INFORMATION AND CONTROL 37, 19–22 (1978)

# An Elementary Proof of the MacWilliams Theorem on Equivalence of Codes

KENNETH BOGART, DON GOLDBERG, AND JEAN GORDON

*Dartmouth College, Hanover, New Hampshire 03755*

In this paper, we prove the following theorem due to MacWilliams. Two codes are equivalent if and only if there is a weight preserving linear isomorphism between them. The proof we give is a simplification and extension of her proof to the most general case.

## 1. INTRODUCTION

An $(n, k)$ code, $C$, over a finite field, $F = GF(q)$, $q$ a prime power, is a $k$ dimensional subspace of the vector space, $V$, of all $n$-tuples of elements of $F$. $C$ can thus be represented by a $k \times n$ matrix, called a generator matrix for $C$, whose rows consist of some chosen basis for $C$.

Two $(n, k)$ codes, $C$ and $D$, are called equivalent, denoted $C \sim D$, if there exists an $n \times n$ monomial matrix, $A$, (i.e., $A$ has exactly one non-zero element of $F$ in each row and column) such that $D = \{vA \mid v \in C\}$ (Peterson, 1961). (The matrix, $A$, represents a monomial transformation of $V$, which can be viewed as a permutation of the coordinates of each vector followed by multiplying one or more coordinates by nonzero scalars.) It is not difficult to show that $C \sim D$ iff given any generator matrix, $X$, for $C$, there exists a generator matrix, $Y$, for $D$ and a monomial matrix, $A$, over $F$ such that $XA = Y$.

Although the above definition is useful, we would like a coordinate-free description of equivalence. With this aim, we call a $1 - 1$ linear transformation from $C$ to $D$ an isometry if it preserves weights, where the weight of a vector, $v$, in $V$ is the number of its non-zero entries, denoted $w(v)$. We prove that $C \sim D$ iff $C$ is isometric to $D$.

Clearly, an equivalence defines a $1 - 1$ linear transformation of $V$ onto itself which carries the standard basis vectors of $V$ onto scalar multiples of these vectors: $e_iA = l_{ij}e_j$, where $A = (l_{ij})$. Restricted to $C$, this isometry of $V$ is an isometry of $C$ onto $D$.

To obtain an equivalence from an isometry of $C$ to $D$, we choose a generator matrix, $X$, for $C$ and construct, via the isometry, a generator matrix, $Y$, for $D$ whose columns are scalar multiples of those of $X$, i.e., $Y = XA$ for some $A$. In so doing we have actually extended the given isometry to all of $Y$. This analog



0019-9958/78/0371-0019$02.00/0

of Witt's theorem of metric geometry was first proved by F. J. MacWilliams (1962). She proved the case in which $q$ is a prime, but noted that the result held for $q$ a prime power. The proof we present is a simplification and extension of her proof to this general case. K. P. Bogart has given a different, more algebraic proof in the special case $q = 2$.

## 2. Main Results

Let $L_1, \ldots, L_{\mu(k)}$ be a list of the one dimensional subspace of the vector space, $F^k$, of all $k$-tuples of elements of $F$. Clearly, $\mu(k) = (q^k - 1)/(q - 1)$.

Definition. $L_i$ is orthogonal to $L_j$, denote $L_1 \perp L_j$, if $u_i \cdot u_j = 0$, for all non-zero vectors $u_i, u_j$ in $L_i, L_j$, respectively ($u_i, u_j$ will henceforth denote nonzero vectors of $L_i, L_j$) and where "$\cdot$" is the standard inner product in the arithmetic of $F$. It is trivial to check that if $u_i \cdot u_j = 0$, then $u \cdot u' = 0$ for any two non-zero vectors $u, u'$ in $L_i, L_j$.

