Weights in the Third-Order Reed-Muller Codes

H. van Tilborg
Communications Systems Research Section

In order to obtain performance superior to that of the (32,6) first-order Reed-Muller Code used on Mariner Mars 1969 and 1971 spacecraft, bandwidth limitations make it necessary to consider Reed-Muller codes of higher orders. In this paper, we investigate the weights which can actually occur in the third-order Reed-Muller codes of lengths 256 and 512. For length 256, we succeed in finding the exact set of integers which occur as weights. For length 512, we do the same, except that we cannot decide whether 140 and 372 occur as weights or not. We show, however, that there are no words of weight 132 or 380, a result which adumbrates an important new theorem on Reed-Muller codes.

I. Introduction

Reed-Muller (RM) codes are among the most useful binary block codes. For instance, the first-order RM code of length 32 is the celebrated (32,6) biorthogonal code which was used on *Mariners* Mars '69 and '71. In order to obtain performance superior to that of the (32,6) code, one would like to use a longer RM code. Unfortunately, the bandwidth requirements of longer *first*-order RM codes are such as to render them useless for NASA missions. However, higher order RM codes require less bandwidth at a fixed length than the first order codes, and so it becomes important to investigate the feasibility of implementing these codes.

As a first step in this direction, researchers have begun to investigate the weight spectrum of these codes. The weight spectrum of the first-order RM code is trivial: except for the all-zero word and the all-one word, all words have weight half the block length. Recently, through the work of Kasami, Berlekamp, and Sloane, the complete weight enumerator for the second-order RM codes has been obtained.

The weight enumerator for the third-order RM codes, however, remains unknown, although for lengths 128 or less it can be obtained by various *ad hoc* techniques. In this paper we investigate the weight enumerator for the third-order RM code of lengths 256 and 512, with the preliminary goal being to identify those weights which actually occur in these codes. For length 256, our result is that all weights which are not eliminated by known theorems can actually occur. For 512, however, we discover that, although no previous theorem suggests it, no words of weights 132 or 380 occur; this adumbrates an important new theorem on RM codes. Finally, weights 140 and 372 remain undecided; i.e., we can neither show that they do not occur nor exhibit words of that weight.[1]

II. Summary of Known Results

RM(r;2^m) denotes the rth order RM code of length 2^m. The following theorems are known:

THEOREM 1 (Ref. 1). *The minimum distance d in RM (r;2^m) is 2^{m-r}.*

THEOREM 2 (Ref. 2). *If*

$$\sum_{i=0}^{2^m} A_i z_i$$

is the weight enumerator of RM $(r;2^m)$ then

$$A_i = A_{2^m - i}$$

THEOREM 3 (McEliece, from Ref. 1). *For the same weight enumerator,*

$$i \not\equiv 0 \pmod{2^{\lceil \frac{m}{r} \rceil - 1}} \text{ implies } A_i = 0$$

By the definition of RM $(r;2^m)$ (Ref. 1) each code vector corresponds with an rth degree polynomial in m variables over GF (2), and the weight of this vector is the number of times that this polynomial has value 1.

So instead of studying the vectors we can study the polynomials. In this paper we need both points of view. We denote by $|f|_m$ the number of times that f, as a function of m variables, is 1.

Example. Let f be an rth degree polynomial in m variables (over GF (2)); then Theorem 1 says

$$|f|_m = 0 \text{ or } |f|_m \geq 2^{m-r}$$

and Theorem 3 says $|f|_m$ is divisible by $2^{\lceil \frac{m}{r} \rceil - 1}$

THEOREM 4 (T. Kasami and N. Tokura from Ref. 3). *If f is an rth degree polynomial of m variables, $r \leq 2$ and $0 < |f|_m < 2^{m-r+1}$ $(0 < |f|_m < 2d)$, then f is transformable by any appropriate affine transformation of the variables into one of the following forms:*

(4a) $x_1 x_2 \cdots x_{r-\mu}(x_{r-\mu+1} \cdots x_\mu + x_{\mu+1} \cdots x_{\mu+r})$
where $m \geq r + \mu \quad r \geq \mu \geq 3$, or

(4b) $x_1 \cdots x_{r-2}(x_{r-1}x_r + x_{r+1}x_{r+2} + \cdots + x_{r+2\mu-3}x_{r+2\mu-2})$
where $m - r + 2 \geq 2\mu \geq 2$

and in both cases

(4c) $|f|_m = 2^{m-r+1} - 2^{m-r+1-\mu}$
$= 2d - 2d \cdot 2^{-\mu}$

Remark. $|f|_m$ is invariant under affine transformation so that this theorem characterizes the codewords with weight $< 2d$.

[1]Since this paper was written it has been possible to show that no words of weight 140 or 372 occur, either. In addition, the weight enumerator for the third-order code of length 256 has been found.

