JOURNAL OF ALGEBRA **67**, 415–435 (1980)

Codes with Prescribed Permutation Group

WOLFGANG KNAPP AND PETER SCHMID

Mathematisches Institut der Universität Tübingen, Auf der Morgenstelle 10, D-7400 Tübingen 1, West Germany

Communicated by B. Huppert

Received October 20, 1978

In this paper a program is proposed how to determine codes with given transitive permutation group. The approach is module theoretic, based on a study of monomial actions and projective representations. Some highly transitive groups are discussed in detail.

There appear slightly different concepts of (linear) codes in the literature. Following Ward [16] and Rasala [11] a code over some commutative ring F with unity will be a triple (V, B, C), where V is a free F-module of finite rank with basis B and submodule C. By convention we then call C a code having ambient space V and ambient basis B. F is the alphabet of C, the rank n of V its length, and C is an (n, k)-code if C is free of rank k. (In this paper F will always be a field.)

The Hamming weight of a vector (word) in V is the cardinality of its support with respect to the given basis. The minimum weight of a code C is a measure for its error-correcting capability. Hence morphisms between codes should preserve the Hamming weight. This leads to the definition: A morphism $(V, B, C) \to (V', B', C')$ of codes over F is 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 $C\mu = C'$.

$ML(C)$ denotes the group of all (code) automorphisms from (V, B, C) onto itself, the *monomial linear group* of C. ($ML(C)$ can be represented, with respect to B, by monomial matrices.) Let $B = (e_i)$, $i \in \Omega = \{0,..., n-1\}$. Every $\mu \in ML(C)$ determines a permutation $\bar{\mu}$ on Ω by $e_i\mu \in \langle e_{i\bar{\mu}}\rangle$. The map $\mu \mapsto \bar{\mu}$ is an epimorphism of $ML(C)$ onto a subgroup $PML(C)$ of the symmetric group on Ω. $PML(C)$ is called the *permutation group* of C. C admits a permutation group G on Ω if G is a subgroup of $PML(C)$. The elements of $\ker(\mu \mapsto \bar{\mu})$ are the diagonal automorphisms of C.

Observe that the transitivity behaviour of the permutation group of a code is a measure for its homogeneity. Codes having (multiply) transitive permutation groups have good error-correcting properties and provide for powerful decoding methods. Actually there are many interesting codes with a

0021-8693/80/120415–21\$02.00/0

481/67/2-11

multiply transitive permutation group. For instance the extended quadratic residue (QR-) code of length $p+1$, p an odd prime, admits $PSL(2, p)$. (A generalization to symplectic groups can be found in Ward [16].) The 5-transitive Mathieu groups $\mathfrak{M}_{12}$ and $\mathfrak{M}_{24}$ are the permutation groups of the extended ternary and binary Golay codes, respectively. The binary Reed–Muller codes of length 2^m admit the affine groups $\mathrm{Aff}(2^m, 2)$. (A general reference for this is MacWilliams and Sloane [9].)

For theoretical and practical reasons one may ask for a method to determine all codes with prescribed permutation group. In attacking this problem we show, via some kind of Krull–Schmidt decomposition for codes, that it suffices to construct those codes whose diagonal automorphisms are scalar multiplications (see Section 1). Every diagonal automorphism of a nontrivial code C is scalar, for instance, if $PML(C)$ is primitive (Theorem 1.3). In this case we have a central group extension

$$(*) \qquad F^{\#} \rightarrowtail ML(C) \twoheadrightarrow PML(C),$$

where $F^{\#}$ denotes the multiplicative group of the field F.

A group E is said to act (monomially) on a code (V, B, C) if there is given a homomorphism $E \rightarrow ML(C)$. E induces a permutation group G on Ω, the index set of B. In the situation (*) we obtain a projective representation of G on V which lifts back to the given (ordinary) representation of E on V. Under suitable assumptions, this projective representation can be lifted also by stem covers of G ("Darstellungsgruppen" in Schur's terminology). Moreover, if G acts transitively on Ω and E_0 is the subgroup of E fixing $U = \langle e_0 \rangle$, then the monomial action of E on V can be replaced by that induced on $U^E = U \otimes_{E_0} FE$ (Proposition 2.1).

This will serve as a principle for constructing codes admitting a given primitive permutation group (G, Ω): Suppose E is a stem cover of G and E_0 is the inverse image in E of a point stabilizer. Then the FE-submodules of all induced modules U^E, U being a 1-dimensional FE_0-module, yield a complete list of codes over F admitting (G, Ω), provided $\mathrm{Ext}(G/G', F^{\#}) = 0$ (Theorem 3.1). This condition is fulfilled, for instance, if F is algebraically closed or $G = G'$ is perfect. In general one can start with an algebraically closed field of scalars, which is appropriate also for module theoretic reasons. Then one has to find, for any submodule C of U^E, the smallest fields of realization.

To illustrate the program we will determine all codes admitting alternating groups or Mathieu groups. It turns out that the alternating groups $\mathfrak{A}_n$ of degree $n \geqslant 7$ occur only in the permutation group of the repetition code and its dual (Theorem 4.4). Here we make use of Schur's work [12] on the multipliers of alternating groups. The Mathieu groups only leave invariant Golay codes, besides the repetition code and its dual. This depends on results of Burgoyne and Fong [2] (and P. Mazet [18]) on the Schur multipliers of the Mathieu groups.

The paper is concluded by a discussion of QR-codes. We show that the extended QR-codes (of length $p+1$) are characterized by the property that they admit $PSL(2, p)$ but not $PGL(2, p)$ (Theorem 6.2). It is conjectured that the (full) permutation group G of such a code is precisely $PSL(2, p)$ provided $p > 23$. We can prove, at least, that G is a proper subgroup of $\mathfrak{A}_{p+1}$ if $p > 5$. This answers a conjecture by Rasala [11] to the affirmative. If $p > 23$ and $G \neq PSL(2, p)$, then G would be an "unknown" simple group being 4-transitive on $p+1$ letters (Theorem 6.4).

1. Indecomposable Codes

Let C be a code over F with ambient basis $B = (e_i)$, $i \in \Omega = \{0, \ldots, n-1\}$. If $B' \subseteq B$ then $C' = C \cap \langle B' \rangle$ is regarded as a code with ambient space $\langle B' \rangle$ and ambient basis B'. C is called decomposable if B can be partitioned into at least two nonempty subsets B_j such that $C = \bigoplus C_j$, where $C_j = C \cap \langle B_j \rangle$, and indecomposable otherwise. There is a unique partition of B into subsets B_j such that $C = \bigoplus C_j$ and each C_j is indecomposable (Krull–Schmidt).

The decomposition of C into its indecomposable components C_j can be studied from a different point of view. Call a nonzero vector $v \in C$ indecomposable if v is not the sum of two nonzero vectors in C with disjoint supports. Every vector is a sum of indecomposables which, however, are not uniquely determined. If d is the minimum weight of C, then any nonzero vector in C of weight at most $2d-1$ is indecomposable. (Recall that the weight of $v = \sum a_i e_i$ is the cardinality of $\operatorname{supp}(v) = \{i \mid i \in \Omega,\ a_i \neq 0\}$.)

Define the binary relation $\Lambda = \Lambda_C$ on Ω to be the set of all pairs $(i, j) \in \Omega^2$ such that there is an indecomposable $v \in C$ having i, j in its support. Let $\bar{\Lambda} = \bar{\Lambda}_C$ be the smallest equivalence relation on Ω containing Λ. Then $(i, j) \in \bar{\Lambda}$ if and only if $i = j$ or there are indecomposable $v_k \in C$ $(1 \leqslant k \leqslant m)$ such that $i \in \operatorname{supp}(v_1)$, $j \in \operatorname{supp}(v_m)$, and $\operatorname{supp}(v_{k-1}) \cap \operatorname{supp}(v_k) \neq \varnothing$ for $2 \leqslant k \leqslant m$. Note that Λ_C and $\bar{\Lambda}_C$ are invariant under the automorphism group $ML(C)$, i.e., under $PML(C)$.

(1.1) Lemma. *Let (B_j) be the partition of B corresponding to the equivalence classes of $\bar{\Lambda}_C$ and $C_j = C \cap \langle B_j \rangle$. Then $C = \bigoplus C_j$ is the decomposition of C into its indecomposable components.*

Proof. If $v \in C$ is indecomposable, $\operatorname{supp}(v)$ is contained in just one equivalence class of $\bar{\Lambda}$. Since any $v \in C$ is a sum of indecomposable vectors in C, it is enough to show that each C_j is indecomposable. Assume $B_j = B' \cup B''$ (disjoint, $B' \neq \varnothing \neq B''$) and $C_j = (C_j \cap \langle B' \rangle) \oplus (C_j \cap \langle B'' \rangle)$.