Let $T = (t_{ij})$ be the $\mu(k) \times \mu(k)$ matrix of 0's and 1's where

$$t_{ij} = \begin{cases} 0 & \text{if } L_i \perp L_j \\ 1 & \text{otherwise.} \end{cases}$$

$T$ is the "orthogonality matrix" of the one dimensional subspaces of $F^k$. We will next show that $T$ is invertible over $Q$ ($Q$ = rational numbers) and for this purpose, prove the following four propositions. ($| S |$ is the size of the set $S$.)

Proposition 1. $|\{L_j \mid L_j \perp L_i\}| = \mu(k - 1)$.

*Proof.* The above set consists of the one dimensional subspaces of the kernel of the map $P: F^k \to F$ where $P(u) = u \cdot u_i$, $u_i \in L_i$. Since dim(domain of $P$) = dim(kernel of $P$) + dim(image of $P$), dim(kernel of $P$) $= k - 1$.

Proposition 2. *If* $i \neq j$, $|\{L_k \mid L_k \perp L_i$ *and* $L_k \perp L_j\}| = \mu(k - 2)$.

*Proof.* The above set consists of the one dimensional subspaces of the kernel of the map $P': F^k \to F^2$ where $P'(u) = (u \cdot u_i, u \cdot u_j)$, $u_i, u_j \in L_i, L_j$. By the dimension argument used in Prop. 1, dim(kernel of $P'$) $= k - 2$.

Proposition 3. *The sum over* $Q$ *of the rows of* $T$ *is the constant row vector,* $x = (x_1, \ldots, x_{\mu(k)})$, *with* $x_i = \mu(k) - \mu(k - 1)$ *for all* $i$.

*Proof.* Let $x$ be the sum of the rows of $T$. Then $x_i = |\{L_j \mid L_j \not\perp L_i\}| = \mu(k) - |\{L_j \mid L_j \perp L_i\}| = \mu(k) - \mu(k - 1)$ by Proposition 1.

Proposition 4. *The sum of the rows of* $T$ *which are* 0 *in column* $j$ *is the row vector,* $y(j) = (y_1, \ldots, y_{\mu(k)})$, *with* $y_j = 0$ *and* $y_i = \mu(k - 1) - \mu(k - 2)$ *for all* $i$ *different from* $j$.

*Proof.* If $i \neq j$, $y_i = |\{L_k \mid L_k \perp L_j \text{ and } L_k \not\perp L_i\}| = |\{L_k \mid L_k \perp L_j\}| - |\{L_k \mid L_k \perp L_j \text{ and } L_k \perp L_i\}| = \mu(k-1) - \mu(k-2)$.

LEMMA 1. *$T$ is invertible over $Q$.*

*Proof.* First, $\mu(k) - \mu(k-1) \neq 0$, $\mu(k-1) - \mu(k-2) \neq 0$, by simple computation. For $j = 1,\ldots, \mu(k)$, let

$$e_j = \frac{x}{\mu(k) - \mu(k-1)} - \frac{y(j)}{\mu(k-1) - \mu(k-2)}.$$

Then the set $\{e_1, \ldots, e_{\mu(k)}\}$ is just the standard basis for $Q^{\mu(k)}$. Therefore, the row space of $T$ is all of $Q^{\mu(k)}$ and the rank of $T$ is $\mu(k)$. $T$ is thus invertible.

Choose a generator matrix, $X$, for $C$. Let $f: F^k \to C$ be the isomorphism defined by $f(u) = uX$, $u \in F^k$. Then $X$ is the matrix of $f$ relative to the standard basis for $F^k$; i.e., $f(e_i)$ is the $i$-th row of $X$, where $\{e_1, \ldots, e_k\}$ is the standard basis for $F^k$. Clearly, $f$ maps the one-dimensional subspaces of $F^k$ onto those of $C$, where $f[L_i] = \langle f(u_i) \rangle$, $u_i \in L_i$.

