Automorphism groups of cyclic codes

Rolf Bienert · Benjamin Klopsch

Abstract In this article we study the automorphism groups of binary cyclic codes. In particular, we provide explicit constructions for codes whose automorphism groups can be described as (a) direct products of two symmetric groups or (b) iterated wreath products of several symmetric groups. Interestingly, some of the codes we consider also arise in the context of regular lattice graphs and permutation decoding.

Keywords Binary cyclic codes · Automorphism groups

1 Introduction

In coding theory one frequently establishes in a natural way a connection between codes and groups. For instance, a group acting on a code may provide valuable insights into the structure of the code, as with the Mathieu groups acting on the Golay codes.

Let $\mathcal{C}$ be a binary linear code of length N over $\mathbb{F}_2$. Up to isomorphism, this simply means that $\mathcal{C}$ is a subspace of the standard vector space $\mathbb{F}_2^N$ of dimension N over the prime field $\mathbb{F}_2$ of characteristic 2. There is a natural action of the symmetric group $\mathrm{Sym}(N)$ of degree N on $\mathbb{F}_2^N$ by means of coordinate permutations. The automorphism group $\mathrm{Aut}(\mathcal{C})$ of $\mathcal{C}$ is the subgroup of $\mathrm{Sym}(N)$ consisting of all permutations which map the subspace $\mathcal{C}$ into itself. (In general, there are several ways of associating an automorphism group to a linear code, but the distinctions between these variations

R. Bienert
Mathematisches Institut, Heinrich-Heine-Universität Düsseldorf, 40225 Düsseldorf, Germany
e-mail: Rolf.Bienert@t-online.de

B. Klopsch (✉)
Department of Mathematics, Royal Holloway, University of London, Egham TW20 0EX, UK
e-mail: Benjamin.Klopsch@rhul.ac.uk

disappear in the context of binary linear codes; cf. [3, Section 1.5].) It can be shown that every finite group arises as the automorphism group of a suitable binary linear code; cf. [9]. The question which finite permutation groups, i.e. finite groups with a fixed faithful permutation representation, arise as automorphism groups of binary linear codes is more subtle; a possible approach to this problem was indicated in [7].

Recall that the binary linear code $\mathcal{C}$ of length N is said to be cyclic if its automorphism group contains a regular cycle of length N. The class of binary cyclic codes is both of theoretical and of practical interest, containing well-known families of codes such as the quadratic residue codes. It turns out that the class of groups which occur as automorphism groups of cyclic codes is much more restricted. Indeed, one motivating force behind our work is the natural and fundamental

Problem *Determine the class of finite groups which arise as the automorphism groups of* (*binary*) *cyclic codes.*

We bracket the word 'binary', because it would be equally interesting to investigate the problem for other ground fields. Moreover, one can ask a corresponding question for permutation groups rather than groups; cf. Theorem E below.

We now give a summary of our results. First we exhibit two explicit families of groups which do not arise as automorphism groups of binary cyclic codes.

Proposition A *The automorphism group of a binary cyclic code is not isomorphic* (*as an abstract group*) *to a non-trivial cyclic group of odd order.*

Theorem B *The automorphism group of a binary cyclic code is not isomorphic* (*as an abstract group*) *to an alternating group* Alt(n) *of degree* $n \in \{3, 4, 5, 6, 7\}$ *or* $n \geq 9$. *The group* Alt(8) *occurs as the automorphism group of a binary cyclic code of length* 15.

The exceptional appearance of Alt(8) can be explained by the isomorphism Alt(8) $\cong$ PSL(4, 2) = PΓL(4, 2); cf. our remarks following Theorem E.

Extensive computer calculations show that the automorphism groups of binary cyclic codes can often be described as iterated wreath products of symmetric groups; see [2] for a systematic account of automorphism groups of binary cyclic codes up to length 70. We provide an explicit construction of codes with a prescribed automorphism group of this type.

Theorem C *Let* $r \in \mathbb{N}$, *and let* $n_1, \ldots, n_r \in \mathbb{N}_{\geq 3}$ *be odd. Let* $G := \mathrm{Sym}(n_1) \wr \ldots \wr \mathrm{Sym}(n_r)$ *be the iterated wreath product of symmetric groups of degrees* $n_1, \ldots, n_r$. *Then there exists a binary cyclic code* $\mathcal{C}$ *of length* $N := n_1 \cdots n_r$ *such that* Aut($\mathcal{C}$) $\cong$ G.

It remains an open problem to construct binary cyclic codes such that the corresponding automorphism groups are iterated wreath products of symmetric groups of arbitrary degrees. The computational evidence suggests that such products occur frequently, but that extra care must be taken if the product is to involve as factors the symmetric group of degree 2. A few explicit examples are given in Section 8.

More rarely, one encounters codes whose automorphism group is a direct product of two symmetric groups. Again we are able to offer an explicit construction of binary linear codes $C_0(a, b)$, parameterised by $a, b \in \mathbb{N}$ with $a \leq b$, whose automorphism groups are of this type; for exceptional values of a, b the automorphism groups are, in fact, slightly larger. A detailed description of the family of codes $C_0(a, b)$ is given in Propositions 3.1, 3.2 and Corollary 3.3. As a consequence we record

Theorem D *Let $a, b \in \mathbb{N}$ with $2 < a < b$ and $\gcd(a, b) = 1$. Then there exist binary cyclic codes C such that $\mathrm{Aut}(C) \cong \mathrm{Sym}(a) \times \mathrm{Sym}(b)$.*

Interestingly, some of the codes $C_0(a, b)$ were recently studied by Key and Seneviratne in the context of regular lattice graphs and permutation decoding. In fact, we provide a new, unified treatment of a related family $C_1(a, b)$ of binary linear codes whose study was initiated in [5]. Our approach leads to a complete description of the automorphism groups of these codes, allowing us, for instance, to decide which of the codes $C_1(a, b)$ are cyclic. A detailed description of the family of codes $C_1(a, b)$ is given in Propositions 4.1, 4.2 and 4.3.

Finally, we use results from the well-developed theory of permutation groups and modular permutation representations to give a description of the primitive permutation groups which occur as automorphism groups of binary cyclic codes.

Theorem E *Let $G \leq \mathrm{Sym}(N)$ be the automorphism group of a binary cyclic code C, and suppose that G is a primitive permutation group. Then one of the following holds.*

(1) $C_p \lneqq G \lneqq \mathrm{AGL}(1, p)$ *where $p = N \geq 5$ is a prime.*
(2) $G = \mathrm{Sym}(N)$; *in this case C is one of four elementary codes.*
(3) $G = \mathrm{P\Gamma L}(d, q)$ *where $d \geq 3$, $q = 2^k$ for $k \in \mathbb{N}$ and $N = (q^d - 1)/(q - 1)$.*
(4) $G = M_{23}$ *and $N = 23$.*

Moreover, each of the groups listed in (2)–(4) *does occur as the automorphism group of a suitable binary cyclic code.*

It remains an open problem to find out precisely which subgroups of affine groups occur as automorphism groups of binary cyclic codes. This appears to be essentially a question in combinatorial number theory. Computer calculations show that, for instance, there exists a binary cyclic [17, 8, 6]-code whose automorphism group is $C_8 \ltimes C_{17} \leq \mathrm{AGL}(1, 17)$. More explicit examples are given in Section 8.

Part (3) of Theorem E can be regarded as a generalisation of the well-known fact that the automorphism group of the binary Hamming code of length $2^d - 1$ is $\mathrm{PSL}(d, 2) = \mathrm{P\Gamma L}(d, 2)$.

Organisation The paper is divided into eight sections. Section 2 contains a brief summary of general notions and terminology as well as the constructions of the specific code families $C_0(a, b)$, $C_1(a, b)$ and $\mathcal{K}(n_1, \ldots, n_r)$. Propositions 3.1, 3.2 and Corollary 3.3 in Section 3 describe the structure of the codes $C_0(a, b)$ and imply Theorem D. Propositions 4.1, 4.2 and 4.3 in Section 4 describe the structure of the codes

$\mathcal{C}_1(a, b)$ related to rectangular lattice graphs. In Section 5 we determine the automorphism groups of the codes $\mathcal{K}(n_1, \ldots, n_r)$ and thereby prove Theorem C. Proposition A and Theorem B are established in Section 6. In Section 7 we describe the primitive permutation groups which occur as automorphism groups of binary cyclic codes, thus proving Theorem E. Finally, in Section 8 we give several examples of binary cyclic codes with automorphism groups which are not fully explained by the results in this paper.

2 Preliminaries and basic set-up

2.1 General notions

Let Ω be a finite set of size $N := |\Omega|$. Consider an N-dimensional vector space $\mathcal{V}$ over the field $\mathbb{F}_2$, with a fixed *standard basis* $\mathbf{e}_\omega$ indexed by $\omega \in \Omega$. Binary linear codes $\mathcal{C}$ of length N can then be constructed as subspaces of $\mathcal{V}$ with respect to the standard basis. As the standard basis is indexed by elements of the set Ω we regard the automorphism group $\text{Aut}(\mathcal{C})$ of any linear code $\mathcal{C} \leq \mathcal{V}$ as a subgroup of $\text{Sym}(\Omega) \cong \text{Sym}(N)$.

The *support* and the *weight* of $\mathbf{v} = \sum_{\omega \in \Omega} v_\omega \mathbf{e}_\omega \in \mathcal{V}$ are defined as

$$\text{supp}(\mathbf{v}) := \{\omega \in \Omega \mid v_\omega \neq 0\} \quad \text{and} \quad \text{wt}(\mathbf{v}) := |\text{supp}(\mathbf{v})|.$$

The *common weight* of $\mathbf{v}, \mathbf{w} \in \mathcal{V}$ is defined as

$$\text{com}(\mathbf{v}, \mathbf{w}) := |\text{supp}(\mathbf{v}) \cap \text{supp}(\mathbf{w})|,$$

Clearly, the weight and common weight functions are invariant under coordinate permutations. The *weight spectrum* and the *minimum distance* of a linear code $\mathcal{C} \leq \mathcal{V}$ are given by

$$\text{wspec}(\mathcal{C}) := \{\text{wt}(\mathbf{v}) \mid \mathbf{v} \in \mathcal{C}\} \quad \text{and} \quad d(\mathcal{C}) := \min(\text{wspec}(\mathcal{C}) \setminus \{0\}).$$

The *co-weight* of $\mathbf{v} \in \mathcal{V}$ is defined as

$$\text{co-wt}(\mathbf{v}) := |\Omega \setminus \text{supp}(\mathbf{v})| = N - \text{wt}(\mathbf{v}).$$

We call $\widehat{d}(\mathcal{C}) := \min\{\text{co-wt}(\mathbf{v}) \mid \mathbf{v} \in \mathcal{C}\}$ the *minimum co-distance* of $\mathcal{C}$.

