INFORMATION AND CONTROL 14, 442–456 (1969)

Restrictions on Weight Distribution of Reed–Muller Codes

E. R. BERLEKAMP AND N. J. A. SLOANE

Bell Telephone Laboratories, Murray Hill, New Jersey

It is shown that in the rth order binary Reed–Muller code of length $N = 2^m$ and minimum distance $d = 2^{m-r}$, the only codewords having weight between d and $2d$ are those with weights of the form $2d - 2^i$ for some i. The same result also holds for certain supercodes of the RM codes.

1. DESCRIPTION OF BINARY REED–MULLER CODE [Kasami, Lin, and Peterson (1968) and Berlekamp (1968)]

DEFINITION. The weight of an integer k, $W(k)$, is the number of 1's in the binary expansion of k.

The binary Reed–Muller code is conveniently defined as an extension of a cyclic code. Let α be a primitive element of $GF(2^m)$.

DEFINITION. For $1 \leqq r \leqq m - 2$, the rth order binary Punctured Reed–Muller code of length $2^m - 1$ is a cyclic code whose generator polynomial has as roots those α^k such that

$$1 \leqq W(k) \leqq m - r - 1$$

DEFINITION. For $1 \leqq r \leqq m - 2$, codewords of the rth order binary Reed–Muller code of length $N = 2^m$ are formed by adding an overall parity check c_∞ to the codewords $[c_0, c_1, \cdots, c_{N-2}]$ of the rth order Punctured Reed–Muller code.

Thus $[c_\infty, c_0, c_1, \cdots, c_{N-2}]$, $c_i \in GF(2)$, is a codeword of the rth order Reed–Muller code of length $N = 2^m$ iff

$$c_\infty = \sum_{i=0}^{N-2} c_i$$

and

$$\sum_{i=0}^{N-2} c_i \alpha^{ik} = 0 \text{ for all } k \in K^1, \tag{1}$$

where K^1 is the set of integers k such that

$$1 \leqq W(k) \leqq m - r - 1 \quad \text{and} \quad 1 \leqq k \leqq 2^m - 1.$$

It is known [Berlekamp (1968)] that this code has $\sum_{i=0}^{r} \binom{m}{i}$ information symbols and minimum distance $d = 2^{m-r}$. In the special case of $r = 2$, $d = 2^{m-2}$, Kasami[1] has shown that every codeword of weight $< 2d$ has weight of the form

$$w = 2d - 2^i \quad \text{for some } i, \qquad i \geqq \left[\frac{m-1}{2}\right].$$

One generalization of Kasami's theorem was recently obtained by McEliece (1967), who showed that all of the codewords in the rth order RM code have weights divisible by $2^{\lfloor (m-1)/r \rfloor}$. In this paper, we present another generalization of Kasami's theorem. The combination of our theorem with McEliece's theorem in the special case $r = 2$ yields Kasami's theorem.

THEOREM. *If a codeword in the* rth *order Reed–Muller code of length* $N = 2^m$ *and minimum distance* $d = 2^{m-r}$ *has weight* w *and* $d \leqq w \leqq 2d$, *then*

$$w = 2d - 2^i \qquad \textit{for some } i.$$

Before proving this theorem in Section 5, we review necessary preliminaries in Sections 2 and 3, and introduce a crucial Lemma in Section 4.

The special cases $m - r = 1$ and $m - r = 2$ of the theorem are trivial. From now on, we assume $m - r \geqq 3$.

2. POWER SERIES ASSOCIATED WITH THE CODEWORDS

Let $\mathbf{c} = [c_\infty, c_0, c_1, \cdots, c_{N-2}]$ be an arbitrary codeword of the rth order binary Reed–Muller code of length $N = 2^m$. We associate two power series with $\mathbf{c}$ as follows. Suppose $\mathbf{c}$ has Hamming weight e, and has 1's in positions $c_{i_1}, c_{i_2}, \cdots, c_{i_e}$. Then define

$$X_r = \begin{cases} \alpha^{i_r} & \text{if } \ 0 \leqq i_r \leqq N - 2 \\ 0 & \text{if } \ i_r = \infty \end{cases}$$

for $r = 1, 2, \cdots, e$. These are the "locations" of the 1's. The locations are elements of $GF(2^m)$.

[1] Theorem 16.34 of Berlekamp (1968).

