Permutation Groups and Binary Self-Orthogonal Codes

Permutation Groups and Binary Self-Orthogonal Codes

Naoki Chigira
Department of Mathematical Sciences
Muroran Institute of Technology
Muroran, Hokkaido 050–8585, Japan
chigira@mmm.muroran-it.ac.jp

Masaaki Harada*
Department of Mathematical Sciences
Yamagata University
Yamagata 990–8560, Japan
harada@kdw.kj.yamagata-u.ac.jp
and
Masaaki Kitazume
Department of Mathematics and Informatics
Chiba University
Chiba 263–8522, Japan
kitazume@math.s.chiba-u.ac.jp

June 1, 2006

Abstract

Let G be a permutation group on an n-element set Ω. We study the binary code $C(G, \Omega)$ defined as the dual code of the code spanned by the sets of fixed points of involutions of G. We show that any G-invariant self-orthogonal code of length n is contained in $C(G, \Omega)$. Many self-orthogonal codes related to sporadic simple groups, including the extended Golay code, are obtained as $C(G, \Omega)$. Some new

*corresponding author

self-dual codes invariant under sporadic almost simple groups are constructed.

Keywords: permutation group, sporadic simple group, self-orthogonal code and self-dual code

1 Introduction

In [3], we constructed a binary self-dual $[100, 50, 10]$ code C_{10} whose automorphism group is isomorphic to $J_2{:}2$, which is the extension of the Hall–Janko group J_2 by its outer automorphism. It was also proved that the code C_{10} is spanned by the codewords of weight 14, which are the sets of fixed points of the outer involutions. On the other hand, the extended Golay code G_{24} is spanned by the codewords of weight 8, called the octads, which are the sets of fixed points of $2A$-involutions of its automorphism group, which is isomorphic to the Mathieu group M_{24}; recall that this group has precisely two classes of involutions labelled $2A$ and $2B$ (see [4]).

Motivated by such observations, in this paper, we consider the sets of fixed points of involutions of a permutation group. Let G be a permutation group on an n-element set Ω. We define the binary code $C(G, \Omega)$ (or simply $C(G, n)$) as the dual code of the code spanned by the sets of fixed points of involutions of G. Here $C(G, \Omega)$ is contained in the power set $\mathcal{P}(\Omega)$ of Ω, which is regarded as an n-dimensional vector space over a field of two elements by defining the sum as the symmetric difference. We consider a subspace (i.e. a code of length n) C of $\mathcal{P}(\Omega)$. Our main theorem (given in Section 2) is as follows:

Theorem A. *Let C be a G-invariant binary self-orthogonal code of length n. Then $C \subset C(G, \Omega)$.*

Our idea is simple and the main theorem can be easily proved, yet many known self-orthogonal codes related to sporadic simple groups are obtained as $C(G, \Omega)$. For example, the above codes C_{10} and G_{24} are obtained as $C(J_2{:}2, 100)$ and $C(M_{24}, 24)$, respectively. More known examples are listed in Section 2. Moreover, the equality $C_{10} = C(J_2 : 2, 100)$ (resp. $G_{24} = C(M_{24}, 24)$) means that this code is the unique $J_2{:}2$- (resp. M_{24}-) invariant self-dual code of length 100 (resp. 24). In this way, Theorem A is used to characterize or classify some self-orthogonal (or self-dual) codes with a fixed automorphism group. In Section 3, we give a list of the codes $C(G, \Omega)$ for sporadic almost simple groups G of degree ≤ 1000 satisfying the condition $N_G(I(H)) = H$ for the stabilizer H of a point, where $I(H)$ denotes the set of

involutions of H. A group G is said to be almost simple if $G_0 \triangleleft G \subseteq \mathrm{Aut}(G_0)$ for some non-abelian simple group G_0. Consequently, we find all self-dual codes of lengths ≤ 1000 invariant under such sporadic almost simple groups satisfying the above condition, including some new self-dual codes. We note that this condition is equivalent to the condition that the minimum weight of $C(G, \Omega)$ is greater than 2 (Lemma 2.15). Many known codes are related to some graphs or designs. Typical examples are C_{10} and G_{24} again. In Section 4, we show that $C(M_{22}, 176)$ is related to a new 2-$(176, 16, 9)$ design with automorphism group M_{22}.

Almost all calculations in this paper are done by computer, especially using Magma [1]. This system has several databases of groups, and we use some of them to define a group G and its subgroup H. Then we determine the permutation representation of G on G/H by calculating the coset table. We further calculate the sets of fixed points of involutions, and then the code $C(G, G/H)$ is defined by Magma. Many properties of codes, e.g. the dimensions, the minimum weights, and the automorphism groups, are obtained by using built-in functions of Magma. We can also construct combinatorial configurations, e.g. 2-designs defined by codewords, in Magma, and their properties, e.g. the automorphism groups are calculated. Any G-invariant code can be viewed as a G-submodule over $\mathbb{F}_2$. For a given G, it is not easy to determine all G-submodules in general. But Magma can construct these for modest degrees n. We sometimes use the classification of G-submodules by Magma, in order to classify self-dual codes invariant under G. In many cases, we report the results of explicit computations without further comment.

We use the following notation and terminology. The symbols for almost simple groups are due to [4].

