MATHEMATICS OF COMPUTATION
VOLUME 57, NUMBER 195
JULY 1991, PAGES 403-414

A CLASSIFICATION OF THE COSETS OF THE REED-MULLER CODE $\mathscr{R}(1, 6)$

JAMES A. MAIORANA

ABSTRACT. The weight distribution of a coset of a Reed-Muller code $\mathscr{R}(1, m)$ is invariant under a large transformation group consisting of all affine rearrangements of a vector space with dimension m. We discuss a general algorithm that produces an ordered list of orbit representatives for this group action. As a by-product the procedure finds the order of the symmetry group of a coset.

With $m = 6$ we can implement the algorithm on a computer and find that there are 150357 equivalence classes. These classes produce 2082 distinct weight distributions. Their symmetry groups have 122 different orders.

1. INTRODUCTION

This paper presents an algorithm that allows us to classify the cosets of the Reed-Muller code $\mathscr{R}(1, m)$ for any m. The general procedure reduces the calculation to a lower dimension, $m - 1$.

Rather than discussing the Reed-Muller codes here, we assume Chapters 13 and 14 of [2]. Our algorithm in principle solves research problem (14.2) in [2], but in practice we produce a new result only for $m = 6$. The actual computer run provides much additional information about the cosets of the $\mathscr{R}(1, 6)$ code.

The articles [3, 4] provide a good background about the type of calculation we consider here. Berlekamp and Welch classify the cosets of $\mathscr{R}(1, 5)$ in [1].

First we construct a precise mathematical framework for our calculation. We must classify the orbits of a finite group G acting on a finite function space $[V, F]$. One orbit of this action is isomorphic to the code $\mathscr{R}(1, m)$. The other orbits are affine equivalence classes of cosets of $\mathscr{R}(1, m)$. By Theorem 4 of Chapter 14 of [2], equivalent cosets possess identical weight distributions. Two cosets are equivalent if one transforms into the other by an affine rearrangement of the underlying dimension-m vector space V over the field F with two elements.

Next we decompose the space V into a subspace Q and its complementary hyperplane $P = V - Q$. This allows calculations in dimension $m - 1$ to determine a representative for each orbit of G. In dimension $m - 1$ we

Received February 23, 1989.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 94-04; Secondary 05-04, 51E20, 94B05.

determine by induction orbit representatives and their symmetry groups. Using this knowledge, we outline a complete program that enumerates the orbits in dimension m.

To run this procedure on a computer, we restrict attention to the case $m = 6$. For this dimension we give more details about the actual calculations. We also outline a verification algorithm that provides supporting evidence for the accuracy of the computer run. The Appendix to this paper contains two tables that summarize the output from the computer. The first table lists information about the minimum weight of a member of a coset, while the second provides information about some of the symmetry groups of the cosets of $\mathscr{R}(1, 6)$.

2. Background

This section defines the action of a group G on a function space $[V, F]$. First we build the affine group $\mathrm{AG}(m)$ from the general linear group $\mathrm{GL}(m, 2)$ by adjoining translations of V. The Reed-Muller code $\mathscr{R}(1, m)$ corresponds to the space of affine functions $\mathrm{AF}(m) \subseteq [V, F]$. The group $\mathrm{AG}(m)$ acts naturally on the space $[V, F]$. Letting $AF(m)$ act on $[V, F]$ by addition of functions, we define G as the semidirect product of $\mathrm{AG}(m)$ and $\mathrm{AF}(m)$.

Let $F = \{0, 1\}$ be the field with two elements, and let V be the vector space over F with dimension m. The function space $[V, F]$ of all maps $f: V \to F$ is a finite set with 2^{2^m} elements. Let $\mathrm{GL}(m, 2)$, the general linear group, be the collection of vector space automorphisms of V. For each $u \in V$ define a translation $T_u: V \to V$ by $T_u(w) = u + w$ for $w \in V$. Since $T_u T_w = T_{u+w}$, the collection of translations form a group isomorphic to V.

