Every Finite Group Is the Automorphism Group of Some Perfect Code

K. T. Phelps

School of Mathematics, Georgia Institute of Technology, Atlanta, Georgia 30332

Communicated by the Managing Editors

Received November 5, 1984

In this paper we prove the every finite group is isomorphic to the full automorphism group of some perfect binary single error correcting code.

1. INTRODUCTION

A code $C$ of length $n$ over an alphabet $A$ is a subset of $A^n$. The distance between any two codewords $u, v \in C$, is the number of positions in which they disagree. The parameters $(n, M, d)$ of a $q$-ary code $C$ represent the length $n$, the number of codewords $M$, and $d$, the minimum distance between any two codewords in $C$ when the alphabet $A$ has order $q$. A binary code $C$ having alphabet $\{0, 1\}$ and minimum distance 3 which meets the sphere-packing bound is a perfect binary single error correcting code, or, more briefly, a perfect 1-code. Such perfect 1-codes exist if and only if the length $n$ is of the form $2^k - 1$. Recently, it was established there are at least $2^{2n}$ non-equivalent perfect 1-codes of length $n$, for $n$ sufficiently large. Still, little is known about the automorphism groups of such codes.

Briefly, an automorphism of a code $C$ of length $n$ is a permutation $\alpha$ of the indices (positions) of the codewords which maps codewords to codewords. In the linear perfect 1-code of length $n = 2^k - 1$, one can find $k$ positions such that any permutation of these positions can be uniquely extended to an automorphism of the code [4, p. 231]. Since every finite group is isomorphic to a subgroup of $S_k$ (symmetric group on $k$ symbols), for some $k$, it follows that every finite group is isomorphic to a subgroup of $\text{Aut } C$, the full automorphism group of some perfect 1-code $C$. What we intend to establish in this paper is that every finite group is isomorphic to the full automorphism group of some perfect 1-code.

If a perfect 1-code, $C$, contains the zero-vector, then the words of weight 3 are the characteristic vectors of a Steiner triple system; similarly the
words of weight 4 in the extended code, $C^*$, are the characteristic vectors of a Steiner quadruple system [4, p. 63]. Mendelsohn [6] proved that every finite group is the automorphism group of some Steiner triple system and moreover the same thing is true about Steiner quadruple systems. It is our purpose to establish this result for perfect 1-codes.

2. Preliminaries

A $n$-ary distance 2-code of length $m+1$, having $n^m$ codewords, is equivalent to an $m$-ary quasigroup of order $n$. If $q$ is such an $m$-quasigroup then

$$Q = \{ (x_1, x_2, ..., x_m, q(x_1, x_2, ..., x_m)) \mid x_i \in \{1, 2, ..., n\} \}$$

is an $n$-ary distance 2-code of length $m+1$; the converse is equally obvious. In the language of orthogonal arrays and $m$-quasigroups, an automorphism of the code $Q$ is called an (invariant) conjugation of the array; the automorphism group of $Q$ is called the conjugate invariant subgroup of $q(x_1, ..., x_n)$. Hoffman [3] established some very strong results about the conjugate invariant subgroups of $m$-quasigroups of order $n$, when $n > m$. Unfortunately, his results do not fit our needs but some of his methods will prove useful.

These distance 2-codes (or $m$-quasigroups) are an important part of Phelps' construction of perfect 1-codes [9]. The other part which is important for our considerations is a partition of $V^{(n+1)}$ into extended perfect 1-codes. Given any extended perfect 1-code $C^*$, then there exists a partition of $V^{(n+1)}$, $C_j$, $i = 0, 1$, $j = 0, 1, ..., n$, where each $C'_j$ is an extended perfect 1-code of length $n+1$, and $C_0^0 = C^*$. If $C^*$ is linear then the $C'_j$ could be its cosets, otherwise the $C'_j$ could be appropriately chosen translates. Our basic construction is as follows: let $C'_j$, $i = 0, 1$, $j = 0, 1, ..., n$ be a partition of $V^{(n+1)}$ into extended perfect 1-codes, where $C'_j$ has only even weight words and $C'_j$ only odd weight words; let $R^*$ be any extended perfect 1-code of length $m+1$; let $Q_r$ be any $m$-ary quasigroup of order $n+1$. Let

$$C^* \otimes R^* = \bigcup_{r \in R^*} \bigcup_{j \in Q_r} C^0_{j_0} \oplus \cdots \oplus C^0_{j_m},$$

where $r = (r_0, ..., r_m)$ and $j = (j_0, ..., j_m)$.