Since B_j corresponds to an equivalence class of $\bar{\Lambda}$, there must be an indecomposable vector $v \in C_j$ such that supp(v) meets the index sets of both B' and B'', which is impossible. ∎

The indecomposable components of C can be related to the structure of $ML(C)$. To explain this we introduce a further equivalence relation $\Delta = \Delta_C$ on Ω. Let $(i, j) \in \Delta$ if each diagonal automorphism of C multiplies both e_i and e_j with the same scalar. Of course, if $F = \mathbb{F}_2$ then Δ is the universal relation on Ω. Thus Δ is interesting only when $F \neq \mathbb{F}_2$.

(1.2) THEOREM. *Suppose $F \neq \mathbb{F}_2$. Then $\bar{\Lambda}_C$ and Δ_C coincide. In particular, C is indecomposable if and only if every diagonal automorphism of C is a scalar multiplication.*

Proof. From Lemma 1.1 it follows $\Delta \subseteq \bar{\Lambda}$, because of $|F| > 2$. To prove the converse let (B'_j) be the partition of B associated to the equivalence classes of Δ. Let $v \in C$. Then there are unique $v_j \in \langle B'_j \rangle$ such that $v = \sum v_j$. We claim that all v_j belong to C. Define $m_v = \max\{j \mid v_j \neq 0\}$, $m_0 = 0$. The claim is obvious if $m_v \leqslant 1$. Let $m_v = m > 1$. Fix j between 1 and $m - 1$. By definition of Δ there exists a diagonal automorphism x of C such that $v_k x = a_k v_k$ $(1 \leqslant k \leqslant m)$ and $a_j \neq a_m$. Then

$$w = a_m v - vx = \sum_{k=1}^{m-1} (a_m - a_k)\, v_k$$

is in C and satisfies $m_w \leqslant m - 1$. By induction $w_j = (a_m - a_j)\, v_j \in C$, hence $v_j \in C$. Also $v_m = v - \sum_{k=1}^{m-1} v_k \in C$, as claimed.

We have established that, for every indecomposable $v \in C$, supp(v) is completely contained in some equivalence class of Δ. Therefore $\Lambda \subseteq \Delta$, hence also $\bar{\Lambda} \subseteq \Delta$. ∎

We now give a sufficient condition for a code to be indecomposable in terms of its permutation group.

(1.3) THEOREM. *If C is a nontrivial code such that $PML(C)$ is primitive, then C is indecomposable and every diagonal automorphism of C is scalar.*

Proof. The minimum weight d of C is at least 2, by transitivity of $G = PML(C)$. Consequently $\bar{\Lambda}$ is not the diagonal in Ω^2. Since $\bar{\Lambda}$ is G-invariant and G is primitive, it follows that $\bar{\Lambda}$ is the universal relation on Ω. By (1.1) C is indecomposable. Finally apply Theorem 1.2. ∎

Observe that there are decomposable codes having a transitive permutation group, e.g., $V = F^4$, $C = \langle 1010 \rangle \oplus \langle 0101 \rangle$. Here C is cyclic. However, we have the following criterion.

(1.4) PROPOSITION. *Let C be cyclic. If C contains an indecomposable vector v such that there are i, j in* $\operatorname{supp}(v)$ *with $i-j$ coprime to the length n of C, then C is indecomposable.*

Proof. Straighforward. ∎

The structure of a code C is completely determined by the structure of its indecomposable components. So, in principle, we may restrict our attention to the study of indecomposable codes.

2. ACTIONS ON CODES AND INDUCED MODULES

Let (V, B, C) be an (n, k)-code over F, $B=(e_i)$, $i \in \Omega=\{0,\ldots, n-1\}$. Suppose we have a group homomorphism $\varphi: E \to ML(C)$. Then E is said to act (monomially) on C (via φ). Composing φ and the natural epimorphism from $ML(C)$ onto $PML(C)$ yields a map $E \to PML(C)$ whose image G is a permutation group on Ω.

Clearly V is an FE-module via φ, with invariant subspace C. Assume E (i.e., G) is transitive on Ω. Let E_0 be the largest subgroup of E leaving invariant the 1-dimensional subspace $U=\langle e_0\rangle$. Then, for each $i \in \Omega$, there exists $x_i \in E$ mapping U onto $\langle e_i\rangle$. Hence

$$V=\bigoplus Ux_i$$

is an FE-module induced by the FE_0-module U.

(2.1) PROPOSITION. *Assume E acts on (V, B, C) and is transitive on Ω. Let E_0 be the subgroup of E leaving invariant $U=\langle e_0\rangle$ and let $V'=U \otimes_{E_0} FE$. Choose a right transversal (x_i) to E_0 in E indexed such that $e_0 x_i \in \langle e_i\rangle$, say $e_o x_i=a_i e_i$. Let $e_i'=e_o \otimes x_i$ and $B'=(e_i')$. Then the linear map $\mu: V' \to V$ given by $e_i' \mapsto a_i e_i$ is a monomial isomorphism $(V', B') \to (V, B)$ of FE-modules, and the preimage C' of C represents a code isomorphic to C.*

Proof. It is immediate that $B'=(e_i')$ is a basis for V'. E operates on V' by

$$e_i' x=(e_0 \otimes x_i)\, x=c_i e_0 \otimes x_j=c_i e_j',$$

where $x_i x=\bar{x}_i x_j$ with $\bar{x}_i \in E_0$ *and* $e_o \bar{x}_i=c_i e_0$. Since also

$$(a_i e_i)\, x=(e_o x_i)\, x=c_i e_0 x_j=c_i(a_j e_j),$$

μ is an FE-isomorphism. We are done. ∎

Identifying V and V' in the situation of Lemma 2.1 is now justified. The code C can be represented as a submodule of the induced module $U^E = U \otimes_{E_0} FE$, $U = \langle e_0 \rangle$, equipped with a basis $B = (e_i)$, where $e_i = e_o \otimes x_i$ for some right transversal (x_i) to E_0 in E, choosing $x_0 = 1$. This notation is fixed in the sequel.

(2.2) *Remark.* In theory, we may construct all codes over F admitting a transitive permutation group (G, Ω) as follows: Consider any group extension $A \rightarrowtail E \twoheadrightarrow G$ with A abelian. Let E_0 be the inverse image in E of a point stabilizer G_0. Inducing up to E all 1-dimensional FE_0-modules U we obtain all (transitive) monomial representations of E with permutation group (G, Ω). The codes admitting (G, Ω) occur as submodules of all $V = U^E$.

By a monomial action of an extension E of a (transitive) permutation group (G, Ω) we always mean a monomial representation of E inducing (G, Ω).

In general, it is fairly hopeless to construct all required group extensions of G. However, in order to obtain all those codes which are indecomposable we have to consider only the case where A is central in E and isomorphic to a subgroup of $F^{\#}$ (Theorem 1.2). Moreover, any supplement to A in E will leave invariant the same subspaces. When F is finite we may take minimal supplements yielding central Frattini extensions of G. There exists, to any finite group G and any finite field F, a unique maximal (central) Frattini extension $A_F \rightarrowtail G_F \twoheadrightarrow G$, with A_F of exponent dividing $|F^{\#}|$, having any other such extension of G as epimorphic image over G (i.e., inducing the identity on G). This is a slight generalization of a classical result by Gaschütz [5]. We omit the details. In Section 3 we will see that one can use without loss stem covers of G instead.

We present some basic facts concerning monomial actions and induced modules. Throughout let E be a finite extension of the transitive permutation group (G, Ω) and $V = U^E$ for some 1-dimensional FE_0-module U, the basis $B = (e_i)$ of V indexed by Ω. (If W is an FH-module and α is (or induces) an automorphism of H, then W_α is the vector space W with module structure $w \circ x = wx^\alpha$ for $w \in W$, $x \in H$.)