THEOREM 5 (McEliece, Ref. 1).

$$|f|_m = \sum_{\substack{g \subset f \\ g \neq 0}} (-1)^{|g|} 2^{|g|+\nu(g)-1}$$

where

$|g|$ = *the number of terms in the polynomial* g

$\nu(g)$ = *the number of variables not involved in* g

$g \subset f$ *means all terms of* g *are terms of* f

As an immediate consequence of Theorem 5 we find

$$|f(x_1, \cdots, x_{m-2}) + x_{m-1}x_m|_m = 2^{m-2} + 2 \cdot |f(x_1, \cdots, x_{m-2})|_{m-2} \quad (1)$$

$$|f(x_1, \cdots, x_{m-3}) + x_{m-2}x_{m-1}x_m|_m = 2^{m-3} + 6 \cdot |f(x_1, \cdots, x_{m-3})|_{m-3} \quad (2)$$

$$|f(x_1, \cdots, x_{m-3}) + x_{m-2}x_{m-1}x_m + x_m|_m = 3 \cdot 2^{m-3} + 2 \cdot |f(x_1, \cdots, x_{m-3})|_{m-3} \quad (3)$$

These relations will be useful in the next paragraph.

III. Tables

We start our work with some tables. We wish to know whether there are more gaps in the weight enumerator than those given by Theorems 1 through 4. We have formulated Tables 1 and 2 for RM $(3;2^8)$ and RM $(3;2^9)$. By Theorem 2 we are only interested in weights up to 2^{m-1}, and because we are looking for gaps, we only need to find code words of a certain weight to see that there is no gap.

We did not succeed in finding a codeword of weight 132 or 140. We are therefore left with only the possible gaps $A_{132} = 0$ or $A_{140} = 0$. In the next section we will show that $A_{132} = 0$.

For a while we believed that if one adds to a codeword $c \in \text{RM}(3;2^m)$ an appropriate codeword $d \in \text{RM}(2;2^m)$, the weight of $c + d$ would be less than twice the minimum distance in RM $(3;2^m)$ so that Theorem 4 would be applicable. However, by counting the number of codewords in the second- and third-order RM codes and the number of equivalence classes of the codewords of weights less than $2d$, it can be shown that this cannot be true for $m = 9$.

IV. $A_{132} = 0$ in RM $(3;2^9)$

Let $f(x_1, \cdots, x_9) = p(x_1, \cdots, x_8) + x_9\, q(x_1, \cdots, x_8)$; then $|f|_9 = |p|_8 + |p + q|_8$.

Lemma 1. *If $f(x_1, \cdots, x_9) = p(x_1, \cdots, x_8) + x_9\, q(x_1, \cdots, x_8)$ and $|p|_8 > |p + q|_8$ then there is $f'(x_1, \cdots, x_9) = p'(x_1, \cdots, x_8) + x_9\, q'(x_1, \cdots, x_8)$ with $|p'|_8 < |p' + q'|_8$, $|p'|_8 = |p + q|_8$, $|p' + q'|_8 = |p|_8$ and therefore $|f|_9 = |f'|_9$.*

Proof. Take $p'(x_1, \cdots, x_8) = p(x_1, \cdots, x_8) + q(x_1, \cdots, x_8)$ and $q'(x_1, \cdots, x_8) = q(x_1, \cdots, x_8)$. Q.E.D.

If $f(x_1, \cdots, x_9) = p(x, \cdots, x_8) + x_9\, q(x_1, \cdots, x_8)$ is a third-degree polynomial then $p(x_1 \cdots, x_8)$ is of third degree and $q(x_1, \cdots, x_8)$ of second degree. By Lemma 1 we need only look for a polynomial $p(x_1, \cdots, x_8)$ of third degree and a polynomial $q(x_1, \cdots, x_8)$ of second degree with the property $|p|_8 + |p + q|_8 = 132$ and $|p|_8 \leqq |p + q|_8$. The occurring weights in the third order RM code of length 2^8 are 0,32,48,56,64,68,72, $\cdots$, so by Lemma 1 we only have to consider $|p|_8 = 0,32,48,56,64$. This proves Lemma 2.

Lemma 2. *If $f(x_1, \cdots, x_9) = p(x_1, \cdots, x_8) + x_9\, q(x_1, \cdots, x_8)$ has weight 132, then we may assume*

$$(|p|_8, |p + q|_8) = \text{a) } (0,132) \text{ or}$$
$$\text{b) } (32,100) \text{ or}$$
$$\text{c) } (48,84) \text{ or}$$
$$\text{d) } (56,76) \text{ or}$$
$$\text{e) } (64,68)$$

We now consider these possibilities separately.

(a) $(|p|_8, |p + q|_8) = (0,132)$

$|p|_8 = 0$ implies $p \equiv 0$, so we want $|q|_8 = 132$ but q is second degree, and 132 does not occur in RM $(2;2^8)$. (See Theorem 3.) So (a) is impossible.

(b) $(|p|_8, |p + q|_8) = (32,100)$

By Theorem 4 is p transformable to $x_1x_2x_3$. So the question is, is there a second polynomial $q(x_1, \cdots, x_8)$ with

$$|x_1x_2x_3 + q(x_1, \cdots, x_8)|_8 = 100?$$
$$|x_1x_2x_3 + q(x_1, x_2, \cdots, x_8)|_8 = |q(0, x_2, \cdots, x_8)|_7 + |x_2x_3 + q(1, x_2, \cdots, x_8)|_7$$

Both terms are weights in RM $(2;2^7)$ and by Theorem 3 divisible by 8; but 100 is not divisible by 8.

Conclusion. (b) is impossible.

