAut}(C)$, we define $\sigma/\mathbb{F}_q = \psi(P)$ and for $H \leq \mathrm{MAut}(C)$, we let $H/\mathbb{F}_q = \{\psi(P) : PD \in H\}$. Clearly $\psi(\mathrm{PAut}(C)) \leq \mathrm{MAut}(C)/\mathbb{F}_q$.

**Lemma 1.8** *If G is finite and abelian, then* $Z_{\mathcal{MM}_n(q)}(\hat{G}_L) = \hat{G}_L \times \mathcal{S}_n(q)$.

*Proof* It is straightforward to verify that $\langle \hat{G}_L, \mathcal{S}_n(q)\rangle \leq Z_{\mathcal{MM}_n(q)}(\hat{G}_L)$. Let $\delta \in Z_{\mathcal{MM}_n(q)}(\hat{G}_L)$. Then $\psi(\delta)$ centralizes $\psi(\hat{G}_L) = G_L$, and as a transitive abelian group is self-centralizing [2, Theorem 4.2A (v)], $\delta/\mathbb{F}_q \in G_L$. It thus suffices to show that if $\delta \in \mathcal{D}_n(q)$ centralizes $\hat{G}_L$, then $\delta \in \mathcal{S}_n(q)$. Now, $\xi(\delta)(i, j) = (i, \alpha_i j)$, $\alpha_i \in \mathbb{F}_q^*$, and

$$(gi, j) = \xi(\hat{g}_L)(i, j) = \xi(\delta^{-1}\hat{g}_L\delta)(i, j) = (gi, \alpha_{gi}^{-1}\alpha_i j).$$

We conclude that $\alpha_{gi}^{-1}\alpha_i = 1$ for all $g, i \in G$ and so $\alpha_i = \alpha_{gi}$ for all $i, g \in G$. As the left action of $G$ on itself is transitive, we see that $\alpha_i = \alpha_j$ for all $i, j \in G$, and so $\delta \in \mathcal{S}_n(q)$. Then $Z_{\mathcal{MM}_n(q)}(\hat{G}_L) = \langle \hat{G}_L, \mathcal{S}_n(q)\rangle$. Clearly $\hat{G}_L \cap \mathcal{S}_n(q) = \{I_n\}$ and every element of $\mathcal{S}_n(q)$ commutes with $\hat{G}_L$. Then $\hat{G}_L, \mathcal{S}_n(q) \lhd \langle \hat{G}_L, \mathcal{S}_n(q)\rangle$ and so $\langle \hat{G}_L, \mathcal{S}_n(q)\rangle = \hat{G}_L \times \mathcal{S}_n(q)$. □

**Lemma 1.9** *Let G be a finite abelian group of order n, $S \subseteq S_G$ a set of permutations, and C a $\hat{G}$-invariant code over $\mathbb{F}_q$. Then the following are equivalent:*

*(1) S is a monomial solving set for C,*
*(2) whenever $\delta \in \mathcal{MM}_n(q)$ such that $\delta^{-1}\hat{G}_L\delta \leq \mathrm{MAut}(C)$, then there exists $s \in S$, and $v \in \mathrm{MAut}(C)$ such that $v^{-1}\delta^{-1}\hat{g}_L\delta v = s^{-1}\hat{g}_L s$ for every $g \in G$.*

*Proof* (1) implies (2). Let $\delta \in \mathcal{MM}_n(q)$ such that $\delta^{-1}\hat{G}_L\delta \leq \mathrm{MAut}(C)$. Then $\delta(C)$ is a $\hat{G}$-invariant code as $\mathrm{MAut}(\delta(C)) = \delta\mathrm{MAut}(C)\delta^{-1}$. As $S$ is a monomial solving set for $C$, $\delta(C) = s(C)$ for some $s \in S$. Thus $v = \delta^{-1}s \in \mathrm{MAut}(C)$ and if $g \in G$, then $(\delta^{-1}s)^{-1}\delta^{-1}\hat{g}_L\delta(\delta^{-1}s) = s^{-1}\hat{g}_L s$ as required.

