Theorem 6: $\mathcal{G}$ has minimum distance 8.

Proof: Again it is sufficient to show that $\mathcal{G}$ has minimum weight 8. By Theorem 3 there are only two possibilities which we must consider. The first of these is $X = \varnothing$, $|Y| \geqslant 6$. In this case Y corresponds to a codeword in $\overline{\mathcal{D}}'$, so $|Y| \geqslant 8$ by Lemma 4. The second possibility is $|X| = 2$, $|Y| \geqslant 4$. The automorphisms a) and c) of Theorem 2 show that we may assume without loss of generality that $X = \{0, 1\}$. From Definition 2 c) and d) we find that Y corresponds to a codeword in $\overline{\mathcal{D}}$, i.e., $|Y| \geqslant 6$ by Lemma 3. Finally we observe that $|X| = |Y| = 4$ is possible by taking $X = Y = \{0, \alpha, \beta, \alpha + \beta\}$. □

To find the cardinality of $\mathcal{G}$ we can use exactly the same method as in the proof of Theorem 4. Since $(n, r) = (n, s) = 1$ the polynomials $m_r(x)$ and $m_s(x)$ have degree m. Hence $\mathcal{D}'$ has dimension $n - 3m$. The argument of Theorem 4 now shows that $|\mathcal{G}| = 2^l$, where $l = 2^{m+1} - 3m - 2$.

References

[1] R. D. Baker, "Partitioning the planes $AG_{2m}(2)$ into 2-designs," *Discrete Math.*, vol. 15, pp. 205–211, 1976.

[2] P. J. Cameron and J. H. van Lint, "Graphs, codes and designs," *London Math. Soc. Lecture Note Series*, vol. 43, Cambridge Univ., 1980.

[3] J. M. Goethals, "Nonlinear codes defined by quadratic forms over GF(2)," *Inform. Contr.*, vol. 31, pp. 43–74, 1976.

[4] W. M. Kantor, "On the equivalence of generalized Preparata Codes," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 345–348, May 1983.

[5] J. H. van Lint, *Introduction to Coding Theory.* New York: Springer Verlag, 1982.

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

[7] F. P. Preparata, "A class of optimum non-linear double-error-correcting codes," *Inform. Contr.*, vol. 13, pp. 378–400, 1968.

[8] G. V. Zaitsev, V. A. Zinovjev, and N. V. Semakov, "Interrelation of Preparata and Hamming codes and extension of Hamming codes to new double-error-correcting codes," B. N. Petrov and F. Csaki, Eds., in *Proc. 2nd Int. Symp. Inform. Theory*, Akadémiai Kiadó, Budapest, pp. 257–263, 1973.

[9] C. Roos, "A new lower bound for the minimum distance of a cyclic code,'" *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 330–332, May 1983.

On the Inequivalence of Generalized Preparata Codes

WILLIAM M. KANTOR

DEDICATED TO JESSIE MACWILLIAMS ON THE OCCASION OF HER RETIREMENT FROM BELL LABORATORIES

***Abstract*—If m is odd and $\sigma \in \operatorname{Aut} GF(2^m)$ is such that $x \to x^{\sigma^2 - 1}$ is $1-1$, there is a $[2^{m+1} - 1, 2^{m+1} - 2m - 2]$ nonlinear binary code $P(\sigma)$ having minimum distance 5. All the codes $P(\sigma)$ have the same distance and weight enumerators as the usual Preparata codes (which rise as $P(\sigma)$ when $x^\sigma = x^2$). It is shown that $P(\sigma)$ and $P(\tau)$ are equivalent if and only if $\tau = \sigma^{\pm 1}$, and Aut $P(\sigma)$ is determined.**

I. Introduction

In [13], Preparata introduced a family of $[2^{m+1} - 1, 2^{m+1} - 2m - 2]$ nonlinear binary 2-error correcting codes, where m is odd and $m > 1$. These have remarkable combinatorial properties: they are nearly perfect codes (Goethals and Snover [7]; Cameron and van Lint [4, ch. 16]) and, in particular, they are uniformly packed (Semakov, Zinovjev, and Zaitsev [14]); they give rise to designs [14], [15], [7], [12, p. 473], [4, pp. 89–90]; and they produce parallelisms of the lines of $PG(m,2)$ [15]; [1]. The published descriptions of these codes [13], [15], [12, § 15.6], [4] are complicated and difficult to work with. Fortunately, Baker and Wilson [2] have found a relatively simple description which led to a generalization of Preparata's codes.