For an n-element set Ω, the power set $\mathcal{P}(\Omega)$ – the family of all subsets of Ω – is regarded as an n-dimensional vector space with the inner product $(X, Y) \equiv |X \cap Y| \pmod 2$ for $X, Y \in \mathcal{P}(\Omega)$. The *weight* of X is defined to be the integer $|X|$. A subspace C of $\mathcal{P}(\Omega)$ with dimension k and minimum weight d is called an $[n, k, d]$ code. The integer n is called the length of C, and a member of C is called a *codeword*. The automorphism group $\mathrm{Aut}(C)$ of the code C is the set of permutations of Ω which preserve C. Two codes are *equivalent* if one can be obtained from the other by a permutation of Ω. The *dual code* $C^\perp$ of C is the set of all $X \in \mathcal{P}(\Omega)$ satisfying $(X, Y) = 0$ for all $Y \in C$. A code C is said to be *self-orthogonal* if $C \subset C^\perp$, and *self-dual* if $C = C^\perp$. A *doubly even* (resp. *even*) code is a code whose codewords have weight divisible by 4 (resp. 2). A doubly even code is always self-orthogonal, and a self-orthogonal code is always even. A self-orthogonal code is said to be

singly even if it is not doubly even. It is known that a doubly even self-dual code of length n exists if and only if n is divisible by 8. Two self-dual codes C and C' are called *neighbors* if their intersection $C \cap C'$ is of codimension 1. For a singly even self-dual code C, the doubly even subcode C_0 is defined as a subcode of codimension 1 consisting of the codewords of C having weight $\equiv 0 \pmod 4$.

A t-(v, k, λ) *design* D is a set X of v points together with a collection of k-subsets of X (called blocks) such that every t-subset of X is contained in exactly λ blocks. The block intersection numbers of D are the cardinalities of the intersections of any two distinct blocks. A t-(v, k, λ) design D is called *self-orthogonal* if the block intersection numbers have the same parity as the block size k [15] and a 2-(v, k, λ) design D is called *symmetric* if all block intersection numbers are λ.

2 Main theorem and examples

Let G be a permutation group on an n-element set Ω. We define the binary code $C(G, \Omega)$ by

$$C(G, \Omega) = \langle \mathrm{Fix}(\sigma) | \sigma \in I(G) \rangle^{\perp}$$

where $I(G)$ denotes the set of involutions of G and $\mathrm{Fix}(\sigma)$ is the set of fixed points by σ. When G acts transitively on Ω and the permutation representation of degree n of G is uniquely determined up to equivalence, we write simply $C(G, n) = C(G, \Omega)$.

Theorem A. *Let C be a G-invariant binary self-orthogonal code of length n. Then $C \subset C(G, \Omega)$.*

Proof. Suppose that $\emptyset \neq X \in C$ and $\sigma \in I(G)$. Then $\langle \sigma \rangle$ acts on the set $X \cap \sigma(X)$. Since C is self-orthogonal, $|X \cap \sigma(X)|$ is even. We see that $\mathrm{Fix}(\sigma) \cap X \subset X \cap \sigma(X)$. Set $Y = (X \cap \sigma(X)) \setminus (\mathrm{Fix}(\sigma) \cap X)$. Then Y is the disjoint union of the sets $\{a, \sigma(a)\}$ for $a \in Y$. Thus $|Y|$ is even. Hence $|\mathrm{Fix}(\sigma) \cap X|$ is even. Therefore $X \in \langle \mathrm{Fix}(\sigma) | \sigma \in I(G) \rangle^{\perp}$. □

The following lemmas are useful to study $C(G, \Omega)$.

Lemma 2.1. *Let K act on Ω and G be a normal subgroup of K. Then $C(G, \Omega)$ is K-invariant.*

Proof. Take $x \in K$ and $\sigma \in I(G)$. For $i \in \mathrm{Fix}(\sigma)$, we have $(x\sigma x^{-1})(x(i)) = x\sigma(i) = x(i)$. Hence $\mathrm{Fix}(x\sigma x^{-1}) = x(\mathrm{Fix}(\sigma))$. Since $G \lhd K$, we have $C(G, \Omega)^{\perp} = \langle \mathrm{Fix}(\sigma) | \sigma \in I(G) \rangle$ is K-invariant. Thus the result follows. □

Lemma 2.2. *Let K act on Ω and G be a normal subgroup of K. If $C(G,\Omega)$ is self-orthogonal, then $C(G,\Omega) = C(K,\Omega)$.*

Proof. Since $G \subseteq K$, we have $C(K,\Omega) \subseteq C(G,\Omega)$. On the other hand, since $C(G,\Omega)$ is K-invariant by Lemma 2.1 and $C(G,\Omega)$ is self-orthogonal, we have $C(G,\Omega) \subseteq C(K,\Omega)$ by Theorem A. □

Lemma 2.3. *Suppose $G = \mathrm{Aut}(C(G,\Omega))$. If C_1, C_2 are distinct subcodes of $C(G,\Omega)$ satisfying $G = \mathrm{Aut}(C_1) = \mathrm{Aut}(C_2)$, then these are inequivalent.*

Proof. Suppose that there exists some permutation π on Ω such that $\pi(C_1) = C_2$. Then we have $\pi G \pi^{-1} = \mathrm{Aut}(\pi(C_1)) = \mathrm{Aut}(C_2) = G$. Hence π preserves $\langle \mathrm{Fix}(\sigma) | \sigma \in I(G) \rangle$, and thus $\pi \in \mathrm{Aut}(C(G,\Omega))$ $(= \mathrm{Aut}(C_1))$. This means that $C_1 = \pi(C_1) = C_2$, a contradiction. □

Lemma 2.4. *Let D be a self-orthogonal t-(n,k,λ) design with even k. Suppose that D is invariant under a permutation group G on the point set Ω. Then the code generated by the rows of its block-point incidence matrix of D is contained in $C(G,\Omega)$.*

Proof. Follows from the fact that the code is a G-invariant self-orthogonal code. □

There are several known self-orthogonal codes with sporadic almost simple groups as the automorphism groups. We illustrate the relation between these codes and $C(G,\Omega)$.

Example 2.5. Let $G = M_{24}$ and $n = 24$. It is well known that the set of fixed points of $2A$-involutions of G forms the Witt system (5-$(24,8,1)$ design) W_{24}, and $2B$-involutions are fixed point free. Since W_{24} generates G_{24}, we have $C(G,24)^{\perp} = G_{24}$. Since G_{24} is a self-dual code, we have $C(G,24) = G_{24}$. The code G_{24} is also obtained as $C(M_{12}\!:\!2, 24)$.