(2.3) Lemma. *Assume G acts 2-transitively on Ω. Then the F-dimension of* $\mathrm{End}_E(V)$ *is at most* 2, *and it is* 1 *if and only if the restriction W of U to $H = E_0 \cap E_0^{y^{-1}}$, for any $y \in E - E_0$, is not isomorphic to W_y.*

Proof. Apply Frobenius reciprocity and Mackey decomposition. ∎

Observe that the F-algebra $\mathrm{End}_E(V)$ is commutative if its dimension is at most 2. If $\dim_F \mathrm{End}_E(V) = 1$, V is absolutely indecomposable such that no proper submodule is an epimorphic image of V. In case $V = F^E$ is a permutation module, i.e., U is the trivial FE_0-module F, and G acts 2-transitively, $\mathrm{End}_E(V)$ always is of F-dimension 2.

Write $e_i = e_0 \otimes x_i$ for some right transversal (x_i) to E_0 in E. If $U^* = \langle e_0^* \rangle$ is the dual module of U, $(U^*)^E$ can be viewed as the dual module V^*, with dual basis $B^* = (e_0^* \otimes x_i)$. The duality $W \mapsto W^\perp$ from V to V^* preserves E-invariance. So every code (V, B, C) invariant under E corresponds to an E-invariant code $(V^*, B^*, C^\perp)$. If $U = U^*$ then we may identify (V, B) and (V^*, B^*). This is familiar in case $V = F^E$ is a permutation module. Clearly $U = U^*$ whenever the corresponding character is of order at most 2 (e.g., $|F| \leqslant 3$).

(2.4) LEMMA. *Suppose that α is an automorphism of E normalizing E_0. Let $B_\alpha = (e_0 \otimes x_i^{\alpha^{-1}})$. Then $e_0 \otimes x_i \mapsto e_0 \otimes x_i^{\alpha^{-1}}$ defines a monomial isomorphism $(U^E, B) \to ((U_\alpha)^E, B_\alpha)$ which gives a 1–1 correspondence between E-invariant codes.*

Proof. It is immediate that B_α is a basis of $\bar{V} = (U_\alpha)^E$. One checks that $e_0 \otimes x_i \mapsto e_0 \otimes x_i^{\alpha^{-1}}$ defines a monomial isomorphism $(V_\alpha, B) \to (\bar{V}, B_\alpha)$ of FE-modules. Moreover, the identity map $(V, B) \to (V_\alpha, B)$ is a monomial isomorphism respecting E-invariance of subspaces, by definition of V_α. ∎

Thus for instance the E-invariant codes in $V = U^E$ and $V^* = (U^*)^E$ are pairwise isomorphic if there is an automorphism α of E normalizing E_0 and inverting the elements in $E_0/C_{E_0}(U)$.

(2.5) LEMMA. *Let E be embedded in a finite group L. There exists a monomial action of L on $V = U^E$ extending that of E if and only if there is a subgroup L_0 with the following properties:*

(i) *$L = EL_0$ and $E \cap L_0 = E_0$;*

(ii) *U affords an FL_0-action extending that of E_0.*

Proof. Straightforward. ∎

If the field F of scalars is sufficiently large, condition (ii) in (2.5) is fulfilled exactly when there is a normal subgroup of L_0, with cyclic factor group, intersection E_0 in the centralizer $C_{E_0}(U)$. We apply Lemma 2.5 mostly in the following situation: Suppose E is a subgroup of $ML(C)$ for some indecomposable code C. If E induces a perfect permutation group $G = G'$, then E' is contained in any supplement L to $F^\#$ in $ML(C)$.

(2.6) LEMMA. *Suppose $\operatorname{char} F = p > 0$ and $\tilde{F}$ is a p-adic field with residue class field F. Then U can be lifted in a unique way to an $\tilde{F}E_0$-module $\tilde{U}$ preserving the order of the character, and V is the reduction of $\tilde{V} = \tilde{U} \otimes_{E_0} \tilde{F}E$.*

Proof. The order of the character λ afforded by U is prime to p. By Hensel's lemma there exists a unique $\tilde{F}$-character $\tilde{\lambda}$ having the same order and lifting λ. ∎

We finally give some comment concerning the fields of realization for codes. Let C be an FE-submodule of V and F_0 a subfield of F. C can be written in F_0 (with respect to E) if there is an E-invariant code (V_0, B_0, C_0) over F_0 such that tensoring with F yields a code isomorphic to (V, B, C).

(2.7) LEMMA. *Suppose F is a splitting field for E of characteristic $p > 0$. Let ε be a root of unity in F such that all values of the (Frobenius) characters of the composition factors of $V = U^E$ and of the character afforded by U are powers of ε. If every semisimple section of V is multiplicity-free, then every code occurring as a submodule of V can be written in $F_0 = \mathbb{F}_p(\varepsilon)$.*

Proof. Let $V_0 = U_0 \otimes_{E_0} F_0 E$, where U_0 affords the F_0-character satisfying $F \otimes U_0 = U$. Since Schur indices over finite fields are 1, every composition factor of the F_0E-module V_0 is absolutely irreducible. Using that the Jacobson radical $J(FE) = F \otimes J(F_0E)$ we may conclude that $W_0 \mapsto F \otimes W_0$ is an isomorphism from the lattice of submodules of V_0 to that of V. ∎

A corresponding result holds in characteristic 0 if the relevant Schur indices are 1, e.g., when G is 2-transitive (2.3).

3. PROJECTIVE PERMUTATION REPRESENTATIONS

In order to construct indecomposable codes we may use Schur's theory of projective representations. For the theoretical background we refer to [15].

(3.1) THEOREM. *Let (V, B, C) an indecomposable code over F admitting a permutation group (G, Ω), where B is indexed by $\Omega = \{0,..., n-1\}$. If* $\mathrm{Ext}(G/G', F^{\#}) = 0$, *every stem cover E of G affords an action on C inducing (G, Ω).*

Proof. For each $g \in G$ choose a preimage x_g in $ML(C)$. Then, by Theorem 1.2, $g \mapsto x_g$ is a projective representation in the sense of Schur. Since $\mathrm{Ext}(G/G', F^{\#}) = 0$ by hypothesis, there exists a homomorphism $\varphi: E \to ML(C)$ making the diagram

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & ML(C) \\ \downarrow & & \downarrow \\ G & \longrightarrow & PML(C) \end{array}$$

commutative [15, Proposition V.5.5]. ∎

(3.2) Corollary. *Assume (G, Ω) is a primitive permutation group and F a field such that* $\operatorname{Ext}(G/G', F^{\#}) = 0$. *Let E be a stem cover of G and E_0 be the inverse image in E of the stabilizer G_0. Induce up to E all 1-dimensional FE_0-modules. Then the submodules of the resulting FE-modules provide for a complete list of codes over F admitting (G, Ω) as permutation group.*

Proof. Apply Proposition 2.1 and Theorems 1.3 and 3.1. ∎

(3.3) *Remark.* Let $\bar{F}$ be an algebraic closure of F. If (V, B, C) is a code over F, then tensoring with $\bar{F}$ gives a code $(\bar{V}, \bar{B}, \bar{C})$ over $\bar{F}$. If C admits (G, Ω) then so does $\bar{C}$. Note that $\operatorname{Ext}(G/G', \bar{F}^{\#}) = 0$ since $\bar{F}^{\#}$ is a divisible group. Therefore we may carry out the program of (3.2) over $\bar{F}$ and then check whether the resulting codes can be written in F or not. Here Lemma 2.7 will be useful.

Clearly $\operatorname{Ext}(G/G', F^{\#}) = 0$ if $G = G'$. In case F is finite $\operatorname{Ext}(G/G', F^{\#}) = 0$ precisely when $|G/G'|$ and $|F^{\#}|$ are relatively prime. Then every central Frattini extension $A \rightarrowtail E \twoheadrightarrow G$ with A of exponent dividing $|F^{\#}|$ must be a stem extension, hence an epimorphic image over G of any stem cover of G [15, Proposition V.5.5]. Therefore only that part of the Schur multiplier $H_2(G) = H_2(G, Z)$ of G will be relevant in (3.1) and (3.2) which is of exponent dividing $|F^{\#}|$.

