On the Weight Distributions of Optimal Cosets of the First-Order Reed–Muller Codes

Anne Canteaut

***Abstract*—We study the weight distributions of cosets of the first-order Reed–Muller code $R(1,m)$ for odd m, whose minimum weight is greater than or equal to the so-called quadratic bound. Some general restrictions on the weight distribution of a coset of $R(1,m)$ are obtained by partitioning its words according to their weight divisibility. Most notably, we show that there are exactly five weight distributions for optimal cosets of $R(1,7)$ in $R(5,7)$ and that these distributions are related to the degree of the function generating the coset. Moreover, for any odd $m \geq 9$, we exhibit optimal cubic cosets of $R(1,m)$ whose weights take on exactly five values.**

***Index Terms*—Boolean function, covering radius, nonlinearity, Reed–Muller code, weight distribution.**

I. Introduction

This correspondence is devoted to the determination of the weight distributions of cosets of the first-order Reed–Muller code of length 2^m, $R(1,m)$, which have a high minimum weight. We notably focus on almost optimal cosets, which are those whose minimum weight is greater than or equal to $2^{m-1} - 2^{(m-1)/2}$ for odd m. This lower bound, called the quadratic bound, coincides with the covering radius of $R(1,m)$ for $m \leq 7$. The addressed problem is of great importance in cryptography since the weight distributions of cosets of $R(1,m)$ correspond to the Fourier spectra of Boolean functions with m variables. Most notably, the nonlinearity of such a function is the minimum weight of the corresponding coset. But most cryptographic applications require many other properties for a Boolean function, beyond a high nonlinearity: balancedness, correlation-immunity, propagation criterion, etc. All these criteria are related to the weight distribution of the corresponding coset (see, e.g., [1]–[3]).

The weight distributions of all cosets of $R(1,5)$ have been determined by computer [4] but any enumerative search is obviously out of reach for higher values of m. Some properties concerning the weight divisibility of cosets of $R(1,m)$ [5] nevertheless yield restrictions on their possible weight distributions. We here generalize a technique introduced by Brouwer [6], Simonis [7], and Hou [8], [9], which consists in splitting the words of the coset into two subsets depending on their weight divisibility. This makes the determination of the weight distribution easier since both parts can be studied independently.

Section II recalls some important definitions and presents some preliminary results on the weight divisibility of Boolean functions. We then focus in Section III on a subset of a coset of $R(1,m)$ in $R(r,m)$, which is composed of all words whose weights are divisible by a higher value than the one given by Katz theorem. We exhibit the remarkable structure of this subset when r does not divide $(m-2)$. The size of this subset can also be determined when $r = m-2$ as shown in Section IV. Section V, finally, focuses on almost optimal cosets of $R(1,7)$ and $R(1,9)$.

II. Preliminary Results

Let $\mathcal{P}_m$ denote the algebra

$$\boldsymbol{F}_2[X_1,\ldots,X_m]/(X_1^2 - X_1,\ldots,X_m^2 - X_m).$$

Manuscript received January 26, 2000; revised July 20, 2000.

The author is with INRIA, Projet CODES, 78153 Le Chesnay Cedex, France (e-mail: Anne.Canteaut@inria.fr).

Communicated by A. Barg, Associate Editor for Coding Theory.
Publisher Item Identifier S 0018-9448(01)00369-8.

Any Boolean function with m variables, i.e., a function from $\boldsymbol{F}_2^m$ into $\boldsymbol{F}_2$, can be represented by a unique polynomial of $\mathcal{P}_m$, called its *algebraic normal form*. It can also be identified with the binary vector of length 2^m consisting of all values $f(x)$, $x \in \boldsymbol{F}_2^m$. The *Reed–Muller* code of length 2^m and of order $r, 0 \leq r \leq m$, denoted by $R(r,m)$, is then the linear binary code of length 2^m composed of the vectors corresponding to all Boolean functions with m variables of degree less than or equal to r. The code $R(r,m)$ can, therefore, be identified with the set of all elements of $\mathcal{P}_m$ of degree at most r.