(c) $(|p|_8, |p + q|_8) = (48,84)$

Theorem 4 shows that p is equivalent to $x_1(x_2x_3 + x_4x_5)$. By the same reasoning as in (b),

$$|x_1(x_2x_3 + x_4x_5) + q(x_1, \cdots, x_8)|_8 = |q(0, x_2, \cdots, x_8)|_7 + |x_2x_3 + x_4x_5 + q(1, x_2, \cdots, x_8)|_7$$

and is therefore divisible by 8, but 84 is not divisible by 8. Thus (c) is impossible.

(d) $(|p|_8, |p + q|_8) = (56,76)$

Theorem 4 gives that p is equivalent to $x_1(x_2x_3 + x_4x_5 + x_6x_7)$ or to $x_1x_2x_3 + x_4x_5x_6$. $x_1(x_2x_3 + x_4x_5 + x_6x_7)$ can be excluded in the same way as (c) because 76 is not divisible by 8. So we want to find a second degree polynomial $q(x_1, \cdots, x_8)$ with $|x_1x_2x_3 + x_4x_5x_6 + q(x_1, \cdots, x_8)|_8 = 76$. This turns out to be impossible.

(d1) Suppose x_7x_8 is a term in $q(x_1, \cdots, x_8)$, so

$$q(x_1, \cdots, x_8) = p(x_1, \cdots, x_6) + x_7a(x_1, \cdots, x_6) + x_8b(x_1, \cdots, x_6) + x_7x_8$$

p is second degree, a and b first degree. Consider the affine transformation $x_7' = x_7 + b(x_1, \cdots, x_6)$ $x_8' = x_8 + a(x_1, \cdots, x_6)$ $x_i' = x_i$, $i = 1, \cdots, 6$ which does not affect $x_1x_2x_3 + x_4x_5x_6$. This transformation reduces our problem to: can $|x_1x_2x_3 + x_4x_5x_6 + p'(x_1, \cdots, x_6) + x_7x_8|_8$ be 76? Equation (1) gives us that this form is $64 + |x_1x_2x_3 + x_4x_5x_6 + p'(x_1, \cdots, x_6)|_6$ and Theorem 1 gives that this last part is 0 or $\geqq 16$; so it is never 76.

(d2) Suppose now that x_7x_8 is not a term in $q(x_1, \cdots, x_8)$, so $q(x_1, \cdots, x_8) = p(x_1, \cdots, x_6) + x_7a(x_1, \cdots, x_6) + x_8b(x_1, \cdots, x_6)$. p is second degree; a and b first degree. If $a = 0$ then $|x_1x_2x_3 + x_4x_5x_6 + p(x_1, \cdots, x_6) + x_8b(x_1, \cdots, x_6)|_8 = 2|x_1x_2x_3 + x_4x_5x_6 + p(x_1, \cdots, x_6) + x_8b(x_1, \cdots, x_6)|_7$ and so by Theorem 3 is divisible by 8; but 76 is not divisible by 8.

So $a \not\equiv 0$ and also $b \not\equiv 0$. If $a \equiv 1$ then $|x_1x_2x_3 + x_4x_5x_6 + p(x_1, \cdots, x_6) + x_7 + x_8b(x_1, \cdots, x_6)|_8 = 2^7$ and not 76. So $a \not\equiv 1$, and also $b \not\equiv 1$. So both a and b are affinely equivalent to x_1, not necessarily simultaneously.

Therefore, $x_1x_2x_3 + x_4x_5x_6 + q(x_1, \cdots, x_8)$ has to be equivalent to either: (1) $k(x_1, \cdots, x_6) + x_1x_7 + x_1x_8$ if $a = b$, or (2) $k(x_1, \cdots, x_6) + x_1x_7 + x_2x_8$ if $a \neq b$, where $k(x_1, \cdots, x_6)$ is of third degree. In (1) apply $x_8' = x_8 + x_7$,

$x_i' = x_i$, $i \neq 8$ and then we are in a previous case. In (2) $|k(x_1, \cdots, x_6) + x_1x_7 + x_2x_8|_8 = |k(0, x_2, \cdots, x_6) + x_2x_8|_7 + |k(1, x_2, \cdots, x_6) + x_7 + x_2x_8|_7 = |k(0, x_2, \cdots, x_6) + x_2x_8|_7 + 64$ and is therefore by Theorem 1 $\geq 16 + 64 = 80$. Conclusion: (d) is also impossible.

Lemma 3. *If $|f(x_1, \cdots, x_9)|_9 = 132$ for $f \in RM(3;2^9)$, then for any i, $(|f(x_i = 0)|_8, |f(x_i = 1)|_8) = (64,68)$ or $(68,64)$.*

Lemma 4. *If $f(x_1, \cdots, x_9) \in RM(3;2^9)$ and $|f|_9 = 132$, then $(|f(0, 0, x_3, \cdots, x_9)|_7, |f(0, 1, x_3, \cdots, x_9)|_7, |f(1, 0, x_3, \cdots, x_9)|_7, |f(1, 1, x_3, \cdots, x_9)|_7) = (32,32,32,36)$ or $32,32,36,32)$ or $(32,36,32,32)$ or $(36,32,32,32)$.*