The first power series is the *locator polynomial*

$$\sigma(z) = \prod_{i=1}^{e} (1 - X_i z),$$

$$\triangleq \sum_{i=0}^{e} \sigma_i z^i, \qquad \sigma_0 = 1.$$

The roots of the locator polynomial are the reciprocals of the locations of the 1's. By definition $\sigma(z)$ is a polynomial over $GF(2^m)$ with distinct roots, i.e. $\sigma(z)$ and the derivative $\sigma'(z)$ have no common factor in $GF(2^m)$, i.e.

$\sigma(z)$ *and the odd part of* $\sigma(z)$, $\tilde{\sigma}(z)$, *are relatively prime over* $GF(2^m)$. (2)

Clearly

$$\deg \sigma = \begin{cases} e & \text{if } c_\infty = 0 \\ e - 1 & \text{if } c_\infty = 1 \end{cases}$$

To prove the theorem, we will only consider codewords of weight $\leqq 2d - 6 \leqq N - 6$. Since every Reed–Muller code is invariant under a triply transitive permutation group [Berlekamp (1968, Theorem 14.45)], we may assume $c_\infty = 0$ and

$$\deg \sigma(z) = \textit{weight of codeword}. \tag{3}$$

Let us define the *power sum symmetric functions as*

$$S_k = \sum_{i=1}^{e} X_i^k, \qquad k \geqq 1. \tag{4}$$

Since $X_i \in GF(2^m)$,

$$S_{k+N-1} = S_k \tag{5}$$

and then the second power series associated with $\mathbf{c}$ is the generating function

$$S(z) = \sum_{k=1}^{\infty} S_k z^k.$$

S and σ are related by the basic equation [(Berlekamp (1968), Eq. 9.32)]

$$S\sigma = \tilde{\sigma} = \textit{odd part of } \sigma. \tag{6}$$

From (1), (4), if $1 \leqq k \leqq 2^m - 1$ then $S_k = 0$ if $k \in K^1$. From (5), if $k \geqq 2^m$, $S_k = 0$ if

$$W(h) \leqq m - r - 1,$$

where $h \equiv k \bmod 2^m - 1$ and $0 \leqq h \leqq 2^m - 2$. It is easy to see that if $W(k) \leqq m - r - 1$ then $W(h) \leqq m - r - 1$.

So if we define the set $K(n)$, $n \geqq 0$, by

$$\begin{aligned} K(n) &= \{k \geqq 0 \mid W(k) \geqq n\} \\ &= \{k_1, k_2, k_3, \cdots ; k_i \leqq k_{i+1}\}, \end{aligned} \tag{7}$$

then $S_k = 0$ if $k \notin K(m - r)$, and

$$S(z) = \sum_{k \in K(m-r)} S_k z^k \tag{8}$$

(Some of the terms in this sum may be zero but all the nonzero terms of $S(z)$ are contained in (8).)

3. DESCRIPTION OF $K(n)$

It will be convenient to have a list of the elements $k_1, k_2, \cdots$ of $K(n)$, and of their differences $\delta_i(n) = k_{i+1} - k_i$, for $k_i \leqq 2^{n+2} - 1$. Table I gives the binary expansion of $k_1, k_2, \cdots$, using the notation 0^a for a string of a0's and 1^b for a string of b1's. Table II gives $\delta_1(n), \delta_2(n), \cdots$, reading from left to right and from top to bottom. We also define $\delta_0(n) = 0$.

4. INTRODUCTION TO LEMMA 1 AND ITS PROOF

Let $P^{(n)}$, $n \geqq 0$, be any power series of the form

$$P^{(n)} = \sum_{k \in K(n)} a_k z^k = \sum_{i=1}^{\infty} a_{k_i} z^{k_i}. \tag{8a}$$

Clearly any power occurring in $P^{(n)}$ is of the form

$$2^n - 1 + \sum_{i=0}^{j} \delta_i(n), \qquad \text{for some } j. \tag{9}$$

Thus $S(z)$ is of the form of $P^{(m-r)}$. Power series of this type will play an important part in the proof of the theorem.