(2) implies (1). Let $C'$ be a $\hat{G}_L$-invariant code with $\delta : C \to C'$ a monomial isomorphism. As $\hat{G}_L \leq \mathrm{MAut}(C')$, $\delta^{-1}\hat{G}_L\delta \leq \mathrm{MAut}(C)$. By hypothesis, there exists $s \in S$ and $v \in \mathrm{MAut}(C)$ such that $v^{-1}\delta^{-1}\hat{h}_L\delta v = s^{-1}\hat{h}_L s$ for every $h \in G$, or $sv^{-1}\delta^{-1}\hat{h}_L = \hat{h}_L sv^{-1}\delta^{-1}$. By Lemma 1.8, $sv^{-1}\delta^{-1} = \hat{g}_L T$ for some $g \in G$ and $T \in \mathcal{S}_n(q)$, and so $s = \hat{g}_L T\delta v$. Then $s(C) = \hat{g}_L T\delta v(C) = \hat{g}_L T\delta(C) = \hat{g}_L T(C') = C'$ as $\hat{g}_L, T \in \mathrm{MAut}(C')$. □

**Lemma 1.10** *Let $C$ be a $\hat{G}_L$-invariant linear code over $\mathbb{F}_q$, where $G$ has order $n$. Then the following are equivalent:*

*(1) if $S$ is a permutation solving set of $C$ then $S$ is a monomial solving set of $C$,*
*(2) whenever $C'$ is a $\hat{G}_L$-invariant code monomially isomorphic to $C$ with $\delta \in \mathcal{MM}_n(q)$ a monomial isomorphism, then there exists $\gamma \in \mathrm{MAut}(C)$ such that $\gamma^{-1}\delta^{-1}\hat{G}_L\delta\gamma \leq \mathrm{PAut}(C)$.*

*Proof* (1) implies (2). Let $S$ be a permutation solving set for $C$ such that $S$ is a monomial solving set for $C$, and $C'$ a $\hat{G}_L$-invariant code monomially isomorphic to $C$ with $\delta : C \mapsto C'$ a monomial isomorphism. By Lemma 1.9 there exists $s \in S$, and $v \in \mathrm{MAut}(C)$ such that $v^{-1}\delta^{-1}\hat{g}_L\delta v = s^{-1}\hat{g}_L s$ for every $g \in G$. As $s$ and $\hat{g}_L$ are both permutation matrices, setting $\gamma = v$ we see that $\gamma^{-1}\delta^{-1}G_L\delta\gamma \leq \mathrm{PAut}(C)$ as required.

(2) implies (1). Let $S$ be a permutation solving set of $C$, $C'$ a $\hat{G}_L$-invariant code monomially isomorphic to $C$ with $\delta \in \mathcal{MM}_n(q)$ a monomial isomorphism, and $\gamma \in \mathrm{MAut}(C)$ such that $\gamma^{-1}\delta^{-1}\hat{G}_L\delta\gamma \leq \mathrm{PAut}(C)$. Considering $\mathrm{PAut}(C)$ as a subgroup of the $|G| \times |G|$ permutation matrices identified with $S_G$, we have that $\hat{G}_L$ and $\gamma^{-1}\delta^{-1}\hat{G}_L\delta\gamma$ are isomorphic regular subgroups of $S_G$. By [2, Lemma 1.6B] $\hat{G}_L$ and $\gamma^{-1}\delta^{-1}\hat{G}_L\delta\gamma$ are equivalent permutation groups, and so there exists $\omega \in S_G$ such that $\omega^{-1}\hat{g}_L\omega = \gamma^{-1}\delta^{-1}\hat{g}_L\delta\gamma$ for every $g \in G$. By Lemma 1.6 there exists $v \in \mathrm{PAut}(C)$ and $s \in S$ such that

$$s^{-1}\hat{g}_L s = v^{-1}\omega^{-1}\hat{g}_L\omega v = v^{-1}\gamma^{-1}\delta^{-1}\hat{g}_L\delta\gamma v$$

for every $g \in G$. The result then follows by Lemma 1.9 as $\gamma v \in \mathrm{MAut}(C)$. □

The following conjugation result [3, Lemma 2.5] will be crucial. Before stating it, we will need some additional terminology. For terms regarding permutation groups not defined here, see [2].

**Definition 1.11** Let $G$ be a transitive group. We denote by $\mathrm{Stab}_G(x)$ the stabilizer of the element $x$ in the set on which $G$ acts, and for $B \in \mathcal{B}$, $\mathrm{Stab}_G(B)$ is the set-wise stabilizer of the block $B$. That is, $\mathrm{Stab}_G(x) = \{g \in G : g(x) = x\}$ and $\mathrm{Stab}_G(B) = \{g \in G : g(B) = B\}$. Define a partial order $\preceq$ on the set of all block systems of $G$ by $\mathcal{B} \preceq \mathcal{C}$ if and only if every block of $\mathcal{C}$ is a union of blocks of $\mathcal{B}$. We define $\mathcal{B}|_C$ to be the block system of $\mathrm{Stab}_G(C)$ consisting of all those blocks of $\mathcal{B}$ that are contained in $C$, $C \in \mathcal{C}$. By $\mathrm{fix}_G(\mathcal{B})$ we mean the subgroup of $G$ which fixes each block of $\mathcal{B}$ set-wise. That is, $\mathrm{fix}_G(\mathcal{B}) = \{g \in G : g(B) = B \text{ for all } B \in \mathcal{B}\}$. Finally, by $G/\mathcal{B}$ we mean the induced action of $G$ on $\mathcal{B}$. That is, for $g \in G$, $g/\mathcal{B}(B) = B'$ if and only if $g(B) = B'$, and $G/\mathcal{B} = \{g/\mathcal{B} : g \in G\}$. We remark that many authors denote this by $G^{\mathcal{B}}$.

