On the Codes Related to the Higman-Sims Graph

Wolfgang Knapp
Mathematisches Institut
Universität Tübingen, Germany
wolfgang.knapp@uni-tuebingen.de

Hans-Jörg Schaeffer
Mathematisches Institut
Universität Tübingen, Germany
hjs@hjschaeffer.de

Submitted: Apr 10, 2014; Accepted: Jan 10, 2015; Published: Jan 27, 2015
Mathematics Subject Classifications: 94B25 94B27 20B25 20D08 05C25

Abstract

All linear codes of length 100 over a field F which admit the Higman-Sims simple group HS in its rank 3 representation are determined. By group representation theory it is proved that they can all be understood as submodules of the permutation module $F\Omega$ where Ω denotes the vertex set of the Higman-Sims graph. This module is semisimple if $\mathrm{char}F \neq 2, 5$ and absolutely indecomposable otherwise. Also if $\mathrm{char}F \in \{2, 5\}$ the submodule lattice is determined explicitly. The binary case $F = \mathbb{F}_2$ is studied in detail under coding theoretic aspects. The HS-orbits in the subcodes of dimension $\leqslant 23$ are computed explicitly and so also the weight enumerators are obtained. The weight enumerators of the dual codes are determined by MacWilliams transformation. Two fundamental methods are used: Let v be the endomorphism determined by an adjacency matrix. Then in $H_{22} = \mathrm{Im}\, v$ the HS-orbits are determined as v-images of HS-orbits of certain low weight vectors in $F\Omega$ which carry some special graph configurations. The second method consists in using the fact that H_{23}/H_{21} is a Klein four group under addition, if H_{23} denotes the code generated by H_{22} and a "Higman vector" $x(m)$ of weight 50 associated to a heptad m in the shortened Golay code G_{22}, and H_{21} denotes the doubly even subcode of $H_{22} \leqslant H_{78} = {H_{22}}^{\perp}$. Using the mentioned observation about H_{23}/H_{21} and the results on the HS-orbits in H_{23} a model of G. Higman's geometry is constructed, which leads to a direct geometric proof that G. Higman's simple group is isomorphic to HS. Finally, it is shown that almost all maximal subgroups of the Higman-Sims group can be understood as stabilizers in HS of code words in H_{23}.

Keywords: Higman-Sims simple group, rank 3 representation, graph, linear code, Hamming weight, Higman's geometry

Introduction

In [20] a systematic program to determine all codes admitting a prescribed permutation group G has been proposed. Hitherto in many cases good codes have been obtained from doubly-transitive permutation groups. In this paper the program of [20] is carried out for $G = \mathrm{HS}$, the simple group of Higman-Sims in its rank 3 permutation representation of degree 100. It turns out that any code over a field F admitting G can be obtained as a submodule of the permutation module $F\Omega$ over F, considering Ω as the ambient basis.

The binary codes are of particular interest. There is exactly one G-invariant subcode H_{23} of dimension 23 over $\mathbb{F}_2$ which may be viewed as an amalgamation of 100 copies of the (shortened) binary Golay code of length 22. Let v be the endomorphism determined by an adjacency matrix and let $H_{22} = \operatorname{Im} v$. Then $H_{22} \leqslant H_{78} = {H_{22}}^{\perp}$. Let H_{21} denote the doubly even subcode of H_{22}. Then $H_{22} \leqslant H_{23}$ and H_{23}/H_{21} is a Klein four group under addition. The G-orbits on the weight classes of the codes of dimension at most 23 (which are all contained in H_{23}) are determined by elementary algebraic and combinatorial arguments. The two G-invariant subcodes H'_{22} and H''_{22} of dimension 22 containing H_{21} and different from H_{22} are related to the G-orbits on the set of "Higman vectors" $x(m)$ of weight 50 associated to heptads m in the shortened Golay code G_{22}. Two fundamental methods are used: the G-orbits in H_{22} are determined as v-images of G-orbits of certain low weight vectors in $F\Omega$ which carry some special graph configurations. The second method consists in using the mentioned fact that H_{23}/H_{21} is a Klein four group under addition. Also the natural action of the automorphism group $\overline{G}$ on H_{23}/H_{21} is considered. Now, using also MacWilliams transformation, the weight enumerators for all non-trivial G-invariant binary subcodes are computed; some of them have rather good error correction capacity.

It turns out that the weight structure of H_{23} is highly relevant for the combinatorial properties of the Higman-Sims graph. The structure of the subcodes of H_{23} allows also the construction of a model of G. Higman's geometry [17] admitting an action of $G = \mathrm{HS}$. Thereby an isomorphism of HS and G. Higman's simple group is obtained. H_{23} may also be used to describe a large part of the subgroup structure of HS in a similar way as it has been done for the Mathieu group M_{24} and the (extended) binary Golay code of length 24 by Conway and Curtis. One can check that the parameters of several HS-invariant binary codes meet the Gilbert-Varšamov bound, see also [5].

The methods developed in this paper are not restricted to the case of the Higman-Sims simple group. In particular, one may obtain codes of length $77, 56, 50$ and 16 from rank 3 groups corresponding to strongly regular subgraphs of the Higman-Sims graph. Note that N. Loebich has shown in [21] that $\mathcal{G}_{100}$ contains every known strongly regular graph having a vertex transitive group of automorphisms and no triangles as a subgraph.

Remark

This paper is based on talks of the first author in a research seminar in 1980 at the university of Tübingen and was completed essentially in 1982, in the time before TEX or LATEX were available to the authors and before the Group ATLAS [1] and the Atlas of Brauer Characters [2] appeared. Due to its considerable length it could not be published at that time. Now, many years later, the first author found the time to rewrite the paper in LATEX, so also making an electronic version available. Only a few changes of the original text were made, in particular some more recent references (e.g. to the ATLASes and to GAP) were added. It is clear that nowadays many of the results can be obtained easily just by computing using computer algebra systems like GAP (with packages GRAPE and GUAVA) or Sage. Note that in the present work only the MacWilliams transformations of several code enumerators were carried out by computer; all other results are obtained by arguments and computation by hand. It should be acknowledged that also some more recent research publications have some overlap with this paper, in particular V.D. Tonchev's paper [37]. Moreover, the code H_{22} represents a particular instance of more recent general investigations, e.g. by Brouwer and Eijl [4] and Haemers, Peeters and van Ruckevorsel [12].

We thank the referees for some valuable suggestions.

1 Background and preliminary results

In this paper sets and groups are assumed finite, unless specified otherwise. If Ω is a set, then $\mathcal{P}(\Omega)$ denotes the set of all subsets of Ω; Sym_Ω and Alt_Ω denote the alternating and symmetric group of the set Ω, A_n and Σ_n the alternating and symmetric group on n letters. If A and B are groups then $A \,\mathrm{wr}\, B$ denotes the regular wreath product of order $|B|^{|A|}|A|$. $A \overset{k}{\curlywedge} B$ denotes a subdirect product of A and B where a factor group of order k is identified. M_{24-i} and M_{12-i} denote the Mathieu groups of degree $24-i$ resp. $12-i$. E_{p^f} denotes an elementary abelian group of order p^f.

Actions of a group G onto a set Ω are right actions denoted by $(\alpha, g) \mapsto \alpha g$. If G acts on Ω we write (G, Ω) for this action and - following a suggestion of H.Wielandt - we denote the set of G-orbits on Ω by $\Omega : G$. If $H \leqslant G$ then $G : H = \{Hx \mid x \in G\}$ and $G : (H, H) = \{HxH \mid x \in G\}$.

$\mathbb{F}_q$ denotes a finite field of order q. Modules are always assumed to be finitely generated. If R is a commutative ring with 1 and M a free R-module then $\mathrm{rk}_R M$ denotes the R-rank of M. If F is a field and G a group then FG denotes the group algebra of G over F. If U is an FG-module then U^* denotes the dual FG-module. $U =_{FG} X \oplus Y$ denotes a direct decomposition of the FG-module U into FG-submodules X and Y. $J(A)$ denotes the Jacobson radical of an algebra A.

All other general notations are standard.

We shall need an elementary result concerning module reductions whose idea of proof is taken from Thompson [36, Theorem 1].

(1.1) Proposition.
Let R be a principal ideal domain, K its field of fractions, P a maximal ideal of R and $k = R/P$ its residue class field. Let G be a finite group and V an RG-lattice (i.e. a finitely generated R-free RG-module). Suppose $K \otimes_R V =_{KG} X \oplus Y$ is a direct sum of KG-submodules where $\dim_K X = s$. Then the following hold:

(1) $W = V \cap X$ is an RG-submodule and a pure R-submodule of X.

(2) $\mathrm{rk}_R V/W = \dim_K Y = \mathrm{rk}_R V - s$.

(3) *$k \otimes_R W$ is a kG-submodule of $k \otimes_R V$ of dimension s.*

Proof. Clearly W and V are RG-submodules of $K \otimes_R V$. Since $V/W \cong (V+X)/X$ is isomorphic to an RG-submodule of Y we see that V/W is torsion free, hence W is a pure submodule of V. Let $t = \mathrm{rk}_R V$. Then, of course, $\mathrm{rk}_R V/W = \dim_K Y = t - a$. By the theorem of elementary divisors there exists an R-basis $(b_i)_{1\leqslant i\leqslant t}$ of V and $(a_i)_{1\leqslant i\leqslant t} \in R^t$ such that $a_i \mid a_{i+1}$ for $1 \leqslant i \leqslant t-1$ and $(a_i b_i)_{1\leqslant i\leqslant t}$ is an R-basis of W. The fact that W is a pure submodule entails that we may choose $a_i = 1$ for $1 \leqslant i \leqslant t-s$ and $a_i = 0$ for $t-s+1 \leqslant i \leqslant t$. Now it is obvious that $k \otimes_R W$ is an s-dimensional subspace of $k \otimes_R V$. $\square$

Proposition (1.1) is applied in this paper in the case $R = \mathbb{Z}, K = \mathbb{Q}, P = p\mathbb{Z}, k = \mathbb{F}_p$ and $V = \mathbb{Z}\Omega$, the integral permutation module of a group G acting (transitively) on a set Ω. In this case $\mathbb{Q} \otimes_{\mathbb{Z}} V = \mathbb{Q}\Omega$ and $\mathbb{F}_p \otimes_{\mathbb{Z}} V = \mathbb{F}_p\Omega$ are viewed in the obvious way as the permutation modules over $\mathbb{Q}$ resp. $\mathbb{F}_p$ defined by the same action of G on Ω.

(1.2) Lemma.
Let G be a group and let V be an FG-module over a finite field F with dual module V^*. Let u_1V and u_1V^* denote the set of all 1-dimensional subspaces of V and V^*, respectively. Then the following hold:

(1) *$|u_1V^* : G| = |u_1V : G|$,*

(2) *If $F = \mathbb{F}_2$ then $|V^* : G| = |V : G|$.*

Proof. Obviously, (2) is a consequence of (1). The natural G-invariant pairing $\phi : V \times V^* \to F : (x, y) \mapsto xy$ may be used to show that $(u_1V, u_1V^*, \{(Fx, Fy) \mid xy = 0\})$ is a projective space (with the hyperplanes in the rôle of blocks) admitting G as a group of automorphisms. Brauer's Lemma ([3, p.933 f]) or the theorem of Dembowski-Hughes-Parker ([9, p.81]) shows that G has on u_1V and on u_1V^* the same permutation character, so (1) easily follows. $\square$

We shall use the following concepts from coding theory.

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

Let $B = (e_i)$ and let $x = \sum x_i e_i$ for any $x \in V$.

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

(ii) V is a commutative and associative F-algebra with respect to the coordinatewise multiplication $(x, y) \mapsto \sum (x_i y_i) e_i$.

(iii) V carries the norm $w_B : x \mapsto w(x) = w_B(x) := \sum |x_i|$ where $|\cdot|$ denotes the trivial absolute value of F. $w(x) = w_B(x)$ is called the (Hamming) *weight* of x. Let $\operatorname{supp}(x) = \operatorname{supp}_B(x) = \{e_i \mid x_i \neq 0\}$ denote the support of x with respect to B. Then, of course, $w(x) = |\operatorname{supp}(x)|$. To the norm w_B there corresponds canonically the *Hamming metric* d_B defined by $d_B(x, y) := w_B(x - y)$.

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

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

If C is a code of length n, the $(n + 1)$-tuple $(|W_i(C)|)_{0 \leqslant i \leqslant n}$ is called the weight distribution of C, and the homogeneous polynomial $\sum |W_i(C)| \xi^i \eta^{n-i} \in \mathbb{C}[\xi, \eta]$ of degree n is called the weight enumerator of C. The weight enumerators of a code C and of its "dual" $C^\perp$ determine each other via the MacWilliams identities, see e.g. [16].

A morphism $(V, B, C) \to (V', B', C')$ of codes over F is by definition an injective F-linear map $\mu : V \to V'$ with $C\mu \subseteq C'$ sending any $e \in B$ to a scalar multiple of some $e' \in B'$. The codes C and C' are isomorphic if μ is bijective and $C\mu = C'$.

$\mathrm{ML}(C)$ denotes the group of all (code) automorphisms from (V, B, C) to itself, the *monomial linear group* of C. ($\mathrm{ML}(C)$ can be represented by monomial matrices, with respect to the ambient basis B.) Let $B = (e_i)_{i \in \Omega}$. Every $\mu \in \mathrm{ML}(C)$ determines a permutation $\bar{\mu}$ of Ω by $e_i\mu \in \langle e_{\bar{\mu}} \rangle = Fe_{\bar{\mu}}$. The map $\mu \mapsto \bar{\mu}$ is an epimorphism of $\mathrm{ML}(C)$ onto a subgroup $P\mathrm{ML}(C)$ of the symmetric group Sym_Ω. We call $\mathrm{PML}(C)$ the *permutation group* of C. The code C is said to admit a permutation group G acting on Ω if G is a subgroup of $\mathrm{PML}(C)$. The elements of $\ker(\mu \mapsto \bar{\mu})$ form the group $\mathrm{DL}(C)$ of diagonal automorphisms of C.

In the following we fix a $3-(22, 6, 1)$-design $\mathcal{W}_{22} = (P_{22}, B_{22}, I_{22})$. It is a result of Witt [39, 40] that such a design exists and is unique up to isomorphism. $\mathcal{W}_{22}$ may be viewed as an extension of the projective plane $\mathrm{PG}(2, 4) = (P_{21}, B_{21}, I_{21})$ where $P_{22} = P_{21} \cup \{\infty\}$ and B_{22} is the union of $B'_{21} = \{\{\infty\} \cup g \mid g \in B_{21}\}$ and an orbit $\mathcal{H}_1$ of $\mathrm{PSL}(3, 4)$ on the set of hyperovals of $\mathrm{PG}(2, 4)$, see [15]. The full group of automorphisms is the automorphism group $\mathrm{Aut}(M_{22}) = \overline{M_{22}}$ of the Mathieu simple group M_{22} of order $443, 520$ where $|\overline{M_{22}} : M_{22}| = 2$. The permutation group M_{22} acting on P_{22} is a transitive extension of $M_{21} = \mathrm{PSL}(3, 4)$.

The (shortened) binary Golay code of length 22 may be described in terms of $\mathcal{W}_{22}$ as follows, see also [20, 5.3]. Let $V = \mathbb{F}_2 P_{22}$ be the $\mathbb{F}_2$-vector space with basis P_{22}. Then (V, P_{22}) is a Hamming space. Let G_{11} be the subspace of V generated by all characteristic functions of blocks of $\mathcal{W}_{22}$, i.e. $G_{11} = \langle b^\bullet \mid b \in B_{22} \rangle$ where $b^\bullet = \sum\{\delta(b, x)x \mid x \in P_{22}\}$ and $\delta(b, x) = 0$ if $x \not{\mathrm{I}}_{22} b$, $\delta(b, x) = 1$ if $x \mathrm{I}_{22} b$.

It is easily seen that G_{11} is a $(22, 11)$-code which is self-dual, i.e. $G_{11}^{\perp} = G_{11}$. Moreover $G_{11} = \langle \mathbb{1}_{22} \rangle \oplus G_{10}$ where $\mathbb{1}_{22} = \sum P_{22}$ and $G_{10} = \langle b^{\bullet} + c^{\bullet} \mid \{b, c\} \subseteq B_{22} \rangle = \langle \mathbb{1}_{22} + b^{\bullet} \mid b \in B_{22} \rangle$.

Let $G_{12} = G_{10}^{\perp}$. Then G_{12} is called the (shortened) Golay code of length 22. Of course, G_{12} is a $(22, 12)$-code containig G_{11}. There are two more codes G'_{11} and G''_{11} properly between G_{10} and G_{12}. The following assertions about the binary Golay code of length 22 are well known and easy to prove.

(1.3) Proposition.
G_{12} and its subcodes have the following properties.

(1) $\mathrm{ML}(G_{12}) = \mathrm{ML}(G_{11}) = \mathrm{ML}(G_{10}) = \overline{M_{22}}$.

(2) $\mathrm{ML}(G'_{11}) = \mathrm{ML}(G''_{11}) = M_{22}$, *and* $\overline{M_{22}}$ *interchanges* G'_{11} *and* G''_{11}. $(G'_{11})^{\perp} = G''_{11}$.

(3) M_{22} *acts (as a linear group) irreducibly on* G_{10} *and trivially on* G_{12}/G_{10}.

(4) The weight distributions of the codes are as follows:

i	$\lvert W_i(G_{10})\rvert$	$\lvert W_i(G_{11})\rvert$	$\lvert W_i(G'_{11})\rvert$	$\lvert W_i(G_{12})\rvert$
0	1	1	1	1
6	$-$	77	$-$	77
7	$-$	$-$	176	352
8	330	330	330	330
10	$-$	616	$-$	616
11	$-$	$-$	672	$1,344$
12	616	616	616	616
14	$-$	330	$-$	330
15	$-$	$-$	176	352
16	77	77	77	77
22	$-$	1	$-$	1

In the table only occurring weights i are displayed; $-$ is printed in place of 0.

Note that $|W_i(G'_{11})| = |W_i(G''_{11})|$, *since* G'_{11} *and* G''_{11} *are conjugate under* $\overline{M_{22}}$.

Moreover,

$$G_{11} = \{x \in G_{12} \mid w(x) \equiv 0 \pmod 2\},$$
$$G_{10} = \{x \in G_{12} \mid w(x) \equiv 0 \pmod 4\}.$$

(5) M_{22} *acts transitively on each nonempty* $W_i(G_{12}), i \neq 7, 11, 15$.

$W_i(G_{12}), i \in \{7, 11, 15\}$, *splits into two* M_{22}*-orbits* $W_i(G'_{11})$ *and* $W_i(G''_{11})$ *which are fused under* $\overline{M_{22}}$.

$\overline{M_{22}}$ *acts transitively on every nonempty* $W_i(G_{12})$.

(6) Let $x \in W_i(G_{12}), 0 \neq i \neq 22$. Then the stabilizer subgroup $(M_{22})_x$ is a maximal subgroup of M_{22} having the following structure:

i	structure of $(M_{22})_x$
6 / 16	$E_{16}A_6$
7 / 15	A_7
8 / 14	$E_8\mathrm{GL}(3,2)$
10 / 12	M_{10}
11	$\mathrm{PSL}(2,11)$

In each case $(M_{22})_x$ acts transitively on $\mathrm{supp}(x)$*. There are exactly two conjugacy classes in M_{22} of such stabilizers for $i \in \{7, 11, 15\}$ which are fused under* $\mathrm{Aut}(M_{22}) \cong \overline{M_{22}}$.

Remark. Of course, $(M_{22})_x = (M_{22})_{x+\mathbb{1}_{22}}$. There is exactly one more conjugacy class of maximal subgroups of M_{22}, namely the stabilizers in M_{22} of 2-subsets of P_{22}. These maximal subgroups, of index 231, are isomorphic to $E_{16}\Sigma_5$, see [7, Table 3].

It will be convenient to identify the vectors of $\mathbb{F}_2P_{22}$ with their supports in P_{22}. So $\mathbb{F}_2P_{22}$ may be viewed as the (power) set $\mathcal{P}(P_{22})$ of all subsets of P_{22}. We recall the following notions.

(1.4) Definition.
The elements of $W_i(G_{12})$, resp. their supports, are called *hexads* ($i = 6$), *heptads* ($i = 7$), *octads* ($i = 8$), *decads* ($i = 10$), *endecads* ($i = 11$) and *dodecads* ($i = 12$) of $\mathcal{W}_{22}$.

The hexads of the definition are the blocks of $\mathcal{W}_{22}$. For later use we set $\mathcal{M}' = W_7(G'_{11})$ and $\mathcal{M}'' = W_7(G''_{11})$. Then $\mathcal{M}'$ and $\mathcal{M}''$ are the orbits of M_{22} in the set of heptads of $\mathcal{W}_{22}$.

We shall need some more detailed properties of G_{12}. A subset T of P_{22} is called *independent* if there is no hexad of $\mathcal{W}_{22}$ incident with every element of T, otherwise *dependent*. Furthermore, we introduce the block graph $\mathcal{G}_{77} = (B_{22}, \Delta_{77})$ by taking the 77 blocks of $\mathcal{W}_{22}$ as vertices, joining two vertices by an edge in Δ_{77} if and only if they are disjoint. ($\mathcal{G}_{77}$ is a strongly regular graph of valency 16, having $\overline{M_{22}}$ in its action on the blocks of $\mathcal{W}_{22}$ as its group of automorphisms.)

(1.5) Lemma.
Let B be a set of at most 5 blocks of $\mathcal{W}_{22}$ such that $\sum\{b^\bullet \mid b \in B\} = \mathbb{1}_{22}$. Then $|B| = 5$ and exactly one of the following holds:

(i) There exists a 2-subset $T = \{x, y\}$ of P_{22} such that B is the set of all blocks incident with x and y. $\mathcal{G}_{77}$ induces on B the null graph.

(ii) There exists an independent 4-subset T of P_{22} such that B is the union of the set B_0 of all blocks defined by the 4 triangles in T and the unique block b_1 disjoint from $\bigcup\{b \mid b \in B_0\}$. $\mathcal{G}_{77}$ induces on B a 4-claw.

(iii) *There exist two disjoint* 2*-subsets* $T_1 = \{x_1, y_1\}$ *and* $T_2 = \{x_2, y_2\}$ *such that* $T_1 \cup T_2$ *is dependent and* B *consists of the unique block* b_0 *determined by* $T_1 \cup T_2$ *and of four blocks* b_1, b_2, b_3, b_4 *such that* b_1 *intersects* b_2 *in* T_1*,* b_3 *intersects* b_4 *in* T_2 *and* $b_1 \cup b_2$ *is disjoint from* $b_3 \cup b_4$*.* $\mathcal{G}_{77}$ *induces on* B *a quadrangle and an isolated point.*

Moreover, any block configuration B *described above has the property* $\sum\{b^\bullet \mid b \in B\} = \mathbb{1}_{22}$*.*

Proof. Assume $|B| \leqslant 4$. Then $|B| = 4$ since $3 \cdot 6 = 18 < 22$. Let $B = \{b_0, b_1, b_2, b_3\}$. The b_i are not pairwise disjoint. Without loss of generality we may suppose that b_1,b_2 and b_3 intersect in the point ∞ which implies that b_1,b_2 and b_3 correspond to lines of $\mathrm{PG}(2, 4)$ and b_0 corresponds to a hyperoval which immediately leads to a contradiction. Therefore we have $|B| = 5$.

Let $M_i = \{x \mid x \in P_{22}$ and x is incident with exactly i elements of $B\}$ for $0 \leqslant i \leqslant 5$. We have the partition $P_{22} = M_1 \uplus M_3 \uplus M_5$.

If $|M_5| \geqslant 2$ then $|M_5| = 2$ and (i) holds. $|M_5| = 1$ is impossible, as is seen by considering the projective plane $(\mathcal{W}_{22})_x$ where $M_5 = \{x\}$.

If $M_5 = \emptyset$ then we have $M_3 \neq \emptyset$ since the blocks of B cannot be pairwise disjoint. We may assume without loss of generality that $\infty \in M_3$. Let $B = \{b_0, b_1, b_2, b_3, b_4\}$ such that ∞ is incident with $\{b_0, b_1, b_2\}$. Then b_0, b_1, b_2 may be viewed as lines and b_3, b_4 as hyperovals in $\mathrm{PG}(2, 4)$. If b_0, b_1, b_2 are confluent lines then it easily follows that (iii) holds. If b_0, b_1, b_2 are not confluent it follows that (ii) holds. Note that in both cases $|M_3| = 4$ holds.

It is immediate that all configurations B of types (i), (ii), (iii) have the required property $\sum\{b^\bullet \mid b \in B\} = \mathbb{1}_{22}$. □

(1.6) Lemma.
Let C *be a set of blocks of* $\mathcal{W}_{22}$ *such that* $|C| = 4$ *and* $\sum\{b^\bullet \mid b \in C\} = 0$*. Set* $M_i = \{x \mid x \in P_{22}$ *and* x *is incident with exactly* i *elements of* $C\}$*,* $m_i = |M_i|$ *for* $0 \leqslant i \leqslant 4$*. Then* $m_0 = 10$ *and* $m_2 = 12$*.*

Proof. Of course $m_0 + m_2 + m_4 = 22$. It is easy to derive a contradiction if $m_4 \neq 0$. Therefore $m_4 = 0$ and we may assume without loss that $\infty \in M_2$. In this case C consists of 2 lines and 2 hyperovals and the assertion is easily verified. (Note that C cannot contain two disjoint blocks.) □

(1.7) Lemma.
Let C *be a set of blocks of* $\mathcal{W}_{22}$ *such that* $|C| = 6$ *and* $\sum\{b^\bullet \mid b \in C\} = 0$*. Set* $M_i = \{x \mid x \in P_{22}$ *and* x *is incident with exactly* i *elements of* $C\}$*,* $m_i = |M_i|$ *for* $0 \leqslant i \leqslant 6$*.*

Then exactly one of the following holds:

(i) *Two elements of* C *are disjoint.*

(ii) $m_6 \neq 0$*.*

(iii) $m_0 = 7, m_2 = 12$ *and* $m_4 = 3$*.*

Proof. Suppose that $m_6 = 0$ and that no two elements of C are disjoint. Let $b \in C$. The remaining 5 blocks in C intersect b in exactly 2 points. Counting incidences yields that b contains exactly 2 elements of M_4 and 4 elements of M_2. Now it easily follows that $m_4 = |M_4| = (6 \cdot 2)/4 = 3$ and $m_2 = (6 \cdot 4)/2 = 12$. So (iii) holds. $\square$

Note that examples for the cases (ii) and (iii) in (1.7) easily can be constructed. In case (ii) C is formed by a dual hyperoval in the projective plane $\mathrm{PG}(2,4)$ if $\infty \in M_6$.