We say that $P^{(n)}$ has *degeneracy of order* π, $\pi \geqq 0$, if $a_{k_i} = 0$ for $1 \leqq i \leqq \pi$, $a_{k_{\pi+1}} \neq 0$. In this case we define

$$\varepsilon^{(n,\pi)} \triangleq \frac{P^{(n)}}{z^{k_{\pi+1}}}.$$

TABLE I

BINARY EXPANSION OF ELEMENTS $k_1, k_2, \cdots$ OF $K(n)$ IN INCREASING ORDER

Elements	Length
1^n	n
$1^r01^{n-r}, \quad 1 \leqq r \leqq n$	$n+1$
1^{n+1}	
$1^s01^r01^{n-r-s}\}1 \leqq s \leqq n$ $1^s01^{n-s+1}\}0 \leqq r \leqq n-s\}$	$n+2$
$1^{n+1}0$	
1^{n+2}	
$\cdots$	$\cdots$

TABLE II

DIFFERENCES $\delta_i(n) = k_{i+1} - k_i$, $i = 1, 2, \cdots$, BETWEEN ELEMENTS OF $K(n)$

2^{n-1}	2^{n-2}	2^{n-3}	$\cdots$	2	1	1
2^{n-1}	2^{n-2}	2^{n-3}	$\cdots$	2	1	1
	2^{n-2}	2^{n-3}	$\cdots$	2	1	1
		2^{n-3}	$\cdots$	2	1	1
			$\cdots$	.	.	.
				2	1	1
					1	1
						1
						1
						$\cdots$

It follows that $\mathcal{E}^{(n,\pi)}$ is any power series with nonzero constant term and differences between successive powers given by Table II with π initial terms removed, i.e. by Table III. Formally, let

$$d_i(n,\pi) = \begin{cases} 0 & \text{if } 0 \leqq i \leqq \pi \\ \delta_i(n) & \text{if } \pi+1 \leqq i \end{cases}$$

Then $\mathcal{E}^{(n,\pi)}$, $n, \pi \geqq 0$, is any power series of the form

$$\left.\begin{aligned} &\mathcal{E}^{(n,\pi)} = \sum_{i=0}^{\infty} e_{r_i} z^{r_i}, \qquad r_0 = 0, \qquad r_{i+1} > r_i, \\ &\text{where } e_0 \neq 0 \text{ and} \\ &r_i = \sum_{j=0}^{\pi+i} d_j(n,\pi), \qquad i \geqq 0. \end{aligned}\right\} \tag{10}$$

TABLE III

DIFFERENCES $d_i(\pi, n)$ BETWEEN SUCCESSIVE TERMS IN $\mathcal{E}^{(n, \pi)}$[a]

0	0	0	⋯	0	$2^{n-\pi-1}$	⋯	2	1	1
2^{n-1}	2^{n-2}	2^{n-3}	⋯	$2^{n-\pi}$	$2^{n-\pi-1}$	⋯	2	1	1
	2^{n-2}	2^{n-3}	⋯	$2^{n-\pi}$	$2^{n-\pi-1}$	⋯	2	1	1
		2^{n-3}	⋯	$2^{n-\pi}$	$2^{n-\pi-1}$	⋯	2	1	1
				⋯		⋯			
				$2^{n-\pi}$	$2^{n-\pi-1}$	⋯	2	1	1
					$2^{n-\pi-1}$	⋯	2	1	1
						⋯	·	·	·
							2	1	1
							2	1	1
								1	1
									1
									1
								(+	Others)

[a] Starting with the top left hand zero and reading from left to right and top to bottom gives $d_1(n, \pi)$, $d_2(n, \pi)$, ⋯ . Starting with the bottom 1 and reading from right to left and bottom to top gives $\Delta_1(n, \pi)$, $\Delta_2(n, \pi)$, ⋯ where $\Delta_i(n, \pi) = d_{J(n)+1-i}(n, \pi)$.

Table III gives $d_i(n, \pi)$ in the important case $0 < \pi < n$. Table III contains

$$J(n) = (n + 2)(n + 3)/2,$$

terms, including the initial zeros.

We shall now calculate the form of the inverse power series to $\mathcal{E}^{(n, \pi)}$, as far as the end of Table III, that is, modulo $z^{M(n, \pi)}$, where

$$\begin{aligned} M(n, \pi) &= \sum_{i=0}^{J(n)} d_i(n, \pi) \\ &= 2^{n+1} + 2^{n-\pi} \qquad \text{if} \quad 0 \leqq \pi \leqq n. \end{aligned} \tag{11}$$

LEMMA 1. *If* $1 \leqq n$, $0 \leqq \pi \leqq n - 1$, *and* $\mathcal{E}^{(n, \pi)}$ *is of the form* (10), *then*

$$(\mathcal{E}^{(n, \pi)})^{-1} = A + z^{\theta+1} P^{(n-\pi-1)} \bmod z^{M(n, \pi)}$$

where A *is a polynomial of degree at most* $\theta = 2^{n+1} - 2^{n-\pi}$ *with nonzero constant term, and* $P^{(n-\pi-1)}$ *is a power series of the form given by Eq.* (8a).