An element of $\mathrm{AG}(m)$ will be a pair (A, u) with $A \in \mathrm{GL}(m, 2)$ and $u \in V$. Define an action of $\mathrm{AG}(m)$ on V by

$$(A, u)(w) = A(w) + u \tag{2.1}$$

for $w \in V$. From (2.1) we derive the group operations for $\mathrm{AG}(m)$ as

$$(A, u)(B, w) = (AB, A(w) + u), \tag{2.2}$$

$$(A, u)^{-1} = (A^{-1}, A^{-1}(u)) \tag{2.3}$$

for $A, B \in \mathrm{GL}(m, 2)$ and $u, w \in V$. Thus, $\mathrm{AG}(m)$ is the semidirect product of $\mathrm{GL}(m, 2)$ with V.

The affine group $\mathrm{AG}(m)$ is the collection of all invertible transformations $a: V \to V$ that satisfy

$$a(u + w) = a(u) + a(w) + a(0) \tag{2.4}$$

for all $u, w \in V$.

A set $\{u_0, u_1, \dots, u_m\} \subseteq V$ is in general position if $u_1 - u_0, u_2 - u_0, \dots, u_m - u_0$ form a linearly independent set of vectors. A member $a \in \mathrm{AG}(m)$ is

parametrized uniquely by the values $a(u_0), a(u_1), \ldots, a(u_m)$ which are also in general position.

The space $\mathrm{AF}(m) \subseteq [V, F]$ of affine functions on V is the collection of all maps $f: V \to F$ that satisfy

$$f(u+w) = f(u) + f(w) + f(0) \tag{2.5}$$

for all $u, w \in V$. The values $f(u_0), f(u_1), \ldots, f(u_m)$ of f are arbitrary, and in fact, $\mathrm{AF}(m)$ is a vector space with dimension $m+1$.

We define a group G, that as a set is the product of $\mathrm{AG}(m)$ with $\mathrm{AF}(m)$, by defining its action on the function space $[V, F]$. For $A \in \mathrm{AG}(m)$, $b \in \mathrm{AF}(m)$, and $f: V \to F$ we have that $c = (A, b)$ is a general element of G. We define $g = c(f): V \to F$ by

$$g(u) = f(A^{-1}(u)) + b(u) \tag{2.6}$$

for $u \in V$. From (2.6) we derive the group operations for G as

$$(A, b)(C, d) = (AC, A(d) + b), \tag{2.7}$$

$$(A, b)^{-1} = (A^{-1}, A^{-1}(b)) \tag{2.8}$$

for $A, C \in \mathrm{AG}(m)$ and $b, d \in \mathrm{AF}(m)$. Thus, G is the semidirect product of $\mathrm{AG}(m)$ with $\mathrm{AF}(m)$.

The action of $\mathrm{AF}(m)$ on $[V, F]$ generates the cosets of the Reed-Muller code $\mathscr{R}(1, m)$. The automorphism group of this code is $\mathrm{AG}(m)$ by Theorem 24 of Chapter 13 of [2]. Two cosets of $\mathscr{R}(1, m)$ are affinely equivalent if one is mapped to the other by some element of $\mathrm{AG}(m)$. By Theorem 4 of Chapter 14 of [2], affinely equivalent cosets have identical weight distributions. Since an orbit of G is an affine equivalence class of cosets of $\mathscr{R}(1, m)$, a classification of the orbits of G provides a global understanding of $\mathscr{R}(1, m)$.

The order of G is approximately $.29 \times 2^{(m+1)^2}$ while $[V, F]$ contains 2^{2^m} elements. Thus, a lower bound for the number of orbits of G is $3.4 \times 2^{2^m - (m+1)^2}$. Only for $m \leq 6$ will an enumeration be reasonable.

3. The general algorithm

Using the framework from the previous section, we develop an algorithm that produces orbit representatives for the action of G on $[V, F]$. By introducing a mapping N of the function space $[V, F]$ into the integers Z, we identify a unique element f inside each orbit of G, namely the one which minimizes N. Our procedure makes a list of these f ordered by their values $N(f)$. As a by-product the order o of the symmetry group of f is found.

