On the binary codes of length 552 which admit the simple group Co_3 as a transitive permutation group

Wolfgang Knapp, Mathematisches Institut, Universität Tübingen, Germany

wolfgang.knapp@uni-tuebingen.de

Bernardo Rodrigues, Mathematics, University of Pretoria, South Africa

bernardo.rodrigues@up.ac.za

Abstract

In this this paper all binary codes of length 552 are determined which admit the sporadic simple group Co_3 as an imprimitive transitive permutation group. Our aim is to understand the results also by arguments and to discuss the combinatorial properties of the codes as well as their relation to some special properties of the Leech lattice group Co_3. We obtain for all codes the weight enumerators (with two exceptions) and in many interesting cases the classification of codewords under the action of the group of code automorphisms Co_3. The exempted codes are both self-dual and have minimum weight 12

Mathematics Subject Classifications: 05B05 05B20 05B25 05C25 20B25 20B40 20C05 20D08 94B05 94B25

Keywords: linear code, Hamming weight, weight distribution, dual code, self-dual, MacWilliams' identities, automorphism group, permutation group, Conway simple groups, representation theory, module, dual module, permutation module.

Introduction

The purpose of this paper is to determine all binary codes of length 552 which admit the sporadic simple group Co_3 as an imprimitive transitive permutation group. The second author has obtained the codes by computation. Our aim is to get these results , but presenting theoretical arguments and to discuss the combinatorial properties of the codes and their relation to some special properties of the Leech lattice group Co_3. We obtain all weight enumerators (with two exceptions) and in many interesting cases the classification of codewords under the action of the group of code automorphisms Co_3. The two exempted codes are both self-dual and have minimum weight 12. This work grew out of a collaborative research visit of the second author at the University of Tübingen in November 2018.

We prove the following

Main Theorem.
Let $F = \mathbb{F}_2$ and let Ω be a set of size 552 on which Co_3 acts transitively. The FG-submodule lattice of $F\Omega$ (lattice of FG-invariant codes of length 552) is as displayed in the overview Table I. The 19 codes of the lattice obey the orthogonality rule ${C_i}^{\perp} = C_{552-i}$. For all occurring $i \neq 276$ we have exactly one code C_i of dimension i and all 5 codes C^j_{276} of dimension 276 are self-dual. The group theoretic and combinatorial properties of these codes are described in detail in Section 3.

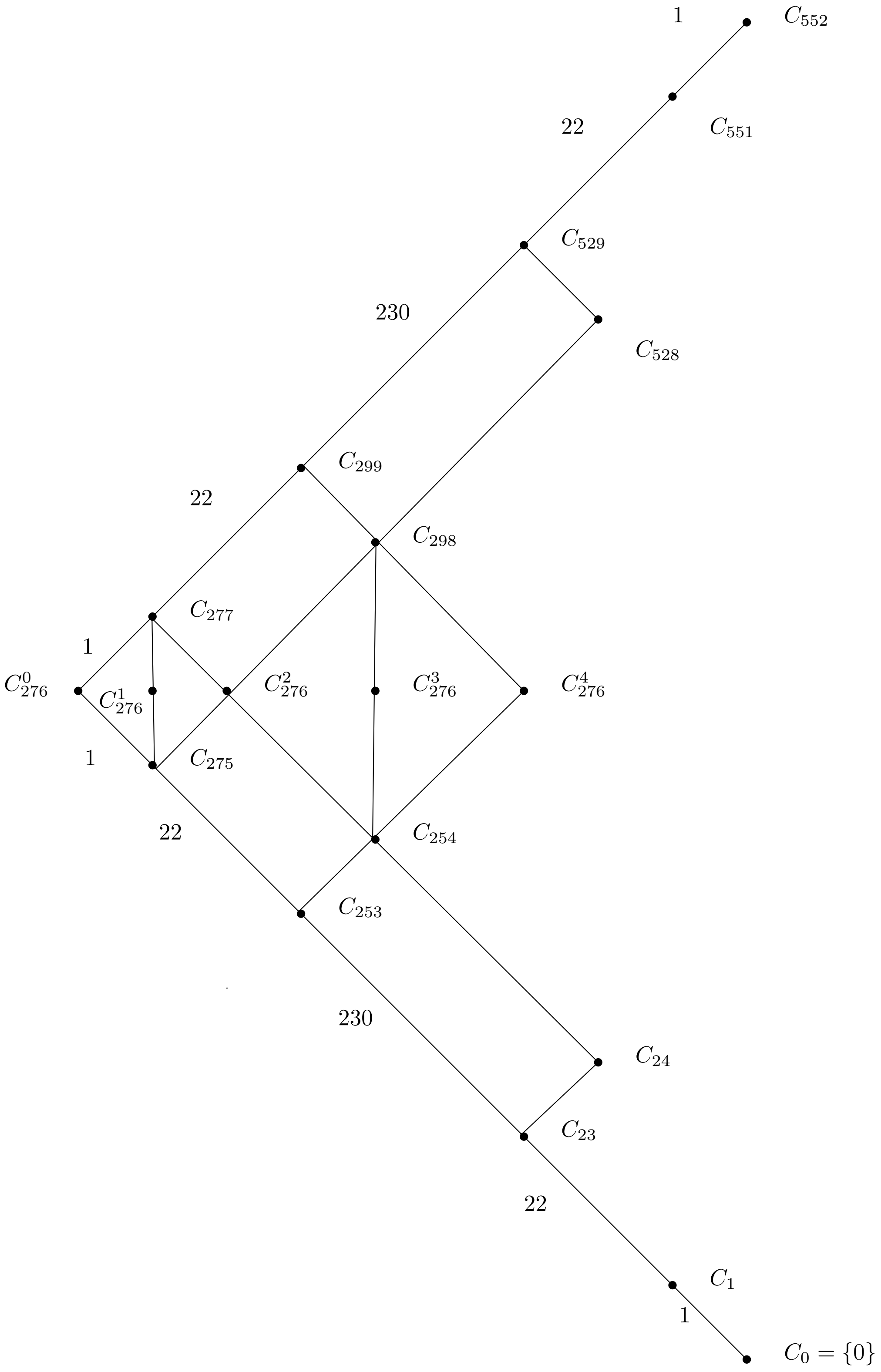
1
C_{552}
22
C_{551}
C_{529}
230
C_{528}
C_{299}
22
C_{298}
C_{277}
1
C^0_{276}
C^1_{276}
C^2_{276}
C^3_{276}
C^4_{276}
1
C_{275}
22
C_{254}
C_{253}
230
C_{24}
C_{23}
22
C_1
1
$C_0 = \{0\}$