Proof. (i) If $\pi = n - 1$, the lemma is trivial, so we assume $\pi \leqq n - 2$.

(ii) *Obtaining* $\mathcal{E}^{-1}$. For convenience we abbreviate $\mathcal{E}^{(n, \pi)}$ to $\mathcal{E}$,

$M(n, \pi)$ to M, and $d_i(n, \pi)$ to d_i. Since $\mathcal{E}/e_0 \equiv 1 \bmod z$, in a field of characteristic two we have

$$\left(\frac{\mathcal{E}}{e_0}\right)^{-1} = \frac{\mathcal{E}}{e_0} \cdot \left(\frac{\mathcal{E}}{e_0}\right)^{2^1} \cdot \left(\frac{\mathcal{E}}{e_0}\right)^{2^2} \cdot \left(\frac{\mathcal{E}}{e_0}\right)^{2^3} \cdots$$

and

$$\mathcal{E}^{-1} = \text{const} \cdot \mathcal{E} \cdot \mathcal{E}^2 \cdots \mathcal{E}^{2^H} \bmod z^M \tag{12}$$

for some H depending on n and π.

(iii) *What is H?* The smallest nonzero power in $\mathcal{E}$ is $2^{n-\pi-1}$; the smallest nonzero power in $\mathcal{E}^{2^h}$ is $2^{n-\pi-1+h}$, so in (12) we need only consider $\mathcal{E}^{2^h}$ for which

$$2^{n-\pi-1+h} \leqq M = 2^{n+1} + 2^{n-\pi}$$

or

$$H \leqq \pi + 2.$$

However, we next show that $\mathcal{E}^{2^{\pi+2}}$ does not contribute anything new to the product (12), therefore we may take

$$H = \pi + 1. \tag{13}$$

In fact, we assert that

$$\mathcal{E}^{2^{\pi+1}} \cdot \mathcal{E}^{2^{\pi+2}} \equiv \mathfrak{F}^{2^{\pi+1}} \bmod z^M, \tag{14}$$

where $\mathfrak{F}$, like $\mathcal{E}$, is of the form given by Eq. (10). To prove (14), we write down the powers occurring in $\mathcal{E}^{2^{\pi+1}}$ and $\mathcal{E}^{2^{\pi+2}}$. These are easily obtained from Table III. $\mathcal{E}^{2^{\pi+1}} \bmod z^M$ contains the powers

$$0, 2^n, 2^n + 2^{n-1}, \cdots, 2^n + 2^{n-1} + \cdots + 2^{\pi+2}, 2^{n+1},$$

and $\mathcal{E}^{2^{\pi+2}} \bmod z^M$ contains

$$0, 2^{n+1}.$$

Equation (14) follows immediately.

(iv) *Restatement of Lemma* 1. From (10), (11), and (12), any power in $\mathcal{E}^{-1} \bmod z^M$ is

$$\sum_{\nu=0}^{\pi+1} 2^\nu \sum_{i=0}^{k_\nu} d_i, \qquad 0 \leqq k_\nu \leqq J(n). \tag{15}$$

Therefore from (9) and (15), Lemma 1 may be restated as follows:

If $0 \leqq k_\nu \leqq J(n)$, and if

$$\theta + 1 \leqq \sum_{\nu=0}^{\pi+1} 2^\nu \sum_{i=0}^{k_\nu} d_i \leqq M,$$

then

$$\sum_{\nu=0}^{\pi+1} 2^\nu \sum_{i=0}^{k_\nu} d_i - \theta - 2^{n-\pi-1} = \sum_{i=0}^{j} \delta_i(n - \pi - 1),$$

for some j, $0 \leqq j \leqq J(n - \pi - 1)$.