Proof. Divide the word into the four parts corresponding to $(x_1, x_2) = (0, 0)(0, 1)(1, 0)(1, 1)$:

x_1:	0	0	1	1
x_2:	0	1	0	1
	a	b	c	d

and let a, b, c, and d be the weights of these parts. Then from Lemma 3

$$\begin{aligned} a + b &= 64, \quad c + d = 68 && A_1 \\ \text{or } a + b &= 68, \quad c + d = 64 && A_2 \\ \text{and } a + c &= 64, \quad b + d = 68 && B_1 \\ \text{or } a + c &= 68, \quad b + d = 64 && B_2 \end{aligned}$$

This gives four possible weight structures:

(1) A_1B_1	$64 - b$	b	b	$68 - b$
(2) A_1B_2	$64 - b$	b	$b + 4$	$64 - b$
(3) A_2B_1	$68 - b$	b	$b - 4$	$68 - b$
(4) A_2B_2	$68 - b$	b	b	$64 - b$

By $x_2' = x_2 + 1$, (2) is equivalent to (1); by $x_1' = x_1 + 1$, (3) is equivalent to (1); by $x_1' = x_1 + 1$, $x_2' = x_2 + 1$, (4) is equivalent to (1). So every codeword of weight 132 is in one of the forms (1) (2) (3) or (4) and is transformable into form (1). Under the transformation $x_1' = x_1 + x_2, x_2' = x_2$, (1) goes into the form

$$(64 - b, \quad 68 - b, \quad b, \quad b)$$

and this form has to be equivalent with (1) (2) (3) or (4). This is only possible if $b = 32$ or $b = 34$, but $b = 34$ is excluded by Theorem 3. (Each part $\in RM(3;2^7)$) for $b = 32$, (1) is (32,32,32,36), (2) is (32,32,36,32), (3) is (32,36,35,32), (4) is (36,32,32,32). Q.E.D.

Lemma 5. *Let $f(x_1, \cdots, x_m)$ be a third degree polynomial which is not a second degree polynomial of m variables. Then f can be transformed by an appropriate affine transformation into $x_1x_2x_3 + x_1p(x_4, \cdots, x_m) + x_2q(x_4, \cdots, x_m) + x_3r(x_4, \cdots, x_m) + k(x_4, \cdots, x_m)$ where p, q and r are polynomials of degree 2 and k of degree 3.*

Proof. w.l.o.g. $f(x_1, \cdots, x_m) = x_1x_2x_3 + x_1x_2a(x_4, \cdots, x_m) + x_1x_3b(x_4, \cdots, x_m) + x_2x_3c(x_4, \cdots, x_m) + x_1p(x_4, \cdots, x_m) + x_2q(x_4, \cdots, x_m) + x_3r(x_4, \cdots, x_m) + k(x_4, \cdots, x_m)$ where a, b and c have degree 1, p, q, and r have degree 2 and k has degree 3. The substitution of

$$x_3' = x_3 + a(x_4, \cdots, x_m)\, x_i' = x_i, i \neq 3$$

cancels $x_1x_2a(x_8, \cdots, x_m)$, affects only p, q, and k, which remain of 2nd, 2nd, and 3rd degree. Now the substitution $x_2' = x_2 + b(x_8, \cdots, x_m)\, x_1' = x_1 + c(x_8, \cdots, x_m)$ proves the theorem.

If $f(x_1, \cdots, x_9)$ is a third degree polynomial, we can divide it in the 8 parts where $(x_1,x_2,x_3) = (0,0,0) \cdots (1,1,1)$ and each part corresponds with a code word in RM $(3;2^6)$. We use the symbols p, q, r and k for the polynomial and the corresponding codeword.

Form 1. $x_1x_2x_3 + x_1p(x_4, \cdots, x_9) + x_2q(x_4, \cdots, x_9) + x_3r(x_4, \cdots, x_9) + k(x_4, \cdots, x_9)$ is of the form

Position	0	1	2	3	4	5	6	7
x_1	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_3	0	1	0	1	0	1	0	1
								1
					p	p	p	p
			q	q			q	q
		r		r		r		r
	k	k	k	k	k	k	k	k

We will need this form constantly in the rest of this proof.

Lemma 6. *If there is a codeword of weight 132 in $RM(3;2^9)$ then when it is transformed into Form 1, the weight of the position 6 and 7 has to be 36. Therefore (by Lemma 4) the positions 0 and 1, 2 and 3, 4 and 5 all have weight 32.*

Proof. Lemma 4 gives that 6, 7 has weight 32 or 36, so assume 6, 7 has weight 32, and that 2, 3 has weight 32. 2, 3 is an element in RM $(3;2^7)$ like 0, 1 and 4, 5 and 6, 7. 2, 3 is $k(x_4, \cdots, x_9) + q(x_4, \cdots, x_9) + x_3 r(x_4, \cdots, x_9)$ and has weight 32. 6, 7 is $k(x_4, \cdots, x_9) + q(x_4, \cdots, x_9) + p(x_4, \cdots, x_9) + x_3 r(x_4, \cdots, x_9) + x_3$ and has weight 32 (by assumption). So we see that $6, 7 = 2, 3 + p(x_4, \cdots, x_9) + x_3$. Now $|p(x_4, \cdots, x_9) + x_3|_7 = 2^6 = 64$, so we have added to 2, 3 (weight 32) a word of weight 64 $(p(x_4, \cdots, x_9) + x_3)$ and we get 6, 7, which also has weight 32. This is only possible if the positions of the *ones* of 2, 3 are a subset of the positions of the ones of $p(x_4, \cdots, x_9) + x_3$. This is equivalent to $p(x_4, \cdots, x_9) + x_3 = 0$ implies $k(x_4, \cdots, x_9) + q(x_4, \cdots, x_9) + x_3 r(x_4, \cdots, x_9) = 0$. In general, if a and b are polynomials over GF (2) and $a = 0$ implies $b = 0$, $b = ba$. So $k + q + x_3 r = (k + q + x_3 r)(p + x_3)$. Comparing the coefficients of x_3 gives

LEMMA 7. $k = pr + q$.