Table I

1 Background and Preliminary results

We shall use the following concepts from coding theory.

An ordered pair (V, B), where V is a finitely generated free (left) F-module over a commutative ring F and B is an F-basis of V, is called a *Hamming space* over F. In this paper F will always be a field whose multiplicative group is denoted by $F^{\#}$. $\dim_F V$ is called the length of the Hamming space (V, B). A Hamming space (V, B) carries the following canonical structures.

Let $B = (e_i)_{i \in \Omega}$ and let $x = \sum x_i e_i$ for any $x \in V$.

(i) V carries the nondegenerate symmetric bilinear form $(x, y) \mapsto \langle x, y \rangle = \langle x, y \rangle_B = \sum x_i y_i$.

(ii) V carries the norm $w_B : x \mapsto w(x) = w_B(x) := \sum |x_i|$ where $| \cdot |$ denotes the trivial absolute value of F. $w(x) = w_B(x)$ is called the (Hamming) *weight* of x. Let $\text{supp}(x) = \text{supp}_B(x) = \{e_i : x_i \neq 0\}$ denote the support of x with respect to B. Then, of course, $w(x) = |\text{supp}(x)|$.

(iii) To the norm $w = w_B$ there corresponds canonically the *Hamming metric* $d = d_B$ defined by $d_B(x, y) := w_B(x - y)$.

For any subset X of V let $W_i(X)$ denote the set of all vectors in X of weight i, called the *i-weight class* of X. Furthermore let $X^\perp$ denote the set of all vectors in V orthogonal to every element of X with respect to $\langle \cdot, \cdot \rangle$. Of course, $X^\perp = \langle X \rangle^\perp$ is a (linear) subspace of V of dimension $\dim V - \dim\langle X \rangle$.

Any triple (V, B, C) where C is a subspace of V is called a *linear code* having *ambient space* V and *ambient basis* B. If the Hamming space (V, B) is given by the context we usually write $C = (V, B, C)$. C is said to be an $[n, k]$-code if $\dim V = n$ and $\dim C = k; n = \dim V$ is called also the *length* of C. Throughout the paper we shall follow the convention that a "code" is always understood to be a linear code.

If C is a code of length n, the $(n+1)$-tuple $(w_i(C))_{0 \le i \le n}$ where $w_i(C) = |W_i(C)|$ is called the weight distribution of C, and the homogeneous polynomial $\sum w_i(C) \xi^i \eta^{n-i} \in \mathbb{C}[\xi, \eta]$ of degree n is called the weight enumerator of C. The weight enumerators of a code C and of its "dual" $C^\perp$ determine each other via the MacWilliams identities, see e.g. [12].

If $F = \mathbb{F}_2$ is the field of 2 elements, a code C is also called a binary code; if all occuring weights in a binary code are even, then C is called even; if all occurring weights in a binary code C are multiples of 4 then C is called doubly-even; if all occurring weights in a binary code C are multiples of 8 then C is called triply-even.

If $C \neq 0$ then $\mu(C) := \min\{i : 0 \neq i \text{ and } w_i(C) \neq 0\}$ is called the *minimum weight* of C. By convention we denote a linear code over F of length n, dimension k and minimum weight d as an $[n, k, d]$-code over F, in short as an $[n, k, d]_q$-code if $|F| = q$.

For computational purposes the ambient vector space V of a code C can be standardized as F^n with $n = \dim V$ and standard ambient basis $B = (e_i)_{1 \le i \le n}$.

It is clear that permutations of the ambient basis in their linear extension to the ambient space preserve the Hamming weight. In this paper we will consider mostly binary codes ($F = \mathbb{F}_2$). Then all code automorphims can be understood as permutations of the ambient basis which (linearly extended) leave the code invariant; the corresponding concept of isomorphism is accordingly simple. (In the non-binary case one has to consider in general monomial transformations as isomorphisms and a more complicated concept of automorphisms involving field automorphisms. However, it makes sense to consider permutation automorphisms also in the non-binary case.)