Now let $\Delta_1, \Delta_2, \cdots, \Delta_{J(n)}$ be the differences occurring in Table III, starting at the bottom and reading from right to left, so that

$$\Delta_i = d_{J(n)-i+1}, \qquad 1 \leqq i \leqq J(n);$$

also let $\Delta_0 = 0$. Then

$$\sum_{i=0}^{k_\nu} d_i = M - \sum_{i=0}^{J(n)-k_\nu} \Delta_i$$

$$\sum_{i=0}^{j} \delta_i(n - \pi - 1) = 2^{n-\pi} + 2^{n-\pi-1} - \sum_{i=0}^{J(n-\pi-1)-j} \Delta_i$$

for $0 \leqq k_\nu \leqq J(n), 0 \leqq j \leqq J(n - \pi - 1)$. The statement of Lemma 1 now becomes:

If $0 \leqq k_\nu \leqq J(n)$ and if

$$\begin{aligned} L \triangleq (2^{\pi+2} - 2)M &\leqq \sum_{\nu=0}^{\pi+1} 2^\nu \sum_{i=0}^{k_\nu} \Delta_i \\ &\leqq (2^{\pi+2} - 2)M + M - \theta - 1 \triangleq U, \end{aligned} \tag{16}$$

then

$$\sum_{\nu=0}^{\pi+1} 2^\nu \sum_{i=0}^{k_\nu} \Delta_i - L = \sum_{i=0}^{j} \Delta_i, \tag{17}$$

for some j, $0 \leqq j \leqq J(n - \pi - 1)$.

(v) *Completing the Proof of Lemma* 1. Inspection of Table III shows that $\sum_{i=0}^{j} \Delta_i$, $j \leqq J(n)$, generates all numbers of weight 0, 1 and 2 in the range from 0 to $M(n, \pi)$; and so

$$\sum_{\nu=0}^{\pi+1} 2^\nu \sum_{i=0}^{k_\nu} \Delta_i, \qquad 0 \leqq k_\nu \leqq J(n),$$

generates only numbers of weight $\leqq 2\pi + 4$.

From (16), (17) we must show that if $\sum 2^r \sum \Delta_i$ is in the range from L to U then

$$\sum 2^r \sum \Delta_i - L \text{ has weight } \leqq 2. \tag{18}$$

Now

$$L = (2^{n+1} + 2^{n-\pi})(2^{\pi+2} - 2) = 2^{n+1-\pi}(2^{2\pi+2} - 1),$$

and

$$U = L + 2^{n+1-\pi} - 1,$$

so L has weight $2\pi + 2$. The binary expansions of L and U are

$$L = 1^{2\pi+2}0^{n+1-\pi}$$

$$U = 1^{2\pi+2}1^{n+1-\pi}$$

Equation (16) implies

$$\sum 2^r \sum \Delta_i = 1^{2\pi+2}X$$

where X is some $(n + 1 - \pi)$-digit binary number. Since the weight of $\sum 2^r \sum \Delta_i$ is at most $2\pi + 4$, X has weight $\leqq 2$. This gives (18) and completes the proof of Lemma 1.

5. PROOF OF THE THEOREM

We now prove a strengthened version of the theorem stated in the introduction:

THEOREM. *If $w \leqq 2^{m+1-r}$ and if the roots of the generator polynomial of a cyclic code include all $\alpha^k (1 \leqq k \leqq 2^m - 1)$ for which*

$$k \leqq 2w,$$

and

$$1 \leqq W(k) \leqq m - r - 1$$

then the extended cyclic code contains no codewords of weight w unless $w = 2^{m+1-r} - 2^i$ for some i.

The idea of the proof is to assume that a codeword of weight w exists, $d \leqq w \leqq 2d$, and then if w is not of the form $2d - 2^i$ to obtain a nontrivial common factor of σ and $\tilde{\sigma}$, thus contradicting (2). The common factor is found iteratively, beginning with the basic Eq. (6) and proceeding in a manner similar to the Euclidean algorithm.

We begin by giving in Fig. 1 a flow diagram outlining the steps in the proof, and then give a detailed discussion of the steps.

Throughout this section m, r, and $\mu \triangleq m - r$ are fixed.

DISCUSSION OF THE STEPS IN THE FLOW DIAGRAM

Step (A). We begin by assuming that a codeword of weight w exists, where w is even and

$$d = 2^{\mu} \leqq w \leqq 2d - 6 = 2^{\mu+1} - 6. \tag{19}$$

Using (3) we assume

$$\deg \sigma(z) = w \tag{20}$$

Step (B). This sets up the beginning of the iteration.