(1.8) Lemma.
Let C be a set of blocks of $\mathcal{W}_{22}$ such that $|C| = 7$ and $\sum\{b^\bullet \mid b \in C\} = \mathbb{1}_{22}$. Set $M_i = \{x \mid x \in P_{22}$ and x is incident with exactly i elements of $C\}$, $m_i = |M_i|$ for $0 \leqslant i \leqslant 7$. Then either $m_5 + m_7 > 0$ or $m_1 = 12$ and $m_3 = 10$.

Proof. Suppose $m_5 + m_7 = 0$. Then $m_1 + m_3 = 22$, and by counting incidences we obtain $42 = 7 \cdot 6 = m_1 + 3m_3$. It follows $m_1 = 12$ and $m_3 = 10$. $\square$

(1.9) Proposition. *(1) The heptads of $\mathcal{W}_{22}$ are exactly the hyperblocks in the sense of Lüneburg [22, p.98].*

(2) Recall that $V = \mathbb{F}_2 P_{22}$. Let $y \in W_7(V)$. Then the following assertions are equivalent:

(a) y is a heptad.

(b) $\langle y, b^\bullet \rangle = 1$ for all $b \in B_{22}$.

(c) $|\mathrm{supp}(y) \cap b| \in \{1,3\}$ for all $b \in B_{22}$.

(3) Let y, z be heptads of $\mathcal{W}_{22}$. Then the following assertions are equivalent:

(a) y and z belong to the same M_{22}-orbit.

(b) $\langle y, z \rangle = 1$.

(c) $|\mathrm{supp}(y) \cap \mathrm{supp}(z)| \in \{1,3,7\}$.

(4) Let y, z be heptads of $\mathcal{W}_{22}$. Then the following assertions are equivalent:

(a) y and z belong to distinct M_{22}-orbits.

(b) $\langle y, z \rangle = 0$.

(c) $|\mathrm{supp}(y) \cap \mathrm{supp}(z)| \in \{0,2,4\}$.

Proof. (2), (3) and (4) immediately follow from (1.3). (1) is then obvious. $\square$

For any $x \in V = \mathbb{F}_2 P_{22}$ set $B_i(x) = \{b \in B_{22} \mid |\mathrm{supp}(x) \cap \mathrm{supp}(b)| = i\}$, $0 \leqslant i \leqslant 6$.

(1.10) Lemma.
Let y be a heptad of $\mathcal{W}_{22}$. Then the following hold.

(1) $B_{22} = B_1(y) \uplus B_3(y)$, $|B_1(y)| = 42$ and $|B_3(y)| = 35$.

(2) $(M_{22})_y \cong A_7$ has the orbits $B_1(y)$ and $B_3(y)$ in B_{22}.

Proof. The assertion follows from (1.3) and (1.9), see also [22, 14.12]. □

(1.11) Lemma.
Let y be a heptad of $\mathcal{W}_{22}$, $y \in \mathcal{M}'$, say. For $0 \leqslant i \leqslant 7$ let $D_i(y) = \{z | z$ a heptad such that $|\mathrm{supp}(y) \cap \mathrm{supp}(z)| = i\}$. Then the following hold:

(1) If $D_i(y) \neq \emptyset$ then $(M_{22})_y \cong A_7$ acts transitively on $D_i(y)$.

(2) $\mathcal{M}' = D_1(y) \uplus D_3(y) \uplus D_7(y)$ and $\mathcal{M}'' = D_0(y) \uplus D_2(y) \uplus D_4(y)$.

(3) The cardinalities of $D_i(y)$ are given in the following table:

i	0	1	2	3	4	7
$\lvert D_i(y)\rvert$	15	70	126	105	35	1

Proof. (3) may be obtained from the Leech triangle [7, p.226]. It is clear from the definition that the sets $D_i(y)$ are $(M_{22})_y$-invariant. Inspection of the character table of M_{22} and Frobenius reciprocity then yield (1) and (2). □

We also need a result on endecads of $\mathcal{W}_{22}$.

(1.12) Lemma.
Let e be an endecad of $\mathcal{W}_{22}$, $\overline{e} = e + \mathbb{1}_{22}$ its complement. Then the following hold.

(1) $|B_1(e)| = |B_5(e)| = 11$ and $|B_3(e)| = 55$.

(2) $B_{22} = B_1(e) \uplus B_3(e) \uplus B_5(e)$.

(3) $B_3(e) = B_3(\overline{e}), B_1(e) = B_5(\overline{e})$ and $B_5(e) = B_1(\overline{e})$.

(4) $(M_{22})_e \cong \mathrm{PSL}(2, 11)$ acts transitively on $\mathrm{supp}(e)$, $\mathrm{supp}(\overline{e})$ and any nonempty $B_i(e)$.

Proof. (1) and (2) may be obtained from (1.3). (3) is obvious from the definition of the $B_i(x)$. (4) is verified by inspection. (Note that $\mathrm{PSL}(2, 11)$ acts 3-homogeneously on 11 points; this forces $(M_{22})_e$ to act transitively on $B_3(e)$.) □

We use the original definition of the Higman-Sims graph and group [16, 22] as follows.
Let $\alpha \notin P_{22} \uplus B_{22}$ and set $\Omega = \{\alpha\} \uplus P_{22} \uplus B_{22}$.Then $|\Omega| = 1 + 22 + 77 = 100$. A graph $\mathcal{G}_{100} = (\Omega, E)$ with vertex set Ω is defined by

$$\begin{aligned} E &= \{\{\alpha, x\} \mid x \in P_{22}\} \\ &\uplus \{\{x, y\} \mid x \in P_{22}, y \in B_{22} \text{ and } (x, y) \in \mathrm{I}_{22}\} \\ &\uplus \{\{y, z\} \mid y, z \in B_{22} \text{ and } y \text{ disjoint from } z \text{ in } \mathcal{W}_{22}\}. \end{aligned}$$

It is easily shown that $\mathcal{G}_{100}$ is a strongly regular graph with valency $k = 22$ and intersection parameters $\lambda = 0, \mu = 6$ in D.G. Higman's sense [14]. $\mathcal{G}_{100}$ is called the *Higman-Sims graph.*

Let $\overline{G} = \mathrm{Aut}(\mathcal{G}_{100})$. Then $\overline{G}$ contains a simple normal subgroup $G = \mathrm{HS}$ of index 2, the *Higman-Sims simple group* of order $44,352,000 = 2^9 3^2 5^3 \cdot 7 \cdot 11$. $\overline{G}$ acts as a rank 3 permutation group primitively on Ω. Of course, $G_\alpha \cong M_{22}$ and $\overline{G}_\alpha \cong \overline{M_{22}}$. Moreover, $\overline{G} \cong \mathrm{Aut}(G)$.

We need some more detailed notation for the action of G (resp. $\overline{G}$) on Ω.

G and $\overline{G}$ have the orbits $\Delta_0, \Delta_1, \Delta_2$ in Ω^2 where

$$\begin{aligned}\Delta_0 &= \{(\xi,\xi) \mid \xi \in \Omega\} \text{ is the diagonal,}\\ \Delta_1 &= \{(\xi,\eta) \mid \{\xi,\eta\} \in E\} \text{ and}\\ \Delta_2 &= \{(\xi,\eta) \mid \xi,\eta \in \Omega, \xi \neq \eta \text{ and } \{\xi,\eta\} \notin E\}.\end{aligned}$$

We use the notation $\Delta_i(\xi) = \{\eta \mid (\xi,\eta) \in \Delta_i\}$ for the corresponding G_ξ-orbits. Of course, $|\Delta_i(\xi)| = 1, 22, 77$ respectively.
The matrix V_i in the centralizer algebra of (G, Ω) is defined by

$$V_i = (f_i(\xi,\eta))_{(\xi,\eta)\in\Omega^2}$$

where $f_i(\xi,\eta) = 1$ if $(\xi,\eta) \in \Delta_i$ and $f_i(\xi,\eta) = 0$ otherwise ($i = 0, 1, 2$).

V_i may be viewed as a matrix over any integral domain. If F is a field and $F\Omega$ denotes the permutation module of (G, Ω) over F, to each V_i there is naturally associated an endomorphism v_i with the property

$$\xi \mapsto \xi v_i = \sum f_i(\xi,\eta)\eta.$$

We use the convention $\Delta = \Delta_1$ and $v = v_1$ throughout the paper.

It is convenient to identify the $\mathbb{F}_2$ vector spaces $\mathcal{P}(\Omega)$ and $\mathbb{F}_2\Omega$ in the obvious way. We introduce special names for some interesting elements:

The elements $\Delta(\xi), \xi \in \Omega$, are called *adjacency vectors* of $\mathcal{G}_{100}$; arranged in a suitable way they form a (binary) adjacency matrix of $\mathcal{G}_{100}$.

$x \in \mathbb{F}_2\Omega$ is called a *β-hexad* for some $\beta \in \Omega$ if and only if there exists a $g \in G$ such that $\beta g = \alpha$ and xg is a hexad of $\mathcal{W}_{22}$ (viewed as a subset of P_{22}). In the same way *β-heptads*, *β-octads*, *β-decads*, *β-endecads* and *β-dodecads* are defined.

If m is an α-heptad then the vector $x(m) = \alpha + m + B_1(m) \in W_{50}(\mathbb{F}_2\Omega)$ is called a *Higman vector*, see (1.10). (The terminus "Higman vector" refers to G. Higman's geometry and will be justified in Section 4.)

Note that if x is a β-hexad and a γ-hexad then $\beta = \gamma$ or $\mathrm{supp}(x) = \Delta(\beta) \cap \Delta(\gamma)$; in the latter case $\{\beta, \gamma\}$ is uniquely determined by x. For β-heptads, β-octads, β-decads, β-endecads and β-dodecads y the vertex β is uniquely determined by y.

Let $U \leqslant \overline{G} = \mathrm{Aut}(\mathcal{G}_{100})$ and let $\Omega : U = \{\Phi_i \mid 0 \leqslant i \leqslant t-1\}$. Then the *matrix* of the Higman-Sims graph *with respect to* $(\Phi_i)_{0\leqslant i\leqslant t-1}$ (or less precisely *with respect to* U) is the matrix

$$A = (a_{ij}) \in \mathbb{Z}^{t\times t} \text{ where } a_{ij} = |\Delta(\xi) \cap \Phi_j| \text{ for } \xi \in \Phi_i.$$

Note that A is an adjacency matrix of $\mathcal{G}_{100}$ if $U = 1$ and the transpose of an intersection matrix of (Ω, G) in D.G. Higman's sense [14] if $U = G_\alpha$.

(1.13) Lemma.
Let m be an α-heptad. Then $G_{\alpha,m} = G_{\alpha+m} \cong A_7$ and the $G_{\alpha,m}$-orbits in Ω are

$$(\Psi_i)_{0\leqslant i\leqslant 4} = (\{\alpha\}, m, B_1(m), \Delta(\alpha) + m, B_3(m))$$

with orbit lengths

$$(|\Psi_i|)_{0\leqslant i\leqslant 4} = (1, 7, 42, 15, 35).$$

The matrix of the Higman-Sims graph with respect to (Ψ_i) is

$$A = \begin{bmatrix} 0 & 7 & 0 & 15 & 0 \\ 1 & 0 & 6 & 0 & 15 \\ 0 & 1 & 6 & 5 & 10 \\ 1 & 0 & 14 & 0 & 7 \\ 0 & 3 & 12 & 3 & 4 \end{bmatrix}.$$

Proof. The assertion follows from (1.10) or [22, 14.12]. □

(1.14) Proposition.
Let $\mathbb{F}_2B_{22}$ be the permutation module over $\mathbb{F}_2$ for M_{22} of dimension 77 given by the action on the blocks of $\mathcal{W}_{22}$, $\mathbb{1}_{77} = \sum B_{22}$. Then $\mathbb{F}_2B_{22} =_{\mathbb{F}_2M_{22}} \langle \mathbb{1}_{77}\rangle \oplus Y$ where $Y = \langle \mathbb{1}_{77}\rangle^\perp$ is an indecomposable $\mathbb{F}_2M_{22}$-module of dimension 76.

Proof. Since 77 is odd we have the decomposition $\mathbb{F}_2B_{22} = \langle \mathbb{1}_{77}\rangle \oplus Y$ where $Y = \langle \mathbb{1}_{77}\rangle^\perp$. Since M_{22} acts as a rank 3 permutation group on B_{22} we infer that either Y is indecomposable or $E = \mathrm{End}_{\mathbb{F}_2M_{22}}(\mathbb{F}_2B_{22})$ is semisimple. Now consider the intersection matrix of M_{22} acting on B_{22}

$$S = \begin{bmatrix} 0 & 1 & 0 \\ 16 & 0 & 4 \\ 0 & 15 & 12 \end{bmatrix}$$

(see [14] for example). It follows that E contains a proper nilpotent element. Hence E is not semisimple, therefore Y is indecomposable. □

(1.15) Corollary.
Let $\mathbb{F}_2\Omega$ be the permutation module over $\mathbb{F}_2$ for $G = \mathrm{HS}$ of dimension 100 given by the action on the vertices of $\mathcal{G}_{100}$, $\mathbb{1} = \sum \Omega$. Then $\langle \mathbb{1}\rangle^\perp/\langle \mathbb{1}\rangle =_{\mathbb{F}_2M_{22}} Y \oplus Z$ where Y and Z are indecomposable $\mathbb{F}_2M_{22}$-modules of dimension 76 and 22 respectively.

Proof. Restriction of coordinates shows that $\langle \mathbb{1}\rangle^\perp \cong \mathbb{F}_2P_{22} \oplus \mathbb{F}_2B_{22}$ as an $\mathbb{F}_2M_{22}$-module. From (1.3) it follows that $\mathbb{F}_2P_{22}$ is indecomposable of dimension 22. Now (1.14) and the isomorphism theorems for modules yield the assertion. □

In an appendix to this section for the convenience of the reader two distinct adjacency matrices of the Higman-Sims graph $\mathcal{G}_{100}$ are displayed. We thank an anonymous referee for pointing out that an adjacency matrix for $\mathcal{G}_{100}$ is provided also by the graph database of Sage [34]. An adjacency matrix of $\mathcal{G}_{100}$ can also easily be computed directly by GAP using the Package AtlasRep. But such a matrix still would have to be transformed by additional programs to one of the shapes in Figure 1 or Figure 2 which visualize a better understanding of the graph structure.

In Figure 1 an adjacency matrix in a "canonical" form according to the definition of $\mathcal{G}_{100}$ is given. Here Ω is ordered according to a particular rank 3 stabilizer series: α is taken first, then two Singer-cycle orbits separated by a fixed-point follow. In this ordering of Ω the adjacency matrix displays the well known fact that $\mathcal{G}_{100}$ contains strongly regular subgraphs with vertex number 77 and valency 16 (the graph $\mathcal{G}_{77}$ mentioned above) and with vertex number 56 and valency 10 (called the "Gewirtz graph").

Detached at the bottom of the matrix a Higman vector $x(m)$ in the same ordering of Ω is printed.

In Figure 2 the ordering of Ω is such that the support of the given Higman vector $x(m)$ is taken first. The ordering is chosen also such that $\mathcal{G}_{100}$ induces on $\mathrm{supp}(x(m))$ and on its complement the "same" strongly regular graph of valency 7 (called the "Hoffman-Singleton graph"). Figure 2 also obviously displays the $2 \cdot 50$ cocliques of size 15 of the Hoffman-Singleton graph in the sense of [6] where they are of fundamental importance for the code construction. These cocliques were also used by Hafner [13] in his alternative construction of the Higman-Sims graph from the Hoffman-Singleton graph which is used in Sage [34].

Note: For better reading in the figures the matrix entries " 0" are printed as "·" .

2 The codes of length 100 which admit G = HS

In this section all linear codes C of length 100 which admit G in the sense of [20] are determined.

Let E be a stem cover of G and E_α be the inverse image of the stabilizer G_α. Then by [20, 3.2], all linear codes over a field F admitting G as a permutation group are obtained by the following procedure:

Induce up to E all 1-dimensional FE_α-modules. The submodules of the resulting FE-modules provide for a complete list of codes admitting (G, Ω) as permutation group.

In our case $G = \mathrm{HS}$ there exists only one 1-dimensional FE_α-module, namely the trivial on F, which induces up to the permutation module. This result is stated in [29] without reference. Since it is relevant for our purpose, we indicate a proof.

(2.1) Lemma.
Let E be a stem cover of $G = \mathrm{HS}$ and let E_α be the inverse image of $G_\alpha \cong M_{22}$ under the canonical epimorphism $E \to G$. Then E_α is a stem extension of G_α.

(Note that $H_2(M_{22}) \cong Z_{12}$ by a theorem of Mazet [26].)

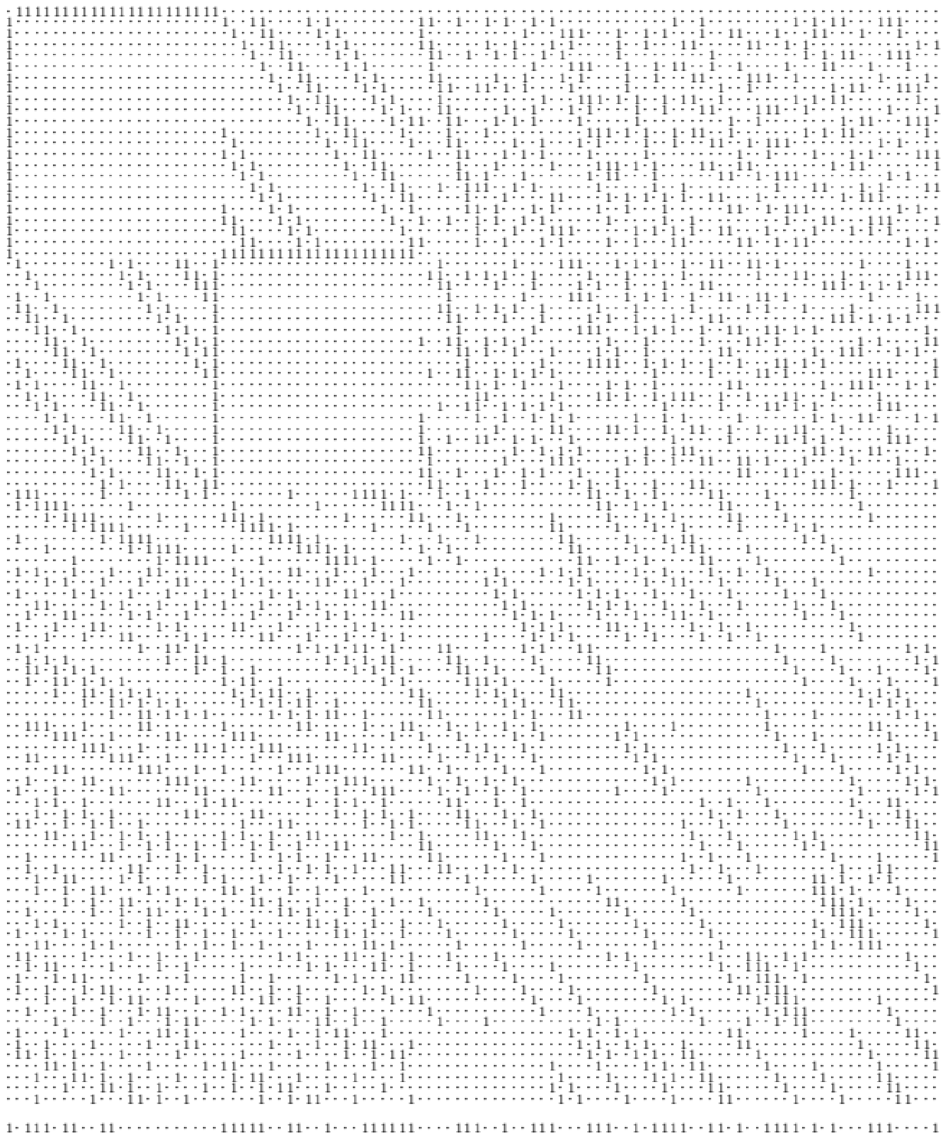


Figure 1: An adjacency matrix of the Higman-Sims graph and a Higman vector.

Proof. By [25] G has exactly two conjugacy classes of involutions, say 2_1 and 2_2. The involutions in 2_1 have exactly 20 fixed-points in Ω while the involutions in 2_2 act fixed-point freely on Ω. Thus any involution in 2_2 moves exactly $100 \equiv 4 \pmod 8$ points. Following Griess [11] we consider now the stem cover $\widehat{A}$ of $\mathrm{Alt}_\Omega \geqslant G$, and we conclude that the inverse image E of G under the canonical epimorphism $\widehat{A} \to \mathrm{Alt}_\Omega$ is a stem extension. By [27] E is the stem cover of G (uniquely determined up to isomorphism).

To be explicit, Griess' argument shows that any inverse image $\widehat{t}$ of an involution $t \in 2_2$

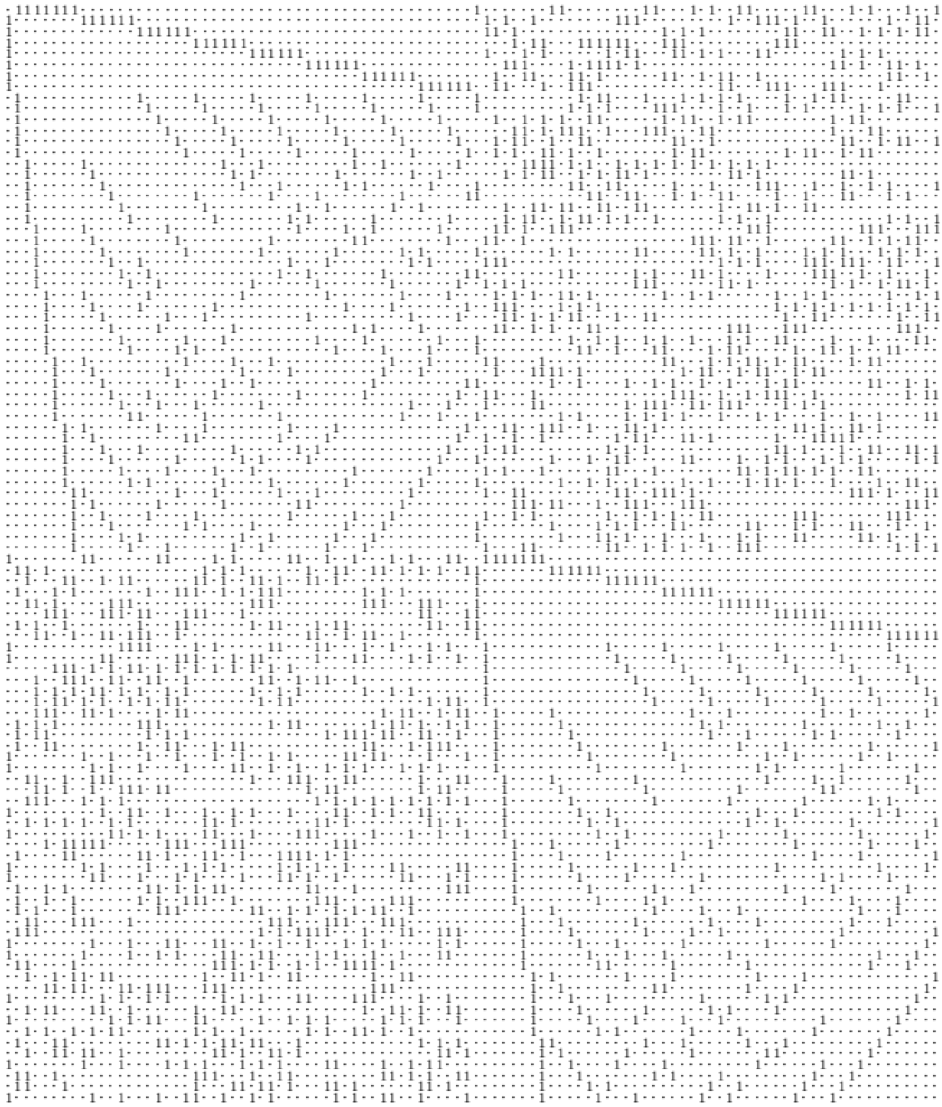


Figure 2: An adjacency matrix of the Higman-Sims graph displaying also the Hoffman-Singleton graph.

is an element of order 4 such that $\widehat{t}^2 = z$, where $\langle z \rangle = Z(A) = Z(E)$, see [18]. Now let $G_\alpha = M$ and let h be an α-hexad. By [25] the stabilizer H of h in G is a semidirect product of $H_1 \cong \Sigma_6$ by $N \cong Z_2^4$ such that $H_2 = H_1 \cap M \cong A_6$ acts irreducibly on N; of course, $NH_2 = H \cap M$ and $|H : H \cap M| = 2$. We claim that there exists an involution $t \in 2_2$ such that $H = (H \cap M)\langle t \rangle$. To see this fact we recall the following results of [25]:

Let S be a Sylow 2-subgroup of G containing a Sylow 2-subgroup S_2 of M. S contains an elementary abelian subgroup V of order 4 whose involutions all belong to 2_2. Since

$S_2 \cap V = 1$ we conclude that $S = S_2V$. S_2 is contained in a Sylow 2-subgroup S_1 of H, therefore $S_1 \cap V = \langle t \rangle$ for some involution $t \in 2_2$ and the claim is established.