**Definition 1.12** Let $n = \Pi_{i=1}^r p_i^{a_i}$ and $m = \Sigma_{i=1}^r a_i$. We will call $m$ the **exponent of** $n$. A transitive group $G$ of degree $n$ is $m$**-step imprimitive** if there exists a sequence of block systems $\mathcal{B}_0 \prec \mathcal{B}_1 \prec \ldots \prec \mathcal{B}_m$. A block system $\mathcal{B}$ will be said to be **normal** if $\mathcal{B}$ is formed by the orbits of a normal subgroup. We will say that $G$ is **normally** $m$**-step imprimitive** if each $\mathcal{B}_i$, $0 \leq i \leq m$, is formed by the orbits of a normal subgroup of $G$.

Note that the definition of $m$-step imprimitive implies that if $B_{i+1} \in \mathcal{B}_{i+1}$ and $B_i \in \mathcal{B}_i$, then $|B_{i+1}|/|B_i|$ is prime for every $0 \le i \le m-1$.

**Definition 1.13** Let $G$ be a permutation group acting on $X$ and $H$ a permutation group acting on $Y$. Define the **wreath product of** $G$ **and** $H$, denoted $G \wr H$, to be the group of all permutations of $X \times Y$ of the form $(x, y) \to (g(x), h_x(y))$.

The following result is also proven in [3]. The proof is included here for completeness.

**Lemma 1.14** *Let $n$ be a positive integer and $G_1, G_2$ be transitive abelian groups of degree $n$ such that $\langle G_1, G_2\rangle$ is $m$-step imprimitive. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ be the prime-power decomposition of $n$. Then there exists $\delta \in \langle G_1, G_2\rangle$ and a sequence of primes $q_1, \ldots, q_m$ such that $n = q_1 \cdots q_m$ and $\langle G_1, \delta^{-1}G_2\delta\rangle$ is permutation isomorphic to a subgroup of* $\mathrm{AGL}(1, q_1) \wr (\mathrm{AGL}(1, q_2) \wr (\cdots \wr \mathrm{AGL}(1, q_m)))$. *Furthermore, if $\langle G_1, G_2\rangle$ is solvable, then we may take $\delta = 1$.*

*Proof* We proceed by induction on $m$. If $m = 1$, then $n$ is prime, and both $G_1$ and $G_2$ are Sylow $n$-subgroups of $S_n$. Hence there exists $\delta \in \langle G_1, G_2\rangle$ such that $\delta^{-1}G_2\delta = G_1$, and the result is trivial as $\langle G_1, \delta^{-1}G_2\delta\rangle$ is cyclic of order $n$. If $\langle G_1, G_2\rangle$ is solvable, then the result follows by [2, Exercise 3.5.1]. Now assume that the result is true for all $m - 1 \ge 1$, and let $G_1, G_2$ be transitive abelian groups of degree $n$, where $n$ has exponent $m$, such that $\langle G_1, G_2\rangle$ is $m$-step imprimitive.