The passage to an algebraic closure can be avoided sometimes, even when $|G/G'|$ is not coprime to $|F^{\#}|$:

(3.4) Proposition. *Suppose (V, B, C) is an indecomposable code over the finite field F admitting a transitive permutation group (G, Ω) of degree n. Assume the greatest common divisor of n, $|G/G'|$, and $|F^{\#}|$ is 1. Let A be the π-component of $H_2(G)$, where π is the set of primes dividing n. Then every stem extension $A \rightarrowtail E \twoheadrightarrow G$ affords an action on C inducing (G, Ω).*

Proof. Let L be the inverse image in $ML(C)$ of G and L_0 that of G_0. By Proposition 2.1 we may assume $V = U^L$ where $U = \langle e_0 \rangle$ is a 1-dimensional FL_0-module and $B = (e_0 \otimes x_i)$ for some right transversal (x_i) to L_0 in L. By Theorem 1.2, L is a central extension of G by $F^{\#}$. It is immediate that $L_0 = F^{\#} \times C_{L_0}(U)$.

Let B be the π-component of $F^{\#}$. By Gaschütz's splitting theorem [6, Hauptsatz I. 17.4] there exists a supplement K to $F^{\#}$ in L intersecting $F^{\#}$ in B. Since $|G/G'|$ is relatively prime to $|B|$ by hypothesis, we have $\operatorname{Ext}(G/G', B) = 0$. Therefore there exists a homomorphism φ: $E \to K$ such that

$$\begin{tikzcd} E \arrow[rr, "\varphi"] \arrow[dr] & & K \arrow[dl] \\ & G & \end{tikzcd}$$

commutes [15, Proposition V. 5.5]. This completes the proof. (Alternatively one could argue showing that any minimal supplement to B in K is a stem extension.) ∎

Investigating codes along the lines given in Corollary 3.2 the following proposition will be useful.

(3.5) LEMMA. *Let $A \rightarrowtail E \twoheadrightarrow G$ be a stem extension of the finite group G and E_0 be the inverse image in E of some subgroup G_0 of G. Let $m = |G:G_0|$. Then*:

(a) *$A \cap E_0'$ is an epimorphic image of $H_2(G_0)$ containing the m-th powers of the elements in A.*

(b) *If the corestriction map $H_2(G_0) \to H_2(G)$ is surjective, $A \rightarrowtail E_0 \twoheadrightarrow G_0$ is again a stem extension.*

Proof. In view of the 5-term exact sequence [15, Sect. II.3], the injection $E_0 \rightarrowtail E$ yields the commutative diagram

$$\begin{array}{ccccccccccc}
H_2(E_0) & \longrightarrow & H_2(G_0) & \longrightarrow & A & \longrightarrow & E_0/E_0' & \longrightarrow & G_0/G_0' & \longrightarrow & 1 \\
\downarrow & & \downarrow & & \| & & \downarrow & & \downarrow & & \\
H_2(E) & \longrightarrow & H_2(G) & \longrightarrow & A & \longrightarrow & E/E' & \longrightarrow & G/G' & \longrightarrow & 1
\end{array}$$

having exact rows. By assumption the transgression $H_2(G) \to A$ $(A = H_1(A))$ is epimorphic. (It is an isomorphism if and only if E is a stem cover of G.) This proves (b) and the first part of (a).

Consider the transfer from E to E_0/E_0'. Since $A \subseteq E' \cap Z(E)$, any $x \in A$ is mapped onto $E_0' = x^m E_0'$. Thus $x^m \in A \cap E_0'$. ∎

We shall illustrate the program of (3.2) by discussing some highly transitive groups (G, Ω), namely the alternating groups and the Mathieu groups.

4. Alternating Groups

We construct, up to isomorphism, all codes of length $n \geqslant 4$ admitting the alternating group $\mathfrak{A}_n$. Of course, the repetition code $(\langle \sum e_i \rangle)$ and its dual even admit the symmetric group $\mathfrak{S}_n$. It turns out that for $n \geqslant 7$ no further code occurs. For $n \leqslant 6$ we obtain some other codes which, however, are well known. It is easily seen that all non-trivial codes admitting $\mathfrak{A}_3$ are isomorphic to the repetition code or its dual.

(4.1) $\mathfrak{A}_4$

According to (3.3) we start with an algebraically closed field F of scalars. Up to group isomorphism, $E = SL(2, 3)$ is the unique stem cover of $\mathfrak{A}_4$. Following (3.2) we have to determine the nontrivial submodules of U^E where U is any 1-dimensional FE_0-module (E_0 being the preimage of a point stabilizer).

(a) Let char $F = 2$. There are three nonisomorphic 1-dimensional FE_0-modules F, U, and U^*, which are restrictions of FE-modules F, W, and W^*, respectively. The obvious module isomorphisms $U^E \cong W \otimes F^E$, $(U^*)^E \cong W^* \otimes F^E$ are monomial (w.r.t. natural bases). So it is enough to study the permutation module $V = F^E$ $(= F^{\mathfrak{A}_4})$. V has two distinct submodules C_1 and $C_1^\perp$ which are interchanged by $\mathfrak{S}_4$. These are the (isomorphic) extended QR-codes over F.

From Lemma 2.7 it follows that the codes C_1 and $C_1^\perp$ can be written pecisely in those fields containing a primitive third root of unity.

We claim that $PML(C_1) = \mathfrak{A}_4$. At a first glance this seems to be obvious since the permutation group $\mathfrak{S}_4$ interchanges C_1 and $C_1^\perp$. But we have to exclude that there is a monomial action of a stem cover of $\mathfrak{S}_4$ on V fixing C_1 (Theorem 3.1). Since $H_2(\mathfrak{S}_4) = Z_2$ and char $F = 2$, we actually are reduced to the permutation action.

(b) Assume char $F = 3$. There are just three irreducible FE-modules of dimensions $1, 2, 3$, which can be realized over $\mathbb{F}_3$. The permutation module splits into the repetition code and its (irreducible) dual. Inducing up to E the unique nontrivial FE_0-module U gives an indecomposable FE-module $V = U^E$ whose unique proper submodule C_2 has dimension 2. V affords a monomial action of $GL(2, 3)$ extending that of $E = SL(2, 3)$ by (2.5). C_2 is invariant under $GL(2, 3)$ as follows from Clifford theory. Hence $PML(C_2) = \mathfrak{S}_4$. Of course, C_2 can be written in $\mathbb{F}_3$ and then represents the (4, 2) Hamming code.

(c) It remains to consider the semisimple situation. We make use of the character table of $SL(2, 3)$ [4, Theorem 38.1]. Let U be the 1-dimensional FE_0-module affording the unique character of order 2, $V = U^E$. Then $V = C_3 \oplus C_4$, where C_3 and C_4 are irreducible (but nonisomorphic) FE-modules of dimension 2. By (2.5) we can extend the monomial action of E on V to $GL(2, 3)$ in two different ways. In both cases $GL(2, 3)$ interchanges C_3 and C_4, which are the (isomorphic) extended QR-codes over F. C_3 and C_4 can be written just in such fields containing a primitive third root of unity, because of (2.7).

All induced FE-modules of interest are of type $W \otimes V$ or $W \otimes F^E$ where W is a 1-dimensional FE-module. But the permutation module F^E only yields the repetition code and its dual.

We assert that $PML(C_3) = \mathfrak{A}_4$. Assuming the contrary there is a monomial action on V of the stem cover $L = GL(2, 3)$ of $\mathfrak{S}_4$ leaving C_3 invariant. The restriction defines a monomial action of $E = SL(2, 3)$ leaving C_3 invariant. The preceding discussion shows that L cannot fix C_3. ▮

(4.2) $\mathfrak{A}_5$

As $H_2(\mathfrak{A}_5) = Z_2$ [12], by (3.2) and (3.5a) we only have to investigate monomial actions of $\mathfrak{A}_5$ (with permutation part $\mathfrak{A}_5$).

The permutation module $F^{\mathfrak{A}_5}$ yields the repetition code and its dual. If the field F does not contain a primitive third root of unity we do not get a proper monomial action.

Assume F contains a primitive third root of unity. Then the nontrivial 1-dimensional $F\mathfrak{A}_4$-modules induce up to an $F\mathfrak{A}_5$-module V and its dual V^*. V is absolutely irreducible when char $F \neq 2$. (Note that char $F \neq 3$.) When char $F = 2$, V has a unique composition series $0 \subset C_5' \subset C_5 \subset V$ where C_5 is a $(5, 2)$ QR-code and C_5' is the expurgated QR-code.

Since $\mathfrak{A}_5$ has an automorphism normalizing $\mathfrak{A}_4$ and inverting $\mathfrak{A}_4/\mathfrak{A}_4'$, by Lemma 2.4 the dual module V^* gives codes isomorphic to C_5 and C_5'. We claim that $PML(C_5) = \mathfrak{A}_5$. Otherwise, by passage to an algebraic closure, we have a monomial action of a stem cover L of $\mathfrak{S}_5$ (Theorem 3.1). Lemma 2.5 and the remark following it lead to the desired contradiction.