DEFINITION. Let $c$ denote a column of $X$. We define $r = (r_1, \ldots, r_{\mu(k)})^t$ to be the column vector with entries

$$r_i = |\{c \neq 0 \mid c^t \in L_i\}|.$$

The vector $r$ specifies the non-zero columns of $X$ up to scalar multiplication and ordering. Note that $X$ has $(n - \sum_{i=1}^{\mu(k)} r_i)$ zero columns. We now interpret the column vector $Tr$ as a list of the weights of the one dimensional subspaces of $C$ in the order defined by the list $L_1, \ldots, L_{\mu(k)}$, the one dimensional subspaces of $F^k$.

LEMMA 2. *$(Tr)_i = w(f[L_i])$ where $w(f[L_i])$ is defined to be $w(f(u_i))$, $u_i \in L_i$.*

*Proof.*

$$\begin{aligned}
(Tr)_i &= \sum_{j=1}^{\mu(k)} t_{ij} r_j \\
&= \sum_{j: L_j \not\perp L_i} r_j \\
&= \sum_{j: L_j \not\perp L_i} |\{c \neq 0 \mid c^t \in L_j\}| \\
&= |\{c \neq 0 \mid c^t \in L_j \text{ and } c^t \not\perp u_i, u_i \in L_i\}| \\
&= w(u_i X) \\
&= w(f(u_i)) \\
&= w(f[L_i]).
\end{aligned}$$

We will now construct a generator matrix, $Y$, for the code $D$ isometric to $C$, whose columns will be scalar multiples of those of $X$; i.e. $Y = X\Lambda$, $\Lambda$ an $n \times n$ monomial matrix over $F$. Let $g: F^k \to D$ be defined by $g = \varphi \circ f$ where $\varphi: C \to D$ is the given isometry. Thus

$$g(u) = \varphi \circ f(u) = \varphi(uX), \quad u \in F^k.$$

Let $Y$ be the matrix of $g$ relative to the standard basis for $F^k$. $Y$ is clearly a generator matrix for $D$.

By Lemma 2, $(Tr')_i = w(g[L_i])$ where $r'$ is the column vector for $Y$ corresponding to $r$.

THEOREM 1. *There exists a monomial matrix, $\Lambda$, such that $X\Lambda = Y$.*

*Proof.* We first show $w(g[L_i]) = w(f[L_i])$ for all $i$.

$$\begin{aligned} w(g[L_i]) &= w(g(u_i)),\ u_i \in L_i\,. \\ w(f[L_i]) &= w(f(u_i)). \\ w(g(u_i)) &= w(\varphi \circ f(u_i)) = w(f(u_i)) \text{ since } \varphi \text{ is weight-preserving} \\ \therefore w(g[L_i]) &= w(f[L_i]). \end{aligned}$$

By Lemma 2, $(Tr)_i = (Tr')_i$. Now, $Tr = Tr' \Rightarrow r = r'$ by Lemma 1. Recall that $r, r'$ list the number of nonzero columns of $X$, $Y$, respectively, which lie in $L_1, \ldots, L_{\mu(k)}$. Since $r = r'$, the columns of $Y$ are just various scalar multiples of those of $X$, ordered in some way. If $X$ has some zero columns, clearly $Y$ has the same number of zero columns.

$\therefore X\Lambda = Y$ for the $n \times n$ monomial matrix $\Lambda = DP$, where the $n \times n$ diagonal matrix $D$ specifies the scalar multiplication and the $n \times n$ permutation matrix $P$, the reordering.

COROLLARY 1. *$C \sim D$ iff $C$ is isometric to $D$.*

*Proof.* Immediate from remarks made in the introduction.

## REFERENCES

BOGART, K. P., An elementary proof of the binary case of MacWilliams' theorem on the equivalence of codes, Submitted for publication.

MACWILLIAMS, F. J., Combinatorial problems of elementary abelian groups, Ph.D. Dissertation, Harvard University, Cambridge, Mass.

PETERSON, W. W. (1961), *Error Correcting Codes*, MIT Press, Cambridge, Mass.