As $\langle G_1, G_2\rangle$ is $m$-step imprimitive, $\langle G_1, G_2\rangle$ admits a normal block system $\mathcal{B}$ consisting of $n/q_m$ blocks of size $q_m$ for some prime $q_m|n$, and both $G_1/\mathcal{B}$ and $G_2/\mathcal{B}$ are transitive abelian groups of degree $n/q_m$ and exponent $m - 1$. Note that $\mathcal{B}$ is normal as every block system of a permutation group that contains a regular abelian subgroup is normal. Furthermore, as $\langle G_1, G_2\rangle$ is $m$-step imprimitive, $\langle G_1, G_2\rangle/\mathcal{B}$ is $(m - 1)$-step imprimitive by [6, Lemma 8], so by the induction hypothesis, there exists $\delta_1 \in \langle G_1, G_2\rangle$ such that $\langle G_1, \delta_1^{-1}G_2\delta\rangle/\mathcal{B}$ is permutation isomorphic to a subgroup of $\mathrm{AGL}(1, q_1) \wr (\mathrm{AGL}(1, q_2) \wr (\cdots \wr \mathrm{AGL}(1, q_{m-1})))$ for some sequence of primes $q_1, \ldots, q_{m-1}$ such that $n/q_m = q_1 \cdots q_{m-1}$, and if $\langle G_1, G_2\rangle$ is solvable, we may take $\delta_1 = 1$. Furthermore, $\mathrm{fix}_{G_1}(\mathcal{B})$ is semiregular of order $q_m$, and $\mathrm{fix}_{\delta_1^{-1}G_2\delta_1}(\mathcal{B})$ is also semiregular of order $q_m$. Hence there exists $\delta_2 \in \mathrm{fix}_{\langle G_1, \delta_1^{-1}G_2\delta_1\rangle}(\mathcal{B})$ such that $\delta_2^{-1}\mathrm{fix}_{\delta_1^{-1}G_2\delta_1}(\mathcal{B})\delta_2$ is contained in the same Sylow $q_m$-subgroup of $\mathrm{fix}_{\langle G_1, \delta_1^{-1}G_2\delta_1\rangle}(\mathcal{B})$ as $\mathrm{fix}_{G_1}(\mathcal{B})$. If $\langle G_1, G_2\rangle$ is solvable, then $\mathrm{fix}_{\langle G_1, G_2\rangle}(\mathcal{B})$ is solvable, so $\mathrm{fix}_{\langle G_1, G_2\rangle}(\mathcal{B})|_B$ is solvable for every $B \in \mathcal{B}$, and by [2, Exercise 3.5.1], $\mathrm{fix}_{\langle G_1, G_2\rangle}(\mathcal{B})|_B$ has a unique Sylow $q_m$-subgroup for every $B \in \mathcal{B}$. Hence we may take $\delta_2 = 1$. Let $\delta = \delta_1\delta_2$. As a Sylow $q_m$-subgroup of $\mathrm{fix}_{\langle G, \delta^{-1}G\delta\rangle}(\mathcal{B})$ is contained in $1_{S_{n/q_m}} \wr \mathbb{Z}_{q_m}$ we have that both $G_1$ and $\delta^{-1}G_2\delta$ normalize $1_{S_{n/q_m}} \wr \mathbb{Z}_{q_m}$. This then implies that $\mathrm{Stab}_{\langle G_1, \delta^{-1}G_2\delta\rangle}(B)|_B$ has a normal Sylow $q_m$-subgroup, so that $\mathrm{Stab}_{\langle G_1, \delta^{-1}G_2\delta\rangle}(B)|_B$ is permutation isomorphic to a subgroup of $\mathrm{AGL}(1, q_m)$ for every $B \in \mathcal{B}$. It then follows by the Embedding Theorem [15, Theorem 2.6], that $\langle G_1, \delta^{-1}G_2\delta\rangle$ is permutation isomorphic to a subgroup of $\mathrm{AGL}(1, q_1) \wr (\mathrm{AGL}(1, q_2) \wr (\cdots \wr \mathrm{AGL}(1, q_m)))$, and the result follows by induction. □

## 2 The main results

We now give conditions under which every permutation solving set for a code over $\mathbb{F}_q$ is also a monomial solving set.

**Theorem 2.1** *Let $G$ be an abelian group of order $n$ such that whenever $\delta \in S_G$ then there exists $\gamma \in \langle G_L, \delta^{-1}G_L\delta\rangle$ such that $\langle G_L, \gamma^{-1}\delta^{-1}G_L\delta\gamma\rangle$ is normally $m$-step imprimitive.*

*Let $q$ be a prime-power such that* $\gcd(n, q-1) = 1$*, and $C$ be a $\hat{G}$-invariant code over $\mathbb{F}_q$. Then every permutation solving set for $C$ is also monomial solving set for $C$.*

*Proof* By Lemma 1.10, we must show that whenever $C'$ is a $\hat{G}_L$-invariant code monomially isomorphic to $C$ with $\delta \in \mathcal{MM}_n(q)$ a monomial isomorphism, then there exists $\gamma \in \mathrm{MAut}(C)$ such that $\gamma^{-1}\delta^{-1}\hat{G}_L\delta\gamma \le \mathrm{PAut}(C)$. Let $\delta = PD$, where $P \in \mathcal{P}_n(q)$ and $D \in \mathcal{D}_n(q)$. By hypothesis, there exists $\gamma \in \mathrm{MAut}(C)$ such that $\langle \hat{G}_L, \delta^{-1}\gamma^{-1}\hat{G}_L\gamma\delta\rangle/\mathbb{F}_q$ is normally $m$-step imprimitive, so we assume without loss of generality that $\langle \hat{G}_L, \delta^{-1}\hat{G}_L\delta\rangle/\mathbb{F}_q$ is normally $m$-step imprimitive. After an additional conjugation, we may additionally assume by Lemma 1.14 that there is a sequence of primes $q_1, \ldots, q_m$ such that $n = q_1 \cdots q_m$ and $\langle \hat{G}_L, \delta^{-1}\hat{G}_L\delta\rangle/\mathbb{F}_q$ is permutation isomorphic to a subgroup of $\mathrm{AGL}(1, q_1) \wr (\mathrm{AGL}(1, q_2) \wr (\cdots \wr \mathrm{AGL}(1, q_m)))$, which is solvable.