Manuscript received September 11, 1981; revised March 23, 1982.

The author is with the Department of Mathematics, University of Oregon, Eugene, OR 97403.

Let m be odd, $m > 1$, and let $\sigma \in \operatorname{Aut} GF(2^m)$, where $x \to x^{\sigma^2 - 1}$ is $1-1$. (Thus, if $x^\sigma = x^{2^i}$ for all x then i and m are relatively prime.) Baker and Wilson constructed a code $P(\sigma)$ having the same parameters as Preparata's codes (cf. (1)), and hence having the same combinatorial properties. Moreover, their description makes a group of $(2^m - 1)m$ automorphisms very visible. We will show that this group is precisely $\operatorname{Aut}(P(\sigma)$ when $m > 3$, and that two generalized Preparata codes $P(\sigma)$ and $P(\tau)$ are equivalent if and only if $\tau = \sigma^{\pm 1}$. Similar results are obtained for the extended codes $\bar{P}(\sigma)$ of length 2^{m+1}.

All the codes $P(\sigma)$ (for fixed m) have the same distance and weight enumerators (by Goethals and Snover [7, p. 85]). One of the many curious properties of the extended Preparata codes is that their weight enumerators are related to those of the Kerdock codes [11] in exactly the same manner as are the enumerators of a linear code and its dual [11], [7], [12, p. 468]. This naturally leads to speculations as to whether extended Preparata and Kerdock codes are dual in some direct, nonarithmetic sense. However, the results in this paper and in Kantor [10] strongly suggest that this apparent relationship between these codes is merely a coincidence.

II. Definitions

Let $F = GF(2^m)$, where m is odd and $m > 1$. Form the $(m+1)$-dimensional GF(2)-space $V = F \oplus GF(2)$. If $x \in F$ and $i \in GF(2)$ we will write $(x, i) = x_i$. Also, if $X, Y \subseteq F$ we will write

$$X_0Y_1 = (X,0) \cup (Y,1).$$

Let 2^V denote the set of all subsets of V. This is a 2^{m+1}-dimensional GF(2)-space under symmetric difference Δ. (We use Δ in order to avoid confusion with addition in F and V).

If $X \subseteq F$ and $0 \leqslant k \in \mathbb{Z}$, write $\Sigma X^k = \Sigma_{x \in X} x^k$. (We use the convention $0^0 = 1$.)

Let $\sigma \in \operatorname{Aut} F$, where $x \to x^{\sigma^2 - 1}$ is $1-1$. Then the generalized extended Preparata code $\bar{P}(\sigma)$ is the following subset of 2^V:

$$\bar{P}(\sigma) = \Big\{ X_0Y_1 \Big| \sum X^0 = \sum Y^0 = 0, \sum X^1 = \sum Y^1, \sum X^{\sigma+1} + \sum Y^{\sigma+1} + \big(\sum X^1\big)^{\sigma+1} = 0 \Big\}. \quad (1)$$

Here, $|\bar{P}(\sigma)| = 2^{2^{m+1}} - 2m - 2$, and $|A \Delta B| \geqslant 6$ for all distinct $A, B \in \bar{P}(\sigma)$ (Preparata [13] if $x^\sigma = x^2$ for all x; Baker and Wilson [2] in general). Thus, $\bar{P}(\sigma)$ is a $[2^{m+1}, 2^{m+1} - 2m - 2]$ code with minimum distance 6. (It is a straightforward but amusing exercise to verify all of these assertions.)

The generalized Preparata code $P(\sigma)$ is obtained by deleting 0_0 from V and from all members of $\bar{P}(\sigma)$. This is a $[2^{m+1} - 1, 2^{m+1} - 2m - 2]$ code with minimum distance 5.