By splitting the space V into a pair P, Q of hyperplanes, the calculation of the orbits of G reduces to dimension $m-1$. In this dimension we need

orbit representatives $h_1, h_2, \ldots, h_L$ and their symmetry groups $S^{m-1}(h_i)$. An orbit representative f has the property that $f|_P$ must be an h_i. Further, $f|_Q$ must be an orbit representative under the action of a group $S^{m-1}(h_i)M$. For each f we consider the other decompositions of V into a pair of hyperplanes. We test in two stages whether one of these decompositions proves that f is not minimal. Any f that passes these tests is an orbit representative.

We map the two vector spaces V and $[V, F]$ into the integers by choosing a basis $u_1, u_2, \ldots, u_m$ for V. Each $u \in V$ has a unique expression as $e_1u_1 + e_2u_2 + \cdots + e_mu_m$ with $e_i \in F$. Define the integer

$$n(u) = \sum_{i=1}^{m} e_i 2^{i-1}. \tag{3.1}$$

For a function $f \in [V, F]$ define the integer

$$N(f) = \sum_{u \in V} f(u) 2^{n(u)}. \tag{3.2}$$

Here we consider $F = \{0, 1\}$ as a subset of the integers.

We use N to order the set $[V, F]$ by $f \leq g$ if $N(f) \leq N(g)$. The action of G on $[V, F]$ produces for each $g \in [V, F]$ an orbit $g^G = \{a(g) | a \in G\}$. Since we have totally ordered $[V, F]$, each orbit g^G has a unique minimal element f. We can produce a list $f_1 < f_2 < \cdots < f_K$ that contains all such orbit representatives by using the following naive algorithm.

Loop through the integers from 0 to $2^{2^m} - 1$. For each i set $f = N^{-1}(i)$ and check whether $a(f) \geq f$ for each $a \in G$. If so, then f is the representative for its orbit f^G and is added to the list. As a by-product we can observe how many times $a(f) = f$, and this is the order of the symmetry group

$$S(f) = \{a \in G | a(f) = f\} \tag{3.3}$$

of f. In addition to the list $f_1 < f_2 < \cdots < f_K$ we obtain the invariants $o_i = |S(f_i)|$ of the orbits of G. That is, if $g = a(f)$ for some $a \in G$, then $S(g) = aS(f)a^{-1}$, and two conjugate subgroups have the same order.

This procedure is practical only for $m \leq 5$. In order to push into new territory, we must reduce the work involved. In fact, we may carry out the calculation in one lower dimension. Consider the decomposition of V into two disjoint hyperplanes $V = P \cup Q$, where $Q = \langle u_1, u_2, \ldots, u_{m-1} \rangle$ is a subspace and $P = u_m + Q = V - Q$ is its translate. A function $f \in [V, F]$ decomposes into two functions f_0 and f_1 on dimension-$(m-1)$ space $V^{m-1} = Q$. Here,

$f_0(u) = f(u)$ and $f_1(u) = f(u_m + u)$ for $u \in V^{m-1} \subset V^m$. We have that

$$N(f) = N(f_1)2^{2^{m-1}} + N(f_0). \tag{3.4}$$

We can specify f by giving its two pieces f_0 and f_1.

Let H be the subgroup of G that preserves the decomposition $V = P \cup Q$. More precisely, remember that G is the semidirect product of $\mathrm{AG}(m)$ with $\mathrm{AF}(m)$, and then

$$H = \{(A, b) | A \in \mathrm{AG}(m),\ b \in \mathrm{AF}(m),\ AQ = Q\}. \tag{3.5}$$

Thus, H induces actions on the function spaces $[P, F]$ and $[Q, F]$. Let M be the normal subgroup of H defined by

$$M = \{a \in H | a(g) \in g \text{ for all } g \in [P, F]\}. \tag{3.6}$$

The group H/M acts on the space $[P, F]$. This action is isomorphic to the action of G on $[V, F]$ in dimension $m-1$. In fact, H possesses a subgroup G^{m-1} with $H = G^{m-1}M$, and G^{m-1} is the dimension-$(m-1)$ version of G. In fact, G^{m-1} consists of all $(A, b) \in H$ that satisfy $A(0) = 0$ and $b(0) = 0$.