In [9] it was established that $C^* \otimes R^*$ is an extended perfect 1-code of length $(n+1)(m+1)$. Moreover if $C^*$ and $R^*$ are linear and $C'_j$ are the cosets of $C^*$ with $C'_j = C^0_j + (1, 0, ..., 0)$ then $Q_r$ can be chosen so that $C^* \otimes R^*$ is the linear extended Hamming code. Simply, define

$$Q_r = Q = \{ (j_0, j_1, ..., j_m) \mid C^0_{j_0} + C^0_{j_1} + \cdots + C^0_{j_m} = C^0_0 = C^* \}.$$
Our construction allows great flexibility, which will permit us to limit the symmetries of the perfect 1-codes \( C^* \otimes R^* \). Let \( D'_i, i = 0, 1, j = 0, 1, \ldots, n \) be some other partition of \( V^{(n+1)} \) into extended perfect 1-codes; then a variant of the prior construction is

\[
C^* \otimes R'^* = \left( \bigcup_{r \in R^*} \bigcup_{j \in Q_r} C'_{j_0}^0 \oplus \cdots \oplus C'_{j_m}^0 \right) \cup \left( \bigcup_{j \in Q} D'_0 \oplus \cdots \oplus D'_m \right).
\]

If \( C^* \otimes R^* \) constructed as in (1) was linear then a suitable choice of \( Q_r \) and \( D'_j \) will limit the symmetries of \( C^* \otimes R'^* \). In particular if \( D'_0 \) is rigid or automorphism free and the partition has an additional property, then the only automorphisms of \( C^* \otimes R'^* \) induce automorphisms of \( R^* \) and the \( m \)-ary quasigroup \( Q \). So the \( \text{Aut} \ C^* \otimes R'^* \) is isomorphic to a subgroup of \( \text{Aut} R^* \) and a subgroup of \( \text{Aut} Q \).

The variant presented above (Eq. (2)) is subject to further modification. Consider any \( \alpha \in \text{Aut} C^* \otimes R'^* \), \( \alpha : (x_0, \ldots, x_m) \rightarrow (x_{i_0}, \ldots, x_{i_m}) \). If \( r_i \) is the parity of the \( n+1 \) bit vector \( x_i \) then \( \alpha \) induces an automorphism, \( \hat{\alpha} \), of \( R^* \) which maps \( (r_0, \ldots, r_m) \rightarrow (r_{i_0}, \ldots, r_{i_m}) \), with \( r_{i_j} \) being the parity of \( x_{i_j} \). This in turn induces an isomorphism from \( Q_r \) to \( Q_{s(r)} \). By assiduous choice of the \( Q_r \) one can sufficiently limit these automorphisms so that the resulting code will have the desired automorphism group.

Our problem then is two-fold: Find a "suitable" partition \( D'_j \) of \( V^{(16)} \) and, choose the proper \( m \)-quasigroups \( Q_r \).

3. \( m \)-Quasigroups and Perfect 1-Codes

In this section we again assume that \( C^* \otimes R'^* \) is the code constructed in Eq. (2) and moreover the only automorphisms of \( C^* \otimes R'^* \) are "block" automorphisms mapping codewords \( (x_0, x_1, \ldots, x_m) \) to codewords \( (x_{i_0}, \ldots, x_{i_m}) \).

Earlier, it was remarked that one can find \( k \) positions such that any permutation of these \( k \) positions can be uniquely extended to an automorphism of \( R \), where \( m + 1 = 2^k \). These \( k \) positions correspond to \( k \) linearly independent column vectors in the parity check matrix for \( R \). One might as well assume that these vectors are the natural basis vectors \( e_1, e_2, \ldots, e_k \) and that the positions are \( 1, 2, \ldots, k \).