Example 2.6. Let $G = J_2 : 2$ and $n = 100$. By Theorem A, we have $C_{10} \subset C(G,100)$ since C_{10} is a self-dual code. Since C_{10} is generated by the set of fixed points of $2C$-involutions of G, we have $C_{10} \subseteq C(G,100)^{\perp}$. Taking the dual code, we have $C(G,100) = C_{10}$. In particular, C is the unique G-invariant self-dual code of length n.

Example 2.7. The third Conway group Co_3 has a 2-transitive action on a set Ω of 276 points. In [6], a doubly even $[276, 23, 100]$ code invariant under Co_3 is constructed. By comparing their dimensions, this code is equivalent to $C(Co_3, 276)$. It is mentioned in [6] that the set of the codewords of a fixed weight in the code $C(Co_3, 276)$ is a single Co_3-orbit and forms a 2-design. By

Lemma 2.4, there are no other self-orthogonal 2-$(276, 2k, \lambda)$ designs invariant under Co_3.

The stabilizer of a point of Ω is $McL{:}2$, the extension of the McLaughlin group by its outer automorphism, whose action on 275 points is of rank 3. It is shown in [6] that the code generated by the adjacency matrix of the rank 3 graph is a doubly even $[275, 22, 100]$ code (see also [12]). By comparing their dimensions, this code is equivalent to $C(McL, 275) = C(McL{:}2, 275)$.

Example 2.8. The Higman–Sims group HS has a 2-transitive action on a set Ω of 176 points. In [2], a self-orthogonal $[176, 22, 50]$ code with automorphism group HS is constructed. By comparing their dimensions, we have that this code is equivalent to $C(HS, 176)$. Moreover, in [2], it is shown that the codewords of weight 50 in the code form a symmetric 2-$(176, 50, 14)$ design which is isomorphic to the design D_{176} discovered by G. Higman [7], and the code is generated by the incidence matrix of the design. The automorphism group of the code is determined by the fact $\mathrm{Aut}(D_{176}) \cong HS$ in [7] .

Here we note that Higman's design is defined by using only the notion of M_{22} [7]. Indeed, the set Ω of 176 points can be described by using the Witt system W_{24}. That is, Ω can be identified as the set of blocks X of W_{24} satisfying $a \in X$ and $b \notin X$ for some fixed distinct points a, b of W_{24}. The group M_{22} acts transitively on Ω, and acts on $C(HS, 176)$. By comparing their dimensions, we have $C(M_{22}, 176) = C(HS, 176)$. Hence $\mathrm{Aut}(C(M_{22}, 176)) \cong HS$.

Example 2.9. The Higman–Sims graph is a rank 3 graph of 100 vertices whose automorphism group is $HS : 2$, the extension of the Higman–Sims group by its outer automorphism. By [16], the code generated by the adjacency matrix of the graph is a self-orthogonal $[100, 22, 22]$ code with automorphism group $HS{:}2$. By comparing their dimensions, the code $C(HS{:}2, 100)$ is equivalent to this code.

The code $C(HS, 100)$ is a $[100, 23, 22]$ code and $C(HS, 100) \cap C(HS, 100)^{\perp}$ is a doubly even $[100, 21, 32]$ code. By Theorem 2.1 in [10], there are three self-orthogonal $[100, 22]$ subcodes containing $C(HS, 100) \cap C(HS, 100)^{\perp}$. Two of them are $[100, 22, 32]$ codes and the other is a $[100, 22, 22]$ code. The former two codes are equivalent to C_{100} in [16], whose automorphism group is HS, and the latter one is equivalent to $C(HS{:}2, 100)$.

The following example is an infinite series of codes obtained as $C(G, \Omega)$.

Example 2.10. Let $G = AGL(n, 2)$ be the affine transformation group of the vector space of dimension n over a field of two elements. Then G acts transitively on the set of 2^n vectors of this space. The set of fixed points of

an involution in G is an affine subspace of dimension $n-k$ for some k with $1 \leq k \leq [n/2]$. Hence the code spanned by the set of fixed points of the involutions is equivalent to the Reed–Muller code $R([n/2], n)$ (see [9] for the definition of Reed–Muller codes). Hence the code $C(G, 2^n)$ is equivalent to the Reed–Muller code $R(n - [n/2] - 1, n)$.

Lemma 2.11. *If there exists a G-invariant self-dual code D ($\subset \mathcal{P}(\Omega)$), then $C(G,\Omega)^\perp \subset D \subset C(G,\Omega)$. In particular, the code $\langle \mathrm{Fix}(\sigma) | \sigma \in I(G) \rangle$ is self-orthogonal.*

Proof. By Theorem A, $D \subset C(G,\Omega)$. Then $C(G,\Omega)^\perp \subset D^\perp = D \subset C(G,\Omega)$. □

Lemma 2.11 is used in the next section in order to construct or classify all self-dual codes invariant under a fixed group. As an example, self-dual codes of length 132 with automorphism groups M_{11} are constructed from $C(M_{11}, 132)$ (see Section 3). However, there does not always exist a self-dual code even if $C(G,\Omega)^\perp \subset C(G,\Omega)$ (see the next example).

Example 2.12. Let $G = S_4(3)$ and $H = 3_+^{1+2} : 2A_4$. The code $C = C(G, G/H)$ is a $[40, 25, 4]$ code and $C^\perp$ is a doubly even $[40, 15, 8]$ code. We have by MAGMA that there are only four G-invariant subcodes between $C^\perp$ and C with dimensions 15, 16, 24 and 25. Hence there is no G-invariant self-dual code between $C^\perp$ and C.