We denote by $\widehat{}$ any inverse image under the canonical epimorphism $E \to G$. Since $\widehat{t}^2 = z$ we infer that $\widehat{H}$ is stem extension of H. It is fairly obvious that $\widehat{N}$ is elementary abelian (recall that $\widehat{N}/\langle z \rangle \cong Z_2^4$ is an irreducible module). Since $\widehat{H}$ is a stem extension, $\widehat{N}$ is an indecomposable $\widehat{H}/\widehat{N}$-module where $\widehat{H}/\widehat{N} \cong \mathrm{Sym}_6$. But then N is also an indecomposable $\widehat{H \cap M}/\widehat{N}$-module where $\widehat{H \cap M}/\widehat{N} \cong \mathrm{Alt}_6$, as one can see by restricting the natural permutation module over $\mathbb{F}_2$ from Σ_6 to A_6. Consequently we infer that $\widehat{H \cap M}$ is a stem extension of $H \cap M$ and so also $\widehat{M} = E_\alpha$ is a stem extension of G_α. $\square$

As a consequence of (2.1) and [20, (3.2)], every code admitting $G = \mathrm{HS}$ may be viewed as a submodule of the permutation module of (G, Ω). So the next step is to determine all such submodules. Clearly, we may consider first the case of characteristic 0 and then proceed by reduction modulo the prime characteristic p. In the modular case we first determine those submodules which are kernels or images of module endomorphisms; this type of submodules will be called *endo-submodules*. The complete lattice of submodules then is obtained from relations between endo-submodules, their perpendicular spaces and some extra considerations.

We recall from Section 1 the notations: Ω denotes the set of vertices of the Higman-Sims graph, the Higman-Sims simple group $G = \mathrm{HS}$ has the orbitals $\Delta_0, \Delta_1, \Delta_2$ where $|\Delta_i(\alpha)| = 1, 22, 77$ respectively. V_0, V_1, V_2 are the matrices in the centralizer algebra of (G, Ω) corresponding to the orbitals $\Delta_0, \Delta_1, \Delta_2$ and v_i denotes the endomorphism of the permutation module $F\Omega$ associated with the matrix V_i or the orbital Δ_i. As a general convention we write $\Delta = \Delta_1$ and $v = v_1$.

Clearly, the endomorphism algebra $E(F\Omega) := \mathrm{End}_{FG}(F\Omega)$ has basis (v_0, v_1, v_2) where $v_0 = \mathrm{id}_{F\Omega}$.

The right regular representation of $E(F\Omega)$ on itself defines a faithful matrix representation of $E(F\Omega)$ into $F^{3\times 3}$ by

$$a \mapsto (a_{ik}) \text{ where } v_i a = \sum a_{ik} v_k.$$

The matrices $S_j = ((v_j)_{ik})$ are the intersection matrices of the graphs (Ω, Δ_j) in the sense of D.G. Higman [14] if $\mathrm{char} F = 0$. The structure of the Higman-Sims graph gives the following values:

$$S_0 = \mathrm{I}_3, \qquad S_1 = \begin{bmatrix} 0 & 1 & 0 \\ 22 & 0 & 6 \\ 0 & 21 & 16 \end{bmatrix}, \qquad S_2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 21 & 16 \\ 77 & 56 & 60 \end{bmatrix}.$$

(In abuse of notation m also denotes the element $m \cdot 1$ in the field F for any integer m.)

S_1 has eigenvalues $22, -8, 2$ and S_2 has eigenvalues $77, 7, -3$. By construction, $E(F\Omega)$ is isomorphic to the algebra A generated by S_0, S_1 (and S_2). Therefore we get the following.

(2.2) Proposition.
Suppose F is a field of characteristic 0. Then the following hold:

(1) $F\Omega =_{FG} C \oplus X \oplus Y$ is the unique decomposition of $F\Omega$ into irreducible FG-submodules, where $\dim C = 1$, $\dim X = 22$ and $\dim Y = 77$.

(2) The eigenvalues of the v_i are distributed as follows:

	v_0	v_1	v_2
C	1	22	77
X	1	-8	7
Y	1	2	-3

(3) The projections in $E(F\Omega)$ onto the irreducible submodules C, X, Y are given by

$$\pi_C = \frac{1}{100}(v_0 + v_1 + v_2), \pi_X = \frac{1}{100}(22v_0 - 8v_1 + 2v_2), \pi_Y = \frac{1}{100}(77v_0 + 7v_1 - 3v_2).$$

Furthermore we have

$$C = \mathrm{Im}(v_0 + v_1 + v_2), X = \mathrm{Im}(11v_0 - 4v_1 + v_2), Y = \mathrm{Im}(77v_0 + 7v_1 - 3v_2).$$

Proof. The algebra A is generated by S_1 (or S_2); A is commutative, semisimple and 3-dimensional over F. The same holds for $E(F\Omega) \cong A$. Since $F\Omega$ is a completely reducible FG-module and since v_1 has 3 distinct eigenvalues, the permutation module $F\Omega$ decomposes into a sum of 3 absolutely irreducible submodules C, X and Y. We choose the notation so that C is the eigenspace of v_1 belonging to the eigenvalue 22 and that X is the eigenspace of v_1 belonging to the eigenvalue -8. $j = v_0 + v_1 + v_2$ is the endomorphism with matrix $J = V_0 + V_1 + V_2$ whose entries are all 1. Hence we may conclude that the eigenvalues of the v_i are distributed as claimed in (2). Obviously $\dim C = 1$ holds. Let $x = \dim X$ and $y = \dim Y$. Then we have $0 = \operatorname{trace} v_1 = 22 - 8x + 2y$ and $2,200 = \operatorname{trace} v_1^2 = 484 + 64x + 4y$, since V_1 is symmetric (see [38, 28.10]). It follows that $x = 22$ and $y = 77$ as asserted in (1). From (2) it now may be deduced that the projection idempotents in $E(F\Omega)$ onto the irreducible submodules are those given in (3). The rest follows. ☐

The submodule structure of $F\Omega$ is completely clear by the results of (2.2) if $\mathrm{char}F = 0$. If $\mathrm{char}F$ does not divide $|G| = 44,352,000 = 2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$ then we have the same situation. Note that in all these cases the irreducible submodules are unique and absolutely irreducible over the prime field.

For notation of characters and Brauer characters we use the following conventions:

If χ denotes a (Brauer) character of $G = \mathrm{HS}$ then χ_m denotes the restriction of χ to $G_\alpha \cong M_{22}$. If there is no ambiguity characters (of any group) are denoted by their degrees.

(2.3) Lemma.
Let 100 be the permutation character of $G = \mathrm{HS}$ acting on Ω and let 1, 22 and 77 denote

the characters belonging to the modules C, X and Y respectively. Then the following holds:

$$\begin{array}{rrcl} (i) & 22_m & = & 1+21. \\ (ii) & 77_m & = & 1+21+55. \\ (iii) & 100_m & = & 3\cdot 1+2\cdot 21+55. \end{array}$$

Proof. The assertion follows from the well known suborbit structure of $G = \mathrm{HS}$ and of M_{22} acting on the points and blocks of $\mathcal{W}_{22}$, see Section 1. □

(2.4) Proposition.
If F is a field of prime characteristic $p \neq 2,5$ then all assertions of (2.2) hold (with scalars read modulo p).

Proof. It suffices to consider the case $F = \mathbb{F}_p$ for $p \in \{3,7,11\}$. Since p does not divide 100 the reductions modulo p of the projections π_C, π_X and π_Y are distinct pairwise orthogonal idempotents. So it follows that $F\Omega$ is the direct sum of the reductions modulo p $\overline{C}$, $\overline{X}$ and $\overline{Y}$ of C, X and Y. It is now sufficient to show that $\overline{C}$, $\overline{X}$ and $\overline{Y}$ are absolutely irreducible. This is trivial for $\overline{C}$. Of course, we have $\dim \overline{X} = 22$ and $\dim \overline{Y} = 77$.

(i) If $p = 11$ then X and Y both belong to blocks of defect 0. We immediately conclude that X and Y are absolutely irreducible.

(ii) Let $p = 7$. Then Y belongs to a block of defect 0, and again $\overline{Y}$ must be absolutely irreducible. Let β denote the Brauer character of $\overline{X}$. Then by James' [19, 5.1], we have $\beta_m = 1+21$. Again it follows that $\overline{X}$ is absolutely irreducible, since $\overline{C}$ contains the fixed-points of G in $F\Omega$.

(iii) Let $p = 3$. By James' [19, 7.3], the characters 21 and 55 of M_{22} remain irreducible when reduced modulo 3. Hence we may conclude from (2.2) that $\overline{X}$ and $\overline{Y}$ are again absolutely irreducible, using the obvious fact that $\overline{X}$ and $\overline{Y}$ are self-dual modules.

□

It remains to consider the case that $\mathrm{char}F$ divides 100. At first we consider the direct decomposition of $F\Omega$.

(2.5) Proposition.
If $\mathrm{char}\, F = p \in \{2,5\}$ *then the following hold:*

(1) $F\Omega$ is absolutely indecomposable.

(2) $E(F\Omega)$ is a local F-algebra such that $\dim E(F\Omega)/J(E(F\Omega)) = 1$.

(3) If $p = 5$ then $J(E(F\Omega))$ has F-basis (w, w^2) where $w = 2v_0 - v_1$. If $p = 2$ then $J(E(F\Omega))$ has F-basis $(v_1, v_0 + v_1 + v_2)$.

Proof. (1) and (2) follow from (3). (3) may be established by direct computation. □

(2.6) Proposition.
Let $\operatorname{char} F = 5$ *and set* $w = 2v_0 - v_1 \in E(F\Omega)$. *Let* $H_{100} = F\Omega$, $H_0 = 0$, $H_{99} = \operatorname{Ker} w^2$, $H_1 = \operatorname{Im} w^2$, $H_{77} = \operatorname{Ker} w$, $H_{23} = \operatorname{Im} w$, $H_{78} = H_{77} + H_{23}$ *and* $H_{22} = H_{77} \cap H_{23}$. *Then the following hold.*

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

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

(3) $H_i^\perp = H_{100-i}$ *for all* i.

Proof. From James' [19, 4.3], it follows that the characters 1, 21 and 55 of $G_\alpha \cong M_{22}$ remain irreducible when reduced modulo 5. Therefore we conclude from (2.2) that in a composition series of $F\Omega$ viewed as an FG-module we have exactly 3 (trivial) composition factors of dimension 1, 2 composition factors of dimension 21 and 1 composition factor of dimension 55.

From (2.5) it follows that the FG-submodules H_i of $F\Omega$ defined above are pairwise distinct and that $H_1 \leqslant H_{22}$ and $H_{78} \leqslant H_{99}$. It follows that $0 = H_0 < H_1 < H_{22} < H_k < H_{78} < H_{99} < H_{100} = F\Omega$, where $k \in \{23, 77\}$ are two composition series of $F\Omega$ as an FG-module. hence (2) holds.

The matrices in the centralizer algebra of $F\Omega$ which is spanned by V_0, V_1 and V_2 are all symmetric. Therefore $\operatorname{Ker} a = (\operatorname{Im} a)^\perp$ for any $a \in E(F\Omega)$. Referring to the definition of the H_i we see that (3) holds.

Using (3), from $\dim E(F\Omega) = 3$ it follows that H_{23} and H_{100}/H_{77} are uniserial. We claim that also H_{77} (and therefore $H_{100}/H_{23} \cong H_{77}^*$) is uniserial.

First of all, from (2.5) it follows that H_{77} is indecomposable. For the claim it is sufficient to prove that also H_{77}/H_1 is indecomposable. Otherwise there would be an FG-submodule Y of H_{77} such that $H_{77} = Y + H_{22}$ and $Y \cap H_{22} = H_1$. For $M = G_\alpha$ we have the double module decomposition

$$G : (M, M) = \{M, MxM, MyM\}$$

for some $x, y, \in G$, notation so that $|\{zM \mid zM \subseteq MxM\}| = 22$. The FM-Module Y/H_1 is irreducible in a block of defect 0, hence Y/H_1 is a projective FM-module. It follows that there must exist an irreducible FM-submodule X of dimension 55 such that $Y = X \oplus H_1$. But then $Y_0 = \bigcap\{Xxg \mid g \in M\}$ would be a proper FM-submodule of Y of codimension at most 22 and so it would follow that $X = Y_0$, therefore in particular $X = Xx$. Since $G = \langle M, x\rangle$, Xwould be an FG-submodule, contradicting the indecomposability of H_{77}.

Now let U be any FG-submodule of $F\Omega$. We have to show that U is one of the H_i:

By taking orthogonal subspaces, if necessary, we may suppose $\dim U \leqslant 50$ because of (3). Since $F\Omega/H_{23}$ has a unique minimal irreducible submodule of dimension 55, it follows $U \leqslant H_{23}$. But then $U = H_i$ for some i, hence (1) holds. □

The only remaining case is now $\operatorname{char} F = 2$. Of course, this is the most interesting case in view of possible applications. It turns out that it is also highly relevant for the combinatorial properties of the Higman-Sims graph and for the structure of $G = \mathrm{HS}$. We set again $\mathbb{1} = \sum \Omega \in F\Omega$.

(2.7) Proposition.
If $F = \mathbb{F}_2$ the following hold:

(1) $F\Omega$ has precisely the following endo-submodules H_i with $\dim H_i = i$:

$$H_{100} = F\Omega, \quad H_0 = 0, \quad H_{99} = \operatorname{Ker}(v_0 + v_1 + v_2),$$
$$H_1 = \operatorname{Im}(v_0 + v_1 + v_2), \quad H_{78} = \operatorname{Ker} v_1, \quad H_{22} = \operatorname{Im} v_1.$$

These submodules form a series $H_0 < H_1 < H_{22} < H_{78} < H_{99} < H_{100}$.

(2) For every $a \in E(F\Omega)$ we have $\operatorname{Ker} a = (\operatorname{Im} a)^\perp$, thus $H_i^\perp = H_{100-i}$ for the endo-submodules H_i.

(3) $H_{21} = \{x \mid x \in H_{22}$ and $w(x) \equiv 0 \pmod 4\}$ is an FG-submodule of codimension 1 in H_{22}.

Set $H_{79} = {H_{21}}^\perp$. Then $\dim H_i = i$ for $i \in \{21, 79\}$ and $0 = H_0 < H_1 < H_{21} < H_{22} < H_{78} < H_{79} < H_{99} < H_{100} = F\Omega$ is a composition series of $F\Omega$ as an FG-module. The dimensions of the composition factors in this composition series are $1, 20, 1, 56, 1, 20, 1$. All composition factors of $F\Omega$ are absolutely irreducible.

(4) $F\Omega$ has exactly one FG-submodule H_{23} of dimension 23. Set $H_{77} = {H_{23}}^\perp$; then also $\dim H_{77} = 77$. We have $H_{22} < H_{23} < H_{79}$ and $H_{21} < H_{77} < H_{78}$.

Between H_{21} and H_{23} there are exactly 3 distinct FG-submodules H_{22}, H'_{22} and H''_{22}. Set $H'_{78} = (H'_{22})^\perp$ and $H'_{78} = (H''_{22})^\perp$. Then $\dim H'_i = i = \dim H''_i$ for $i \in \{22, 78\}$ and H_{78}, H'_{78} and H''_{78} are the only FG-submodules between H_{77} and H_{79}. We have $H'_{22} < H'_{78}$ and $H''_{22} < H''_{78}$.

(5) $\{H_0, H_1, H_{21}, H_{22}, H'_{22}, H''_{22}, H_{23}, H_{77}, H_{78}, H'_{78}, H''_{78}, H_{79}, H_{99}, H_{100}\}$ is the complete set of FG-submodules of $F\Omega$.

(6) H_{22} is generated by all adjacency vectors $\Delta(\beta)$ of the Higman-Sims graph; H_{78} is generated by all β-hexads, $\beta \in \Omega$.

(7) H_{21} (respectively H_{77}) is the set of all sums of an even number of adjacency vectors of the Higman-Sims graph (respectively of β-hexads).

(8) $H_{79} \setminus H_{78} = \{x \mid x \in F\Omega$ and $(x, \Delta(\beta)) = 1$ for all $\beta \in \Omega\}$,

$$H_{23} \setminus H_{22} = \{x \mid x \in F\Omega \text{ and } (x, h) = 1 \text{ for all } \beta\text{-hexads } h, \beta \in \Omega\}.$$

(9) *For any heptad m of $\mathcal{W}_{22}$ in the sense of (1.4) let $x(m) = \alpha + m + B_1(m)$ be the corresponding Higman vector. Let $\mathcal{M}'$ and $\mathcal{M}''$ be the two orbits of $G_\alpha \cong M_{22}$ on the set of heptads in $\mathcal{W}_{22}$ (see Section 1). Then, with appropriate notation, we have*

$$H'_{22} = H_{21} + Fx(m) \text{ for any } m \in \mathcal{M}' \text{ and } H''_{22} = H_{21} + Fx(m) \text{ for any } m \in \mathcal{M}''.$$

(10) $H_{21} = \{x \mid x \in H_{23} \text{ and } w(x) \equiv 0 \pmod 4\}$.

(11) *The action of G on $F\Omega$ extends in a natural way to $\overline{G} \cong \mathrm{Aut}(G)$. Every H_i is invariant under $\overline{G}$, but $\overline{G}$ interchanges the submodules H'_{22}, H''_{22} and H'_{78}, H''_{78}.*

In the case of arbitrary fields $F \supseteq \mathbb{F}_2$ we have essentially the same situation, since $F\Omega \cong F\otimes_{\mathbb{F}_2}\mathbb{F}_2\Omega$ and almost all completely reducible factors are multiplicity-free. Only the factors H_{23}/H_{21} and H_{79}/H_{77} yield a number of submodules increasing with the size of the field F.

Remark. Because of the last statement of the Proposition, and since all composition factors of $\mathbb{F}_2\Omega$ as an $\mathbb{F}_2G$-module are absolutely irreducible, we restrict our attention in characteristic 2 to the case $F = \mathbb{F}_2$. It does not seem promising to consider larger fields F for code theoretic applications.

Proof.

(i) From (2.5) it follows that $R = J(E(F\Omega)) = \{0, v_1, v_0 + v_2, v_0 + v_1 + v_2\}$. It is immediate that $R^2 = 0$. We also see that the submodules H_i defined in (1) are endo-submodules and that for all $a \in E(F\Omega)$ $\operatorname{Ker} a = (\operatorname{Im} a)^\perp$, since the matrix belonging to a is symmetric. From $R^2 = 0$ we infer that $0 = H_0 \leqslant H_1, H_{22} \leqslant H_{78}, H_{99} \leqslant H_{100} = F\Omega$. To establish that there are no other endo-submodules it suffices to show that $\operatorname{Im}(v_0 + v_2) = \operatorname{Im} v_1 = H_{22}$. Clearly $H_1 = F\mathbb{1}$ holds. Since V_1 and $V0 + V_2$ are complementary $0,1$-matrices, we have $\operatorname{Im}(v_0 + v_2) + H_1 = \operatorname{Im} v_1 + H_1$. So it is sufficient to show that $H_1 \leqslant \operatorname{Im} v_1 = H_{22}$. If $H_1 \not\leqslant H_{22}$ then $U = H_{22} \cap \operatorname{Im}(v_0 + v_2) \cong U^*$ would be the image of an endomorphism $u \in R$, which is impossible. Therefore we have $\operatorname{Im}(v_0 + v_2) = H_{22}$ as claimed. It also follows that we have a series $0 = H_0 < H_1 < H_{22} < H_{78} < H_{99} < H_{100} = F\Omega$ of FG-submodules. Of course, $\dim H_0 = 0, \dim H_1 = 1, \dim H_{99} = 99$ and $\dim H_{100} = 100$. We assert that $\dim H_{22} = 22$ and $\dim H_{78} = 78$. From (2.2)(3) it follows that H_{22} is the reduction modulo 2 of $X \cap \mathbb{Z}\Omega$, hence $\dim H_{22} \leqslant \dim X = 22$. From (1.3) it follows that the matrix V_1 of v_1 which is the adjacency matrix of the Higman-Sims graph over $F = \mathbb{F}_2$ has rank at least 22. Therefore we have $\dim H_{22} = 22$ and $\dim H_{78} = 78$. (1) and (2) of the proposition are now proved completely.

(ii) Since $H_{22} \leqslant {H_{22}}^\perp = H_{78} \leqslant H_{99} = \{x \mid x \in F\Omega \text{ and } w(x) \equiv 0 \pmod 2\}$, we get that

$$H_{21} = \{x \mid x \in H_{22} \text{ and } w(x) \equiv 0 \pmod 4\}$$

is an FG-submodule of dimension 21, contained in H_{22}. Set $H_{79} = {H_{21}}^\perp$. Of course, then $\dim H_{79} = \dim {H_{21}}^\perp = 100 - 21 = 79$ holds. The series of FG-submodules of

$F\Omega$ $0 = H_0 < H_1 < H_{21} < H_{22} < H_{78} < H_{79} < H_{99} < H_{100} = F\Omega$ has successive factors of dimensions $1, 20, 1, 56, 1, 20, 1$ respectively. According to J. Thackray [35] (see also the atlas of Brauer Characters [2]) all these factor modules are absolutely irreducible. (For the factors of dimension 1 and 20 this is quite elementary; for the factor of dimension 56 a direct elementary proof should also be possible. Note that we can use Lemma (2.3).) The proof of (3) is now complete.

(iii) From (2) and (1) it follows that the FG-modules H_{100}/H_{78} and H_{22} are self-dual and uniserial. Proposition (1.1) gives that the reduction modulo 2 of $(X + C) \cap \mathbb{Z}\Omega$ is a 23-dimensional submodule H_{23} of $F\Omega$. H_{23} contains H_{22} which is the reduction of $X \cap \mathbb{Z}\Omega$. Set $H_{77} = {H_{23}}^{\perp}$. Of course, we then have $\dim H_{23} = 23$ and $\dim H_{77} = 77$. Since $H_{23} \cap H_{78} = H_{22}$ we obtain from the structure of H_{100}/H_{78} that $H_{79} = H_{78} + H_{23}$ and therefore $H_{77} \cap H_{22} = H_{21}$. We claim that H_{77} is uniserial. Otherwise there were an FG-submodule Y such that $H_{77} = Y + H_{21}$ and $Y \cap H_{21} = H_1$, and we had the direct decomposition $H_{99}/H_1 = Y/H_1 \oplus Y/H_1$ into submodules of dimensions 56 and 42. Viewing H_{99}/H_1 as an FG_α-module this contradicts (1.15) by the Krull-Schmidt theorem. Since $H_{100}/H_{23} \cong {H_{77}}^*$, also H_{100}/H_{23} is uniserial.

By counting we see that there are besides H_{22} precisely two further FG-submodules H'_{22} and H''_{22} between H_{21} and H_{23}. We set $H'_{78} = (H'_{22})^\perp$ and $H''_{78} = (H''_{22})^\perp$. Then by duality H_{78}, H'_{78} and H''_{78} are precisely the FG-submodules between H_{77} and H_{79}. We have $H'_{22} = H_{21} + Fx'$ for some vector x' of even weight. Since ${H_{21}}^\perp = H_{79} \geqslant H'_{22}$ it follows that $H'_{22} \leqslant (H'_{22})^\perp = {H_{78}}^\perp$. Similarly, also $H''_{22} \leqslant H''_{78}$.

(iv) Now let X be any FG-submodule of $F\Omega$. We claim that $X = H_i$ or $X = H'_i$ or $X = H''_i$ for some i. Since the set of the H_i, H'_i, H''_i is closed under orthogonal complements, we may assume that $\dim X \leqslant 50$. If X were not contained in H_{23} we would have $X + H_{23} > H_{23}$ and $\dim(X + H_{23}/H_{23}) \geqslant 56$, since H_{100}/H_{23} contains a unique minimal FG-submodule of dimension 56, see (iii). This contradicts $\dim X \leqslant 50$. Therefore $X \leqslant H_{23}$ holds. Taking into account that $H_1 = \langle \mathbb{1} \rangle$ is the FG-submodule of $F\Omega$ containing all vectors fixed by the perfect group G we now get immediately that $X = H_i$ or $X = H'_i$ or $X = H''_i$ for some $i \leqslant 23$. (4) and (5) are now proved completely.

(v) Since $H_{22} = \operatorname{Im} v_1$ it is plainly clear that H_{22} is generated by all the adjacency vectors of the Higman-Sims graph. From (1) it follows that every β-hexad is orthogonal to every adjacency vector $\Delta(\beta)$ of the Higman-Sims graph. Therefore the FG-submodule H of $F\Omega$ generated by all β-hexads, $\beta \in \Omega$, is contained in $H_{78} = {H_{22}}^\perp$. From (1.3) we infer that H_{22} is contained in H, since $\Delta(\alpha)$ is a sum of α-hexads. We shall show later in Section 3 (independently) that the minimum weight of H_{22} is 22. Therefore no β-hexad is contained in H_{22}, so it follows that $H = H_{78}$, since H_{78}/H_{22} is irreducible. The proof of (6) is complete; (7) immediately follows from (3) and (6).

(vi) By the homomorphism theorem for FG-modules we have $H_{79} \setminus H_{78} = \{x \in F\Omega \mid xv = \mathbb{1}\}$. Since v is the linear extension of the map $\beta \mapsto \Delta(\beta)$ from (6) and

(7) it follows that $H_{79} \setminus H_{78} = \{x \in F\Omega \mid (x, \Delta(\beta)) = 1 \text{ for all } \beta \in \Omega\}$. Clearly $A = \{x \in F\Omega \mid (x, h) = 1 \text{ for all } \beta\text{-hexads}\}$ is contained in $H_{23} \setminus H_{22}$ by (7). Also $A + H_{22} = A$ holds. Since $\mathbb{1} \in H_{78}$ from (6) and elementary linear algebra it follows that $A \neq \emptyset$ and hence $A = H_{23} \setminus H_{22}$. The proof of (8) is complete.

