On some projective triply-even binary codes invariant under the Conway group Co_1

B. G. Rodrigues*
Department of Mathematics and Applied Mathematics
University of Pretoria
Hatfield 0028, South Africa

Abstract

A binary triply-even $[98280, 25, 47104]_2$ code invariant under the sporadic simple group Co_1 is constructed by adjoining the all-ones vector to the faithful and absolutely irreducible 24-dimensional code of length 98280. Using the action of Co_1 on the code we give a description of the nature of the codewords of any non-zero weight relating these to vectors of types 2, 3 and 4, respectively of the Leech lattice. We show that the stabilizer of any non-zero weight codeword in the code is a maximal subgroup of Co_1.
Key words and phrases: automorphism group, modular representation, Conway group.
AMS subject classifications: Primary 05B05, 20D08, 94B05.

1 Introduction

A triply-even binary code is a linear code in which the weight of every codeword is divisible by 8; such codes have previously been classified up to length 48 by Betsumiya and Munemasa [4]. Recent interest is growing in the study of Δ-divisible codes large length, of which triply-even codes are a special case. A linear code C over $\mathbb{F}_q$ is said to be Δ-divisible if the Hamming weight $\mathrm{w}(c)$ of every codeword $c \in C$ is divisible by $\Delta > 1$, and C is said to be a projective code if $d(C^{\perp}) \geq 3$. In particular, binary Δ-divisible codes have been studied in [9] and applications of these have been given. Particular relevance is placed on the fact that these codes are optimal with respect to some bound on linear codes.

In [11] we examined the properties of a projective two-weight code of dimension 24 invariant under the simple group Co_1 of Conway and explored its connection with the Leech lattice. In that paper we also described the properties of a new strongly regular graph with parameters $(16777216, 98280, 4600, 552)$ constructed using the non-zero codewords of the said 24-dimensional two-weight code, as well as the combinatorial properties of the self-dual, symmetric, flag-transitive, point- and block-primitive 1-$(98280, 47104, 47104)$ design invariant under Co_1. The present note is a sequel to [11] and in it we answer a question posed by Wolfgang Knapp on the combinatorial properties of a 25-dimensional submodule of the permutation module of dimension 98280 invariant under Co_1 which contains the above-mentioned 24-dimensional code as a subcode of codimension 1. In addition, we study these codes as examples of triply-even projective binary codes of large length admitting the simple group Co_1 of Conway as a permutation group of automorphisms. Further, we

*This work is based on the research supported by the National Research Foundation of South Africa (Grant Number 120846)

examine the properties of some point- and block-primitive 1-designs obtained as support 1-designs of the non-zero codewords of the two triply-even binary codes of length 98280 discussed in this paper. In the theorem given below, we summarize our results; the specific results relating to the codes are given as propositions in the following sections.

Theorem 1.1 *Let G be the simple Conway group* Co_1 *and* $\mathbb{F}_2\Omega$ *the permutation module of degree* 98280 *invariant under G. Then the following hold:*

(a) $\mathbb{F}_2\Omega$ *contains a unique submodule of dimension* 25*. Let* C_{25} *denote the unique submodule of dimension* 25*, then* $\mathrm{C}_{25} = \langle \mathrm{C}_{24}, \mathbf{1}\rangle$*, where* C_{24} *is the unique faithful and irreducible* Co_1*-invariant* $\mathbb{F}_2$*-module of dimension* 24*.*

(b) C_{25} *is a projective triply-even code.*

(c) C_{25} *is not spanned by its minimum-weight codewords.*

(d) $\mathrm{Aut}(\mathrm{C}_{25}) \cong \mathrm{Co}_1$.

(e) *the codewords of non-zero weight in* C_{25} *are stabilized by maximal subgroups of G.*

The paper is organized as follows: in Section 2 we outline our background and notation and in Section 3 we give a brief but complete overview on the Co_1 group. In Section 4 we describe the construction method used and give our results on the 25-dimensional binary code invariant under Co_1 in the ensuing sections.

2 Terminology

In this section, we state some useful facts in coding theory, design theory and finite group theory. Our notation for designs and groups will be standard, and it is as in [3] and 𝔸𝕋𝕃𝔸𝕊 [8].

Let $\mathbb{F}$ be a finite field of order $q = p^t$, where p is a prime and $t \in \mathbb{N}$; and G a finite group. Let Ω be a finite G-set, i.e. Ω is a finite set and there is a G-action on Ω, namely, a map $\cdot : G \times \Omega \longrightarrow \Omega$ given by $(g, \omega) \mapsto g \cdot \omega$, satisfying $(g \cdot h) \cdot \omega = g \cdot (h \cdot \omega)$ for all $g, h \in G$ and all $\omega \in \Omega$, and that $1 \cdot \omega = \omega$ for all $\omega \in \Omega$.

Then $\mathbb{F}\Omega = \{\sum_{\omega\in\Omega} g_\omega \omega \mid g_\omega \in \mathbb{F}\}$ is a vector space over $\mathbb{F}$ with basis Ω. Extending the G-action on Ω linearly, $\mathbb{F}\Omega$ becomes an $\mathbb{F}G$-module, called an $\mathbb{F}G$-permutation module with permutation basis Ω, (we remark that the permutation module $\mathbb{F}\Omega$ need not be semisimple in general). The $\mathbb{F}$-vector space $\mathbb{F}\Omega$ is equipped with a non-degenerate symmetric bilinear form

$$\langle \sum_{\omega\in\Omega} g_\omega \omega, \sum_{\omega\in\Omega} h_\omega \omega \rangle = \sum_{\omega\in\Omega} g_\omega h_\omega, \ \forall \mathbf{g} = \sum_{\omega\in\Omega} g_\omega \omega \text{ and } \mathbf{h} = \sum_{\omega\in\Omega} h_\omega \omega \in \mathbb{F}\Omega$$

called the standard inner product on $\mathbb{F}\Omega$. For any $a \in G$ and any $\mathbf{g} = \sum_{\omega\in\Omega} g_\omega \omega$ and $\mathbf{h} = \sum_{\omega\in\Omega} h_\omega \omega \in \mathbb{F}\Omega$, we have

$$\begin{aligned}
\langle a(\mathbf{g}), a(\mathbf{h})\rangle &= \langle a(\sum_{\omega\in\Omega} g_\omega \omega), a(\sum_{\omega\in\Omega} h_\omega \omega)\rangle \\
&= \langle \sum_{\omega\in\Omega} g_\omega a\omega, \sum_{\omega\in\Omega} h_\omega a\omega \rangle = \sum_{\omega\in\Omega} g_\omega h_\omega \\
&= \langle \mathbf{g}, \mathbf{h}\rangle.
\end{aligned}$$

