ISSN: 1017-060X (Print)

ISSN: 1735-8515 (Online)

Bulletin of the

Iranian Mathematical Society

Vol. 43 (2017), No. 7, pp. 2183–2204

Title:

Linear codes with complementary duals related to the complement of the Higman-Sims graph

Author(s):

B.G. Rodrigues

Published by the Iranian Mathematical Society
http://bims.ims.ir

Bull. Iranian Math. Soc.
Vol. 43 (2017), No. 7, pp. 2183–2204
Online ISSN: 1735-8515

LINEAR CODES WITH COMPLEMENTARY DUALS RELATED TO THE COMPLEMENT OF THE HIGMAN-SIMS GRAPH

B.G. RODRIGUES

(Communicated by Ali Reza Ashrafi)

Dedicated to Professor Jamshid Moori on the occasion of his 70^{th} *birthday*

Abstract. In this paper we study codes $C_p(\overline{\mathrm{HiS}})$ where $p = 3, 7, 11$ defined by the 3- 7- and 11-modular representations of the simple sporadic group HS of Higman and Sims of degree 100. With exception of $p = 11$ the codes are those defined by the row span of the adjacency matrix of the complement of the Higman-Sims graph over $GF(3)$ and $GF(7)$. We show that these codes have a similar decoding performance to that of their binary counterparts obtained from the Higman-Sims graph. In particular, we show that these are linear codes with complementary duals, and thus meet the asymptotic Gilbert-Varshamov bound. Furthermore, using the codewords of weight 30 in $C_p(\overline{\mathrm{HiS}})$ we determine a subcode of codimension 1, and thus show that the permutation module of dimension 100 over the fields of 3, 7 and 11-elements, respectively is the direct sum of three absolutely irreducible modules of dimensions 1, 22 and 77. The latter being also the subdegrees of the orbit decomposition of the rank-3 representation.

Keywords: Strongly regular graph, Higman-Sims graph, linear code, automorphism group.
MSC(2010): Primary: 94B05; Secondary: 05B05, 20D45.

1. Introduction

Tonchev [24] proved that the binary codes of the Higman-Sims graph are optimal and in most cases attain the recorded distance, and moreover are amenable to majority logic decoding. It seems thus natural to ask whether this remains true for other primes p such that $p \mid |G|$, where $G = \mathrm{HS}$ is the Higman-Sims group. In the present paper, we answer this question in the affirmative for the p-ary codes of the complementary graph $\overline{\mathrm{HiS}}$ of the Higman-Sims

Article electronically published on December 30, 2017.
Received: 31 May 2016, Accepted: 15 January 2017.

graph HiS. In particular, for $p = 3, 7, 11$ we show that the codes are optimal since they meet the asymptotic Gilbert-Varshamov bound. This is achieved by showing that these codes belong to the class of codes known as linear codes with complementary duals. A linear code with complementary dual (an LCD code) was defined in [19] to be a linear code C whose dual code $C^{\perp}$ satisfies $C \cap C^{\perp} = \{0\}$. Furthermore, using tools from representation theory we answer a question posed by Lux and Pahlings [17], by showing that the permutation module of the Higman-Sims group of dimension 100 over the field of 3-elements is the direct sum of three absolutely irreducible modules of dimensions 1, 22 and 77, respectively. Observe that the dimensions of these modules are precisely the sizes of the suborbits of the rank-3 representation of the Higman-Sims group of degree 100 on the cosets of the Mathieu group M_{22}. As a by-product we show that the same is true over the field of 7- and 11-elements, i.e., the permutation module of dimension 100 over the field of 7- and 11 elements is the direct sum of three absolutely irreducible submodules (i.e., subcodes) of dimensions 1, 22 and 77 respectively.

Hence, we deduce the following main result summarized in Theorem 1.1. In the theorem we collect the parameters and some properties of the codes defined by the row span over $\mathbb{F}_p$ $(p = 3, 7)$ of the rows of the adjacency matrix of the complementary graph $\overline{\mathrm{HiS}}$ of the Higman-Sims graph HiS.

Theorem 1.1. *Let* $\overline{\mathrm{HiS}}$ *denote the complementary graph of the Higman-Sims graph* HiS *and let* $C_p(\overline{\mathrm{HiS}})$ $(p = 3, 7)$ *be the codes of length 100 defined by the* p*-ary row span of the adjacency matrix of* $\overline{\mathrm{HiS}}$. *Then the following hold*

(a) $C_p(\overline{\mathrm{HiS}})$ *is a linear code with complementary dual.*

(b) $C_3(\overline{\mathrm{HiS}}) = [100, 23, 23]_3$ *and* $C_7(\overline{\mathrm{HiS}})^{\perp} = [100, 23, 23]_7$, *and their dual codes* $C_p(\overline{\mathrm{HiS}})^{\perp} = [100, 77, 8]_p$ *are irreducible optimal codes.*

(c) *The permutation module of Higman-Sims group of dimension 100 over* $\mathbb{F}_p$ *for* $p \in \{3, 7, 11\}$ *is the direct sum of three absolutely irreducible modules of dimensions 1, 22 and 77 respectively.*

(d) *(d)* $\mathrm{Aut}(C_p(\overline{\mathrm{HiS}})) \cong \mathrm{HS{:}2}$.

The proof of Theorem 1.1 follows from a series of lemmas and propositions in Sections 4.1 and 5. The paper is organized as follows: after a brief description of our terminology and some background in Section 2, Section 3 outlines the background material related with the Higman-Sims graph and its group, and in Sections 4, 4.1, and in subsections 5.1 through to 5.4 we present our results. Our results are described explicitly as being those related with the 3-, and 7-ary codes defined by the row span of the adjacency matrix of the complementary graph $\overline{\mathrm{HiS}}$ of the Higman-Sims graph HiS, and the 11-ary codes given by the decomposition of the permutation module of dimension 100 invariant under the Higman-Sims group.

2. **Preliminaries and notation**

Let $\mathbb{F}$ be a finite field of order $q = p^t$, where p is a prime and $t \in \mathbb{N}$; let G be 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 $\mathbb{F}\Omega = \{\sum_{\omega \in \Omega} g_\omega \omega \,|\, g_\omega \in \mathbb{F}\}$ 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

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

for all $\mathbf{g} = \sum_{\omega \in \Omega} g_\omega \omega$ 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 $a \in G$, $\mathbf{g} = \sum_{\omega \in \Omega} g_\omega \omega$ 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. 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. If C_1 is an $[n_1, k_1]$-code, and C_2 is an $[n_2, k_2]$-code, then we say that C is the *direct sum* of C_1 and C_2 if (up to reordering of coordinates) $C = \{(x, y) \,|\, x \in C_1, y \in C_2\}$. We denote this by $C = C_1 \oplus C_2$. If moreover C_1 and C_2 are nonzero, then we say that C decomposes into C_1 and C_2. A code C is said to be *decomposable* if and only if it is equivalent to a code which is the direct sum of two or more linear codes. Otherwise, it is called *indecomposable*.

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. 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 $\mathrm{Aut}(C)$. We are interested in finding all G-invariant $\mathbb{F}G$-submodules, i.e., codes in $\mathbb{F}\Omega$.

Remark 2.1. For $x \in \mathbb{F}^n$ and a permutation $\sigma \in S_n$ we set

$$\sigma x = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \ldots, x_{\sigma^{-1}(n)}). \tag{2.1}$$

Let C be a linear code over $\mathbb{F}$ of length n and let $G \leq \mathrm{Aut}(C)$. If the action of G on C is defined by Equation (2.1) then the code C becomes an $\mathbb{F}G$-module. Note that the ambient space $\mathbb{F}^n$ is also an $\mathbb{F}G$-module with respect to the same action of G. The fact that C is an $\mathbb{F}G$-module is formulated in the following statement.