(vii) Let m be any heptad of $\mathcal{W}_{22}$ in the sense of Section 1 and let $x(m) = \alpha + m + B_1(m)$ be the corresponding Higman vector. From (1.10) it follows that $(x(m), h) = 1$ for all β-hexads $h, \beta \in \Omega$. Therefore $x(m) \in H_{23} \setminus H_{22}$ follows from (8). Consequently we have $H_{23} = H_{22} + Fx(m)$ and $H_{21} + Fx(m) \in \{H'_{22}, H''_{22}\}$.

$G = \mathrm{HS}$ has two orbits $\mathcal{M}'$ and $\mathcal{M}''$ in the set of heptads of $\mathcal{W}_{22}$. Independently, it will be shown later in (4.1), that if $m' \in \mathcal{M}'$ and $m'' \in \mathcal{M}''$ then $x(m') + x(m'') \in H_{22} \setminus H_{21}$. Hence we may choose the notation so that $H'_{22} = H_{21} + Fx(m')$ if $m' \in \mathcal{M}'$ and $H''_{22} = H_{21} + Fx(m'')$ if $m'' \in \mathcal{M}''$. Since the G-orbits $\mathcal{M}'$ and $\mathcal{M}''$ are interchanged by $\overline{M_{22}} \cong \mathrm{Aut}(M_{22})$ we also conclude that $\overline{G}$ interchanges H'_{22} and H''_{22}.

The assertions (9) and (11) now readily follow. The rest of the Proposition is clear.

□

We may collect the results of this section:

(2.8) Theorem.
Let $G = \mathrm{HS}$ be the Higman-Sims simple group in its rank 3 representation on Ω of degree 100. Then every linear code C over a field F admitting G is obtained within isomorphy from one of the FG-submodules of the permutation module $F\Omega$ which are given in the propositions (2.2), (2.4), (2.6) and (2.7).

Proof. The theorem follows from [20, (3.2)], Lemma (2.1) and the preceding propositions. □

The submodule structure of $H_{100} = \mathbb{F}_2\Omega$ is displayed in Figure 3.

3 The binary linear codes of length 100 admitting G = HS and their relation to the combinatorial structure of the Higman-Sims graph

Our aim is to determine the weight structure of the binary linear codes of length 100 which admit the Higman-Sims group $G = \mathrm{HS}$ and to discuss its combinatorial meaning. Throughout this section let $F = \mathbb{F}_2$. We may tacitly assume that $F\Omega$ is always the ambient space and that Ω is the ambient basis. By abuse of notation we denote these linear codes by the corresponding submodules of $F\Omega$, as introduced in Section 2. We may identify $F\Omega$ with the power set $\mathcal{P}(\Omega)$ in the canonical way whenever it is convenient.

Let $\mathbb{1} = \sum \Omega = \sum\{\beta \mid \beta \in \Omega\}$ denote the all 1 vector in $F\Omega$. We recall from Section 1 the notation $W_i(X) = \{x \in X \mid w(x) = i\}$ for $X \subseteq F\Omega$ and $0 \leqslant i \leqslant 100$. Set

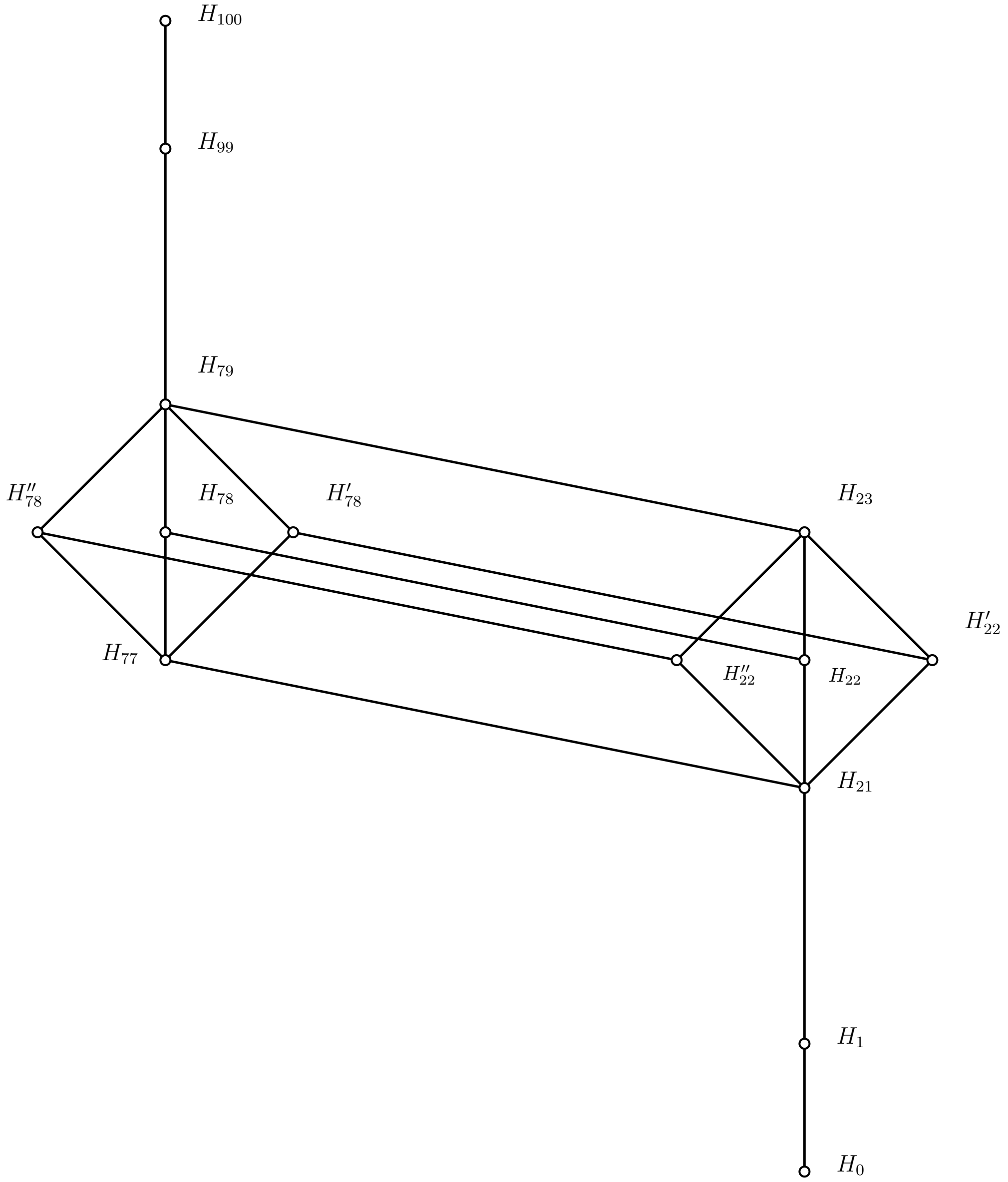


Figure 3: The binary permutation module of $G = \mathrm{HS}$ and its submodules.

$w_i(X) := |W_i(X)|$. Let $m(X)$ denote the minimum (non-zero) weight of X (whenever it is defined).

We begin by studying the vectors of small weight in H_{79}, H_{78} and H_{22}. It will be useful for this purpose to have a classification of vectors in $F\Omega$ of weight at most 4 under the action of $G = \mathrm{HS}$.

(3.1) Proposition.
The G-orbits in $W_i(F\Omega)$ for $1 \leqslant i \leqslant 4$ are as follows:

(1) G acts transitively on $W_1(F\Omega) = \Phi_1$, $|\Phi_1| = 100$.

(2) $W_2(F\Omega) : G = \{\Phi_{21}, \Phi_{22}\}$, where $|\Phi_{21}| = 1,100$ and $|\Phi_{22}| = 3,850$.

(3) $W_3(F\Omega) : G = \{\Phi_{31}, \Phi_{32}, \Pi_{33}\}$, where $|\Phi_{31}| = 77,000, |\Phi_{32}| = 61,000$ and $|\Phi_{33}| = 23,100$.

(4) $W_4(F\Omega) : G = \{\Phi_{4,i} \mid 1 \leqslant i \leqslant 9\}$, where $|\Phi_{41}| = 57,750, |\Phi_{42}| = 616,000, |\Phi_{43}| = 231,000$. $|\Phi_{44}| = 1,386,000, |\Phi_{45}| = 154,000, |\Phi_{46}| = 924,000$. $|\Phi_{47}| = 369,600$, $|\Phi_{48}| = 154,000$ and $|\Phi_{49}| = 28,875$.

Representatives of the orbits are given in the table on the following page.

In the table $\bullet \quad \bullet$ indicates two vertices not joined by an edge in the Higman-Sims graph, $\bullet - \bullet$ indicates two vertices joined by an edge in the Higman-Sims graph and $\bullet < \genfrac{}{}{0pt}{}{\bullet}{\bullet}$ as well as $\genfrac{}{}{0pt}{}{\bullet}{\bullet} > \bullet$ indicate a vertex joined by edges to two distinct vertices etc.

The type *of an element $x \in F\Omega$ has the obvious meaning indicated by the edges and non-edges in the support of x.*

The term "i-vertical" for some $x \in F\Omega$ means that the maximum number of vertices $\xi \in \Omega$ such that $\mathrm{supp}(x) \subseteq \Delta(\xi)$ *is precisely i.*

orbit	*type of orbit element*	*orbit length*
Φ_1	$\bullet$	100
Φ_{21}	$\bullet - \bullet$	$1,100$
Φ_{22}	$\bullet \quad \bullet$	$3,850$
Φ_{31}	$\bullet \quad \bullet \quad \bullet$	$77,000$
Φ_{32}	$\bullet - \bullet \quad \bullet$	$61,600$
Φ_{33}	$\bullet - \bullet - \bullet$	$23,100$
Φ_{41}	$\bullet \quad \bullet \quad \bullet \quad \bullet$ 2-*vertical*	$57,750$
Φ_{42}	$\bullet \quad \bullet \quad \bullet \quad \bullet$ 1-*vertical*	$616,000$
Φ_{43}	$\bullet \quad \bullet \quad \bullet \quad \bullet$ 0-*vertical*	$231,000$
Φ_{44}	$\bullet - \bullet \quad \bullet \quad \bullet$	$1,386,000$
Φ_{45}	$\bullet - \bullet \quad \bullet - \bullet$	$154,000$
Φ_{46}	$\bullet - \bullet - \bullet \quad \bullet$	$924,000$
Φ_{47}	$\bullet - \bullet - \bullet - \bullet$	$369,600$
Φ_{48}	$\bullet - \bullet < \genfrac{}{}{0pt}{}{\bullet}{\bullet}$	$154,000$
Φ_{49}	$\bullet < \genfrac{}{}{0pt}{}{\bullet}{\bullet} > \bullet$	$28,875$

Proof. Since the Higman-Sims graph is triangle-free ($\lambda = 0$) it is readily shown that all the vectors $x \in W_i(F\Omega)(1 \leqslant i \leqslant 4)$ belong to one of the types shown in the table. The known facts about the action of $G_\alpha \cong M_{22}$ ([16, 22]) are now sufficient to establish the proposition. □

It is fairly easy to compute the weight of the images $xv \in H_{22}$ of the vectors x given in (3.1). Of course, the weight depends only on the G-orbit.

(3.2) Lemma.
The Hamming weight $w(xv)$ of the vectors xv for $x \in W_i(F\Omega)(1 \leqslant i \leqslant 4)$ is given by the following table where x is contained in the indicated G-orbit.

orbit	Φ_1	Φ_{21}	Φ_{22}	Φ_{31}	Φ_{32}	Φ_{33}
$w(xv)$	22	44	32	38	42	54

orbit	Φ_{41}	Φ_{42}	Φ_{43}	Φ_{44}	Φ_{45}	Φ_{46}	Φ_{47}	Φ_{48}	Φ_{49}
$w(xv)$	32	40	48	44	40	48	52	60	64

Proof. If $x = \sum x_\beta \beta$ then $xv = \sum\{\Delta(\beta) \mid x_\beta \neq 0\}$. Elementary calculations in the Higman-Sims graph easily give the weights. □

As a consequence of (3.2) we immediately get the minimum weight vectors of H_{79} and H_{78}.

(3.3) Proposition. *(1) $m(H_{79}) = m(H_{78}) = 6$.*

(2) $W_6(H_{79}) = W_6(H_{78})$ is the set of all β-hexads, $\beta \in \Omega$.

(3) $|W_6(H_{79})| = |W_6(H_{78})| = 3,850$.

Proof. From (2.7) we have $H_{78} \leqslant H_{79} \leqslant H_{99} = \{x \in F\Omega \mid w(x) \text{ even }\}$. Since H_{78} is generated by all β-hexads, we also have $m(H_{78}) \leqslant 6$. Now suppose $0 \neq x \in H_{79}$ and $w(x) \leqslant 6$. Since H_{79} is mapped by v onto $H_1 = F\mathbb{1}$ it follows $w(xv) \in \{0, 100\}$. From (3.2) follows that $w(x) = 6$, hence (1) holds. Since $\mathcal{G}_{100}$ is triangle-free there exist $x_1 \in \Phi_{22}$ and $x_2 \in W_4(F\Omega)$ such that $x = x_1 + x_2$, hence $xv = x_1v + x_2v$. It follows by (3.2) that $w(xv) \leqslant w(x_1v) + w(x_2v) \leqslant 32 + 64 = 96 < 100$, thus necessarily $xv = 0$, so $x \in \operatorname{Ker} v = H_{78}$. So we also have $x_1v = x_2v$ and $32 = w(x_1v) = w(x_2v)$, hence $x_2 \in \Phi_{41}$ according to (3.2). Consequently there exist distinct $\gamma, \beta \in \Omega$ such that $\operatorname{supp}(x_2) \subseteq \Delta(\beta) \cap \Delta(\gamma)$. Since $m(H_{78}) = 6$ and $y = \Delta(\beta)\Delta(\gamma)$ (written with pointwise multiplication in $F\Omega$) is a β-hexad belonging to H_{78} we have necessarily $x = y$, so also (2) holds. (3) follows from (2). □

We shall also need a classification of weight 8 vectors in H_{78}. For this purpose and for later use it is convenient to introduce the following notation for vectors $x \in F\Omega$ and $0 \leqslant i \leqslant 22$:

$$\Lambda_i(x) = \{\beta \in \Omega \mid |\operatorname{supp}(x) \cap \Delta(\beta)| = i\} \text{ and } \lambda_i(x) = |\Lambda_i(x)|.$$

Call two vectors $x, y \in F\Omega$ $\mathcal{G}_{100}$-*disjoint* iff $\operatorname{supp}(x) \cap \operatorname{supp}(y) = \emptyset$ and $\mathcal{G}_{100}$ has no edge joining a vertex in $\operatorname{supp}(x)$ and a vertex in $\operatorname{supp}(y)$.

(3.4) Proposition. *(1)* $w_8(H_{78}) = 119,625$.

(2) $W_8(H_{78}) : G = \{\Phi_{81}, \Phi_{82}\}$ *where* $|\Phi_{81}| = 33,000$ *and* $|\Phi_{82}| = 86,625$. Φ_{81} *is the set of β-octads, $\beta \in \Omega$. The elements of* Φ_{82} *are called* skew octads *; they are sums of two $\mathcal{G}_{100}$-disjoint vectors in Φ_{49} and any such sum is a skew octad.*

(3) The stabilizer in G of a skew octad is a Sylow 2-subgroup of G.

Proof. (1) and (3) are straightforward consequences of (2). Let Φ_{81} denote the set of all β-octads, $\beta \in \Omega$. Then clearly $|\Phi_{81}| = 100 \cdot 330 = 33,000$, and Φ_{81} is a G-orbit in $W_8(H_{78})$. Let $\Phi_{82} := W_8(H_{78}) \setminus \Phi_{81}$ and call the elements of Φ_{82} skew octads.

Let z be a skew octad. We set $\lambda_i = \lambda_i(z)$. Counting the edges of the Higman-Sims graph between then vertices in $\mathrm{supp}(z)$ and Ω gives the equations

$$\lambda_0 + \lambda_2 + \lambda_4 + \lambda_6 + \lambda_8 = 100 \text{ and } 2\lambda_2 + 4\lambda_4 + 6\lambda_6 + 8\lambda_8 = 8 \cdot 22 = 176.$$

(i) $\lambda_8 = \lambda_6 = 0$.

For, if $\lambda_8 \neq 0$ then z would be a β-octad for some $\beta \in \Lambda_8(z)$ against the choice of z. If $\lambda_6 \neq 0$ there existed a $\gamma \in \Lambda_6(z)$; taking the trace of zv on $\Delta(\gamma)$ we see that $zv \neq 0$ against $z \in H_{78} = \mathrm{Ker}\, v$.)

(ii) The Higman-Sims graph does not induce the null graph on $\mathrm{supp}(z)$, i.e. $\mathrm{supp}(z) \not\subseteq \Lambda_0(z)$.

Otherwise from (1.8) we deduce that for every $\xi \in \mathrm{supp}(z)$ the set $\Delta(\xi)$ is the disjoint union of te 10-set $\Delta(\xi) \cap \Lambda_4(z)$ and the 12-set $\Delta(\xi) \cap \Lambda_2(z)$. Consequently $\lambda_4 = (8 \cdot 10)/4 = 20, \lambda_2 = (8 \cdot 12)/2 = 48$ and $\lambda_0 = 32$. We consider the $\mathcal{G}_{100}$-edges between $\Lambda_4(z)$ and $\mathrm{supp}(z)$. Call a subset of $\mathrm{supp}(z)$ *hexadic* iff it is contained in the support of a β-hexad, $\beta \in \Omega$. Any 3-subset T of $\mathrm{supp}(z)$ is contained in exactly one β-hexad where $\beta \in \Lambda_4(z)$ since $\Delta(\beta) \cap \mathrm{supp}(z) \geqslant 3$; therefore T is contained in exactly one hexadic 4-subset $\Delta(\beta) \cap \Delta(\gamma)$ where $\beta, \gamma \in \Lambda_4(z)$. Any hexadic 4-subset contains exactly 4 distinct 3-subsets. Double counting now gives for the number h of all hexadic 4-subsets of $\mathrm{supp}(z)$ that $4h = \binom{8}{3} \cdot 1 = 56$, so $h = 14$. For each hexadic 4-subset $H = \Delta(\beta_H) \cap \Delta(\gamma_H)$ there are distinct $\beta_H, \gamma_H \in \Lambda_4(z)$ such that $\Delta(\beta_H) \cap \mathrm{supp}(z) = \Delta(\gamma_H) \cap \mathrm{supp}(z) = H$; moreover the map $H \mapsto \{\beta_H, \gamma_H\}$ has the property that $\{\beta_H, \gamma_H\} \cap \{\beta_{H'}, \gamma_{H'}\} = \emptyset$ if $H \neq H'$. So we may deduce the absurdity $28 = 2 \cdot 14 \leqslant 20$. Therefore the Higman-Sims graph does not induce the null graph on $\mathrm{supp}(z)$.

(iii) $\mathrm{supp}(z) \cap \Lambda_4(z) = \emptyset$.

If there were a $\beta \in \mathrm{supp}(z) \cap \Lambda_4(z)$ we would obtain a contradiction from (1.5) by considering the trace of zv on $\Delta(\beta)$.

(iv) From (ii) and (iii) it follows that $\mathrm{supp}(z) \subseteq \Lambda_0(z) \cup \Lambda_2(z)$ and $\Lambda_2(z) \cap \mathrm{supp}(z) \neq \emptyset$. Without loss we may assume that $\alpha \in \Lambda_2(z) \cap \mathrm{supp}(z)$. From (1.5) we now derive that z is the sum of two vectors in Φ_{49} which are $\mathcal{G}_{100}$-disjoint. Let $z = x + y$ be the sum of two $\mathcal{G}_{100}$-disjoint vectors $x, y \in \Phi_{49}$. From (1.5) we infer that $\mathrm{supp}(zv) \cap \Delta(\beta) = \emptyset$ for all $\beta \in \mathrm{supp}(z)$. Since $\mathrm{supp}(zv) \subseteq \bigcup\{\Delta(\beta) \mid \beta \in \mathrm{supp}(z)\}$ it follows $zv = 0$, hence $z \in H_{78}$ is a skew octad.
From the properties of $\mathcal{G}_{100}$ resp. $\mathcal{W}_{22}$ we deduce via (1.5) that the support of any element in Φ_{49} is contained in the support of exactly 6 distinct skew octads. Since the support of each skew octad contains exactly two different 4-sets which are supports of vectors in Φ_{49} we have

$$|\Phi_{82}| = (6|\Phi_{49}|)/2 = 3 \cdot 28,875 = 86,825$$

which is also the index of a Sylow 2-subgroup in $G = \mathrm{HS}$. To complete the proof it now suffices to prove that the stabilizer G_z in G of a skew octad z is a 2-group. Let K be the largest normal subgroup of G_z fixing every vertex in $\mathrm{supp}(z)$. Then G_z/K is isomorphic to a subgroup of $Z_2 \,\mathrm{wr}\, D_8$, hence $|G_z : K|$ is a power of 2. But it is straightforward from the definition of the Higman-Sims graph that K is a 2-group (see (1.5)(iii)). Therefore G_z is a Sylow 2-subgroup and Φ_{82} is a G-orbit. The proof is complete.

□

Remark. The arguments in the preceding proofs show that there are precisely $|\Phi_{49}|/7 = 4,125$ distinct elements $u \in W_{28}(F\Omega)$ such that u is the sum of 7 pairwise $\mathcal{G}_{100}$-disjoint elements of Φ_{49}. Of course, such a u does not belong to H_{79} since u is congruent to an element of Φ_{49} modulo H_{78}. In fact $uv = xv$ for any $x \in \Phi_{49}$ with $\mathrm{supp}(x) \subseteq \mathrm{supp}(u)$ and $\mathrm{supp}(x) \subseteq \mathrm{supp}(u)$ holds for any $x \in \Phi_{49}$ such that $uv = xv$.

(3.5) Theorem.
The weight distribution of H_{21} and the orbits of $G = \mathrm{HS}$ in H_{21} are as described in the following table.

i	$w_i(H_{21})$	*length of G-orbits in $W_i(H_{21})$*
0/100	1	1
32/68	3,850	3,850
36/64	4,125	4,125
40/60	92,400	15,400 *and* 77,000
44/56	347,600	1,100 *and* 346,500
48/52	600,600	231,000 *and* 369,600

In particular $m(H_{21}) = 32$ and G has precisely 18 orbits in H_{21}.

Proof. Since $\mathbb{1} \in H_{21}$ vectors and also G-orbits occur in complementary pairs belonging to weights i and $100-i$. From (2.7) we infer that $xv \in H_{21}$ for all $x \in H_{99}$, therefore $xv \in H_{21}$ for all $x \in \Phi_{2j} \cup \Phi_{4k}$ by (3.2). We recall that $xv = yv$ if and only if $x + y \in H_{78} = \mathrm{Ker}\, v$.

Of course, v maps G-orbits to G-orbits.
It immediately follows that $\Psi_1 = \{xv \mid x \in \Phi_{21}\}$ is a G-orbit in $W_{44}(H_{21})$ of length $|\Psi_1| = 1,100$ and that $\Psi_2 = \{xv \mid x \in \Phi_{22}\}$ is a G-orbit in $W_{32}(H_{21})$ of length $|\Psi_2| = 3,850$. In counting with the orbits Φ_{4j} we have to take care of multiple preimages when using Propositions (3.3) and (3.4). From Proposition (3.4) and the remark following its proof we infer that $\Psi_3 = \{xv \mid x \in \Phi_{49}\}$ has exactly $|\Phi_{49}|/7 = 4,125$ elements and by (3.2) we have $\Psi_3 \subseteq W_{64}(H_{21})$. The support of any skew octad contains also exactly 16 distinct 4-subsets of type $\bullet - \bullet \quad \bullet \quad \bullet$ which are supports of vectors in Φ_{44}. From (3.1) it hence follows that the support of any $x \in \Phi_{44}$ is contained in the support of exactly one skew octad. An elementary consideration shows that for any $x \in \Phi_{44}$ there exist also two distinct β-hexads z, $\beta \in \Omega$, such that $z = x + y$ where $y \in \Phi_{44}$. Hence from (3.3) and (3.4) it follows that $\Psi_6 = \{xv \mid x \in \Phi_{44}\}$ has exactly $|\Phi_{44}|/4 = 346,500$ elements and we have $\Psi_6 \subseteq W_{44}(H_{21})$ by (3.2).
The support of every skew octad contains 32 distinct 4-subsets of type $\bullet - \bullet - \bullet \quad \bullet$ which are supports of vectors in Φ_{46}. Hence the support of any $x \in \Phi_{46}$ is contained in the support of exactly 3 distinct skew octads. From (3.3) and (3.4) it now follows that $\Psi_7 = \{xv \mid x \in \Phi_{46}\}$ has exactly $|\Phi_{46}|/4 = 231,000$ elements and we have $\Psi_7 \subseteq W_{48}(H_{21})$ by (3.2).
From (3.3) and (3.4) it also follows that $\Psi_8 = \{xv \mid x \in \Phi_{47}\}$ has exactly $|\Phi_{47}| = 369,600$ elements and from (3.2) we have $\Psi_8 \subseteq W_{52}(H_{21})$.
Taking into account that $\dim H_{21} = 21$ the remarks at the beginning of the proof now show that the weight distribution of H_{21} and the G-orbits in H_{21} are as asserted in the theorem. □

In order to determine the weight distribution of H_{23} and its remaining subcodes it will be useful to get some information about the projection of H_{23} to the neighborhoods $\Delta(\beta), \beta \in \Omega$. Since G acts transitively on Ω we may restrict our attention to $\Delta(\alpha) = P_{22}$. We recall from Section 1 that G_{12} denotes the shortened Golay code, $G_{10} = G_{12}^{\perp}$ its dual and G_{11}, G'_{11} and G''_{11} are the subcodes between G_{10} and G_{12} where $G_{11} = G_{10} + F\mathbb{1}_{22}$ is generated by all hexads of $\mathcal{W}_{22}$.