So, the standard inner product on the vector space $\mathbb{F}\Omega$ is G-invariant in the following sense:

$$\langle a(\mathbf{g}), a(\mathbf{h})\rangle = \langle \mathbf{g}, \mathbf{h}\rangle, \ \forall a \in G, \forall \mathbf{g}, \mathbf{h} \in \mathbb{F}\Omega.$$

Moreover, for any $U \subseteq \mathbb{F}\Omega$ denote $U^{\perp} = \{\mathbf{v} \in \mathbb{F}\Omega \,|\, \langle \mathbf{u}, \mathbf{v}\rangle = 0, \forall \mathbf{u} \in U\}$. If C is an $\mathbb{F}G$-submodule of $\mathbb{F}\Omega$, then for any $a \in G$ and $\mathbf{c}' \in C^{\perp}$, and for any $\mathbf{c} \in C$, by the G-invariance of the inner-product we have that

$$\langle a\mathbf{c}', \mathbf{c}\rangle = \langle a\mathbf{c}', aa^{-1}\mathbf{c}\rangle = \langle \mathbf{c}', a^{-1}\mathbf{c}\rangle = 0,$$

so $a\mathbf{c}' \in C^{\perp}$, i.e., $C^{\perp}$ is G-invariant. Hence, $C^{\perp}$ is an $\mathbb{F}G$-submodule.

We say that C is an $\mathbb{F}G$-permutation code of $\mathbb{F}\Omega$, denoted by $C \subseteq \mathbb{F}\Omega$, if C is an $\mathbb{F}G$-submodule of the $\mathbb{F}G$-permutation module $\mathbb{F}\Omega$; and a permutation code C is said to be irreducible if C is an irreducible $\mathbb{F}G$-submodule of $\mathbb{F}\Omega$. Two linear codes are *isomorphic* if they can be obtained from one another by permuting the coordinate positions. For a linear code C of length n over $\mathbb{F}$, a permutation of the components of a codeword of length n is said to be a permutation automorphism of C if the permutation maps codewords to codewords. By $\mathrm{Aut}(C)$ we denote the automorphism group of C consisting of all the permutation automorphisms of C. With this we have that G acts on C and thus $G \leq \mathrm{Aut}(C)$ so that the code C becomes a $\mathbb{F}G$-submodule of the permutation module $\mathbb{F}\Omega$. In this note we consider only binary linear codes, so we restrict our attention to permutation automorphisms. It is easy to see that C is an $\mathbb{F}G$-permutation code of a G-permutation set Ω of cardinality n if and only if there is a group homomorphism of G to $\mathrm{Aut}(C)$.

A code C is *self-orthogonal* if $C \subseteq C^{\perp}$. The *hull* of C is $\mathrm{Hull}(C) = C \cap C^{\perp}$. The all-one vector will be denoted by $\mathbf{1}$, and is the constant vector of weight the length of the code, and whose coordinate entries consist entirely of 1's. A binary code C is *doubly-even* if all codewords of C have weight divisible by four. Let C be a code of length n. The weight distribution of a code C is the sequence $\{A_i | i = 0, 1, \ldots, n\}$, where A_i is the number of codewords of weight i. The polynomial $W_C(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$is called the weight enumerator of C. The weight enumerator of a code C and its dual $C^{\perp}$ are related via MacWilliams identity.

An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a *t-(v, k, λ) design*, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks. The *complement* of $\mathcal{D}$ is the structure $\tilde{\mathcal{D}} = (\mathcal{P}, \mathcal{B}, \tilde{\mathcal{I}})$, where $\tilde{\mathcal{I}} = \mathcal{P} \times \mathcal{B} - \mathcal{I}$. The *dual* structure of $\mathcal{D}$ is $\mathcal{D}^t = (\mathcal{B}, \mathcal{P}, \mathcal{I}^t)$, where $(B, p) \in \mathcal{I}^t$ if and only if $(P, B) \in \mathcal{I}$. Thus, the transpose of an incidence matrix for $\mathcal{D}$ is an incidence matrix for $\mathcal{D}^t$. We will say that the design is *symmetric* if it has the same number of points and blocks, and *self dual* if it is isomorphic to its dual.

The support of a nonzero vector $x := (x_1, \ldots, x_n), x_i \in \mathbb{F}_q$ is the set of indices of its nonzero coordinates: $\mathrm{supp}(x) = \{i | x_i \neq 0\}$. The *support design* of a code of length n for a given nonzero weight w is the design with n points of coordinate indices and blocks the supports of all codewords of weight w.

3 The Conway group Co_1

The *Leech lattice* is a certain 24-dimensional $\mathbb{Z}$-submodule of the 24-dimensional Euclidean space $\mathbb{R}^{24}$ discovered by John Leech. John Conway showed that the automorphism group of the Leech lattice is a quasisimple group. Its central factor group is the Conway group Co_1. The Conway groups Co_2 and Co_3 are stabilizers of sublattices of the Leech lattice. We give a brief description of the construction of these groups, omitting detail. The content of this section is mostly drawn from [2]. A more recent and comprehensive account is given in [14], see also [6, 12, 13].

Let $H = M_{24}$ and $(\Omega, \mathcal{C})$ be the Steiner system $S(24, 8, 5)$ for H. Let V be the permutation module over $\mathbb{F}_2$ of H with basis Ω and $V_{\mathcal{C}}$ the Golay code submodule. Let $\mathbb{R}^{24}$ be the permutation module over the reals for H with basis Ω and let $\langle\ ,\ \rangle$ be the symmetric bilinear form on $\mathbb{R}^{24}$ for which Ω is an orthogonal basis. Then $\mathbb{R}^{24}$ together with $\langle\ ,\ \rangle$ is simply the 24-dimensional Euclidean space admitting the action of H, and for $\sum_\omega \alpha_\omega \omega$ and $\sum_\omega \beta_\omega \omega$ in $\mathbb{R}^{24}$,

$$\left\langle \sum_\omega \alpha_\omega \omega, \sum_\omega \beta_\omega \omega \right\rangle = \sum_\omega \alpha_\omega \beta_\omega.$$

For $v \in \mathbb{R}^{24}$ define $q(v) = \langle v, v\rangle/16$. Thus q is a positive definite quadratic form on $\mathbb{R}^{24}$. Given $Y \subseteq \Omega$, define $e_Y = \sum_{y\in Y} y \in \mathbb{R}^{24}$. For $\omega \in \Omega$ let $\lambda_\omega = e_\Omega - 4\omega$.