We call an element $\mathbf{v} \in \mathcal{C}$ *decomposable* if it can be written as $\mathbf{v} = \mathbf{w}_1 + \mathbf{w}_2$ where $\mathbf{w}_1, \mathbf{w}_2 \in \mathcal{C} \setminus \{\mathbf{0}\}$ with $\text{supp}(\mathbf{w}_1) \cap \text{supp}(\mathbf{w}_2) = \varnothing$. An element of $\mathcal{C}$ is *indecomposable* if it is non-zero and not decomposable. Clearly, any element of $\mathcal{C}$ of minimum weight $d(\mathcal{C})$ is indecomposable, and the set of indecomposable elements is invariant under the action of $\text{Aut}(\mathcal{C})$.

2.2 The codes $\mathcal{C}_0(a, b)$ and $\mathcal{C}_1(a, b)$

Let $a, b \in \mathbb{N}$ with $a \leq b$, and set $\Omega := \{1, \ldots, a\} \times \{1, \ldots, b\}$ so that $N := |\Omega| = ab$. Consider the N-dimensional vector space $\mathcal{V} := \text{Mat}(a, b, \mathbb{F}_2)$ of all $a \times b$ matrices over the field $\mathbb{F}_2$. As a *standard basis* of $\mathcal{V}$ we fix

$$\{\mathbf{e}_{ij} \mid (i, j) \in \Omega\}, \qquad \text{where } \mathbf{e}_{ij} := (\delta_{ik}\delta_{jl})_{kl} \in \text{Mat}(a, b, \mathbb{F}_2)$$

denotes the elementary matrix whose (k, l)-entry equals 1 if $(k, l) = (i, j)$ and 0 otherwise.

In order to construct specific binary linear codes $\mathcal{C}_0(a, b)$ and $\mathcal{C}_1(a, b)$ of length N as subspaces of $\mathcal{V}$ we define the *elementary row matrices*

$$\mathbf{r}_i := \sum_{j=1}^{b} \mathbf{e}_{ij} = i \rightarrow \begin{pmatrix} 0 & 0 & 0 & \cdots & \cdots & 0 \\ & \cdots & & & & \cdots \\ 1 & 1 & 1 & \cdots & \cdots & 1 \\ & \cdots & & & & \cdots \\ 0 & 0 & 0 & \cdots & \cdots & 0 \end{pmatrix} \qquad \text{for } i \in \{1, \ldots, a\},$$

and the *elementary column matrices*

$$\mathbf{c}_j := \sum_{i=1}^{a} \mathbf{e}_{ij} = \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix} \qquad \text{for } j \in \{1, \ldots, b\}.$$

Writing $\mathbf{R} := \{\mathbf{r}_i \mid 1 \leq i \leq a\}$ and $\mathbf{C} := \{\mathbf{c}_j \mid 1 \leq j \leq b\}$, we define

$$\mathcal{C}_0 := \mathcal{C}_0(a, b) := \operatorname{span}\langle \mathbf{R} \cup \mathbf{C} \rangle$$

to be the vector subspace of $\mathcal{V}$ spanned by the elementary row and column matrices. Basic invariants of the code $\mathcal{C}_0$ and the structure of its automorphism group are determined in Section 3. Here we record an inherent symmetry in the construction of $\mathcal{C}_0$: we notice that $\operatorname{Aut}(\mathcal{C}_0)$ contains the group $\operatorname{Sym}(a) \times \operatorname{Sym}(b)$ which embeds into $\operatorname{Sym}(\Omega)$ via the imprimitive action

$$(i, j)^{(\sigma, \tau)} = (i^\sigma, j^\tau) \qquad \text{for } (i, j) \in \Omega \text{ and } (\sigma, \tau) \in \operatorname{Sym}(a) \times \operatorname{Sym}(b). \quad (2.1)$$

Indeed, in the corresponding action on $\mathcal{V}$, the first factor $\operatorname{Sym}(a)$ permutes the elements of $\mathbf{R}$ among themselves and fixes each elementary column matrix, whereas the second factor $\operatorname{Sym}(b)$ permutes the elements of $\mathbf{C}$ and fixes each elementary row matrix.

Interestingly, the code $\mathcal{C}_0 = \mathcal{C}_0(a, b)$ also arises naturally in the study of binary codes defined from rectangular lattice graphs by Key and Seneviratne [5]. They associate a binary code $\mathcal{C}_1 = \mathcal{C}_1(a, b)$ to the line graph $L_2(a, b)$ of the complete bipartite graph $K_{a,b}$ and show that for such a code permutation decoding can be used for full error-correction. A key observation is that $\operatorname{Aut}(\mathcal{C}_1)$ contains $\operatorname{Sym}(a) \times \operatorname{Sym}(b)$. Using the notation introduced above, one easily checks that

$$\mathcal{C}_1 = \mathcal{C}_1(a, b) = \operatorname{span}\langle \mathbf{r}_i + \mathbf{c}_j \mid (i, j) \in \Omega \rangle$$

from which the inclusion $\operatorname{Sym}(a) \times \operatorname{Sym}(b) \subseteq \operatorname{Aut}(\mathcal{C}_1)$ is now obvious.

2.3 A weight formula for elements of $\mathcal{C}_0(a, b)$

For later use we record a weight formula for elements of $\mathcal{C}_0$ and the weight spectra of $\mathcal{C}_0$, $\mathcal{C}_1$. Let $\mathbf{v} \in \mathcal{C}_0$. Then there are $X \subseteq \{1, \ldots, a\}$ and $Y \subseteq \{1, \ldots, b\}$ such that

$\mathbf{v} = \sum_{i \in X} \mathbf{r}_i + \sum_{j \in Y} \mathbf{c}_j$. Writing $x := |X|$ and $y := |Y|$, we find $\sigma \in \mathrm{Sym}(a)$ and $\tau \in \mathrm{Sym}(b)$ such that $X^\sigma = \{1, \ldots, x\}$ and $Y^\tau = \{1, \ldots, y\}$. Since the weight function is invariant under the action of $\mathrm{Sym}(a) \times \mathrm{Sym}(b)$ on $\mathcal{V}$, corresponding to the action on Ω described in (2.1), this yields

$$\mathrm{wt}(\mathbf{v}) = \mathrm{wt}(\mathbf{v}^{(\sigma,\tau)}) = \mathrm{wt}\left(\sum_{i=1}^{x} \mathbf{r}_i + \sum_{j=1}^{y} \mathbf{c}_j\right) = (a-x)y + (b-y)x. \qquad (2.2)$$

Observe that $\mathbf{v} \in \mathcal{C}_1$ if and only if $x + y \equiv_2 0$. Thus we obtain

$$\mathrm{wspec}(\mathcal{C}_0) = \{(a-x)y + (b-y)x \mid 0 \le x \le a, \, 0 \le y \le b\},$$

$$\mathrm{wspec}(\mathcal{C}_1) = \{(a-x)y + (b-y)x \mid 0 \le x \le a, \, 0 \le y \le b, \, x + y \equiv_2 0\}.$$

2.4 The codes $\mathcal{K}(n_1, \ldots, n_r)$

Let $r \in \mathbb{N}$, and let $n_1, \ldots, n_r \in \mathbb{N}_{\ge 3}$ be odd. We put $n_0 := 1$. In this subsection we provide a recursive definition for a sequence of codes $\mathcal{K}_i = \mathcal{K}(n_1, \ldots, n_i)$, $i \in \{1, \ldots, r\}$, whose automorphism groups are later shown to be iterated wreath products of symmetric groups; see Theorem 5.1. Set

$$\Omega_0 := \{1\} \quad \text{and} \quad \Omega_i := \{1, \ldots, n_i\} \times \Omega_{i-1} \text{ for } i \in \{1, \ldots, r\}.$$

For $i \in \{0, \ldots, r\}$ we fix an $\mathbb{F}_2$-vector space

$$\mathcal{V}_i := \bigoplus_{\omega \in \Omega_i} \mathbb{F}_2 \mathbf{e}_\omega, \qquad \dim(\mathcal{V}_i) = |\Omega_i| = n_1 \cdots n_i,$$

with standard basis $\mathbf{e}_\omega$ indexed by $\omega \in \Omega_i$ and we set

$$\mathcal{A}_i := \mathrm{span}\langle \mathbf{a}_i^{(k,l)} \mid k, l \in \{1, \ldots, n_i\} \text{ with } k \ne l \rangle \le \mathcal{V}_i$$

where $\mathbf{a}_i^{(k,l)} := \sum_{\omega \in \Omega_{i-1}} \mathbf{e}_{(k,\omega)} + \mathbf{e}_{(l,\omega)}$ for any distinct $k, l \in \{1, \ldots, n_i\}$. We put $\mathcal{K}_0 := \{0\}$, and for $i \in \{1, \ldots, r\}$ we define recursively

$$\mathcal{K}_i := \mathcal{K}(n_1, \ldots, n_i) := \begin{cases} \mathcal{K}_{i-1}^{(1)} \oplus \ldots \oplus \mathcal{K}_{i-1}^{(n_i)} \oplus \mathcal{A}_i & \text{if } i \equiv_2 1, \\ \mathcal{K}_{i-1}^{(1)} \oplus \ldots \oplus \mathcal{K}_{i-1}^{(n_i)} & \text{if } i \equiv_2 0, \end{cases} \qquad (2.3)$$

where for each $k \in \{1, \ldots, n_i\}$ the summand

$$\mathcal{K}_{i-1}^{(k)} := \left\{ \sum_{\omega \in \Omega_{i-1}} c_\omega \mathbf{e}_{(k,\omega)} \mid \sum_{\omega \in \Omega_{i-1}} c_\omega \mathbf{e}_\omega \in \mathcal{K}_{i-1} \right\} \le \mathcal{V}_i \qquad (2.4)$$

is an isomorphic copy of $\mathcal{K}_{i-1}$ with

$$\mathrm{supp}(\mathcal{K}_{i-1}^{(k)}) = \{k\} \times \Omega_{i-1} \qquad \text{if } i \ge 2.$$

The directness of the sums in (2.3) will be justified in the proof of the following proposition.

Proposition 2.1 *Let $i \in \{1, \ldots, r\}$. Then $\mathcal{K}_i = \mathcal{K}(n_1, \ldots, n_i)$ is a binary cyclic code of length $n_1 \cdots n_i$. It has minimum distance $d(\mathcal{K}_i) = 2$ and minimum co-distance $\widehat{d}(\mathcal{K}_i) = \prod_{j=1}^{\lfloor i/2 \rfloor} n_{2j}$. Its dimension is*

$$\dim(\mathcal{K}_i) = \begin{cases} \sum_{j=1}^{i+1} (-1)^{j+1} \prod_{k=j}^{i} n_k & \text{if } i \equiv_2 1, \\ \sum_{j=1}^{i} (-1)^{j+1} \prod_{k=j}^{i} n_k & \text{if } i \equiv_2 0. \end{cases}$$

Proof Clearly, $\mathcal{K}_i$ is a binary linear code of length $|\Omega_i| = n_1 \cdots n_i$. A short induction argument shows that $\mathrm{Aut}(\mathcal{K}_i)$ contains the iterated wreath product $\mathrm{Sym}(n_1) \wr \ldots \wr \mathrm{Sym}(n_i)$, in its natural imprimitive action on Ω_i. The wreath product contains a regular cyclic subgroup; cf. the treatment of the case $2 = a < b$ in the proof of Corollary 3.3. Hence $\mathcal{K}_i$ is a cyclic code.