Observe that C_5, written over $\mathbb{F}_4$, is the 1-perfect $(5, 3)$ Hamming code. ▮

(4.3) $\mathfrak{A}_6$

In view of (4.2) just the repetition code and its dual will occur when char $F \neq 2$ or F does not contain a primitive third root of unity. So assume $\mathbb{F}_4 \subseteq F$.

It is known that $H_2(\mathfrak{A}_6) = Z_6$ [12]. Since char $F = 2$ we only have to investigate te monomial actions of the 3-fold cover $A \rightarrowtail E \twoheadrightarrow \mathfrak{A}_6$ ($|A| = 3$; E is the so-called Valentiner group). Let E_0 be the inverse image in E of a point stabilizer $\mathfrak{A}_5$. Since $H_2(\mathfrak{A}_5) = Z_2$ we have $E_0 = E_0' \times A$. Inducing up to E the nontrivial 1-dimensional FE_0-modules gives an FE-module V and its dual V^*.

There is a noninner involutory automorphism $\bar{\alpha}$ of $\mathfrak{A}_6$ normalizing $\mathfrak{A}_5$. By [15, Proposition V. 5.5] $\bar{\alpha}$ can be lifted to an automorphism α of E. Since $\mathfrak{S}_6 = \langle \bar{\alpha}, \mathfrak{A}_6 \rangle$ and $H_2(\mathfrak{S}_6) = Z_2$, α cannot centralize A. Therefore α inverts E_0/E_0'. By Lemma 2.4 every E-invariant code in V^* is isomorphic to one in V. V contains a unique proper submodule C_6, the extended $(6, 3)$ QR-code.

E has a 2-transitive subgroup $H \cong PSL(2, 5)$ such that $V = F^H$ as an FH-module. F^H has two distinct submodules C_6 and $C_6^\perp$ of dimension 3 being interchanged by $PGL(2, 5)$ (see also Theorem 6.2 below). Since $PGL(2, 5)$ supplements $\mathfrak{A}_6$ in $\mathfrak{S}_6$, we may conclude from (2.5) that $PML(C_6) = \mathfrak{A}_6$. ▮

(4.4) THEOREM. *Let C be a nontrivial (n, k)-code over F. If $n \geqslant 7$ and $PML(C) \supseteq \mathfrak{A}_n$, then C is isomorphic to the repetition code or its dual.*

Proof. The permutation module for $\mathfrak{A}_n$ has the repetition code and its dual as unique proper submodules [7]. The theorem is established by showing that every monomial action of the stem cover E of $\mathfrak{A}_n$ is the natural permutation action of $\mathfrak{A}_n$.

Let E_0 be the inverse image in E of a stabilizer $\mathfrak{A}_{n-1}$ (fixing the letter $n-1$). We have to show that $E_0 = E_0'$. This will be a consequence of the fact that the corestriction $H_2(\mathfrak{A}_{n-1}) \to H_2(\mathfrak{A}_n)$ is epimorphic, because of Lemma 3.5(b). In order to prove this we make use of Schur's work [12]. One knows that $H_2(\mathfrak{A}_7) = Z_6$ and $H_2(\mathfrak{A}_n) = Z_2$ for $n \geqslant 8$. However, we need more details and have to examine Schur's arguments more closely.

Consider the Moore presentation $R \rightarrowtail L \twoheadrightarrow \mathfrak{A}_n$ of $\mathfrak{A}_n$, L being free on $x_1, \ldots, x_{n-2}$ and R generated as an L-group by x_1^3, x_i^2 for $2 \leqslant i \leqslant n-2$, $(x_i x_{i+1})^3$ for $1 \leqslant i \leqslant n-3$, and $(x_i x_j)^2$, where $1 \leqslant j < i-1$, $i \leqslant n-2$. The explicit presentation is given by $x_1 \mapsto (0\,1\,2)$, $x_i \mapsto (0\,1)(i, i+1)$ for $2 \leqslant i \leqslant n-2$. Setting $T = \langle x_1, \ldots, x_{n-3} \rangle$ and $S = T \cap R$ we obtain a free presentation $S \rightarrowtail T \twoheadrightarrow \mathfrak{A}_{n-1}$, and the corestriction $H_2(\mathfrak{A}_{n-1}) \to H_2(\mathfrak{A}_n)$ is the natural map $T' \cap S/[T, S] \to L' \cap R/[L, R]$.

Schur [12, p. 117] proved that there is a word z in $x_1, \ldots, x_4$ such that $z[L, R]$ generates $L' \cap R/[L, R]$. (One may take, for instance,

$$z = x_1 x_2 x_1 x_2 x_1^{-2} x_2^{-3} x_3 x_4^{-1} x_3^{-1} x_1^{-1} x_3^{-1} x_1^{-1} x_4 x_1 x_4.)$$

Since $n \geqslant 7$ we have also $T' \cap S/[T, S] = \langle z[T, S] \rangle$. This gives the desired conclusion. ∎

(4.5) *Remark.* It readily follows from Lemma 3.5 that the corestriction $H_2(\mathfrak{A}_{n-1}) \to H_2(\mathfrak{A}_n)$ is epimorphic if n is odd, $n \geqslant 5$. Using this information one can establish Theorem 4.4 inductively by shortening the codes of even length.

5. MATHIEU GROUPS

For a discussion of the Mathieu groups $\mathfrak{M}_n$ we refer to Conway [3] and Lüneburg [8]. It is known that the (extended) Golay codes admit Mathieu groups as permutation groups [3]. We will show that there are no further interesting codes with this property.

(5.1) $\mathfrak{M}_{11}$

As $H_2(\mathfrak{M}_{11}) = 0$ [2], by (3.2) we have to investigate induced modules $V = U^{\mathfrak{M}_{11}}$, where U is a 1-dimensional $F\mathfrak{M}_{10}$-module over some field F. The commutator factor group of the point stabilizer $\mathfrak{M}_{10}$ has order 2. The permutation module $F^{\mathfrak{M}_{11}}$ yields the repetition code and its dual [7, Satz 4]. In case char $F \neq 2$ we have a nontrivial 1-dimensional $F\mathfrak{M}_{10}$-module U. Let $V = U^{\mathfrak{M}_{11}}$ for that U.

We first show that V is irreducible if char $F \neq 3$. Let $F = \mathbb{Q}$. Applying (2.3) we see that the $\mathbb{Q}\mathfrak{M}_{11}$-module V is absolutely irreducible. In view of (2.6) we have to verify that V remains irreducible modulo 11 and 5 ($|\mathfrak{M}_{11}| = 11 \cdot 10 \cdot 9 \cdot 8$). This is clear mod 11 since V belongs to an 11-block of defect 0 [4 Sect. 62]. Looking up the character table for $\mathfrak{M}_{11}$ in [2] one realizes the character decomposition

$$\chi_{44} = \chi_1 + \chi_{11} + \chi_{16} + \chi_{16}^*$$

on 5-regular elements (χ_{11} = character of V; $\chi_n(1) = n$). There are five 5-blocks of defect 0 and 9 conjugacy classes of 5-regular elements. Since the Sylow 5-subgroups of $\mathfrak{M}_{11}$ have order 5, the decomposition numbers are 0 or 1 by Brauer-Dade [4, Theorem 68.1]. We may conclude that the restrictions to 5-regular elements of χ_1, χ_{11}, χ_{16}, χ_{16}^* are just the irreducible Brauer characters in the principal 5-block for $\mathfrak{M}_{11}$. In particular, V is irreducible as well when F is a field of characteristic 5.