The Iteration

Step (C). Follows initially from (19) and inductively from Step (I).

Step (D). Follows initially from (6) and the definitions, and inductively from (J).

Step (E) and Section 4 imply that

$$P^{(n_i)} = z^{\theta_i - 1} g^{(n_i, \pi_{i+1})},$$

where

$$\begin{cases} \theta_i = 2^{n_i+1} - 2^{n_i - \pi_{i+1}} & \text{if } 0 \leqq \pi_{i+1} \leqq n_i - 2 \qquad (21) \\ \theta_i \geqq 2^{n_i+1} - 2 & \text{if } n_i - 1 \leqq \pi_{i+1} \qquad (22) \end{cases}$$

and from Step (D),

$$h^{(n_i)} z^{\theta_i - 1} g^{(n_i, \pi_{i+1})} \equiv g^{(n_i)} \bmod z^{2H_i} \tag{23}$$

Step (G). The contradiction if $P^{(n_i)}$ is very degenerate.

$$\begin{aligned} \deg g^{(n_i)} &\leqq w - 2^{\mu+1} + 2^{n_i+1} - 1 && \text{from (D)} \\ &\leqq 2^{n_i+1} - 7 && \text{from (19)} \\ &< \theta_i - 1 && \text{from (22)} \end{aligned}$$

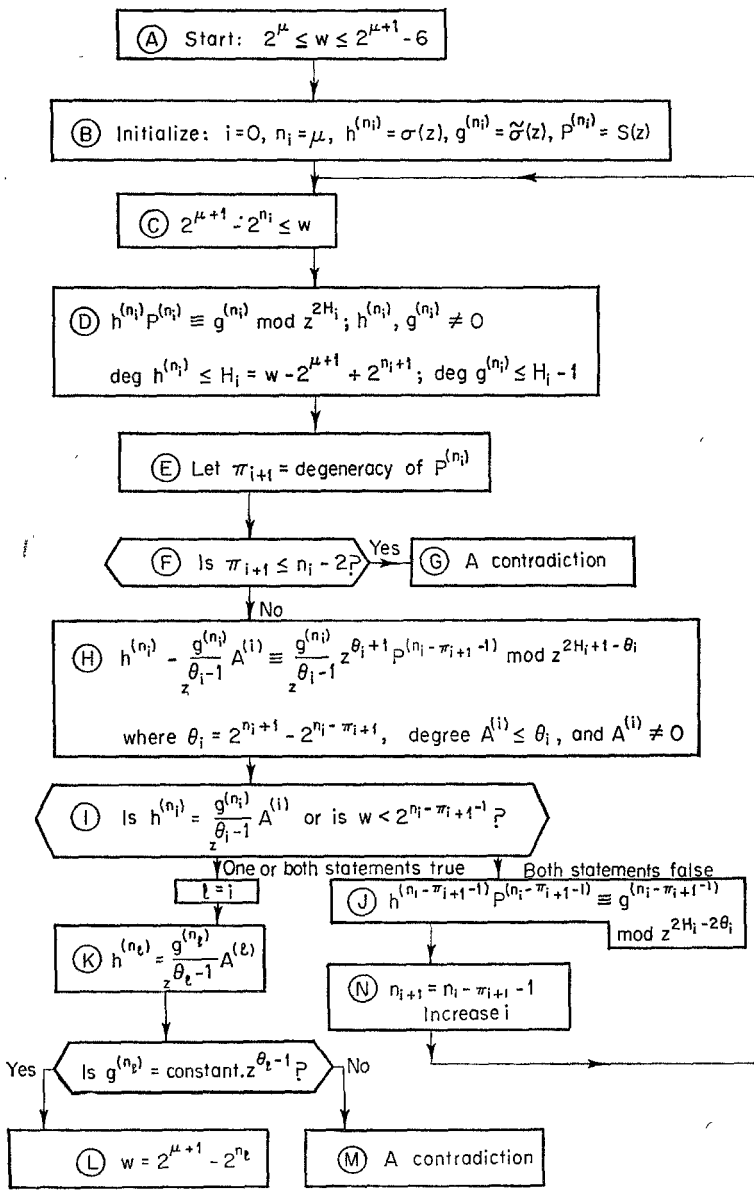

FIG. 1: Flow diagram of the proof

therefore

$$g^{(n_i)} = h^{(n_i)} = 0 \qquad \text{from (23)}$$

which contradicts (D).