Aut $\bar{P}(\sigma)$ is the group of permutations of V sending $\bar{P}(\sigma)$ to itself. This group is easily seen to contain the 2^{m+1} translations of V:

$$x_i \to (x+b)_{i+j} \qquad \text{for fixed } b, j. \quad (2)$$

It also contains the group

$$\{x_i \to (ax^\varphi)_i | a \in F^*, \varphi \in \operatorname{Aut} F\} \quad (3)$$

of order $(2^m - 1)m$. Clearly, this group is contained in Aut $P(\sigma)$, and has the normal subgroup

$$\{x_i \to (ax)_i | a \in F^*\}. \quad (4)$$

(In fact, (4) is the commutator subgroup of (3).)

Since Aut $\bar{P}(\sigma)$ is transitive on V, all punctured codes of $\bar{P}(\sigma)$ are equivalent to $P(\sigma)$.

III. Statement of Results

Our goals are the following theorems.

Theorem 1: $\bar{P}(\sigma)$ and $\bar{P}(\tau)$ are equivalent if and only if $\sigma = \tau^{\pm 1}$.

Theorem 2: $P(\sigma)$ and $P(\tau)$ are equivalent if and only if $\sigma = \tau^{\pm 1}$.

In view of the transitivity of Aut $\bar{P}(\sigma)$, Theorem 1 is an immediate consequence of Theorem 2.

Theorem 3: If $m > 3$, then Aut $\bar{P}(\sigma)$ is the group of order $2^{m+1}(2^m - 1)m$ generated by the permutations in (2) and (3).

Theorem 4: If $m > 3$, then Aut $P(\sigma)$ is the group (3).

Once again, Theorem 3 follows immediately from Theorem 4. If $m = 3$ then Aut $P(\sigma) \cong A_7$, while Aut $\bar{P}(\sigma)$ is a semidirect product of the group of translations of V with A_7 (Berlekamp [3]).

Theorem 2 will be proved using elementary linear algebra, Sylow's theorem and a standard number theoretic result. Theorem 4 requires more complicated machinery.

Notation: Write $G(\sigma) = \operatorname{Aut} P(\sigma)$.

IV. Recovering the Hamming Codes

Each code $P(\sigma)$ is a $[2^{m+1} - 1, 2^{m+1} - 2m - 2]$ code with minimum distance 5. Such codes have been studied by Semakov, Zinovjev, and Zaitsev [14], [15] and Goethals and Snover [7]. They showed that the distance enumerator depends only on m. Moreover, they showed that, if the words at distance $\geqslant 3$ from each codeword are adjoined to the code, the resulting code is a perfect 1-error correcting code [15, p. 258], [7, p. 86].

Proposition 1: Let $H(P(\sigma))$ consist of $P(\sigma)$ and all words in 2^V at distance $\geqslant 3$ from $P(\sigma)$. Then $H(P(\sigma))$ is the Hamming code of length $2^{m+1} - 1$ determined by V.

Proof: Set $H = \{X_0Y_1 \in 2^{V - \{0\}} | 1 + \Sigma X^0 = \Sigma Y^0 = 0, \Sigma X^1 = \Sigma Y^1\}$. Then H is the Hamming code of length $2^{m+1} - 1$. By (1), $P(\sigma) \subset H$. Since H has minimum distance 3 $H \subseteq H(P(\sigma))$. As already noted, $H(P(\sigma))$ is a perfect 1-error correcting code, and hence $|H| = |H(P(\sigma))|$. Consequently, $H = H(P(\sigma))$.

Corollary 1: Each isomorphism $P(\sigma) \to P(\tau)$ is induced by a linear transformation of V. (In particular, $G(\sigma) \leqslant GL(m+1, 2)$.)

Proof: $H(P(\sigma)) = H(P(\tau))$ is the Hamming code determined by V, and Aut $H(P(\sigma)) = GL(m+1, 2)$.

V. Proof of Theorem 2

Assume that h is a permutation of V sending $P(\sigma)$ to $P(\tau)$. By Corollary 1, $G(\sigma)$, $G(\tau)$, and h all belong to $GL(m+1, 2)$. Note that $h^{-1}G(\sigma)h = G(\tau)$.