Let Sym_Ω denote the full symmetric permutation group of the set Ω and we write Sym_n for the symmetric group acting on $\{1, \ldots, n\}$ and Alt_n for the alternating group on $\{1, \ldots, n\}$. Recall that a group G acting on a set $\Omega \neq \emptyset$ from the right via $(\alpha, g) \mapsto \alpha^g$ is called *transitive* if for any $\alpha, \beta \in \Omega$ there exists an element $g \in G$ auch that $\alpha^g = \beta$. (The corresponding definition for left actions is obvious.) A group G of permutations of Ω is called transitive if the natural action of G is transitive. Let k be a positive integer. The action of G on Ω (or the permutation group G on Ω) is called k-fold transitive (in short k-transitive) if the action of G on the set of injective k-tuples over Ω $((\alpha_i)_{1 \leq i \leq k}, g) \mapsto (\alpha_i^g)_{1 \leq i \leq k}$ is transitive. The action of G on Ω (or the permutation group G on Ω) is called *primitive* if there are no G-invariant equivalence relations besides the trivial ones $\{(\alpha, \alpha) : \alpha \in \Omega\}$ and $\Omega \times \Omega$. A transitive action of G or permutation group G is called *imprimitive* if there exists a non-trivial G-invariant equivalence relation (or "system of imprimitivity"); the equivalence classes $\eta(\alpha)$ of such a equivalence relation η are called *blocks* of G belonging to η, We write $\Omega/\eta = \{\eta(\alpha) : \alpha \in \Omega\}$ for the block system defined by η.

If a group G acts transitively on a set Ω and $\alpha \in \Omega$ then there is a natural bijection between the subgroups U of G containing the point stabilizer G_α and the set of blocks containing α belonging to G-invariant equivalence relations , given by $U \mapsto \alpha^U = \{\alpha^g : g \in U\}$. In particular, the length of the corresponding block is the subgroup index $|U : G_\alpha|$, an invariant of the G-invariant equivalence relation. Consequently, G acts primitively on Ω if and only if G acts transitively on Ω and G_α is a maximal subgroup of G for any $\alpha \in \Omega$.

If G acts transitively on Ω and $\alpha \in \Omega$ then the number of orbits of G_α in Ω (the "suborbits of G in Ω") is independent of the choice of α and is called the *rank* of the action (or of G), denoted by $\mathrm{rk}_\Omega(G) = \mathrm{rk}(G)$. Clearly, the rank of G is also the number of orbits of G on the set $\Omega \times \Omega$ with componentwise action; these orbits are called *orbitals* of G (on Ω). With the rule $\Delta(\alpha) = \{\beta : (\alpha, \beta) \in \Delta\}$ for orbitals Δ we have the convenient notation $\Delta(\alpha)^g = \Delta(\alpha^g)$ for any $g \in G$ and $\alpha \in \Omega$. To any orbital Δ we associate its mirror image (or paired orbital) $\Delta' = \{(\beta, \alpha) : (\alpha, \beta) \in \Delta\}$. An orbital Δ of G is called symmetric (or self-paired) if and only if $\Delta = \Delta'$.

Clearly, a transitive group G acts 2-transitively on Ω if and only if G has rank 2. The discussion above shows that 2-transitive groups are primitive.

For our purpose the relations of these concepts to properties of the "permutation modules" related to the action of a finite group G are important. Let G act on the finite set Ω and let F be a field. The formal sums $\sum_{\alpha \in \Omega} r_\alpha \alpha$ constitute an F vector-space on which G acts as a group of F-linear mappings via $(\sum_{\alpha \in \Omega} r_\alpha \alpha)^g = \sum_{\alpha \in \Omega} r_\alpha \alpha^g$, giving the structure of an FG-module denoted by $F\Omega$. This module is called the *permutation module* over F to the action of G on Ω (or the permutation group G if G is a permutation group on Ω). Clearly the set Ω can be viewed as an F-basis of the permutation module and $(F\Omega, \Omega)$ is a Hamming space in the sense introduced above. Moreover, the action of G on $F\Omega$ preserves the Hamming weight and the canonical bilinear form with orthonormal basis Ω. So the submodules of $F\Omega$ can be considered as linear codes with ambient space $F\Omega$ and ambient basis Ω whereas G acts as a group of code automorphisms on any such code. For simplicity - with this understanding - we denote the codes and submodules with the same letters.

We need a short discussion of the relation of the rank of an action to the corresponding permutation module. The complex character of G associated with the permutation module $\mathbb{C}G$ is called the *permutation character* of G on Ω, denoted by π_Ω. Recalling the definition of a group character as value of the trace function we see that the permutation character just counts the number $\pi_\Omega(g)$ of fixed-points of $g \in G$ in Ω. If $\pi_\Omega = \sum_i m_i \chi_i$ for distinct irreducible complex characters χ_i of G then $\sum_i {m_i}^2 = \mathrm{rk}_\Omega(G)$. $m_i = (\pi_\Omega, \chi_i)$ is called the multiplicity of χ_i in π_Ω; π_Ω is called multiplicty-free iff all multiplicities of irreducible characters in π_Ω are at most 1. Note that the multiplicity of the trivial character $\mathbf{1}_G$ in π_Ω is the number of G-orbits in Ω as follows from the Cauchy-Frobenius Lemma (sometimes incorrectly called Burnside's Lemma).

In order to discuss the general fundamental properties of the endomorphism ring (F-algebra) of a permutation module $F\Omega$ we associate to any orbital Δ_i of G the endomorphism ε_i of $F\Omega$ given by $\alpha \mapsto \sum_{\beta \in \Delta_i(\alpha)} \beta$. (So the matrix of ε_i with regard to the canonical basis Ω is just the indicator matrix of the orbital Δ_i.) It is easy to check that the endomorphisms $\varepsilon_i, 1 \leq i \leq r = \mathrm{rk}_\Omega(G)$, form a basis of the F-algebra of FG-endomorphisms of $F\Omega$. This holds regardless of the field F, therefore we always have $\mathrm{rk}_\Omega(G) = \dim \mathrm{End}_{FG}(F\Omega)$. Note that the endomorphism algebra in its canonical matrix form is also called the centralizer algebra of the action of G on Ω. Recall that an FG-module is called *uniserial* if it has a unique composition series. Clearly, uniserial FG-modules are indecomposable.