If all the involutions in G act fixed point freely on Ω, then $C(G,\Omega)$ is the whole space $\mathcal{P}(\Omega)$. In this case, our theorem gives only a trivial result as follows.

Example 2.13. If $q \equiv 3 \pmod 4$, then we have $C(L_2(q),\Omega) = \mathcal{P}(\Omega)$ since a point stabilizer is of odd order. It is known that there exists a self-dual code of length $q+1$ invariant under $L_2(q)$ if $q \equiv -1 \pmod 8$, which is of course contained in $\mathcal{P}(\Omega) = C(L_2(q),\Omega)$.

For $q \not\equiv 3 \pmod 4$, we have $C(L_2(q),\Omega) = \{0\}$ if $q \equiv 0 \pmod 2$ and we have $C(L_2(q),\Omega)$ is a $[q+1, 1, q+1]$ code if $q \equiv 1 \pmod 4$.

Here we consider the imprimitive case. For the remainder of this section, we assume that the action of G on Ω is transitive for simplicity. So we may assume $\Omega = G/H$ for some subgroup H of G.

Lemma 2.14. *Let $\sigma \in I(G)$. If $\sigma(aH) = aH$ for some $a \in N_G(I(H))$, then $\sigma(bH) = bH$ for all $b \in N_G(I(H))$.*

Proof. If $\sigma(aH) = aH$, then $a^{-1}\sigma a \in I(H)$, and thus $\sigma \in I(H)$. For each $b \in N_G(I(H))$, we have $b^{-1}\sigma b \in H$, and thus $\sigma(bH) = bb^{-1}\sigma(bH) = bH$. □

Lemma 2.15. *For $a \in G \setminus H$, the following conditions are equivalent:*
(1) $a \in N_G(I(H))$;
(2) $\{H, aH\} \in C(G, G/H)$.
In particular, $N_G(I(H)) \neq H$ if and only if the minimum weight of $C(G, G/H)$ is equal to 2.

Proof. Let $a \in N_G(I(H)) \setminus H$ and $\sigma \in I(G)$. By Lemma 2.14, if $aH \in \mathrm{Fix}(\sigma)$ then $N_G(I(H))/H \subset \mathrm{Fix}(\sigma)$. Hence $|\{H, aH\} \cap \mathrm{Fix}(\sigma)| = 0$ or 2, that is, $\{H, aH\} \in C(G, G/H)$.

Conversely suppose $\{H, aH\} \in C(G, G/H)$. Let $s \in I(H)$. Then $sH = H$ and s also fixes aH by the assumption. Hence $saH = aH$ and $a^{-1}sa \in I(H)$. □

Suppose that $N_G(I(H)) \neq H$. Set $N = N_G(I(H))$, $r = |G : N|$, $m = |N : H|$, i.e., $n = mr$, and $\Omega' = G/N$. Let $G/N = \{g_1N, \dots, g_rN\}$, and set

$$X_i = g_i(N/H) = \{g_iaH \mid a \in N\} \ (i = 1, \dots, r).$$

Then $\Omega = G/H = X_1 \cup \cdots \cup X_r$, and $|X_i| = m$ for each i. For $\sigma \in I(G)$, set

$$F_1(\sigma) = \{g_iN \mid X_i \subset \mathrm{Fix}(\sigma)\},$$
$$F_2(\sigma) = \{g_iN \mid \sigma(X_i) = X_i\}.$$

By definition, $C(G, \Omega') = \langle F_2(\sigma) \mid \sigma \in I(G)\rangle^{\perp}$ $(\subset \mathcal{P}(\Omega'))$. Set

$$C' = \langle F_1(\sigma) \mid \sigma \in I(G)\rangle^{\perp} (\subset \mathcal{P}(\Omega')).$$

Proposition 2.16. *Under the above notations,*

$$C(G, G/H) = \{W \subset \Omega \mid \{g_iN \mid |W \cap X_i| = \text{odd}\} \in C'\}.$$

The group $\mathrm{Aut}(C(G, G/H))$ *is isomorphic to the wreath product* $S_m \wr \mathrm{Aut}(C')$.

Proof. Let $W \subset \Omega$. Set $E(W) = \{g_iN \mid |W \cap X_i| = \text{odd}\}$. Then $W \in C(G, G/H)$ if and only if $|W \cap \mathrm{Fix}(\sigma)|$ is even for each $\sigma \in I(G)$. This is equivalent to the condition that $|E(W) \cap F_1(\sigma)|$ is even, that is, $E(W) \in C'$, as required. Since $|\tau(W) \cap X_i| = |W \cap X_i|$ for any permutation τ on X_i, the symmetric group on X_i is contained in $\mathrm{Aut}(C(G, G/H))$.

Let $\rho \in \mathrm{Aut}(C(G, G/H))$. We denote by $\bar{\rho}$ the permutation on Ω' induced by ρ. Then the image of the map $\rho \mapsto \bar{\rho}$ is $\mathrm{Aut}(C')$, and further the kernel of this map is the direct product of the symmetric groups on X_i. Hence we have $\mathrm{Aut}(C(G, G/H)) \cong S_m \wr \mathrm{Aut}(C')$. □

Proposition 2.17. *Under the same notations as Proposition 2.16, the following statements hold:*
(1) *if m is even, then $C(G, G/H)^{\perp}$ is self-orthogonal;*
(2) *if m is odd, then $C(G, G/H)^{\perp}$ is self-orthogonal if and only if $C'^{\perp}$ is self-orthogonal;*
(3) *if $N_G(I(H)) \setminus H$ contains no involutions (note that this assumption holds if m is odd.), then $C' = C(G, \Omega')$.*