Let $\pi$ be the set of primes dividing $n$. As $\langle \hat{G}_L, \delta^{-1}\hat{G}_L\delta\rangle/\mathbb{F}_q$ and $\mathbb{F}_q^*$ are solvable, $\langle \hat{G}_L, \delta^{-1}\hat{G}_L\delta\rangle \le (\langle \hat{G}_L, \delta^{-1}\hat{G}_L\delta\rangle)/\mathbb{F}_q \wr \mathbb{F}_q^*$ is solvable. Then $\langle \hat{G}_L, \delta^{-1}\hat{G}_L\delta\rangle$ contains a Hall $\pi$-subgroup, and so $\hat{G}_L$ and $\delta^{-1}\hat{G}_L\delta$ are contained in Hall $\pi$-subgroups $H_1$ and $H_2$ of $\langle \hat{G}_L, \delta^{-1}\hat{G}_L\delta\rangle$, respectively. By Hall's Theorem, [12, Proposition II.7.14], after an appropriate conjugation, we may assume without loss of generality that $H_1 = H_2$ and so $\langle \hat{G}_L, \delta^{-1}\hat{G}_L\delta\rangle$ is a $\pi$-group. Now let $g, h \in G$. Then there exists $\ell \in G$ such that $(\delta^{-1}\hat{g}_L\delta\hat{\ell}_L/\mathbb{F}_q)(h) = h$. As no prime divisor of $q-1$ divides $|\delta^{-1}\hat{g}_L\delta\hat{\ell}_L|$, we see that the action of $\delta^{-1}\hat{g}_L\delta\hat{\ell}_L$ on a codeword in the coordinate corresponding to $h$ is the identity. As $h \in G$ was arbitrary, this then implies that $\delta^{-1}\hat{g}_L\delta \in \mathrm{PAut}(C)$, and so $\langle \hat{G}_L, \delta^{-1}\hat{G}_L\delta\rangle \le \mathrm{PAut}(C)$ as required. □

**Corollary 2.2** *Let $G$ be a cyclic group of order $n$ or an abelian group of prime-power order $n$. Then for any $\hat{G}$-invariant code $C$ over $\mathbb{F}_q$ a permutation solving set for $C$ is also a monomial solving set for $C$ if* $\gcd(n, q-1) = 1$*. Additionally, when $G$ is cyclic, for any cyclic code $C$ of length $n$ over $\mathbb{F}_q$ a permutation solving set for $C$ is a monomial solving set for $C$ if and only if* $\gcd(n, q-1) = 1$.

*Proof* For the first statement, in view of Theorem 2.1, we need only show that whenever $\delta \in S_G$ then there exists $\gamma \in \langle G_L, \delta^{-1}G_L\delta\rangle$ such that $\langle G_L, \gamma^{-1}\delta^{-1}G_L\delta\gamma\rangle$ is normally $m$-step imprimitive. That this is true for cyclic groups $\mathbb{Z}_n$ is [20, Theorem 4.9]. For groups $G$ of prime-power order $p^\ell$, $p$ a prime, by a Sylow Theorem there exists $\gamma \in \langle G_L, \delta^{-1}G_L\delta\rangle$ such that $\langle G_L, \gamma^{-1}\delta^{-1}G_L\delta\gamma\rangle$ is a $p$-group. It is then easy to show using induction that a transitive $p$-group of degree $p^\ell$ is genuinely $\ell$-step imprimitive using the fact that the center contains an element of order $p$ and the orbits of a normal subgroup form a block system [24, Proposition 7.1].

Additionally, we need only show the converse of the if and only if statement. If $G$ is cyclic and $\gcd(n, q-1) \ne 1$, then by Example 1.1 there exists monomially isomorphic cyclic codes that are not permutationally isomorphic. □

**Corollary 2.3** *Let $G$ be a cyclic group of order $n$ or an abelian group of prime-power order $n$. If* $\gcd(n, q(q-1)) = 1$*, and $C$ is a $\hat{G}$-invariant code over $\mathbb{F}_q$, then every permutation solving set $S$ for $C$ is also monomial solving set for $C$ and $\psi(S)$ is the solving set of a Cayley color digraph of $G$.*

*Proof* In view of Corollary 2.2, we need only show that if $\gcd(n, q) = 1$, then $\psi(S)$ is a solving set for a Cayley digraph of $G$. This follows by Theorem 1.7. □

As Muzychuk has solved the isomorphism problem for circulant color digraphs [16], the following result holds.