For any triple \( \{k_1, k_2, k_3\} \subseteq \{1, 2, \ldots, k\} \) there is a unique extended perfect 1-subcode on the 8 positions \( \{0, k_1, k_2, k_3, j_4, \ldots, j_7\} \) corresponding to the column vectors in the subspace spanned by \( \{e_{k_1}, e_{k_2}, e_{k_3}\} \). In particular, given an ordered triple \( k = (k_1, k_2, k_3) \) there is a canonical labeling of these 8 positions and a codeword \( r_k \in R^* \) which has ones only in these positions.
Lemma 3.1. For every finite group $G$ there exists a ternary relation $K$ of order $k$, $K \subseteq \{1, 2, \ldots, k\}^3$ having an automorphism group $\text{Aut} K$ isomorphic to $G$. Moreover any two triples in $K$ agree in at most one position.

Proof. Let $(V, E)$ be a directed graph with no loops, isolated points, or multiple edges having $\text{Aut}(V, E) \simeq G$, $G, ([4, 6])$, let $K = \{(v_1, v_2, e) | v_1, v_2 \in V, e \in E, e = (v_1, v_2)\}$. Clearly $\text{Aut}(V, E) \simeq \text{Aut} K$.

Now for each $k \in K$, let $r_k \in R^*$ be the canonical codeword of weight 8.

Lemma 3.2. There exists an $m$-quasigroup of order 16, $P$, such that every automorphism of $P$ fixes the positions 0, 1, ..., 7 and moreover every permutation which fixes these positions is an automorphism.

Proof. Consider $Z_8 \times Z_2$ and define the vectors in $P$ as follows:

(a) $[(0, p_0), (1, p_1), \ldots, (7, p_7), (0, 0), \ldots, (0, 0)] \in P$ whenever $p_0 + p_1 + \cdots + p_7 = 1 \mod 2$;

(b) for $(x_0, x_1, \ldots, x_7) \neq (0, 1, \ldots, 7)$, $[(x_0, p_0)(x_1, p_1), \ldots, (x_7 + y_0, p_7 + q_0), (y_1, q_1), \ldots, (y_{m-7}, q_{m-7})] \in P$;

whenever

$$x_0 + x_1 + \cdots + x_7 \equiv 4 \mod 8,$$

$$y_0 + y_1 + \cdots + y_{m-7} \equiv 0 \mod 8,$$

$$p_0 + p_1 + \cdots + p_7 \equiv 0 \mod 2,$$

and

$$q_0 + q_1 + \cdots + q_{m-7} \equiv 0 \mod 2,$$

$P$ will clearly have the required property. This construction is essentially the same one used by Hoffman [3].

Lemma 2 implies that there is a canonical isomorphism from $P$ to $Q_{r_k}$ which maps the fixed positions of $P$ to the canonically labeled positions of $r_k$ which contain ones. If $Q$ is the (linear) $m$-quasigroup defined in the Introduction then for each $\mathbf{r} \in R^*$ let

$$Q_\mathbf{r} = \begin{cases} Q_{r_k} & \text{if } \mathbf{r} = r_k, k \in K, \\ Q & \text{otherwise.} \end{cases}$$

Then applying construction (2) with the above choices for $Q_{r_k}$ will produce a code $C^* \otimes R^*$ such that the $\text{Aut} C^* \otimes R^* \simeq \text{Aut} K \simeq G$.

Clearly, if $\alpha \in \text{Aut} K$, $\alpha : k \rightarrow k'$, then there exists $\tilde{\alpha} \in \text{Aut} R^*$, the unique extension of $\alpha$, such that $\tilde{\alpha}(r_k) = r_{k'}$, and $\tilde{\alpha} : Q_{r_k} \rightarrow Q_{r_{k'}}$. Thus $\text{Aut} K$ is isomorphic to a subgroup of $\text{Aut} C^* \otimes R^*$. Conversely, if $\tilde{\alpha} \in \text{Aut} C^* \otimes R^*$,
and \( \hat{a}(r_k) = r \), then \( Q_{r_k} \simeq Q_r \) and thus \( r = r_k \). Moreover, the isomorphism restricted to the canonically labeled positions is unique, thus the map \( \hat{a}(r_k) = r_k \) induces a mapping of \( k \to k' \) for each \( k \in K \) and thus an automorphism.