(3.6) Proposition.
Let $p_\alpha : x \mapsto x\Delta(\alpha)$ denote the coordinate restriction of H_{23} to $\Delta(\alpha) = P_{22}$ and let $K = \operatorname{Ker} p_\alpha$. Then the following hold:

(1) The sequence $0 \longrightarrow K \xrightarrow{\text{incl}} H_{23} \xrightarrow{p_\alpha} G_{12} \longrightarrow 0$ is exact.

(2) K is contained in H_{22}, but not in H_{21}. p_α maps H_{21} and H_{22} onto G_{11} and $H'_{22}, H''_{22}, H_{23}$ onto G_{12}.

(3) K has the weight distribution

i	0/78	22/56	32/46	38/40
$w_i(K)$	1	22	231	770

Proof. Since H_{22} is generated by all adjacency vectors $\Delta(\beta)$, $\beta \in \Omega$, it follows from (1.3) that p_α maps H_{22} onto G_{11}. Furthermore $x(m)p_\alpha = m \in G_{12} \setminus G_{11}$ for any heptad m of

$\mathcal{W}_{22}$. Therefore p_α maps H_{23} onto G_{12} and (1) is established. Since H_{22} is mapped by p_α onto a proper subspace of G_{12}, K must be contained in H_{22}. Evidently K contains the vector $\mathbb{1}+\Delta(\alpha)$ of weight $78 \not\equiv 0 \mod 4$. Hence K is not contained in H_{21}. The rest of (2) now easily follows. It remains to determine the weight distribution of K. We use the fact that $K \subseteq H_{22} = \operatorname{Im} v$. If $xv = yv$ then $(x+y)v = 0$, i.e. $x+y \in \operatorname{Ker} v = H_{78}$. From this remark it follows by (3.2) that K contains 22 vectors $\beta v = \Delta(\beta), \beta \in P_{22}$, of weight 22, $\binom{22}{2} = 231$ vectors xv of weight 32 where $\operatorname{supp}(x)$ is a 2-subset of P_{22} and $\binom{22}{3}/2 = 770$ vectors yv of weight 28 where $\operatorname{supp}(y)$ is a 3-subset of P_{22}. Since $\mathbb{1}+\Delta(\alpha)$ is the only vector in K of weight 78, assertion (3) now follows from $\dim K = 11$. □

(3.7) Corollary.
Let $x \in H_{22}$ and $\beta \in \Omega$. Then $w(x\Delta(\beta)) \in \{0, 6, 8, 10, 12, 14, 16, 22\}$.

Proof. The assertion follows from (3.6) and (1.2) since G acts transitively on Ω. □

(3.8) Lemma.
Let $u \in \Phi_{49}$. Then G_u induces the dihedral group D_8 on the 4 vertices in $\operatorname{supp}(u)$.

Proof. The largest subgroup of G_u fixing every vertex in $\operatorname{supp}(u)$ has index 8 in G_u by (3.1). □

(3.9) Proposition.
Let $x \in W_{36}(H_{21})$ and $\overline{x} = x + \mathbb{1}$ its complementary vector.
Then $\Omega : G_x = \{\Lambda_6(x), \Lambda_{14}(x), \Lambda_8(x)\}$ where $\operatorname{supp}(x) = \Lambda_6(x) \cup \Lambda_{14}(x)$, $\operatorname{supp}(\overline{x}) = \Lambda_8(x)$ and $\lambda_6(x) = 8, \lambda_{14}(x) = 28, \lambda_8(x) = 64$. The matrix of the Higman-Sims graph with respect to G_x is

$$\begin{bmatrix} 0 & 14 & 8 \\ 4 & 2 & 16 \\ 1 & 7 & 14 \end{bmatrix}.$$

Moreover, $(\sum \Lambda_6(x))v = \overline{x}$ holds.

Proof. From (3.5) and (3.2) it follows that there exists a $u_0 \in \Phi_{49}$ such that $u_0 v = x$, and one easily checks that $u_0 \cap \operatorname{supp}(\overline{x}) = \emptyset$. From the remark following the proof of (3.4) we infer that the union of all $\operatorname{supp}(u)$, $u \in \Phi_{49}$ such that $uv = x$, forms a set B of cardinality 28, disjoint from $\operatorname{supp}(\overline{x})$ and therefore contained in $\operatorname{supp}(x)$.

Clearly $(\sum B)v = \overline{x}$ holds. Set $A = \operatorname{supp}(x) \setminus B$ and $\Gamma = \operatorname{supp}(\bar{x})$. Obviously, A, B and Γ are fixed by G_x ; we show that G_x acts transitively on A, B and Γ. The elements of order 7 in G have exactly 2 fixed-points in Ω. Since $|G_x|$ does not divide $|M_{22}|$ the subgroup G_x has no fixed-point in Ω. From $7 \mid |G_x|$ we readily conclude that G_x acts 2-transitively on A and that G_x permutes transitively the 7 elements of Φ_{49} whose supports are contained in B. Let $u \in \Phi_{49}$ be such that $\operatorname{supp}(u)$ is contained in B. Since v is a G-homomorphism $G_u \leqslant G_{uv} = G_{\bar{x}} = G_x$. So from (3.8) it follows that G_x acts transitively on B.

Let $G_{\dot{u}}$ denote the largest subgroup of G_u fixing every vertex in $\operatorname{supp}(u)$. From the fundamental properties of the Higman-Sims graph it follows that $G_{\dot{u}}$ has exactly 4 orbits of length 16 which are conjugate under G_u by (3.8). Hence G_u acts transitively on Γ. Since G_x acts doubly-transitively on A the Higman-Sims graph induces on A the null graph. Moreover, the preceding discussion shows that for $\beta \in B$ we have $|\Delta(\beta) \cap B| = 2$ and $|\Delta(\beta) \cap \Gamma| = 16$. It easily follows that the matrix of the Higman-Sims graph with respect to G_x is as asserted; in particular, $A = \Lambda_{14}(x)$, $B = \Lambda_6(x)$ and $\Gamma = \Lambda_8(x)$. $\square$

(3.10) Proposition. *(1)* $w_i(H_{22}) = 0$ *for* $0 < i < 32$ *and* $i \neq 22, 30$.

(2) $w_{22}(H_{22}) = 100$ *and* $w_{30}(H_{22}) = 1,100$.

(3) $W_{22}(H_{22}) = \{\Delta(\gamma) \mid \gamma \in \Omega\}$ *is a G-orbit;* $G_{\Delta(\gamma)} = G_\gamma$ *for* $\gamma \in \Omega$.

(4) $W_{30}(H_{22})$ *is a G-orbit. For* $x \in W_{30}(H_{22})$ *we have* $\Omega : G_x = \{\Lambda_8(x), \Lambda_6(x)\}$ *where* $\mathrm{supp}(x) = \Lambda_8(x)$, $\mathrm{supp}(x + \mathbb{1}) = \Lambda_6(x)$. *In particular,* $\lambda_8(x) = 30$ *and* $\lambda_6(x) = 70$.

Proof. $H_{22} \leqslant H_{99} = \langle \mathbb{1} \rangle^\perp$ implies that $w_i(H_{22}) = 0$ for every odd i. Let $0 \neq x \in H_{22}$ such that $w(x) < 32$. From (3.5) it follows that either $w(x) = 30$ or $w(x) \leqslant 26$. Set $\lambda_j = \lambda_j(x)$.

(i) Suppose that $w(x) \neq 30$. We claim that in this case $w(x) = 22$ and $x = \Delta(\gamma)$ for some $\gamma \in \Omega$.

Assume the contrary. We may choose x as a counterexample of minimal weight. If $\lambda_{22} \neq 0$ there would exist a $\gamma \in \Lambda_{22}(x)$ and then $w(x) \geqslant 22$ and $w(x + \Delta(\gamma)) \leqslant 4$, consequently $x + \Delta(\gamma) = 0$ and $x = \Delta(\gamma)$ by (3.3), contrary to the assumption. If $\lambda_0 \neq 0$ we would have also $\lambda_{22} \neq 0$ by (3.6). Hence we may suppose that $\lambda_{22} = 0 = \lambda_0$. We have $w(x + \Delta(\beta)) \geqslant w(x)$ for all $\beta \in \Omega$. For, otherwise, $x + \Delta(\beta) = \Delta(\gamma)$ by the minimal choice of x, so $x = \Delta(\beta) + \Delta(\gamma) = (\beta + \gamma)v$ which contradicts (3.5) because of $\beta + \gamma \in \Phi_{21} \cup \Phi_{22}$, see (3.2). For $\beta \in \Lambda_j(x)$ we therefore have $w(x) + 22 - 2j \geqslant w(x)$ and $j \leqslant 11$ follows. Therefore $\lambda_j \neq 0$ implies $j \in \{6, 8, 10\}$ by (3.7). Counting the edges of the Higman-Sims graph between $\mathrm{supp}(x)$ and Ω now yields the equations

$$22w(x) = 6\lambda_6 + 8\lambda_8 + 10\lambda_{10} \quad \text{and} \quad 100 = \lambda_6 + \lambda_8 + \lambda_{10}.$$

From these equations we deduce $11w(x) = 300 + \lambda_8 + 2\lambda_{10} \geqslant 300$ and $w(x) > 27$, again a contradiction.

So the claim is proved and (1) holds. By the arguments above we also have obtained that $W_{22}(H_{22})$ is precisely the set of all adjacency vectors $\Delta(\beta), \beta \in \Omega$. Hence (3) holds and $w_{22}(H_{22}) = 100$.

(ii) Suppose $w(x) = 30$. Our first claim is that $\lambda_8 = 30$ and $\lambda_6 = 70$.

Since $w_8(H_{22}) = 0$ by (1) we have $\lambda_{22} = 0$. From (3.6) we infer that $\lambda_0 = 0$. Furthermore, for all $\beta \in \Omega$ we have $w(x + \Delta(\beta)) \geqslant 30$ since otherwise $x + \Delta(\beta) = \Delta(\gamma)$ for some $\gamma \in \Omega$ and $x \in H_{21}$ which is impossible. Therefore we have again

$\lambda_j \neq 0$ only possibly for $j \in \{6, 8, 10\}$ by (3.7). We assert that also $\lambda_{10} = 0$. For, if $\beta \in \Lambda_{10}(x)$ we had $w(x + \Delta(\beta)) = 32$, hence $x + \Delta(\beta) = \Delta(\gamma) + \Delta(\delta)$ for suitable $\gamma, \delta \in \Omega$ by (3.5) and (3.7), which entails that

$$x = \Delta(\beta) + \Delta(\gamma) + \Delta(\delta) = (\beta + \gamma + \delta)v,$$

a contradiction against (3.2). Counting edges now yields the equations

$$6\lambda_6 + 8\lambda_8 = 22 \cdot 30 = 660 \quad \text{and} \quad \lambda_6 + \lambda_8 = 100$$

which have the unique solution $\lambda_6 = 70$ and $\lambda_8 = 30$.

(iii) For every $x \in W_{30}(H_{22})$ and every $\beta \in \Lambda_8(x)$ we have $x + \Delta(\beta) \in W_{36}(H_{22}) = W_{36}(H_{21})$ which is a G-orbit of length $4,125$. On the other hand for every $z \in W_{36}(H_{22}) = W_{36}(H_{21})$ and $\gamma \in \Lambda_{14}(z)$ we have $z + \Delta(\gamma) \in W_{30}(H_{22})$. Hence $W_{30}(H_{22}) \neq \emptyset$. We consider the incidence structure

$$\mathcal{I} = (W_{30}(H_{22}), W_{36}(H_{22}), \mathrm{I})$$

where $\mathrm{I} = \{(x, z) \mid x \in W_{30}(H_{22}), z \in W_{36}(H_{22}) \text{ and } x + z \in W_{22}(H_{22})\}$. It follows from (3.9) that G acts transitively on I. Since G acts transitively on $W_{36}(H_{21})$ we conclude that also $W_{30}(H_{22})$ is a G-orbit and that G_x acts transitively on $\Lambda_8(x)$ for $x \in W_{36}(H_{22})$. Double counting of I then gives

$$w_{30}(H_{22}) \cdot 30 = |\mathrm{I}| = w_{36}(H_{22}) \cdot 8 = 4,125 \cdot 8 = 33,000,$$

hence $w_{30}(H_{22}) = 1,100$. From (3.9) we may deduce that for $x \in W_{30}(H_{22})$ we have $\Lambda_8(x) \cap \mathrm{supp}(x + \mathbb{1}) = \emptyset$, hence $\Lambda_8(x) = \mathrm{supp}(x)$ and $\Lambda_6(x) = \mathrm{supp}(x + \mathbb{1})$. One checks by inspection that for $z \in W_{36}(H_{22})$ and $\beta \in \Lambda_{14}(z)$ the subgroup $G_{z,\beta}$ has an orbit of length 14 in $\mathrm{supp}(z + \Delta(\beta) + \mathbb{1})$. It again follows by counting of edges that for $x \in W_{30}(H_{22})$ the subgroup G_x acts transitively on $\mathrm{supp}(x + \mathbb{1}) = \Lambda_6(x)$.

□

Remark. It will be shown in (4.9) that $G_x \cong \Sigma_8$ for $x \in W_{30}(H_{22})$.

The results we have yet obtained are sufficient to determine the weight distribution of the code H_{22} via the MacWilliams identities.

(3.11) Theorem.
The weight distribution of H_{22} and the orbits of G in H_{22} are as described in Table 1. In particular, G has precisely 34 orbits in H_{22}. Complementary vectors of weight 50 are in the same G-orbit.

Proof. Let $a_i = w_i(H_{22})$ and $b_i = w_i(H_{78})$. We recall that $H_{78} = {H_{22}}^{\perp}$. Hence the families (a_i) and (b_i) are related to each other by the MacWilliams identities.

We have $H_{22} \leqslant H_{78} \leqslant H_{99}$; hence $a_i = b_i = 0$ holds for every odd i. Since $\mathbb{1} \in H_{22}$ we have $a_i = a_{100-i}$ for all i. From (3.10) we have the information that

$$a_i = 0 \text{ for } 0 < i < 32 \text{ with the exceptions } a_{22} = 100,\ a_{30} = 1,100.$$

i	$w_i(H_{22})$	length of G-orbits in $W_i(H_{22})$.
0/100	1	1
22/78	100	100
30/70	1,100	1,100
32/68	3,850	3,850
36/64	4,125	4,125
38/62	38,500	38,500
40/60	92,400	15,400 and 77,000
42/58	193,600	61,600 and 132,000
44/56	347,600	1,100 and 346,500
46/54	485,100	23,100 and 462,000
48/52	600,600	231,000 and 369,600
50	660,352	44,352 and 616,000

Table 1: The weight distribution of H_{22} and the orbits of G in H_{22}.

Furthermore $a_0 = a_{100} = 1$ trivially holds, and from (3.5) every a_i with $i \equiv 0 \pmod 4$ is known. So the only unknown weight numbers of H_{22} with $i \leqslant 50$ are

$$a_{34}, a_{38}, a_{42}, a_{46} \text{ and } a_{50}.$$

On the other hand we know from (3.3) and (3.4) the values

$$b_0 = 1,\ b_2 = b_4 = 0,\ b_6 = 3,850,\ b_8 = 119,625.$$

It follows from the general theory of MacWilliams identities that the weight distribution (a_i) is uniquely determined by the known values of the a_i, and b_j, see e.g. [28]. Explicit calculations yield the values asserted in the theorem.

It remains to determine the G-orbits in $H_{22} \setminus H_{21}$. It is convenient to consider first the factor module H_{22}/H_1 which consists of pairs $\{x, x + \mathbb{1}\} = x + H_1$ of complementary vectors, $x \in H_{22}$. Because of $H_{79} = H_{21}^{\perp}$ we clearly have $H_{22}/H_1 \cong_{FG} H_{100}/H_{79} \cong_{FG} {H_{21}}^*$.

Since $F = \mathbb{F}_2$, by Lemma (1.2) G has the same number of orbits in H_{21}^* as in H_{21}. By (3.5) therefore G has exactly 18 orbits in H_{21}/H_1. By (3.5) G also has 9 orbits in H_{21}/H_1, so G has exactly 9 orbits in $H_{22}/H_1 \setminus H_{21}/H_1$.

For $x+H_1 \in F\Omega/H_1$ we define the *weight* $w(x+H_1) = \{w(x), w(x+\mathbb{1})\}$. From (3.10) it follows that G has in H_{22}/H_1 one orbit of elements of weight $\{22, 78\}$ of length 100 and one orbit of elements of weight $\{30, 70\}$ and length $1,100$. From (3.1), (3.2), and (3.3) it follows that G has in H_{22}/H_1 an orbit of elements of weight $\{38, 62\}$ and length $38,500$. The weight distribution of H_{22} which we have determined tells us that all remaining pairs $x + H_1$ have weight $\{i, 100 - i\}$ where $i \in \{42, 46, 50\}$. From (3.1), (3.2) and (3.3) we also obtain that G has in H_{22}/H_1 an orbit of elements of weight $\{42, 58\}$ and length $61,600$ and an orbit of elements of weight $\{46, 54\}$ and length $23,100$. Since $a_{50}/2 = 330,176$ is not a divisor of the order of G we have at least two G-orbits of elements of weight $\{50, 50\}$ in H_{22}/H_1. Since G has exactly 9 orbits in $H_{22}/H_1 \setminus H_{21}/H_1$ it follows that

G has precisely two more orbits: one of length $132,000$ consisting of elements of weight $\{42, 58\}$ and one of length $462,000$ consisting of elements of weight $\{46, 54\}$. To complete the proof of the theorem we have to consider vectors of weight 50. We claim that there are even only 2 G-orbits in $W_{50}(H_{22})$, i.e. that complementary vectors in $W_{50}(H_{22})$ are in the same G-orbit. This assertion and the length of the two G-orbits in $W_{50}(H_{22})$ are obtained in the following lemma. $\square$

(3.12) Lemma.
Let P, Q be two distinct elements of $\Delta(\alpha)$ and $h, k, \ell \in \Delta_2(\alpha)$ such that

$$Q \in h, Q \notin k \cup \ell, h \cap k = \emptyset, h \cap \ell \neq \emptyset \text{ and } P \in k \cap \ell.$$

Set $u = \alpha + P + Q + h, u_1 = u + k$ and $u_2 = u + \ell$ and let 50_i denote the G-orbit containing $x_i = u_i v$ $(i = 1, 2)$. Then the following hold.

(1) $W_{50}(H_{22}) = 50_1 \cup 50_2$.

(2) $|50_1| = 44,352$ and $|50_2| = 616,000$.

Proof. Set $\overline{x} = uv$ and $x = \overline{x} + \mathbb{1}$. By construction $u \in \Phi_{47}$ and from (3.2) it follows that $x \in 48_2$ where 48_2 denotes the G-orbit in $W_{48}(H_{22})$ of length $369,600$ as above. Furthermore, we have $G_x = G_{\overline{x}} = G_u \cong \Sigma_5$ (by considering a hexad stabilizer). Elementary considerations show that $\Lambda_{10}(x)$ splits into a unique G_x-orbit Ψ_1 of length 6 and its complement Ψ_2 of cardinality 30. Moreover, $k \in \Psi_1$ and $\ell \in \Psi_2$.

It is easy to show that G_{x_1} acts transitively on $\mathrm{supp}(x_1) = \Lambda_{12}(x_1)$. We therefore can count the incidences in the incidence structure $\mathcal{I}_1 = (48_2, 50_1, \mathrm{I}_1)$ where

$$\mathrm{I}_1 = \{(w, z) \mid w \in 48_2, z \in 50_1 \text{ and } w + \Delta(\gamma) = z \text{ such that } |\gamma G_w| = 6\},$$

obtaining $369,600 \cdot 6 = |50_1| \cdot 50$, hence $|50_1| = 44,352$. (It easily follows that G_{x_1} acts transitively also on $\mathrm{supp}(\overline{x_1}) = \Lambda_{10}(x_1)$ where $\overline{x_1} = x_1 + \mathbb{1}$ and that x_1 and $\overline{x_1}$ are in the same G-orbit.)

The preceding arguments also show that $50_2 \neq 50_1$. Since G has exactly 2 orbits of vectors of weight $\{50, 50\}$ in H_{22}/H_1 we have either $|50_2| = 616,000$ or $|50_2| = 308,000$. In order to decide this alternative we consider $\Lambda_{16}(x_2)$ and we find $|\Lambda_{16}(x_2)| = 2$ by direct examination. If $\gamma \in \Lambda_{16}(x_2)$ then $x_2 + \Delta(\gamma) \in W_{40}(H_{22}) = 40_1 \cup 40_2$ where 40_1 denotes the G-orbit of length $15,400$ and 40_2 denotes the G-orbit of length $77,000$, see (3.11). From (3.5) we infer that for $y \in 40_2$ the set $\Lambda_6(y)$ is a G_y-orbit of length 16 and that $\Lambda_6(z) = \emptyset$ for any $z \in 40_1$. Therefore we consider the incidence structure

$$\mathcal{I}_2 = (40_1, 50_2, \mathrm{I}_2) \text{ where } \mathrm{I}_2 = \{(w, z) \mid w \in 40_1, z \in 50_2 \text{ and } w + \Delta(\gamma) = z \text{ for some } \gamma\}.$$

Counting incidences gives $|40_1| \cdot 16 = |50_2| \cdot 2$, hence $|50_2| = |40_1| \cdot 8 = 616,000$ which completes the proof of the lemma. $\square$

The argumentation in (3.12) (and in (3.9)) may be extended to all G-orbits in H_{22} in order to obtain results concerning the "set connectivity" in the Higman-Sims graph. We list the results in the following proposition, omitting proofs which tend to be tedious calculations.

G-orbits consisting of vectors of weight k are denoted by k or k_1, k_2 using the convention that $|k_1| < |k_2|$. We give the relevant information in the *graph matrix* of the G-orbits in H_{22} which is defined as follows:

The row and colomn indices are the G-orbits in H_{22}. The entry $m; n$ belonging to the ordered index pair (k, ℓ) tells that there are exactly m vertices $\beta \in \Omega$ such that $x + \Delta(\beta) \in \ell$ for any $x \in k$ and that there are exactly n vertices $\gamma \in \Omega$ such that $y + \Delta(\gamma) \in k$ for any $y \in \ell$. The entry $0; 0$ is replaced by $--$ for better readability.

We give the graph matrix in a *reduced form* from which the complete matrix is easily derived by considering complementary vectors.

(3.13) Proposition.
The graph matrix of the G-orbits in H_{22} is given by the following submatrix.

	22	30	38	42_1	42_2	46_1	46_2	50_1	50_2
0	$100;1$	$--$	$--$	$--$	$--$	$--$	$--$	$--$	$--$
32	$2;77$	$--$	$60;6$	$32;2$	$--$	$--$	$--$	$--$	$--$
68	$--$	$--$	$--$	$--$	$--$	$6;1$	$--$	$--$	$--$
36	$--$	$8;30$	$--$	$--$	$64;2$	$28;5$	$--$	$--$	$--$
40_1	$--$	$--$	$--$	$40;10$	$--$	$--$	$60;2$	$--$	$--$
40_2	$--$	$1;70$	$16;32$	$--$	$24;14$	$6;20$	$36;6$	$--$	$16;2$
60_2	$--$	$--$	$1;2$	$--$	$--$	$--$	$--$	$--$	$16;2$
44_1	$2;22$	$--$	$--$	$56;1$	$--$	$--$	$--$	$--$	$--$
56_1	$--$	$--$	$--$	$--$	$--$	$42;2$	$--$	$--$	$--$
44_2	$--$	$--$	$4;36$	$8;45$	$16;42$	$--$	$32;24$	$--$	$32;18$
56_2	$--$	$--$	$--$	$--$	$--$	$--$	$8;6$	$--$	$32;18$
48_1	$--$	$--$	$4;24$	$8;30$	$--$	$--$	$32;16$	$--$	$32;12$
52_1	$--$	$--$	$--$	$--$	$8;14$	$4;40$	$12;6$	$--$	$32;12$
48_2	$--$	$--$	$--$	$--$	$10;28$	$2;32$	$30;24$	$6;50$	$30;18$
52_2	$--$	$--$	$--$	$2;12$	$--$	$--$	$20;16$	$6;50$	$30;18$

Proof. Omitted. □

From (3.13) (or other elementary considerations) we can derive for any G-orbit k the minimum weight $m(k)$ of a vector $u \in F\Omega$ such that $uv \in k$.

(3.14) Corollary.
The values $m(k)$ for the G-orbits k in H_{22} are given in Table 2. Moreover, every $x \in F\Omega$ is congruent to a vector of weight at most 8 *modulo H_{78} and to a vector of weight at most* 5 *modulo H_{79}. Hence every coset leader of H_{78} has weight at most* 8.

Now we may use the MacWilliams transformation to obtain the weight distributions of the codes $H_{78} = {H_{22}}^{\perp}$ and $H_{79} = {H_{21}}^{\perp}$. (This computation has been carried out first

k	$m(k)$	k	$m(k)$
0	0	100	8
32	2	68	6
36	6	64	4
40_1	4	60_1	4
40_2	4	60_2	4
44_1	2	56_1	6
48_1	4	52_1	6
48_2	6	52_2	4
22	1	78	7
30	5	70	5
38	3	62	5
42_1	3	58_1	7
42_2	5	5_2	5
46_1	5	54_1	3
46_2	5	54_2	5
50_1	5	50_2	5

Table 2: The values $m(k)$ for the G-orbits k in H_{22}.

in 1980 by F.H Florian at the Rechenzentrum of Tübingen University using the ALDES program for computing with large numbers; nowadays it is easy to obtain the result by suitable computer algebra software like e.g. GAP [10].)

(3.15) Proposition.
The weight distributions of H_{78} and of H_{79} are as given in Table 3.