This implies that the positions 2, 3 (of Lemma 5) have the form

2	3
pr	$(p + 1)r$

if $r = 0$, pr and $(p + 1)r$ are both zero. If $r = 1$ then pr and $(p + 1)r$ are complementary. So 2, 3 has weight equal to the weight of r. But 2, 3 has weight 32, so $|r|_6 = 32$.

Supposition 1. 0, 1 has weight 36, so that 4, 5 has weight 32 (like 2, 3). If we now compare 4, 5 with 6, 7 (as we did above with 2, 3 and 6, 7), we find $k = qr + p$. Together with Lemma 7 this gives $r(p + q) = p + q$ or

LEMMA 8. *$r = 0$ implies $p + q = 0$.*

Now we divide positions 0 and 1 into the parts, where $r = 0$ and $r = 1$ (remember that $|r|_6 = 32$); then 0, 1 looks like

x_3	0	0	1	1
r	0	1	0	1
	$k(r = 0)$	$k(r = 1)$	$k(r = 0)$	$k(r = 1) + 1$
	u	v	w	x

v and x are complementary and so together have weight 32. The total weight is 36 (by assumption), so

LEMMA 9. *k has weight 2 on the positions where $r = 0$.*

Now we divide positions 6 and 7 into the parts where $r = 0$ and $r = 1$. Then 6, 7 looks like (by Lemma 8)

x_3	0	0	1	1
r	0	1	0	1
	$k(r = 0)$	$k(r = 1) + p(r = 1) + q(r = 1)$	$k(r = 0) + 1$	$k(r = 1) + p(r = 1) + q(r = 1)$
	a	b	c	d

$b = d$ and a and c are complementary, and so together have weight 32. The total weight is 32, so $b = d = 0$. So position $6 = (a, b) = (a, 0)$ and has weight 2 by Lemma 9. But position 6 is a codeword in RM $(3;2^6)$ and by Theorem 1 weight 2 is impossible. Hence, 0, 1 must have weight 32.

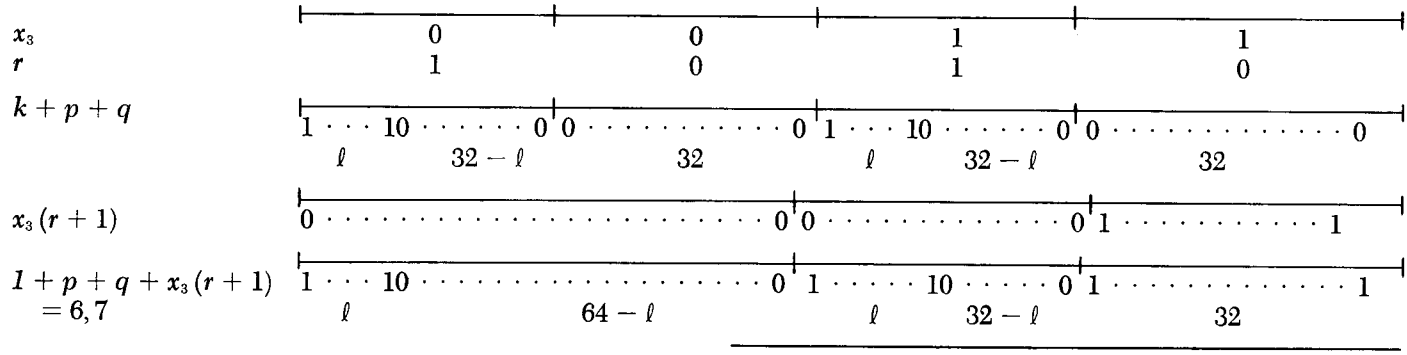
Supposition 2. 4, 5 has weight 36 and hence 0, 1 has weight 32. If we now compare 0, 1 with 6, 7 (the same way as done above with 4, 5 and 6, 7 and also with 2, 3 and 6, 7), we find $k = (p + q)r$ so $r = 0$ implies $k = 0$ and because $k = pr + q$ (Lemma 7), $r = 0$ implies $q = 0$. If we now compare 4, 5 with 6, 7 the same way as at the end of A), we get the same contradiction. The only assumption made is that 6, 7 has weight 32. The conclusion is that its weight is not 32 and by Lemma 3 its weight is 36. Q.E.D.