If $f \in [V, F]$ is minimal in its orbit, then $f \leq a(f)$ for all $a \in G^{m-1}$. By (3.4) we have that $f_1 \leq a(f_1)$. By induction we have a list $h_1 < h_2 < \cdots < h_L$ of orbit representatives for dimension $m-1$, and f_1 must equal h_i for some i. Let

$$S^{m-1}(h_i) = \{a \in G^{m-1} | a(h_i) = h_i\}; \tag{3.7}$$

then the subgroup $T(h_i) = S^{m-1}(h_i)M$ of H leaves f_1 invariant. It follows that $f_0 \leq a(f_0)$ for all $a \in T(h_i)$. The action of $T(h_i)$ on $[Q, F]$ is easy to describe. First, for $a \in M$ there are elements $u \in Q$ and $e \in F$ such that

$$a(g)(w) = g(w + u) + e \tag{3.8}$$

for $g \in [Q, F]$ and $w \in Q$. If $(A, b) \in G^{m-1}$ leaves u_m fixed, that is $A(u_m) = u_m$ while $b(u_m) = 0$, then (A, b) acts on the spaces $[P, F]$ and $[Q, F]$ identically under the correspondence $u_m + u \leftrightarrow u$. The remainder of the action of G^{m-1} on $[Q, F]$ is determined by noting that G^{m-1} possesses a normal subgroup M_1, isomorphic to M, that acts as the identity on $[Q, F]$.

We recapitulate at this point. So far, the algorithm says that if f is minimal under the action of G, then $f_1 = h_i$ and f_0 is minimal under the action of $T(h_i)$. This all takes place in dimension $m-1$ and guarantees that f is minimal under the action of $H \subset G$. But H has $2 \times (2^m - 1)$ cosets, one for each hyperplane of V. Choose coset representatives for H,

$$G = H + Hc_1 + \cdots + Hc_I, \tag{3.9}$$

where $I = 2^{m+1} - 3$. Define $f^j = c_j(f)$. The function f is minimal when $f \leq a(f^j)$ for all $a \in H$ and j from 1 to I.

For each j some element $d_j \in G^{m-1} \subset H$ puts f_1^j in minimal form, $d_j(f_1^j) = h_k$. If h_k precedes $f_1 = h_i$ in the list $h_1 < h_2 < \cdots < h_L$ of $m-1$ forms, then f is not minimal. If h_k follows h_i, then for all $a \in Hc_j$ we have $f < a(f)$. Only when $h_k = h_i$ do we need consider the action of H on f_0^j.

Having understood the dimension-$(m-1)$ case and produced the list $h_1 < h_2 < \cdots < h_L$, we can go further and find an efficient invariant $\mathscr{I}(h)$ that maps any member h of $[V^{m-1}, F]$ to the representative h_k for its orbit under G^{m-1}. The next step in the algorithm is to check that

$$\mathscr{I}(f_1^j) \geq h_i = f_1 \tag{3.10}$$

for all j. If f passes this test we can define the set

$$EQ = \{j \mid \mathscr{I}(f_1^j) = f_1\}. \tag{3.11}$$

The final step of our procedure restricts attention to the set EQ. If $j \in EQ$, then we must find $d_j \in G^{m-1}$ with $d_j(f_1^j) = f_1$. Let $g_j = d_j(f_0^j)$. We must check that $a(g_j) \geq f_0$ for all $a \in T(f_1)$. While doing so, we find the set

$$EQQ = \{j \in EQ \mid f_0 = a(g_j) \text{ for some } a \in T(f_1)\}. \tag{3.12}$$

Any f that survives is minimal under the action of G, and we append f to our output list. Since we consider candidates in numerical order, the output list is ordered. While proving f minimal, we can find the order of the subgroup of $T(f_1)$ that leaves f_0 invariant. The product of this order with the cardinality of EQQ is the order of $S(f)$.

We conclude this section with a formal summary of the general algorithm.