There is a prime q such that $q | 2^m - 1$ but $q \nmid 2^j - 1$ for $1 \leqslant j < m$ (Zsigmondy [16]). Let Q be a Sylow q-subgroup of the group (4). Then Q is also a Sylow q-subgroup of $GL(m+1, 2)$, and $Q \leqslant G(\sigma) \cap G(\tau)$.

Since $h^{-1}Qh \leqslant G(\tau)$, by Sylow's theorem $h_1^{-1}(h^{-1}Qh)h_1 = Q$ for some $h_1 \in G(\tau)$. Set $g = hh_1$. Then g is an isomorphism from $P(\sigma)$ to $P(\tau)$, and $g^{-1}Qg = Q$.

The cyclic group Q has exactly two proper invariant subspaces: F_0 and $\{0_0, 0_1\}$. The normalizer N of Q in $GL(m+1,2)$ must leave each of these invariant. Then $|N| = (2^m - 1)m$ (see the Appendix), and hence $N \leqslant G(\sigma)$ by (3).

Consequently, $g \in G(\sigma)$, and hence $P(\tau) = P(\sigma)^g = P(\sigma)$.

Lemma 1: $P(\sigma) = P(\tau)$ if and only if $\tau = \sigma^{\pm 1}$.

Proof: If $\tau = \sigma^{-1}$, then $(X^{\sigma+1})^\tau = X^{\tau+1}$, so that $P(\sigma) = P(\tau)$ by definition (1).

Conversely, assume that $P(\sigma) = P(\tau)$. Let $\{y\}_0\{a, b, c, x\}_1 \in P(\sigma)$. By definition, a, b, c, and x are distinct, $y = a + b + c + x \neq 0$, and

$$y^{\sigma+1} + (a^{\sigma+1} + b^{\sigma+1} + c^{\sigma+1} + x^{\sigma+1}) + y^{\sigma+1} = 0.$$

Conversely, if a, b, c, are distinct and if $x^{\sigma+1} = a^{\sigma+1} + b^{\sigma+1} + c^{\sigma+1}$, then $x \neq a + b + c$ (since $\{a, b, c, a+b+c\}_0 \notin \overline{P}(\sigma)$), $y = a + b + c + x \neq 0$, and $\{y\}_0\{a, b, c, x\}_1 \in P(\sigma)$.

Thus, if $a^{\sigma+1} + b^{\sigma+1} + c^{\sigma+1} = x^{\sigma+1}$ then $a^{\tau+1} + b^{\tau+1} + c^{\tau+1} = x^{\tau+1}$. The identity

$$(a^{\sigma+1} + b^{\sigma+1} + c^{\sigma+1})^{\tau+1} = (a^{\tau+1} + b^{\tau+1} + c^{\tau+1})^{\sigma+1} \qquad (5)_{\sigma,\tau}$$

must hold for all distinct $a, b, c \in F^*$. Of course, $(5)_{\sigma,\tau}$ also holds if $a = b$.

We will show that $(5)_{\sigma,\tau}$ implies that $\tau = \sigma^{\pm 1}$. Apply σ^{-1} to $(5)_{\sigma,\tau}$ in order to obtain $(5)_{\sigma^{-1},\tau}$. We can therefore replace σ by σ^{-1} if desired.

Let $x^\sigma = x^{2^i}$ and $x^\tau = x^{2^j}$ for some i, j where $0 \leqslant i, j < m$. Replacing σ and τ by their inverses if necessary, we may assume that $i, j \leqslant \frac{1}{2}(m-1)$. We wish to prove that $i = j$. Assume that $i < j$.

Fix b and c with $b \neq c$. Set $d = b^{\sigma+1} + c^{\sigma+1}$ and $e = b^{\tau+1} + c^{\tau+1}$. Then $(5)_{\sigma,\tau}$ asserts that the polynomial

$$f(t) = (t^{\sigma+1} + d)^{\tau+1} - (t^{\tau+1} + e)^{\sigma+1}$$

vanishes on F^*. Consequently, $t^{2^m-1} - 1$ divides $f(t)$. However, since $d \neq 0$ the degree of f is $2^{i+j} + 2^j < 2^m - 1$.