As a particular case we may consider $F = \mathbb{C}$. Let for the permutation character hold $\pi_\Omega = \sum_i m_i \chi_i$ with distinct irreducible complex characters. Then the $\mathbb{C}$-algebra of $\mathbb{C}G$-endomorphims of the permutation module $\mathbb{C}G$ is semisimple and has structure $\bigoplus_i \mathbb{C}^{m_i \times m_i}$ where $\mathbb{C}^{m_i \times m_i}$ denotes the algebra of complex $m_i \times m_i$-matrices. This explains the formula $\mathrm{rk}_\Omega(G) = \sum_i {m_i}^2$.

(1.1) Lemma.
Let a finite group G act transitively on a set Ω such that the permutation character $\pi_\Omega(G)$ is multiplicity-free, and let F be a field. Then the following hold.

(i) The endomorphism F-algebra of the permutation module $F\Omega$ is commutative.

(ii) If all constituents of the permutation character are real then all orbitals of G on Ω are symmetric (self-paired).

Proof. In the case $F = \mathbb{C}$ assertion (i) is immediate considering the structure of the endomorphism algebra. Considering the basis given by the orbital endomorphisms ε_i (whose matrices have only $0, 1$ entries) now shows that commutativity carries over to any field F in any characteristic. For (ii) recall that the number of symmetric orbitals is equal to the number of real characters occurring in the permutation character π_Ω since it is multiplicity-free, see [1]. □

In the present paper we consider the simple group Co_3 in its imprimitive action on 552 points with block length 2. We show that in such a situation the permutation module $\mathbb{F}_2\Omega$ has a very special non-trivial square-nilpotent endomorphism.

(1.2) Proposition.
Let G be a finite group acting transitively but imprimitively on a set Ω with a G-invariant equivalence relation τ in Ω such that the corresponding system of imprimitivity Ω/τ consists of blocks of length 2. We may choose a transversal T of Ω/τ such that $T' = \Omega \setminus T$ is also a transversal and a bijective mapping $\alpha \mapsto \alpha'$ of T onto T' such that the blocks in Ω/τ are just the sets $\{\alpha, \alpha'\} = \tau(\alpha) = \tau(\alpha')$ for $\alpha \in T$. Let F be a field of characteristic 2. We consider the permutation module $F\Omega$. Let ε denote the endomorphism of $F\Omega$ defined by assigning $\alpha \mapsto \sum_{\beta\in\tau(\alpha)} \beta$ for $\alpha \in \Omega$, extended linearly. Then the following hold.

(i) *ε is a non-zero FG-module endomorphism of $F\Omega$ with the properties*

$\mathrm{Ker}(\varepsilon) = \mathrm{Im}(\varepsilon) = \{\sum_{\alpha\in T} r_\alpha(\alpha + \alpha') : r_\alpha \in F\}$ *and* $\varepsilon^2 = 0$.

(ii) $\mathrm{Ker}(\varepsilon) = \mathrm{Im}(\varepsilon)$ *and* $F\Omega/\mathrm{Ker}(\varepsilon)$ *are isomorphic to the permutation FG-module $F(\Omega/\tau)$ via the homomorphism theorem and the naturally given map assigning $\alpha + \alpha'$ to $\tau(\alpha)$ for $\alpha \in T$.*

(iii) $\mathrm{Ker}(\varepsilon) = \mathrm{Im}(\varepsilon) = \mathrm{Im}(\varepsilon)^\perp$ *is a maximal isotropic subspace of $F\Omega$. So it is self-dual considered as a code with ambient space $F\Omega$ and ambient basis Ω.*

Proof. We have $F(\Omega/\tau) = \mathrm{W}(\tau)$ in the sense of [8]. (i) and (ii) follow from Theorems 3 and 7 in [8] and basic algebra. (Note that we do not need the multiplicative properties of $\mathrm{W}(\tau)$). (iii) follows from (i) and (ii) by [8, Theorem 7], counting dimensions. □

All groups and combinatorial structures in this paper are assumed to be finite. In the following let $F = \mathbb{F}_2 = GF(2)$ denote the prime field in characteristic 2. Also in the following let $G = \mathrm{Co}_3$ denote the third simple group of Conway of order $2^{10}\cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23 = 496,766,566,000$.

2 The binary Co_3-invariant codes of length 276

According to the ATLAS [2] the group G has a doubly-transitive permutation representation on a set $\overline{\Omega}$ of size 276 with a point stabilizer isomorphic to the maximal subgroup

$\mathrm{M^cL} : 2$ where $\mathrm{M^cL}$ denotes the simple group of McLaughlin. The corresponding permutation character is $\pi_{\overline{\Omega}} = 1 + 275$, written as a sum of irreducible complex characters, denoted by their degree.

We determine all FG-submodules of the permutation module $F\overline{\Omega}$ and their coding theoretic properties with respect to the canonical Hamming space $(F\overline{\Omega}, \overline{\Omega})$.

(2.1) Theorem. *(i) $F\overline{\Omega}$ is a uniserial FG-module with unique composition series*

$\{0\} = C_0 < C_1 < C_{23} < C_{253} < C_{275} < C_{276} = F\overline{\Omega}$ and sequence of composition factor dimensions $(1, 22, 230, 22, 1)$.

(ii) We have $C_i^{\perp} = C_{276-i}$ for all i. C_1 is the repetition code and C_{275} is the even weight code of length 276.

