INFORMATION AND CONTROL 20, 410–414 (1972)

Coset Analysis of Reed Muller Codes Via Translates of Finite Vector Spaces

R. P. KURSHAN AND N. J. A. SLOANE

Bell Telephone Laboratories, Incorporated Murray Hill, New Jersey 07974

In order to calculate the error probability of a code it is necessary to know the distribution of the coset leaders. The enumeration of cosets of the first order Reed Muller code has been studied (i) by Berlekamp and Welch (1972) by associating with each coset a class of Boolean functions, and (ii) by Sloane and Dick (1971) by associating with each coset a class of single-error-correcting codes called structure codes. It is shown here that it is possible to have two vectors of the same weight and in the same coset, which yet have inequivalent structure codes, at least for lengths $\geqslant 128$, thus giving a negative answer to a question raised by Sloane and Dick.

INTRODUCTION

The set of all binary vectors of length n forms an n-dimensional vector space V_n over $GF(2)$, and we will often think of these vectors as coordinates of the vertices of a unit cube in n dimensions. Let $V_n{}^*$ denote the set of nonzero vectors of V_n.

A set of 2^k binary vectors of length n is called an (n, k) linear *error-correcting code* if it is closed under componentwise addition modulo 2. An important family of such codes are the (binary) simplex codes or shortened first-order Reed Muller codes (Wozencraft and Jacobs, 1965; Berlekamp, 1968a; Posner 1968). Any such code is a subgroup of V_n and so partitions V_n into cosets. The classification of these cosets is an unsolved problem for most codes, the cosets of the first order Reed Muller code having received attention recently in Berlekamp (1968b and 1970), Sloane and Dick (1971), Holmes (1971), and Berlekamp and Welch (1972). In this note we examine some properties of the structure code of a vector, and answer a question proposed by Sloane and Dick (1971).

The $(2^m - 1, m)$ *simplex code* $\mathscr{C}_m$ consists of all linear combinations over $GF(2)$ of the rows of the $m \times 2^m - 1$ matrix whose columns are the binary representations of the numbers from 1 to $2^m - 1$. These columns will

also be thought of as coordinate vectors for the positions of the codewords, and thus set up a one-one correspondence between these positions and the set V_m^*.

With this coordinatization there is a one-one correspondence between binary vectors $\mathbf{x} = (x_1, \ldots, x_n)$ of length $n = 2^m - 1$ and subsets S of V_m^*. Thus if $S = \{S_1, \ldots, S_e\}$ then $\mathbf{x}$ has 1's in positions $S_1, \ldots, S_e$ and 0's elsewhere. e is called the weight of $\mathbf{x}$.

The points of S will in general satisfy certain linear equations with binary coefficients, of the form $S_i + S_j + S_k + \cdots = 0$. These equations form a vector space over $GF(2)$. If these equations are represented by binary vectors of length e, they form a code of length e, which is called the *structure code* $SC(\mathbf{x})$. Since the points S_i are nonzero and distinct, equations of the form $S_i = 0$ or $S_i + S_j = 0$ cannot occur. Therefore the weight of any vector in $SC(\mathbf{x})$ is at least three, or $SC(\mathbf{x})$ is at least a single-error-correcting code.

If $\mathbf{x}$ has 1's in positions $S = \{S_1, \ldots, S_e\}$ and $\mathbf{y}$ has 1's in positions $T = \{T_1, \ldots, T_e\}$, we say that $SC(\mathbf{x})$ is *equivalent* (Peterson, 1961) to $SC(\mathbf{y})$ if there is a bijection $\Pi: S \to T$ such that

$$S_i + S_j + S_k + \cdots = 0 \Leftrightarrow \Pi(S_i) + \Pi(S_j) + \Pi(S_k) + \cdots = 0.$$

The question was asked by Sloane and Dick (1971) whether it is possible to have two vectors $\mathbf{x}, \mathbf{y}$ in the same coset of $\mathscr{C}_m$, having the same weight, such that $SC(\mathbf{x})$ and $SC(\mathbf{y})$ are inequivalent.

Now $\mathscr{C}_m$ is generated by the vectors corresponding to those m faces of the cube which do not contain the origin. Considering V_{m-1} as a subspace of V_m, any such face is an affine subspace $V_{m-1} + x$, for $x \in V_m - V_{m-1}$.

We will give a negative answer to the above question for $m \geqslant 7$ by proving

(I) There exists some partition of $V_{m-1} + x = W \cup W'$ with $|W| = |W'|$ (so that W and W' correspond to vectors of equal weight in the same coset) such that for each bijection $\Pi: W \to W'$ there is some $S \subset W$ such that $\Sigma S = 0 (\Sigma S = \sum_{s \in S} s)$ and yet $\Sigma \Pi S \neq 0$.

Actually, we will prove the following:

(II) For each V_n, $n \geqslant 6$, there exists some partition $V_n = U \cup U'$ such that $|U| = |U'|$ and yet for each bijection $\Pi: U \to U'$ there is some $S \subset U$ such that $\Sigma S = 0$, $2 \mid |S|$, but $\Sigma \Pi S \neq 0$.