Procedure. To produce an ordered list

$$f_1 < f_2 < \cdots < f_L$$

of orbit representatives for the action of G on $[V, F]$ together with the orders o_i of their symmetry groups do the following:

(A) In dimension $m-1$ produce a list

$$h_1 < h_2 < \cdots < h_K$$

of representatives for the action of G^{m-1} on $[V^{m-1}, F]$.

(B) Find the symmetry groups $S^{m-1}(h_i)$.

(C) Loop through the h_i in numerical order.

(D) Find in numerical order all f_0 that are minimal under the action of $T(h_i) = S^{m-1}(h_i)M$.

(E) For $f \in [V, F]$ with $f_1 = h_i$ from step (C) and f_0 from step (D), form $f^j = c_j(f)$ and check that $\mathscr{I}(f_1^j) \geq f_1$ for j from 1 to $2^{m+1} - 3$.

(F) When $\mathscr{I}(f_1^j) = f_1$ find $d_j \in G^{m-1}$ such that $d_j(f_1^j) = f_1$ and check that $a(d_j(f_0^j)) \geq f_0$ for all $a \in T(f_1)$.

(G) Append to the output list the survivors f of steps (E) and (F) along with the order o of $S(f)$ implicitly calculated by steps (D), (E), and (F).

4. The practical application of the algorithm

In this section we discuss implementation details for our algorithm. The classification of the cosets of the Reed-Muller code $\mathscr{R}(1, 5)$ was done by Berlekamp and Welch in [1]. For $m > 6$ the number of orbits exceeds our ability to store them. This leaves only $m = 6$ as practical while producing new information.

In order to execute our procedure on a computer, we need concrete realizations of the objects G and $[V, F]$. The map N makes a function $f: V \to F$ into a 2^m-bit integer. A special case of the theory developed by Sims in [5, 6] allows us to view the group G as a product set $C_0 \times C_1 \times \cdots \times C_m$. We also present an explicit algorithm for the invariant $\mathscr{I}$ on the function space $[V^5, F]$. For the remainder of this section we consider only the $m = 6$ case of the general algorithm.

We represent a function $f \in [V, F]$ as the integer $N(f)$. An element of G is a pair (A, b) with $A \in \mathrm{AG}(m)$ and $b \in \mathrm{AF}(m)$. Now A acts on V as a permutation. Therefore, the integer $N(A(f))$ arises as a rearrangement of the 2^m bits in the binary expansion (3.2) of $N(f)$. The element $b \in \mathrm{AF}(m) \subseteq [V, F]$ acts on $[V, F]$ by function addition $b(f) = f + b$. Thus $N(b(f))$ is the bit-by-bit addition modulo 2 of the integers $N(b)$ and $N(f)$.

The first steps of our procedure concern the $m = 5$ situation. We must produce 48 orbit representatives $h_1 < h_2 < \cdots < h_{48}$ and then describe their symmetry groups $S^5(h_i)$. To do this, we need a better description of G. We use an $(m+1)$-fold product $C_0 \times C_1 \times \cdots \times C_m$ connected with the geometry of V.

For each I from 0 to m choose elements $A(I, J) \in \mathrm{AG}(m)$ for J from $e(I)$ to $2^m - 1$, where $e(0) = 0$ and $e(I) = 2^{I-1}$ for $I > 0$. We require that the element $A(I, J)$ fixes all $u \in V$ with $n(u) < e(I)$ and takes $n^{-1}(e(I)) \in V$ to $n^{-1}(J) \in V$. Also choose $b(I) \in \mathrm{AF}(m)$ such that $b(I)(u) = 0$ when $n(u) < e(I)$ while $b(I)(u) = 1$ when $n(u) = e(I)$. The set C_I consists of the $2(2^m - e(I))$ elements $(A(I, J), 0)$ and $(A(I, J), b(I))$, where $e(I) \leq J < 2^m$. Each element $a \in G$ has a *unique* expression as $c_0 c_1 \cdots c_m$ with $c_I \in C_I$. Further, the sets $G_I = C_I \times C_{I+1} \times \cdots \times C_m$ are all subgroups of G. In fact, G_{I+1} is a subgroup of G_I with the set C_I as coset representatives.