(iii) C_{23} is a doubly-even self-orthogonal code with minimum weight 100 and weight enumerator $1(\xi^0\eta^{276} + \xi^{276}\eta^0) + 11,178(\xi^{100}\eta^{176} + \xi^{176}\eta^{100}) + 37,950(\xi^{112}\eta^{148} + \xi^{148}\eta^{112}) + 1,536,975(\xi^{128}\eta^{164} + \xi^{164}\eta^{128}) + 2,608,200(\xi^{132}\eta^{144} + \xi^{144}\eta^{132})$.

All Hamming-weight classes in C_{23} are G-orbits with point-stabilizers either G or maximal subgroups of G of ATLAS type $\mathrm{HS}, \mathrm{U}_4(3) : (2^2)_{133}, 2^4{\cdot}A_8, 2{\times}\mathrm{M}_{12}$ respectively.

(iv) The minimum weight of $C_{253} = C_{23}^{\perp}$ is 6 and the class of minmum weight vectors is a G-orbit of size 708,400, whose point stabilizer is a maximal subgroup of G with ATLAS type $3_+^{1+4} : 4S_6$.

(v) The weight distributions of all G-invariant subcodes C_i of $F\overline{\Omega}$ are known.

Proof. According to [14] the 2-modular permutation character of the FG-module $F\overline{\Omega}$ is the sum of irreducible 2-modular characters (denoted by their degrees) $2 \cdot 1 + 2 \cdot 22 + 1 \cdot 230$. Since $\dim \mathrm{End}_{FG}(F\overline{\Omega}) = 2$ it follows that $F\overline{\Omega}$ has a unique irreducible submodule C_1, of dimension 1. Moreover, the permutation module $F\overline{\Omega}$ is self-dual. It follows that $F\overline{\Omega}$ has a composition series as asserted in (i). Application of MeatAxe yields that there are no other submodules, so we get assertion (i). Assertion (ii) now easily follows since $F\overline{\Omega}$ is a self-dual FG-module. (iii) has been proved in [5]; alternatively it can be obtained as in [9, Section 4]. MacWilliams' identities now give the weight enumerator of $C_{253} = C_{23}^{\perp}$. Using the ATLAS [2] establishes (iv). (v) follows from all previous asssertions. □

3 The binary Co_3-invariant codes of length 552

Now we consider the simple group Co_3 in its imprimitive action on 552 points with block length 2. We know from Proposition (1.2) that the permutation module $\mathbb{F}_2\Omega$ has a very special non-trivial square-nilpotent endomorphism ε. We use the notation introduced in Proposition (1.2) and add the following notational convention:

We fix an (arbitrary) element $x \in \Omega$ and set $M^cL := G_x$. Then M^cL is isomorphic to MacLaughlin's simple group $\mathrm{M^cL}$. The group M^cL fixes in Ω exactly 2 points, x and x', and has two long orbits, Δ and Δ' of length 275 on which M^cL acts as a primitive rank 3 group. We can take $T := \Delta \cup \{ x\}$ as the chosen transversal of Ω/τ. Then $T' := \Delta' \cup \{x'\}$ is the transversal complementary to T and we may take the bijection $\Delta \to \Delta' : \beta \mapsto \beta'$ as an isomorphism of M^cL-sets. Later we will see in Proposition (3.8)(iv) that – surprisingly – there is an essential difference between x and x' when all other notations are fixed.

We use in the following always the same names for the FG-submodules of $F\Omega$ and the associated codes with ambient space $F\Omega$ and ambient basis corresponding to Ω, see the introduction. Using Proposition (1.2) we get immediately a "canonical" composition series of the permutation module as an FG module which comprises most submodules (respectively subcodes).

(3.1) Proposition.
Let $C^0_{276} := \mathrm{Ker}(\varepsilon)(= \mathrm{Im}(\varepsilon))$. Then there is a unique composition series of the permutation module $F\Omega$ containing C^0_{276}, namely

$$\{0\} = C_0 < C_1 < C_{23} < C_{253} < C_{275} < C^0_{276} < C_{277} < C_{299} < C_{529} < C_{551} < C_{552} = F\Omega,$$

where $\dim C_i = i$ for all i and C_{276+i} is the full preimage of C_i under ε for $0 < i < 276$.

Moreover, the following hold:

(1) C^0_{276} is self-dual as an FG-module and a self-dual code as well.

(2) For all i we have $C_i{}^\perp = C_{552-i}$.

(3) The weight enumerators of all codes occurring in the composition series are known:

For C^0_{276} and the codes $C_i, 0 < i < 276$, the weight enumerators can be computed starting from (2.1) by an obvious "doubling procedure" and then the weight enumerators of $C_i, 276 < i \leq 552$ are obtained by MacWilliams' identities.

Proof. Applying the FG-endomorphism ε of $F\Omega$ means that $x \in \Omega$ is replaced by $x + x'$, F-linearly extended. So one may think of C^0_{276} as the permutaion module $F\overline{\Omega}$ where the basis elements $\alpha = \{x, x'\} \in \overline{\Omega} = \Omega/\tau$ are "doubly" written as $x + x'$ in $F\Omega$. So the first part of the assertion easily follows from Proposition (1.2) and Theorem (2.1). Note that the module (code) denoted C_i in Theorem (2.1) corresponds to a module (code) denoted here also by C_i which, however, should not cause confusion. Assertion (1) is now immediate and assertion (2) follows; assertion (3) is another easy consequence. □

(3.2) Corollary.
Using the notation of Proposition (3.1) the following hold.

(i) The FG-module C_1 of fixed points is the unique minimal FG-submodule of $F\Omega$. Hence $F\Omega$ is an indecomposable FG-module. C_1 is the repetition code and has minimum weight 552.

(ii) The FG-module $C_{551} = C_1{}^\perp$ is the unique maximal FG-submodule of $F\Omega$. C_{552} is the even weight subcode of $F\Omega$.