The Leech lattice is the set Λ of vectors $v = \sum_\omega \alpha_\omega \omega \in \mathbb{R}^{24}$ such that:

(Λ1) $\alpha_\omega \in \mathbb{Z}$ for all $\omega \in \Omega$.

(Λ2) $m(v) = (\sum_\omega \alpha_\omega)/4 \in \mathbb{Z}$.

(Λ3) $\alpha_\omega \equiv m(v) \pmod 2$ for all $\omega \in \Omega$.

(Λ4) $\mathcal{C}(v) = \{\omega \in \Omega \mid \alpha_\omega \not\equiv m(v) \pmod 4\} \in V_{\mathcal{C}}$.

The Leech lattice Λ is a $\mathbb{Z}$-submodule of $\mathbb{R}^{24}$. Let Λ_0 denote the set of vectors $v \in \Lambda$ such that $m(v) \equiv 0 \pmod 4$. Then Λ_0 is a $\mathbb{Z}$-submodule spanned by the set $\{2e_B \mid B \subset \mathcal{C}\}$. Further, Λ as a $\mathbb{Z}$-submodule is generated by Λ_0 and λ_{ω_0}, for $\omega_0 \in \Omega$. Write $O(\mathbb{R}^{24})$ for the subgroup of $\mathrm{GL}(\mathbb{R}^{24})$ preserving the bilinear form $\langle\ ,\ \rangle$, or equivalently preserving the quadratic form q. Let G be the subgroup of $O(\mathbb{R}^{24})$ acting on Λ. The group G is the automorphism group of the Leech lattice. For $Y \subset \Omega$, write ϵ_Y for the element of $\mathrm{GL}(\mathbb{R}^{24})$ such that

$$\epsilon_Y(\omega) = \begin{cases} -\omega & ,\text{if} \quad \omega \in Y, \\ \omega & ,\text{if} \quad \omega \notin Y. \end{cases}$$

Let $Q = \{\epsilon_Y \mid Y \in V_{\mathcal{C}}\}$. Then $K = H{\cdot}Q \leq G$. Given any positive integer l, write Λ_l for the set of all vectors v in Λ with $q(v) = l$. Then $\Lambda = \cup_l \Lambda_l$. For $v = \sum_\omega \alpha_\omega \omega \in \Lambda$ and i a non-negative integer, let

$$S_i(v) = \{\omega \in \Omega : |\alpha_\omega| = i\}\ ,$$

and define the shape of v to be $(0^{l_0}, 1^{l_1}, \ldots)$, where $l_i = |S_i(v)|$. Let Λ_2^2 be the set of all vectors in Λ of shape $(2^8, 0^{16})$, Λ_2^3 the vectors in Λ of shape $(3, 1^{23})$, and Λ_2^4 the vectors in Λ of shape $(4^2, 0^{22})$. Then Λ_2^i, $2 \leq i \leq 4$, are the orbits of K on Λ_2, with $|\Lambda_2^2| = 2^7{\cdot}759$, $|\Lambda_2^3| = 2^{12}{\cdot}24$ and $|\Lambda_2^4| = 2^2{\cdot}\binom{24}{2}$. Moreover, $|\Lambda_2| = 2^4{\cdot}3^3{\cdot}5{\cdot}7{\cdot}13$ and $K = N_G(\Lambda_2^4)$. Using this information it can be shown that G acts transitively on Λ_2, Λ_3, and Λ_4. Also K is a maximal subgroup of G and $|G| = 2^{22}{\cdot}3^9{\cdot}5^4{\cdot}7^2{\cdot}11{\cdot}13{\cdot}23$. Notice that ϵ_Ω is the scalar map on $\mathbb{R}^{24}$ determined by -1, and hence is in the center of G. Denote by Co_1 the factor group $G/\langle\epsilon_\Omega\rangle$. Denote by Co_2 the stabilizer of a vector in Λ_2 and denote by Co_3 the stabilizer of a vector in Λ_3. The groups Co_1, Co_2 and Co_3 are the *Conway groups*, with $|\mathrm{Co}_1| = 2^{21}{\cdot}3^9{\cdot}5^4{\cdot}7^2{\cdot}11{\cdot}13{\cdot}23$, $|\mathrm{Co}_2| = 2^{18}{\cdot}3^6{\cdot}5^3{\cdot}7{\cdot}11{\cdot}23$ and $|\mathrm{Co}_3| = 2^{10}{\cdot}3^7{\cdot}5^3{\cdot}7{\cdot}11{\cdot}23$. Recall that Co_1, Co_2 and Co_3 are finite simple groups.

In Table 1 we give the primitive representations of Co_1 of degree ≤ 8386560. The first column gives the ordering of the primitive representations as given by the $\mathbb{ATLAS}$ [8] and as used in our computations; the second gives the degrees (the number of cosets of the point stabilizer), the third the number of orbits, and the remaining columns give the size of the non-trivial orbits of the respective point stabilizers.

No.	Max. sub.	Deg.	#	length					
1	Co_2	98280	4	4600	46575	47104			
2	$3^{\cdot}Suz{:}2$	1545600	5	5346	22880	405405	11119682		
3	$2^{11}{:}M_{24}$	8292375	6	3542	48576	1457280	2637824	4145152	
4	Co_3	8386560	7	11178	37950	257600	1536975	2608200	3934656

Table 1: Maximal subgroups of Co_1 of degree ≤ 8386560

4 The construction of codes

Our approach is representation theoretic and based on Theorem 4.1.