Proof. (1), (2) By Lemma 2.14, the set $\mathrm{Fix}(\sigma)$ ($\sigma \in I(G)$) is a union of some X_i's. Since the condition $X_i \subset \mathrm{Fix}(\sigma)$ is equivalent to $g_i N \in F_1(\sigma)$, we have

$$|\mathrm{Fix}(\sigma) \cap \mathrm{Fix}(\tau)| = m \times |F_1(\sigma) \cap F_1(\tau)|$$

for $\sigma, \tau \in I(H)$. Hence the assertions (1), (2) are easily verified.
(3) Clearly $F_1(\sigma) \subset F_2(\sigma)$. Let $g_i N \in F_2(\sigma)$. Then we have $\sigma(g_i(N/H)) = g_i(N/H)$, that is, $g_i^{-1}\sigma g_i \in N$. By the assumption, $g_i^{-1}\sigma g_i \in H$ and thus $g_i H \in \mathrm{Fix}(\sigma)$. This means that $X_i \subset \mathrm{Fix}(\sigma)$ and $g_i N \in F_1(\sigma)$. Hence we have $F_1(\sigma) = F_2(\sigma)$, that is, $C' = C(G, \Omega')$. □

3 Sporadic simple groups of degree ≤ 1000

In this section, we consider the codes $C = C(G, \Omega)$ ($\Omega = G/H$) when G is a sporadic almost simple group, such that $N_G(I(H)) = H$ and $|G/H| \leq 1000$, where H denotes a subgroup of G. Consequently, we find all self-dual codes of lengths ≤ 1000 invariant under such sporadic almost simple groups satisfying the above condition. In particular, new self-dual codes of lengths $330, 132, 132, 220, 352$ invariant under $M_{22} : 2, M_{11}, M_{12} : 2, M_{12}, HS : 2$ are constructed, respectively.

3.1 Results

The parameters of C and $C \cap C^{\perp}$ and the automorphism groups $\mathrm{Aut}(C)$ of C are listed in Table 1. When C is self-dual, self-orthogonal or doubly even, we indicate this in the third column. In the last column, we list the subgroups H when there are two codes of the same length for a given G. There are pairs of identical codes constructed from different groups. Some of them are explained by Lemma 2.2, and are denoted by † in the last column. The other identities are denoted by $\star$. Due to computer time limitations, we do not calculate the minimum weights and the automorphism groups for some codes. However, the automorphism groups are (theoretically) determined for some cases as we describe below.

Table 1: Sporadic groups of degree ≤ 1000

G	C	$C \cap C^{\perp}$	$\mathrm{Aut}(C)$	Remarks
M_{11}	$[11, 0]$	—	—	
	$[12, 1, 12]$	doubly even	S_{12}	$\star 1$
	$[55, 0]$	—	—	
	$[66, 21, 16]$	$[66, 1, 66]$	M_{11}	
	$[132, 67, 6]$	$[132, 65, 12]$	M_{11}	$\sharp$ (Example 3.5)
	$[165, 56, 18]$	$[165, 54, 20]$	M_{11}	
	$[330, 176, 6]$	$[330, 154, 8]$		$\sharp$
	$[396, 252, 6]$	$[396, 90]$		
	$[495, 341, 6]$	$[495, 109, 36]$		
	$[660, 506, 4]$	$[660, 144]$		
M_{12}	$[12, 1, 12]$	doubly even	S_{12}	$\star 1$
	$[66, 11, 20]$	self-orthogonal	S_{12}	
	$[144, 89, 12]$	$[144, 55, 20]$	$M_{12}:2$	$\sharp$, primitive ($L_2(11)$)
	$[144, 69, 12]$	$[144, 65, 16]$	$M_{12}:2$	imprimitive ($L_2(11)$)
	$[220, 111, 18]$	$[220, 109, 20]$	M_{12}	$\sharp$ (Example 3.7), $\diamond$
	$[396, 143]$	$[396, 109]$	$M_{12}:2$	$\diamond$
	$[495, 197]$	$[495, 143]$	$M_{12}:2$	$\diamond$, $4^2:D_{12}$
	$[495, 232]$	$[495, 118]$	$M_{12}:2$	$\star 2$, $\diamond$, $M_8.S_4 \cong 2^{1+4}_{+}.S_3$
	$[660, 353]$	$[660, 297]$		
	$[792, 539, 6]$	$[792, 243]$		
	$[880, 661, 4]$	$[880, 209]$	$M_{12}:2$	$\diamond$ (Example 3.3)
$M_{12}:2$	$[24, 12, 8]$	doubly even self-dual	M_{24}	$\star 3$
	$[132, 67, 12]$	$[132, 65, 12]$	$M_{12}:2$	$\sharp$ (Example 3.6)
	$[144, 57, 12]$	$[144, 55, 20]$	$M_{12}:2$	G' is primitive.
	$[144, 68, 12]$	$[144, 66, 16]$	$M_{12}:2$	G' is imprimitive.
	$[396, 111]$	$[396, 109]$	$M_{12}:2$	$\diamond$
	$[440, 286]$	$[440, 154]$		$\sharp$
	$[495, 232]$	$[495, 118]$	$M_{12}:2$	$\star 2$, $\diamond$, $(2^{1+4}_{+}.S_3).2$
	$[495, 155]$	$[495, 153]$	$M_{12}:2$	$\diamond$, $(4^2:D_{12}).2$
	$[880, 476]$	$[880, 362]$	$M_{12}:2$	$\diamond$

Table 1: Sporadic groups of degree ≤ 1000 (continued)