Let $\rho(1,m)$ denote the covering radius of $R(1,m)$. When m is even, it is known that $\rho(1,m) = 2^{m-1} - 2^{(m/2)-1}$ and the cosets achieving this minimum weight are generated by *bent functions* [10]. When m is odd, the determination of $\rho(1,m)$ is still an open problem. In the general case, we know [11] that

$$2^{m-1} - 2^{\frac{m-1}{2}} \leq \rho(1,m) < 2^{m-1} - 2^{\frac{m}{2}-1}$$

where the lower bound, called the *quadratic bound*, is notably tight for $m \in \{3,5,7\}$ [4], [12], [13]. On the other hand, it is known that

$$\rho(1,m) \geq 2^{m-1} - (27/32)2^{\frac{m-1}{2}}$$

when $m \geq 15$ [14], [15].

Definition 1: Let m be an odd integer. A coset of $R(1,m)$ is said to be *almost optimal* if its minimum weight is greater than or equal to the quadratic bound $2^{m-1} - 2^{(m-1)/2}$. Moreover, it is said to be *optimal* if its minimum weight is equal to $\rho(1,m)$.

Even when $\rho(1,m)$ is unknown, we may have some information on the covering radius of $R(1,m)$ in $R(r,m)$, denoted by $\rho_r(1,m)$. This parameter corresponds to the highest possible minimum weight for a coset $f + R(1,m)$ where $f \in R(r,m)$. It is proved, for example, that, for any odd $m \leq 13$

$$\rho_3(1,m) = 2^{m-1} - 2^{\frac{m-1}{2}}$$

[16], [8]. Moreover, the quadratic case is completely solved [17, p. 441]: for any odd m

$$\rho_2(1,m) = 2^{m-1} - 2^{\frac{m-1}{2}}$$

and all almost optimal cosets of $R(1,m)$ in $R(2,m)$ have the same weight distribution, namely,

weight	$2^{m-1} \pm 2^{\frac{m-1}{2}}$	2^{m-1}
number of words	2^{m-1}	2^m

For odd m, any almost optimal coset of $R(1,m)$ whose weights take on exactly three values has the previous weight distribution. This weight distribution is then called *the three-weight almost-optimal distribution*. Note that any Boolean function with m variables which generates a coset with the three-weight almost-optimal distribution has degree at most $(m+1)/2$ [18, Proposition 4].

In the following, we denote by $\mathrm{wt}\,(x)$ the Hamming weight of a binary vector x, i.e., the number of its nonzero components. A Boolean function will often be identified with the binary vector composed of all its values. The Hamming weight of a Boolean function f with m variables then refers to the Hamming weight of the corresponding vector $(f(x), x \in \boldsymbol{F}_2^m)$. We now recall a classical formula for computing the Hamming weight of a Boolean function from its algebraic normal form (see [19] or [20, p. 240]).

Lemma 1: Let f be a Boolean function with m variables. Let $(f_1, \ldots, f_s)$ denote the monomials in the algebraic normal form of f. Then we have

$$\mathrm{wt}\,(f) = \sum_{k=1}^{s} \left((-1)^{k-1} 2^{k-1} \sum_{1 \le i_1 < \cdots < i_k \le s} 2^{m - r(i_1, \ldots, i_k)} \right)$$

where $r(i_1, \ldots, i_k)$ is the degree of the monomial $\prod_{j=1}^{k} f_{i_j}$ in $\mathcal{P}_m$.

We immediately deduce the following lemma.

Lemma 2: Let f and g be two Boolean functions with m variables. Let $(f_1, \ldots, f_{s_1})$ (resp., $(g_1, \ldots, g_{s_2})$) denote the monomials in the algebraic normal form of f (resp., g). Then we have

$$\mathrm{wt}\,(f+g) = \mathrm{wt}\,(f) + \sum_{k=1}^{s_1+s_2} (-1)^{k-1} 2^{k-1} \times \sum_{n=1}^{\min(k, s_2)} \sum_{\substack{1 \le i_1 < \cdots < i_{k-n} \le s_1 \\ 1 \le j_1 < \cdots < j_n \le s_2}} 2^{m - r(i_1, \ldots, i_{k-n}, j_1, \ldots, j_n)}$$

where $r(i_1, \ldots, i_{k-n}, j_1, \ldots, j_n)$ is the degree of the monomial

$$\prod_{u=1}^{k-n} f_{i_u} \prod_{v=1}^{n} g_{j_v}$$

in $\mathcal{P}_m$.