A straightforward induction shows that

$$d(\mathcal{K}_i) = 2 \quad \text{and} \quad \mathcal{K}_i \subseteq \{\mathbf{v} \in \mathcal{V}_i \mid \mathrm{wt}(\mathbf{v}) \equiv_2 0\}.$$

Next we comment on the directness of the sums in (2.3). The sum $\mathcal{B}_i := \mathcal{K}_{i-1}^{(1)} \oplus \ldots \oplus \mathcal{K}_{i-1}^{(n_i)}$ is direct, since $\mathrm{supp}(\mathcal{K}_{i-1}^{(k)})$ and $\mathrm{supp}(\mathcal{K}_{i-1}^{(l)})$ are disjoint for any distinct $k, l \in \{1, \ldots, n_i\}$. It remains to explain that $\mathcal{B}_i \cap \mathcal{A}_i = \{\mathbf{0}\}$. Observe that if $\mathbf{a} \in \mathcal{A}_i$ is non-zero, then there exists $k \in \{1, \ldots, n_i\}$ such that $\mathrm{supp}(\mathcal{K}_{i-1}^{(k)}) \subseteq \{k\} \times \Omega_{i-1} \subseteq \mathrm{supp}(\mathbf{a})$. Hence $\mathbf{a} \in \mathcal{B}_i$ would imply $\sum_{\omega \in \Omega_{i-1}} \mathbf{e}_{(k,\omega)} \in \mathcal{K}_{i-1}^{(k)}$. But $\mathrm{wt}(\sum_{\omega \in \Omega_{i-1}} \mathbf{e}_{(k,\omega)}) = |\Omega_{i-1}| \equiv_2 1$, whereas $\mathrm{wt}(\mathbf{v}) \equiv_2 0$ for any $\mathbf{v} \in \mathcal{K}_{i-1}^{(k)}$. Therefore $\mathbf{a} \notin \mathcal{B}_i$, and $\mathcal{B}_i \cap \mathcal{A}_i = \{\mathbf{0}\}$.

From this we can easily compute the dimension of $\mathcal{K}_i$. We have $\dim(\mathcal{K}_i) = n_i \dim(\mathcal{K}_{i-1}) + \dim(\mathcal{A}_i) = n_i \dim(\mathcal{K}_{i-1}) + (n_i - 1)$ if $i \equiv_2 1$, and $\dim(\mathcal{K}_i) = n_i \dim(\mathcal{K}_{i-1})$ if $i \equiv_2 0$. Induction gives the desired formula.

Finally, we determine the minimum co-distance of $\mathcal{K}_i$. We contend that $\widehat{d}(\mathcal{K}_i) = \widehat{d}(\mathcal{K}_{i-1})$ if $i \equiv_2 1$, and $\widehat{d}(\mathcal{K}_i) = n_i \widehat{d}(\mathcal{K}_{i-1})$ if $i \equiv_2 0$. Induction then yields the desired formula. For $i \equiv_2 0$ our claim follows directly from (2.3). Now suppose that $i \equiv_2 1$. Recalling that $n_i \equiv_2 1$, it is not difficult to see that a typical element realising minimum co-distance in $\mathcal{K}_i$ is $\mathbf{v} = \mathbf{v}^{(1)} + \sum_{j=1}^{\lfloor n_i/2 \rfloor} \mathbf{a}_i^{(2j, 2j+1)}$ where $\mathbf{v}^{(1)} \in \mathcal{K}_{i-1}^{(1)}$ corresponds to an element realising minimum co-distance in $\mathcal{K}_{i-1}$. □

3 The codes $\mathcal{C}_0(a, b)$ and their automorphism groups

Let $a, b \in \mathbb{N}$ with $a \leq b$. We make free use of the notation introduced in Sections 2.1, 2.2 and 2.3. The aim of this section is to establish the following results concerning the binary linear code $\mathcal{C}_0 = \mathcal{C}_0(a, b)$ and its automorphism group.

Proposition 3.1 *The code $\mathcal{C}_0 = \mathcal{C}_0(a, b)$ has dimension $\dim(\mathcal{C}_0) = a + b - 1$ and minimum distance $d(\mathcal{C}_0) = a$.*

The special case $a \in \{1, 2\}$ allows the following explicit description.

(1) *If $1 = a \leq b$, then $\mathcal{C}_0 = \mathcal{V}$.*

(2) *If* $2 = a = b$, *then* $\mathcal{C}_0 = \{\mathbf{v} \in \mathcal{V} \mid \mathrm{wt}(\mathbf{v}) \equiv_2 0\}$.

(3) *If* $2 = a < b$, *then* $\mathcal{C}_0 = \{\sum c_{ij} \mathbf{e}_{ij} \mid \forall j, k : c_{1j} + c_{2j} = c_{1k} + c_{2k}\}$.

Proposition 3.2 *Let* $\mathcal{C}_0 = \mathcal{C}_0(a, b)$ *as above.*

(1) *If* $1 = a \leq b$, *then* $\mathrm{Aut}(\mathcal{C}_0) = \mathrm{Sym}(\Omega) \cong \mathrm{Sym}(b)$.

(2) *If* $2 = a = b$, *then* $\mathrm{Aut}(\mathcal{C}_0) = \mathrm{Sym}(\Omega) \cong \mathrm{Sym}(4)$.

(3) *If* $2 = a < b$, *then* $\mathrm{Aut}(\mathcal{C}_0) = C_2 \wr \mathrm{Sym}(b)$.

(4) *If* $2 < a = b$, *then* $\mathrm{Aut}(\mathcal{C}_0) = \mathrm{Sym}(a) \wr C_2$.

(5) *If* $2 < a < b$, *then* $\mathrm{Aut}(\mathcal{C}_0) = \mathrm{Sym}(a) \times \mathrm{Sym}(b)$.

As a corollary, we record for which values of (a, b) the code $\mathcal{C}_0$ is cyclic, i.e. for which (a, b) the permutation group $\mathrm{Aut}(\mathcal{C}_0) \leq \mathrm{Sym}(\Omega)$ contains a regular cyclic subgroup.

Corollary 3.3 *Let* $\mathcal{C}_0 = \mathcal{C}_0(a, b)$ *as above. Then* $\mathcal{C}_0$ *is cyclic, if and only if* $a \in \{1, 2\}$ *or* $\gcd(a, b) = 1$.

Note that Theorem D follows from Proposition 3.2 and Corollary 3.3. We now supply the proofs of the stated results.

Proof of Proposition 3.1 First we determine the dimension of $\mathcal{C}_0 = \mathrm{span}\langle \mathbf{R} \cup \mathbf{C} \rangle$. For each $(i, j) \in \Omega$ there are precisely two elements in $\mathbf{R} \cup \mathbf{C}$ which have a non-zero entry in the (i, j)-position, namely $\mathbf{r}_i$ and $\mathbf{c}_j$. Therefore $\sum_{i=1}^{a} \mathbf{r}_i + \sum_{j=1}^{b} \mathbf{c}_j = \mathbf{0}$ and this is the only non-trivial linear dependence relation among the $a + b$ elementary row and column matrices. Hence $\dim \mathcal{C}_0 = a + b - 1$.

In order to determine $d(\mathcal{C}_0)$ we employ the weight formula (2.2). Let $\mathbf{v} = \sum_{i \in X} \mathbf{r}_i + \sum_{j \in Y} \mathbf{c}_j$ and write $x := |X|$, $y := |Y|$, as in Subsection 2.3. If $x \in \{1, \ldots, a - 1\}$, then

$$\mathrm{wt}(\mathbf{v}) = (a - x)y + (b - y)x \geq y + (b - y) = b,$$

with equality if and only if $a = 2$ or $(x, y) \in \{(1, 0), (a - 1, b)\}$. In the latter case, $\mathbf{v} \in \mathbf{R}$. If $x \in \{0, a\}$, then $\mathrm{wt}(\mathbf{v}) = (a - x)y + (b - y)x$ is a multiple of a, and equal to a if and only if $(x, y) \in \{(0, 1), (a, b - 1)\}$, equivalently $\mathbf{v} \in \mathbf{C}$. This analysis shows, in particular, that $d(\mathcal{C}_0) = a$.

It remains to justify the explicit description of $\mathcal{C}_0$ for $a \in \{1, 2\}$. The cases $1 = a \leq b$ and $2 = a = b$ are easily dealt with, noting that $\dim(\mathcal{C}_0) = b = N$ and $\dim(\mathcal{C}_0) = 3 = N - 1$, respectively. Now suppose that $2 = a < b$. The description of $\mathcal{C}_0$ can be checked by counting: clearly, $\{\sum c_{ij} \mathbf{e}_{ij} \mid \forall j, k : c_{1j} + c_{2j} = c_{1k} + c_{2k}\} \subseteq \mathcal{C}_0$ and both sets contain the same number of elements, namely $2^b + 2^b = 2^{a+b-1} = 2^{\dim(\mathcal{C}_0)}$. $\square$

Proof of Proposition 3.2 We treat the cases (1), (2); (3); and (4), (5).

(1), (2) From Proposition 3.1 it is clear that $\mathrm{Aut}(\mathcal{C}_0) = \mathrm{Sym}(\Omega)$, if $1 = a \leq b$ or $2 = a = b$.

(3) For $2 = a < b$ the explicit description of $\mathcal{C}_0$ in Proposition 3.1 shows that $\mathrm{Aut}(\mathcal{C}_0)$ contains $C_2 \wr \mathrm{Sym}(b) = \mathrm{Sym}(b) \ltimes C_2^b$, where the action on $(i, j) \in \Omega$ of

elements of the top group, respectively base group, of the wreath product is given by

$$(i, j)^\sigma = (i, j^\sigma) \text{ if } \sigma \in \text{Sym}(b),$$
$$(i, j)^\tau = (i^{\tau_j}, j) \text{ if } \tau = (\tau_1, \dots, \tau_b) \in C_2^b. \tag{3.1}$$

It remains to show that the automorphism group is not larger than the wreath product. Consider $\varphi \in \text{Sym}(\Omega) \setminus (C_2 \wr \text{Sym}(b))$. The group $C_2 \wr \text{Sym}(b)$ acts transitively on Ω. In fact, the top group acts as the full symmetric group on column-coordinates, and elements of the base group allow us to flip row-coordinates independently for each fixed column-coordinate; see (3.1). Therefore, multiplying φ by a suitable element of $C_2 \wr \text{Sym}(b)$, we may assume that $(1, 1)^\varphi = (1, 1)$ and $(2, 1)^\varphi = (1, 2)$. Pictorially, φ acts on a 'generic' element $\sum_{i,j} c_{ij} \mathbf{e}_{ij} \in \mathcal{V}$ as follows:

$$\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1b} \\ c_{21} & c_{22} & \cdots & c_{2b} \end{pmatrix}^\varphi = \begin{pmatrix} c_{11} & c_{21} & * & \cdots & * \\ * & * & * & \cdots & * \end{pmatrix}.$$

In particular, the image of $\mathbf{c}_1$ under φ is

$$\mathbf{c}_1^\varphi = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \end{pmatrix}^\varphi = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Because the two entries in the first column of $\mathbf{c}_1^\varphi$ sum to 1, but the two entries in the third column sum to 0, we conclude that $\mathbf{c}_1^\varphi \notin \mathcal{C}_0$. Thus $\varphi \notin \text{Aut}(\mathcal{C}_0)$.