G	C	$C \cap C^{\perp}$	$\mathrm{Aut}(C)$	Remarks
M_{22}	$[22, 11, 6]$	self-dual	$M_{22}{:}2$	†1
	$[77, 21, 16]$	self-orthogonal	$M_{22}{:}2$	†2
	$[176, 22, 50]$	self-orthogonal	HS	⋆4
	$[231, 87]$	$[231, 45, 48]$	$M_{22}{:}2$	⋄ (Example 3.1)
	$[330, 176]$	$[330, 154]$	$M_{22}{:}2$	♯, ⋄
	$[462, 273, 6]$	$[462, 91, 30]$		$2^4{:}A_5 \not\subset L_3(4)$
	$[462, 308, 6]$	$[462, 154]$	$M_{22}{:}2$	♯, $2^4{:}A_5 \subset L_3(4)$
	$[616, 418, 6]$	$[616, 164]$	$M_{22}{:}2$	⋄
	$[672, 473]$	$[672, 199]$	$M_{22}{:}2$	♯, ⋄ (Example 3.2)
	$[770, 473]$	$[770, 199]$		
$M_{22}{:}2$	$[22, 11, 6]$	self-dual	$M_{22}{:}2$	†1
	$[77, 21, 16]$	self-orthogonal	$M_{22}{:}2$	†2
	$[231, 76, 30]$	$[231, 56, 32]$	$M_{22}{:}2$	⋄
	$[330, 165, 10]$	self-dual	$M_{22}{:}2$	⋄
	$[352, 198]$	$[352, 154, 16]$		♯
	$[462, 298, 6]$	$[462, 164, 24]$	$M_{22}{:}2$	♯, $2^4{:}S_5 \subset L_3(4){:}2_2$
	$[462, 122, 6]$	$[462, 102, 24]$		$2^4{:}S_5 \not\subset L_3(4){:}2_2$
	$[616, 231]$	$[616, 211]$	$M_{22}{:}2$	⋄
	$[672, 322]$	$[672, 210]$	$M_{22}{:}2$	⋄
	$[770, 287, 10]$	$[770, 245]$		
M_{23}	$[23, 11, 8]$	doubly even	M_{23}	
	$[253, 77, 28]$	$[253, 55, 56]$	M_{23}	$L_3(4){:}2_2$
	$[253, 66, 32]$	doubly even	M_{23}	$2^4{:}A_7$
	$[506, 67, 56]$	self-orthogonal	M_{23}	⋄
M_{24}	$[24, 12, 8]$	doubly even self-dual	M_{24}	⋆3
	$[276, 78, 36]$	doubly even	M_{24}	⋄
	$[759, 264]$	$[759, 242]$	M_{24}	⋄
J_1	$[266, 1, 266]$	self-orthogonal	S_{266}	
J_2	$[100, 63, 8]$	$[100, 37, 16]$	$J_2{:}2$	♯
	$[280, 92, 28]$	self-orthogonal	$J_2{:}2$	†3, ⋄
	$[315, 118]$	$[315, 36, 80]$	$J_2{:}2$	⋄
	$[525, 140]$	doubly even	$J_2{:}2$	†4, ⋄
	$[840, 329]$	$[840, 231]$	$J_2{:}2$	⋄

Table 1: Sporadic groups of degree ≤ 1000 (continued)

G	C	$C \cap C^{\perp}$	$\mathrm{Aut}(C)$	Remarks
$J_2{:}2$	$[100, 50, 10]$	self-dual	$J_2{:}2$	
	$[280, 92, 28]$	self-orthogonal	$J_2{:}2$	†3, $\diamond$
	$[315, 77, 42]$	self-orthogonal	$J_2{:}2$	$\diamond$
	$[525, 140]$	doubly even	$J_2{:}2$	†4, $\diamond$
	$[840, 280]$	doubly even	$J_2{:}2$	$\diamond$
HS	$[100, 23, 22]$	$[100, 21, 32]$	$HS{:}2$	
	$[176, 22, 50]$	self-orthogonal	HS	$\star$4
$HS{:}2$	$[100, 22, 22]$	self-orthogonal	$HS{:}2$	
	$[352, 177, 16]$	$[352, 175, 16]$		♯ (Example 3.8)
McL	$[275, 22, 100]$	doubly even	$McL{:}2$	†5
$McL{:}2$	$[275, 22, 100]$	doubly even	$McL{:}2$	†5
Co_3	$[276, 23, 100]$	doubly even	Co_3	

If G is primitive on Ω, then $\mathrm{Aut}(C(G, \Omega))$ is also primitive since $G \subset \mathrm{Aut}(C(G, \Omega))$. The primitive groups of degree < 2500 are classified in [13, 14] and MAGMA has a database of these groups. From the classification, we can determine $\mathrm{Aut}(C(G, \Omega))$ for some cases, which are denoted by $\diamond$ in the last column. We give some typical cases in the following examples. Similar arguments determine the automorphism groups for other primitive cases.

Example 3.1. Let $G = M_{22}$ and $|\Omega| = 231$. Set $C = C(G, \Omega)$. By Lemma 2.1, we have that C is $M_{22}{:}2$-invariant. By the classification of all primitive groups of degree 231, $\mathrm{Aut}(C) = M_{22}{:}2$, A_{22}, S_{22}, A_{231} or S_{231}. By MAGMA, we have $C(A_{22}, 231) = C(S_{22}, 231)$ is a self-orthogonal $[231, 21, 40]$ code. Since $C \cap C^{\perp}$ is self-orthogonal, we have $C \cap C^{\perp} \subset C(\mathrm{Aut}(C \cap C^{\perp}), \Omega)$ by Theorem A. Since $C \cap C^{\perp}$ is a $[231, 45, 48]$ code, we have $\mathrm{Aut}(C \cap C^{\perp}) = M_{22}{:}2$. Since $\mathrm{Aut}(C) \subseteq \mathrm{Aut}(C \cap C^{\perp})$, we have $\mathrm{Aut}(C) = M_{22}{:}2$.

Example 3.2. Consider the case that $G = M_{22}$ and $|\Omega| = 672$. By Lemma 2.1, we have $C(M_{22}, 672)$ is $M_{22}{:}2$-invariant. The primitive groups of degree 672 are M_{22}, $M_{22}{:}2$, $U_6(2)$, $U_6(2){:}2$, $U_6(2){:}3$, $U_6(2){:}S_3$, A_{672} and S_{672}. Take a subgroup M_{22} of $U_6(2)$. Then we have verified by MAGMA that $C(M_{22}, 672)$ is not $U_6(2)$-invariant. Thus we have $\mathrm{Aut}(C(M_{22}, 672)) = M_{22}{:}2$.