Result 2.2. *Let C be an $[n, k, d]_q$ code and let $G \leq \mathrm{Aut}(C)$. Then C is a k-dimensional submodule of the ambient space $\mathbb{F}^n$, considered as an $\mathbb{F}G$-module.*

Our notation for designs, graphs and groups will be standard, and it is as in [1, 6] and 𝔸𝕋𝕃𝔸𝕊 [9]. 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 *graphs* $\Gamma = (V, E)$ with vertex set V and edge set E, discussed here are undirected and simple, that is, with no loops or multiple edges, apart from the case in where *all* loops are included in which case the graph is called *reflexive*. A graph is *regular* if all its vertices have the same valency. An *adjacency matrix* A of a graph of order $n := |V|$ is an $n \times n$ matrix with entries a_{ij} such that $a_{ij} = 1$ if vertices v_i and v_j are adjacent, and $a_{ij} = 0$ otherwise. A regular graph is *strongly regular* of type (n, k, λ, μ) if it has n vertices, each of degree k, and if any two adjacent vertices are together adjacent to λ vertices, while any two non-adjacent vertices are together adjacent to μ vertices. The complementary graph of a strongly regular graph of type (n, k, λ, μ) is a strongly regular graph of type $(n, n-k-1, n-2k+\mu-2, n-2k+\lambda)$. If x is a vertex of Γ then the *neighbourhood graph* $\Gamma(x)$ with respect to x is the subgraph of Γ which is induced by all vertices that are adjacent to x. The neighbourhood graph of a vertex x of a strongly regular graph Γ is also called the *first subconstituent* of Γ. The subgraph of Γ induced on all vertices of Γ which are not adjacent to (and different from) x, is called a *second subconstituent.* The *neighbourhood design* of a regular graph is the 1-design formed by taking the points to be the vertices of the graph and the blocks to be the sets of neighbours of a vertex, for each vertex. The *code* of a graph Γ over a finite field F is the row span of an adjacency matrix A over the field F, denoted by $C_F(\Gamma)$ or $C_F(A)$. The dimension of the code is the rank of the matrix over F, also written $\mathrm{rank}_p(A)$ if $F = \mathbb{F}_p$, in which case we will speak of the *p-rank* of A or Γ, and write $C_p(\Gamma)$ or $C_p(A)$ for the code.

3. **The Higman-Sims graph and its group**

The notation $G.H$, $G:H$, and $G^{\cdot}H$ is used to denote a general extension, a split extension and a non-split extension, respectively. For a prime p, the symbol p^n denotes an elementary abelian group of that order. If p is an odd prime, p_+^{1+2n} and p_-^{1+2n} denote the extraspecial groups of order p^{1+2n} and exponent p or p^2 respectively.

The simple group $G = \mathrm{HS}$ of Higman and Sims can be constructed from the Higman-Sims graph HiS. Let $\mathrm{HiS} = (\Omega, \mathcal{E})$ be a graph of valence 22 on the set Ω of 100 points such that any given vertex has 22 neighbours (points) and the remaining 77 vertices are joined to 6 of these points and may be labelled by the corresponding hexad. Two of the 77 vertices are joined only if the corresponding hexads are disjoint. The hexads form a Steiner system $S(3, 6, 22)$. The Higman-Sims simple group HS is the subgroup of even permutations of $\mathrm{Aut(HiS)} \cong$ HS:2, the automorphism group of HS. The point stabilizer in Aut(HiS) on Ω is $\mathrm{Aut}(S(3, 6, 22)) \cong \mathrm{M}_{22}{:}2$ and the order of the Higman-Sims group HS is $44352000 = 2^9{\cdot}3^2{\cdot}5^3{\cdot}7{\cdot}11$. The action of HS on Ω yields a unique primitive rank-3 representation of degree 100, in which the point stabilizer is the Mathieu group M_{22}, and the orbits have lengths 1, 22 and 77 respectively. The Higman-Sims graph HiS has parameters $(100, 22, 0, 6)$ and spectrum $22^1 2^{77}(-8)^{22}$. The parameters of the complementary graph $\overline{\mathrm{HiS}}$ of HiS are $(100, 77, 60, 56)$ and spectrum $77^1, 7^{22}, (-3)^{77}$. HS and $\mathrm{Aut}(HS)$ have the orbits Γ_0, Γ_1, and Γ_2 in $\Omega \times \Omega$ where

$$\begin{aligned}
\Gamma_0 &= \{(\alpha, \alpha) \,|\, \alpha \in \Omega\},\\
\Gamma_1 &= \{(\alpha, \beta) \,|\, \{\alpha, \beta\} \in \mathcal{E}\},\\
\Gamma_2 &= \{(\alpha, \beta) \,|\, \alpha, \beta \in \Omega,\ \alpha \neq \beta \text{ and } \{\alpha, \beta\} \notin \mathcal{E}\}.
\end{aligned}$$

Table 1. Maximal subgroups of HS and HS:2

No.	Max. sub. of HS	Deg.	Max. sub. of HS:2	Deg.
1	M_{22}	100	HS	2
2	$U_3(5):2$	176	$M_{22}:2$	100
3	$U_3(5):2$	176	$L_3(4){:}2^2$	1100
4	$L_3(4):2_1$	1100	$S_8\times 2$	1100
5	S_8	1100	$2^5\cdot S_6$	3850
6	$2^4\cdot S_6$	3850	$4^3{:}(L_3(2)\times 2)$	4125
7	$4^3:L_3(2)$	4125	$2_+^{1+6}{:}S_5$	5775
8	M_{11}	5600	$2\times A_6\cdot 2^2\cdot 2$	15400
9	M_{11}	5600	$5^{1+2}{:}(Q_8{:}4)$	22176
10	$4{\cdot}2^4{:}S_5$	5775	$5{:}4\times S_5$	36960
11	$2\times A_6.2^2$	15400		
12	$5:4\times A_5$	36960		

We use the notation $\Gamma_i(\alpha)=\{\beta\,|\,(\alpha,\beta)\in\Gamma_i\}$ for the G_α-orbits. With this we observe that $|\Gamma_i(\alpha)|=1,22,77$ for $i=0,1,2$.

For more information on the Higman-Sims group we refer the reader to the $\mathbb{ATLAS}$ [9, p.80] or [25, Section 5.5.1] and for the Higman-Sims graph the reader could consult [11].

Result 3.1 (Magliveras [18])**.** *The Higman-Sims group* HS *has exactly* 12 *conjugacy classes of maximal subgroups, as follows:*

M_{22}
$L_3(4){:}2_1$
$2^4.S_6$
M_{11} (2 *classes*)
$2\times A_6{\cdot}2^2$

$U_3(5){:}2$ (2 *classes*)
S_8
$4^3{:}L_3(2)$
$4{\cdot}2^4{:}S_5$
$5{:}4\times A_5$.

The primitive representations described in Result 3.1 are of degrees 100, 176, 176, 1100, 1100, 3850, 4125, 5600, 5600, 5575, 15400 and 36960 respectively. In Table 1 below the first column depicts the ordering of the primitive representations of HS and HS:2 respectively, as given by Magma (or the $\mathbb{ATLAS}$ [9]) and as used in our computations; the second gives the maximal subgroups; the third gives the degrees (the number of cosets of the point stabilizer).

4. The p-ary codes of length 100 related with the $\overline{\text{HiS}}$ graph

Applying [16, Corollary 3.2], we consider a stem cover U of the group $G=\text{HS}$ and take U_ω to be the inverse image of the stabilizer G_ω. Then all linear codes of a given length over a field $\mathbb{F}$ and invariant under a permutation group G are obtained by inducing all 1-dimensional $\mathbb{F}U_\omega$-modules up to U. The submodules of the resulting $\mathbb{F}U$-modules form a complete list of codes invariant under $(G,\ \Omega)$ as a permutation group. Since we are in the modular case we determine those submodules which are kernels or images of module endomorphisms and as in [15] we term these types of submodules endo-submodules. The complete lattice of submodules then is obtained from relations between endo-submodules, their orthogonal spaces and some possible additional considerations.

The reader is reminded of the notation introduced in Section 3 where Ω represents the set of vertices of HiS and of $\overline{\text{HiS}}$, and Γ_0, Γ_1, and Γ_2 are the orbitals of HiS with $|\Gamma_i(x)| = 1, 77, 22$. The matrix A_i in the centralizer algebra of (G, Ω) is defined by

$$A_i = (f_i(\alpha, \beta))_{(\alpha,\beta)\in\Omega\times\Omega},$$

where $f_i(\alpha, \beta) = 1$, if $(\alpha, \beta) \in \Gamma_i$ and $f_i(\alpha, \beta) = 0$, otherwise. Recall from Section 2 that $\mathbb{F}$ is the finite field $\mathbb{F}_q$ and that $\mathbb{F}\Omega$ is the permutation module of (G, Ω) over $\mathbb{F}$ so that to each A_i there is a naturally assigned endomorphism $\mathbf{a}_i$ such that

$$\beta \mapsto \beta\mathbf{a}_i = \sum f_i(\alpha, \beta)\beta.$$

Let A_0, A_1, A_2 be the matrices in the centralizer algebra of (G, Ω) associated with the orbitals Γ_0, Γ_1, and Γ_2 and $\mathbf{a}_i$ denotes the endomorphism of the permutation module $\mathbb{F}\Omega$ corresponding to the matrix A_i or the orbital Γ_i. The endomorphism algebra $E(\mathbb{F}\Omega) = \text{End}_{\mathbb{F}G}\mathbb{F}\Omega$ has basis $(\mathbf{a}_0, \mathbf{a}_1, \mathbf{a}_2)$ where $\mathbf{a}_0 = Id_{\mathbb{F}\Omega}$. This basis is called Schur basis in [17]. According to [17, Theorem 1.2.20] (see also [5, Chapter 3] or [14, 15]),

$$E(\mathbb{F}\Omega) \to \mathbb{F}^{3\times3},\ \mathbf{a}_i \mapsto A_i = [a_{ijk}]_{j,k=1,\ldots,3} \quad (1 \le i \le 3),$$

gives the regular matrix representation of $E(\mathbb{F}\Omega)$ with respect to the Schur basis. The matrices $M_j = ((a_j)_{ik})$ are called the intersection matrices of the orbital graphs (Ω, Γ_i) or of Ω.