This description of G is shared by each of its subgroups. Given $h = h_i$ for some i from 1 to 48, we describe $S^5(h)$ as a product $S_0 \times S_1 \times \cdots \times S_5$. Each S_I is a set of coset representatives for $S^5(h) \cap G_{I+1}$ as a subgroup of $S^5(h) \cap G_I$.

If $s \in S_I$, then there is a unique $c \in C_I$ with $c^{-1}s \in G_{I+1}$, that is, $s \in cG_{I+1}$. Each time the intersection $cG_{I+1} \cap S^5(h)$ for $c \in C_I$ is not empty, we generate one element of S_I.

The actual calculation of S_0 involves a search through the product space $C_0 \times C_1 \times \cdots \times C_5$ for elements that fix h. This is a search through a tree with $32 - e(I)$ branches at each node on level I. This follows from the fact that elements of C_I occur in pairs $(A, 0)$ and (A, b), where at most one of these elements may fix h. Since the elements of C_I leave the space $V_I^5 = \{u | n(u) < e(I)\}$ fixed and the values of h on V_I^5 unchanged, we can accelerate the search. Only when $(c_0c_1 \cdots c_I)(h)$ agrees with h on V_{I+1}^5 will further extension of this product produce a symmetry of h. Once we find a symmetry $(c_0c_1 \cdots c_5)(h) = h$, we add $c_0c_1 \cdots c_5$ to S_0 and consider the next possibility for c_0. Finally, the sets S_I for $I > 0$ are found by a similar search over a part of the tree that begins on level I.

Steps (C) and (D) of our procedure involve finding in numerical order all functions $f_0 \in [V^5, F]$ that are minimal in the orbits of $T(h) = S^5(h)M$. This is accomplished by simple exhaustion. Using a six-deep set of nested loops, we form all products $s = s_0s_1 \cdots s_5$ with $s_I \in S_I$ for I from 0 to 5. Form $g = s(f_0)$ and check whether $a(g) < f_0$ for any $a \in M$. If so, we are finished with f_0. Otherwise, count how many times $a(g) = f_0$ and accumulate this number. If we successfully exhaust over $S^5(h)$, then f_0 is minimal and we have accumulated the order of $S(f) \cap H$. That is, any element of the subgroup H of G that fixes the function f formed from $f_1 = h$ and f_0 must appear as a symmetry of f_0 as acted upon by $T(h)$.

Step (E) requires the evaluation of the invariant $\mathscr{I}$ on the function f_1^j. When $m = 4$, the group G^4 makes eight orbits as it acts on $[V^4, F]$. The weight distribution of the cosets of the Reed-Muller code $\mathscr{R}(1, 4)$ provides a complete invariant $\mathscr{I}_4$ that maps the space $[V^4, F]$ into these eight orbits. See [2, Chapter 14] for more details.

For $m = 5$, a more involved calculation produces a complete invariant $\mathscr{I}$. Consider the 31 distinct dimension-four subspaces of V^5. Given $g \in [V^5, F]$, each subspace W of V^5 creates a pair of functions on V^4, namely by restriction to W and to $V^5 - W$. Using the invariant $\mathscr{I}_4$, we form an unordered pair of orbits of G^4. There are $36 = 8 \times (8 + 1)/2$ possible pairs. We tabulate the number of times each pair occurs while exhausting over the 31 subspaces W of V^5. This forms a distribution $D(g) = (D_1, D_2, \ldots, D_{36})$ of counts that sums to 31. This 36-long vector of integers is a complete invariant for the action of G^5 on $[V^5, F]$. We store the 48 count vectors $D(h_i)$ associated with the known forms $h_1 < h_2 < \cdots < h_{48}$. Given any $g \in [V^5, F]$, we calculate its count vector $D(g)$ and compare against the known list. We set $\mathscr{I}(g) = h_i$ when $D(g) = D(h_i)$ for some i from 1 to 48.