**Corollary 2.4** *Let $n$ be an integer and $q$ a prime-power such that* $\gcd(n, q(q-1)) = 1$. *Let $C$ be a cyclic code of length $n$ over $\mathbb{F}_q$. Then a monomial solving set for $C$ is known.*

We say that a pair $(G, \mathbb{F}_q)$ is an **MCI-pair** if every $\hat{G}_L$-invariant code over $\mathbb{F}_q$ is an MCI-code.

**Corollary 2.5** *Let $q$ be a prime-power and $G = \mathbb{Z}_n$, $\mathbb{Z}_{2n}$, or $\mathbb{Z}_p^{\ell}$, $1 \leq \ell \leq 4$, where $n$ is square-free and $p$ is an odd prime. If* $\gcd(n, q(q-1)) = 1$ *in the former case and* $\gcd(p, q(q-1)) = 1$ *in the latter case, then $(G, \mathbb{F}_q)$ is an MCI-pair. Additionally, if* $\gcd(p, q(q-1)) = 1$, *then any $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$-invariant code over $\mathbb{F}_q$ is either an MCI-code, or is also a $\mathbb{Z}_p^3$-invariant code, and is an MCI-code with respect to $\mathbb{Z}_p^3$.*

*Proof* If $n$ is square-free, then $\mathbb{Z}_n$ and $\mathbb{Z}_{2n}$ are CI-groups with respect to color digraphs [18,19]. Additionally, $\mathbb{Z}_p$, $\mathbb{Z}_p^2$, $\mathbb{Z}_p^3$, and $\mathbb{Z}_p^4$ are CI-groups with respect to color digraphs [4,8,9,23]. Finally, it was shown in [5] that every Cayley color digraph of $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ is either a CI-color digraph of $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$, or is a Cayley color digraph of $\mathbb{Z}_p^3$. The result then follows by Corollary 2.3. □

## 3 Monomail isomorphisms of codes of prime length

We now turn to monomial isomorphisms of cyclic codes of prime length $p$ over fields $\mathbb{F}_q$ where the arithmetic conditions of Corollary 2.5 are not satisfied. That is, when $p|(q-1)$ or $q$ is a power of $p$. We will consider the two cases separately. The following result shows that, in some sense, the codes given in Example 1.1 are the "only" codes of prime length $p$ which are not permutationally isomorphic when $p|(q-1)$. In what follows, we denote the $p \times p$ diagonal matrix with entries $\alpha_1, \ldots, \alpha_p$ on the main diagonal by $\mathrm{diag}(\alpha_1, \ldots, \alpha_p)$.

**Theorem 3.1** *Let $p$ be prime and $q$ a prime-power such that $p|(q-1)$. Let $C$ and $C'$ be cyclic codes of length $p$ over $\mathbb{F}_q$. Let $\alpha \in \mathbb{F}_q^*$ be of order $p$, and $s$ a generator of $\mathbb{F}_p^*$. Then $C$ and $C'$ are monomially isomorphic if and only if they are monomially isomorphic by an element of $\langle P, D\rangle$, where $P \in \mathcal{P}_p(q)$ such that $\psi(P)(i) = si$ and* $D = \mathrm{diag}(1, \alpha, \alpha^2, \ldots, \alpha^{p-1})$.

*Proof* Let $\delta : C \to C'$ be a monomial isomorphism. Note that $(\hat{\mathbb{Z}}_p)_L = \langle \hat{1}_L\rangle$, and hence $\delta^{-1}\langle \hat{1}_L\rangle\delta \leq \mathrm{MAut}(C)$. Then $\langle \hat{1}_L\rangle/\mathbb{F}_q$ and $\delta^{-1}\langle \hat{1}_L\rangle\delta/\mathbb{F}_q$ are Sylow $p$-subgroups of $\mathrm{PAut}(C)$ and so there exists $\gamma \in \mathrm{MAut}(C)$ such that $\langle \gamma^{-1}\delta^{-1}\hat{1}_L\delta\gamma\rangle/\mathbb{F}_q = \langle \hat{1}_L\rangle/\mathbb{F}_q$. Thus $\delta\gamma/\mathbb{F}_q$ normalizes $\langle \hat{1}_L\rangle/\mathbb{F}_q$, and hence $(\delta\gamma/\mathbb{F}_q)(i) = ai + b$, where $a \in \mathbb{Z}_p^*$ and $b \in \mathbb{Z}_p$. As $\hat{1}_L \in \mathrm{MAut}(C)$, we assume without loss of generality that $b = 0$. Let $\delta\gamma = RA$, where $R \in \mathcal{P}_p(q)$ and $A \in \mathcal{D}_p(q)$. Note that $\psi(R)(i) = ai$. If $C$ is trivial (that is, either consisting of the 0 codeword or the entire space $\mathbb{F}_q^p$), then $A \in \mathrm{MAut}(C)$ so that $R$ is a monomial isomorphism from $C$ to $C'$, and the result follows. We thus assume without loss of generality that $C$ is nontrivial. Then $\gamma^{-1}\delta^{-1}\hat{1}_L\delta\gamma = QE$, where $Q \in \mathcal{P}_p(q)$ and $\psi(Q)(i) = i + a^{-1}$, and $E \in \mathcal{D}_p(q)$. Then $E = \hat{1}_L^{-a^{-1}}\gamma^{-1}\delta^{-1}\hat{1}_L\delta\gamma$ is a diagonal automorphism of $C$, so by [13, Theorem 1.3] we have that $E$ is scalar.