This contradiction proves Lemma 1 and completes the proof of Theorem 2.

Remark 1: We have seen that $\{a+b+c+x\}_0\{a, b, c, x\}_1 \in P(\sigma)$ whenever a, b, and c are distinct elements of F such that $a^{\sigma+1} + b^{\sigma+1} + c^{\sigma+1} = x^{\sigma+1}$.

VI. Proof of Theorem 4

By Corollary 1, $G(\sigma)$ is a subgroup of $GL(m+1,2)$.

Lemma 2: If $g \in G(\sigma)$ and g fixes every element of F_0 then $g = 1$.

Proof: Assume that $g \neq 1$. Since g is the identity on the hyperplane F_0 of V, g has the form

$$g\colon \begin{cases} x_0 \to x_0 \\ x_1 \to (x+k)_1 \end{cases}$$

for a fixed $k \in F^*$. Let $X_0Y_1 \in P(\sigma)$. Then $X_0(Y+k)_1 \in P(\sigma)$, so that $\Sigma(Y+k)^{\sigma+1} = \Sigma Y^{\sigma+1}$. Expanding, we find that $k^{-1}\Sigma Y^1 \in GF(2)$ for each choice of (X, Y). By Remark 1, this is ridiculous.

Lemma 3: Let H be the subgroup of $G(\sigma)$ consisting of all elements fixing F_0 and 0_1. Then $|H| = (2^m - 1)m$.

Proof: By Lemma 2, H is essentially a subgroup of $GL(m,2)$, acting on the hyperplane F_0. Moreover, H contains the group (4). All subgroups of $GL(m,2)$ containing (4) were determined in Kantor [9]. Namely, we can write $m = de$ in such a way that H contains $SL(d, 2^e)$ as a normal subgroup. Moreover, when F is regarded as a d-dimensional vector space over $GF(2^e)$, the group H consists of $GF(2^e)$—semilinear transformations of F.

If $d = 1$ then $GF(2^e) = F$, in which case Lemma 3 holds. We will therefore assume that $d > 1$ and derive a contradiction.

Let a and b be any elements of F linearly independent over $GF(2^e)$. Define c by $c^{\sigma+1} = a^{\sigma+1} + b^{\sigma+1}$, so that $\{a+b+c\}_0\{0, a, b, c\}_1 \in P(\sigma)$ by Remark 1. Then $SL(d, 2^e)$ has an element interchanging a and b while moving c, unless c is a $GF(2^e)$-multiple of $a + b$, in which case (since $c \neq a + b$) $SL(d, 2^e)$ has an element interchanging a and c while moving b. By symmetry, we may assume that H has an element interchanging a and b while moving c. This element sends the above codeword to another codeword of the form $\{u\}_0\{0, b, a, c'\}_1$ with $c' \neq c$. Since we now have two different codewords whose distance is at most 4, this is impossible.

Lemma 4: $|G(\sigma)| = (2^m - 1)m$ or $2^m(2^m - 1)m$.

Proof: Since H is transitive on F_0, one of the following holds (Cameron–Kantor [5, p. 403 and th. I]): $G(\sigma) = SL(m+1,2)$, $G(\sigma)$ fixes F_0, or $G(\sigma)$ fixes 0_1. (*Note*: When $m = 3$, [5] also allows $G(\sigma)$ to be A_7, which is indeed the case.) By Lemma 3, $G(\sigma) \neq SL(m+1,2)$.

Assume that $G(\sigma)$ fixes F_0 but moves 0_1. Then $G(\sigma)$ is transitive on F_1 (since H is already transitive on $F^*{}_1$). By Lemma 3, $|G(\sigma)| = |F_1||H| = 2^m(2^m - 1)m$.

If $G(\sigma)$ fixes 0_1 but moves F_0, then $G(\sigma)$ is transitive on the 2^m hyperplanes not containing 0_1, and hence $|G(\sigma)| = 2^m \cdot (2^m - 1)m$ by Lemma 3.

Lemma 5: $G(\sigma)$ fixes 0_1.