Step (H). From (23) and Lemma 1,

$$h^{(n_i)} \equiv \frac{g^{(n_i)}}{z^{\theta_i - 1}} \left(A^{(i)} + z^{\theta_i + 1} P^{(n_i - \pi_{i+1} - 1)}\right) \bmod z^{2H_i + 1 - \theta_i}$$

where $A^{(i)} \neq 0$, $\deg A^{(i)} \leqq \theta_i$, and where θ_i is given by (21).

Step (I). Since n_i decreases with each iteration, and $w \leqq 2d - 6$, eventually the iteration will end and go to Step (K).

Step (J). The equation of Step (H) becomes

$$h^{(n_i - \pi_{i+1} - 1)} P^{(n_i - \pi_{i+1} - 1)} \equiv g^{(n_i - \pi_{i+1} - 1)} \bmod z^{2(H_i - \theta_i)}$$

if we define

$$g^{(n_i - \pi_{i+1} - 1)} = \frac{1}{z^{\theta_i + 1}} \left(h^{(n_i)} - \frac{g^{(n_i)} A^{(i)}}{z^{\theta_i - 1}}\right) \qquad (24)$$

$$h^{(n_i - \pi_{i+1} - 1)} = \frac{g^{(n_i)}}{z^{\theta_i - 1}} \qquad (25)$$

We must verify that the statements of Step (D) are still true. From Step (I) and $g^{(n_i)} \neq 0$ it follows that

$$g^{(n_i - \pi_{i+1} - 1)}, h^{(n_i - \pi_{i+1} - 1)} \neq 0.$$

Also

$$\begin{aligned} \deg g^{(n_i - \pi_{i+1} - 1)} &\leqq H_i - \theta_i - 1 && \text{from (24)} \\ &= w - 2^{\mu+1} + 2^{n_i - \pi_{i+1}} - 1 && \text{from (D)} \end{aligned}$$

and similarly

$$\deg h^{(n_i - \pi_{i+1} - 1)} \leqq w - 2^{\mu+1} + 2^{n_i - \pi_{i+1}}$$

as they should be.

This completes the description of the iteration.

Establishing the Contradiction

Step (K). Step (C) implies that at this point w satisfies

$$2^{\mu+1} - 2^{n_l} \leqq w. \tag{26}$$

If the answer to the first question of Step (I) was yes,

$$h^{(n_l)} = \frac{g^{(n_l)}}{z^{\theta_l - 1}} A^{(l)} \tag{27}$$

follows immediately. If the answer to the second question of Step (I) was yes, then

$$\begin{aligned} H_l &< 2^{n_l+1} - 2^{n_l - n_{l+1} - 1} \\ &= \theta_l + 2^{n_l - n_{l+1} - 1} \end{aligned}$$

whence we may deduce that

$$z^{\theta_l+1} P^{(n_l - n_{l+1} - 1)} \equiv 0 \bmod z^{H_l+1}. \tag{28}$$

But since $z^{\theta_l - 1}$ divides $g^{(n_l)}$, we know that $\theta_l - 1 \leqq \deg g^{(n_l)} \leqq H_l - 1$, so we may take the congruence of Step (H), Fig. 1 mod z^{H_l+1}. Using (28), this gives

$$h^{(n_l)} - \frac{g^{(n_l)} A^{(l)}}{z^{\theta_l - 1}} \equiv 0 \bmod z^{H_l+1}.$$

Since the degree of this polynomial is at most H_l, we again obtain Eq. (27).

Step (M). In this case it follows from (27) that $h^{(n_l)}$ and $g^{(n_l)}$ have a nontrivial common factor (that is, a common factor of degree greater than zero). From (24), (25), $h^{(n_i)}$ and $g^{(n_i)}$ have a nontrivial common factor, for all i. In particular $h^{(n_0)} = \sigma$ and $g^{(n_0)} = \tilde{\sigma}$ have a nontrivial common factor, contradicting (2).

Step (L). We now have

$$g^{(n_l)} = \text{constant} \cdot z^{\theta_l - 1} \tag{29}$$

$$h^{(n_l)} = \text{constant} \cdot A^{(l)} \tag{30}$$

and it will be shown that in this case w has the form $2d - 2^i$ for some i.