(4), (5) Finally, we consider the case $2 < a \le b$. Clearly, any automorphism of $\mathcal{C}_0$ is uniquely determined by its effect on the elements of $\mathbf{R} \cup \mathbf{C}$.

First suppose that $2 < a < b$, and recall the weight formula (2.2) and the argument given in the proof of Proposition 3.1. From the latter we deduce that $\mathbf{C} = \{\mathbf{v} \in \mathcal{C}_0 \mid \text{wt}(\mathbf{v}) = a\}$ is invariant under $\text{Aut}(\mathcal{C}_0)$, and furthermore that

$$\mathbf{R} = \{\mathbf{v} \in \mathcal{C}_0 \mid \text{wt}(\mathbf{v}) = b\} \setminus \left\{ \sum_{j \in Y} \mathbf{c}_j \mid Y \subseteq \{1, \dots, b\} \right\}$$

is $\text{Aut}(\mathcal{C}_0)$-invariant. Hence both sets $\mathbf{R}$ and $\mathbf{C}$ are invariant under the action of $\text{Aut}(\mathcal{C}_0)$. Comparing with the action described in (2.1), this implies that $\text{Aut}(\mathcal{C}_0) = \text{Sym}(a) \times \text{Sym}(b)$.

Now consider the case $2 < a = b$. A similar argument as above shows that the union $\mathbf{R} \cup \mathbf{C} = \{\mathbf{v} \in \mathcal{C}_0 \mid \text{wt}(\mathbf{v}) = a\}$ is invariant under the action of $\text{Aut}(\mathcal{C}_0)$. Next observe that for any distinct $\mathbf{r}_i, \mathbf{r}_k \in \mathbf{R}$ and any distinct $\mathbf{c}_j, \mathbf{c}_l \in \mathbf{C}$ we have

$$\text{wt}(\mathbf{r}_i + \mathbf{r}_k) = \text{wt}(\mathbf{c}_j + \mathbf{c}_l) = 2a, \quad \text{but} \quad \text{wt}(\mathbf{r}_i + \mathbf{c}_j) = 2a - 2.$$

This implies that $\mathbf{R}, \mathbf{C}$ form a system of imprimitivity for the action of $\text{Aut}(\mathcal{C}_0)$ on $\mathbf{R} \cup \mathbf{C}$. Comparing with the action described in (2.1) and noticing that ordinary matrix transposition yields an involution which swaps elementary row and column matrices, this implies that $\text{Aut}(\mathcal{C}_0) = \text{Sym}(a) \wr C_2$. $\qquad \square$

Proof of Corollary 3.3 We use without further ado the description of $\text{Aut}(\mathcal{C}_0)$ provided by Proposition 3.2. Clearly, it suffices to examine the situation where $2 \le a \le b$, but $b \ne 2$.

First consider the case $2 = a < b$, where $\text{Aut}(\mathcal{C}_0) = C_2 \wr \text{Sym}(b)$. Let $\sigma :=$ $(1\,2\,\ldots\,b) \in \text{Sym}(b)$ be a regular cycle in the top group, and let $\tau := (1, 0, \ldots, 0) \in$ C_2^b be an element of the base group acting non-trivially precisely in the first column. Then $\sigma\tau$ generates a regular cyclic subgroup. Indeed, one checks easily that the action of $\sigma\tau$ on Ω is given by $(i, j)^{\sigma\tau} = (i, j + 1)$ if $(i, j) \in \Omega$ with $j < b$, and by $(1, b)^{\sigma\tau} = (2, 1)$, $(2, b)^{\sigma\tau} = (1, 1)$ in the remaining two cases.

Next consider the case $2 < a < b$, where $\text{Aut}(\mathcal{C}_0) = \text{Sym}(a) \times \text{Sym}(b)$. Let $(\sigma, \tau) \in \text{Sym}(a) \times \text{Sym}(b)$. The number of orbits of (σ, τ) on Ω is at least as large as the number of orbits of σ times the number of orbits of τ. Hence, if (σ, τ) is to generate a regular cyclic permutation group on Ω, then σ and τ are necessarily regular cycles of length a and b, respectively. But in this case the order of (σ, τ) is $ab = |\Omega|$ precisely if $\gcd(a, b) = 1$.

Finally consider the case $2 < a = b$ where $\text{Aut}(\mathcal{C}_0) = \text{Sym}(a) \wr C_2$. Assume for a contradiction that $\text{Sym}(a) \wr C_2$ contains a regular cyclic subgroup. Then $\text{Sym}(a) \times \text{Sym}(a)$ contains a cyclic subgroup $\langle(\sigma, \tau)\rangle$ with two orbits, each of length $a^2/2$. Since the number of orbits of (σ, τ) is at least as large as the number of orbits of σ times the number of orbits of τ, we may assume without loss of generality that σ is a regular cycle of length a and that τ is the product of two disjoint cycles of length $a - c$ and c, say. Since the number of orbits of (σ, τ) is two, we deduce that $1 = \gcd(a, a - c) = \gcd(a, c) = \gcd(a - c, c)$. Hence the order of τ is $(a - c)c$, and the order of (σ, τ) equals $(a - c)ac$. Comparing with the orbit lengths, this gives $a^2/2 = (a - c)ac$. Then $\gcd(a, a - c) = \gcd(a, c) = 1$ implies $(a, c) = (2, 1)$, in contradiction to $2 < a$. $\square$

4 Binary codes associated to rectangular lattice graphs

Let $a, b \in \mathbb{N}$ with $a \leq b$. We make free use of the notation introduced in Sections 2.1, 2.2 and 2.3. The aim of this section is to establish the following results concerning the binary linear code $\mathcal{C}_1(a, b)$ and its automorphism group.

Proposition 4.1 *If $a + b \equiv_2 1$, then $\mathcal{C}_1(a, b) = \mathcal{C}_0(a, b)$.*

Proposition 4.2 *Suppose that $a + b \equiv_2 0$. Then $\mathcal{C}_1 = \mathcal{C}_1(a, b)$ has dimension $\dim(\mathcal{C}_1) = \dim(\mathcal{C}_0(a, b)) - 1 = a + b - 2$. Moreover, the minimum distance of $\mathcal{C}_1$ is $d(\mathcal{C}_1) = 2a$ if $1 \leq a < b$, and $d(\mathcal{C}_1) = 2a - 2$ if $1 < a = b$.*

In special cases we have the following explicit description of $\mathcal{C}_1$.

(1) *If $1 = a = b$, then $\mathcal{C}_1 = \{0\}$.*
(2) *If $2 = a = b$, then $\mathcal{C}_1 = \left\{ \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) \right\}$.*
(3) *If $1 \equiv_2 a \equiv_2 b$, then $\mathcal{C}_1 = \{\mathbf{v} \in \mathcal{C}_0 \mid \text{wt}(\mathbf{v}) \equiv_2 0\}$.*
(4) *If $(a, b) = (2, 4)$, then $\mathcal{C}_1$ is the extended Hamming code of length 8.*

Proposition 4.3 *Suppose that $a + b \equiv_2 0$. Let $\mathcal{C}_1 = \mathcal{C}_1(a, b)$ and $\mathcal{C}_0 = \mathcal{C}_0(a, b)$ as above. If $(a, b) = (2, 4)$, then $\text{Aut}(\mathcal{C}_1) = \text{AGL}(3, 2)$. If $(a, b) \neq (2, 4)$, then $\text{Aut}(\mathcal{C}_1) \leq \text{Aut}(\mathcal{C}_0)$, with equality if $1 \equiv_2 a \equiv_2 b$ or $2 < a$. In the remaining cases we have*

(1) *If $2 = a = b$, then $\mathrm{Aut}(\mathcal{C}_1) = D_8$ is a dihedral group of order* 8 *in its natural action of degree* 4.

(2) *If $a = 2$ and $b > 4$ with $b \equiv_2 0$, then $\mathrm{Aut}(\mathcal{C}_1) = \mathrm{Sym}(b) \ltimes B$, where $B = \{(\tau_1, \ldots, \tau_b) \in C_2^b \mid \sum_{j=1}^b \tau_j = 0\}$; consequently, $\mathrm{Aut}(\mathcal{C}_1)$ has index* 2 *in $\mathrm{Aut}(\mathcal{C}_0) = C_2 \wr \mathrm{Sym}(b)$.*

We recall that the structure of $\mathcal{C}_0(a, b)$ and its automorphism group are described in Section 3. We now give the proofs of the stated results. As before we write $\mathcal{C}_1 = \mathcal{C}_1(a, b)$ and $\mathcal{C}_0 = \mathcal{C}_0(a, b)$. Moreover, we define

$$\mathbf{a} := \sum_{i=1}^a \mathbf{r}_i = \sum_{j=1}^b \mathbf{c}_j = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}.$$

Proof of Proposition 4.1 Suppose that $a \equiv_2 1$ and $b \equiv_2 0$. Since the underlying field has characteristic 2, we have

$$\mathbf{c}_j = \mathbf{a} + (\mathbf{a} + \mathbf{c}_j) = \sum_{l=1}^b (\mathbf{r}_1 + \mathbf{c}_l) + \sum_{i=1}^a (\mathbf{r}_i + \mathbf{c}_j) \in \mathcal{C}_1 \quad \text{for } 1 \leq j \leq b.$$

Moreover, from $\mathbf{c}_1 \in \mathcal{C}_1$ we deduce that $\mathbf{r}_i = (\mathbf{r}_i + \mathbf{c}_1) + \mathbf{c}_1 \in \mathcal{C}_1$ for $1 \leq i \leq a$. It follows that $\mathbf{R} \cup \mathbf{C} \subseteq \mathcal{C}_1$, hence $\mathcal{C}_1 = \mathrm{span}\langle \mathbf{R} \cup \mathbf{C} \rangle = \mathcal{C}_0$. The argument for $a \equiv_2 0$, $b \equiv_2 1$ is very similar. □

Proof of Proposition 4.2 The special cases $1 = a = b$ and $2 = a = b$ are easily dealt with. Now suppose that $2 < b$, and assume for the moment that we can prove the assertion concerning $d(\mathcal{C}_1)$. Observe that the claimed value for $d(\mathcal{C}_1)$ is strictly larger than $d(\mathcal{C}_0) = a$; cf. Proposition 3.1. On the other hand, we clearly have $\mathcal{C}_1 + \mathrm{span}\langle \mathbf{c}_1 \rangle = \mathcal{C}_0$, and it follows that $\dim(\mathcal{C}_1) = \dim(\mathcal{C}_0) - 1 = a + b - 2$. Moreover, we have $\mathrm{wt}(\mathbf{r}_i + \mathbf{c}_j) = a + b - 2 \equiv_2 0$ for all $(i, j) \in \Omega$, and thus $\mathcal{C}_1 \subseteq \mathcal{W}$ where $\mathcal{W} := \{\mathbf{v} \in \mathcal{C}_0 \mid \mathrm{wt}(\mathbf{v}) \equiv_2 0\}$. Note that in the special case $1 \equiv_2 a \equiv_2 b$ the vector $\mathbf{c}_1 \in \mathcal{C}_0$ has weight $\mathrm{wt}(\mathbf{c}_1) = a \equiv_2 1$ so that $\dim(\mathcal{W}) = \dim(\mathcal{C}_0) - 1 = \dim(\mathcal{C}_1)$. From this we obtain $\mathcal{C}_1 = \mathcal{W}$ as wanted. Similarly one easily computes $\mathcal{C}_1$ in the special case $(a, b) = (2, 4)$.