Proof: Assume that $G(\sigma)$ moves 0_1. By Lemmas 2 and 4, $G(\sigma)$ induces a group of order $2^m(2^m - 1)m$ on F_0. On the other hand, as in Lemma 3 we can write $m = de$ so that $G(\sigma)$ contains $SL(d, 2^e)$. Since $|G(\sigma)| = 2^m(2^m - 1)m$, we have $d > 1$, and then $|SL(d, 2^e)|$ does not divide $2^m(2^m - 1)m$. (*Note*: When $m = 3$, $2^m(2^m - 1)m = |SL(3,2)|$ is the order of the stabilizer of F_0 in $G(\sigma)$.)

Lemma 6: $G(\sigma)$ fixes F_0.

Proof: Assume that $G(\sigma)$ moves F_0. Then $G(\sigma)$ again acts on an m-dimensional vector space, namely, $\overline{V} = V/\{0_0, 0_1\}$. Once again, we find that $|SL(d, 2^e)|$ divides $2^m(2^m - 1)m$ for some d and e satisfying $de = m$. However, this time we can only conclude that $d = 1$. That is, $G(\sigma)$ induces a group of order $(2^m - 1)m$ on $\overline{V}$.

Consequently, $G(\sigma)$ contains 2^m elements inducing the identity on $\bar{V}$. There are exactly 2^m such elements g of $GL(m+1,2)$, and they can be described as follows (by an elementary calculation): there is a linear functional T: $F \to GF(2)$ such that g sends $x_i \to x_i + T(x)0_1$ for all x.

Let $\{u\}_0\ \{0, a, b, c\}_1 \in P(\sigma)$ (cf. Remark 1). Then $a+b+c=u$, so $c \neq a+b$. Since T can be any linear functional, choose it so that $u, c \in \operatorname{Ker} T$, but $a, b \notin \operatorname{Ker} T$. Applying the above automorphism, we obtain a codeword $\{u, a, b\}_0\ \{0, c\}_1$ at distance 4 from the original one. This contradiction proves Lemma 6.

Now Theorem 4 follows from Lemmas 4–6.

VII. Concluding Remarks

1) In order to clarify the relationship between Theorems 2 and 4, we will show how to deduce the former from the latter. (This also provides further motivation for the proof in Section V.)

Let g: $P(\sigma) \to P(\tau)$ be an isomorphism. By Theorem 4 and (3), g sends the unique fixed point 0_1 of $G(\sigma)$ to the unique fixed point 0_1 of $G(\tau)$. Similarly, $G(\sigma)$ sends F_0 to F_0. If $(1_0)^g = a_0$, compose g with $x_i \to (a^{-1}x)_i$ in order to assume that $(1_0)^g = 1_0$.

By Theorem 4, g normalizes the commutator subgroup (4) of $G(\sigma) = G(\tau)$. By the Appendix, there is a field automorphism φ such that $(x_0)^g = (x^\varphi)_0$ for all x, while $(0_1)^g = 0_1$. Thus $g \in G(\sigma)$, and hence $P(\sigma) = P(\tau)$. Now Lemma 1 completes the proof.

2) Baker and Wilson [2] have shown that one of the codes found by Goethals [6] can be described as $\bar{P}(\sigma) \cap \bar{P}(\tau)$, where $x^\sigma = x^{2^t}$, $x^\tau = x^{2^{t+1}}$ and $m = 2t+1 > 3$. This code has minimum distance 8. It clearly admits $G(\sigma)$. Imitating the proof of Theorem 4, we find that its group of affine linear automorphisms has order $2^{m+1}(2^m-1)m$ and is generated by the permutations in (2) and (3). However, it is not clear how to recover the extended Hamming code from $\bar{P}(\sigma) \cap \bar{P}(\tau)$.

Appendix

In Sections V and VI we used a standard, elementary result concerning certain linear transformations (Huppert [8, (7.3a)]). For completeness, we will include a short proof of the required result.

Let $F = GF(q^m)$, and regard F as a vector space over $GF(q)$. The group

$$H = \{x \to ax \mid a \in F^*\}$$

is a cyclic group of linear transformations.