LEMMA 10. *If $x_1x_2x_3 + x_1 p(x_4, \cdots, x_9) + x_2 q(x_4, \cdots, x_9) + x_3 r(x_4, \cdots, x_9) + k(x_4, \cdots, x_9)$ has weight 132, where p, q and r are of degree 2 and k of degree 3, then $|p|_6 = |q|_6 = |r|_6 = 28$.*

Proof. We have seen that 0, 1 in Form 1 has weight 32, so $|r + k|_6 + |k|_6 = 32$ and $|r|_6 - |k|_6 \leq |r + k|_6 = 32 - |k|_6$ so $|r|_6 = 32$. 6, 7 in Form 1 has weight 36, so $|r + 1|_6 - |p + q + k|_6 \leq |r + p + q + k + 1|_6 = 36 - |p + q + k|$ or $|r + 1|_6 \leq 36$, so $|r|_6 \geq 28$. So $28 \leq |r|_6 \leq 32$. But $r \in$ RM $(2;2^6)$, so Form 1 gives that $|r|_6$ is 28 or 32.

Suppose $|r|_6 = 32$. If we look at positions 0 and 1, then we see that 0 and 1 are complementary on the positions where $r = 1$, so have weight 32 on these positions (32 positions). Because the total weight is 32 (Lemma 6), we see that $r = 0$ implies $k = 0$.

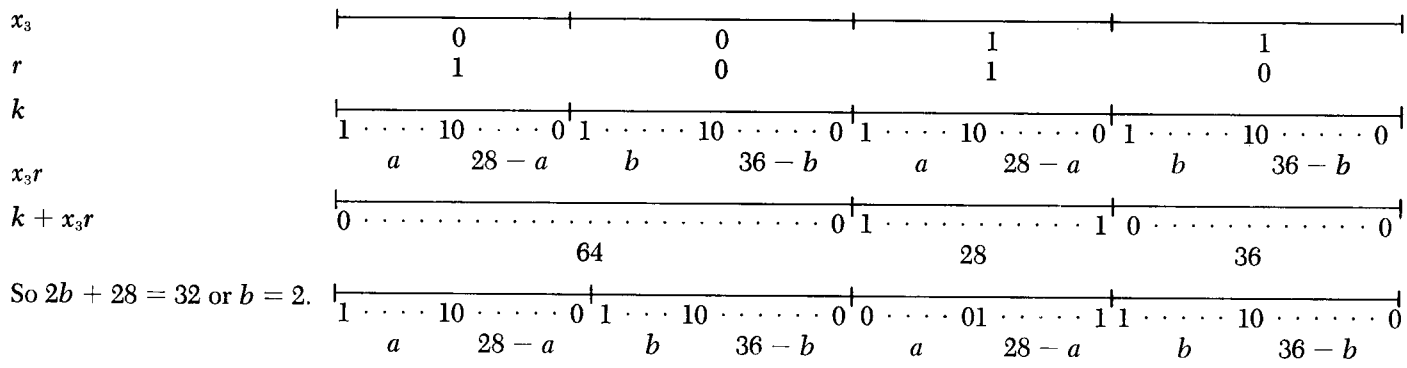
By the same reasoning on 2, 3, $r = 0$ implies $k + q = 0$, and on 4, 5 $r = 0$ implies $k + p = 0$. So we have $r = 0$ implies $(k = 0)$ and $(p = 0)$ and $(q = 0)$. This gives for positions 6, 7:



So $2\ell + 32 = 36$ or $\ell = 2$ but $|k+p+q|_6 = \ell$ ($k+p+q$ is position 6) so $\ell = 0$ or $\ell \geq 8$ by Theorem 1. This is a contradiction, hence $|r| = 28$. By interchanging x_1 and x_3 or x_2 and x_3 we also get $|p| = |q| = 28$. Q.E.D.

THEOREM 5. *In RM* $(3;2^9)$, $A_{132} = 0$.

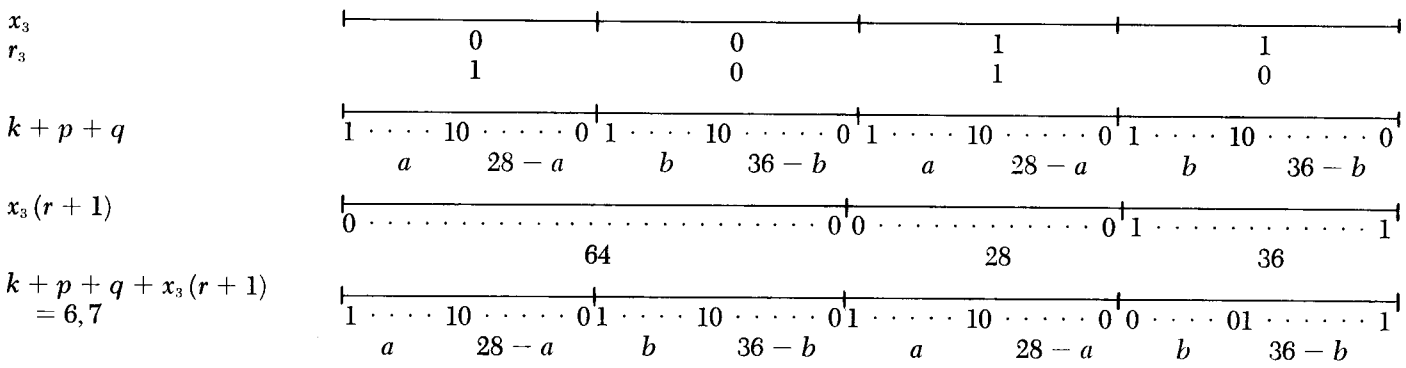
Proof. $|f|_9 = 132$. Then by Lemma 4 f can be written in the form Lemma 5, and by Lemma 10 $|p| = |q| = |r| = 28$. Positions 0, 1 have weight 32, so $|k + x_3 r|_7 = 32$.