**Theorem 3.3.** Every finite group is isomorphic to the full automorphism group of some (extended) perfect 1-code.

**Proof.** Actually the construction and arguments have been for extended perfect 1-codes. However, note that every automorphism of \( C^* \otimes R^* \) is based on a canonical labeling of the positions \( \{0, k_1, k_2, k_3, j_4, ..., j_7\} \). In particular, position 0 is always fixed; therefore one can puncture the code so that the automorphism group remains unchanged.

In closing, note that in varying the choice of \( Q_r \) for \( r \in R^* \), \( \text{wt}(r) = 8 \), we have not effected the words of weight 4 in \( C^* \otimes R^* \); for any \( x \in \bigcup_{i \in Q_r} C^*_{m_0} \oplus \cdots \oplus C^*_{m_m}, \text{wt}(x) \geq 8 \), since \( \text{wt}(r_0, r_1, ..., r_m) = 8 \).

4. Codes of Length 16

It remains for us to establish the needed results regarding extended perfect 1-codes of order 16. First we need an automorphism-free perfect 1-code of length 16. In fact, many such codes have been constructed [8], however, one must still prove that the code is in fact rigid.

Consider the doubling construction presented by Phelps [7], in particular as it applies to codes of length 16. Let \( C^*_0, C^*_1, ..., C^*_7 \) and \( B^*_0, B^*_1, ..., B^*_7 \) be the partition \( \mathcal{V}_I \) and \( \mathcal{V} \), respectively (as listed in [7, p. 204]). Choose the permutation \( \alpha = (23)(56) \), then,

\[
D = \bigcup_{i=0}^{7} C^*_i \oplus B^*_d(i)
\]

will be a rigid extended perfect 1-code of length 16. To prove this all we need to do is establish that the Steiner quadruple system of order 16 (briefly SQS (16)), which corresponds to the words of weight 4 in \( D \) is automorphism-free.

Remark that each partition \( \mathcal{V}_I, \mathcal{V} \) induces a 1-factorization of \( K_8 \) and that these 1-factorizations have no sub-1-factorizations of order 4. Thus, the two disjoint subsystems of order 8 are unique and any automorphism of this SQS (16) must consist of 2 parts \( (\alpha, \beta) \) where \( \alpha \) is an automorphism of the subsystem \( (C^*_\alpha) \) and the 1-factorization \( \mathcal{V}_I \) as well. Similarly \( \beta \) must be an automorphism of the other subsystem \( (B^*_\beta) \) and the 1-factorization \( \mathcal{V} \) as well. The only automorphisms of \( \mathcal{V}_I \) fix the point 0 (Brouwer [1, p. 10]). The derived triple system associated with the point 0 is No. 11 (Brouwer...
K. T. PHELPS

[1, p. 9–10]; Mathon, Rosa, and Phelps [5, p. 30]), whose automorphism group has order 2. The automorphism for this system is (25) (46) (89) (1011) (1214) (1315), but (25) (46) = x is not an automorphism of VI. Hence the SQS(16) is rigid and so is the extended perfect 1-code D.

Taking this code D* and its translates one has a partition of V(16), Dj, i = 0, 1, j = 0, 1, ..., 15. Using this partition in our construction (2) with Q being any totally symmetric m-quasigroup, then we claim the resulting code C* ⊗ R* which has only “block” automorphism as required. Again we will consider the SQS(16) formed by the words of weight 4 in C* ⊗ R*. This SQS(16(m + 1)) will have m + 1 disjoint copies of our rigid SQS(16) in it (assuming that (0, 0, ..., 0) ∈ Q) and if these are the only copies of our SQS(16) then the only automorphism of this SQS(16(m + 1)) must permute these copies among themselves and hence the automorphism must be of the required form. Thus it suffices to prove the following:

**Lemma 4.1.** The only copies of the rigid SQS(16) in the SQS((m + 1) 16) associated with C* ⊗ R* are the m + 1 disjoint copies of it.