Lemma: Let $g \in H$, and assume that $|g| \nmid q^j - 1$ whenever $1 \leqslant j < m$. Then the normalizer N of $\langle g \rangle$ in $GL(m,q)$ is isomorphic to the group of transformations $x \to ax^\varphi$ for $a \in F^*$ and $\varphi \in \operatorname{Aut} F$. In particular, $|N| = (q^m-1)m$.

Proof: Clearly, N contains H. If $n \in N$ and $1^n = a$ then $1^{nh} = 1$ for some $h \in H$. It therefore suffices to show that, if $1^n = 1$, then $x \to x^n$ is an automorphism of F.

Each $GF(q)$-linear combination of powers of g lies inside the field $H \cup \{0\}$. By hypothesis, $GF(q)[g]$ cannot be $GF(q^j)$ for $1 \leqslant j < m$. Thus, $GF(q)[g] = H \cup \{0\}$. In particular, n normalizes H.

If $H = \langle d \rangle$ and $n^{-1}dn = d^l$ for some $l \in \mathbb{Z}$, then $n^{-1}hn = h^l$ for all $h \in H$.

Let $f \in F^*$, and let h: $x \to fx$. Then

$$f^n = (f1)^n = 1^{hn} = 1^{n^{-1}hn} = 1^{h^l} = f^l 1 = f^l.$$

Since $f \to f^l$ is an automorphism of F^*, so is n. Consequently $n \in \operatorname{Aut} F$, as required.

Acknowledgment

I am grateful to R. D. Baker for providing me with the elegant description of the codes $\bar{P}(\sigma)$; to J. H. van Lint for many helpful comments; and to Bell Laboratories, where much of this research took place.

References

[1] R. D. Baker, "Partitioning the planes of $AG_{2m}(2)$ into 2-designs," *Disc. Math.*, vol. 15, pp. 205–211, 1976.
[2] R. D. Baker and R. M. Wilson (1974; unpublished).
[3] E. R. Berlekamp, "Coding theory and the Mathieu groups." *Inform. Contr.*, vol. 18, pp. 40–64, 1971.
[4] P. J. Cameron and J. H. van Lint, "Graph theory, coding theory and block designs." *LMS Lecture Note Series*, no. 19, 1975.
[5] P. J. Cameron and W. M. Kantor, "2-transitive and antiflag transitive collineation groups of finite projective spaces." *J. Algebra*, vol. 60, pp. 384–422, 1979.
[6] J.-M. Goethals, "Nonlinear codes defined by quadratic forms over GF(2)," Inform. Contr., vol. 31, pp. 43–74, 1976.
[7] J.-M. Goethals and S. L. Snover, Nearly perfect binary codes," *Disc. Math.*, vol. 3, pp. 65–88, 1972.
[8] B. Huppert, Endliche Gruppen I. New York: Springer, 1967.
[9] W. M. Kantor, "Linear groups containing a Singer cycle," *J. Algebra*, vol. 62, pp. 232–234, 1980.
[10] W. M. Kantor, "An exponential number of generalized Kerdock codes," *Inform. Contr.*, to appear.
[11] A. M. Kerdock, "A class of low-rate non-linear binary codes." *Inform. Contr.*, vol. 20, pp. 182–187, 1972.
[12] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes. Amsterdam: North Holland, 1977.
[13] F. P. Preparata, "A class of optimum nonlinear double-error-correcting codes," *Inform. Contr.*, vol. 13, pp. 378–400, 1968.
[14] N. V. Semakov, V. A. Zinovjev, and G. V. Zaitsev, "Uniformly packed codes," *Probl. Peredaci Inform.*, vol. 7, pp. 38–50, 1971 (Russian); trans. in *Problems of Information Transmission*, vol. 7, pp. 30–39, 1971.
[15] G. V. Zaitsev, V. A. Zinovjev, and N. V. Semakov, "Interrelation of Preparata and Hamming codes and extension of Hamming codes to new double-error correcting codes," in *Proc. 2nd Int. Symp. Inform. Theory*, Akademiai Kaidó, Budapest, pp. 257–263, 1973.
[16] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. f. Math. u. Phys.*, vol. 3, pp. 265–284, 1892.