Hence it suffices to prove that $d(\mathcal{C}_1) = 2a$ if $1 \leq a < b$, and $d(\mathcal{C}_1) = 2a - 2$ if $1 < a = b$. As explained, we shall assume that $2 < b$ throughout.

Recall the weight formula (2.2). As stated in Subsection 2.3, the elements of $\mathcal{C}_1$ are of the form $\mathbf{v} = \sum_{i \in X} \mathbf{r}_i + \sum_{j \in Y} \mathbf{c}_j$ where $x := |X|$ and $y := |Y|$ satisfy the condition $x + y \equiv_2 0$. Since $\mathbf{a} + \mathbf{a} = \mathbf{0}$, we deduce for any such $\mathbf{v}$ that

$$\mathbf{v} = \left(\sum_{i \in X} \mathbf{r}_i + \mathbf{a} \right) + \left(\mathbf{a} + \sum_{j \in Y} \mathbf{c}_j \right) = \sum_{i \notin X} \mathbf{r}_i + \sum_{j \notin Y} \mathbf{c}_j.$$

For our analysis we may therefore assume that $x \leq \lfloor a/2 \rfloor$. Of course, we shall also assume that $\mathbf{v} \neq \mathbf{0}$.

If $x = 0$, then $y \geq 2$ and $\mathrm{wt}(\mathbf{v}) = ay \geq 2a$, with equality if and only if $y = 2$. In this case, $\mathbf{v} = \mathbf{c}_j + \mathbf{c}_l$ for suitable $j \neq l$. Likewise, if $x \geq 2$, then

$$\mathrm{wt}(\mathbf{v}) = (a - x)y + (b - y)x = (a - 2x)y + (bx - 2a) + 2a \geq 2a,$$

with equality if and only if $(a, b, x) = (4, 4, 2)$ or $(a, x, y) = (b, 2, 0)$. In the latter case, $\mathbf{v} = \mathbf{r}_i + \mathbf{r}_k$ for suitable $i \neq k$. Finally, if $x = 1$ (and consequently $1 < a$ and $y \equiv_2 1$), then

$$\text{wt}(\mathbf{v}) = (a - 1)y + (b - y) = (a - 2)y + b.$$

The last expression takes its minimum non-zero value for $y = 1$: in this case $\mathbf{v} = \mathbf{r}_i + \mathbf{c}_j$ for suitable i, j and

(i) $\text{wt}(\mathbf{v}) = 2a - 2 < 2a$ if $1 < a = b$;
(ii) $\text{wt}(\mathbf{v}) = a + b - 2 \geq 2a$ if $1 < a < b$, with equality if and only if $b = a + 2$.

This analysis shows that $d(\mathcal{C}_1) = 2a$ if $1 \leq a < b$, and $d(\mathcal{C}_1) = 2a - 2$ if $1 < a = b$, as wanted.   □

Proof of Proposition 4.3 If $(a, b) = (2, 4)$ then $\text{Aut}(\mathcal{C}_1)$ can be computed from the description of $\mathcal{C}_1$ in Proposition 4.2. Now consider the situation for $(a, b) \neq (2, 4)$. First we treat the special cases (1) and (2). Then we deal with the remaining cases (3) $1 \equiv_2 a \equiv_2 b$ and (4) $2 < a \leq b$ with $a \equiv_2 b \equiv_2 0$.

(1) If $2 = a = b$, the group $\text{Aut}(\mathcal{C}_1)$ is easily calculated from the explicit description of $\mathcal{C}_1$ in Proposition 4.2.

(2) Next consider the case $a = 2$ and $b > 4$ with $b \equiv_2 0$. From the weight analysis in the second half of the proof of Proposition 4.2 we see that $\mathcal{C}_1$ contains only one type of elements of minimum weight $2a = 4$, namely those of the form $\mathbf{c}_j + \mathbf{c}_l$. Therefore the set

$$\mathbf{C} \dotplus \mathbf{C} := \{\mathbf{c}_j + \mathbf{c}_l \mid 1 \leq j, l \leq b \text{ with } j \neq l\}$$

is invariant under $\text{Aut}(\mathcal{C}_1)$. Furthermore, we observe that the set $\mathbf{C}$ can be described as

$$\mathbf{C} = \{\mathbf{v} \in \mathcal{V} \mid \text{wt}(\mathbf{v}) = 2 \text{ and } \exists \mathbf{w}_1, \mathbf{w}_2 \in \mathbf{C} \dotplus \mathbf{C} :$$
$$\text{com}(\mathbf{w}_1, \mathbf{w}_2) = \text{com}(\mathbf{v}, \mathbf{w}_1) = \text{com}(\mathbf{v}, \mathbf{w}_2) = 2\}.$$

Hence $\mathbf{C}$ is invariant under $\text{Aut}(\mathcal{C}_1)$. As $\mathcal{C}_1$ is complemented in $\mathcal{C}_0$ by $\text{span}\langle \mathbf{c}_j \rangle$ for any $j \in \{1, \ldots, b\}$, this shows that $\text{Aut}(\mathcal{C}_1) \leq \text{Aut}(\mathcal{C}_0)$. Now $\text{Aut}(\mathcal{C}_0) = C_2 \wr \text{Sym}(b)$ by Proposition 3.2. Note that $\text{Sym}(b) \ltimes B$, where $B = \{(\tau_1, \ldots, \tau_b) \in C_2^b \mid \sum_{i=1}^{b} \tau_i = 0\}$, is a subgroup of index 2 in $C_2 \wr \text{Sym}(b)$. From $\mathbf{C} \dotplus \mathbf{C} \subseteq \mathcal{C}_1$ it is easily seen that $\text{Sym}(b) \ltimes B \leq \text{Aut}(\mathcal{C}_1)$, and in order to prove equality it suffices to exhibit a single element in $C_2 \wr \text{Sym}(b)$ which does not leave $\mathcal{C}_1$ invariant. Take $\boldsymbol{\tau} := (1, 0, \ldots, 0) \in C_2^b$. One readily computes that $(\mathbf{r}_1 + \mathbf{c}_2)^{\boldsymbol{\tau}} + (\mathbf{r}_1 + \mathbf{c}_2) = \mathbf{c}_1 \notin \mathcal{C}_1$, hence $\mathcal{C}_1$ is not invariant under the action of $\boldsymbol{\tau}$, as wanted.

(3) Consider the case $1 \equiv_2 a \equiv_2 b$. From the explicit description of $\mathcal{C}_1$ in Proposition 4.2 we see that $\text{Aut}(\mathcal{C}_0) \leq \text{Aut}(\mathcal{C}_1)$. It remains to prove the reverse inclusion. Since $\text{wt}(\mathbf{a}) = ab \equiv_2 1$, we have $\mathcal{C}_0 = \mathcal{C}_1 + \text{span}\langle \mathbf{a} \rangle$. Since both summands in this decomposition are $\text{Aut}(\mathcal{C}_1)$-invariant, it follows that $\text{Aut}(\mathcal{C}_1) \leq \text{Aut}(\mathcal{C}_0)$.

(4) The final case to consider is $2 < a \leq b$ and $a \equiv_2 b \equiv_2 0$. From Proposition 3.2 it is clear that $\text{Aut}(\mathcal{C}_0) \leq \text{Aut}(\mathcal{C}_1)$. It remains to prove the reverse inclusion. We claim

that $\mathbf{R} + \mathbf{C} = \{\mathbf{r}_i + \mathbf{c}_j \mid (i, j) \in \Omega\}$ is invariant under $\mathrm{Aut}(\mathcal{C}_1)$. Indeed, we contend that this set is equal to

$$\mathbf{S} := \{\mathbf{v} \in \mathcal{C}_1 \mid \mathrm{wt}(\mathbf{v}) = a + b - 2 \text{ and}$$

$$\forall \mathbf{w} \in \mathcal{C}_1 : \mathrm{wt}(\mathbf{w}) = a + b - 2 \Rightarrow \mathrm{com}(\mathbf{v}, \mathbf{w}) \geq 1\}.$$

We use again the weight formula (2.2) and an analysis similar to the one in the proof of Proposition 4.2. Elements of weight $a + b - 2$ in $\mathcal{C}_1$ are obtained from solutions (x, y) of the equation $(a - x)y + (b - y)x = a + b - 2$ satisfying the extra condition $x + y \equiv_2 0$. As described earlier we may assume that $x \leq a/2$. We consider three cases

  (i) If $x = 0$, then $ay = a + b - 2$ has a permissible solution $y = 1 + (b - 2)/a$ if this number is an even positive integer. A corresponding element of $\mathcal{C}_1$ would have the form $\sum_{j \in Y} \mathbf{c}_j$ where $|Y| = 1 + (b - 2)/a$. Since $2(1 + (b - 2)/a) \leq b$, for any such element $\mathbf{v}$ there would be a similar element $\mathbf{w}$ such that $\mathrm{com}(\mathbf{v}, \mathbf{w}) = 0$. Hence none of these elements would belong to the set $\mathbf{S}$.
 (ii) If $x = 1$, then $(a - 1)y + (b - y) = a + b - 2$ only admits the solution $y = 1$, corresponding to elements of the form $\mathbf{r}_i + \mathbf{c}_j$ which we want to characterise.
(iii) If $x \geq 2$, then $(a - x)y + (b - y)x = a + b - 2$ implies

$$0 = (a - 2x)y + b(x - 1) - a + 2 \geq 0 + b - a + 2 \geq 2,$$

a contradiction.