To implement the final step, the only new algorithm needed is the production of an element $d \in G^5$ such that $d(g) = \mathscr{I}(g)$, given $g \in [V^5, F]$. Using the product structure $G^5 = C_0 \times C_1 \times \cdots \times C_5$, we exhaust over G^5 by walking through the associated tree. We eliminate a branch when it cannot produce the desired transformation. With a three-fold product $d = c_0 c_1 c_2$ there is one chance in two that $d(g) = \mathscr{I}(g)$ is impossible. For a four-fold product this increases to seven chances in eight. This cut-down effect makes the work of finding d manageable.

5. The answer and a verification algorithm

The algorithm of the previous section was run on a computer and an answer obtained. We found 150357 orbits for the action of G on $[V, F]$ when $m = 6$. These orbits produced a total of 2082 distinct weight distributions on the associated cosets of the $\mathscr{R}(1, 6)$ code. Our calculation found 122 different orders among the symmetry groups for these orbits. The Appendix presents some of the information generated by the computer.

The answer is a binary file of 150357 pairs (f, o) of 64-bit numbers. Here, f is an orbit representative, the numerically least element in its orbit, while $o = |S(f)|$ is the order of its symmetry group. Because of the complexity of the calculation, there was no certainty that the computer would execute the algorithm correctly. We ran a verification algorithm that provided 48 checks on the accuracy of the answer. We finish by outlining this procedure.

Consider the entire space $[V, F]$ of functions when $m = 6$. Since V decomposes into pairs of hyperplanes in 63 ways, each member f of $[V, F]$ yields 126 functions on dimension-five space. An exhaustion over $[V, F]$ produces a total of 126×2^{64} functions on V^5. We classify each by equivalence under G^5 and generate 48 counts $y_1, y_2, \ldots, y_{48}$. Each y_I is a function of the size of the orbit of h_I. We have that

$$y_I = 126 \times 2^{32} \times |G^5|/|S^5(h_I)| \tag{5.1}$$

for I from 1 to 48.

We can calculate the numbers y_I from the output of our computer run. For each f on the output list, consider its restriction to the 126 hyperplanes inside V. Classify the resulting functions on V^5 using the invariant $\mathscr{I}$ and produce a count $z_I(f)$ of the number of times h_I occurred. Each function in the orbit of f will produce $z_I(f)$ contributions toward the count y_I. Since there are $|G|/|S(f)|$ functions in this orbit, we have that

$$y_I = \sum_{J=1}^{150357} z_I(f_J) \times |G|/o_J \tag{5.2}$$

for each I from 1 to 48. Here, (f_J, o_J) are the pairs on our output list for J from 1 to 150357.

APPENDIX

The Appendix consists of two tables. The first table describes the minimum weight that occurs in the weight distribution of a coset of the Reed-Muller code $\mathscr{R}(1, 6)$. The column labeled MIN WEIGHT contains the possible values for the minimum weight of a coset. Column ORBITS reports the number of equivalence classes of cosets that have this minimum weight. Column FIRST FUNCTION is the numerically smallest function, written in hexadecimal, with a given minimum weight. Column INDEX is the position of its equivalence class in the output file where the first output has INDEX $= 0$.

The second table reports the orders of the symmetry groups that are associated with a unique equivalence class of cosets. That is, for each of the 34 entries in this table the factored number that appears in the column ORDER OF SYMMETRY is the order of the symmetry group $S(f)$ only for f in a single equivalence class of cosets. The other two columns are similar to those in Table 1.

TABLE 1
Minimum weight

MIN WEIGHT	ORBITS	INDEX	FIRST FUNCTION
0	1	0	0
1	1	1	1
2	1	2	3
3	1	3	7
4	2	4	F
5	2	6	1F
6	4	7	3F
7	6	8	7F
8	11	9	FF
9	15	14	1FF
10	29	20	3FF
11	46	23	7FF
12	92	24	FFF
13	160	28	1FFF
14	325	29	3FFF
15	626	30	7FFF
16	1326	31	FFFF
17	2647	226	100017FFF
18	5496	412	300033FFF
19	10789	1521	700071FFF
20	19964	4185	F000F0FFF
21	31521	15521	1F001F1F3F
22	38142	22826	3F011F1F37
23	27795	28859	7F070F0FF1
24	10280	29599	FF0F0F0FF0
25	983	147138	1017F0F333C55
26	84	149839	3033F0775D3C4
27	4	150349	7133D156E7A68
28	4	150353	F333C555A6669