Example 3.3. Consider the case that $G = M_{12}$ and $|\Omega| = 880$. We note that M_{12} is not primitive on 880 points. We have $C(M_{12}, 880)$ is $M_{12} : 2$-invariant by Lemma 2.1. Since $M_{12} : 2$ is primitive on 880 points, we have $\mathrm{Aut}(C(M_{12}, 880)) = M_{12}{:}2$ by the classification of primitive groups.

3.2 Self-dual codes

Table 1 contains three known self-dual codes with parameters $[24, 12, 8]$ for $G = M_{12}:2$, M_{24}, $[22, 11, 6]$ for $G = M_{22}$, $M_{22}:2$, $[100, 50, 10]$ for $G = J_2:2$, together with the following (new) self-dual code.

Proposition 3.4. *The code $C(M_{22}:2, 330)$ is a self-dual $[330, 165, 10]$ code whose automorphism group is $M_{22}:2$.*

By Lemma 2.11, there are possibilities of the existence of new G-invariant self-dual codes in the following cases (denoted by $\sharp$ in Table 1):

$$\begin{aligned}
G =& M_{11}, [132, 67], [330, 176],\\
G =& M_{12}, [144, 89], [220, 111],\\
G =& M_{12}:2, [132, 67], [440, 286],\\
G =& M_{22}, [330, 176], [462, 308], [672, 473],\\
G =& M_{22}:2, [352, 198], [462, 298],\\
G =& J_2, [100, 63],\\
G =& HS:2, [352, 177].
\end{aligned}$$

In Examples 3.5, 3.6, 3.7, 3.8, we consider the four cases where $C^\perp (\subset C)$ is doubly even, and $\dim(C/C^\perp) = 2$. There exist exactly three self-dual subcodes of C. Let D be one of them. We have $\mathrm{Aut}(D) \subset \mathrm{Aut}(C^\perp) = \mathrm{Aut}(C)$, since $\mathrm{Aut}(D)$ preserves its doubly even subcode $C^\perp$ of D.

Example 3.5. Suppose that $G = M_{11}$ and $|\Omega| = 132$. $C = C(G, \Omega)$ is a $[132, 67, 6]$ code. Two self-dual codes $C_{132,1}, C_{132,2}$ have minimum weight 12 and the other $C_{132,3}$ has minimum weight 6. The group G acts on the set of the three self-dual codes. Since G contains no subgroup of index ≤ 3, the code $C_{132,i}$ is G-invariant, that is, $G \subset \mathrm{Aut}(C_{132,i})$ for each $i = 1, 2, 3$. Since $\mathrm{Aut}(C_{132,i}) \subset \mathrm{Aut}(C) = G$, we have $G = \mathrm{Aut}(C_{132,i})$ for each $i = 1, 2, 3$. By Lemma 2.3, these are inequivalent to each other.

Example 3.6. Suppose that $G = M_{12} : 2$ and $|\Omega| = 132$. $C = C(G, \Omega)$ is a $[132, 67, 12]$ code. The three self-dual codes $C_{132,4}, C_{132,5}, C_{132,6}$ have minimum weight 12. We note that the equality $G = \mathrm{Aut}(C)$ is verified by Magma. By Lemma 2.3, these are inequivalent to each other.

Example 3.7. Suppose that $G = M_{12}$ and $|\Omega| = 220$. $C = C(G, \Omega)$ is a $[220, 111, 18]$ code. The three self-dual codes have minimum weights $18, 20, 20$. Let D be one of them. We determine the automorphism group $\mathrm{Aut}(D)$. By [14], a primitive permutation group of degree 220 is one of M_{12},

A_{12}, S_{12}, A_{220}, S_{220}. Since $C(A_{12}, 220) = C(S_{12}, 220)$ is a $[220, 55, 28]$ code, the groups A_{12}, S_{12} (and also A_{220}, S_{220}) do not act on D. Hence we have $\mathrm{Aut}(D) = M_{12}$. Similarly we have $\mathrm{Aut}(C) = M_{12}$. By Lemma 2.3, these are inequivalent to each other.

Example 3.8. Suppose that $G = HS\!:\!2$ and $|\Omega| = 352$. $C = C(G, \Omega)$ is a $[352, 177]$ code. The three self-dual codes have minimum weight 16. Since the length is divisible by eight, two self-dual codes are doubly even and the other is singly even (see Theorems 2.1 and 2.2 in [10]). We do not calculate the automorphism groups of the codes, and do not determine the (in)equivalence of the two doubly even codes.

To find all G-invariant self-dual codes for the other cases, we determine all G-submodules of $C(G, n)$. The code $C(J_2, 100)$ is a $[100, 63, 8]$ code and $C(J_2, 100)^\perp$ is a doubly even $[100, 37, 16]$ code. The adjacency matrix of the Hall-Janko graph of 100 vertices generates a doubly even $[100, 36, 16]$ code C_A [8] (see also [3]). The code $C(J_2, 100)^\perp$ is generated by C_A and the all-ones vector. We constructed three self-dual codes C_{10}, C_{16}, C'_{16} invariant under J_2 in [3]. By Theorem A, they are contained in $C(J_2, 100)$. We verify by MAGMA that $C(J_2, 100)$ has exactly 7 J_2-invariant submodules (subcodes) containing $C(J_2, 100)^\perp$, three of which are self-dual. Hence we have the following:

Theorem 3.9. *Let C be a self-dual code of length 100 invariant under J_2. Then C is equivalent to one of the codes C_{10}, C_{16} and C'_{16} given in [3].*

Similarly, by determining all G-submodules, the numbers # of distinct self-dual codes of length n invariant under G are determined for the remaining groups G. We do not determine the (in)equivalence of the codes. The results are listed in Table 2. From the table, we have the following result.