This analysis shows that $\mathbf{R} + \mathbf{C} = \mathbf{S}$ is invariant under $\mathrm{Aut}(\mathcal{C}_1)$ as claimed. Observe that for all $i, k \in \{1, \dots, a\}$ and $j, l \in \{1, \dots, b\}$,

$$\mathrm{wt}((\mathbf{r}_i + \mathbf{c}_j) + (\mathbf{r}_k + \mathbf{c}_l)) = \begin{cases} 2a + 2b - 4 & \text{if } i \neq k \text{ and } j \neq l, \\ 2a & \text{if } i = k \text{ and } j \neq l, \\ 2b & \text{if } i \neq k \text{ and } j = l, \\ 0 & \text{if } i = k \text{ and } j = l. \end{cases}$$

Since $2 < a \leq b$, we have $0 < 2a \leq 2b < 2a + 2b - 4$. Suppose first that $a < b$. A simple computation shows that the set $\mathbf{R} + \mathbf{C}$ can be partitioned uniquely into subsets $\mathbf{S}_1, \dots, \mathbf{S}_a$, each of size b, such that for every $i \in \{1, \dots, a\}$ and all $\mathbf{v}, \mathbf{w} \in \mathbf{S}_i$ one has $\mathrm{wt}(\mathbf{v} + \mathbf{w}) = 2a$. Moreover, we can order the sets $\mathbf{S}_1, \dots, \mathbf{S}_a$ such that for every $i \in \{1, \dots, a\}$ the vector $\mathbf{r}_i$ is characterised as the unique element $\mathbf{v} \in \mathcal{V}$ with $\mathrm{wt}(\mathbf{v}) = b$ and $\mathrm{com}(\mathbf{v}, \mathbf{w}) = b - 1$ for all $\mathbf{w} \in \mathbf{S}_i$. This shows that $\mathbf{R}$ is $\mathrm{Aut}(\mathcal{C}_1)$-invariant. If $a = b$ a similar argument proves that the union $\mathbf{R} \cup \mathbf{C}$ is $\mathrm{Aut}(\mathcal{C}_1)$-invariant. Since $\mathcal{C}_0 = \mathcal{C}_1 + \mathrm{span}\langle \mathbf{v} \rangle$ for any $\mathbf{v} \in \mathbf{R} \cup \mathbf{C}$, this implies that in any case $\mathrm{Aut}(\mathcal{C}_1) \leq \mathrm{Aut}(\mathcal{C}_0)$, as wanted. □

5 The codes $\mathcal{K}(n_1, \dots, n_r)$ and their automorphism groups

Let $r \in \mathbb{N}$, and let $n_1, \dots, n_r \in \mathbb{N}_{\geq 3}$ be odd. Theorem C is an immediate consequence of the following description of the automorphism group of the code $\mathcal{K}_r = \mathcal{K}_r(n_1, \dots, n_r)$, which was defined in Section 2.4.

Theorem 5.1 *Let $r \in \mathbb{N}$, and let $n_1, \ldots, n_r \in \mathbb{N}_{\geq 3}$ be odd. Then $\mathcal{K}_r = \mathcal{K}_r(n_1, \ldots, n_r)$ satisfies $\mathrm{Aut}(\mathcal{K}_r) = \mathrm{Sym}(n_1) \wr \ldots \wr \mathrm{Sym}(n_r)$, where the wreath product acts imprimitively as a permutation group of degree $n_1 \cdots n_r$.*

We make free use of the notation introduced in Sections 2.1 and 2.4. Let $i \in \{3, \ldots, r\}$ with $i \equiv_2 1$, and let $k \in \{1, \ldots, n_i\}$. Since $\mathcal{K}_{i-1}^{(k)}$ is an isomorphic copy of $\mathcal{K}_{i-1}$, we can use the decomposition $\mathcal{K}_{i-1} = \mathcal{K}_{i-2}^{(1)} \oplus \ldots \oplus \mathcal{K}_{i-2}^{(n_{i-1})}$ given by (2.3) to write

$$\mathcal{K}_{i-1}^{(k)} = \mathcal{K}_{i-2}^{(k,1)} \oplus \ldots \oplus \mathcal{K}_{i-2}^{(k,n_{i-1})} \tag{5.1}$$

where $\mathcal{K}_{i-2}^{(k,m)}$, similarly defined as in (2.4), is an isomorphic copy of $\mathcal{K}_{i-2}$ with

$$\mathrm{supp}(\mathcal{K}_{i-2}^{(k,m)}) = \{(k,m)\} \times \Omega_{i-2} \quad \text{for } m \in \{1, \ldots, n_{i-1}\}.$$

Our strategy for understanding the structure of $\mathrm{Aut}(\mathcal{K}_i)$ is based on the description of certain indecomposable elements in $\mathcal{K}_i$.

Lemma 5.2 *Let $i \in \{3, \ldots, r\}$ with $i \equiv_2 1$.*
(1) *Let $k, l \in \{1, \ldots, n_i\}$ with $k \neq l$. Then there exists an indecomposable element $\mathbf{v} \in \mathcal{K}_i$ such that*

  (i) $\mathbf{v} \in \mathbf{a}_i^{(k,l)} + \mathcal{K}_{i-1}^{(k)} + \mathcal{K}_{i-1}^{(l)}$,
  (ii) $\mathrm{wt}(\mathbf{v}) = 2\widehat{d}(\mathcal{K}_{i-1}) = 2n_2 n_4 \cdots n_{i-1}$,
  (iii) $\mathrm{supp}(\mathbf{v}) \cap \{(k,m)\} \times \Omega_{i-2} \neq \varnothing$ *for all $m \in \{1, \ldots, n_{i-1}\}$,*
  (iv) $\mathrm{supp}(\mathbf{v}) \cap \{(l,m)\} \times \Omega_{i-2} \neq \varnothing$ *for all $m \in \{1, \ldots, n_{i-1}\}$,*

(2) *Let $\mathbf{v} \in \mathcal{K}_i$, and let $\mathbf{a} := \pi(\mathbf{v})$ where $\pi : \mathcal{K}_i \to \mathcal{A}_i$ denotes the natural projection induced by the direct decomposition (2.3). Then*

$$\mathrm{wt}(\mathbf{v}) \geq (\mathrm{wt}(\mathbf{a})/|\Omega_{i-1}|) \cdot \widehat{d}(\mathcal{K}_{i-1}).$$

In particular, if $\mathbf{a} \neq \mathbf{0}$, then $\mathrm{wt}(\mathbf{v}) \geq 2\widehat{d}(\mathcal{K}_{i-1})$.
(3) *If $\mathbf{v} \in \mathcal{K}_i$ is indecomposable with $\mathrm{wt}(\mathbf{v}) \leq 2\widehat{d}(\mathcal{K}_{i-1})$, then*

(a) $\mathbf{v} \in \mathbf{a}_i^{(k,l)} + \mathcal{K}_{i-1}^{(k)} + \mathcal{K}_{i-1}^{(l)}$ *for suitable $k, l \in \{1, \ldots, n_i\}$ with $k \neq l$ and $\mathrm{wt}(\mathbf{v}) = 2\widehat{d}(\mathcal{K}_{i-1})$, or*
(b) $\mathbf{v} \in \mathcal{K}_{i-2}^{(k,m)}$ *for suitable $k \in \{1, \ldots, n_i\}$ and $m \in \{1, \ldots, n_{i-1}\}$.*

Proof Everything follows from the decompositions (2.3) and (5.1), together with the fact that $2\widehat{d}(\mathcal{K}_{i-1}) = 2n_{i-1}\widehat{d}(\mathcal{K}_{i-2}) = 2n_2 n_4 \cdots n_{i-1}$; see Proposition 2.1. $\qquad \square$

Proof of Theorem 5.1 In Section 2.4 it was observed that the wreath product, with its natural imprimitive action, is contained in $\mathrm{Aut}(\mathcal{K}_r)$. Hence, by induction, it suffices to show that the collection

$$\mathrm{supp}(\mathcal{K}_{r-1}^{(k)}) = \{k\} \times \Omega_{r-1}, \quad k \in \{1, \ldots, n_r\}, \tag{5.2}$$

constitutes a system of blocks for the action of $\mathrm{Aut}(\mathcal{K}_r)$ on Ω_r. For $r = 1$ this is clearly the case. Hence suppose that $r \geq 2$.

For $t \in \mathbb{N} \cup \{\infty\}$ we define an undirected graph $\Gamma_t(\mathcal{K}_r)$ with the following vertex set and edge set: $\mathbf{V}\Gamma_t(\mathcal{K}_r) := \Omega_r$, and $\mathbf{E}\Gamma_t(\mathcal{K}_r)$ consists of edges, joining ω_1 and ω_2 whenever there exists an indecomposable element $\mathbf{v} \in \mathcal{K}_r$ such that $\mathrm{wt}(\mathbf{v}) \leq t$ and $\{\omega_1, \omega_2\} \subseteq \mathrm{supp}(\mathbf{v})$. Clearly, $\mathrm{Aut}(\mathcal{K}_r)$ preserves the graph structure of $\Gamma_t(\mathcal{K}_r)$.

By a simple induction argument we deduce from Lemma 5.2 (1) that

(i) $\Gamma_\infty(\mathcal{K}_r)$ is connected if $r \equiv_2 1$,
(ii) $\Gamma_\infty(\mathcal{K}_r)$ has precisely n_r connected components if $r \equiv_2 0$.

Moreover, in the case $r \equiv_2 0$, the vertex sets of the connected components of $\Gamma_\infty(\mathcal{K}_r)$ are exactly the sets listed in (5.2) which thus form a system of blocks, as wanted.

Now suppose that $r \equiv_2 1$ and put $t(r) := 2n_2 n_4 \cdots n_{r-1}$. Again by induction we draw from Lemma 5.2 the more precise conclusion that $\Gamma_{t(r)}(\mathcal{K}_r)$ is connected, while $\Gamma_{t(r)-1}(\mathcal{K}_r)$ falls into $n_r n_{r-1}$ connected components whose vertex sets are precisely the sets

$$\mathrm{supp}(\mathcal{K}_{r-2}^{(k,m)}) = \{(k,m)\} \times \Omega_{r-2}, \quad (k,m) \in \{1, \ldots, n_r\} \times \{1, \ldots, n_{r-1}\}. \quad (5.3)$$

In order to proceed we define a variation of the graphs considered thus far. For $\mathbf{v} \in \mathcal{K}_r$ let $\widetilde{\Gamma}_{\mathbf{v}}(\mathcal{K}_r)$ denote the graph which is obtained from $\Gamma_{t(r)-1}(\mathcal{K}_r)$ by adding possibly extra edges, connecting ω_1 and ω_2 whenever $\{\omega_1, \omega_2\} \subseteq \mathrm{supp}(\mathbf{v})$. Let $\Delta_{\mathbf{v}} := \Delta_{\mathbf{v}}(\mathcal{K}_r)$ denote the vertex set of the connected component in $\widetilde{\Gamma}_{\mathbf{v}}(\mathcal{K}_r)$ which contains $\mathrm{supp}(\mathbf{v})$.