(iii) *C_{23} is a self-orthogonal triply-even code with minimum weight 200, the codewords of minimum weight forming a G-orbit of length $11,178$ with point stabilizer isomorphic to the Higman-Sims group* HS.

(iv) *C_{253} is a self-orthogonal doubly-even code with minimum weight 12, the codewords of minimum weight forming a G-orbit of length $708,400$ with point stabilizer isomorphic to a group of ATLAS type $3^{1+4}_{+} : 4S_6$.*

(v) *C_{275} is a self-orthogonal doubly-even code with minimum weight 4, the codewords of minimum weight ($x + x' + y + y'$ where $\{x, x'\}$ and $\{y, y'\}$ are distinct G-blocks in Ω) forming a G-orbit of length $37,950$ with point stabilizer isomorphic to a group of ATLAS type* $\mathrm{U}_4(3) : (2^2)_{133}$.

(vi) *C^0_{276} is a self-dual even code with minimum weight 2, the codewords of minmum weight ($x + x'$ where $\{x, x'\}$ are G-blocks in Ω) forming a G-orbit of length 276 with point stabilizer isomorphic to* $\mathrm{M^cL} : 2$.

(vii) *If $x \in C_{529} \setminus C^0_{276}$ then the Hamming weight $w_\Omega(x) \geq 6$ and is even. Therefore all subcodes C_i with $276 < i < 551$ are even of minimum weight 2, the minimum weight codewords being contained in C^0_{276}.*

(viii) *G has 3 orbits on minimum weight codewords of the even weight subcode C_{551}. Each of the two orbits not contained in C^0_{276} generates C_{551}. Representatives for these two orbits are $x + y$ and $x + y'$ (where $\{x, x'\}$ and $\{y, y'\}$ are two distinct G-blocks) and the point stabilizers belonging to these orbits, both of length 552, are isomorphic to* $\mathrm{M^cL}$.

Proof. Since G acts transitively on Ω, the dimension of the fixed-point FG-submodule of $F\Omega$ is 1. Hence C_1 is the fixed-pont submodule of $F\Omega$. Now, let X be any irreducible FG-submodule of $F\Omega$. If $X \leq C^0_{276}$ then $X = C_1$. If $X \not\leq C^0_{276} = \mathrm{Ker}(\varepsilon)$ then $X + C^0_{276}/C^0_{276} \cong X$ is isomorphic to the trivial FG-module C_1, hence $X \leq C_1 \leq C^0_{276}$, a contradiction. So the assertions (i) and (ii) easily follow. Assertions (iii), (iv) and (v) follow from Proposition (3.1)(3) in conjunction with Theorem (2.1). Since C^0_{276} is isomorphic to $F\overline{\Omega}$ as an FG-module (vi) follows from Proposition (3.1). Since $C^0_{276} = \mathrm{Ker}(\varepsilon)$ and ε maps C_{529} onto C_{253} we get (vii). (viii) is easily verified looking at the action of ε. □

We want to determine also those FG-invariant subcodes of $F\Omega$ which do not occur in the composition series obtained in Proposition (3.1). It is useful to refine the arguments used in the proof of Corollary (3.2)(vii) by introducing a suitable notational concept.

(3.3) Definition.
Let $u \in F\Omega$. Then u is called *(partial) transversal* if and only if $\mathrm{supp}_\Omega(u)$ intersects each G-block $B = \{x, x'\}$ in at most one element. u is called *fully tranversal* if u is a transversal of the system of G-blocks, i.e. transversal and of Hamming weight 276.

(3.4) Lemma.
Let $0 \neq u \in F\Omega$.

(i) There exists a unique transversal u_1 *and a unique* $u_0 \in C^0_{276} = \mathrm{Ker}(\varepsilon)$ *such that* $u = u_o + u_1$. *We have* $\varepsilon(u) = \varepsilon(u_1)$ *and* $w_\Omega(\varepsilon(u)) = 2w_\Omega(u_1)$.

(ii) u *is transversal iff* $w_\Omega(\varepsilon(u)) = 2w_\Omega(u)$ *holds.*

Proof. Considering the action of the endomorphism ε gives (i); (ii) follows. □

(3.5) Lemma.
All elements of $C_{277} \setminus C^0_{276}$ *are fully transversal, hence have Hamming weight* 276.

Proof. All elements of $C_{277} \setminus C^0_{276}$ are mapped by ε onto $\mathbf{1}_\Omega$ of Hamming weight 552. (Of course, $C_{277} \setminus C^0_{276}$ is the full preimage of $\mathbf{1}_\Omega$.) The assertion follows from Lemma (3.4). □

(3.6) Lemma.
C_{23} *is the unique* FG*-submodule of* $F\Omega$ *of composition length* 2. *So* C_{529} *is the unique* FG*-submodule* Y *of* $F\Omega$ *such that* $F\Omega/Y$ *has composition length* 2.

Proof. Let X be an FG-submodule of composition length 2. If $X \leq C^0_{276}$ nothing has to be shown. Since by Corollary (3.2)(i) C_1 is the only minimal submodule of $F\Omega$ the composition factors of X must both be isomorphic to the trivial module C_1 if $X \not\leq C^0_{276}$, a contradiction against Corollary (3.2)(i), since G is nonabelian simple. □

(3.7) Lemma.
If X *is an* FG*-submodule of* $F\Omega$ *not contained in* C^0_{276} *then* $X \cap C^0_{276} \geq C_{23}$.