So let char $F = 3$. Then V is a uniserial $F\mathfrak{M}_{11}$-module with composition series $0 \subset C_{11}^{\perp} \subset C_{11} \subset V$, where C_{11} is the ternary Golay code of dimension 6. (Note that $C_{11}^{\perp}$ is the expurgated Golay code.) All these facts can be established using the information given in Conway [3]. $C_{11}^{\perp}$ is absolutely irreducible because its dimension is the prime 5 [4, Theorem 24.6]. From (2.3) it follows that $C_{11}^{\perp}$ is not isomorphic to V/C_{11} which, in fact, is the dual module of $C_{11}^{\perp}$. ∎

(5.2.) $\mathfrak{M}_{12}$

By [2] $H_2(\mathfrak{M}_{12}) = Z_2$. Let E be the stem cover of $\mathfrak{M}_{12}$ and E_0 the inverse image in E of a point stabilizer $\mathfrak{M}_{11}$. Then E_0 is a direct product of Z_2 and a copy of $\mathfrak{M}_{11}$. As before the permutation module gives only the repetition code and its dual. If char $F \neq 2$, the unique nontrivial 1-dimensional FE_0-module induces up to an $F\mathfrak{M}_{12}$-module V. When char $F = 3$, V has a unique proper submodule $C_{12} = C_{12}^{\perp}$, the extended ternary Golay code of dimension 6. C_{12} is an absolutely irreducible $F\mathfrak{M}_{12}$-module being not isomorphic to its dual V/C_{12}. If char $F \neq 3$, V is irreducible by (5.1). ∎

(5.3) $\mathfrak{M}_{22}$

It is known that $H_2(\mathfrak{M}_{22}) = Z_{12}$ [18]. Let $A \rightarrowtail E \twoheadrightarrow \mathfrak{M}_{22}$ be the stem cover of $\mathfrak{M}_{22}$ and E_0 be the inverse image in E of a point stabilizer $\mathfrak{M}_{21} = PSL(3, 4)$. By Lemma 3.5(a), 3 divides $|A \cap E_0'|$. Assuming $A \not\subseteq E_0'$ we get a character of order 2 of E_0/E_0', producing a faithful complex module

M of dimension 22 for the 2-fold proper covering $\bar{E}$ of $\mathfrak{M}_{22}$. By (2.3) M has at most two irreducible components. But $\bar{E}$ has only faithful irreducible complex representations of degree 10 and of degree larger than 55 [2, p. 304] and $\mathfrak{M}_{22}$ only those of degree 21 and at least 55 [2, p. 744]. This forces $A \subseteq E_0' = E_0$. (As a matter of fact, we see that 12 divides $|H_2(\mathfrak{M}_{21})|$; it is known that $H_2(\mathfrak{M}_{21}) = Z_{12} \times Z_4$.)

In order to determine the codes admitting $\mathfrak{M}_{22}$ we therefore have to discuss the permutation module $V = F^{\mathfrak{M}_{22}}$. If char $F \neq 2$, we just obtain the repetition code C_F and its dual $C_F^\perp$ [7, Satz 4]. Suppose $F = \mathbb{F}_2$. It is well known that $\mathfrak{M}_{22}$ leaves invariant a (22, 12)-code C_{22} over $\mathbb{F}_2$ which is obtained by shortening the binary Golay code C_{23}. We have $V = C_F^\perp + C_{22}$ and $C_F^\perp \cap C_{22} = C_F \oplus C_{22}^\perp$. $\mathfrak{M}_{22}$ acts trivially on $C_{22}/C_{22}^\perp$ and, as 11 does not divide $2^a - 1$ for $a < 10$, irreducibly on $C_{22}^\perp \cong (V/C_{22})^*$. From [7, Satz 4] it follows that $C_F^\perp/C_F$ is (absolutely) indecomposable.

Hence all interesting $\mathfrak{M}_{22}$-invariant codes (over $\mathbb{F}_2$) are situated between C_{22} and $C_{22}^\perp$. We claim that $C_{22}^\perp$ is an absolutely irreducible $\mathbb{F}_2\mathfrak{M}_{22}$-module. Note first that $C_{22}^\perp$ is the set of all vectors in C_{22} of weights 0, 8, 12, 16. $C_{22}^\perp$ contains 77 vectors of weight 16 complementary to the blocks of the Steiner system $S(3, 6, 22)$. The stabilizer T in $\mathfrak{M}_{22}$ of a vector of weight 16 is a maximal subgroup having two orbits of length 6 and 16 on the 22 letters [3, Table 3]. Hence T fixes only 2 vectors in $C_{22}^\perp$. It follows $\mathrm{End}_{\mathfrak{M}_{22}}(C_{22}^\perp) = \mathbb{F}_2$.

Thus the situation is the same for $F \supseteq \mathbb{F}_2$. ∎

(5.4) $\mathfrak{M}_{23}$

As $H_2(\mathfrak{M}_{23}) = 0$ [2] and $\mathfrak{M}_{22} = \mathfrak{M}_{22}'$, we just have to investigate the permutation module $V = F^{\mathfrak{M}_{23}}$. As before only the case where char $F = 2$ is interesting. Then $V = C_F \oplus C_F^\perp$, where $C_F^\perp$ has a unique proper submodule $C_{23}^\perp$. $C_{23} = C_F \oplus C_{23}^\perp$ is the "binary" (23, 12) Golay code. ∎

(5.5) $\mathfrak{M}_{24}$

As $H_2(\mathfrak{M}_{24}) = 0$ [2] and $\mathfrak{M}_{23} = \mathfrak{M}_{23}'$, again only the permutation module $V = F^{\mathfrak{M}_{24}}$ is of interest, where char $F = 2$. Then V has a unique composition series $0 \subset C_F \subset C_{24} = C_{24}^\perp \subset C_F^\perp \subset V$. Here C_{24} is the extended "binary" (24, 12) Golay code. The indecomposability of $C_F^\perp/C_F$ again follows from [7, Satz 4]. By weight consideration (over $\mathbb{F}_2$), using the fact that $\mathfrak{M}_{24}$ acts transitively on the set of dodecads [3], one realizes that C_{24} is (absolutely) indecomposable. ∎

(5.6) *Permutation Groups*

We determine the permutation groups $PML(C_n)$. Clearly the Golay codes are (extended) QR-codes. We will see in Section 6 that an extended QR-code of length $p + 1$ does not admit $PGL(2, p)$. Since $\mathfrak{M}_n$ is a maximal subgroup of $\mathfrak{A}_n$, we may conclude from Theorem 4.4 that $PML(C_n) = \mathfrak{M}_n$ for

$n = 12, 24$. This holds also for $n = 11, 23$, because $\mathfrak{M}_{11}$ and $\mathfrak{M}_{23}$ have no outer automorphisms. Of course, these facts are well known [3, Theorems 2.4 and 3.6].

The situation is different for $\mathfrak{M}_{22}$. $\mathrm{Aut}(\mathfrak{M}_{22})$ is a permutation group of degree 22 [8, 12.5], having $\mathfrak{M}_{22}$ as a normal subgroup of index 2 [3]. In fact, $\mathrm{Aut}(\mathfrak{M}_{22})$ is induced by the normalizer $N_{\mathfrak{M}_{24}}(\mathfrak{M}_{22})$ and so leaves invariant C_{22} and $C_{22}^{\perp}$. There is only one $\mathfrak{M}_{22}$-invariant code of dimension 11 which admits $\mathrm{Aut}(\mathfrak{M}_{22})$, namely, $C_{22} \cap C_F^{\perp}$. Since $\mathrm{Aut}(\mathfrak{M}_{22})$ is a maximal subgroup of $\mathfrak{S}_{22}$, (4.4) gives $PML(C_{22}) = \mathrm{Aut}(\mathfrak{M}_{22})$. ∎

6. Extended QR-Codes

By the Gleason–Prange theorem [1, Theorem 3.1] the extended QR-codes of length $p+1$, p an odd prime, admit $PSL(2, p)$. We will characterize these codes by the property that their permutation group contains $PSL(2, p)$ but not $PGL(2, p)$. The case $p = 3$ is already handled in (4.1) so that we may assume $p \geqslant 5$. Then $PSL(2, p)$ is simple.

$G = PSL(2, p)$ is 2-transitive on $p+1$ letters, the points of the projective line Ω over $\mathbb{F}_p$. It is known that $E = SL(2, p)$ is the unique stem cover of G [6, Satz V. 25.7]. Because of Theorem 3.1 we have to investigate monomial actions of E. Write $a = \left(\begin{smallmatrix} \nu & 0 \\ 0 & \nu^{-1} \end{smallmatrix}\right)$ for some generator ν of $\mathbb{F}_p^{\#}$, and let $u = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $c = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. We have $u^{-1}au = a^{-1}$. $E_0 = \langle a, c \rangle$ is the normalizer of the Sylow p-subgroup $S = \langle c \rangle$ of E. $H = \langle a \rangle$ complements S in E_0. E_0 is the inverse image of a point stabilizer G_0 (fixing ∞). The normalizer $N = N_E(H)$ is generated by a and u. For any $x \in H$ with $x^2 \neq 1$, $C_E(x) = H$ and $N_E(\langle x \rangle) = N$.