Hence the work k has two ones on the positions where $r = 0$. By a similar argument on 2, 3 and 4, 3 we see that the same holds for $k + p$ and $k + q$. Because $k + p + q = k + (k + p) + (k + q)$, we know that

LEMMA 11. *$k + p + q$ has ≤ 6 ones on the positions where $r = 0$.*

Now we look again at 6, 7: $|k + p + q + x_3(r+1)|_6 = 36$.



So $2a + 36 = 36$, or $a = 0$. That means that all the ones of $k + p + q$ are on the positions where $r = 0$. But by Lemma 11 this is a contradiction with Theorem 1 ($k + p + q \in \mathrm{RM}(3;2^6)$) unless $k + p + q = 0$.

So the only possibility for a codeword of weight 132 is $k = p + q$, but then $k = p + q$ and $k = q + r$ and hence $p = q = r$, and that means $k = p + q = 0$ and that is impossible because then $32 = |k + x_3 r|_7 = |x_3 r|_7 = |r|_6 = 28$. Q.E.D.

References

1. van Lint, J. H., "Coding Theory," *Springer Lecture Notes in Mathematics No. 201*, Springer-Verlag, Berlin, 1971.

2. Berlekamp, E. R., *Algebraic Coding Theory*, pp. 361–367. McGraw Hill Book Co., Inc., New York, 1968.

3. Kasami, T., and Tokura, N., "On the Weight Structure of Reed-Muller Codes," *IEEE Trans. Inf. Theory*, Vol. IT-16, No. 6, pp. 752–758, Nov. 1970.

Table 1. RM $(3;2^8)$

Weight w	Words of this weight	Comment
0	0	
32	$x_1x_2x_3$	by (4b); ϵ RM $(3;2^3)$
48	$x_1(x_2x_3 + x_4x_5)$	by (4b); ϵ RM $(3;2^5)$
56	$x_1(x_2x_3 + x_4x_5x_6x_7)$ $x_1x_2x_3 + x_4x_5x_6$	by (4b); ϵ RM $(3;2^7)$ by (4a); ϵ RM $(3;2^6)$
64	x_1x_2	$w = 2d$; ϵ RM $(2;2^2)$
68	$x_1(x_2x_3 + x_4x_5) + x_6x_7x_8$	Compare with $w = 48$ and apply Eq. (2)
72	$x_1x_2x_3 + x_4x_5x_6 + x_1x_4$	ϵ RM $(3;2^6)$
76	$x_1(x_2x_3 + x_4x_5) +$ $x_6x_7x_8 + x_1x_6$	
80	$x_1x_2x_3 + x_4x_5$	ϵ RM $(3;2^5)$
84	$x_1(x_2x_3 + x_4x_5) +$ $x_6x_7x_8 + x_2x_6$	
88	$x_1(x_2x_3 + x_4x_5) + x_6x_7$	ϵ RM $(3;2^7)$; compare with $w = 48$ and apply Eq. (1)
92	$x_1x_2x_3 + x_4x_5x_6 + x_7x_8$	compare with $w = 56$ and apply Eq. (1)
96	$x_1x_2 + x_3x_4$	ϵ RM $(2;2^4)$
100	$x_1x_2x_3 + x_4x_5x_6 +$ $x_1x_4 + x_7x_8$	compare with $w = 72$ and apply Eq. (1)
104	$x_1x_2x_3 + x_4x_5 + x_6x_7$	compare with $w = 80$ and apply Eq. (1); ϵ RM $(3;27)$
108	$x_1(x_2x_3 + x_4x_5) +$ $x_6x_7x_8 + x_6$	compare with $w = 48$ and apply Eq. (3)
112	$x_1x_2 + x_3x_4 + x_5x_6$	ϵ RM $(2;2^6)$
116	$x_1x_2x_3 + x_4x_5 +$ $x_6x_7x_8 + x_6$	compare with $w = 80$ and apply Eq. (3)
120	$x_1x_2 + x_3x_4 + x_5x_6 + x_7x_8$	ϵ RM $(2;2^8)$
124	$x_1x_2x_3 + x_4x_5x_6 +$ $x_7x_8 + x_1x_4$	
128	x_1	ϵ RM $(1;2^1)$; $128 = 2^{m-1}$
$d = 2^{8-3} = 32$, $2^{\left\lceil \frac{8}{3} \right\rceil - 1} = 4$, so the weights are divisible by 4		

This table shows that there are no gaps in RM $(3;2^8)$ other than the ones already known.