Theorem 4.1 *Let G be a finite group and let V be an $\mathbb{F}G$-module over a finite field $\mathbb{F}$ and let Ω be a G-invariant subset of V. Let $\mathbb{F}\Omega$ be the (formal) permutation module with basis $\overline{\Omega} = \{\overline{\alpha} \mid \alpha \in \Omega\}$ where $\overline{\alpha} = (\delta_{\beta\alpha})_{\beta\in\Omega}$ where $\delta_{\beta\alpha}$ denotes the Kronecker δ function.*
Then

$$\rho\colon \sum_{\alpha\in\Omega} r_\alpha\overline{\alpha} \mapsto \sum_{\alpha\in\Omega} r_\alpha\alpha$$

is an $\mathbb{F}G$-homomorphism of $\mathbb{F}\Omega$ into V with kernel of $\rho = M = \{\sum_{\alpha\in\Omega} r_\alpha\overline{\alpha} \mid \sum_{\alpha\in\Omega} r_\alpha\alpha = 0$ in $V\}$ and image U where U is the submodule of V generated by Ω. Hence, we have

$$\mathbb{F}\Omega/M \cong U \quad (\textit{by the homomorphism theorem}) \quad \textit{and}$$
$$M^\perp \cong U^* \quad (\textit{by orthogonality})$$

where $M^\perp$ denotes the submodule of $\mathbb{F}\Omega$ orthogonal to M with respect to the canonical bilinear form on $\mathbb{F}\Omega$ and $U^* = \mathrm{Hom}(U,\mathbb{F})$ denotes the $\mathbb{F}G$-module dual to U in the sense of representation theory.

Proof: The action of G on Ω is given by restricting the action of $G(\subseteq \mathbb{F}G)$ on V. So the theorem is basically just a restatement of the universal property of the permutation module as a free structure over Ω using in addition some elementary facts of representation theory and linear algebra. We leave to the reader to complete the details of the proof. ■

Remark 4.2 Usually α is identified with $\overline{\alpha}$ and Ω is identified with $\overline{\Omega}$, but for the purposes of Theorem 4.1 we keep them distinct.

Corollary 4.3 *With the same assumptions of Theorem 4.1 the following hold:*
(i) *Let V be irreducible. Then $\mathbb{F}\Omega$ has an irreducible submodule W isomorphic to V^*, if $\Omega \neq \varnothing$.*
(ii) *Let $V \cong V^*$ be irreducible and self-dual (in the sense of representation theory). Then $\mathbb{F}\Omega$ has an irreducible submodule W isomorphic to V.*

Remark 4.4 Theorem 4.1 is useful in other situations, for instance if V has a unique maximal submodule V_0 and $\varnothing \neq \Omega \subseteq V \setminus V_0$. Then necessarily $U = V$.

Theorem 4.1, Corollary 4.3 and Remark 4.4 above have been suggested [10] as means of construction of codes.

5 Binary codes of small dimension invariant under Co_1 of degree 98280

With the notation established in Section 3, for $v \in \Lambda$ let $\Lambda_l(v, i)$ denote the set of $u \in \Lambda_l$ for which $\langle v, u\rangle = 8i$. Let $2\Lambda = \{2v : v \in \Lambda\}$. Then 2Λ is a $2^{\cdot}\mathrm{Co}_1$-invariant $\mathbb{Z}$-module, and $2^{\cdot}\mathrm{Co}_1$ acts on the quotient module $\tilde{\Lambda} = \Lambda/2\Lambda$. The module $\tilde{\Lambda}$ is the reduction modulo 2 of the Leech lattice. For $v \in \Lambda$, let $\tilde{v} = v + 2\Lambda$ and for $S \subseteq \Lambda$ let $\tilde{S} = \{\tilde{s} : s \in S\}$. Then $2\tilde{v} = 0$ for all $v \in \Lambda$, and $\tilde{\Lambda}$ is an elementary abelian 2-group which may be viewed as a $\mathbb{F}_2 2^{\cdot}\mathrm{Co}_1$-module. Recall from Section 3 that $\mathrm{Co}_1 \cong 2^{\cdot}\mathrm{Co}_1/\langle \epsilon_\Omega\rangle$. Since $\langle \epsilon_\Omega\rangle$ acts trivially on $\tilde{\Lambda}$ it follows that $\tilde{\Lambda}$ is a $\mathbb{F}_2\mathrm{Co}_1$-module. In [2, Lemma 23.2 (4), Lemma 23.3] Aschbacher showed that $\tilde{\Lambda}$ is a 24-dimensional, faithful and irreducible $\mathbb{F}_2\mathrm{Co}_1$-submodule, see [1] for relevant information on this submodule. Using these and other properties of $\tilde{\Lambda} \cong \mathbb{F}_2^{24}$ in [11] we denoted this module C_{24} and examined its combinatorial properties. We state the pertinent result below

Result 5.1 *Let G be the simple Conway group Co_1 in its rank 5 primitive permutation action of degree 98280 and let C_{24} denote a submodule of dimension 24 of the permutation module of degree 98280 over $\mathbb{F}_2$. Then*
(i) C_{24} *is a self-orthogonal doubly-even projective two-weight* $[98280, 24, 47104]_2$ *code with* 98280 *words of weight* 47104.
(ii) *The dual code* ${\mathrm{C}_{24}}^{\perp}$ *of* C_{24} *is a* $[98280, 98256, 3]_2$ *uniformly packed code with* 75348000 *codewords of weight* 3.
(iii) $\mathbf{1} \in {\mathrm{C}_{24}}^{\perp}$ *and* C_{24} *is the unique submodule of its dimension on which* Co_1 *acts absolutely irreducibly.*
(iv) $\mathrm{Aut}(\mathrm{C}_{24}) \cong \mathrm{Co}_1$.

Remark 5.2 (i) The weight distribution of C_{24} is given by

$$A_0 = 1,\ A_{47104} = 98280,\ A_{49152} = 16678935. \tag{1}$$

(ii) The code C_{24} can be constructed as an application of Theorem 4.1.
(iii) Observe that C_{24} is a triply-even code, since $\mathrm{wt}(c) \mid 8$ for every $c \neq \mathbf{0}$ in C_{24}, where $\mathbf{0}$ represents the zero vector in C_{24}.