Lemma 5.2 shows that, if $\mathbf{v} \in \mathcal{K}_r$ is indecomposable with $\mathrm{wt}(\mathbf{v}) = t(r)$, then either $|\Delta_{\mathbf{v}}| = 2|\Omega_{r-1}|$ or $|\Delta_{\mathbf{v}}| = |\Omega_{r-2}|$. Indeed, in the former case $\Delta_{\mathbf{v}}$ is the union of two distinct sets listed in (5.2), while in the latter case $\Delta_{\mathbf{v}}$ is one of the sets listed in (5.3). This implies that the sets in (5.2) can be characterised as intersections $\Delta_{\mathbf{v},\mathbf{w}} := \Delta_{\mathbf{v}} \cap \Delta_{\mathbf{w}}$ where $\mathbf{v}, \mathbf{w} \in \mathcal{K}_r$ are indecomposable with $\mathrm{wt}(\mathbf{v}) = \mathrm{wt}(\mathbf{w}) = t(r)$ and $|\Delta_{\mathbf{v},\mathbf{w}}| = |\Omega_{r-1}|$. From this description it follows that the sets in (5.2) form a system of blocks, as wanted. □

6 Symmetric, alternating and cyclic groups

Let $N \in \mathbb{N}$, and let $\mathcal{V} = \bigoplus_{i=1}^{N} \mathbb{F}_2 \mathbf{e}_i$ be an $\mathbb{F}_2$-vector space of dimension N, with fixed standard basis $\mathbf{e}_i$ indexed by $i \in \{1, \ldots, N\}$. Put $\mathbf{a} := \sum_{i=1}^{N} \mathbf{e}_i$. We refer to the following four codes as *elementary codes*:

$$\mathcal{E}_0 := \{\mathbf{0}\}, \quad \mathcal{E}_1 := \mathbb{F}_2 \mathbf{a}, \quad \mathcal{E}_2 := \{\mathbf{v} \in \mathcal{V} \mid \mathrm{wt}(\mathbf{v}) \equiv_2 0\}, \quad \mathcal{E}_3 := \mathcal{V}.$$

If $N = 1$, then $\mathcal{E}_0 = \mathcal{E}_2$ and $\mathcal{E}_1 = \mathcal{E}_3$; if $N = 2$, then $\mathcal{E}_1 = \mathcal{E}_2$. Otherwise the four codes are distinct. But note that $\mathcal{E}_0$ and $\mathcal{E}_3$, respectively $\mathcal{E}_1$ and $\mathcal{E}_2$, are orthogonal to one another with respect to the standard inner product. Clearly, the automorphism group of any of the elementary codes is the full symmetric group $\mathrm{Sym}(N)$. We record the following observation and, for completeness, indicate a short proof; cf. [7, Section 4].

Proposition 6.1 *Let $\mathcal{C}$ be a binary linear code of length N. If $\mathrm{Alt}(N) \leq \mathrm{Aut}(\mathcal{C})$ and $N \neq 2$, then $\mathcal{C}$ is one of the elementary codes $\mathcal{E}_0, \ldots, \mathcal{E}_3$.*

Proof Suppose that $\mathrm{Alt}(N) \leq \mathrm{Aut}(\mathcal{C})$ and $N \geq 3$. We may assume that $\mathcal{C} \nsubseteq \mathcal{E}_1$ so that we find $\mathbf{v} \in \mathcal{C}$ with $0 < \mathrm{wt}(\mathbf{v}) < N$. Put $k := \mathrm{wt}(\mathbf{v})$. As $\mathrm{Alt}(N)$ acts k-homogeneously, we may assume that $\mathbf{v} = \sum_{i=1}^{k} \mathbf{e}_i$ where $1 \leq k < N$. If $k = 1$, then $\mathcal{C} = \mathcal{E}_3$. If $k \geq 2$, then applying the 3-cycle $\sigma := (1, k, k+1) \in \mathrm{Alt}(N)$, we see that $\mathbf{e}_1 + \mathbf{e}_{k+1} = \mathbf{v} + \mathbf{v}^\sigma \in \mathcal{C}$, hence $\mathcal{E}_2 \subseteq \mathcal{C}$. $\square$

Corollary 6.2 *Let $\mathcal{C}$ be a binary linear code of length $N \geq 3$. Then $\mathrm{Aut}(\mathcal{C}) \neq \mathrm{Alt}(N)$.*

Now we prove Proposition A and Theorem B.

Proof of Proposition A Let $\mathcal{C}$ be a binary cyclic code of length N such that $G = \mathrm{Aut}(\mathcal{C})$ is cyclic of odd order. Since G contains a regular cyclic subgroup of order N and since any transitive cyclic subgroup of $\mathrm{Sym}(N)$ has order precisely N, we deduce that $\mathrm{Aut}(\mathcal{C}) = C_N$. We may realise a code isomorphic to $\mathcal{C}$ as an ideal $\mathcal{I}$ of the finite ring $\mathcal{R} := \mathbb{F}_2[X]/(X^N - 1)$, equipped with the standard basis $1, X, \ldots, X^{N-1}$. The ideal $\mathcal{I}$ is principal and invariant under the Frobenius automorphism of $\mathcal{R}$. The latter induces a permutation π of the standard basis, given by $X^m \mapsto X^{2m}$ where exponents are to be read as integers modulo N. As π fixes the basis element 1, it can only belong to a regular cyclic group, if it is trivial. Thus $N = 1$ or $N = 2$. Since N is odd, we conclude that $\mathcal{C} = \{0\}$, and $\mathrm{Aut}(\mathcal{C})$ is trivial. $\square$

Proof of Theorem B Let $\mathcal{C}$ be a binary cyclic code of length N such that $\mathrm{Aut}(\mathcal{C})$ is isomorphic to an alternating group $\mathrm{Alt}(n)$ of degree $n \geq 3$. An exact factorisation of $\mathrm{Alt}(n)$ consists of two subgroups $G, H \leq \mathrm{Alt}(n)$ such that $\mathrm{Alt}(n) = GH$ and $G \cap H = 1$. Since $\mathrm{Aut}(\mathcal{C})$ contains a regular cyclic subgroup of order N which is complemented by any point stabiliser, this provides an exact factorisation $\mathrm{Alt}(n) = GH$ with one of the groups G, H cyclic of order N. Exact factorisations of alternating groups were studied by Wiegold and Williamson [10]. Adhering to the notation in [10, Theorem A], our setting allows for two possibilities. It could be that G is cyclic of odd order $n = N$ and $H \cong \mathrm{Alt}(n-1)$, but this would contradict Corollary 6.2. The only other possibility is that $n = 8$, that $G \cong \mathrm{AGL}(3, 2)$ is an affine group and H is cyclic of order $N = 15$. Noting that $\mathrm{Alt}(8) \cong \mathrm{PSL}(4, 2) = \mathrm{P\Gamma L}(4, 2)$, we observe that this group does indeed arise as the automorphism group of the binary Hamming code of length $2^4 - 1 = 15$. $\square$

7 Primitive permutation groups

In this section we prove Theorem E, using results from the well-developed theory of permutation groups and modular permutation representations.

Let $N \in \mathbb{N}$. Let $G \leq \mathrm{Sym}(N)$ be the automorphism group of a binary cyclic code $\mathcal{C}$, and suppose that G is a primitive permutation group. Then G contains a regular cyclic subgroup and hence one of the following holds; see [4, Theorem 3].

(1) $C_p \leq G \leq \mathrm{AGL}(1, p)$ where $p = N$ is prime.
(2) $G = \mathrm{Sym}(N)$, or $G = \mathrm{Alt}(N)$ where $N \geq 3$ is odd.
(3) $\mathrm{PGL}(d, q) \leq G \leq \mathrm{P\Gamma L}(d, q)$ where $d \geq 2$, $q = p^k$ is a prime power and $N = (q^d - 1)/(q - 1)$.
(4) $G = \mathrm{PSL}(2, 11)$, M_{11} or M_{23} where $N = 11, 11$ or 23 respectively.

Proof of Theorem E We consider the four cases listed above.

(1) Suppose that $C_p \leq G \leq \mathrm{AGL}(1, p)$ where $p = N$ is prime. Here $\mathrm{AGL}(1, p)$ denotes the affine group of degree 1. If $p = 2$ then $G = \mathrm{Sym}(2)$ will be covered by case (2) below. So suppose that $p \geq 3$. Proposition A shows that $C_p \lneqq G$. If $p = 3$, then $G = \mathrm{AGL}(1, 3) = \mathrm{Sym}(3)$ will be covered by case (2) below. Now suppose that $p \geq 5$. For a contradiction assume that $G = \mathrm{AGL}(1, p)$. From [8, Table 1 and Lemma 2] we deduce that the underlying code $\mathcal{C}$ is elementary, and hence $G = \mathrm{Aut}(\mathcal{C}) = \mathrm{Sym}(p)$, a contradiction.

(2) In Section 6 it was shown that the symmetric group $\mathrm{Sym}(N)$ occurs as the automorphism group of the elementary codes. According to Corollary 6.2 the alternating group $\mathrm{Alt}(N)$, $N \geq 3$, does not occur as the automorphism group of a binary linear code of length N.

(3) Suppose that $\mathrm{PGL}(d, q) \leq G \leq \mathrm{P\Gamma L}(d, q)$ where $d \geq 2$, $q = p^k$ is a prime power and $N = (q^d - 1)/(q - 1)$. First we assume that $d = 2$ and arrive at a contradiction. As $\mathrm{PGL}(2, q)$ acts 3-transitively on 1-dimensional projective space $\mathbb{P}^1(\mathbb{F}_q)$, we deduce from [8, Table 1 and Lemma 2] that the underlying code $\mathcal{C}$ is elementary, and hence $G = \mathrm{Aut}(\mathcal{C}) = \mathrm{Sym}(N)$, a contradiction. Hence $d \geq 3$, and, similarly, we deduce from [8, Table 1 and Lemma 2] that $p = 2$ and hence $q = 2^k$.

Let $\mathcal{V}$ denote the permutation module over $\mathbb{F}_2$, associated to the natural action of $\mathrm{PGL}(d, q)$ on $(d - 1)$-dimensional projective space $\mathbb{P}^{d-1}(\mathbb{F}_q)$. Let $\mathcal{U}_1$ be a $\mathrm{PGL}(d, q)$-submodule of $\mathcal{V}$. We claim that $\mathcal{U}_1$ is automatically $\mathrm{P\Gamma L}(d, q)$-invariant. Indeed, let σ be a generator of the cyclic group $\mathrm{P\Gamma L}(d, q)/\mathrm{PGL}(d, q) \cong \mathrm{Aut}(\mathbb{F}_q | \mathbb{F}_2)$. Then $\mathcal{U}_2 := \mathcal{U}_1^\sigma$, regarded as a $\mathrm{PGL}(d, q)$-module, is simply a twist of $\mathcal{U}_1$. Writing $\overline{\mathbb{F}_2}$ for the algebraic closure of $\mathbb{F}_2$, we conclude that the composition factors of the $\overline{\mathbb{F}_2}\mathrm{PGL}(d, q)$-modules $\overline{\mathcal{U}_1} := \overline{\mathbb{F}_2} \otimes \mathcal{U}_1$ and $\overline{\mathcal{U}_2} := \overline{\mathbb{F}_2} \otimes \mathcal{U}_2$ are the same. The submodules of the $\overline{\mathbb{F}_2}\mathrm{PGL}(d, q)$-module $\overline{\mathcal{V}} := \overline{\mathbb{F}_2} \otimes \mathcal{V}$ are uniquely determined by their composition factors; see [1]. Hence we conclude that $\overline{\mathcal{U}_1} = \overline{\mathcal{U}_2}$ and this implies $\mathcal{U}_1 = \mathcal{U}_2$. We obtain $G = \mathrm{P\Gamma L}(d, q)$, as wanted.