Proof. This follows from Corollary (3.2)(i) and Lemma (3.6). □

(3.8) Proposition.
$F\Omega$ *has exactly one* FG*-submodule* C_{24} *of dimension* 24. *We have* $C_{277} = C_{24} + C^0_{276}$ *and* $C_{24} \cap C^0_{276} = C_{23}$. *As an* FG*-module* C_{24} *is isomorphic to* $L = \Lambda/2\Lambda$ *where* Λ *denotes the Leech lattice whose group of automorphisms contains* G *as a subgroup fixing a given vector of Leech norm* 3. *Moreover, the weight distribution of* C_{24} *and the* G*-orbits on the set of elements of* C_{24} *are known. More explicitly, we have:*

(i) The weight enumerator C_{24} *is*

$$1(\xi^0\eta^{552} + \xi^{552}\eta^0) + 11,178(\xi^{200}\eta^{352} + \xi^{352}\eta^{200}) + 37,950(\xi^{224}\eta^{296} + \xi^{296}\eta^{224}) +$$

$$1,536,975(\xi^{256}\eta^{328} + \xi^{328}\eta^{256}) + 2,608,200(\xi^{264}\eta^{288} + \xi^{288}\eta^{264}) + 2^{23}\xi^{276}\eta^{276}.$$

(ii) All Hamming-weight classes contained in C_{23} *(of Hamming weight* $\neq 276$*) are* G*-orbits with point-stabilizers either* G *or maximal subgroups of* G *of ATLAS type* $\mathrm{HS}, \mathrm{U}_4(3) : (2^2)_{133}, 2^4 \cdot A_8, 2 \times \mathrm{M}_{12}$ *respectively.*

(iii) *In* $C_{24} \setminus C_{23} = W_{276}(C_{24})$ *there are exactly* 5 *G-orbits, exactly one with length* 552 *(point stabilizer* $\mathrm{M^cL}$*), the remaining two with length* $48,600$ *(point stabilizers* M_{23}*),* $934,656$ *(point stabilizer* $\mathrm{U}_3(5)$*) and* $4,098,600$ *(point stabilizer* $\mathrm{L}_3(4) : \mathrm{D}_6$ *).*

(iv) *We can choose the notation so that for* $T = \{x\} \cup \Delta$ *the indicator function* $\sum_{y \in T} y$ *belongs to the G-orbit of length* 552 *in (iii). Then the indicator function* $\sum_{y \in S} y$ *of* $S = \{x'\} \cup \Delta$ *is not contained in* C_{24}*. (Recall that the G-block containing x is by convention* $\{x, x'\}$*.) However, the indicator function of the transversal* $T' = \{x'\} \cup \Delta'$ *is contained in* C_{24} *and belongs to the mentioned G-orbit.*

Proof. The assertions follows from Theorems (1.3) and [9, (4.3)], see also Application [9, (4.8)]. Only (iv) needs an additional argument: If in addition $\sum_{y \in S} y$ of $S = \{x'\} \cup \Delta$ were contained in C_{24} we would have $x + x' \in C_{24}$, hence also $C^0_{276} \leq C_{24}$, clearly a contradiction. (Note that $2^{23} = 8,388,508$.) □

(3.9) Proposition.
Let $C^1_{276} := C_{275} + Fs$ *where for* $x \in T$ *and the* G_x*-orbit* Δ *and* $S = \{x'\} \cup \Delta$ *the transversal element* $s = \sum_{y \in S} y$ *is not contained in* C_{24} *(Recall that* $G_x \cong \mathrm{M^cL}$*). In addition, we define the FG-submodules (FG-invariant subcodes)* $C_{254} := C_{253} + C_{24}$*,* $C_{275} := C_{253} + C_{24}$ *and* $C^2_{276} := C_{275} + C_{24}$*, all contained in* C_{277}*. We immediately see that* $\dim C_i = i$ *and* $\dim C^k_{276} = 276$ *for* $k = 1, 2$*. Then the following hold:*

(i) *The unique composition series of* C_{277} *as an FG-module containing* C_{24} *is*

$$C_0 < C_1 < C_{23} < C_{24} < C_{254} < C^2_{276} < C_{277}.$$

(ii) *The unique composition series of* C_{277} *as an FG-module containing* C^1_{276} *is*

$$C_0 < C_1 < C_{23} < C_{253} < C_{275} < C^1_{276} < C_{277}.$$

(iii) *The unique composition series of* C_{277} *as an FG-module containing* C^0_{276} *is*

$$C_0 < C_1 < C_{23} < C_{253} < C_{275} < C^0_{276} < C_{277}.$$

(iv) *Every non-trivial FG-submodules of* $F\Omega$ *contained in* C_{277} *is one of the submodules defined above. All proper subcodes* C_i*,* $i < 277$*, are self-orthogonal and the* $C^k_{276}, k = 0, 1, 2$ *are self-dual codes. The FG-submodules* C^0_{276}*,* C^1_{276} *and* C^2_{276} *are the only maximal submodules of* C_{277} *; their pairwise intersection is* $C_{275} = {C_{277}}^{\perp}$*.*

(v) *The weight enumerators of all codes defined above are known. The codewords of minimum weight are for all these codes contained in* C^0_{276}*.*

(vi) C^0_{276} *has minimum weight* 2 *whereas* C^1_{276} *and* C^2_{276} *have minimum weight* 4*. The mimimum weight codewords form a G-orbit in all three cases.*

Proof. The argument in the proof of Proposition (3.8) shows that s is not contained in C^2_{276}. Therefore C^1_{276} is a well defined subspace of C_{277} of Dimension 276. Since C_{277}/C_{275} is a trivial FG-module it follows that C^1_{276} is an FG-submodule. Standard arguments for lattices of submodules now show that (i), (ii) and (iii) hold. (iv) can then be directly checked. (v) follows from Proposition (3.1) and Lemma (3.5). (vi) follows likewise. Note that the minimum weight codewords of C^1_{276} and of C^2_{276} are the same. □

Next we proceed by looking more closely at the somehow exceptional submodule C^1_{276} and at the orthogonal modules.