As stated in Remark 5.2 (ii) one can apply Theorem 4.1 to the situation given in Result 5.1 by identifying $V = \tilde{\Lambda}$ and $\Omega = \overline{\Lambda}_2 = \Lambda_2 + \Lambda/2\Lambda$ with $\mathbb{F} = \mathbb{F}_2$, i.e., the reduction image of Λ_2 modulo 2Λ, and $G = \mathrm{Co}_1$. Notice that $V \cong V^*$ follows since G acts as an orthogonal group on V and C_{24} can be identified with the submodule U of $\mathbb{F}_2\Omega$ given by Theorem 4.1. Notice also that ${\mathrm{C}_{24}}^{\perp}$ is the module denoted M in Theorem 4.1.

The following results concerning with C_{24} appeared as a proposition and a lemma in [11].

Result 5.3 *The generating words of* C_{24} *form the blocks of the unique, self-dual, symmetric, flag transitive and point primitive* 1-$(98280, 47104, 47104)$ *design* $\mathcal{D}_{24}$ *invariant under* Co_1. *Moreover,* $\mathrm{Aut}(\mathcal{D}_{24}) \cong \mathrm{Co}_1$.

Since C_{24} is a two-weight code, it follows by a well-known construction that if we let w_1 and w_2 (where $w_1 < w_2$) be the non-zero weights of C_{24} one can associate a graph on the $2^{24} = 16777216$ vertices. The vertices of the graph are identified with the non-zero weight codewords and two vertices corresponding to the codewords x and y are adjacent if and only if $d(x, y) = w_1$. Using the above, a strongly regular graph with new parameters denoted $\Gamma(\mathrm{C}_{24})$ associated to C_{24} was constructed. We record the properties of the graph in

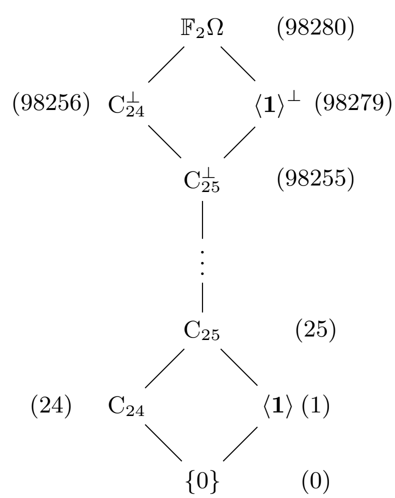
Result 5.4 $\Gamma(\mathrm{C}_{24})$ *is a strongly regular* $(16777216, 98280, 4600, 552)$ *graph with spectrum* $[98280]^1, [4072]^{98280}, [-24]^{16678935}$. *The complementary graph* $\overline{\Gamma(\mathrm{C}_{24})}$ *of* $\Gamma(\mathrm{C}_{24})$ *is a strongly regular* $(16777216, 16678935, 16581206, 16585256)$ *graph. This graph has spectrum* $[16678935]^1, [23]^{16678935}$, $[-4073]^{98280}$.

5.1 The $[98280, 25, 47104]_2$ code

Observe that C_{24} does not contain the all-ones vector $\mathbf{1}$. Below, we construct a binary linear code of dimension 25, denoted C_{25} which results by adjoining the all ones vector to C_{24}. In fact, $\mathrm{C}_{25} \setminus \mathrm{C}_{24}$ consists of the codewords complementary with those of C_{24}.

In Figure 1 below we give a partial description of the submodule structure (the composition factors can be derived from this) of the permutation module $\mathbb{F}_2\Omega$ of degree 98280. The vector space dimension is given in parentheses.

Figure 1: Partial submodule lattice for $\mathbb{F}_2\Omega$



Naturally, one can ask what are the combinatorial properties of the code C_{25}?

In Proposition 5.5 we examine the combinatorial properties of C_{25} and give its main parameters. In addition, in Proposition 6.1 we determine the orbits of the action of Co_1 on C_{25} and describe the corresponding geometric subgroups, i.e., stabilizers of points or blocks, and finally in Remark 6.3 we give a geometric significance of the nature of the complementary pairs of non-zero codewords, in particular those of minimum weight. Notice that the notation $\langle\, , \rangle$ used in Proposition 5.5 parts (i) and (v) and their proofs differs from that used for the bilinear form. Here we mean subspace generation.

Proposition 5.5 *Let G be the simple Conway group* Co_1 *and* $\mathbb{F}_2\Omega$ *denote the permutation module of degree* 98280 *over* $\mathbb{F}_2$. *Then*
(i) *There exists a unique submodule of* $\mathbb{F}_2\Omega$ *of dimension* 25 *invariant under* Co_1. *Let* C_{25} *be this submodule. Then* $\mathrm{C}_{25} = \langle \mathrm{C}_{24}, \mathbf{1} \rangle$, *where* C_{24} *is the smallest non-trivial faithful* Co_1*-invariant irreducible* $\mathbb{F}_2$*-module of dimension* 24 *of Result* 5.1*;*
(ii) C_{25} *is a triply-even projective* $[98280, 25, 47104]_2$ *code with* 98280 *codewords of weight* 47104, $\mathbf{1} \in {\mathrm{C}_{25}}^{\perp}$ *and in* C_{25}.

(iii) C_{25} *is not spanned by its minimum-weight codewords.*
(iv) *The dual code* ${\mathrm{C}_{25}}^{\perp}$ *of* C_{25} *is a* $[98280, 98255, 4]_2$ *code with* 297601053750 *codewords of weight* 4.
(v) $\mathrm{Aut}(\mathrm{C}_{25}) \cong \mathrm{Co}_1$.