For $d \geq 3$ and $q = 2^k$ we still need to justify that the permutation group $\mathrm{P\Gamma L}(d, q)$ does indeed occur as the automorphism group of a suitable binary cyclic code $\mathcal{K}$. The explicit description of permutation modules of $\mathrm{PGL}(d, q)$ in [1] guarantees the existence of a non-elementary binary cyclic code $\mathcal{K}$ of length $N = (q^n - 1)/(q - 1)$ such that $\mathrm{PGL}(d, q) \leq \mathrm{Aut}(\mathcal{K})$. From [6] we conclude that either $\mathrm{Aut}(\mathcal{K}) \subseteq \mathrm{P\Gamma L}(d, q)$ or $\mathrm{Alt}(N) \subseteq \mathrm{Aut}(\mathcal{K})$. Proposition 6.1 rules out the second possibility, and hence our argument above implies that $\mathrm{Aut}(\mathcal{K}) = \mathrm{P\Gamma L}(d, q)$.

(4) A finite computation shows that of the three possible permutation groups precisely one, namely the Mathieu group M_{23} acting as a permutation group of degree 23, occurs as the automorphism group of a binary cyclic code, namely the binary Golay code. □

Table 1 Selected examples of automorphism groups of binary cyclic codes

Ref. no.	$[N, k, d]$-code $\mathcal{C}$	Aut($\mathcal{C}$)	Ref. in [2]
1	$[40, 35, 2]$	$\mathrm{Sym}(5) \wr \mathrm{Sym}(2) \wr \mathrm{Sym}(4)$	E.11-4
2	$[48, 43, 2]$	$\mathrm{Sym}(6) \wr \mathrm{Sym}(2) \wr \mathrm{Sym}(4)$	E.17-6
3	$[48, 34, 2]$	$\mathrm{Sym}(2) \wr \mathrm{Sym}(2) \wr \mathrm{Sym}(6) \wr \mathrm{Sym}(2)$	E.17-17
4	$[35, 20, 3]$	$\mathrm{PSL}(3, 2) \wr \mathrm{Sym}(5)$	E.7-6
5	$[35, 28, 4]$	$\mathrm{Sym}(5) \times \mathrm{PSL}(3, 2)$	E.7-4
6	$[45, 27, 4]$	$(\mathrm{Sym}(5) \times \mathrm{Sym}(3)) \wr \mathrm{Sym}(3)$	E.15-16
7	$[48, 32, 4]$	$(\mathrm{Sym}(8) \wr \mathrm{Sym}(2)) \times \mathrm{Sym}(3)$	E.17-21
8	$[35, 20, 6]$	$\mathrm{Sym}(5) \times (C_3 \ltimes C_7)$	E.7-7
9	$[85, 73, 4]$	$\mathrm{Sym}(5) \times (C_8 \ltimes C_{17})$	cf. B.3

8 Examples

In this section we give several explicit examples of binary cyclic codes with automorphism groups whose appearance can not be fully explained by the results in this paper. The examples are based on computer calculations carried out by the first author as part of his PhD project [2].

8.1 Other types of groups

In [2, Appendices B-I] one finds, in particular, a systematic listing of the non-soluble groups which occur as automorphism groups of binary cyclic codes up to length 70. In Table 1 we select nine single examples, in order to illustrate that groups more complicated than those covered by Theorems C, D and E occur.

The first three examples indicate that one should be able to generalise Theorem C to include symmetric groups of even degree. However, the experimental evidence in [2] also suggests that the automorphism group of a binary cyclic group is never an iterated wreath product of symmetric groups ending in $\mathrm{Sym}(2) \wr \mathrm{Sym}(2)$.

8.2 Automorphism groups of affine type

Theorem E gives a description of the primitive permutation groups which occur as automorphism groups of binary cyclic codes. However, it remains an open problem to find out precisely which subgroups of the affine groups $\mathrm{AGL}(1, p)$ occur, where $p \geq 5$ is prime.

Let p be a prime. Then every binary cyclic code of length $N = p$ can be realised as an ideal of the residue class ring $R := \mathbb{F}_2[X]/(X^p - 1)$. Let f denote the order of 2 in the multiplicative group $\mathbb{F}_p^*$ and put $e := (p - 1)/f$. Then $X^p - 1$ factorises over $\mathbb{F}_2$ as a product of $X - 1$ and e distinct irreducible polynomials of degree f. Accordingly, R decomposes as a direct sum of the field $\mathbb{F}_2$ and e copies of the field $\mathbb{F}_{2^f}$. Hence the number of ideals of R is 2^{e+1}. The binary cyclic codes corresponding to these ideals fall into a certain number of isomorphism classes. The dimensions of the codes range over the values kf and $kf + 1$, where $k \in \{0, \ldots, e\}$. In the special

Table 2 Subgroups of AGL(1, p) as automorphism groups of binary cyclic codes of length $N = p$ in the range $5 \leq p \leq 79$

p	$p-1$	param. m such that $\mathrm{Aut}(\mathcal{C}) \cong C_m \ltimes C_p$	$[N, k, d]$-parameters for codes $\mathcal{C}$ (in pairs, corresponding to dual codes)
17	$16 = 2^4$	$8 = 2^3$	$[17, 8, 6]$, $[17, 9, 5]$
31	$30 = 2 \cdot 3 \cdot 5$	5	$[31, 10, 12]$, $[31, 21, 5]$; $[31, 11, 11]$, $[31, 20, 6]$; $[31, 15, 6]$, $[31, 16, 5]$; $[31, 15, 8]$, $[31, 16, 6]$
		$10 = 2 \cdot 5$	$[31, 10, 10]$, $[31, 21, 5]$; $[31, 11, 10]$, $[31, 20, 6]$
		$15 = 3 \cdot 5$	$[31, 15, 8]$, $[31, 16, 7]$
41	$40 = 2^3 \cdot 5$	$20 = 2^2 \cdot 5$	$[41, 20, 10]$, $[41, 21, 9]$
43	$42 = 2 \cdot 3 \cdot 7$	$14 = 2 \cdot 7$	$[43, 14, 14]$, $[43, 29, 6]$; $[43, 15, 13]$, $[43, 28, 6]$
47	$46 = 2 \cdot 23$	23	$[47, 23, 12]$, $[47, 24, 11]$
71	$70 = 2 \cdot 5 \cdot 7$	$35 = 5 \cdot 7$	$[71, 35, 12]$, $[71, 36, 11]$
73	$72 = 2^3 \cdot 3^2$	$9 = 3^2$	$[73, 9, 28]$, $[73, 64, 3]$; $[73, 10, 28]$, $[73, 63, 4]$; $[73, 18, 24]$, $[73, 55, 6]$; $[73, 19, 21]$, $[73, 54, 6]$; $[73, 27, 16]$, $[73, 46, 8]$; $[73, 27, 16]$, $[73, 46, 9]$; $[73, 27, 18]$, $[73, 46, 9]$; $[73, 27, 20]$, $[73, 46, 9]$; $[73, 28, 13]$, $[73, 45, 8]$; $[73, 28, 16]$, $[73, 45, 10]$; $[73, 28, 17]$, $[73, 45, 10]$; $[73, 36, 10]$, $[73, 37, 9]$; $[73, 36, 12]$, $[73, 37, 9]$; $[73, 36, 12]$, $[73, 37, 10]$; $[73, 36, 14]$, $[73, 37, 9]$; $[73, 36, 14]$, $[73, 37, 12]$; $[73, 36, 14]$, $[73, 37, 13]$
		$18 = 2 \cdot 3^2$	$[73, 18, 24]$, $[73, 55, 6]$; $[73, 19, 19]$, $[73, 54, 6]$; $[73, 36, 12]$, $[73, 37, 12]$
		$36 = 2^2 \cdot 3^2$	$[73, 36, 14]$, $[73, 37, 13]$
79	$78 = 2 \cdot 3 \cdot 13$	$39 = 3 \cdot 13$	$[79, 39, 16]$, $[79, 40, 15]$

case where $e = 1$, there are only four codes, namely the elementary codes discussed in Section 6. Considering a different example, if $p = 2^l - 1$ is a Mersenne prime, then $e = (p-1)/l$ and $f = l$ so that there are $2^{((2^l-2)/l)+1} \approx 2^{p/\log(p)}$ ideals and a priori an equal number of corresponding binary cyclic codes of length p to consider. Clearly, as p increases efficient algorithms are required to study such a large number of codes.

Computer calculations show that, in the range $5 \leq p \leq 79$, there exists a binary cyclic code $\mathcal{C}$ of prime length $N = p$ such that $\mathrm{Aut}(\mathcal{C})$ is a subgroup of the affine group AGL(1, p) if and only if $p \in \{17, 31, 41, 43, 47, 71, 73, 79\}$. For primes p in this range, Table 2 lists the basic parameters $[N, k, d]$ of all binary cyclic codes $\mathcal{C}$ of length $N = p$ such that $\mathrm{Aut}(\mathcal{C}) \cong C_m \ltimes C_p$ is a subgroup of the affine group AGL(1, p). For convenience the prime factorisations of $p - 1$ and m are exhibited. For $p \in \{5, 7, 11, 13, 19, 23, 29, 37, 53, 59, 61, 67\}$ there exists no binary cyclic code $\mathcal{C}$ of prime length $N = p$ such that $\mathrm{Aut}(\mathcal{C})$ is a subgroup of AGL(1, p). Except for $p = 7$ and $p = 23$, this fact can be explained by the observation that the polynomial $X^p - 1$ admits over $\mathbb{F}_2$ only one irreducible factor in addition to the trivial factor

$X - 1$: according to the argument given above this implies that all binary cyclic codes of the lengths in question are elementary.

References

1. Bardoe, M., Sin, P.: The permutation modules for GL($n + 1$, $\mathbb{F}_q$) acting on $\mathbb{P}^n(\mathbb{F}_q)$ and $\mathbb{F}_q^{n+1}$. J. London Math. Soc. **61**, 58–80 (2000)
2. Bienert, R.: Über Automorphismengruppen von zyklischen Codes. Dissertation, Heinrich-Heine-Universität (2007)
3. Huffman, W.C.: Codes and groups. In: Handbook of Coding Theory, vol. II, pp. 1345–1440. North-Holland, Amsterdam (1998)
4. Jones, G.: Cyclic regular subgroups of primitive permutation groups. J. Group Theory **5**, 403–407 (2002)
5. Key, J.D., Seneviratne, P.: Binary codes from rectangular lattice graphs and permutation decoding. European J. Combin. **28**, 121–126 (2007)
6. Kantor, W.M., McDonough, T.P.: On the maximality of PSL($d + 1$, q), $d \geq 2$. J. London Math. Soc. **8**, 426 (1974)
7. Knapp, W., Schmid, P.: Codes with prescribed permutation group. J. Algebra **67**, 415–435 (1980)
8. Mortimer, B.: The modular permutation representations of the known doubly transitive groups. Proc. London Math. Soc. **41**, 1–20 (1980)
9. Phelps, K.T.: Every finite group is the automorphism group of some linear code. Congr. Numer. **49**, 139–141 (1985). Proceedings of the Sixteenth Southeastern International Conference on Combinatorics, Graph Theory and Computing (Boca Raton, Fl., 1985)
10. Wiegold, J., Williamson, A.G.: The factorisation of the alternating and symmetric groups. Math. Z. **175**, 171–179 (1980)