The structure of the Higman-Sims graph (and its complement) gives the following values:

$$M_0 = \mathbf{I}_3, \quad M_1 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 21 & 16 \\ 77 & 56 & 60 \end{bmatrix}, \ M_2 = \begin{bmatrix} 0 & 1 & 0 \\ 22 & 0 & 6 \\ 0 & 21 & 16 \end{bmatrix}.$$

The common eigenspaces $\xi_i(a_j)$ of the intersection matrices over a field of characteristic zero are displayed in the "character table" $[\xi_i(a_j)]_{1\le i,j\le 3}$ given below

$$[\xi_i(a_j)] = \begin{bmatrix} 1 & 77 & 22 \\ 1 & 7 & -8 \\ 1 & -3 & 2 \end{bmatrix}.$$

This is also the character table of multiplicity-free endomorphism rings of Higman-Sims group in its rank-3 permutation representation of degree 100 as given in [20, 22].

4.1. **The p-ary codes of length 100 from the** HiS**-graph.** Using representation theory, Knapp and Schaeffer [15] provided an algebraic and geometric description of the binary codes related with the Higman-Sims graph. To some extent this paper is a sequel to [15] in that we obtain results on the p-ary codes defined by the row span of the adjacency matrices of the HiS-graph and its complement $\overline{\text{HiS}}$. It turns out that all faithful irreducible modules of HS over these fields, and defined as the p-ary row span of the adjacency matrix of the complementary $\overline{\text{HiS}}$ graph can be represented in this way as the code, the dual code or the hull of the code. We start by examining the p-ary codes of the HiS-graph.

Unless $p = 2$, the p-ary codes defined by the adjacency matrix of the HiS-graph are not interesting as it can be seen in Lemma 4.1.

Lemma 4.1. *The p-ary codes of length 100 defined by the row span of the adjacency matrix of the* HiS*-graph over $\mathbb{F}_p$ are trivial unless $p = 2$.*

Proof. Recall that the eigenvalues of the adjacency matrix A of the HiS-graph are $\beta_0 = 22, \beta_1 = 2$, and $\beta_2 = -8$ with corresponding multiplicities $m_0 = 1, m_1 = 22$ and $m_2 = 77$. Since none of the $\beta_i \bmod p$ vanishes, whenever $p = 3, 5, 7$ we deduce from [4, Proposition 13.7.1(iv)] that $\text{rank}_p(\text{HiS}) = 100$. That $\text{rank}_p(\text{HiS}) = 22$ for $p = 2$, follows from [3] or [24]. Finally, we can show that $\text{rank}_{11}(\text{HiS}) = 99$. □

Remark 4.2. In Lemma 4.1 we saw that the only interesting codes associated with the HiS-graph are binary. This is essentially the motivation to examine in the ensuing sections the p-ary codes of the adjacency matrix of the complementary graph $\overline{\text{HiS}}$. In particular, the reader will notice in Lemma 4.5 that in this case the interesting primes are $p = 3, 7$. We shall show in Section 5 that the codes are asymptotically good and hence optimal. In view of the preceding discussion, in the immediate section we use representation theory to understand the submodule structure of the permutation module of dimension 100 over $\mathbb{F}_3$ and discuss the 7-, and 11-ary codes in the subsequent sections of the paper.

The submodule structure of $\mathbb{F}_3\Omega$ is displayed in Table 3.

Proposition 4.3. *Let $\mathbb{F} = \mathbb{F}_3$. Then $F\Omega$ has precisely the following endo-submodules N_i with* $\dim N_i = i$*. $N_{100} = \mathbb{F}\Omega$, $N_0 = 0$, $N_{99} = Ker(a_0 + a_1 + a_2)$, $N_1 = Im(a_0 + a_1 + a_2)$, $N_{77} = Ker(a_1)$, $N_{23} = Im(a_1)$, $N_{78} = N_{77} + N_1$, $N_{22} = N_{100}/N_{78}$. In addition the following hold:*

(i)

$$\{N_i \,|\, i \in \{0,\ 1,\ 22,\ 23,\ 77,\ 78,\ 99,\ 100\}\}$$

Table 2. Incidence matrix of the poset of submodules of $\mathbb{F}_3\Omega = {\mathbb{F}_3}^{100\times 1}$

dim	0	1	22	23	77	78	99	100
0	1	1	1	1	1	1	1	1
1	.	1	.	1	.	1	.	1
22	.	.	1	1	.	.	1	1
23	.	.	.	1	.	.	.	1
77	.	.	.	.	1	1	1	1
78	.	.	.	.	.	1	.	1
99	.	.	.	.	.	.	1	1
100	.	.	.	.	.	.	.	1

is the complete set of $\mathbb{F}G$-submodules of $\mathbb{F}\Omega$ and $\dim N_i = i$ *for all i.*

(ii) *We have $0 = N_0 < N_{22} < N_{99} < N_{100} = \mathbb{F}\Omega$ is a composition series of $\mathbb{F}\Omega$ as an $\mathbb{F}G$-module. The dimensions of the composition factors in the composition series are 22, 77, 1. All composition factors are absolutely irreducible.*

(iii) *Every composition factor of $\mathbb{F}\Omega$ remains irreducible when restricted to $G_\omega \cong M_{22}$.*

(iv) *${N_i}^\perp = N_{100-i}$ for all i.*

Proof. In this case the result holds, with the proof virtually the same as that of [15, Proposition 2.6]. Thus we omit the details. □

We summarize the results of this section in the following:

Theorem 4.4. *Let $G =$ HS be the Higman-Sims simple in its rank-3 representations on Ω of degree 100. Then every linear code $C_3(N_i)$ of length 100 over the field $\mathbb{F} = \mathbb{F}_3$ admitting G is obtained up to isomorphism from one of the $\mathbb{F}G$-submodules of the permutation module $\mathbb{F}\Omega$ which are given in Proposition 4.3.*

In Remark 4.2 we suggested that apart from the binary codes the only other codes of length 100 invariant under the HS-group which are of interest for applications are those associated with the primes $p = 3, 7$. Lemma 4.5 deals with the p-ranks of the adjacency matrix $\overline{A}$ of the graph $\overline{\text{HiS}}$.

Lemma 4.5. *The adjacency matrix $\overline{A}$ of the graph $\overline{\text{HiS}}$ has 3-rank 23, 7-rank 77, 11-rank 99, and p-rank 100 for $p = 2, 5$.*

Proof. The 3-rank of the adjacency matrix $\overline{A}$ of $\overline{\text{HiS}}$ and thus the dimension of $C_3(\overline{\text{HiS}})$ can be deduced readily by using the spectrum of the graph. Observe from Section 3 that $\overline{A}$ has eigenvalues $\theta_0 = 77, \theta_1 = 7$, and $\theta_2 = -3$

with multiplicities $m_0 = 1, m_1 = 22$ and $m_2 = 77$. Now, using [4, Proposition 13.7.1] or [3, Section 3] we obtain an upper bound on the 3-rank of $\overline{A}$, namely that $\mathrm{rank}_3(\overline{A}) \leq \min(m_1 + 1, m_2 + 1) = 23$. Since by [4, Proposition 13.3.2] $\mathrm{rank}_3(\overline{A}) \geq \sum\{m_i \,|\, \theta_i \not\equiv 0 \pmod 3\} = 1 + 22$, the assertions follows.