TABLE 2
Symmetry group orders

ORDER OF SYMMETRY	INDEX	FIRST FUNCTION
$2^5 \cdot 3 \cdot 5$	149873	3033F555659A6
$2^7 \cdot 5$	201	1173DED
$2^5 \cdot 3 \cdot 7$	150350	7133D156EB6A4
$2^6 \cdot 3^2 \cdot 5$	1499	35556566A
$2^8 \cdot 3 \cdot 7$	225	100013FFF
$2^7 \cdot 3^2 \cdot 5$	103315	1011703586428
$2^9 \cdot 3 \cdot 5$	22971	3F030F333C
$2^9 \cdot 3^3$	28422	3F5555556A
$2^7 \cdot 3^3 \cdot 5$	149871	3033F5556566A
$2^{11} \cdot 3 \cdot 7$	150356	F33553C66695A
$2^{12} \cdot 3 \cdot 5$	112	7333C
$2^{10} \cdot 3^2 \cdot 7$	412	300033FFF
2^{16}	148	F33FF
$2^{15} \cdot 3$	29604	FF0F0F333C
$2^7 \cdot 3^3 \cdot 5 \cdot 7$	226	100017FFF
$2^{14} \cdot 3 \cdot 7$	81	33FFF
$2^{17} \cdot 3$	29602	FF0F0F3333
$2^9 \cdot 3^3 \cdot 5 \cdot 7$	1494	355555556
$2^{15} \cdot 3 \cdot 7$	150354	F333C555A6696
$2^{15} \cdot 3^3$	28	1FFF
$2^{12} \cdot 3^2 \cdot 5 \cdot 7$	52	17FFF
$2^9 \cdot 3^4 \cdot 5 \cdot 7$	150352	7333C555A6669
$2^{18} \cdot 3^2$	134	F0FFF
$2^{17} \cdot 3^3$	24	FFF
$2^{15} \cdot 3^3 \cdot 5$	4185	F000F0FFF
$2^{15} \cdot 3^2 \cdot 7^2$	8	7F
$2^{19} \cdot 3^3 \cdot 5$	29599	FF0F0F0FF0
$2^{15} \cdot 3^4 \cdot 5 \cdot 7$	150353	F333C555A6669
$2^{18} \cdot 3^2 \cdot 7^2$	9	FF
$2^{17} \cdot 3^3 \cdot 5 \cdot 7$	4	F
$2^{16} \cdot 3^2 \cdot 5 \cdot 7 \cdot 31$	2	3
$2^{21} \cdot 3^3 \cdot 5 \cdot 7$	31	FFFF
$2^{15} \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 31$	1	1
$2^{21} \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 31$	0	0

BIBLIOGRAPHY

1. E. R. Berlekamp and L. R. Welch, *Weight distributions of the cosets of the* (32, 6) *Reed-Muller code*, IEEE Trans. Inform. Theory **18** (1972), 203–207.
2. F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, New York, 1977.
3. M. A. Harrison, *Counting theorems and their applications to classification of switching functions*, Recent Developments in Switching Theory, Chapter 4 (A. Mukhopadhyay, ed.), Academic Press, New York, 1971.

4. R. J. Lechner, *Harmonic analysis of switching functions*, Recent Developments in Switching Theory, Chapter 5 (A. Mukhopadhyay, ed.), Academic Press, New York, 1971.
5. C. C. Sims, *Determining the conjugacy classes of a permutation group*, Proc. Sympos. on Computers in Algebra and Number Theory, Amer. Math. Soc., Providence, RI, 1970.
6. ——, *Computation with permutation groups*, Proc. Second Sympos. on Symbolic and Algebraic Manipulation, Assoc. Comput. Mach., New York, 1971.

INSTITUTE FOR DEFENSE ANALYSES, CENTER FOR COMMUNICATIONS RESEARCH, PRINCETON, NEW JERSEY 08540-3699