Now, $R(C)$ is a cyclic code of length $p$ over $\mathbb{F}_q$. Clearly $R(C)$ is monomially isomorphic to $C'$ by $A$. Further, it is easy to see that $C$ and $C'$ are monomially isomorphic by an element of $\langle P, D\rangle$ if and only if $R(C)$ and $C'$ are monomially isomorphic by an element of $\langle P, D\rangle$ as $R \in \langle P, D\rangle$. We thus assume without loss of generality that $R = 1$. If $A$ is scalar, then the result follows, so we also assume without loss of generality that $A$ is not scalar.

Let $A = \mathrm{diag}(\alpha_0, \alpha_1, \ldots, \alpha_{p-1})$. A straightforward computation will now show that

$$E = \mathrm{diag}(\alpha_0\alpha_1^{-1}, \alpha_1\alpha_2^{-1}, \ldots, \alpha_{p-2}\alpha_{p-1}^{-1}, \alpha_{p-1}\alpha_0^{-1}) \in \mathrm{MAut}(C).$$

As every scalar matrix is an automorphism of every cyclic code, we may assume without loss of generality that $\alpha_0 = 1$. As $A$ is not scalar, it the follows that $|A| \neq 1$. As $E$ is scalar, $\alpha_i\alpha_{i+1}^{-1} = \alpha_j\alpha_{j+1}^{-1}$ for all $i, j \in \mathbb{Z}_p$. Also, as $|\gamma^{-1}\delta^{-1}\hat{1}_L\delta\gamma| = p$, and $\gamma^{-1}\delta^{-1}\hat{1}_L\delta\gamma = \hat{1}_L E = E\hat{1}_L$ as $E$ is scalar, we see that $|E|$ divides $p$. As $A$ is not scalar, $|E| \neq 1$ and so $|E| = p$. As $\mathbb{F}_q^*$ is cyclic and so has a unique subgroup of order $p$, we may assume without loss of generality that $\alpha_i\alpha_{i+1}^{-1} = \alpha^{-1}$ for all $i \in \mathbb{Z}_p$. As $\alpha_0 = 1$, we then have that $\alpha_1^{-1} = \alpha^{-1}$, so that $\alpha_1 = \alpha$. If $\alpha_i^{-1} = \alpha^{-i}$, then $\alpha^{-1} = \alpha_i\alpha_{i+1}^{-1}$ and so $\alpha_{i+1} = \alpha^{i+1}$. Hence $A = D$, and the result follows. □

The following result solves the monomial isomorphism problem for cyclic codes of length $p$ over $\mathbb{F}_{p^a}$, $a \geq 1$, with $n = p$ as $\gcd(p, p^a - 1) = 1$.

**Theorem 3.2** *Let $G$ be a CI-group of order $n$ and $p|n$ a prime. If* $\gcd(n, p^a - 1) = 1$*, then $(G, p^a)$ is an MCI-pair. In particular, $(\mathbb{Z}_p, p^a)$ is an MCI-pair for every $a \geq 1$.*