For $p = 7$, since $\theta_0 \equiv \theta_1 \equiv 0 \pmod 7$ and $\theta_2 \not\equiv 0 \pmod 7$, we deduce from [4, Proposition 13.7.1(iv)] that $\mathrm{rank}_7(\overline{A}) = 77$. Since $\det(J - \overline{A}) \not\equiv 0 \pmod{11}$, where J is the all-one matrix we obtain that the 11-rank of $\overline{A}$ equals 99. For $p = 2, 5$ observe that none of the θ_i mod p vanishes, so we obtain $\mathrm{rank}_p\overline{A} = 100$. □

5. Linear codes with complementary duals

Massey [19] defines a linear code with a complementary dual to be a linear code C whose dual $C^{\perp}$ satisfies $C \cap C^{\perp} = \{0\}$, and gives the algebraic characterization of these codes. He showed further that linear codes with complementary duals are asymptotically good codes, but stopping short of showing whether these codes attain the Gilbert-Varshamov bound. Much later Sendrier [23] showed that linear codes with complementary duals meet the asymptotic Gilbert-Varshamov bound in the strong sense. A renewed interest has emerged in recent years in application of these codes to cryptography in improving the security of information processed by sensitive devices, in particular in finding counter-measures to side-channel attacks or fault non-invasive attacks, see [7] for a complete description. In the sections which follow we use results of [23] to show that the codes with parameters $[100, 23, 23]_3$, $[100, 77, 8]_3$, $[100, 77, 8]_7$, and $[100, 23, 23]_7$ obtained from the complementary graph $\overline{\mathrm{HiS}}$ are linear codes with complementary duals and thus meet the asymptotic Gilbert-Varshamov bound. In addition, we show the same to hold for the codes with parameters $[100, 77, 8]_{11}$, and $[100, 23, 23]_{11}$ obtained from the decomposition of the permutation module of dimension 100 over $\mathbb{F}_{11}$.

5.1. Ternary codes of the adjacency matrix of the $\overline{\mathrm{HiS}}$-graph.

Proposition 5.1 is an application of Lemma 4.5, and relates our previous discussions with coding theory. To this end we prove

Proposition 5.1. *$C_3(\overline{\mathrm{HiS}}) = N_3$ is a $[100, 23, 23]_3$ code and $C_3(\overline{\mathrm{HiS}})^{\perp} = {N_3}^{\perp}$ is a $[100, 77, 8]_3$ code with 173250 words of weight 8. The minimum weight 23 of $C_3(\overline{\mathrm{HiS}})$ is the valency of the reflexive graph $(\mathrm{HiS})^r$ with adjacency matrix $A+I$, and the minimum weight vectors are the rows of adjacency matrix of $(\mathrm{HiS})^r$ and their scalar multiples. Moreover $\mathbf{1} \in C_3(\overline{\mathrm{HiS}})$, $C_3(\overline{\mathrm{HiS}}) \oplus C_3(\overline{\mathrm{HiS}})^{\perp} = \mathbb{F}_3^{100}$ and $\mathrm{Aut}(\overline{\mathrm{HiS}}) = \mathrm{Aut}(C_3(\overline{\mathrm{HiS}})) \cong \mathrm{HS{:}2}$. Further, $C_3(\overline{\mathrm{HiS}})^{\perp}$ is the unique $\mathbb{F}_3$-module of its dimension on which HS and HS:2 act faithfully and irreducibly.*

Proof. That the dimension of $C_3(\overline{\mathrm{HiS}})$ is as stated, follows from Lemma 4.5 where we showed that $\mathrm{rank}_3(C_3(\overline{\mathrm{HiS}})) = 23$.
For the automorphism group of the code, it is well known that $\mathrm{Aut}(\overline{\mathrm{HiS}}) \cong \mathrm{HS}{:}2$. Since $C_3(\overline{\mathrm{HiS}})$ is determined by the ternary row span of the adjacency matrix of $\overline{\mathrm{HiS}}$, $\mathrm{Aut}(\overline{\mathrm{HiS}}) \subseteq \mathrm{Aut}(C_3(\overline{\mathrm{HiS}}))$. Now, order consideration give us the result. In addition, the 3-modular character table of HS is completely known (see [13]) and it follows from it that the irreducible 77-dimensional $\mathbb{F}_3$-representation is unique (this can also be deduced from Proposition 4.3(i) and (ii); part(i) (uniqueness) and part (ii) (irreducibility)). It follows from this that $C_3(\overline{\mathrm{HiS}})^{\perp}$ is the unique $\mathbb{F}_3$-module of its dimension on which HS and HS:2 act faithfully and irreducibly. Since $C_3(\overline{\mathrm{HiS}})$ is the code spanned by the rows of the adjacency matrix of the reflexive graph $(\mathrm{HiS})^r$, we see that the minimum weight of $C_3(\overline{\mathrm{HiS}}) \geq 23$. However, computations with Magma [2] show that the minimum weight of $C_3(\overline{\mathrm{HiS}})$ is 23 and so the assertion follows. Taking the images of the supports of the codewords of minimum weight under the action of the automorphism we obtain exactly 200 such codewords, and thus these constitute the rows of $(\mathrm{HiS})^r$ and their scalar multiples. In Table 4, we give the weight distribution of $C_3(\overline{\mathrm{HiS}})$. In this table, i represents the weight of a codeword w_i in $C_3(\overline{\mathrm{HiS}})$ and A_i denotes the number of codewords of weight i.

Computations with Magma show that $C_3(\overline{\mathrm{HiS}})^{\perp}$ has minimum weight 8. That $\mathbf{1} \in C_3(\overline{\mathrm{HiS}})$ follows since $3 \nmid 77$, with 77 being the constant column sums of the adjacency matrix A of the graph $\overline{\mathrm{HiS}}$. Furthermore, Ω is a transitive HS-set and since $|\Omega| = 100$ is invertible in $\mathbb{F}_3$, it follows from [17, Lemma 1.2.4] that $\mathbb{F}_3^{100} = C_3(\overline{\mathrm{HiS}}) \oplus C_3(\overline{\mathrm{HiS}})^{\perp}$ as claimed. Moreover, [23, Corollary 8] assures us that $C_3(\overline{\mathrm{HiS}})$ and $C_3(\overline{\mathrm{HiS}})^{\perp}$ meet the asymptotic Gilbert-Varshamov bound in the strong sense. Finally, it can be verified from [10] that $C_3(\overline{\mathrm{HiS}})^{\perp}$ attains the recorded distance for a code of the given length and dimension. □

Remark 5.2. The code $C_3(\overline{\mathrm{HiS}})$ can also be constructed as the code of the adjacency matrix $A+I$ of the reflexive graph $(\mathrm{HiS})^r$ obtained from the Higman-Sims graph by including all loops. In this way we obtain a self-dual symmetric 1-$(100, 23, 23)$ design $\mathcal{D}$ whose blocks are the incidence vectors of the rows of $A + I$. Notice that the dimension and the minimum weight of $C_3(\overline{\mathrm{HiS}})$ equal 23. These can be given a geometrical interpretation.
The minimum weight is the valency of the reflexive graph $(\mathrm{HiS})^r$, and the words of minimum weight in $C_3(\overline{\mathrm{HiS}})$ are the rows of the adjacency matrix of $\overline{\mathrm{HiS}}$ and their scalar multiples. Under the action of $\mathrm{Aut}(C_3(\overline{\mathrm{HiS}}))$ the set of codewords of weight 23 splits into two orbits of size 100 each. The stabilizers of a codeword in each of these orbits are maximal subgroups of HS and $\mathrm{Aut}(C_3(\overline{\mathrm{HiS}}))$ of orders 443520 and 887040 that are isomorphic to M_{22} and $\mathrm{M}_{22}{:}2$, respectively.

TABLE 3. Weight distribution of $C_3(\overline{\mathrm{HiS}})$

i	A_i	i	A_i	i	A_i
0	1	56	689920000	76	1038633750
23	200	57	966152000	77	708492600
30	2200	58	1426792400	78	429137200
34	30100	59	2077567800	79	231316800
36	8250	60	2940814800	80	122075800
40	38500	61	3840513600	81	48602400
42	2200	62	4745194300	82	25995200
43	259600	63	5603888400	83	7838600
44	824100	64	6647269200	84	1478400
45	1940400	65	7343802400	85	1861200
46	616000	66	8152382700	86	1179200
47	739200	67	7941395000	87	123200
48	5005000	68	7994686700	88	869400
49	1463000	69	6813637600	90	246400
50	21900912	70	6298591200	92	78650
51	15994000	71	5069585400	93	46200
52	92369200	72	4456508650	94	7700
53	129360000	73	3407558000	98	2200
54	292630800	74	2467634400	100	906
55	425656000	75	1652458808		

The dual code $C_3(\overline{\mathrm{HiS}})^{\perp}$ has minimum distance 8 which coincides with the known recorded distance for the parameters $[100, 77]$ (this follows from [2] and also from [10]).