**Proof.** Any two subsystems must intersect in a subsystem. Thus if (Si, Bi), i = 0, 1, 2, ..., m are the m + 1 disjoint SQS(16) and (P, T) is another copy of this SQS(16), then |P ∩ Si| ∈ {0, 1, 2, 4, 8} and ∑i=0m |P ∩ Si| = 16.

First suppose for some i, j |P ∩ Si| > |P ∩ Sj| > 0. Then there exists x, y ∈ P ∩ Si, z ∈ P ∩ Sj with b = {x, y, z, w} ∈ T and w ∈ P ∩ Sk. If x0 = (x0,..., xₘ) is the codeword in C* ⊗ R* which corresponds to b and rᵢ is the parity of xᵢ as before, wt(r₀,..., rₘ) = 2 which is a contradiction, since r = (r₀,..., rₘ) ∈ R*. Thus |P ∩ Si| = |P ∩ Sj| whenever either are non-zero.

**Case 1 (8, 8).** This means that |P ∩ Si| = |P ∩ Sj| = 8. P ∩ Si and P ∩ Sj must be the unique disjoint pair of sub-SQS(8). Assuming that the translates Dj = D + x₀,j (where x₀,j is the characteristic vector for {0, j}), then the 1-factorization induced by this partition will have exactly 2 sub-1-factorizations on the first 8 and last 8 positions, respectively. However, this 1-factorization is the Steiner 1-factorization associated with the No. 11 STS(15). Hence the sub-1-factorizations are isomorphic to I and V, respectively—never VI (see Brouwer [1]). Hence (P, T) cannot be isomorphic to our rigid SQS(16).

**Case 2 (4, 4, 4, 4).** If {x, y} ∈ P ∩ Si and z ∈ P ∩ Sj and {x, y, z, w} ∈ T then w ∈ P ∩ Sj, otherwise a parity argument similar to the one used above would give a contradiction regarding wt(r), r ∈ R*. But this means that (P, T) has a sub-SQS(8) on P ∩ (Si ∪ Sj) whenever |P ∩ Si| = |P ∩ Sj| = 4, which gives us too many sub-SQS(8) in (P, T) for it to be isomorphic to our rigid SQS(16).
Case 3 (\(|P \cap S_i| = 2\)). Again the same argument as in the previous case forces \(P \cap (S_i \cup S_j)\) to be a quadruple in \((P, T)\) whenever \(|P \cap S_i| = |P \cap S_j| = 2\). Moreover for any \(b \in T\), the corresponding codeword \(x_b \in C^* \otimes R^*\) has an associated parity vector \(r_b \in R^*\). The set of \(r_b, b \in T\) such that \(\text{wt}(r_b) = 4\) (i.e., \(b \cap S_j = 0\) or \(1\)) must form a sub-SQS(8) in \(R^*\). We conclude that for each such \(r_b\) with \(r_{b_i} = 1, i = 0, 1, 2, 3\) then on \(P \cap (\bigcup_{i=0}^{3} S_{b_i})\) \((P, T)\) must contain a sub-SQS(8). Again this gives too many sub-SQS(8).

Case 4 (\(|P \cap S_i| = 1\)). For each \(b \in T\) there is a corresponding \(r_b \in R^*\); these must form a sub-SQS(16) in \(R^*\) isomorphic to \((P, T)\) and thus \((P, T)\) is not isomorphic to our rigid SQS(16).

ACKNOWLEDGMENT

The author would like to acknowledge the helpful discussions he had with E. Mendelsohn [7]. In particular Professor Mendelsohn made some key observations which allowed for the relaxation of the hypothesis and greatly facilitated the proof of Lemma 4.1.

REFERENCES

2. R. FRUCHT, Herstellung von Graphen mit vorgegeben abstrakter gruppe, Compositio Math. 6 (1938), 239-250.
7. E. MENDELSOHN, private communication.