Proof: (i) By construction $\mathrm{C}_{25} = \langle \mathrm{C}_{24}, \mathbf{1}\rangle$. Since C_{24} and $\langle \mathbf{1}\rangle$ are Co_1-invariant subspaces, we deduce that C_{25} is a decomposable 25-dimensional $\mathbb{F}_2$-module of Co_1 containing the 24-dimensional $\mathbb{F}_2$-module C_{24}. Thus $\mathrm{C}_{25} = \mathrm{C}_{24} + \langle \mathbf{1}\rangle$. The uniqueness of C_{25} follows from Result 5.1(iii). See also, [2, Lemma 23.2 (4), Lemma 23.3].
(ii) Since $\mathrm{C}_{25} \subseteq {\mathrm{C}_{25}}^{\perp}$, if $w \in \mathrm{C}_{25}$ it follows that $w \in {\mathrm{C}_{25}}^{\perp}$ and so $(w, w) = 0$. Write $w = w_1 w_2 \ldots w_{98280}$. Then $\sum_{i=1}^{98280} w_i^2 = 0$. Furthermore, since $w_i^2 = w_i$ for all $w_i \in \mathbb{F}_2$ then $\sum_{i=1}^{98280} w_i = w_i\mathbf{1}$. Hence $\mathbf{1} \in {\mathrm{C}_{25}}^{\perp}$. That $\mathbf{1} \in \mathrm{C}_{25}$ follows by construction. Now, we have $A_{98280-i} = |\{w_i + \mathbf{1} : w_i \in \mathrm{C}_{25}\}| = |\{w_i : w_i \in \mathrm{C}_{25}\}| = A_i$. Form the latter and expression (1) we deduce

$$A_0 = A_{98280} = 1,\ A_{47104} = A_{51176} = 98280,\ A_{49128} = A_{49152} = 16678935. \tag{2}$$

Observe from (2) that all codewords of C_{25} have weight divisible by four. This shows that C_{25} is doubly-even and hence self-orthogonal. Moreover, C_{25} is triply-even as the weights of all its codewords are divisible by eight.
(iii) By Result 5.1(i) we deduce that the codewords of weight 47104 generate the code C_{24}. We verified through computations with Magma that the codewords of weight 49128 span C_{25}. Hence the result.
(iv) Using MacWilliams identities and Pless' power moment identities the weight distribution of the dual can be obtained. In fact, we used computations with Magma [5] to confirm the full weight distribution. From this we deduce that C_{25}, since $d({\mathrm{C}_{25}}^{\perp}) \geq 4$. [1]
(v) We show here that $\mathrm{Aut}(\mathrm{C}_{25}) \cong \mathrm{Co}_1$. Obviously, $\mathrm{Co}_1 \subseteq \mathrm{Aut}(\mathrm{C}_{24})$. Now, suppose that $\alpha \in \mathrm{Aut}(\mathrm{C}_{24})$. Since $\alpha(\mathbf{1}) = \mathbf{1}$ and $\mathrm{C}_{25} = \langle \mathrm{C}_{24}, \mathbf{1}\rangle$, we have $\alpha \in \mathrm{Aut}(\mathrm{C}_{25})$. So that $\mathrm{Aut}(\mathrm{C}_{24}) \subseteq \mathrm{Aut}(\mathrm{C}_{25})$. Since by Result 5.1(iv) we have $\mathrm{Aut}(\mathrm{C}_{24}) \cong \mathrm{Co}_1$, order considerations show $\mathrm{Aut}(\mathrm{C}_{25}) \cong \mathrm{Co}_1$. ■

6 Geometric subgroups of Co_1 as stabilizers of vectors of the codes

By [13, Theorem A1], we know that there are just three orbits of Co_1 on 1-dimensional spaces in $\Lambda/2\Lambda$ and these orbits have lengths 98280, 8292375 and 8386560, respectively. In Proposition 6.1, we use these facts and the fact that $\mathbf{1} \in \mathrm{C}_{25}$ by part (iv) of Proposition 5.5 to show how the orbits split under the action of Co_1 on the non-zero codewords of C_{25} (see Expression (2)). The reader will notice that since $\mathbf{1} \in \mathrm{C}_{25}$ the weight distribution of C_{25} is symmetric and the codewords of C_{25} occur in complementary pairs. Thus we determine the structure of $(\mathrm{Co}_1)_{w_i}$ where i is in W with $W = \{47104, 49152\}$ and the structure of $(\mathrm{Co}_1)_{\overline{w}_i}$ where i is in $\overline{W}$, the complement of $\overline{W}$ and $\overline{W} = \{51176, 49128\}$. For $i \in W$ (respectively for $i \in \overline{W}$) we define W_i (respectively $\overline{W}_i$) to be $W_i = \{w_i \in \mathrm{C}_{25} \mid \mathrm{wt}(w_i) = i\}$ (respectively $\overline{W}_i = \{\overline{w}_i \in \mathrm{C}_{25} \mid \mathrm{wt}(\overline{w}_i) = i\}$). We show in Proposition 6.1 that $(\mathrm{Co}_1)_{w_i}$ (respectively $(\mathrm{Co}_1)_{\overline{w}_i}$) is a maximal subgroup of Co_1, for all i. Taking the support of w_i (respectively $\overline{w}_i$) and orbiting that under Co_1 we form the blocks of the 1-$(98280, i, k_i)$ support designs $\mathcal{D} = \mathcal{D}_{w_i}$ (respectively $\mathcal{D} = \mathcal{D}_{\overline{w}_i}$) where $k_i = |(w_i)^{\mathrm{Co}_1}| \times \frac{i}{98280}$ (respectively $k_i = |(\overline{w}_i)^{\mathrm{Co}_1}| \times \frac{i}{98280}$). We show that Co_1 acts point primitively on $\mathcal{D}$. For economy we prove the result for the codewords in W. The proof for the codewords in $\overline{W}$ follows by replacing the relevant complementary pairs.

[1] The entire weight distribution can be obtained from the author.

Proposition 6.1 *Let $i \in W$ and $w_i \in W_i$. Then $(\mathrm{Co}_1)_{w_i}$ is a maximal subgroup of Co_1. Furthermore Co_1 is primitive on $\mathcal{D}_{w_i}$.*