Proof. The assertion follows from (3.11) and (3.5) by the MacWilliams transformation. □

Our next purpose is to determine the weight distribution and the G-orbits of the codes H'_{22} and H''_{22}. These codes are conjugate under the permutation group $\overline{G} \cong \mathrm{Aut}(G)$; hence they have the same weight distribution and the same G-orbit structure so that they can be discussed simultaneously. Since $H_{23} = H_{22} \cup H'_{22} \cup H''_{22}$ we obtain all information also about H_{23}.

At first, we complete the classification of vectors in $W_8(H_{79})$.

(3.16) Lemma.
For every $x \in H_{79} \setminus H_{78}$ and every $\beta \in \Omega$ $w(x\Delta(\beta)) = |\mathrm{supp}(x) \cap \Delta(\beta)|$ is odd.

Proof. This is an immediate consequence of (2.7)(8). □

(3.17) Proposition.
$W_8(H_{79}) \setminus W_8(H_{78})$ consists precisely of all vectors $\beta + m$ where m is a β-heptad. In

i	$w_i(H_{78})$	$w_i(H_{79})$
0/100	1	1
6/94	$3,850$	$3,850$
8/92	$119,625$	$154,825$
10/90	$8,625,540$	$16,387,140$
12/88	$504,741,475$	$1,003,835,875$
14/86	$21,060,732,550$	$42,133,634,950$
16/84	$641,604,305,375$	$1,283,480,881,375$
18/82	$14,622,264,133,400$	$29,244,271,163,800$
20/80	$255,578,801,503,795$	$511,152,645,567,795$
22/78	$3,496,197,414,021,950$	$6,992,403,401,202,750$
24/76	$38,040,184,865,580,975$	$76,080,408,035,945,775$
26/74	$333,583,288,959,605,300$	$667,166,480,352,256,500$
28/72	$2,383,620,258,950,558,925$	$4,767,240,353,068,238,925$
30/70	$14,005,822,677,643,540,370$	$28,011,646,019,961,809,810$
32/68	$68,193,674,451,079,227,050$	$136,387,349,145,968,724,650$
34/66	$276,907,651,030,419,444,000$	$553,815,299,356,210,253,600$
36/64	$942,804,612,331,379,390,725$	$1,885,609,223,857,102,552,325$
38/62	$2,703,690,041,528,811,696,900$	$5,407,380,102,022,140,311,300$
40/60	$6,554,715,235,199,646,035,290$	$13,109,430,428,316,832,071,770$
42/58	$13,474,850,115,575,617,584,200$	$26,949,700,280,870,672,877,000$
44/66	$23,545,377,618,939,915,393,150$	$47,090,755,183,602,450,042,750$
46/64	$35,033,702,002,644,035,359,900$	$70,067,404,105,299,389,919,900$
48/52	$44,444,350,668,327,576,562,750$	$88,888,701,152,233,082,111,550$
50	$48,108,741,996,656,177,342,352$	$96,217,484,223,130,147,456,656$

Table 3: The weight distributions of H_{77} and H_{78}.

particular $w_8(H_{79}) = w_8(H_{78}) + 35,2000$ *and* G *has exactly two orbits* Φ_8' *and* Φ_8'' *of length* $17,600$ *in* $W_8(H_{79}) \setminus W_8(H_{78})$. *These* G*-orbits are conjugate under* $\overline{G} \cong \mathrm{Aut}(G)$.

Choosing suitable notation we have $\Phi_8' \subseteq H_{78}'$ *and* $\Phi_8'' \subseteq H_{78}''$.

Proof. Let m be a β-heptad, $\beta \in \Omega$. Then we have $(\beta + m)v = \mathbb{1}$, as follows from (1.9). Hence $\beta + m \in W_8(H_{79}) \setminus H_{78}$. From (1.3) we infer that $G_\alpha \cong M_{22}$ has two orbits on the set of α-heptads, the orbits being conjugate under the action of $\overline{G}_\alpha \cong \mathrm{Aut}(M_{22})$. It follows that G has two orbits Φ_8' and Φ_8'' of length $17,600$ in $W_8(H_{79}) \setminus W_8(H_{78})$ which are conjugate under $\overline{G} \cong \mathrm{Aut}(G)$, where Φ_8' and Φ_8'' consist of vectors $\beta + m$ where m is a β-heptad.

If m is an α-heptad we have $\langle \alpha + m, x(m) \rangle = 0$ for the Higman vector $x(m) = \alpha + m + B_1(m)$, see (1.10) and (2.7). Hence we conclude from (2.7) that we may choose the notation so that $\Phi_8' \subseteq H_{78}'$ and $\Phi_8'' \subseteq H_{78}''$. From (3.15) we have $w_8(H_{79}) = w_8(H_{78}) + 35,200$ and the assertion follows.

However, it is easy to avoid the use of (3.15) in order to obtain the result. We give a sketch of a short direct proof:

Let $y \in W_8(H_{79}) \setminus H_{78}$ and let $k(y) = \max\{|\Delta(\xi) \cap \operatorname{supp}(y)| \mid \xi \in \operatorname{supp}(y)\}$. Then $k(y) \in \{1, 3, 5, 7\}$ by (3.16). The possibility $k(y) \in \{1, 3, 5\}$ is ruled out by easy contradictions. Therefore $k(y) = 7$ and it follows that $y = \beta + m$ for a vector m of weight 7 such that $\operatorname{supp}(m) \subseteq \Delta(\beta)$. Without loss we may assume $\beta = \alpha$; then we obtain from (1.3) that m is a heptad in $\mathcal{W}_{22}$ from the fact that $\langle y, \Delta(\gamma)\rangle = 1$ for every $\gamma \in \Delta_2(\alpha)$. □

(3.18) Lemma.
Let $x \in H_{23} \setminus H_{22}$ and $\beta \in \Omega$. Then $w(x\Delta(\beta)) = |\operatorname{supp}(x) \cap \Delta(\beta)| \in \{7, 11, 15\}$.

Proof. The assertion follows from (3.6) and (1.3) since G acts transitively on Ω. □

(3.19) Proposition.
The code H'_{22} has minimum weight 32.

Proof. H_{21} is the subcode of H'_{22} consisting of all vectors of weight divisible by 4. Since 32 is the minimum weight of H_{21} by (3.5) it suffices to show that $w_i(H'_{22}) = 0$ for all $0 < i < 32$. Let $x \in W_i(H'_{22})$ where $0 < i \leqslant 32$. Let $\lambda_j = \lambda_j(x)$ for $0 \leqslant j \leqslant 22$. Counting the edges of the Higman-Sims graph between $\operatorname{supp}(x)$ and Ω gives by (3.18) the equations

$$\begin{array}{rcl} w(x)\cdot 22 & = & 7\lambda_7 + 11\lambda_{11} + 15\lambda_{15} \\ 100 & = & \lambda_7 + \lambda_{11} + \lambda_{15}. \end{array}$$

It follows $w(x) \cdot 22 = 700 + 4\lambda_{11} + 8\lambda_{15} \geqslant 700$ and $w(x) > 31$, hence $w(x) = 32$. □

We are now in a position to obtain the weight distributions of H'_{22} and H_{23} using the MacWilliams or Pless identities.

(3.20) Theorem.
The weight distribution of H'_{22} and the orbits of G in H'_{22} are as described in the following table.

i	$w_i(H'_{22})$	*length of G-orbits in $W_i(H'_{22})$.*
0/100	1	1
32/68	3,850	3,850
34/66	5,600	5,600
36/64	4,125	4,125
38/62	38,500	38,500
40/60	92,400	15,400 *and* 77,000
42/58	387,200	17,600 *and* 369,600
44/56	347,600	1,100 *and* 346,500
48/52	600,600	231,000 *and* 369,600
50	1,311,552	352, 123,200, 264,000 *and* 924,000

In particular, G has precisely 30 orbits in H'_{22}. Complementary vectors of weight 50 are in the same G-orbit.

Proof. Let $a_i = w_i(H'_{22})$ and $b_i = w_i(H'_{78})$. We recall that $H'_{78} = (H'_{22})^\perp$. Hence the families (a_i) and (b_i) are related to each other by the MacWilliams identities.

We have $H'_{22} \leqslant H'_{78} \leqslant H_{99}$, as follows from (2.7); hence for every odd i we have $a_i = b_i = 0$. Since $\mathbb{1} \in H'_{22}$ we have $a_i = a_{100-i}$ for all i. Moreover, $\{x \mid x \in H'_{22}$ and $w(x) \equiv 0 \pmod 4\} = H_{21}$. In view of (3.19) we therefore have the following information:

$$\begin{aligned} a_i &= 0 \text{ for } 0 < i < 32 \text{ and } 78 < i < 100, \\ a_0 = a_{100} &= 1 \text{ and from (3.5) every } a_i \text{ with } i \equiv 0 \pmod 4 \text{ is known.} \end{aligned}$$

So the only unknown weight numbers of H'_{22} with $i \leqslant 50$ are

$$a_{34}, a_{38}, a_{42}, a_{46} \text{ and } a_{50}.$$

On the other hand we know from (3.3) and (3.18) the values

$$b_0 = 1, b_2 = b_4 = b_6 = 0 \text{ and } b_8 = 17,600.$$

It follows from the general theory of MacWilliams identities that the weight distribution (a_i) is uniquely determined by the known values of the a_i and b_j, see e.g. [28]. Explicit calculations yield the values asserted in the theorem.

It remains to determine the G-orbits in $H'_{22} \setminus H_{21}$. This will be done in a sequence of lemmas, as some detailed investigations are required. Note that the fact that all G-orbits in $W_{50}(H'_{22})$ have different length implies that complementary vectors of weight 50 are in the same G-orbit. ☐

Recall from Section 2 that the permutation group $\overline{G} \cong \mathrm{Aut}(G)$ interchanges the codes H'_{22} and H''_{22} and leaves H_{21} invariant. Therefore we have a natural involutory correspondence between the G-orbits in $H'_{22} \setminus H_{21}$ and those in $H''_{22} \setminus H_{21}$. We agree that X' and X'' will always denote G-orbits corresponding in this sense.

We start by considering the Higman vectors $x(m) = \alpha + m + B_1(m)$ which we know to belong to $H_{23} \setminus H_{22}$ from (2.7). Recall that we denote the G_α-orbits $\mathcal{M}'$ and $\mathcal{M}''$ on the heptads of $\mathcal{W}_{22}$ in such a way that $x(m) \in H'_{22}$ if and only if $m \in \mathcal{M}'$.

(3.21) Proposition.
Let $X'_0 = \{x(m) \mid m \in \mathcal{M}'\} \cup \{x(m) + \mathbb{1} \mid m \in \mathcal{M}'\}$. Then the following hold.

(1) X'_0 is a G-orbit in $W_{50}(H'_{22}) \setminus H_{21}$.

(2) $G_{x(m)} \cong \mathrm{PSU}(3, 5^2) = \mathrm{U}_3(5)$ acts as a rank 3 group on the supports of $x(m)$ and $x(m) + \mathbb{1}$; the supports of $x(m)$ and $x(m) + \mathbb{1}$ are nonisomorphic $G_{x(m)}$-spaces. $G_{\{x(m), x(m)+\mathbb{1}\}} \cong \mathrm{P\Sigma U}(3, 5^2)$ acts transitively on Ω.

(3) $\mathrm{supp}(x(m)) = \Lambda_7(x(m))$ and $\mathrm{supp}(x(m) + \mathbb{1}) = \Lambda_{15}(x(m))$.

(4) The mapping $m \mapsto \{x(m), x(m) + \mathbb{1}\}$ of $\mathcal{M}'$ onto X'_0/H_1 is bijective and a G_α-morphism. In particular $|X'_0| = 2 \cdot 176 = 352$.

Proof. It follows from (2.7) and (1.9) that $X_0'/H_1 = \{\{x, x+\mathbb{1}\} \mid x \in W_{50}(H_{22}')$ and the Higman-Sims graph induces on $\mathrm{supp}(x)$ and on $\mathrm{supp}(x+\mathbb{1})$ a strongly regular graph of valency $7\}$. Therefore X_0'/H_1 and X_0' are invariant under G. It is immediate that $m \mapsto \{x(m), x(m)+\mathbb{1}\}$ is a bijective morphism of G_α-spaces. It follows that $|X_0'/H_1| = 176$ and that G acts transitively on X_0'. From (1.3) and (1.9) we infer that $G_{x(m),\beta} \cong A_7$ for all $\beta \in \Omega$ and that $G_{x(m),\beta}$ acts as a rank 3 group on the supports of $x(m)$ and $x(m)+\mathbb{1}$, the supports being nonisomorphic $G_{x(m)}$-spaces. From D.G. Higman's result [14, 6.1], we may conclude that $G_{\{x(m),x(m)+\mathbb{1}\}} \cong \mathrm{P\Sigma U}(3,5^2)$. The rest of the assertion easily follows. $\square$

Remark. Note that $G_{\{x(m),x(m)+\mathbb{1}\}} \cong \mathrm{P\Sigma U}(3,5^2)$ does not leave invariant the strongly regular graphs induced on $x(m)$ and $x(m)+\mathbb{1}$, but interchanges them blockwise. It follows from (2.7) that $\overline{G}_{\{x(m),x(m)+\mathbb{1}\}} = G_{\{x(m),x(m)+\mathbb{1}\}}$ where $\overline{G} \cong \mathrm{Aut}(G)$ is the automorphism group of the Higman-Sims graph. Hence even $\overline{G}$ induces on the supports of $x(m)$ and of $x(m)+\mathbb{1}$ only the group $\mathrm{PSU}(3,5^2)$, and not the complete automorphism group $\cong$ $\mathrm{P\Sigma U}(3,5^2)$ of the strongly regular graph of valency 7 on 50 vertices.

By the convention above there is a G-orbit X_0'' in $W_{50}(H_{22}''\backslash H_{21})$ which shares analogous properties. X_0' and X_0'' are interchanged by $\overline{G} \cong \mathrm{Aut}(G)$.

It is more complicated to deal with the remaining G-orbits. We use the connections in the Higman-Sims graph as a guide.

(3.22) Lemma.
Let $x = x(m) \in X_0'$; then $\alpha \in \Lambda_{15}(x+\mathbb{1})$. We have $y = (x+\mathbb{1}) + \Delta(\alpha) \in W_{42}(H_{22}'')$ and y has the following properties.

(1) $G_y = G_{x,\alpha} \cong A_7$.

(2) G_y has the following orbits in Ω:

$$\begin{array}{lclcrr}
\Phi_0 & = & \{\alpha\} & = & \mathrm{supp}(x) \cap \Lambda_7(y), & |\Phi_0| = 1, \\
\Phi_1 & = & \mathrm{supp}(m) & = & \mathrm{supp}(x) \cap \Lambda_{15}(y), & |\Phi_1| = 7, \\
\Phi_2 & = & B_1(m) & = & \mathrm{supp}(x) \cap \Lambda_{11}(y), & |\Phi_2| = 42, \\
\Phi_3 & = & \Delta(\alpha)+m & = & \mathrm{supp}(y+\mathbb{1}) \cap \mathrm{supp}(x+\mathbb{1}) \subseteq \Lambda_7(y), & |\Phi_3| = 15, \\
\Phi_4 & = & B_3(m) & = & \mathrm{supp}(y) \cap \Lambda_7(y), & |\Phi_4| = 35.
\end{array}$$

(3) The matrix of the Higman-Sims graph with respect to $(\Phi_i)_{0 \leqslant i \leqslant 4}$ is

$$\begin{bmatrix} 0 & 7 & 0 & 15 & 0 \\ 1 & 0 & 6 & 0 & 15 \\ 0 & 1 & 6 & 5 & 10 \\ 1 & 0 & 14 & 0 & 7 \\ 0 & 3 & 12 & 3 & 4 \end{bmatrix}.$$

Proof. The assertion follows from (1.13) since G_y must leave invariant $\mathrm{supp}(y)$ and all $\Lambda_i(y)$. $\square$

(3.23) Proposition.
Let $x = x(m) \in X_0'$ and $y = (x + \mathbb{1}) + \Delta(\alpha)$. Denote by Y_0'' the G-orbit containing y. Then $|Y_0''| = 17,600$.

Proof. It follows from (3.21) that $|Y_0''| = |G : G_y| = 352 \cdot 50 = 17,600$. $\square$

Note that every vector in Y_0'' (and Y_0') shares the properties of y described in (3.22). In particular $\Lambda_{15}(y)$ is a unique G_y-orbit of length 7 for any $y \in Y_0''$. If $y \in Y_0''$ and $\beta \in \Lambda_{15}(y)$ then $z = y + \Delta(\beta) \in W_{34}(H_{22}')$ and G_z contains a subgroup isomorphic to A_6. We show that G acts transitively on $W_{34}(H_{22}')$ by arguments independent of the preceding discussion.

(3.24) Lemma.
Let $z \in W_{34}(H_{22}')$ and $\lambda_i = |\Lambda_i(z)|$. Then the following hold.

(1) $\lambda_{11} = 12$ *and* $\lambda_7 = 88$.

(2) G_z *does not fix any point in* Ω.

Proof. $\lambda_{15} = 0$ holds since H_{22}' has minimum weight 32. The canonical equations by counting edges

$$\begin{array}{rcrcr} 34 \cdot 22 & = & 7\lambda_7 & + & 11\lambda_{11} \\ 100 & = & \lambda_7 & + & \lambda_{11} \end{array}$$

yield (1).

Assume that G_z fixes a point $\beta \in \Omega$. From the first part of Theorem (3.20) follows $5,600 \geqslant |G : G_z| = |G : G_\beta||G_\beta : G_z| = 100|G_\beta : G_z|$ and $|G_\beta : G_z| \leqslant 56$. Since $G_\beta \cong M_{22}$ either $G_\beta = G_z$ or $G_z = G_{\beta\gamma}$ for some point $\beta \neq \gamma$. By considering the action of G_β and of $G_{\beta\gamma}$ on Ω we see that $|\Lambda_{11}(z)| = 12$ is impossible, a contradiction against (1). Thus (2) holds. $\square$

(3.25) Proposition.
G acts transitively on $W_{34}(H_{22}') = Z'$. Let $z \in Z'$. Then the following hold.

(1) $G_z \cong M_{11}$, *the simple group of order* $7,920$.

(2) $\Lambda_{11}(z) \subseteq \mathrm{supp}(z)$ *and* G_z *acts triply-transitively on* $\Lambda_{11}(z)$. *If* $\beta \in \Lambda_{11}(z)$ *then* $G_{z,\beta} \cong \mathrm{PSL}(2, 11)$. *The orbits of* G_z *in* Ω *are* $\Phi_0 = \Lambda_{11}(z), \Phi_1 = \mathrm{supp}(z) \cap \Lambda_7(z)$ *and* $\Phi_2 = \mathrm{supp}(z + \mathbb{1})$ *of lengths* $12, 22$ *and* 66.

(3) The matrix of the Higman-Sims graph with respect to $(\Phi_i)_{0 \leqslant i \leqslant 2}$ *is*

$$\begin{bmatrix} 0 & 11 & 11 \\ 6 & 1 & 15 \\ 2 & 5 & 15 \end{bmatrix}.$$

Proof. (i) From the first part of Theorem (3.20) we have $w_{34}(H'_{22}) = 5,600 \not\equiv 0 \pmod{11}$. Therefore there exists $z \in W_{34}(H'_{22})$ such that 11 divides $|G_z|$. From (3.24) we infer that any element of G_z of order 11 fixes exactly one point in $\Lambda_{11}(z)$ and acts fixed-point-freely on $\Lambda_7(z)$. Since G_z does not fix any point in Ω by (3.24) it follows that G_z acts doubly-transitively on $\Lambda_{11}(z)$.

(ii) Let $\beta \in \Lambda_{11}(z)$. Then $|G_z : G_{z,\beta}| = 12$ and we obtain that $|G_{z,\beta}| = |G|/(12|G : G_z|) \geqslant 44,352,000/(12 \cdot 5,600) = 660$. On the other hand it follows from (1.3) that $G_{z,\beta}$ is isomorphic to a subgroup of $\mathrm{PSL}(2,11)$ whose order is 660. Hence $G_{z,\beta} \cong \mathrm{PSL}(2,11)$. Consequently G_z acts faithfully and triply-transitively on $\Lambda_{11}(z)$ and $G_z \cong M_{11}$ by [31]. Another consequence is $|G : G_z| = 5,600$ which implies that $Z' = W_{34}(H'_{22})$ is an orbit of G.

(iii) Since any element of G_z of order 11 fixes exactly one point in Ω it follows that $\Lambda_{11}(z) \subseteq \mathrm{supp}(z)$. From the properties of the Higman-Sims graph we infer that G_z acts transitively on $\mathrm{supp}(z) \cap \Lambda_7(z)$. Without loss we may assume that $\alpha \in \Lambda_{11}(z)$. Using the notation of (1.12) we then may conclude that for the endecad $e = \Delta(\alpha)z$ we have $B_3(e) \subseteq \mathrm{supp}(z + \mathbb{1})$. Since $G_{z,\alpha}$ acts transitively on $B_3(e)$, it now easily follows that G_z acts transitively on $\mathrm{supp}(z+\mathbb{1})$ of cardinality 66. The graph matrix in the assertion is now obtained simply by counting.

□

Remark. A vector $z \in Z'$ may be constructed explicitly as follows: Let e be an endecad such that e and any heptad $m \in \mathcal{M}'$ generate the same M_{22}-invariant subcode of the (shortened) Golay code of length 22. Then $z = \alpha + e + B_1(e) + B_5(e) \in Z'$ and $z + \mathbb{1} = (e + \Delta(\alpha)) + B_3(e)$, see (1.12).

It is now quite obvious how the G-orbits Z' and Y''_0 are linked by the Higman-Sims graph:

$$\begin{array}{rcl} Y''_0 & = & \{z + \Delta(\beta) \mid z \in Z' \text{ and } \beta \in \mathrm{supp}(z) \cap \Lambda_7(z)\} \text{ and} \\ Z' & = & \{y + \Delta(\gamma) \mid y \in Y''_0 \text{ and } \gamma \in \Lambda_{15}(y)\}. \end{array}$$

It is clear that we may construct a second orbit Y''_1 in $W_{42}(H''_{22})$ starting from Z' by making use of the G_z-orbit $\mathrm{supp}(z + \mathbb{1})$ instead of $\mathrm{supp}(z) \cap \Lambda_7(z)$.

(3.26) Proposition.
Let $z \in Z' = W_{34}(H'_{22})$ and let $\gamma \in \mathrm{supp}(z + \mathbb{1})$. Then $y = z + \Delta(\gamma) \in W_{42}(H''_{22})$. Denote by Y''_1 the G-orbit containing y. The following assertions hold.

(1) $G_y = G_{z,\gamma} \cong \Sigma_5$.

(2) $|Y''_1| = 369,600$.

(3) G_y *has exactly* 9 *orbits* $(\Psi_i)_{0\leqslant i\leqslant 8}$ *in* Ω *which are defined as follows:*

$$
\begin{array}{rcll}
\Psi_0 & = & \Lambda_{11}(z)\cap\Delta(\gamma); & |\Psi_0|=2 \textit{ and } \Psi_0\subseteq\Lambda_{11}(y).\\
\Psi_1 & = & \Lambda_{11}(z)\setminus\Psi_0; & |\Psi_1|=10 \textit{ and } \Psi_1\subseteq\Lambda_{11}(y).\\
\Psi_2 & = & \Lambda_7(z)\cap\mathrm{supp}(z)\cap\Delta(\gamma); & |\Psi_2|=5 \textit{ and } \Psi_2\subseteq\Lambda_7(y).\\
\Psi_3,\Psi_4 & \subseteq & \Lambda_7(z)\cap\mathrm{supp}(z)\setminus\Delta(\gamma) \textit{ such that} & |\Psi_3|=5 \textit{ and } |\Psi_4|=12;\\
 & & & \Psi_3\subseteq\Lambda_7(y) \textit{ and } \Psi_4\subseteq\Lambda_{11}(y).\\
\Psi_5 & = & \{\gamma\}=\Lambda_{15}(y). & \\
\Psi_6 & = & \mathrm{supp}(z+\mathbb{1})\cap\Delta(\gamma); & |\Psi_6|=15 \textit{ and } \Psi_6\subseteq\Lambda_7(y).\\
\Psi_7,\Psi_8 & \subseteq & \mathrm{supp}(z+\mathbb{1})\setminus\Delta(\gamma) \textit{ such that} & |\Psi_7|=20 \textit{ and } |\Psi_8|=30;\\
 & & & \Psi_7\subseteq\Lambda_7(y) \textit{ and } \Psi_8\subseteq\Lambda_{11}(y).
\end{array}
$$

(4) $\mathrm{supp}(y)=\Psi_1\cup\Psi_3\cup\Psi_4\cup\Psi_6$ *and* $\Lambda_7(y)=\Psi_2\cup\Psi_3\cup\Psi_6\cup\Psi_7$*.*

(5) The matrix of the Higman-Sims graph with respect to $(\Psi_i)_{0\leqslant i\leqslant 8}$ *is*

$$
\begin{bmatrix}
0 & 0 & 0 & 5 & 6 & 1 & 0 & 10 & 0\\
0 & 0 & 3 & 2 & 6 & 0 & 3 & 2 & 6\\
0 & 6 & 0 & 1 & 0 & 1 & 0 & 8 & 6\\
2 & 4 & 1 & 0 & 0 & 0 & 3 & 0 & 12\\
1 & 5 & 0 & 0 & 1 & 0 & 5 & 5 & 5\\
2 & 0 & 5 & 0 & 0 & 0 & 15 & 0 & 0\\
0 & 2 & 0 & 1 & 4 & 1 & 0 & 4 & 10\\
1 & 1 & 2 & 0 & 3 & 0 & 3 & 3 & 9\\
0 & 2 & 1 & 2 & 2 & 0 & 5 & 6 & 4
\end{bmatrix}.
$$

Proof. It follows from (3.25) and [7, Table 3], that $G_{z,\gamma}\cong\Sigma_5$. Using the character table of M_{11} we obtain that $G_{z,\gamma}$ has the nine orbits $(\Psi_i)_{0\leqslant i\leqslant 8}$ in Ω as described in assertion (3). From (3.25) we derive the graph matrix given in (5) and it follows that $\Lambda_{15}(y)=\{\gamma\}=\Psi_5$. Therefore $G_y=G_{z,\gamma}$ and the rest of the proposition easily follows. □

Since $w_{42}(H''_{22}) = 17,600 + 369,600$ by the first part of Theorem (3.20) only the remaining G-orbits in $W_{50}(H'_{22})$ have to be determined. We use for the construction of these orbits the same ideas as for the construction of Y''_1. At first we prove a general lemma.