The above notation is fixed through (6.1), (6.2).

(6.1) Lemma. *Suppose U is a 1-dimensional FE_0-module affording a character λ of order greater than* 2; *let $V = U^E$. Then* $\mathrm{End}_E(V)$ *is of F-dimension* 1. *If* $\mathrm{char}\, F \neq p$, *V is absolutely irreducible.*

Proof. Clearly $u \in E - E_0$ and $H = E_0 \cap E_0^{u^{-1}}$. Since u inverts the elements of H and λ has order greater than 2, by (2.3) $\mathrm{End}_E(V)$ has dimension 1. Hence V is absolutely irreducible if $\mathrm{char}\, F$ does not divide $|E| = (p+1)p(p-1)$. We may assume that F is an algebraically closed field such that $\mathrm{char}\, F = q$ divides $p^2 - 1$. Note that the order of λ is prime to q.

Let $\tilde{F}$ be a q-adic field with residue class field F. According to Lemma 2.6 we can lift V in a natural way to an $\tilde{F}E$-module $\tilde{V}$. $\tilde{V}$ is absolutely irreducible. If q is odd and a divisor of $p+1$, the order of a Sylow q-subgroup of E divides $p+1$. If $q = 2$, $G = PSL(2, p)$ operates on $\tilde{V}$, and

$p+1$ is divisible by the order of a Sylow 2-subgroup of G when $p \equiv 3 \pmod 4$. In these cases V and $\tilde{V}$ belong to a q-block of defect 0 and thus V is irreducible [4, Sect. 62].

Assume therefore that either $q = 2$ and $p \equiv 1 \pmod 4$ or q is odd and a divisor of $p-1$. Let $D = \langle x \rangle$ be a Sylow q-subgroup of H. Denote by χ the (ordinary) character afforded by $\tilde{V}$. From the character table of $SL(2,p)$ [4, Theorem 38.1] one sees that

$$\chi(xy) \equiv \lambda(y) + \lambda^*(y) \qquad (\mathrm{mod}\ q)$$

for all $y \in H$; λ^* is the dual character to λ. Now $H = C_E(x)$ since $|D| > 2$. If $\lambda|H$ belongs to the block b of FH, then χ belongs to the q-block $B = b^E$ by Brauer's second main theorem [4, Theorem 63.2]. Clearly D is a defect group of b. As λ has order $\neq 1, 2$ and u inverts the elements of H, we have $N_N(b) = H = C_E(D)$. Applying Brauer's first main theorem [4, Theorems 64.10 and 58.3] shows that D is also a defect group of B. From [4, Theorem 68.1] it follows that V is the unique irreducible FE-module in the block B. This completes the proof. ∎

(6.2) THEOREM. *Besides the repetition code and its dual, there are (up to isomorphism) precisely the following proper codes admitting* $G = PSL(2, p)$:

(i) *If* char $F = 2$ and $\mathbb{F}_4 \subseteq F$, *there is a* $(p+1, (p+1)/2)$*-code over* F; *it can be written in* $\mathbb{F}_2$ *if and only if* $p \equiv \pm 1 \pmod 8$.

(ii) *If* char F *is different from* 2 *and* p *and* $(-1)^{(p-1)/2}p$ *is a square in* $F^{\#}$, *there is a* $(p+1, (p+1)/2)$*-code over* F.

(iii) *In case* char $F = p$ *there exist* $(p+1, k)$*-codes over* F, *one for each* k *between* 2 *and* $p-1$.

The codes in (iii) *admit* $PGL(2, p)$; *the codes appearing in* (i), (ii) *are the extended QR-codes which do not admit* $PGL(2, p)$.

Proof. Recall that $PGL(2, p)$ is sharply 3-transitive on Ω. It is immediate that $GL(2, p)$ is a stem cover of $PGL(2, p)$. Every monomial action of $E = SL(2, p)$ can be extended, in various ways, to $GL(2, p)$.

(i) char $F = 2$.

In view of (6.1) we only have to study the permutation module $V = F^G (= F^E)$. Assume first that F is algebraically closed. Let $1 + \psi$ be the complex permutation character of $G = PSL(2, p)$. From the character table [4, Theorem 38.1] one obtains that there are irreducible characters η_1, η_2 (of G) of degree $(p-1)/2$ such that

$$\psi = 1 + \eta_1 + \eta_2$$

on 2-regular elements; η_1 and η_2 differ on 2-regular elements, and they have there values in $\mathbb{Q}(\varepsilon)$, where $\varepsilon^2 = (-1)^{(p-1)/2}p$.

Now G_0 is a Frobenius group with kernel the image $\bar{S}$ of S in G. Application of [6, Satz V.16.13] and Mackey decomposition shows that the restriction of ψ to G_0 can be written as

$$\psi | G_0 = 1 + \eta_1' + \eta_2',$$

where η_1' and η_2' are different irreducible characters of degree $|G_0/\bar{S}| = (p-1)/2$. Since η_1', η_2' are in a 2-block of defect 0 for G_0, we may deduce that η_1 and η_2 remain irreducible as Brauer characters. Hence V has (unique) submodules $C_F \subset C_F^\perp$ of dimensions 1 resp. p and $M = C_F^\perp/C_F$ has two nonisomorphic composition factors of dimension $(p-1)/2$.

Viewing V as the permutation module for $PGL(2, p)$, M is irreducible. This follows, for instance, from the fact that the permutation character of a point stabilizer is of type $1 + \gamma$, where γ is irreducible of degree $p-1$ and so is in a 2-block of defect 0. Consequently (Clifford) $M = \bar{C}_1 \oplus \bar{C}_2$ for some nonisomorphic irreducible FG-modules $\bar{C}_i = C_i/C_F$. As codes the C_i are isomorphic since they are interchanged by $PGL(2, p)$. Clearly C_1 and C_2 are the (isomorphic) extended QR-codes over F. (For an alternate approach see [16] or [11].)

Since η_1, η_2 have their values in the quadratic field $\mathbb{Q}(\varepsilon)$, from Lemma 2.7 it follows that the codes C_i can be written in the field $\mathbb{F}_4$ and, by elementary properties of 2-adic squares, in $\mathbb{F}_2$ precisely when $p \equiv \pm 1 \pmod 8$.

Finally, since $\operatorname{char} F = 2$, the permutation action of G cannot be extended to a proper monomial action of $GL(2, p)$. Hence $PGL(2, p) \not\subseteq PML(C_i)$.

(ii) $\operatorname{char} F \neq 2, p$.

The permutation module $V = F^E$ now yields only the repetition code and its dual. This can be checked by applying [13, Corollary 2]. (One can verify this also by means of [7, Satz 8] in case $\operatorname{char} F$ does not divide $p+1$, and by a block theoretic argument otherwise.)

In view of (6.1) it remains to consider $V = U^E$, where U is the 1-dimensional FE_0-module affording the unique linear character λ of order 2. Assume first that F is algebraically closed. In the semisimple situation from [4, Theorem 38.1] (and its proof) it follows that $V = C_1 \oplus C_2$ for some irreducible FE-modules C_i of dimension $(p+1)/2$. So let $\operatorname{char} F = q$ be an odd divisor of $p^2 - 1$.

There is a q-adic field $\tilde{F}$, with residue class field F, which is a splitting field for E. Lift V to an $\tilde{F}E$-module $\tilde{V}$ as in (2.6). We already know that there are irreducible characters ξ_1, ξ_2 of degree $(p+1)/2$ such that $\xi_1 + \xi_2$ is the character of $\tilde{V}$. From the character table we infer that ξ_1 and ξ_2 differ on q-regular elements and have their values in $\mathbb{Q}(\varepsilon)$, ε as in (i). We claim that ξ_1, ξ_2 are irreducible also as Brauer characters mod q.

Let D be a Sylow q-subgroup of E. If q is a divisor of $p+1$, $|D|$ divides the degree of the ξ_i and we are done. Suppose next that q is a divisor of $p-1$. We may assume $D \subseteq H$. From [4, Theorem 38.1] once more we obtain that there is an irreducible character χ of E (with values in $\bar{F}$), induced from a linear character of E_0 of order $2|D|$, such that

$$\chi = \xi_1 + \xi_2$$

on q — regular elements. Let B denote the q-block containing χ, hence also ξ_1 and ξ_2. Since $H \supseteq D$ is cyclic and B is not of defect 0, application of [4, Theorem 68.1] shows that ξ_1 and ξ_2, restricted to q-regular elements, are the unique irreducible Brauer characters in B.