Proof: Since Lemma 1 holds even if some monomials appear twice in the algebraic normal form, we can consider that the algebraic normal form of $f + g$ consists of all monomials $(f_1, \ldots, f_{s_1}, g_1, \ldots, g_{s_2})$. It follows that

$$\mathrm{wt}\,(f+g) = \sum_{k=1}^{s_1+s_2} (-1)^{k-1} 2^{k-1} \times \sum_{n=0}^{\min(k, s_2)} \sum_{\substack{1 \le i_1 < \cdots < i_{k-n} \le s_1 \\ 1 \le j_1 < \cdots < j_n \le s_2}} 2^{m - r(i_1, \ldots, i_{k-n}, j_1, \ldots, j_n)}$$

where $r(i_1, \ldots, i_{k-n}, j_1, \ldots, j_n)$ is the degree of the monomial $f_{i_1} \ldots f_{i_{k-n}} g_{j_1} \ldots g_{j_n}$ after the reductions $x_i^2 = x_i$. We deduce that

$$\begin{aligned}\mathrm{wt}\,(f+g) = {} & \sum_{k=1}^{s_1+s_2} (-1)^{k-1} 2^{k-1} \sum_{1 \le i_1 < \cdots < i_k \le s_1} 2^{m - r(i_1, \ldots, i_k)} \\ & + \sum_{k=1}^{s_1+s_2} (-1)^{k-1} 2^{k-1} \times \sum_{n=1}^{\min(k, s_2)} \sum_{\substack{1 \le i_1 < \cdots < i_{k-n} \le s_1 \\ 1 \le j_1 < \cdots < j_n \le s_2}} 2^{m - r(i_1, \ldots, i_{k-n}, j_1, \ldots, j_n)}.\end{aligned}$$

Therefore, we have

$$\mathrm{wt}\,(f+g) = \mathrm{wt}\,(f) + \sum_{k=1}^{s_1+s_2} (-1)^{k-1} 2^{k-1} \times \sum_{n=1}^{\min(k, s_2)} \sum_{\substack{1 \le i_1 < \cdots < i_{k-n} \le s_1 \\ 1 \le j_1 < \cdots < j_n \le s_2}} 2^{m - r(i_1, \ldots, i_{k-n}, j_1, \ldots, j_n)}. \quad \square$$

The previous formula leads to the following well-known result [5], [8], known as Katz theorem, which will be extensively used in the correspondence.

Proposition 1: Let $f \in R(r_1, m)$ and $g \in R(r_2, m)$ with $r_2 \le r_1 \le m$. Then

$$\mathrm{wt}\,(f+g) \equiv \mathrm{wt}\,(f) \bmod 2^{\lceil \frac{m-r_2}{r_1} \rceil}.$$

This proposition applied to $g \in R(1, m)$ notably yields the following corollaries.

Corollary 1: Let $f \in R(m-2, m)$. For any word c in $f + R(1, m)$ we have

$$\mathrm{wt}\,(c) \equiv \mathrm{wt}\,(f) \bmod 4.$$

Corollary 2: Let f be an element of $R(r, m)$ such that $f + R(1, m)$ is an almost optimal coset of $R(1, m)$.

- For $m = 5$: if $r = 3$, $f + R(1, m)$ has the three-weight optimal distribution, and if $r = 4$, the weight of any word of $f + R(1, m)$ belongs to
$$\{2^{m-1}, 2^{m-1} \pm 2^{\frac{m-3}{2}}, 2^{m-1} \pm 2^{\frac{m-1}{2}}\}.$$
- For $m = 7$ and $3 \le r \le 5$, the weight of any word of $f + R(1, m)$ belongs to
$$\{2^{m-1}, 2^{m-1} \pm 2^{\frac{m-3}{2}}, 2^{m-1} \pm 2^{\frac{m-1}{2}}\}$$
- For $m \in \{9, 11\}$ and $r = 3$, the weight of any word of $f + R(1, m)$ belongs to
$$\{2^{m-1}, 2^{m-1} \pm 2^{\frac{m-3}{2}}, 2^{m-1} \pm 2^{\frac{m-1}{2}}\}.$$