Define η_i inductively for $i = l, l-1, \cdots, 1, 0$ by

$$\eta_l = 2^{n_l+1} - 2^{n_l - n_{l+1}} \tag{31}$$

$$\eta_{i-1} = \eta_i + \theta_{i-1} \tag{32}$$

Then

$$\deg h^{(n_i)} \leqq \eta_i \tag{33}$$

$$\deg g^{(n_i)} \leqq \eta_i - 1. \tag{34}$$

In fact for $i = l$, (33) and (34) follow from (29), (30), (31); and for $0 \leqq i \leqq l - 1$ they follow from (24) and (25). Then

$$\begin{aligned} w &= \deg \sigma && \text{from (20)} \\ &\leqq \eta_0 && \text{from (33)} \\ &= \eta_l + \sum_{i=0}^{l-1} \theta_i , && \text{from (32)} \\ &= 2^{\mu+1} - 2^{n_l - \pi_{l+1}} && (35) \end{aligned}$$

from (21), (31) and Step (N).

We get a second bound on w as follows. Define γ_i inductively for $i = 0, 1, \cdots, l$ by

$$\gamma_0 = w,$$

$$\gamma_{i+1} = \gamma_i - \theta_i .$$

It is easy to show that

$$\deg h^{(n_i)} \leqq \gamma_i ,$$

$$\deg g^{(n_i)} \leqq \gamma_i - 1.$$

Then from (29)

$$\gamma_l \geqq \theta_l ,$$

and

$$\gamma_j \geqq \sum_{i=j}^{l} \theta_i ,$$

so

$$\gamma_0 = w \geqq \sum_{i=0}^{l} \theta_i = 2^{\mu+1} - 2^{n_l - \pi_{l+1}}$$

(35) and (36) imply

$$w = 2^{\mu+1} - 2^{n_l - \pi_{l+1}}$$

This completes the proof of the theorem. Q.E.D.

Remarks. Although we have not yet succeeded in doing so, there is some reason to hope that a tightening up of these arguments would yield an enumeration of the codewords of weight $w = 2^{\mu+1} - 2^{i}$.

Addendum. In October 1968 we sent a preprint of this paper to T. Kasami and in December he and his colleagues, N. Tokura and S. Hatanaka, succeeded in enumerating the codewords of weight $w = 2^{\mu+1} - 2^{\epsilon}$. The result was published in a Japanese journal in January 1969. In their notation, $N_{m,r,w}$ denotes the number of codewords of weight w in the rth order RM code of length 2^m; $a = \min(m - r, r)$; $b = (m - r + 2)/2$; and j is defined by $w = 2^{m-r+1} - 2^{m-r+1-j}$ with $\max(a, b) \geqq j > 1$. Their formulas are then as follows:

If $j = 2$ or $\max(a, 2) < j \leqq b$, then

$$N_{m,r,w} = 2^{r-2+j(j+1)} \frac{\prod_{i=0}^{r+2j-3} (2^{m-i} - 1)}{\prod_{i=0}^{r-3} (2^{r-2-i} - 1) \cdot \prod_{i=0}^{j-1} (4^{i+1} - 1)}. \tag{1}$$

If $\max(b, 2) < j \leqq a$, then

$$N_{m,r,w} = 2^{r(r+3)-j-1} \frac{\prod_{i=0}^{3r-j-1} (2^{m-i} - 1)}{\prod_{i=0}^{r-j-1} (2^{r-j-i} - 1) \cdot \left[\prod_{i=0}^{r-1} (2^{r-i} - 1)\right]^2}. \tag{2}$$

If $3 \leqq j \leqq \min(a, b)$, then $N_{m,r,w}$ is equal to the sum of (1) and (2). In August 1968 we obtained the same results for the special case of 2nd order Reed–Muller codes by another method.

RECEIVED: January 6, 1969; revised March 28, 1969.

REFERENCES

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

KASAMI, T., LIN, S., AND PETERSON, W. W. (1968), New Generalizations of the Reed–Muller Codes—Part I: Primitive Codes, *IEEE Trans. Inform. Theory*, **IT-14**, 189–198.

KASAMI, T., TOKURA, N., AND HATANAKA, S. (1969), On the Weight Structure of Reed–Muller Codes, *papers Tech. Group Inf. Theory, I.E.C.E., Japan*

McEliece, R. J. (1967), Linear Recurring Sequences Over Finite Fields, Ph.D. Thesis, California Institute of Technology.