(3.10) Proposition.
For the FG-submodule C^1_{276} the following hold.

(i) C^1_{276} is uniserial and is generated by the G-orbit of the fully transversal codeword s with orbit length 552, where $s = \sum_{y\in S} y$ with $S = \{x'\} \cup \Delta$ as defined previously above.

(ii) There exists an FG-endomorphism η of $F\Omega$ with $\mathrm{Ker}(\eta) = \mathrm{Im}(\eta) = C^1_{276}$ and mapping x^g onto s^g for $g \in G$.

(iii) C^1_{276} is not isomorphic to C^0_{276} neither as an FG-module nor as code.

(iv) C^1_{276} is not isomorphic to C^2_{276} neither as an FG-module nor as code, but both codes have the same weight distribution.

Proof. (i) follows from Proposition (3.9) since C^1_{276} is uniserial. (ii) follows by the universal property of the permutation module from (i). Now observe that C^1_{276} is generated by a codeword in a G orbit of length 552 whereas C^0_{276} and C^2_{276} do not contain a codeword in a generating G-orbit of length 552. So we get (iii) and (iv), the latter also since all elements in $C_{277} \setminus C^0_{276}$ are fully transversal. □

(3.11) Proposition.
Let $C_{528} := C_{24}^{\perp}$ and $C_{298} := C_{254}^{\perp}$. Then

$$C_0 < C_1 < C_{23} < C_{24} < C_{254} < C_{275} < C^2_{276} < C_{298} < C_{528}$$

is the unique FG-module composition series of C_{528} containing C_{275}. The weight enumerators of all these codes are known; the minimum weight codewords of all these codes are contained in $C_{275} = C_{528} \cap C^0_{276}$.

Proof. The mapping $U \mapsto U^{\perp}$ is an involutory antiautomorphism of the lattice of FG-submodules of $F\Omega$. This observation gives the first part of the assertion. The rest follows using MacWilliams' identities, also in view of Lemma (3.4). □

Computation by MeatAxe shows that there are only 2 more FG-submodules, C^3_{276} and C^4_{276} situated between C_{254} and $C_{298} = {C_{254}}^{\perp}$, both self-dual of dimension 276, see Table I.

It seems to be difficult to give a reasonable description of these modules. Using the data produced by MeatAxe one can compute generator matrices mat_3 and mat_4 which differ only in the last 22 rows such that the sums of the last row vectors $mat_3[i] + mat_4[i]$ belong to the submodule C_{275} ($i = 255, \ldots, 276$). We could not determine the weight enumerator, but it is highly probable that both corresponding codes have the same weight distribution and probably are isomophic as FG-modules. Moreover, as a result of many computations it seems that both codes contain no codewords which are transversal but not fully transversal in the sense defined above. So all transversal codewords seem to be contained in C_{254}. Of course, both codes have minimum weight 12 by virtue of Lemma (3.4).

The proof of the Main Theorem is complete.

References

[1] P.J. Cameron : Suborbits in transitive permutation groups. In: Combinatorics, Proceedings of the NATO Advanced Study Institute 8-20 July 1974, D. Reidel Publishing Company Dordrecht-Holland/Boston-USA.

[2] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson : ATLAS of finite groups, Clarendon Press, Oxford 1985.

[3] J.H. Conway and N.J.A. Sloane : Sphere Packings, Lattices and Groups. Springer Verlag, New York 1988.

[4] GAP4 . The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.6.4*; 2013, (`http://www.gap-system.org`).

[5] W.A. Haemers, C. Parker, V. Pless and V.D. Tonchev: A Design and a Code invariant under the simple group Co_3. *J. Combin. Theory*, Series A 62, 225-233 (1993).

[6] W.A. Haemers, R. Peeters, J.M. van Rickevorsel : Binary codes of strongly regular graphs. *Designs Codes Cryptography* 17 (1999) 187-209.

[7] C. Jansen : The minimal degrees of faithful representations of the sporadic simple groups and their covering groups. *LMS J. Comp. Math.* 8 (2005) 122-144.

[8] W. Knapp : Remarks on a theorem of Wielandt. Archiv Math. 30 (1978) ,242 -246.

[9] W. Knapp and B.G. Rodrigues : A useful tool for constructing linear codes, *in preparation.*

[10] W. Knapp and P. Schmid : Codes with prescribed permutation group. *J. Algebra* 67, 415-435 (1980).

[11] W. Knapp and H.-J. Schaeffer: On the codes related to the Higman-Sims graph. *Electronic J. Combinatorics* Pl. 19 22(1) (2015).

[12] F.J. MacWilliams and N.J.A. Sloane : The theory of error correcting codes I, II. North Holland 1977.

[13] J. Moori and B.G. Rodrigues : Concatenated binary self-orthogonal codes related to the simple group Co_2. *In preparation.*

[14] I.A.I. Suleiman and R.A. Wilson : The 2-modular characters of Conway's third group Co_3. *J. Symbolic Comput.* 21 (1997), 493-506 .

[15] V.D. Tonchev: Combinatorial Configurations, Designs, Codes, Graphs.*Pitman monographs and Surveys in Pure and Appled Mathematics* vol. 40. Longman, New York 1988 (translated from the Bulgarian by R.A. Melter).

[16] R.A. Wilson : Vector Stabilizers and Subgroups of Leech Lattice Groups. *J. Algebra* 127 (1989) 387 - 408.