Proof: The proof follows from the two cases discussed below.
Case 1. Consider $W_{47104} = \{w_i \in W \mid \mathrm{wt}(w_i) = 47104\}$. Since W_{47104} is invariant under the action of $\mathrm{Aut}(\mathrm{C}_{25})$ for all $w_i \in W_{47104}$, it follows from Expression (2) that ${w_i}^{\mathrm{Co}_1} = W_{47104}$. Therefore W_{47104} forms an orbit under the action of Co_1 and thus Co_1 is transitive on W_{47104}. Now let $x = w_{(47104)}$. Then $(\mathrm{Co}_1)_x$ is a subgroup of order $2^{18}{\cdot}3^6{\cdot}5^3{\cdot}7{\cdot}11{\cdot}23$ we deduce that thus maximal in Co_1. Using Expression (2) once again and the orbit stabilizer theorem we deduce that $[\mathrm{Co}_1{:}(\mathrm{Co}_1)_x] = 98280$ and by order considerations and Table 1 we have $(\mathrm{Co}_1)_x \cong \mathrm{Co}_2$.
Case 2. Let $W_{49152} = \{w_i \in W \mid \mathrm{wt}(w_i) = 49152\}$. It can be deduced from [13, Theorem A1] that under the action of Co_1 the set W_{49152} splits into two orbits of lengths 8292375 and 8386560, say $W_{(49152)_1}$ and $W_{(49152)_2}$. Let $y = w_{(49152)_1} \in W_{(49152)_1}$ and $z = w_{(49152)_2} \in W_{(49152)_2}$. Then $(\mathrm{Co}_1)_y$ is a subgroup of order 501397585920 and thus maximal in Co_1. Moreover, $(\mathrm{Co}_1)_y \cong 2^{11}{:}\mathrm{M}_{24}$. (Note that there is a misprint in [8, p. 183] for the index $[\mathrm{Co}_1{:}(2^{11}{:}\mathrm{M}_{24})]$.) Similarly, $|(\mathrm{Co}_1)_z| = 2^{10}{\cdot}3^7{\cdot}5^3{\cdot}7{\cdot}11{\cdot}23$, so that $(\mathrm{Co}_1)_z \cong \mathrm{Co}_3$.
By the transitivity of Co_1 on the code coordinate positions, the codewords of W_i form a 1-design $\mathcal{D}_{w_i}$ with A_i blocks. This implies that Co_1 is transitive on the blocks of D_{w_i} for each w_i and since $(\mathrm{Co}_1)_{w_i}$ is a maximal subgroup of Co_1, we deduce that Co_1 acts primitively on $\mathcal{D}_{w_i}$ for each i. This still holds if we replace w_i with $\overline{w}_i$ in each case discussed.

In Table 2 we depict the structure of the vector stabilizer for all the codewords of C_{25}.

i	$(\mathrm{Co}_1)_w$	Maximality	i	$(\mathrm{Co}_1)_w$	Maximality
0	Co_1	No	98280	Co_1	No
47104	Co_2	Yes	51176	Co_2	Yes
$(49152)_1$	Co_3	Yes	$(49128)_1$	Co_3	Yes
$(49152)_2$	$2^{11}{:}\mathrm{M}_{24}$	Yes	$(49128)_2$	$2^{11}{:}\mathrm{M}_{24}$	Yes

Table 2: Stabilizer in Co_1 of a codeword w ($=w_i$ or $\overline{w}_i$)

In Table 3 the first column represents the codewords of weight i and the second column gives the parameters of the designs $\mathcal{D}_w$, where $w = w_i($ or $\overline{w}_i)$ accordingly. In the third column we list the number of blocks of $\mathcal{D}_w$. We test the primitivity for the action of Co_1 on $\mathcal{D}_w$ in the final column.
■

In what follows our main interest is in determining the orbits of Co_1 on the set of codewords of minimum weight in the dual code ${\mathrm{C}_{25}}^{\perp}$. While this is of independent interest our investigation was motivated by a question of Wolfgang Knapp [10] for it would be of help in the classification of these types of codewords. We aim to trace these to vectors of the Leech lattice, thereby providing a geometric description and the nature of this class of codewords.

Proposition 6.2 Co_1 *has* 3 *orbits on the set of minimum weight codewords of* ${\mathrm{C}_{25}}^{\perp}$, *the orbit lengths being* $88114776750, 159134976000$ *and* 50351301000, *respectively.*

Proof: Let $W_4({\mathrm{C}_{25}}^{\perp}) = \{w \in {\mathrm{C}_{25}}^{\perp} \mid \mathrm{wt}(w) = 4\}$ denote the set of weight 4 vectors in ${\mathrm{C}_{25}}^{\perp}$. Then by Proposition 5.5 (iv), we have $|W_4({\mathrm{C}_{25}}^{\perp})| = 297601053750$ and thus Co_1 acts intransitively on $W_4({\mathrm{C}_{25}}^{\perp})$. Under the action of Co_1 we have that $W_4({\mathrm{C}_{25}}^{\perp})$ splits into the orbits $W_4({\mathrm{C}_{25}}^{\perp})_i$

i	$\mathcal{D}_w$	No. of blocks	Primitivity
47104	1-(98280, 47104, 47104)	98280	Yes
51176	1-(98280, 51176, 51176)	98280	Yes
$(49152)_1$	1-(98280, 49152, 4194304)	8386560	Yes
$(49152)_2$	1-(98280, 49152, 4147200)	8292375	Yes
$(49128)_1$	1-(98280, 49128, 4192256)	8386560	Yes
$(49128)_2$	1-(98280, 49128, 4145175)	8292375	Yes

Table 3: Non-trivial point- and block-primitive 1-designs $\mathcal{D}_w$ on 98280 points invariant under Co_1

with $1 \leq i \leq 3$. In particular, $|W_4({\mathrm{C}_{25}}^{\perp})_1| = 88114776750$, $|W_4({\mathrm{C}_{25}}^{\perp})_2| = 159134976000$ and $|W_4({\mathrm{C}_{25}}^{\perp})_3| = 50351301000$, respectively. Let $a \in W_4({\mathrm{C}_{25}}^{\perp})_1, b \in W_4({\mathrm{C}_{25}}^{\perp})_2$ and $c \in W_4({\mathrm{C}_{25}}^{\perp})_3$. Then $(\mathrm{Co}_1)_a$ is a subgroup of order 47185920 and follows from the list of maximal subgroups of Co_1, see $\mathbb{ATLAS}$ [8, p. 183], that $(\mathrm{Co}_1)_a$ is not maximal in Co_1. Notice that $|(\mathrm{Co}_1)_b| = 26127360$ and $|(\mathrm{Co}_1)_c| = 82575360$, and as in the preceding case, these groups are not maximal in Co_1.