5.2. **Orbits of** $\mathrm{Aut}(C_3(\overline{\mathrm{HiS}}))$ **on small weight codewords.** The reader will recall that we use (G, Ω) for the right action of G on Ω. Henceforth, we shall use the notation $\Omega{:}G$ to denote the set of G-orbits on Ω and $\Omega_{i(j)}$ will denote the j-th suborbits of the orbit decomposition of the orbit Ω_i. The reader is cautioned not to confuse this notation with that used for the semidirect product of two groups. Using this notation we give an explicit description of the codewords of $C_3(\overline{\mathrm{HiS}})$ of weight up to 44, and where possible using the geometry of the $\overline{\mathrm{HiS}}$-graph and the knowledge of the structure of the subgroup lattice of HS [8], we provide a geometric description of the nature of some classes of codewords. In particular, for these classes of codewords of given non-trivial weights in the code, we use the well-known Assmus-Mattson Theorem to determine some point- and block-primitive 1-designs which are held by the codewords. To this end, let $M = \{23, 30, 34, 36, 40, 42, 43, 44\}$ and for $m \in M$ we define $W_m(C_3(\overline{\mathrm{HiS}})) = \{w_m \in C_3(\overline{\mathrm{HiS}}) \,|\, wt(w_m) = m\}$, where $\mathrm{wt}(w_m)$ represents the weight of w_m. We have

Proposition 5.3. *The orbits in $W_m(C_3(\overline{\mathrm{HiS}})))$ for $1 \leq m \leq 8$ are as follows:*

(i) $W_{23}(C_3(\overline{\mathrm{HiS}}))$:$\mathrm{Aut}(C_3(\overline{\mathrm{HiS}})) = \{\Omega_{1(1)}, \Omega_{1(2)}\}$ *with* $|\Omega_{1(1)}| = |\Omega_{1(2)}| = 100$.

(ii) $W_{30}(C_3(\overline{\mathrm{HiS}}))$:$\mathrm{Aut}(C_3(\overline{\mathrm{HiS}})) = \{\Omega_{2(1)}, \Omega_{2(2)}\}$ *with* $|\Omega_{2(1)}| = |\Omega_{2(2)}| = 1100$.

(iii) $W_{34}(C_3(\overline{\mathrm{HiS}}))$:$\mathrm{Aut}(C_3(\overline{\mathrm{HiS}})) = \{\Omega_{3(i)} \,|\, 1 \leq i \leq 4\}$ *with* $|\Omega_{3(1)}| = |\Omega_{3(2)}| = 11200$ *and* $|\Omega_{3(3)}| = |\Omega_{3(4)}| = 3850$.

(iv) $W_{36}(C_3(\overline{\mathrm{HiS}}))$:$\mathrm{Aut}(C_3(\overline{\mathrm{HiS}})) = \{\Omega_{4(1)}, \Omega_{4(2)}\}$ *with* $|\Omega_{4(1)}| = |\Omega_{4(2)}| = 4125$.

(v) $W_{40}(C_3(\overline{\mathrm{HiS}}))$:$\mathrm{Aut}(C_3(\overline{\mathrm{HiS}})) = \{\Omega_{5(i)} \,|\, 1 \leq i \leq 4\}$ *where* $|\Omega_{5(1)}| = |\Omega_{5(2)}| = 15400$ *and* $|\Omega_{5(3)}| = |\Omega_{5(4)}| = 3850$.

(vi) $W_{42}(C_3(\overline{\mathrm{HiS}}))$:$\mathrm{Aut}(C_3(\overline{\mathrm{HiS}})) = \{\Omega_{6(1)}, \Omega_{6(2)}\}$ *with* $|\Omega_{6(1)}| = |\Omega_{6(2)}| = 1100$.

(vii) $W_{43}(C_3(\overline{\mathrm{HiS}}))$:$\mathrm{Aut}(C_3(\overline{\mathrm{HiS}})) = \{\Omega_{7(i)} \,|\, 1 \leq i \leq 6\}$ *where* $|\Omega_{7(1)}| = |\Omega_{7(2)}| = 61600$, $|\Omega_{7(3)}| = |\Omega_{7(4)}| = 35200$ *and* $|\Omega_{7(5)}| = |\Omega_{7(6)}| = 33000$.

(viii) $W_{44}(C_3(\overline{\mathrm{HiS}}))$:$\mathrm{Aut}(C_3(\overline{\mathrm{HiS}})) = \{\Omega_{8(i)} \,|\, 1 \leq i \leq 10\}$ *where* $|\Omega_{8(1)}| = |\Omega_{8(2)}| = 154000$, $|\Omega_{8(3)}| = |\Omega_{8(4)}| = 132000$, $|\Omega_{8(5)}| = |\Omega_{8(6)}| = 67200$, $|\Omega_{8(7)}| = |\Omega_{8(8)}| = 57750$, *and* $|\Omega_{8(9)}| = |\Omega_{8(10)}| = 1100$.

Proof. As in the proof of [15, Proposition 3.1], we can use facts about the action of $G_\omega \cong \mathrm{M}_{22}$, where $\omega \in \Omega$ to establish the proposition. □

Remark 5.4. A continuation we give a geometric description of the codewords of minimum weight, even though using the geometry of the graph and possibly of the Steiner systems we could achieve a geometric interpretation of almost all sets $W_m(C_3(\overline{\mathrm{HiS}}))$ given in Proposition 5.3.

(i) $W_{23}(C_3(\overline{\mathrm{HiS}}))$ represents the incidence vectors of the blocks of the 1-(100, 23, 23) design (and their scalar multiples) obtained by taking the support of the codewords of minimum weight and orbiting their images under HS:2; $W_{30}(C_3(\overline{\mathrm{HiS}}))$ are copies of the conics of the Higman's geometry (and their scalar multiples), see [21];

(ii) Each set $W_{36}(C_3(\overline{\mathrm{HiS}}))$ of 4125 codewords of weight 36 forms the blocks of a 1-$(100, 36, 1485)$ design. This is in fact a 2-$(100, 36, 525)$ self-orthogonal design.

In Table 5 the first column represents the codewords of weight m and the second column gives the parameters of the designs $\mathcal{D}_{w_m}$ which were constructed by taking the images of the supports of the codewords of weight m and orbiting these under the action of $\mathrm{Aut}(C_3(\overline{\mathrm{HiS}}))$. In the third column, we list the number

Table 4. 1-designs $\mathcal{D}_{w_m}$ from HS:2

m	$\mathcal{D}_{w_m}$	No. of blocks	Primitivity
$(23)_1$	$1\text{-}(100, 23, 23)$	100	Yes
$(23)_2$	$1\text{-}(100, 23, 23)$	100	Yes
$(30)_1$	$1\text{-}(100, 30, 330)$	1100	Yes
$(30)_2$	$1\text{-}(100, 30, 330)$	1100	Yes
$(34)_1$	$1\text{-}(100, 34, 3808)$	11200	No
$(34)_2$	$1\text{-}(100, 34, 3808)$	11200	No
$(34)_3$	$1\text{-}(100, 34, 1309)$	3850	Yes
$(34)_4$	$1\text{-}(100, 34, 1309)$	3850	Yes
$(36)_1$	$1\text{-}(100, 36, 1485)$	4125	Yes
$(36)_2$	$1\text{-}(100, 36, 1485)$	4125	Yes
$(40)_1$	$1\text{-}(100, 40, 6160)$	15400	Yes
$(40)_2$	$1\text{-}(100, 40, 6160)$	15400	Yes
$(40)_3$	$1\text{-}(100, 40, 1540)$	3850	Yes
$(40)_4$	$1\text{-}(100, 40, 1540)$	3850	Yes
$(43)_1$	$1\text{-}(100, 43, 26488)$	61600	No
$(43)_2$	$1\text{-}(100, 43, 26488)$	61600	No
$(43)_3$	$1\text{-}(100, 43, 15136)$	35200	No

Table 5. 1-designs $\mathcal{D}_{w_m}$ from HS:2

m	$\mathcal{D}_{w_m}$	No. of blocks	Primitivity
$(43)_4$	$1\text{-}(100, 43, 15136)$	35200	No
$(43)_5$	$1\text{-}(100, 43, 14190)$	33000	No
$(43)_6$	$1\text{-}(100, 43, 14190)$	33000	No
$(44)_1$	$1\text{-}(100, 44, 67760)$	154000	No
$(44)_2$	$1\text{-}(100, 44, 67760)$	154000	No
$(44)_3$	$1\text{-}(100, 44, 58080)$	132000	No
$(44)_4$	$1\text{-}(100, 44, 58080)$	132000	No
$(44)_5$	$1\text{-}(100, 44, 29568)$	67200	No
$(44)_6$	$1\text{-}(100, 44, 29568)$	67200	No
$(44)_7$	$1\text{-}(100, 44, 29568)$	57750	No
$(44)_8$	$1\text{-}(100, 44, 29568)$	57750	No
$(44)_9$	$1\text{-}(100, 44, 484)$	1100	Yes
$(44)_{10}$	$1\text{-}(100, 44, 484)$	1100	Yes

of blocks of $\mathcal{D}_{w_m}$. We test the primitivity for the action of HS:2 on $\mathcal{D}_{w_m}$ in the final column.