Proposition 3.10. *There is no self-dual code of lengths 144 and 672 invariant under M_{12} and M_{22}, respectively. The unique self-dual code of length 330 under invariant M_{22} is the $[330, 165, 10]$ code $C(M_{22} : 2, 330)$ given in Proposition 3.4.*

4 HS- and M_{22}-invariant 2-designs

We first consider M_{22} as a permutation group of degree 176. By Example 2.8, the automorphism group of the code $\langle \mathrm{Fix}(u) | u \in I(M_{22}) \rangle$ is also isomorphic to HS. This gives another construction of HS from M_{22} via the code. We

Table 2: Numbers of self-dual codes invariant under G

G	$(n, \#)$
M_{11}	$(330, 3)$
M_{12}	$(144, 0)$
$M_{12}:2$	$(440, 35)$
M_{22}	$(330, 1), (462, 83), (672, 0)$
$M_{22}:2$	$(352, 10), (462, 55)$

remark that HS does not act on the set of generators $\{\mathrm{Fix}(u)|u \in I(M_{22})\}$. It is interesting that the configuration $(\Omega, \{\mathrm{Fix}(u)|u \in I(M_{22})\})$ forms a 2-design with automorphism group M_{22}.

Proposition 4.1. *The incidence structure* $(\Omega, \{\mathrm{Fix}(u)|u \in I(M_{22})\})$ *is a* 2-$(176, 16, 9)$ *design with automorphism group* M_{22}.

Proof. Set $G = M_{22}$. Since $I(G)$ forms a single conjugacy class, $|\mathrm{Fix}(u)|$ does not depend on the choice of u. Let $X, Y \in \Omega$ with $X \neq Y$. Then the stabilizer G_X of X is isomorphic to A_7. Since $|I(A_7)| = 105$ and $|I(G)| = 1155$, we have $|\mathrm{Fix}(u)| = (176 \times 105)/1155 = 16$. Moreover the stabilizer $G_{X,Y}$ of X, Y is isomorphic to S_4 or $3^2:4$ according to $|X \cap Y| = 4$ or 2 as blocks of W_{24}. Hence $|I(G_{X,Y})|$ is always equal to 9. This means that the incidence structure is a 2-$(176, 16, 9)$ design. The automorphism group is calculated by Magma. □

We secondly consider $HS:2$ as a permutation group of degree 100 whose action is of rank 3 (see Example 2.9). It is known [16] that the codewords of weight 36 in the self-orthogonal $[100, 22, 22]$ code $C(HS:2, 100)$ form a self-orthogonal 2-$(100, 36, 525)$ design $D_{100,1}$. We have verified by Magma that the codewords of weight 40 in $C(HS:2, 100)$ form a self-orthogonal 2-$(100, 40, 14560)$ design $D_{100,2}$ and the codewords of the other weights ≤ 50 do not form a 2-design. By Magma, the automorphism groups of the designs are $HS:2$.

In addition, we have verified by Magma that any union of HS-orbits of codewords of each weight in $[100, 22, 32]$ code and the $[100, 22, 22]$ code obtained in Example 2.9 does not form a 2-design. By Lemma 2.4, we have the following:

Proposition 4.2. *The designs* $D_{100,1}, D_{100,2}$ *and their complementary designs are self-orthogonal* 2*-designs whose automorphism groups are* $HS:2$. *There are no other self-orthogonal* 2-$(100, 2k, \lambda)$ *designs invariant under* HS.

References

[1] W. Bosma and J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, Available online at `http://magma.maths.usyd.edu.au/magma/`.

[2] A.R. Calderbank and D.B. Wales, A global code invariant under the Higman–Sims group, *J. Algebra* **75** (1982), 233–260.

[3] N. Chigira, M. Harada and M. Kitazume, Some self-dual codes invariant under the Hall–Janko group, preprint.

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

[5] J.H. Conway and N.J.A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory* **36** (1990), 1319–1333.

[6] W.H. Haemers, C. Parker, V. Pless and V. Tonchev, A design and a code invariant under the simple group Co_3, *J. Combin. Theory Ser. A* **62** (1993), 225–233.

[7] G. Higman, On the simple group of D. G. Higman and C. C. Sims, *Illinois J. Math.* **13** (1969), 74–80.

[8] J.D. Key and J. Moori, Codes, designs and graphs from the Janko groups J_1 and J_2, *J. Combin. Math. Combin. Comput.* **40** (2002), 143–159.

[9] F.J. MacWilliams and N.J.A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1977.

[10] F.J. MacWilliams, N.J.A. Sloane and J.G. Thompson, Good self dual codes exist, *Discrete Math.* **3** (1972), 153–162.

[11] C.L. Mallows and N.J.A. Sloane, An upper bound for self-dual codes, *Inform. Control* **22** (1973), 188–200.

[12] J. Moori and B.G. Rodrigues, A self-orthogonal doubly even code invariant under $M^cL{:}2$, *J. Combin. Theory Ser. A* **110** (2005), 53–69.

[13] C.M. Roney-Dougal, The primitive permutation groups of degree less than 2500, *J. Algebra* **252** (2005), 154–183.

[14] C.M. Roney-Dougal and W.R. Unger, The affine primitive permutation groups of degree less than 1000, *J. Symbolic Comput.* **35** (2003), 421–439.

[15] V.D. Tonchev, A characterization of designs related to the Witt system $S(5, 8, 24)$, *Math. Z.* **191** (1986), 225–230.

[16] V.D. Tonchev, Binary codes derived from the Hoffmon–Singleton and Higman–Sims graphs, *IEEE Trans. Inform. Theory* **43** (1997), 1021–1025.