By order considerations we deduce that $(\mathrm{Co}_1)_a$ is possibly a maximal subgroup of $2^{1+12}{:}(\mathrm{A}_8 \times \mathrm{S}_3)$ or $2^{4+12}{:}(\mathrm{S}_3 \times 3\mathrm{S}_6)$ with index 42 and 18, respectively. By computations with Magma [5] we obtained the maximal subgroups of $2^{1+12}{:}(\mathrm{A}_8 \times \mathrm{S}_3)$ and $2^{4+12}{:}(\mathrm{S}_3 \times 3\mathrm{S}_6)$, and since neither of these subgroups possesses a maximal subgroup of the given index we conclude that $(\mathrm{Co}_1)_a$ is not a second maximal subgroup. Furthermore, using the structure of the composition factors we deduce that $(\mathrm{Co}_1)_a \cong (3 \times 2^{17}){:}S_5$.

Next we consider the group $(\mathrm{Co}_1)_b$. Inspecting the list of maximal subgroups of Co_2 we deduce that $(\mathrm{Co}_1)_b$ is a maximal subgroup of Co_2 isomorphic to $U_4(3) \cdot \mathrm{D}_8$. Furthermore, $(\mathrm{Co}_1)_b$ is the setwise stabilizer in Λ of an S-lattice of type $2^{1+4}{:}3^2$, and point stabilizer isomorphic to $\mathrm{U}_4(3)$, see $\mathbb{ATLAS}$ [8, pp. 52].

Arguing as above we note that $(\mathrm{Co}_1)_c$ is possibly a maximal subgroup of $2^{1+12}{:}(\mathrm{A}_8 \times \mathrm{S}_3)$ of index 24. However, it can be proven by inspecting the list of maximal subgroups of this group computed using Magma that this possibility does not occur. Now, direct calculating using composition factors shows that $(\mathrm{Co}_1)_c \cong 2^{11}{:}L_3(4) \cdot 2$. ■

Remark 6.3 The geometric significance and the nature of the codewords of C_{25} can be described using the Leech lattice as it was the case for the codewords of C_{24}, see [11]. The description that is presented below follows directly by using [13, Theorem A1] and [13, Theorem A2].
(1). The minimum words of C_{25} are the 98280 pairs consisting of a type 2 vector and its negative in the Leech lattice [12, p. 156]. The stabilizer of such a pair has just three non-trivial orbits on the other pairs, where the orbit in which a particular vector lies depends only on the angles its vectors from with the fixed vector. The permutation character of this action is $\chi_1 + \chi_3 + \chi_6 + \chi_{10}$, of degrees 1, 299, 17250, 80730 respectively, see [8, p. 183].
(2). Observe (from Table 2) that the codewords of weight 49152 in C_{25} split into two classes, namely a class of codewords whose stabilizer is isomorphic to $2^{11}{:}\mathrm{M}_{24}$, and another with stabilizer of a codeword isomorphic to Co_3. The class of codewords with stabilizer isomorphic to $2^{11}{:}\mathrm{M}_{24}$ consists of the type 4 base (or A_1^{24}-hole) vectors, while those vectors with stabilizer Co_3 are known to be type 3 vectors in the Leech lattice, see [8, p. 183] or [12, p. 156].
(3). A result along the lines of Result 5.3 can be obtained for the 1-(98280, 51176, 51176) design $\mathcal{D}$

invariant under Co_1.

(4). Observe that in Proposition 6.2 we show that the set $W_4(\mathrm{C}_{25}{}^{\perp})$ of minimum weight codewords of $\mathrm{C}_{25}{}^{\perp}$ is not an orbit of Co_1. In particular, we give a geometric description of the nature of $W_4(\mathrm{C}_{25}{}^{\perp})_2$, tracing it to the Leech lattice, and also showed that the stabilizer of those codewords is a second maximal subgroup of Co_1. It would be of interest to give a geometric description of the nature of the codewords of $W_4(\mathrm{C}_{25}{}^{\perp})_1$ and $W_4(\mathrm{C}_{25}{}^{\perp})_3$, respectively.

Acknowledgements

The author wishes to thank Wolfgang Knapp, for he suggested to examine the Leech lattice modulo 2 applying the general setting provided by Theorem 4.1 thus giving rise to the question on the combinatorial properties of the 25-dimensional code dealt with in the paper.
The author would like to thank the Isaac Newton Institute for Mathematical Sciences, Cambridge, for support and hospitality during the programme *Groups, representations and applications: new perspectives*, where part of the research for this paper was done. This work was supported by EPSRC grant no EP/R014604/1.

References

[1] R. Abbott, J. Bray, S. Linton, S. Nickerson, S. Norton, R. Parker, I. Suleiman, J. Tripp, P. Walsh and R. Wilson. Atlas of finite group representations. `http://brauer.maths.qmul.ac.uk/Atlas/v3/spor/Co1/`. Accessed March 2020.

[2] M. Aschbacher. *Sporadic Groups.* Cambridge University Press, 1994. Cambridge Tracts in Mathematics, Vol. 104.

[3] E. F. Assmus, Jr and J. D. Key. *Designs and their Codes.* Cambridge: Cambridge University Press, 1992. Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[4] K. Betsumiya and A. Munemasa. On triply even binary codes. *J. Lond. Math. Soc.* **86** (1) (2012), 1-16.

[5] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symbolic Comput.*, **24** (1997), 235–265.

[6] J. H. Conway. A group of order 8,315,553,613,086,720,000. *Bull. London Math. Soc.*, **1** (1969), 79–88.

[7] J. H. Conway. A Characterisation of Leech's Lattice. *Invent. Math.*, **7** (1969), 137–142.

[8] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *An Atlas of Finite Groups.* Oxford: Oxford University Press, 1985.

[9] D. Heinlein, T. Honold, M. Kermaier, S. Kurz and A. Wassermann. *Projective divisible binary codes.* In: The Tenth International Workshop on Coding and Cryptography 2017 : WCC Proceedings. Saint-Petersburg, September 2017.

[10] W. Knapp. Private communication.

[11] B. G. Rodrigues. A projective two-weight code related to the simple group Co_1 of Conway. *Graphs and Combin.* **34** (2018) (3), 509—521.

[12] R. A. Wilson. The maximal subgroups of Conway's group Co_1. *J. Algebra*, **85** (1983), 144–165.

[13] R. A. Wilson. Vector Stabilizers and Subgroups of Leech Lattice Groups. *J. Algebra*, **127** (1989), 387–408.

[14] R. A. Wilson. *The finite simple groups*. London: Springer-Verlag London Ltd., 2009. Graduate Texts in Mathematics, Vol. 251.