(3.27) Lemma.
Let $x\in W_{50}(H'_{22})$ *and* $\lambda_i=|\Lambda_i(x)|$*. Then* $\lambda_7=\lambda_{15}$*.*

Proof. Counting the edges of the Higman-Sims graph between $\mathrm{supp}(x)$ and Ω yields the equations

$$
\begin{array}{rcccl}
1,100 & = & 50\cdot 22 & = & 7\lambda_7+11\lambda_{11}+15\lambda_{15}\\
 & & 100 & = & \lambda_7\ +\ \lambda_{11}\ +\ \lambda_{15}.
\end{array}
$$

It follows $\lambda_7=\lambda_{15}$. □

Next we consider the incidence structure

$$\mathcal{I} = (W_{42}(H''_{22}), W_{50}(H'_{22}), \mathrm{I})$$

where $\mathrm{I} = \{(y, x) \mid y \in W_{42}(H''_{22})$ and there exists a $\beta \in \Omega$ such that $x + y = \Delta(\beta)\}$. Note that $(x, y) \in \mathrm{I}$ implies that $x + y = \Delta(\beta)$ where $\beta \in \Lambda_7(y) \cap \Lambda_{15}(x)$.

It is obvious from the definition of $\mathcal{I}$ that G acts on $\mathcal{I}$ as a group of automorphisms. We know that G has exactly 2 orbits Y''_0 and Y''_1 in $W_{42}(H''_{22})$ of lengths $17,600$ and $369,600$ respectively. It is our goal to determine the G-orbits in $W_{50}(H'_{22})$ via the G-orbits in I.

(3.28) Proposition.
G has precisely 7 orbits in I:

$$\begin{aligned}
\mathrm{I}_{00} &= \{(y, y + \Delta(\beta)) \mid y \in Y''_0 \textit{ and } \beta \in \Phi_0(y)\},\\
\mathrm{I}_{01} &= \{(y, y + \Delta(\beta)) \mid y \in Y''_0 \textit{ and } \beta \in \Phi_3(y)\},\\
\mathrm{I}_{02} &= \{(y, y + \Delta(\beta)) \mid y \in Y''_0 \textit{ and } \beta \in \Phi_4(y)\},\\
\mathrm{I}_{10} &= \{(y, y + \Delta(\beta)) \mid y \in Y''_1 \textit{ and } \beta \in \Psi_2(y)\},\\
\mathrm{I}_{11} &= \{(y, y + \Delta(\beta)) \mid y \in Y''_1 \textit{ and } \beta \in \Psi_3(y)\},\\
\mathrm{I}_{12} &= \{(y, y + \Delta(\beta)) \mid y \in Y''_1 \textit{ and } \beta \in \Psi_6(y)\},\\
\mathrm{I}_{13} &= \{(y, y + \Delta(\beta)) \mid y \in Y''_1 \textit{ and } \beta \in \Psi_7(y)\}.
\end{aligned}$$

(Here we write $\Phi_i(y) = \Phi_i$ in the sense of (3.22) and $\Psi_i(y) = \Psi_i$ in the sense of (3.26) for the sake of clarity.)

The orbit lengths are

$$\begin{aligned}
|\mathrm{I}_{00}| &= 17,600 \cdot 1 = 17,600,\\
|\mathrm{I}_{01}| &= 17,600 \cdot 15 = 264,000,\\
|\mathrm{I}_{02}| &= 17,600 \cdot 35 = 616,000,\\
|\mathrm{I}_{10}| &= 369,600 \cdot 5 = 1,848,000,\\
|\mathrm{I}_{11}| &= 369,600 \cdot 5 = 1,848,000,\\
|\mathrm{I}_{12}| &= 369,600 \cdot 15 = 5,544,000,\\
|\mathrm{I}_{13}| &= 369,600 \cdot 20 = 7,392,000.
\end{aligned}$$

Proof. The assertion is a straightforward consequence of (3.22) and (3.26). Note that for $y \in W_{42}(H''_{22})$ we have $y + \Delta(\beta) \in W_{50}(H'_{22})$ if and only if $\beta \in \Lambda_7(y)$. ☐

An immediate consequence of (3.28) is that there are at most 7 G-orbits in $W_{50}(H'_{22})$. We know one of these G-orbits, X'_0, from (3.21). X'_0 corresponds uniquely to I_{00}, as follows from (3.21). From the first part of Theorem (3.20) we know that $w_{50}(H'_{22}) = 1,311,552$. We construct now the remaining G-orbits by considering some particular vectors.

(3.29) Proposition.
Let $y = (x(m) + \mathbb{1}) + \Delta(\alpha) \in Y''_0$ as defined in (3.22), let $\beta \in \Phi_3(y) = \Phi_3$ and let $x = y + \Delta(\beta)$. Set $X'_1 = \{xg \mid g \in G\}$. Then the following hold.

(1) $G_x = G_{y,\beta} \cong \mathrm{PSL}(2, 7)$.

(2) $|X_1'| = 264,000$.

(3) G_x *has precisely* 8 *orbits* $(\Theta_i)_{0\leqslant i\leqslant 7}$ *in* Ω.

$$\begin{array}{rclrcll}
\Theta_0 & = & \{\alpha\}, & |\Theta_0| & = & 1 & \textit{and} \quad \Theta_0 \subseteq \Lambda_7(x);\\
\Theta_1 & = & \operatorname{supp}(m), & |\Theta_1| & = & 7 & \textit{and} \quad \Theta_1 \subseteq \Lambda_{15}(x);\\
\Theta_2 & = & \operatorname{supp}(y)\cap\Delta(\beta)\setminus\{\alpha\}, & |\Theta_2| & = & 14 & \textit{and} \quad \Theta_2 \subseteq \Lambda_{11}(x);\\
\Theta_3 & = & B_1(m)\setminus\Delta(\beta), & |\Theta_3| & = & 28 & \textit{and} \quad \Theta_3 \subseteq \Lambda_{11}(x);\\
\Theta_4 & = & \{\beta\}, & |\Theta_4| & = & 1 & \textit{and} \quad \Theta_4 \subseteq \Lambda_{15}(x);\\
\Theta_5 & = & \Delta(\alpha)\setminus\operatorname{supp}(m)\setminus\{\beta\}, & |\Theta_5| & = & 14 & \textit{and} \quad \Theta_5 \subseteq \Lambda_{11}(x);\\
\Theta_6 & = & \Delta(\beta)\cap\operatorname{supp}(y), & |\Theta_6| & = & 7 & \textit{and} \quad \Theta_6 \subseteq \Lambda_7(x);\\
\Theta_7 & = & B_3(m)\setminus\Delta(\beta), & |\Theta_7| & = & 28 & \textit{and} \quad \Theta_7 \subseteq \Lambda_{11}(x).\\
\operatorname{supp}(x) & = & \Theta_0\cup\Theta_1\cup\Theta_2\cup\Theta_7. & & & &
\end{array}$$

(4) The matrix of the Higman-Sims graph with respect to $(\Theta_i)_{0\leqslant i\leqslant 7}$ *is*

$$\begin{bmatrix}
0 & 7 & 0 & 0 & 1 & 14 & 0 & 0\\
1 & 0 & 2 & 4 & 0 & 0 & 3 & 12\\
0 & 1 & 0 & 6 & 1 & 4 & 0 & 10\\
0 & 1 & 3 & 3 & 0 & 5 & 3 & 7\\
1 & 0 & 14 & 0 & 0 & 0 & 7 & 0\\
1 & 0 & 4 & 10 & 0 & 0 & 1 & 6\\
0 & 3 & 0 & 12 & 1 & 2 & 0 & 4\\
0 & 3 & 5 & 7 & 0 & 3 & 1 & 3
\end{bmatrix}.$$

Proof. We make use of the results of (3.22) : $G_y \cong A_7$ and $|G_y : G_{y,\beta}| = 15$, hence $G_{y,\beta} \cong \mathrm{PSL}(2,7)$. Using the information given in (3.22) we easily obtain that $G_{y,\beta}$ has the orbits $(\Theta_i)_{0\leqslant i\leqslant 7}$ in Ω. Counting the edges of the Higman-Sims graph yields the graph matrix in (4) and shows that every Θ_i is left invariant by G_x. It follows $G_x = G_{y,\beta}$, and hence $|X_1'| = 264,000$. The rest of the assertion is now obvious. ☐

Remark. It can be deduced from (3.21) and (3.22) that x and $x + \mathbb{1}$ are in the same G-orbit X_1'. This will follow also by simple numerical reasons when the proof of Theorem (3.20) is complete. It should be noted that the Higman-Sims graph induces on $\Theta_1 \cup \Theta_6$ the incidence graph of the projective plane of order 2, displaying in this way the well known isomorphy $\mathrm{PSL}(2,7) \cong \mathrm{PSL}(3,2)$ and $\mathrm{PGL}(2,7)$ acting as correlation group of the projective plane of order 2.

(3.30) Lemma.
Let $y = (x(m) + \mathbb{1}) + \Delta(\alpha) \in Y_0''$ *as defined in (3.22), let* $\gamma \in \Phi_4(y) = \Phi_4$ *and let* $x = y + \Delta(\gamma)$. *Set* $X_2' = \{xg \mid g \in G\}$. *Let* $a = |G_x : G_{y,\gamma}|$. *Then the following hold.*

(1) $G_{y,\gamma} \cong \Sigma_4 \overset{2|}{\wedge} \Sigma_3$.

(2) $|X_2'| = 616,000/a$.

(3) $G_{y,\gamma}$ has precisely 12 orbits $(\Xi_i)_{0\leqslant i\leqslant 11}$ in Ω:

$\Xi_0 = \{\alpha\}$, $\quad |\Xi_0| = 1$ *and* $\Xi_0 \subseteq \Lambda_7(x)$;
Ξ_1 *and* Ξ_2 *are the orbits of* $G_{y,\gamma}$ *in* m *such that* $|\Xi_1| = 4$ *and* $|\Xi_2| = 3$;
$\Xi_1 \cup \Xi_2 \subseteq \Lambda_{15}(x)$;
$\Xi_3 = \Delta(\gamma) \cap B_1(m)$, $|\Xi_3| = 12$ *and* $\Xi_3 \subseteq \Lambda_{11}(x)$;
Ξ_4 *and* Ξ_5 *are the orbits of* $G_{y,\gamma}$ *in* $B_1(m) \setminus \Delta(\gamma)$ *such that* $|\Xi_4| = 12$ *and* $|\Xi_5| = 18$;
Ξ_6 *and* Ξ_7 *are the orbits of* $G_{y,\gamma}$ *in* $\Delta(\alpha) \setminus m$ *such that* $|\Xi_6| = 12$ *and* $|\Xi_7| = 3$;
$\Xi_8 = \{\gamma\}$, $|\Xi_8| = 1$ *and* $\Xi_8 \subseteq \Lambda_{15}(x)$;
$\Xi_9 = \Delta(\gamma) \cap B_3(m)$, $|\Xi_9| = 4$ *and* $\Xi_9 \subseteq \Lambda_7(x)$;
Ξ_{10} *and* Ξ_{11} *are the orbits of* $G_{y,\gamma}$ *in* $B_3(m) \setminus (\gamma \cup \Delta(\gamma))$ *such that*
$|\Xi_{10}| = 12$ *and* $|\Xi_{11}| = 18$;
$\mathrm{supp}(x) = \Xi_1 \cup \Xi_3 \cup \Xi_7 \cup \Xi_8 \cup \Xi_{10} \cup \Xi_{11}$.

(4) The matrix of the Higman-Sims graph with respect to $(\Xi_i)_{0\leqslant i\leqslant 11}$ is

$$\begin{bmatrix}
0 & 4 & 3 & 0 & 0 & 0 & 12 & 3 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 3 & 3 & 0 & 0 & 0 & 0 & 3 & 3 & 9 \\
1 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 1 & 0 & 8 & 6 \\
0 & 1 & 0 & 0 & 3 & 3 & 5 & 0 & 1 & 0 & 3 & 6 \\
0 & 1 & 0 & 3 & 0 & 3 & 3 & 2 & 0 & 1 & 3 & 6 \\
0 & 0 & 1 & 2 & 2 & 2 & 4 & 1 & 0 & 2 & 4 & 4 \\
1 & 0 & 0 & 5 & 3 & 6 & 0 & 0 & 0 & 1 & 3 & 3 \\
1 & 0 & 0 & 0 & 8 & 6 & 0 & 0 & 1 & 0 & 0 & 6 \\
0 & 0 & 3 & 12 & 0 & 0 & 0 & 3 & 0 & 4 & 0 & 0 \\
0 & 3 & 0 & 0 & 3 & 9 & 3 & 0 & 1 & 0 & 3 & 0 \\
0 & 1 & 2 & 3 & 3 & 6 & 3 & 0 & 0 & 1 & 0 & 3 \\
0 & 2 & 1 & 4 & 4 & 4 & 2 & 1 & 0 & 0 & 2 & 2
\end{bmatrix}.$$

(5) $\Lambda_{15}(x) \cap \mathrm{supp}(x) = \Xi_1 \cup \Xi_8$ has 5 points. $\Lambda_{15}(x) \cap \mathrm{supp}(x + \mathbb{1}) = \Xi_2 \cup \Xi_4$ has 15 points. G_x has at least 2 orbits in $\Lambda_{15}(x)$.

(6) $|\Lambda_7(x)| = |\Lambda_{15}(x)| = 20$ and $|\Lambda_{11}(x)| = 60$.

Proof. (1) follows from (3.22) since $\gamma \in \Phi_4(y)$. (2) follows from (1). The orbits Ξ_i and the graph matrix are obtained by studying the action of $G_{y,\gamma} \cong \Sigma_4 \ {}^{2}\!\!\bigwedge \Sigma_3$ using (3.22). The remaining part of the assertion follows by inspection. $\square$

(3.31) Lemma.
Let $y \in Y_1''$ as defined in (3.26) and let $\delta \in \Psi_6(y) = \Psi_6$. Let $b = |G_x : G_{y,\delta}|$. Set $x = y + \Delta(\delta)$ and $X_3' = \{xg \mid g \in G\}$. Then the following hold.

(1) $G_{y,\delta} \cong D_8$.

(2) $|X_3'| = 5,544,000/b$.

(3) *$G_{y,\delta}$ has precisely* 26 *orbits in* Ω, 13 *in* $\mathrm{supp}(x)$ *and* 13 *in* $\mathrm{supp}(x+\mathbb{1})$.

(4) $x + \mathbb{1} \in X_3'$.

(5) $|\Lambda_{15}(x) \cap \mathrm{supp}(x)| = 6$ *and* $|\Lambda_{15}(x) \cap \mathrm{supp}(x + \mathbb{1})| = 8$, $|\Lambda_7(x)| = |\Lambda_{15}(x)| = 14$ *and* $|\Lambda_{11}(x)| = 72$. *G_x has at least* 2 *orbits in* $\Lambda_{15}(x)$.

Proof. It follows from (3.26) that $G_{y,\delta} \cong D_8$; hence (1) holds and because of $G_{y,\delta} \leqslant G_x$ we have also (2).

From (3.26) we also infer that $G_{y,\delta}$ has 13 orbits (of lengths $1,1,2,2,4,4,4,4,4,4,4,8,8$) in $\mathrm{supp}(x)$ and 13 orbits (with the same lengths) in $\mathrm{supp}(x+\mathbb{1})$. One easily checks that $\Lambda_7(x) \cap \mathrm{supp}(x) \neq \emptyset$ and $\Lambda_7(x) \cap \mathrm{supp}(x + \mathbb{1}) \neq \emptyset$. Therefore G_x has at least 2 orbits in $\Lambda_7(x)$. It now follows from (3.28) that G has exactly the orbits X_0', X_1', X_2' and X_3' in $W_{50}(H_{22}')$ and that every $x \in W_{50}(H_{22}')$ is in the same G-orbit as its complementary vector $x + \mathbb{1}$. One checks with the help of (3.26) that $\Lambda_7(x) \cap \mathrm{supp}(x)$ contains two $G_{y,\delta}$-orbits of length 4 each and that $\Lambda_{15}(x) \cap \mathrm{supp}(x)$ contains 3 $G_{y,\delta}$-orbits of lengths $1,1,4$. All remaining $G_{y,\delta}$-orbits in $\mathrm{supp}(x)$ are in $\Lambda_{11}(x)$. Since $x + \mathbb{1} \in X_3'$ we obtain (5). □

Remark. For the proof of (3.31) it is not necessary to compute completely the matrix of the Higman-Sims Graph with respect to the orbits of $G_{y,\delta}$; indirect arguments are sufficient.

As a side result of the proof of (3.31) we note the following:

(3.32) Proposition.
The G-orbits in $W_{50}(H_{22}')$ are X_0', X_1', X_2', X_3'. For all $x \in W_{50}(H_{22}')$ the complementary vectors x and $x + \mathbb{1}$ are in the same G-orbit.

It remains to determine the lengths of the orbits X_2' and X_3' and the structure of the corresponding point stabilizers.

(3.33) Proposition.
$|X_3'| = 924,000$ *and* $G_x \cong \mathrm{GL}(2,3)$ *for* $x \in X_3'$. *The center* $Z(G_x) \cong Z_2$ *is spanned by an involution with fixed-points, thus G_x is contained in the centralizer in* $G = \mathrm{HS}$ *of a unique involution which has* 10 *fixed-points in* $\mathrm{supp}(x)$ *and* 10 *fixed-points in* $\mathrm{supp}(x + \mathbb{1})$.

$G_x = G_{x+\mathbb{1}}$ *has exactly* 2 *orbits in* $\Lambda_{15}(x)$, *namely* $\Lambda_{15}(x) \cap \mathrm{supp}(x)$ *of length* 6 *and* $\Lambda_{15}(x) \cap \mathrm{supp}(x+\mathbb{1})$ *of length* 8, *correspondingly exactly* 2 *orbits in* $\Lambda_7(x)$, *namely* $\Lambda_7(x) \cap \mathrm{supp}(x)$ *of length* 8 *and* $\Lambda_7(x) \cap \mathrm{supp}(x + \mathbb{1})$ *of length* 6. *The orbit lengths of G_x in* $\Lambda_{11}(x) \cap \mathrm{supp}(x)$ *resp. in* $\Lambda_{11}(x) \cap \mathrm{supp}(x + \mathbb{1})$ *are* $4, 8, 24$.

Proof. Let $x \in X_3'$ as defined in (3.31). It follows from (3.28) and the known properties of Y_i'' and X_j' that G_x has the orbits $\Lambda_{15}(x) \cap \mathrm{supp}(x)$ of length 6 and $\Lambda_{15}(x) \cap \mathrm{supp}(x + \mathbb{1})$ of length 8 in $\Lambda_{15}(x)$. It follows that $b = |G_x : G_{y,\delta}| = 6$, therefore $|X_3'| = 924,000$ and $|G_x| = 48$. (Note that $\delta \in \Lambda_{15}(x) \cap \mathrm{supp}(x)$, hence $G_{y,\delta} = G_{x,\delta}$.)

An explicit computation of a vector $x \in X_3'$ which may also be carried out with GAP [10] verifies the remaining assertions. Note that an involution in G which is not fixed-point free has exactly 20 fixed-points by the character table of $G = \mathrm{HS}$, see the ATLAS [1]. □

(3.34) Proposition.
$|X_2'| = 123,200$ and $G_x \cong \Sigma_5 \,{}^{2}\!\!\wr\, \Sigma_3$ for $x \in X_2'$. G_x has exactly 2 orbits in $\Lambda_{15}(x)$, namely $\Lambda_{15}(x) \cap \operatorname{supp}(x)$ of length 5 and $\Lambda_{15}(x) \cap \operatorname{supp}(x + \mathbb{1})$ of length 15.

Proof. We may assume that $x \in X_2'$ is as defined in (3.30). The assertion is now easily obtained using (3.28), (3.30) and (3.32). □

Remark. It is not hard to show that in (3.34) the stabilizer G_x has the orbits

$$\begin{gathered}\Lambda_{15}(x) \cap \operatorname{supp}(x) \text{ of length } 5,\\ \Lambda_7(x) \cap \operatorname{supp}(x) \text{ of length } 15,\\ \Lambda_{11}(x) \cap \operatorname{supp}(x) \text{ of length } 30,\\ \Lambda_7(x) \cap \operatorname{supp}(x+\mathbb{1}) \text{ of length } 5,\\ \Lambda_{15}(x) \cap \operatorname{supp}(x+\mathbb{1}) \text{ of length } 15 \quad \text{and}\\ \Lambda_{11}(x) \cap \operatorname{supp}(x+\mathbb{1}) \text{ of length } 30.\end{gathered}$$

The matrix of the Higman-Sims graph with respect to these G_x-orbits (in the given order) is

$$\begin{bmatrix} 0 & 3 & 12 & 4 & 3 & 0 \\ 1 & 0 & 6 & 1 & 8 & 6 \\ 2 & 3 & 6 & 0 & 3 & 8 \\ 4 & 3 & 0 & 0 & 3 & 12 \\ 1 & 8 & 6 & 1 & 0 & 6 \\ 0 & 3 & 8 & 2 & 3 & 6 \end{bmatrix}.$$

One may check that this assertion agrees with Lemma (3.30).
The proof of Theorem (3.20) is now complete.

We conclude this discussion by a diagram (Figure 4) which displays the G-invariant relations between the orbits Z', Y_i'' and X_j' given by addition of adjacency vectors $\Delta(\xi), \xi \in \Omega$. The strokes indicate the G-invariant relations; the numbers at the end of the strokes indicate the length of the stabilizer orbit belonging to the relation orbit of G. Note that Y_1'' is joined to X_2' via the stabilizer orbit Ψ_2, see (3.26) and (3.28).

(3.35) Corollary.
The weight distribution of H_{23} is as described in the following table:

i	0/100	22/78	30/70	32/68	34/66	36/64	38/62
$w_i(H_{23})$	1	100	1,100	3,850	11,200	4,125	38,500
i	40/60	42/58	44/56	46/54	48/52	50	
$w_i(H_{23})$	92,400	968,000	347,600	485,100	600,600	3,283,456	

Proof. The assertion follows from the known structure of H_{23}/H_{21} together with (3.11) and (3.20). □

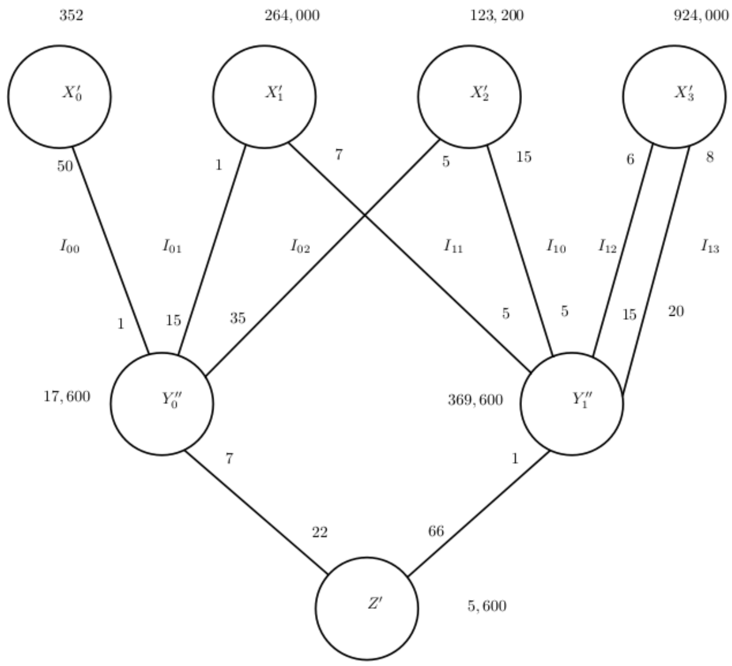


Figure 4: The G-invariant relations between Z', Y''_i and X'_j.

The weight enumerators of H_{77}, H'_{78} and H''_{78} finally can be determined by MacWilliams transformation. (These computations have been carried out first in 1980 by F.H Florian at the Rechenzentrum of Tübingen University using the ALDES program for computing with large numbers; nowadays it is easy to obtain the result by suitable computer algebra software like e.g. GAP [10].)

(3.36) Proposition.
The weight distributions of H_{77}, H'_{78} and H''_{78} are as given in Table 4.

Proof. The assertion follows from (3.35) and (3.20) by the MacWilliams transformation. □

Remark. From (2.7) it directly follows that there exist G-invariant linear forms f', f'' of H_{79} such that $xf' \neq 0 \neq xf''$ for all $x \in H_{78} \setminus H_{77}$ and all $x \in H_{22} \setminus H_{21}$. The results of Section 3 therefore imply that we may obtain by adding two "parity checks" a (binary) $(102, 78)$-code of minimum weight 8 and a $(102, 22)$-code of minimum weight 24.