Next in Lemma 5.5 by considering w_m where $m \in M$ we describe the structures of $(\mathrm{HS{:}2})_{w_m}$ and show that these are with some exceptions always maximal subgroups of HS:2.

Lemma 5.5. *Let $m \in M$ and $w_m \in W_m(C_3(\overline{\mathrm{HiS}}))$. Then the following occur:*

(i) *If* $m \notin \{34, 43, 44\}$ *then* $(\mathrm{HS}{:}2)_{w_m}$ *is a maximal subgroup of* HS:2.
(ii) *If* $m = 34$ *then* $(\mathrm{HS}{:}2)_{w_m} \cong 2^5{:}S_6$ *or* $(\mathrm{HS}{:}2)_{w_m} \cong \mathrm{M}_{11}$ *and* M_{11} *is not a maximal subgroup of* HS:2.
(iii) *If* $m = 43$ *then* $(\mathrm{HS}{:}2)_{w_m}$ *is not a maximal subgroup of* HS:2.
(iv) *If* $m = 44$ *then* $(\mathrm{HS}{:}2)_{w_m} \in \{3{:}S_3 \cdot 2{:}2 \times 2 \times 2 \cdot 2, L_2(7){:}2 \times 2, L_2(11){:}2, 2^{1+6}{:}2{:}S_3, L_3(4){:}2_1\}$ *and unless* $(\mathrm{HS}{:}2)_{w_m} = L_3(4){:}2_1$ *any other group in this list is not a maximal subgroup of* HS:2.

Proof. The proof follows from a case-by-case analysis. For part (i) consider a subset $\overline{M}$ of M such that $\overline{M} = \{23, 30, 36, 40, 42\}$. For each choice of $m \in \overline{M}$, we have that under the action of HS:2 the set $W_{w_m}(C_3(\overline{\mathrm{HiS}}))$ splits into at least two pairwise orbits of the same size, and moreover, the number of suborbits in this action is always even. Without loss of generality, we choose $m = 40$, as a prototype and give an explicit proof in this case. All the remaining cases follow the same arguments, and so we omit them. For $m = 40$ the set $W_{w_{40}}(C_3(\overline{\mathrm{HiS}}))$ splits into four distinct suborbits of pairwise equal size, namely $W_{40}(1), W_{40}(2), W_{40}(3)$, and $W_{40}(4)$, of lengths $15400, 15400, 3850$ and 3850 respectively. Let $a \in W_{40}(1)$, $b \in W_{40}(2)$, $c \in W_{40}(3)$ and $d \in W_{40}(4)$. By the orbit stabilizer Theorem and the $\mathbb{ATLAS}$ (or Table 2) we have $[\mathrm{HS}{:}2 : (\mathrm{HS}{:}2)_{w_m}] \in \{15400, 3850\}$. Using the list of maximal subgroups of $HS{:}2$ (see Table 2), we deduce that $(\mathrm{HS}{:}2)_{w_{40_a}} \in \{2 \times A_6 \cdot 2^2 \cdot 2,\ H,\ K,\ L, N\}$, where H is a subgroup of index 154 in $\mathrm{M}_{22}{:}2$, K of index 4 in $2^5 \cdot S_6$, L of index 14 in $S_8 \times 2$ and N of index 14 in $L_3(4){:}2^2$. We deal with the elimination of H, K, L and N in the following:

(1) From the list of maximal subgroups of $\mathrm{M}_{22}{:}2$, there are two possible candidates for H, either a subgroup of index 7 in $L_3(4){:}2_2$ or of index 2 in $2^4{:}S_6$. The list of maximal subgroups of $L_3(4)$ shows that it contains no subgroup of index 7. The group $2^4{:}S_6$ is a maximal subgroup of $\mathrm{M}_{22}{:}2$ and computations with Magma show that its non-trivial normal subgroups are of type 2^4, and hence it cannot have a subgroup of index 2.
(2) We constructed the maximal subgroup $2^5 \cdot S_6$ inside HS:2 and found out that it does not contain a subgroup of index 4.
(3) Lists of maximal subgroups of $S_8 \times 2$ and $L_3(4){:}2^2$ [9] eliminate the possibilities of L and N.

Therefore, $(\mathrm{HS}{:}2)_a = 2 \times A_6 \cdot 2^2 \cdot 2$. Similarly, $(\mathrm{HS}{:}2)_b = 2 \times A_6 \cdot 2^2 \cdot 2$. Since $(\mathrm{HS}{:}2)_c$ or $(\mathrm{HS}{:}2)_d$ is a subgroup of order 23040, we deduce from Table 2 that $(\mathrm{HS}{:}2)_c \cong 2^5 \cdot S_6$ (respectively $(\mathrm{HS}{:}2)_d \cong 2^5 \cdot S_6$).
Parts (ii), (iii) and (iv) follow similarly. □

In Table 6 we give the structure of the stabilizers of the codewords w_m as described in Lemma 5.5.

TABLE 6. Stabilizer in HS:2 of a word w_m

m	$(\mathrm{HS}{:}2)_{w_m}$	Maximality
23	$M_{22}{:}2$	Yes
30	$S_8 \times 2$	Yes
$(34)_{1,2}$	M_{11}	No
$(34)_{3,4}$	$2^5 \cdot S_6$	Yes
36	$4^3(L_3(2) \times 2)$	Yes
$(40)_{1,2}$	$2 \times A_6 \cdot 2^2 \cdot 2$	Yes
$(40)_{3,4}$	$2^5 \cdot S_6$	Yes
$(42)_{1,2}$	$L_3(4){:}2^2$	Yes
$(43)_{1,2}$	$A_6{:}2{:}2$	No
$(43)_{3,4}$	A_7	No
$(43)_{5,6}$	$2^3{:}L_2(7) \times 2$	No
$(44)_{1,2}$	$3{:}S_3 \cdot 2{:}2 \times 2 \times 2 \cdot 2$	No
$(44)_{3,4}$	$L_2(7){:}2 \times 2$	No
$(44)_{5,6}$	$L_2(11){:}2$	No
$(44)_{7,8}$	$2^{1+6}{:}2{:}S_3$	No
$(44)_{9,10}$	$L_3(4){:}2_1$	Yes

A problem in Lux and Pahlings, see [17, Exercise 1.3.7 (d)] requires to show that the permutation module of the Higman-Sims group of dimension 100 over $\mathbb{F}_3$ is the direct sum of three absolutely irreducible modules of dimensions 1, 22 and 77 respectively. It can be observed from the $\mathbb{ATLAS}$ [9] that these are the irreducible constituents of the permutation representation of HS on the cosets of the Mathieu group M_{22}, and coincide with the subdegrees of this representation. In Lemma 5.6 below, we show that the words of weight 30 in $C_3(\overline{\mathrm{HiS}})$ span a subcode of codimension 1, and that this is the smallest and unique irreducible $\mathbb{F}_3$-module of its dimension invariant under HS and HS:2, respectively. Moreover, we show that $\mathbb{F}_3^{100} = \langle 1 \rangle \oplus \mathcal{L} \oplus \mathcal{K}$, where $\langle 1 \rangle$, $\mathcal{L}$ and $\mathcal{K}$ are absolutely irreducible modules of dimensions 1, 22 and 77, respectively.

Lemma 5.6. *The codewords of weight 30 in $C_3(\overline{\mathrm{HiS}})$ span a subcode $\mathcal{L}$ of codimension 1. $\mathcal{L}$ is a $[100, 22, 30]_3$ code and its dual $\mathcal{L}^\perp$ is a $[100, 78, 8]_3$ code with 189200 codewords of weight 8. Moreover, $\mathcal{L}$ is the smallest and unique irreducible $\mathbb{F}_3$-module of its dimension invariant under* HS *and $\mathcal{L}^\perp = \langle 1 \rangle \oplus \mathcal{K}$ where $\mathcal{K} \cong C_3(\overline{\mathrm{HiS}})^\perp$.* $\mathrm{Aut}(\mathcal{L}) \cong \mathrm{HS{:}2}$ *and $C_3(\overline{\mathrm{HiS}}) \oplus C_3(\overline{\mathrm{HiS}})^\perp = \langle 1 \rangle \oplus \mathcal{L} \oplus \mathcal{K} = \mathbb{F}_3^{100}$.*

Proof. The first statement of the proposition follows from the submodule structure of the permutation module $\mathbb{F}_3\Omega = \mathbb{F}_3{}^{100}$ given in Proposition 4.3(i) as

Table 7. Weight distribution of $\mathcal{L}$

i	A_i	i	A_i	i	A_i
0	1	57	297598400	74	843242400
30	2200	58	492881400	75	542372600
34	7700	59	663108600	76	343169750
40	30800	60	1015568400	77	228782400
42	2200	61	1206436000	78	160941400
43	70400	62	1624299600	79	82051200
44	513900	63	1871284800	80	39732000
46	616000	64	2339880400	81	9240000
48	3480400	65	2385134400	82	9363200
49	231000	66	2685767700	83	3511200
50	4154304	67	2515128000	85	308000
51	3850000	68	2727578700	86	528000
52	29198400	69	2292136000	87	123200
53	48048000	70	2200712800	88	231000
54	101085600	71	1650950400	90	246400
55	144267200	72	1476772000	92	8250
56	240702000	73	1095710000	100	904

$N_{23} = N_1 \oplus N_{22}$. Now, [15, Proposition 2.4] gives the unique decomposition of $\mathbb{F}_3^{100}$ into irreducible submodules of dimensions 1, 22 and 77 respectively, as the reduction modulo 3 of the ordinary characters of M_{22} of degrees 21 and 55 remain irreducible. In addition, we deduce from [12, Table 1] (see also [13]) that 22 is the smallest dimension for a non-trivial irreducible $\mathbb{F}_3$-module invariant under HS (see also Proposition 4.3, part (i) (uniqueness and minimality) and part (ii) (irreducibility)). Finally, Table 7 below gives the weight distribution of $\mathcal{L}$.