Consequently V has two nonisomorphic composition factors of dimension $(p+1)/2$. By (2.3) $\dim_F \operatorname{End}_E(V) = 2$. Thus, as before, $V = C_1 \oplus C_2$ for some irreducible FE-modules C_i of dimension $(p+1)/2$.

In any case, C_1 and C_2 represent the extended QR-code over F. In fact, $GL(2, p)$ interchanges C_1 and C_2 in any monomial action extending that of E. This also can be seen from the character table. From (3.1) and the remark following (2.5) we may conclude that the codes C_i do not admit $GL(2, p)$.

The codes C_i can be written in $\mathbb{F}_q(\varepsilon)$ resp. $\mathbb{Q}(\varepsilon)$, where $\varepsilon^2 = (-1)^{(p-1)/2} p$. This follows from (2.7); (2.3) guarantees that the Schur index of ξ_i over $\mathbb{Q}$ is 1.

(iii) $\operatorname{char} F = p$.

By Brauer–Nesbitt there is, up to isomorphism, exactly one (absolutely) irreducible FE-module W_k of dimension k $(1 \leqslant k \leqslant p)$ [6, V.5.13]. From [4, Theorem 71.3] one obtains that the various 1-dimensional FE_0-modules induce up to FE-modules V_k having a submodule $C_k \cong W_k$ such that $V_k/C_k \cong W_{p+1-k}$ $(1 \leqslant k \leqslant p-1)$. Furthermore $V_{(p+1)/2} = U^E$, where U affords the character of E_0 of order 2. Obviously V_1 is the permutation module, and $V_1 = C_1 \oplus C_1^{\perp}$.

By (2.3), (6.1) $\operatorname{End}_E(V_k)$ has F-dimension 2 precisely when $k = 1$ or $k = (p+1)/2$. Since both composition factors of $V_{(p+1)/2}$ are isomorphic, $V_{(p+1)/2}$ must be indecomposable. This is immediate in the other cases. Hence C_k is the unique proper submodule of V_k, $k = 2, \ldots, p-1$. The code C_k admits $PGL(2, p)$ by Clifford theory. ∎

The codes in (iii) are extensions of the optimal codes in characteristic p described by Assmus and Mattson [1, Sect. 2].

(6.3) *Permutation Groups*

Suppose C is an extended QR-code of length $p+1$ over F and $G = PML(C)$. Then G contains $PSL(2, p)$ but not $PGL(2, p)$. Only four cases are known where $G \neq PSL(2, p)$, namely,

(1) $p=5$, $F \supseteq \mathbb{F}_4$: $G=\mathfrak{A}_6$,

(2) $p=7$, $\operatorname{char} F=2$: $G=\operatorname{Aff}(3,2)$,

(3) $p=11$, $\operatorname{char} F=3$: $G=\mathfrak{M}_{12}$,

(4) $p=23$, $\operatorname{char} F=2$: $G=\mathfrak{M}_{24}$.

It is conjectured that $G=PSL(2,p)$ provided $p>23$. We cannot settle this in generality, but here is some further evidence for its truth.

(6.4) THEOREM. *Let C be an extended QR-code over F of length $p+1 \geqslant 8$, and let G be a subgroup of $PML(C)$ containing $PSL(2,p)$. Then*

(i) *G is a proper subgroup of $\mathfrak{A}_{p+1}$.*

(ii) *If $p>7$ and $G \neq PSL(2,p)$, then G is 4-transitive and simple.*

Proof. Let N be the normalizer in $\mathfrak{S}_{p+1}$ of a Sylow p-subgroup S of $PSL(2,p)$. N has order $p(p-1)$ and contains a $(p-1)$-cycle. It follows that N supplements $PSL(2,p)$ in $PGL(2,p)$, and $\mathfrak{A}_{p+1}$ in $\mathfrak{S}_{p+1}$. Since G contains $PSL(2,p)$ but not $PGL(2,p)$, the normalizer $\bar{N}=N_G(S)$ is a subgroup of $PSL(2,p)$.

S is a Sylow p-subgroup of $G \cap \mathfrak{A}_{p+1}$. Hence from $\bar{N} \subseteq PSL(2,p) \subseteq G \cap \mathfrak{A}_{p+1}$ it follows $G \subseteq \mathfrak{A}_{p+1}$ by the Frattini argument. Because of (4.4) G is a proper subgroup of $\mathfrak{A}_{p+1}$.

Now assume $G \neq PSL(2,p)$ and $p>7$. By Neumann [10, Theorem 2.1] then G is 4-transitive. Suppose $M \neq 1$ is a normal subgroup of G. M cannot be regular [17, Theorem 11.3], hence is at least 3-transitive. This implies that $S \subseteq M$ and $PSL(2,p) \subseteq M$, by simplicity of $PSL(2,p)$. Moreover we have $G=M\bar{N}$, again by the Frattini argument. Now from $\bar{N} \subseteq PSL(2,p)$ it follows $G=M$, as desired. ∎

A group G as in Theorem 6.4(ii) would be an "unknown" simple group, provided $p>23$. Theorem 6.4(i) answers a conjecture of Rasala to the affirmative [11, p. 470]. It should be possible to establish this by more elementary arguments than those used in (4.4). (But the argumentation by Shaughnessy [13, p. 402] cannot work, as follows from [1, Theorem 2.2].) Under additional assumptions, Theorem 6.4 can be improved so that $PML(C)=PSL(2,p)$. For instance, this holds if $p-2$ is a prime [10, Corollary 2.2], or if $(p-1)/2$ is a prime and $23<p \leqslant 4079$. (The latter result has been already stated in [1, p. 146]. But, as Rasala [11] noted, it depends on the validity of his conjecture, i.e., on Theorem 6.4(i).)

REFERENCES

1. E. F. ASSMUS AND H. F. MATTSON, New 5-designs, *J. Combinatorial Theory* **6** (1969), 122–151.

2. N. Burgoyne and P. Fong, The Schur multipliers of the Mathieu groups, *Nagoya Math. J.* **27** (1966), 733–745; *Nagoya Math. J.* **31** (1968), 297–304.
3. J. H. Conway, Three lectures on exceptional groups, *in* "Finite Simple Groups" (M.B. Powell and G. Higman, Eds.), Academic Press, London, 1971.
4. L. Dornhoff, "Group Representation Theory," Parts A and B, Dekker, New York, 1971/1972.
5. W. Gaschütz, Über modulare Darstellungen endlicher Gruppen, die von freien Gruppen induziert werden, *Math. Z.* **60** (1954), 274–286.
6. B. Huppert, "Endliche Gruppen I," Springer–Verlag, Berlin, 1967.
7. M. Klemm, Über die Reduktion von Permutationsmoduln, *Math. Z.* **143** (1975), 113–117.
8. H. Lüneburg, "Transitive Erweiterungen endlicher Permutationsgruppen," Lecture Notes in Mathematics No. 84, Springer–Verlag, Berlin, 1969.
9. F. J. Mac Williams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," I and II, North-Holland, Amsterdam 1977.
10. P. M. Neumann, Transitive permutation groups of prime degree, IV: A problem of Mathieu and a theorem of Ito, *Proc. London Math. Soc. Ser 3* **32** (1976), 52–62.
11. R. Rasala, Split codes and the Mathieu groups, *J. Algebra* **42** (1976), 422–471.
12. I. Schur, Über die Darstellungen der symmetrischen und alternierenden Gruppen durch gebrochene lineare Substitutionen, *J. Math. (Crelle)* **139** (1911), 155–250.
13. L. L. Scott, Permutation modules and 1-cohomology, *Arch. Math.* **27** (1976), 362–368.
14. E. P. Shaughnessy, Codes with simple automorphism groups, *Arch. Math.* **22** (1971), 459–466.
15. U. Stammbach, "Homology in Group Theory," Lecture Notes in Mathematics No. 359, Springer–Verlag, Berlin, 1973.
16. H. N. Ward, Quadratic residue codes and symplectic groups, *J. Algebra* **29** (1974), 150–171.
17. H. Wielandt, "Finite Permutation Groups," Academic Press, New York/London, 1964.
18. P. Mazet, Sur le multiplicateur de Schur du groupe de Mathieu M_{22}, *C.R. Acad. Sci. Paris Sér. A* **289** (1979), 659–661.