4 A model of G. Higman's geometry

In this section we consider the embedding of the Higman vectors $x(m) = \alpha + m + B_1(m)$ in the code H_{23} (where m is a heptad of $\mathcal{W}_{22}$) and derive in this way a natural model of G. Higman's geometry [17] on which the Higman-Sims group $G = \mathrm{HS}$ acts as a group

i	$w_i(H_{77})$	$w_i(H'_{78}) = w_i(H''_{78})$
$0/100$	1	1
$8/92$	$119,625$	$137,225$
$10/90$	$3,351,040$	$7,231,840$
$12/88$	$262,194,275$	$511,741,475$
$14/86$	$10,460,595,200$	$20,997,046,400$
$16/84$	$321,165,892,575$	$642,104,180,575$
$18/82$	$7,309,692,544,000$	$14,620,696,059,200$
$20/80$	$127,793,807,058,995$	$255,580,729,090,995$
$22/78$	$1,748,088,230,732,800$	$3,496,191,224,323,200$
$24/76$	$19,020,111,451,577,775$	$38,040,223,036,760,175$
$26/74$	$166,791,619,843,340,800$	$333,583,215,539,666,400$
$28/72$	$1,191,810,146,845,445,325$	$2,383,620,193,904,285,325$
$30/70$	$7,002,911,342,735,052,800$	$14,005,823,013,894,187,520$
$32/68$	$34,096,837,242,289,671,850$	$68,193,674,589,734,420,650$
$34/66$	$138,453,825,199,499,980,800$	$276,907,649,363,395,385,600$
$36/64$	$471,402,307,704,520,229,125$	$942,804,613,467,381,809,925$
$38/62$	$1,351,845,015,778,272,153,600$	$2,703,690,046,024,936,460,800$
$40/60$	$3,277,357,630,135,281,557,850$	$6,554,715,226,694,274,576,090$
$42/58$	$6,737,425,031,963,982,617,600$	$13,474,850,114,631,510,262,000$
$44/66$	$11,772,688,854,024,011,418,750$	$23,545,377,636,355,278,743,550$
$46/64$	$17,516,850,935,961,851,443,200$	$35,003,701,987,289,528,723,200$
$48/52$	$22,222,175,416,214,614,898,750$	$44,444,350,658,167,367,673,150$
50	$24,054,370,909,850,203,084,800$	$48,108,742,023,087,188,141,952$

Table 4: The weight distributions of H_{77}, H'_{78} and H''_{78}.

of automorphisms. We thereby obtain an easy direct proof that G. Higman's simple group [17] is in fact isomorphic to the Higman-Sims group. Former proofs of this well known fact involve computer calculations [30], the use of the Leech lattice [7] or rather complicated combinatorial investigations, see [32, 33]; for another elementary proof of the isomorphy see [7]. The code theoretic construction of G. Higman's geometry also provides for a simple explanation of G. Higman's "natural correspondence" between the unordered pairs of points and quadrics, not induced by a bijection.

We shall consider all possible sums $x(m_1) + x(m_2)$ of Higman vectors. Recall that the M_{22}-orbits on the set of heptads of $\mathcal{W}_{22}$ are denoted by $\mathcal{M}'$ and $\mathcal{M}''$ and that the notation for the codes is chosen so that $x(m) \in H'_{22}$ if and only if $m \in \mathcal{M}'$. The additive structure of H_{23}/H_{21} leads to the following fact.

(4.1) Lemma.
Let $m_1, m_2 \in \mathcal{M}' \cup \mathcal{M}''$. Then the following hold.

(1) $x(m_1) + x(m_2) \in H_{21}$ if and only if $|\{m_1, m_2\} \cap \mathcal{M}'|$ is even.

(2) $x(m_1) + x(m_2) \in H_{22} \setminus H_{21}$ *if and only if* $|\{m_1, m_2\} \cap \mathcal{M}'| = 1$.

Proof. The assertions follow from (2.7). $\square$

More precise information is given by computing the weights:

(4.2) Lemma.
Let $m_1, m_2 \in \mathcal{M}' \cup \mathcal{M}''$ *and let* $d = w(m_1 m_2) = |\mathrm{supp}(m_1) \cap \mathrm{supp}(m_2)|$. *Then* $w = w(x(m_1) + x(m_2))$ *is given by the following table.*

d	0	1	2	3	4	7
w	70	60	50	40	30	0

Proof. The assertion easily follows from the definition of $x(m_i)$ by using the Leech triangle, [7, p.226]. (Observe that the heptads may be considered as shortened octads of the (extended) Golay code of length 24.) $\square$

The results in (4.2) become more symmetrical when we pass to the factor space H_{23}/H_1 of complementary vectors. For convenience of notation let $\widehat{x} = \{x, x + \mathbb{1}\} \in H_{23}/H_1$ for $x \in H_{23}$ and let $\widehat{x}(m) = \widehat{x(m)}$. As before in Section 3 the weight $w(\widehat{x})$ of $\widehat{x}$ is defined by $w(\widehat{x}) = \{w(x), w(x + \mathbb{1})\}$.

(4.3) Corollary.
Let $m_1, m_2 \in \mathcal{M}' \cup \mathcal{M}''$. *Then the weight* $\widehat{w} = w(\widehat{x}(m_1) + \widehat{x}(m_2))$ *as a function of* $d = w(m_1 m_2)$ *is given by the following table*

d	0	4	2	1	3	7
$\widehat{w}$	$\{30, 70\}$	$\{30, 70\}$	$\{50, 50\}$	$\{40, 60\}$	$\{40, 60\}$	$\{0, 100\}$

Proof. The assertion is essentially a restatement of (4.2) using an ordering according to (4.1). $\square$

In (4.3) we see that the cases $d = 0$ and $d = 4$ (resp. $d = 1$ and $d = 3$) yield the same weights. In the following we shall use the G-orbits structure known from Section 3 to explain this observation.

From Section 3 we know that G has exactly one orbit X in H_{23}/H_1 of elements of weights $\{30, 70\}$ of length $|X| = 1,100$ and that G has exactly 2 orbits in H_{23}/H_1 of elements of weight $\{40, 60\}$, one of them – say Y – of length $15,400$, the other of length $77,000$. Both orbits are in fact contained in H_{22}/H_1. Moreover, G has exactly 2 orbits in H_{22}/H_1 of elements of weight $\{50, 50\}$, one of them – say Z – of length $|Z| = 22,176$, the other of length $308,000$. All these orbits are also $\overline{G}$-invariant.

In addition we set $X' = X_0'/H_1$ and $X'' = X_0''/H_1$ where $X_0\prime$ and X_0'' are the G-orbits of Higman vectors such that $X_0' \subseteq H_{22}'$ and $X_0'' \subseteq H_{22}''$, the modulo notation $/H_1$ having the obvious meaning. Then $|X'| = |X''| = 176$. Note that G acts transitively on X' and X'' and that the stabilizer in G of an element of $X' \cup X''$ is isomorphic to $\mathrm{P\Sigma U}(3, 5^2)$. $\overline{G} \cong \mathrm{Aut}(G)$ acts transitively on $X' \cup X''$.

(4.4) Lemma.
Let $x_1, x_2 \in X' \cup X''$*. Then* $x_1 + x_2 \in X \cup Y \cup Z \cup \{0\}$*.*

Proof. In view of Corollary (4.3) we only have to show that $x_1 + x_2$ does not belong to the orbit of length $77,000$ of elements of weight $\{40, 60\}$ and not to the orbit of length $308,000$ of elements of weight $\{50, 50\}$. But this claim follows from (1.3) and (4.3), as $176(105 + 70) < 77,000$ and $176 \cdot 126 < 308,000$. ☐

As a consequence of (4.4) we may study the ternary relation $R = \{(x_1, x_2, x_1 + x_2) \mid x_1, x_2 \in X' \cup X''\} \subseteq (X' \cup X'')^2 \times (X \cup Y \cup Z \cup \{0\})$ in some detail. Of course, this relation is $\overline{G}$-invariant.

(4.5) Proposition. *(1)* $R' = \{(x_1, x_2, x_1 + x_2) \mid x_1, x_2 \in X'$ *and* $x_1 \neq x_2\}$ *is a* G*-orbit in* $(X')^2 \times Y$ *of length* $176 \cdot 175 = 30,800 = 2 \cdot 15,400$*.*

(2) $R'' = \{(x_1, x_2, x_1 + x_2) \mid x_1, x_2 \in X''$ *and* $x_1 \neq x_2\}$ *is a* G*-orbit in* $(X'')^2 \times Y$ *of length* $176 \cdot 175 = 30,800 = 2 \cdot 15,400$*.*

(3) X' *and* X'' *are interchanged by* $\overline{G}$*.*

Proof. The assertion follows from (4.4), (3.11) and (3.20). ☐

(4.6) Corollary.
G *acts doubly-transitively on* X' *and* X''*.*

Proof. G acts transitively on Y. From (4.5) it follows that G is 2-homogeneous on X' and X''. Therefore, since G is even, G is doubly-transitive. ☐

(4.7) Corollary.
There is a G*-invariant natural correspondence* $\Theta : X'^{\{2\}} \to X''^{\{2\}}$ *given by* $\{x_1, x_2\}\Theta = \{y_1, y_2\}$ *where* $y_1 + y_2 = x_1 + x_2$*.*

Proof. The assertion follows also from (4.5). ☐

Note that Θ is not induced by a bijection $X' \to X''$ since X' and X'' are nonisomorphic G-sets.

Another particular G-orbit in R can be used to construct a model of G. Higman's geometry.

(4.8) Proposition. *(1)* $R_1 = \{(x_1, x_2, x) \mid x_1 \in X', x_2 \in X'', x \in X$ *and* $x = x_1 + x_2\}$ *is a* G*-orbit in* $X' \times X'' \times X$ *of length* $176 \cdot 50 = 8,800 = 8 \cdot 1,100$*.* $R_2 = \{(x_1, x_2, x) \mid x_1 \in X'', x_2 \in X', x \in X$ *and* $x = x_1 + x_2\}$ *is a* G*-orbit in* $X'' \times X' \times X$ *of length* $176 \cdot 50 = 8,800 = 8 \cdot 1,100$*.*

(2) R_1 *and* R_2 *are interchanged by* $\overline{G}$*.*

Proof. The assertion follows from (4.4) and Section 3. ☐

(4.9) Corollary.
The stabilizer in G of an element $x \in X$ is isomorphic to the symmetric group Σ_8.

Proof. $|X| = 1,100$ implies $|G_x| = 40,320 = 8! = |\Sigma_8|$. The assertion now follows from (4.8). □

We are now in a position to define a model of G. Higman's geometry: Call the elements of X' *points*, the elements of X *conics* and the elements of X'' *quadrics*.

The G-invariant relation R_1 (or equivalently R_2) induces the following incidence structures by coordinate restriction:

$$\begin{array}{rcll} \mathcal{I}' & = & (X', X, \mathrm{I}_{ind}) & \text{(point-conic structure)} \\ \mathcal{I}'' & = & (X'', X, \mathrm{I}_{ind}) & \text{(quadric-conic structure)} \\ \mathcal{I} & = & (X', X'', \mathrm{I}_{ind}) & \text{(point-quadric structure)} \end{array}$$

where I_{ind} denotes in each case the incidence relation induced by R_1 (or R_2) in the obvious sense.

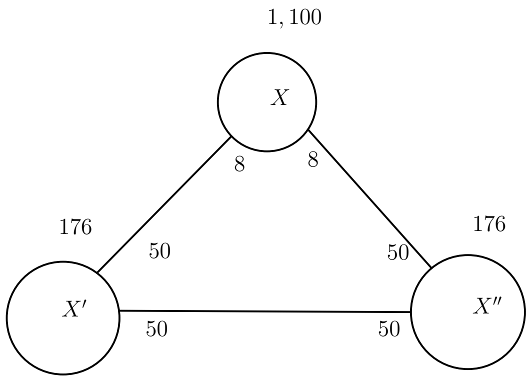
(4.10) Theorem. *(1) $\mathcal{I}'$ and $\mathcal{I}''$ are $2-(176, 8, 2)$ designs on which G acts as a group of automorphisms. $\overline{G}$ induces naturally an isomorphism between $\mathcal{I}'$ and $\mathcal{I}''$.*

(2) $\mathcal{I}$ is a symmetric $2-(176, 50, 14)$ design on which G acts as a group of automorphisms. $\overline{G}$ acts on $\mathcal{I}$ as a group of correlations interchanging points and quadrics.

(3) $(X', X'', X; R_1)$ provides for a model of G. Higman's geometry defined in [17]. G acts on this model as a group of automorphisms, $\overline{G}$ acts on $\mathcal{I}$ as a group of correlations interchanging points and quadrics and leaving the set of conics invariant.

Proof. Since G acts doubly-transitively on X' and X'' and transitively on X we immediately obtain that $\mathcal{I}'$ is a $2-(176, k', \lambda')$ design, that $\mathcal{I}''$ is a $2-(176, k'', \lambda'')$ design and that $\mathcal{I}$ is a $2-(176, k, \lambda)$ design. From (4.8) it follows that $k' = k'' = 8$ and that $k = 50$. The canonical equations for the design parameters now yield $\lambda' = 2 = \lambda''$ and $\lambda = 14$. It is clear from the definition that G acts on $\mathcal{I}', \mathcal{I}''$ and $\mathcal{I}$ as a group of automorphisms. It follows also from (4.8) that $\overline{G}$ induces an isomorphism between $\mathcal{I}'$ and $\mathcal{I}''$ and acts as a group of correlations (inducing a polarity). It is now straightforward to verify that the "axioms" of G. Higman's geometry are fulfilled, see [17]. (Note that the mapping Θ of (4.7) is intimately related to the "conic correspondence" required in G. Higman's property (vi) in an obvious way.) □

The assertion of (4.10) is illustrated by the following diagram, following the conventions used in Section 3.



(4.11) Corollary.
The Higman-Sims group $G = \mathrm{HS}$ *is isomorphic to the automorphism group of G. Higman's geometry.*

Proof. By (4.10) G is isomorphic to a subgroup of the automorphism group of G. Higman's geometry. Comparison of group orders now gives the result. □

Remark. It is plainly clear that – as a general principle of construction – the additive structure of a subquotient of a linear code left pointwise invariant by a group G of code automorphisms may be used to define incidence structures admitting G acting as a group of automorphisms.

5 Subgroups of $\mathbf{G = HS}$ given by the code $\mathbf{H_{23}}$

It has been shown by Conway [7] and Curtis [8] that the major part of the maximal subgroups of the maximal subgroups of the Mathieu group M_{24} may be described in terms of the binary Golay code of length 24. In this section we will show that the code H_{23} serves for this purpose as well in the case of the Higman-Sims group.

We start with the following general concept.

(5.1) Definition.
Let a group G act on a set X.

(1) A subgroup U of G is called an X*-subgroup* if and only if $U = G_x$ for some $x \in X$.

(2) The set of all X-subgroups of G is denoted by $\mathrm{sub}_X(G)$. sub_X is a union of conjugacy classes of subgroups of G.

(3) $\mathrm{sub}_X(G)$ is partially ordered under inclusion. A subgroup U of G is called X-*maximal* if and only if $U \neq G$ and $U \leqslant V \in \mathrm{sub}_X(G)$ implies $V \in \{U, G\}$.

the set of all X-maximal subgroups of G is denoted by $\max_X(G)$.

Note that $\max_X(G) = \emptyset$ if and only if G acts trivially on X.

In the following we retain the notation of the previous sections. In particular $G = \mathrm{HS}$ denotes the Higman-Sims simple group and $F = \mathbb{F}_2$. We consider the action of G on the FG-module H_{23}.

(5.2) Theorem.
Every H_{23}-maximal subgroup of G is conjugate to exactly one subgroup in the following list.

(a) $G_\alpha \cong M_{22}$ *of index* 100*;*

(b) $G_{\{\alpha,\beta\}} \cong \mathrm{P\Sigma L}(3,4)$ *of index* $1,100$ *where* α *and* β *are joined in the Higman-Sims graph;*

(c) $G_{\{\alpha,\gamma\}} \cong E_{16}\Sigma_6$ *of index* $3,850$ *where* α *and* γ *are not joined in the Higman-Sims graph;*

(d) $G_{x_{30}} \cong \Sigma_8$ *of index* $1,100$ *where* $x_{30} \in W_{30}(H_{23})$*, a conic stabilizer in G. Higman's geometry;*

(e) $G_{x_{36}} \cong 2^6\mathrm{GL}(3,2)$ *of index* $4,125$ *where* $x_{36} \in W_{36}(H_{23})$*;*

(f) $G_{x_{40}} \cong Z_2 \times \mathrm{P\Gamma L}(2,9)$ *of index* $15,400$ *where* $x_{40} \in 40_1$*, the centralizer in* G *of a fixed-point free involution;*

(g′) $G_{x'_{34}} \cong M_{11}$ *of index* $5,600$ *where* $x'_{34} \in W_{34}(H'_{22})$*;*

(g″) $G_{x''_{34}} \cong M_{11}$ *of index* $5,600$ *where* $x''_{34} \in W_{34}(H''_{22})$*;*

(h′) $G_{x'_{50}} \cong \mathrm{PSU}(3,5^2)$ *of index* 352 *where* $x'_{50} \in X'_0$*;*

(h″) $G_{x''_{50}} \cong \mathrm{PSU}(3,5^2)$ *of index* 352 *where* $x''_{50} \in X''_0$*.*

Proof. The assertion of the theorem follows essentially from (3.11), (3.20), (3.21) and its proofs. Some arguments of the omitted proof of (3.13) are also required concerning the orbits in Ω of the stabilizers $G_x, x \in H_{22}$. Since these arguments are elementary and tedious we omit the details. □

Note that $\overline{G} \cong \mathrm{Aut}(G)$ fuses the conjugacy classes (g′) and (g″), resp. (h′) and (h″).

It can be shown that all H_{23}-maximal subgroups of $G = \mathrm{HS}$ are in fact maximal subgroups of G with exception of the cases (h′) and (h″). The H_{23}-maximal subgroups of G of types (h′) and (h″) are contained with index 2 in maximal subgroups isomorphic to $\mathrm{P\Sigma U}(3,5^2)$ as easily follows from Section 4. From (3.21) we know that these maximal subgroups are H_{23}/H_1-groups. More precisely we have the following result.

(5.3) Theorem.
Every H_{23}/H_1-maximal subgroup of G is either H_{23}-maximal or a maximal subgroup of index 176 *conjugate to a point-stabilizer or a quadric-stabilizer in G. Higman's geometry.*

Proof. The assertion follows from (5.2), (3.20), (3.21) and Section 4, in particular Theorem (4.10). □

It is not difficult to show that the subgroups of types (a) ... (g$''$) are in fact maximal subgroups of G. Of course, this follows from Magliveras [25] where reference is given to his unpublished dissertation [24]. We give an example for an independent direct argument.

(5.4) Lemma.
Let $x \in W_{30}(H_{23})$. Then $G_x \cong \Sigma_8$ is a maximal subgroup of G.

Proof. Suppose $G_x < H \leqslant G$. Then G_x has just 2 orbits in Ω: $\mathrm{supp}(x) = \Lambda_8(x)$ and $\Lambda_6(x) = \mathrm{supp}(x + \mathbb{1})$, see (3.10). So we conclude that H acts transitively on Ω.

It follows from (3.10) that $(G_x)_\beta$ has orbits of length 8 and 14 in $\Delta(\beta)$ if $\beta \in \Lambda_8(x)$ and that $(G_x)_\gamma$ has orbits of length 16 and 6 in $\Delta(\gamma)$ if $\gamma \in \Lambda_6(x)$. Moreover, $(G_x)_\gamma$ contains a Sylow 7-subgroup of G for $\gamma \in \Lambda_6(x)$. We easily conclude that H_ξ acts primitively on $\Delta(\xi)$ for $\xi \in \Omega$. By a theorem of Wielandt [38, 31.1], the subgroup H_ξ acts 2-transitively on $\Delta(\xi)$ (and it follows that H_ξ has the orbits $\{\xi\}, \Delta(\xi)$ and $\Delta \circ \Delta(\xi) = \Delta_2(\xi)$ in Ω) since M_{22} has no proper subgroup acting doubly-transitively on 22 points. Hence $H = G$. $\square$

It is a result of Magliveras [24, 25] that G has only two conjugacy classes of maximal subgroups which are not H_{23}/H_1-maximal:

(i) The centralizer of an involution with fixed-points (induced by an elation in $\mathrm{PSL}(3,4) = M_{21}$), of index $5,775$ with structure $2^6\Sigma_5$, acting intransitively on Ω with two orbits of lengths 20 and 80.

(ii) The normalizer of the cyclic group generated by an element of order 5 whose centralizer in G is of order 300, of index $36,960$ and acting transitively on Ω with a system of imprimitivity of type 20^5, in ATLAS notation: $5 : 4 \times S_5$. see [1].

We recall that by Proposition (3.33) the groups in class (i) contain H_{23}-subgroups isomorphic to $\mathrm{GL}(2,3)$ with index 160.

It is easy to show that the groups in the class (i) are H_{78}-maximal subgroups of G. Note that H_{79} is the inverse image under v of $H_1 = \langle \mathbb{1} \rangle$ and that $H_{22} = \mathrm{Im}\, v \leqslant H_{79}$, hence a forteriori every intransitive subgroup of G fixes a vector in $H_{79} \setminus H_1$.

References

[1] ATLAS of finite groups by J. H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson. with computational assistance from J.G. Thackray. Clarendon Press, Oxford 1985.

[2] An ATLAS of Brauer Characters by C. Jansen, K. Lux, R. Parker, R. Wilson. Clarendon Press, Oxford 1995.

[3] Brauer, R.D. : On the connections between the ordinary and the modular characters of groups of finite order. *Ann. Math.* 42, 926-935 (1941).

[4] Brouwer, A. E. and van Eijl, C.A. : On the p-rank of the adjacency matrices of strongly regular graphs. *J. Alg. Combinatorics*, vol. 1, 329-346 (1992).

[5] Brouwer, A. E. “Bounds on linear Codes” in : V.S. Pless and W.C. Huffman (Eds.) Handbook of Coding Theory, pp 295-461, Elsevier 1998.

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

[7] Conway, J.H. : Three lectures on Exceptional Groups. In : Finite Simple Groups (Powell and Higman editors), Academic Press 1971.

[8] Curtis, R.T. : The maximal subgroups of M_{24}. *Math. Proc. Camb. Phil. Soc.* 81, 185-192 (1977).

[9] Dembowski, P. : Finite Geometries, Springer 1968.

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

[11] Griess, R.L. : A sufficient condition for a finite group of even order to have a non-trivial Schur multiplicator. *Notices A.M.S.* 17, 644 (1970).

[12] Haemers, Willem H., Peeters, René and van Ruckevorsel, Jeroem M. : Binary codes of strongly regular graphs. *Designs Codes and Cryptography* 17, 187-209 (1999).

[13] Hafner, P. R. : On the graphs of Hoffman-Singleton and Higman-Sims, *Electronic Journal of Combinatorics* 11 (2004) # R77

[14] Higman, D.G. : Primitive rank 3 groups with a prime subdegree. *Math. Z.* 91, 70-86 (1966).

[15] Higman, D.G. : Intersection Matrices for finite permutation groups. *J. Algebra* 6, 22-42 (1967).

[16] Higman, D.G. and Sims, C.C. : A simple group of order $44,352,000$. *Math. Z.* 105, 110-113 (1968).

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

[18] Huppert, B. : Darstellungstheorie endlicher Gruppen III. Vorlesungsausarbeitung, Universität Mainz 1974.

[19] James, G.D. : The modular characters of the Mathieu groups. *J. Algebra* 27, 57-111 (1973).

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

[21] Loebich, N. : Rang 3-Gruppen mit dreiecksfreiem Graphen. Wissenschaftliche Arbeit, Universität Tübingen, 1981.

[22] Lüneburg, H. : Transitive Erweiterungen endlicher Permutationsgruppen. Lecture Notes in Mathematics 84, Springer 1969.

[23] MacWilliams, F.J. and Sloane, N.J.A. : The Theory of Error-Correcting Codes, I and II. North-Holland 1977.

[24] Magliveras, S.S. : The subgroup structure of the Higman-Sims simple group. Ph.D. Thesis, Birmingham University, England 1970.

[25] Magliveras, S.S. : The subgroup structure of the Higman-Sims simple group. *Bulletin A.M.S.* 77, 535-539 (1971).

[26] Mazet, P. : Sur le mutiplicateur de Schur du group de Mathieu M_{22}. *C.R. Acad. Sci. Paris Sér. A* 289, 659-661 (1979).

[27] McKay, J. and Wales, D. : The multiplier of the Higman-Sims simple group. *Bull. London Math. Soc.* 3, 283-285 (1971).

[28] Pless, V. : Power Moment Identities on Weight distributions in Error Correcting Codes. *Information and Control* 6, 147-152 (1963).

[29] Rudvalis, A. : Characters of the Covering Group of the Higman-Sims Group. *J. Algebra* 33, 135-143 (1975).

[30] Sims, C.C. : On the isomorphism of two groups of order $44,352,000$. In: Theory of Finite Groups, a Symposium, ed. by R. Brauer and C. Sah. W.A. Benjamin 1969.

[31] Sims, C.C. : Computational Methods in the study of permutation groups. In: Computational problems in abstract algebra, John Leech (Editor). Pergamon Press 1970.

[32] Smith, M.S. : A Combinatorial Configuration Associated with the Higman-Sims Simple Group. *J. Algebra* 41, 175-195 (1976).

[33] Smith, M.S. : On the isomorphism of two groups of order $44,352,000$. *J. Algebra* 41, 172-174 (1976).

[34] Stein, W.A. et al. : Sage Mathematics Software (Version 6.4.1), The Sage Development Team, 2014. http://www.sagemath.org

[35] Thackray, J. : private Communication, 1980.

[36] Thompson, J. G. : Vertices and Sources. *J. Algebra* 6, 1-6 (1967).

[37] Tonchev, V.D. : Binary codes derived from the Hoffman-Singleton and Higman-Sims graphs. *IEEE Transactions of Information Theory* 43 (3), 1021-1025 (1997).

[38] Wielandt, H. : Finite Permutation Groups. Academic Press 1964.

[39] Witt, E. : Die 5-fach transitiven Gruppen von Mathieu. *Abh. Math. Sem. Univ. Hamb.* 12, 256-264 (1938).

[40] Witt, E. : Über Steinersche Systeme. *Abh. Math. Sem. Univ. Hamb.* 12, 265-275 (1938).