That the minimum distance of $\mathcal{L}^{\perp}$ coincides with the known recorded distance for the given parameters follows from [10] and also from computations with Magma [2]. □

Below we compute the stabilizers of some vectors of small weight in $\mathcal{L}$ (say of weight ≤ 49, as required in [17, Exercise 1.3.7 (d)]) and determine their structure.

5.3. **7-Ary codes of the adjacency matrix of the $\overline{\mathrm{HiS}}$-graph.** Results similar to those discussed in the preceding sections for modules and codes can be obtained for $p = 7$ in relation with the graph $\overline{\mathrm{HiS}}$. The submodule structure of $\mathbb{F}_7\Omega$ is displayed in Table 10

Table 8. 1-designs $\mathcal{D}_{w_l}$ from HS:2

l	$\mathcal{D}_{w_l}$	No. of blocks	Primitivity
30	1-$(100, 30, 330)$	1100	Yes
34	1-$(100, 34, 1309)$	3850	Yes
40	1-$(100, 40, 6160)$	15400	Yes
42	1-$(100, 42, 462)$	1100	Yes
43	1-$(100, 43, 15136)$	35200	Yes
$(44)_1$	1-$(100, 44, 58080)$	132000	No
$(44)_2$	1-$(100, 44, 25410)$	57750	No
$(44)_3$	1-$(100, 44, 29568)$	67200	No
46	1-$(100, 46, 141680)$	308000	No
$(48)_1$	1-$(100, 48, 147840)$	308000	No
$(48)_2$	1-$(100, 48, 354816)$	739200	No
$(48)_2$	1-$(100, 48, 354816)$	739200	No
$(48)_3$	1-$(100, 48, 332640)$	693000	No
49	1-$(100, 49, 56595)$	115500	No

Table 9. Stabilizer in HS:2 of a word w_l

i	$(\mathrm{HS{:}2})_{w_i}$	Maximality	i	$(\mathrm{HS{:}2})_{w_i}$	Maximality
30	$S_8 \times 2$	Yes	$(44)_3$	$2{:}L_2(11)$	No
34	$2^5 \cdot S_6$	Yes	46	$2^5{:}3^2$	No
40	$2 \times A_6 \cdot 2^2 \cdot 2$	Yes	$(48)_1$	$2^5{:}3^2$	No
42	$L_3(4){:}2^2$	Yes	$(48)_2$	S_5	No
43	$A_6{:}2{:}2$	No	$(48)_3$	2^8	No
$(44)_1$	$2 \times L_2(7){:}2$	Yes	49	$2^8{:}3$	No
$(44)_2$	$2^9 \cdot 3$	No			

Table 10. Upper triangular part of the incidence matrix of the poset of submodules of $\mathbb{F}_7\Omega = \mathbb{F}_7{}^{100\times 1}$

dim	0	1	22	23	77	78	99	100
0	1	1	1	1	1	1	1	1
1	.	1	.	1	.	1	.	1
22	.	.	1	1	.	.	1	1
23	.	.	.	1	.	.	.	1
77	.	.	.	.	1	1	1	1
78	.	.	.	.	.	1	.	1
99	.	.	.	.	.	.	1	1
100	.	.	.	.	.	.	.	1

Proposition 5.7. *The code* $C_7(\overline{\mathrm{HiS}})$ *is a* $[100, 77, 8]_7$ *code and* $C_7(\overline{\mathrm{HiS}})^\perp$ *is a* $[100, 23, 23]_7$ *with* 600 *words of weight 23. Moreover* $\mathbf{1} \in C_7(\overline{\mathrm{HiS}})$, $C_7(\overline{\mathrm{HiS}}) \oplus$

TABLE 11. Upper triangular part of the incidence matrix of the poset of submodules of $\mathbb{F}_{11}\Omega = \mathbb{F}_{11}{}^{100\times 1}$

dim	0	1	22	23	77	78	99	100
0	1	1	1	1	1	1	1	1
1	.	1	.	1	.	1	.	1
22	.	.	1	1	.	.	1	1
23	.	.	.	1	.	.	.	1
77	.	.	.	.	1	1	1	1
78	.	.	.	.	.	1	.	1
99	.	.	.	.	.	.	1	1
100	.	.	.	.	.	.	.	1

$C_7(\overline{\mathrm{HiS}})^{\perp} = \mathbb{F}_7^{100}$ and $\mathrm{Aut}(\overline{\mathrm{HiS}}) = \mathrm{Aut}(C_7(\overline{\mathrm{HiS}})) \cong \mathrm{HS{:}2}$. Further, $C_7(\overline{\mathrm{HiS}})$ is the unique $\mathbb{F}_7$-module on which HS and HS:2 act faithfully and irreducibly.

Proof. The dimension 77 of $C_7(\overline{\mathrm{HiS}})$ follows from Lemma 4.5, since $\mathrm{rank}_7(\overline{A}) = 77$. The rest of the proof follows using [15, Proposition 2.4(ii)]. The minimum weight 23 of $C_7(\overline{\mathrm{HiS}})^{\perp}$ was determined by computations with Magma [2]. □

Lemma 5.8. *The codewords of weight 30 in $C_7(\overline{\mathrm{HiS}})^{\perp}$ span a subcode $\mathcal{R}$ of co-dimension 1. $\mathcal{R}$ is a $[100, 22, 30]_7$ code with 6600 codewords of weight 30 and its dual $\mathcal{R}^{\perp}$ is a $[100, 78, 8]_7$ code. Moreover, $\mathcal{R}$ is the smallest and unique irreducible $\mathbb{F}_7$-module invariant under HS and $\mathcal{R}^{\perp} = \langle 1\rangle \oplus \mathcal{S}$ where $\mathcal{S} \cong C_7(\overline{\mathrm{HiS}})$. $\mathrm{Aut}(\mathcal{S}) \cong \mathrm{HS{:}2}$ and $C_7(\overline{\mathrm{HiS}}) \oplus C_7(\overline{\mathrm{HiS}})^{\perp} = \langle 1\rangle \oplus \mathcal{R} \oplus \mathcal{S} = \mathbb{F}_7^{100}$.*

Proof. The proof follows similar arguments to those used in proving Lemma 5.6. So we omit the details. □

Remark 5.9. Up to this point, we dealt with the 3- and 7-modular representations of the Higman-Sims group of degree 100 in relation with the complementary graph $\overline{\mathrm{HiS}}$ of the Higman-Sims graph. In addition, we showed that the permutation module of the Higman-Sims group of dimension 100 over the fields $\mathbb{F}_p$ where $p = 3, 7$ is the direct sum of three absolutely irreducible modules of dimensions 1, 22 and 77 respectively. The next results show that the latter also holds for $\mathbb{F}_{11}$, i.e., the permutation module of the Higman-Sims group of dimension 100 over the field $\mathbb{F}_{11}$ is the direct sum of three absolutely irreducible modules of dimensions 1, 22 and 77 respectively.

5.4. **11-Ary codes from the 100-dimensional modular representation.**

The submodule structure of $\mathbb{F}_{11}\Omega$ is displayed in Table 11.

The reader would have noticed that the assertions of the next results do not follow from either graphs in discussion, since by Lemma 4.1 and Lemma 4.5 we have $\mathrm{rank}_{11}(A) = \mathrm{rank}_{11}(\overline{A}) = 99$, and thus the codes are trivial. The assertions in the next results follow directly from the structure of the module decomposition of the permutation module of dimension 100 over $\mathbb{F}_{11}$ as depicted in Table 11. Below, we describe the submodule $\mathbb{F}_{11}\Omega$ in relation with coding theory.