Then (I) follows, for taking $n = m - 1$ we set $W = U + x$; clearly $W' = (V_{m-1} + x) - W = U' + x$, and if $\Pi: W \to W'$ is a bijection then the map $\overline{\Pi}: U \to U'$ defined by $\overline{\Pi}(u) = \Pi(u + x) + x$ is a bijection and

thus by (II) there is some set $S \subset U$ such that $2 \mid \mid S \mid$, $\Sigma S = 0$ and $\Sigma\overline{\Pi}S \neq 0$. But then clearly $S + x \subset W$, $\Sigma(S + x) = 0$ and

$$\Sigma\Pi(S + x) = \Sigma\overline{\Pi}S + \mid S \mid x = \Sigma\overline{\Pi}S \neq 0.$$

Now, for the proof of (II). In what follows, let V denote some n-dimensional vector space over $F = GF(2)$, where $n \geqslant 6$. Let us define an *affine transformation* of V to be a sum of a linear transformation and a translation of V, and let $\mathscr{E}$ denote the set of linear translates of V ; if $\Pi \in \mathscr{E}$ then $\Pi = T + x$ ($T \in \mathrm{End}_F V$, $x \in V$) where $(T + x)(v) = T(v) + x$. If $\Pi' \in \mathscr{E}$, $\Pi' = T' + x'$ and if $\Pi' = \Pi$ then $x = (T + x)\,0 = (T' + x')\,0 = x'$ and so $T = T'$. Hence $\Pi \in \mathscr{E}$ uniquely determines x and T and as groups $\mathscr{E} \cong V \times \mathrm{End}_F V$.

Let $\{T_{ij}\}_{i,j=1}^{n}$ be a basis for $\mathrm{End}\, V$ over F; as $\Pi \in \mathscr{E}$ is uniquely expressible as $\Pi = x + \Sigma_{i,j} a_{ij} T_{ij}$ ($a_{ij} \in F$), it is clear that $\mid \mathscr{E} \mid = 2^{n^2+n}$.

PROPOSITION 1. *Suppose* $\Pi \in \mathscr{E}$, $K \subset V$, $2 \mid \mid K \mid$ *and* $\Sigma K = 0$. *Then* $\Sigma\Pi K = 0$.

Proof. Write $\Pi = T + x$ as above. Then

$$\Sigma\Pi K = \Sigma(T + x)K = \Sigma TK + \mid K \mid x = T\Sigma K + mpx = T(0) + m \cdot 0 = 0.$$

LEMMA. *Suppose* W *is a subset of* V *and* $T' \colon W \to V$ *such that for* x, y, $x + y \in W$, $T'(x + y) = T'(x) + T'(y)$. *Then there is a* $T \in \mathrm{End}\, V$ *such that the restriction of* T *to* W $T|_W = T'$.

Proof. Let $b_1, \ldots, b_r$ be an independent spanning set of vectors in W and define $T \colon V = [W] \times [W]^{\perp} \to V$ by $T(\Sigma a_i b_i) = \Sigma a_i T'(b_i)$ ($a_i \in F$), $T(v) = 0$ for $v \in [W]^{\perp}$ ($[W]$ is the space generated by W and if U is a subspace, $U^{\perp}$ is a complementary subspace).

PROPOSITION 2. *Suppose* W *is a subset of* V *and* $\Pi \colon W \to V$ *is a function with the property that*

$$[K \subset W, 2 \mid \mid K \mid, \Sigma K = 0] \Rightarrow \Sigma\Pi K = 0.$$

Then there exists $\overline{\Pi} \in \mathscr{E}$ *such that* $\overline{\Pi}\,|_W = \Pi$.

Proof. Set $z = \Pi(0)$ and define $T' \colon W \to V$ by $T'(v) = \Pi(v) - z$. Suppose $x, y, x + y \in W$. If $x = 0$ then $T'(x + y) = T'(y) = T'(x) + T'(y)$; if $x + y = 0$ then $T'(x) + T'(y) = 2T'(x) = 0 = T'(x + y)$. If x, y, $x + y$

are all distinct and nonzero set $K = \{x, y, x + y, 0\}$; then $|K| = 4$ and $\Sigma K = 0$ so $0 = \Sigma\Pi K = \Sigma\Pi K - 4z = T'(x) + T'(y) + T'(x + y) + T'(0)$ so $T'(x) + T'(y) = T'(x + y)$. Hence T' is linear on W and thus may be extended to $T \in \text{End } V$. Then $\overline{\Pi} = T - z \in \mathscr{E}$ extends Π.