*Proof* Let $C$ be a $\hat{G}$-invariant code over $\mathbb{F}_{p^a}$, and $C'$ a $\hat{G}_L$-invariant code monomially isomorphic to $C$ with $\delta$ a monomial isomorphism. As $G$ is a CI-group, there exists $\gamma_1 \in \mathrm{MAut}(C)$ such that $\gamma_1^{-1}\delta^{-1}\hat{G}_L\delta\gamma_1/\mathbb{F}_{p^a} = \hat{G}_L/\mathbb{F}_{p^a}$. Then $\xi(\langle \hat{G}_L, \gamma_1^{-1}\delta^{-1}\hat{G}_L\delta\gamma_1\rangle) \leq G_L \wr \mathbb{F}^*_{p^a}$ is of order dividing $n \cdot (p^a - 1)^n$, and is solvable as by Theorem 1.4 $G$ is solvable. Let $\pi$ be the set of primes dividing $n$. As $\gcd(n, p^a - 1) = 1$, we see that both $\hat{G}$ and $\gamma_1^{-1}\delta^{-1}\hat{G}_L\delta\gamma_1$ are Hall $\pi$-subgroups of $\langle \hat{G}_L, \gamma_1^{-1}\delta^{-1}\hat{G}_L\delta\gamma_1\rangle$, and so by Hall's Theorem there exists $\gamma_2 \in \langle \hat{G}_L, \gamma_1^{-1}\delta^{-1}\hat{G}_L\delta\gamma_1\rangle$ such that $\gamma_2^{-1}\gamma_1^{-1}\delta^{-1}\hat{G}_L\delta\gamma_1\gamma_2 = \hat{G}_L$. Setting $\gamma = \gamma_1\gamma_2$, we see by Theorem 2.1 that a monomial solving set for $C$ is a permutation solving set for $C$, and by Lemma 1.9, $C$ is an MCI-code with respect to $G$. □

**Acknowledgments** The author is indebted as usual to the anonymous referees whose careful reading resulted in suggestions which greatly improved the manuscript.

## References

1. Babai L.: Isomorphism problem for a class of point-symmetric structures. Acta Math. Acad. Sci. Hung. **29**(3–4), 329–336 (1977).
2. Dixon J.D., Mortimer B.: Permutation Groups. Graduate Texts in Mathematics, vol. 163. Springer, New York (1996).
3. Dobson E.: On the Cayley isomorphism problem for Cayley objects of nilpotent groups of some orders (submitted).
4. Dobson E.: Isomorphism problem for Cayley graphs of $\mathbb{Z}_p^3$. Discret. Math. **147**(1–3), 87–94 (1995).
5. Dobson E.: Classification of vertex-transitive graphs of order a prime cubed. I. Discret. Math. **224**(1–3), 99–106 (2000).
6. Dobson E.: On isomorphisms of abelian Cayley objects of certain orders. Discret. Math. **266**(1–3), 203–215 (2003) The 18th British Combinatorial Conference (Brighton, 2001).
7. Filip P., Heise W.: Monomial Code-Isomorphisms, Combinatorics '84 (Bari, 1984). North-Holland Mathematics Study vol. 123, pp. 217–223, North-Holland, Amsterdam (1986).
8. Godsil C.D.: On Cayley graph isomorphisms. Ars Comb. **15**, 231–246 (1983).
9. Hirasaka M., Muzychuk M.: An elementary abelian group of rank 4 is a CI-group. J. Comb. Theory Ser. A **94**(2), 339–362 (2001).
10. Huffman W.C., Job V., Pless V.: Multipliers and generalized multipliers of cyclic objects and cyclic codes. J. Comb. Theory Ser. A **62**(2), 183–215 (1993).

11. Huffman W.C., Pless V.: Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge (2003).
12. Hungerford T.W.: Algebra. Graduate Texts in Mathematics, vol. 73, Springer, New York (1980); reprint of the 1974 original.
13. Knapp W., Schmid P.: Codes with prescribed permutation group. J. Algebra **67**(2), 415–435 (1980).
14. Li C.H.: The finite primitive permutation groups containing an abelian regular subgroup. Proc. Lond. Math. Soc. **87**(3), 725–747 (2003).
15. Meldrum J.D.P.: Wreath Products of Groups and Semigroups, Pitman Monographs and Surveys in Pure and Applied Mathematics, vol. 74. Longman, Harlow (1995).
16. Muzychuk M.: A solution of the isomorphism problem for circulant graphs. Proc. Lond. Math. Soc. **88**(3), 1–41 (2004).
17. Muzychuk M.: A solution of an equivalence problem for semisimple cyclic codes, ArXiv:1105.4320v1 (2011).
18. Muzychuk M.: Ádám's conjecture is true in the square-free case. J. Comb. Theory Ser. A **72**(1), 118–134 (1995).
19. Muzychuk M.: On Ádám's conjecture for circulant graphs. Discret. Math. **176**(1–3), 285–298 (1997).
20. Muzychuk M.: On the isomorphism problem for cyclic combinatorial objects. Discret. Math. **197/198**, 589–606 (1999). 16th British Combinatorial Conference (London, 1997).
21. Pálfy P.P.: Isomorphism problem for relational structures with a cyclic automorphism. Eur. J. Combin. **8**(1), 35–43 (1987).
22. Sendrier N., Simos D.E.: How easy is code equivalence over $\mathbb{F}_q$?, preprint.
23. Turner J.: Point-symmetric graphs with a prime number of points. J. Comb. Theory **3**, 136–145 (1967).
24. Wielandt H.: Finite Permutation Groups, Translated from the German by R. Bercov, Academic Press, New York (1964).