Proposition 5.10. *For $\mathbb{F} = \mathbb{F}_{11}$, the following occurs:*

(i)
$$\{N_i \,|\, i \in \{0,\ 1,\ 22,\ 23,\ 77,\ 78,\ 99,\ 100\}\}$$
is the complete set of $\mathbb{F}G$-submodules of $\mathbb{F}\Omega$ and $\dim N_i = i$ for all i.

(ii) *We have $0 = N_0 < N_1 < N_{78} < N_{100} = \mathbb{F}\Omega$ is a composition series of $\mathbb{F}\Omega$ as an $\mathbb{F}G$-module. The dimensions of the composition factors in the composition series are $1, 77, 22$. All composition factors are absolutely irreducible.*

(iii) ${N_i}^{\perp} = N_{100-i}$ *for all i.*

Proof. In this case the result holds, with the proof virtually the same as that of [15, Proposition 2.6]. Thus we omit the details. □

Results similar to those discussed in the preceding sections on the strongly regular graphs can be obtained for modules and codes for $p = 11$. We state below those results concerned with coding theory and give an outline of the proofs; leaving the full details to the reader.

Proposition 5.11. *N_{77} is a $[100, 77, 8]_{11}$ code, and ${N_{77}}^{\perp}$ is a $[100, 23, 23]_{11}$ code. Moreover $\mathbf{1} \in N_{77}$, $N_{77} \oplus {N_{77}}^{\perp} = \mathbb{F}_{11}^{100}$ and $\mathrm{Aut}(N_{77}) \cong$ HS:2. Further, N_{77} is the unique $\mathbb{F}_{11}$-module on which* HS *and* HS:2 *act faithfully and irreducibly.*

Proof. The dimension 77 of N_{77} follows from the decomposition of the permutation module of dimension 100, as depicted in Table 11. By [15, Proposition 2.4 (i)] it follows that $N_{77} \oplus {N_{77}}^{\perp} = \mathbb{F}_{11}^{100}$ and also that N_{77} is the unique $\mathbb{F}_{11}$-module on which HS and HS:2 act faithfully and irreducibly. □

Lemma 5.12. *The codewords of weight 30 in ${N_{77}}^{\perp}$ span a subcode $\mathcal{U}$ of co-dimension 1. $\mathcal{U}$ is a $[100, 22, 30]_{11}$ code, and its dual $\mathcal{U}^{\perp}$ is a $[100, 78, 8]_{11}$ code. Moreover, $\mathcal{U}$ is the smallest and unique irreducible $\mathbb{F}_{11}$-module invariant under* HS *and $\mathcal{U}^{\perp} = \langle 1 \rangle \oplus \mathcal{V}$ where $\mathcal{V} \cong N_{77}$.* $\mathrm{Aut}(\mathcal{V}) \cong$ HS:2 *and $N_{77} \oplus {N_{77}}^{\perp} = \langle 1 \rangle \oplus \mathcal{U} \oplus \mathcal{V} = \mathbb{F}_{11}^{100}$.*

Proof. Similar arguments to those used in the proof of Lemma 5.6 could be used in conjunction with [12, Table 1] for the irreducibility of $\mathcal{U}$ and the minimality of its dimension as a submodule invariant under HS. □

6. Concluding remarks

In this paper, we showed that the permutation module of the Higman-Sims group of dimension 100 over the fields $\mathbb{F}_p$ where $p = 3, 7, 11$ is the direct sum of three absolutely irreducible codes of dimensions 1, 22 and 77 respectively. Observe that the dimensions of these modules are precisely the sizes of the suborbits of the rank-3 representation of the Higman-Sims group of degree 100 on the cosets of the Mathieu group M_{22}. It is an interesting question to investigate whether there are groups G other than the simple sporadic group HS for which a permutation module of a given degree defined over $\mathbb{F}_p$ where $p \,|\, |G|$, on the cosets of a maximal subgroup is the direct sum of irreducible submodules whose dimensions are precisely the lengths of the suborbits of the orbit decomposition. The author is aware of only two other finite groups with this property, namely the simple unitary group $U_4(2)$ and the sporadic Hall-Janko group J_2 in their rank-3 representations of degrees 36 and 100, respectively. It would be interesting to attempt a classification of such groups, and establish the extent of this class of groups. In addition we have shown that the dual codes $C_p(\overline{\mathrm{HiS}})^{\perp} = [100, 77, 8]_p$ for $p = 3, 7, 11$ are irreducible optimal codes.

Acknowledgements

This work is based on the research supported by the National Research Foundation of South Africa (Grant Numbers 87470 and 91495). The author would like to thank Paul Hafner for bringing to his attention the existence of an unpublished version of the paper [15], and Wolfgang Knapp for sharing the earlier version and subsequent updates.

References

[1] E.F. Assmus Jr. and J.D. Key, Designs and Their Codes, Cambridge Tracts in Math. 103, Cambridge Univ. Press, Cambridge, 1992. (Second printing with corrections, 1993).

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

[3] A.E. Brouwer and C.J. van Eijl, On the p-rank of the adjacency matrices of strongly regular graphs, *J. Algebraic Combin.* **1** (1992) 329–346.

[4] A.E. Brouwer and W.H. Haemers, Spectra of Graphs, Springer-Verlag, New York, 2012.

[5] P.J. Cameron, Permutation Groups, London Math. Soc. Stud. Texts 45, Cambridge Univ. Press, Cambridge, 1999.

[6] P.J. Cameron and J.H. van Lint, Designs, Graphs, Codes and Their Links, London Math. Soc. Stud. Texts 22, Cambridge Univ. Press, Cambridge, 1991.

[7] C. Carlet and S. Guilley, Complementary dual codes for counter-measures to side-channel attacks, *Adv. Math. Commun.* **10** (2016), no. 1, 131–150

[8] T. Connor and D. Leemans, An atlas of subgroup lattices of finite almost simple groups, 2014, http://homepages.ulb.ac.be/~tconnor/atlaslat/hsd2.pdf, Accessed on July 2015.

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

[10] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, Online available at http://www.codetables.de, 2007, Accessed on 25–03–2016.

[11] P.R. Hafner, On the graphs of Hoffman-Singleton and Higman-Sims, *Electron. J. Combin.* **11** (2004), no. 1, Paper 77, 33 pages.

[12] C. Jansen, The minimal degrees of faithful representations of the sporadic simple groups and their covering groups, *LMS J. Comput. Math.* **8** (2005) 122–144.

[13] C. Jansen, K. Lux, R. Parker and R. Wilson, An Atlas of Brauer Characters, Appendix 2 by T. Breuer and S. Norton, London Math. Soc. Monogr. Ser. 11, The Clarendon Press, Oxford Univ. Press, New York, 1995,

[14] M. Klin, C. Rücker, G. Rücker and G. Tinhofer, Algebraic combinatorics in mathematical chemistry. Methods and algorithms. I. Permutation groups and coherent (cellular) algebras, *MATCH Commun. Math. Comput. Chem.* **40** (1999) 7–138.

[15] W. Knapp and H.-J. Schaeffer, On the codes related to the Higman-Sims graph, *Electron. J. Combin.* **22** (2015), no. 1, Paper 1.19, 58 pages.

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

[17] K. Lux and H. Pahlings, Representations of Groups: A Computational Approach, Cambridge Univ. Press, Cambridge, 2010.

[18] S.S. Magliveras, The Subgroup Structure of the Higman-Sims Simple group, *Bull. Amer. Math. Soc.* **77** (1971), no. 4, 535–539.

[19] J. Massey, Linear codes with complementary duals, *Disc. Math.* **106/107** (1992) 337–342.

[20] The Modular Atlas Homepage, Character tables of endomorphism rings of multiplicity-free permutation modules, http://www.math.rwth-aachen.de/ mfer/data/HS/HS $\cdot 2_1$.pdf

[21] J. Moori and B.G. Rodrigues, Some self-orthogonal codes related to Higman's geometry, *Electron. J. Combin.* **23** (2016), no.4, Paper 4.15, 12 pages.

[22] C.E. Praeger and L.H. Soicher, Low rank representations and graphs for sporadic groups, Aust. Math. Soc. Lect. Ser. 8, Cambridge Univ. Press, Cambridge, 1997.

[23] N. Sendrier, Linear codes with complementary duals meet the Gilbert-Varshamov bound, *Discrete Math.* **285** (2004) 345–347.

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

[25] R.A. Wilson, The Finite Simple Groups, Grad. Texts in Math. 251, Springer-Verlag, London, 2009.

(Bernardo Gabriel Rodrigues) School of Mathematics, Statistics and Computer Science, University of KwaZulu-Natal, Durban 4000, South Africa.

E-mail address: rodrigues@ukzn.ac.za