Next, define $\mathscr{V} = \{W \subset V \mid 0 \in W, |W| = 2^{n-1}\}$ and for $\Pi \in \mathscr{E}$ let $\mathscr{V}(\Pi) = \{W \in \mathscr{V} \mid \Pi W = W'\}$ $(W' = V - W)$. Let $T = \Pi - \Pi(0) \in \text{End } V$ and let $k = \dim TV$. Then $|\Pi V| = |TV| = 2^k$. Hence, if $\dim TV < n - 1$, $\mathscr{V}(\Pi) = \varnothing$; if $\dim TV = n - 1$ then

$$W \in \mathscr{V}(\Pi) \Rightarrow W' = \Pi V \Rightarrow W = V - \Pi V$$

so $|\mathscr{V}(\Pi)| = 1$; if $\dim TV = n$ then T is an automorphism and Π may be thought of as a permutation in S_{2^n}, which is expressible uniquely as a product of r disjoint cycles. If $(a_1 a_2 \cdots a_i \cdots a_l)$ is such a cycle and $W \in \mathscr{V}(\Pi)$, then $a_i \in W \Leftrightarrow a_{i+1} \in W'$ for $1 \leqslant i < l$ (note that in particular l must be even). Hence there are two distinct possibilities relative to this cycle: $a_1 \in W$ or $a_1 \in W'$. Making this choice for each cycle, one considers $2^r = |\mathscr{V}(\Pi)|$ possibilities. Thus,

$$|\mathscr{V}(\Pi)| \leqslant 2^{n-1}, \tag{1}$$

$$\mathscr{V}(\Pi) \neq \varnothing \Leftrightarrow \dim(\Pi - \Pi(0))\, V \geqslant n - 1. \tag{2}$$

Let $\mathscr{V}^* = \{W \in \mathscr{V} \mid \exists$ a bijection $\Pi: W \to W'$ satisfying the property in Proposition 2$\}$; since a bijection associated with a $W \in \mathscr{V}^*$ extends to an element of $\mathscr{E}$, it follows that $\mathscr{V}^* = \bigcup_{\Pi \in \mathscr{E}} \mathscr{V}(\Pi)$, so $|\mathscr{V}^*| \leqslant 2^{n-1} |\mathscr{E}|$ and hence $|\mathscr{V}^*| \leqslant 2^{n^2+2n-1}$.

But

$$|\mathscr{V}| = \frac{1}{2}\binom{2^n}{2^{n-1}} \qquad \text{and for} \quad n = 6, \quad \frac{1}{2}\binom{2^n}{2^{n-1}} > 10^{16},$$

whereas $2^{n^2+2n-1} < 10^{15}$. In fact, for $n \geqslant 6$, $|\mathscr{V}| > 2^{n^2+2n-1}$ and hence for $n \geqslant 6$ $\mathscr{V}^* \subsetneq \mathscr{V}$. This completes the proof of (II).

Incidentally, we note here that for $n < 5$, Theorem 1 of Kurshan (to appear) can be used to show that $\mathscr{V}^* = \mathscr{V}$ and hence for $m < 6$, (I) fails; for $n = 5$ $(m = 6)$ it is conjectured that $\mathscr{V}^* \subsetneq \mathscr{V}$ and thus (I) holds. Also, it seems reasonable to conjecture that $W \in \mathscr{V}^* \Leftrightarrow$ there is a partition $W = W_1 \cup W_2$ such that for some $\Pi \in \mathscr{E}$, $\overline{W} = W_1 \cup \Pi W_2$ is $a(n)$ (affine) subspace of cardinality 2^{n-1}.

RECEIVED: April 2, 1971

REFERENCES

BERLEKAMP, E. R. (1968a), "Algebraic Coding Theory," McGraw-Hill, New York.

BERLEKAMP, E. R. (1968b), "Weight Enumeration Theorems," Proceedings of the Sixth Allerton Conference on Circuits and Systems, University of Illinois, Urbana, IL.

BERLEKAMP, E. R. (1970), Some mathematical properties of a scheme for reducing the bandwidth of motion pictures by Hadamard smearing, *Bell System Tech. J.* **49**, 696–986.

BERLEKAMP, E. R. AND WELCH, L. R. (1972), Weight distributions of the cosets of the (32,6) Reed-Muller codes, *IEEE Trans. Inf. Theory* **IT-18**, 203–207.

HOLMES, J. K. (1971), A note on some efficient estimates of the noise variance for first-order Reed–Muller codes, *IEEE Trans. Inf. Theory* **IT-17**, 628–630.

KURSHAN, R. P. $GF(2)^n \times$ Aut $GF(2)^n$ is generated by reflecting faces of the n-cube, to appear.

PETERSON, W. W. (1961), "Error-Correcting Codes," MIT Press, Cambridge, MA.

POSNER, E. C. (1968), Combinatorial structures in planetary reconnaissance, *in* "Error-Correcting Codes" (H. B. Mann, Ed.) Wiley, New York.

SLOANE, N. J. A. AND DICK, R. J. (1971), "On the Enumeration of Cosets of First-Order Reed-Muller Codes," Proceedings IEEE International Conference on Communications, Montreal, Vol. 7, pp. 36-2 to 36-6.

WOZENCRAFT, J. M. AND JACOBS, I. M. (1965), "Principles of Communication Engineering," Wiley, New York.