Table 2. RM $(3;2^9)$

Weight w	Words of this weight	Comment
0	0	
64	$x_1x_2x_3$	by (4b); see $w = 32$ in RM $(3;2^8)$
96	$x_1(x_2x_3 + x_4x_5)$	by (4b); see $w = 48$ in RM $(3;2^8)$
112	$x_1(x_2x_3 + x_4x_5 + x_6x_7)$ $x_1x_2x_3 + x_4x_5x_6$	by (4b); see $w = 56$ in RM $(3;2^8)$ by (4a); see $w = 56$ in RM $(3;2^8)$
120	$x_1(x_2x_3 + x_4x_5 + x_6x_7 + x_8x_9)$	by (4b)
128	x_1x_2	$128 = 2d$; ϵ RM $(2;2^2)$
132	?	
136	$x_1(x_2x_3 + x_4x_5) + x_6x_7x_8$	ϵ RM $(3;2^8)$; see $w = 68$ in Table 1
140	?	
144	$x_1(x_2x_3 + x_4x_5 + x_6x_7) + x_1$	ϵ RM $(3;2^7)$
148	$x_1x_2x_3 + x_4x_5x_6 + x_7x_8x_9$	compare with $s = 112$ in this table and apply Eq. (2)
152	$x_1(x_2x_3 + x_4x_5) + x_6x_7x_8 + x_1x_6$	ϵ RM $(3;2^8)$; see $w = 76$ in Table 1
156	$x_1x_2x_3 + x_4x_5x_6 + x_7x_8x_9 + x_1x_4x_7$	
160	$x_1x_2x_3 + x_4x_5$	ϵ RM $(3;2^5)$
164	$x_1(x_2x_3 + x_4x_5 + x_6x_7) + x_2x_4x_8 + x_3x_5x_9$	
168	$x_1(x_2x_3 + x_4x_5) + x_6x_7x_8 + x_2x_6$	ϵ RM $(3;2^8)$; see $n = 84$ in Table 1
172	$x_1x_2x_3 + x_4x_5x_6 + x_1x_4 + x_7x_8x_9$	compare with $w = 72$ in Table 1 and apply Eq. (2)
176	$x_1(x_2x_3 + x_4x_5) + x_6x_7$	ϵ RM $(3;2^7)$
180	$x_1(x_2x_3 + x_4x_5 + x_6x_7 + x_8x_9) + x_2x_3x_4 + x_5x_6x_7$	
184	$x_1x_2x_3 + x_4x_5x_6 + x_9x_8$	ϵ RM $(3;2^8)$; see $n = 92$ in Table 1
188	$x_1(x_2x_3 + x_4x_5 + x_6x_7 + x_8x_9)$ $x_1 + x_2x_3x_4 + x_5x_6x_7$	
192	$x_1x_2 + x_3x_4$	ϵ RM $(2;2^4)$
196	$x_1x_2x_3 + x_4x_5x_6 + x_1 + x_1x_4 + x_7x_8x_9$	Apply Eq. (2) on first four terms
200	$x_1x_2x_3 + x_4x_5x_6 + x_1x_4 + x_7x_8$	ϵ RM $(3;2^8)$; see $w = 100$ in Table 1
204	$x_1(x_2x_3 + x_4x_5 + x_6x_7) + x_2x_4x_8 + x_3x_5x_9 + x_1$	Compare with $w = 64$
208	$x_1x_2x_3 + x_4x_5x_6 + x_1$	ϵ RM $(3;2^6)$
212	$x_1x_2x_8 + x_4x_5x_6 + x_7x_8x_9 + x_1x_4x_7 + x_1$	
216	$x_1(x_2x_8 + x_4x_5) + x_6x_7x_8 + x_6$	ϵ RM $(3;2^8)$; see $w = 108$ in Table 1
220	$x_1x_2x_3 + x_4x_5x_6 + x_7x_8x_9 + x_1$	Apply Eq. (2) or (3)
224	$x_1x_2 + x_3x_4 + x_5x_6$	ϵ RM $(2;2^6)$
	$x_1x_2 + x_3x_4x_5 + x_3$	ϵ RM $(3;2^5)$
228	$x_1x_2x_3 + x_4x_5x_6 + x_1x_4 + x_7x_8x_9 + x_7$	Compare with $w = 72$ in Table 1 and apply Eq. (3)
232	$x_1x_2x_3 + x_4x_5 + x_6x_7x_8 + x_6$	Compare with $w = 80$ in Table 1 and apply Eq. (3)
236	$x_1(x_2x_3 + x_4x_5 + x_6x_7) + x_2x_4x_8 + x_3x_5x_9 + x_8$	
240	$x_1x_2 + x_3x_4 + x_5x_6 + x_7x_8$ $x_1x_2 + x_3x_4 + x_5x_6x_7 + x_5$	ϵ RM $(2;2^8)$; see $w = 110$ in Table 1 ϵ RM $(3;2^7)$; apply Eq. (3)
244	$x_1x_2x_3 + x_4x_5x_6 + x_1 + x_4 + x_7x_8x_9$	
248	$x_1x_2x_3 + x_4x_5x_6 + x_1 + x_4 + x_7x_8$	ϵ RM $(2;2^8)$; see $w = 124$ in Table 1
252	$x_1x_2x_3 + x_4x_5x_6 + x_7x_8x_9 + x_1 + x_4 + x_7$	Apply Eq. (3)
256	x_1	$w = 2^{m-1}$

$d = 2^{9-3} = 64$, $2^{\left\lceil \frac{9}{3} \right\rceil - 1} = 4$

If $|f(x_1, \cdots, x_8)|_8 = k$, then $|f(x_1, \cdots, x_8)|_9 = 2k$, so half of the words in this table are elements of RM $(3;2^8)$