Proof: In all considered cases, it is known that $\rho_r(1, m)$ is equal to the quadratic bound. Without loss of generality, we may assume that f is a minimum-weight word in the coset, i.e.,

$$\mathrm{wt}\,(f) = 2^{m-1} - 2^{\frac{m-1}{2}}.$$

By applying Proposition 1, we obtain that, for any $\phi \in R(1, m)$

$$\begin{aligned}\mathrm{wt}\,(f+\phi) &\equiv \mathrm{wt}\,(f) \bmod 2^{\lceil \frac{m-1}{r} \rceil} \\ &\equiv 0 \bmod 2^{\lceil \frac{m-1}{r} \rceil}.\end{aligned}$$

We then deduce that, for $f \in R(3, 5)$, the weights of all words in $f + R(1, 5)$ are divisible by $4 = 2^{(m-1)/2}$. For all other considered values of m and r, we have $2^{\lceil (m-1)/r \rceil} = 2^{(m-3)/2}$. It follows that the weight of any word in $f + R(1, m)$ takes one of the following five values: $2^{m-1}, 2^{m-1} \pm 2^{(m-3)/2}, 2^{m-1} \pm 2^{(m-1)/2}$. $\square$

III. Cosets of $R(1, m)$ in $R(r, m)$ when r Does Not Divide $m - 2$

Proposition 1 shows that, if f belongs to $R(r, m)$, then any $\phi \in R(1, m)$ satisfies

$$\mathrm{wt}\,(f+\phi) \equiv \mathrm{wt}\,(f) \bmod 2^{\ell}$$

with $\ell = \lceil (m-1)/r \rceil$. We are now interested in the structure of the following subset of $R(1, m)$:

$$E_f = \{\phi \in R(1, m), \mathrm{wt}\,(f+\phi) \equiv \mathrm{wt}\,(f) \bmod 2^{\ell+1}\}.$$

The following result generalizes a technique used by Hou [8], [9] in some particular cases.

Proposition 2: Let m and r be two integers such that $2 < r \le m$ and r does not divide $(m-2)$. Let $f \in R(r, m)$ and $\ell = \lceil (m-1)/r \rceil$. Suppose that $f + R(1, m)$ contains a word c such that

$$\mathrm{wt}\,(c) \not\equiv \mathrm{wt}\,(f) \bmod 2^{\ell+1}.$$

Then

$$E_f = \{\phi \in R(1,m), \mathrm{wt}\,(f+\phi) \equiv \mathrm{wt}\,(f) \bmod 2^{\ell+1}\}$$

is a linear subspace of $R(1,m)$ of codimension 1. Moreover, E_f contains the all-one vector if and only if $\mathrm{wt}\,(f) \equiv 0 \bmod 2^{\ell}$.

Proof: Let us identify any element of $R(r,m)$ with the corresponding polynomial in the algebra $\mathcal{P}_m$. We can write

$$\mathrm{wt}\,(f+\phi) = \mathrm{wt}\,(f) + \mathrm{wt}\,(\phi) - 2\mathrm{wt}\,(f\phi)$$

where $f\phi$ is the usual product in $\mathcal{P}_m$, i.e., $f\phi(x) = 1$ if and only if $f(x) = \phi(x) = 1$. Since $\mathrm{wt}\,(\phi) \equiv 0 \bmod 2^{m-1}$, we have

$$\mathrm{wt}\,(f+\phi) \equiv \mathrm{wt}\,(f) - 2\mathrm{wt}\,(f\phi) \bmod 2^{\ell+1}.$$

The set E_f can then be defined as

$$E_f = \{\phi \in R(1,m), \mathrm{wt}\,(f\phi) \equiv 0 \bmod 2^{\ell}\}.$$

Let us consider the mapping

$$\begin{array}{rccll} \Psi: & R(1,m) & \longrightarrow & \boldsymbol{F}_2 & \\ & \phi & \longmapsto & 0, & \text{if } \mathrm{wt}\,(f\phi) \equiv 0 \bmod 2^{\ell} \\ & & & 1, & \text{otherwise.} \end{array}$$

We now prove that Ψ is a linear mapping. For any $\phi_1, \phi_2 \in R(1,m)$, we have

$$\mathrm{wt}\,(f(\phi_1+\phi_2)) = \mathrm{wt}\,(f\phi_1) + \mathrm{wt}\,(f\phi_2) - 2\mathrm{wt}\,(f\phi_1\phi_2). \quad (1)$$

Since $\phi_1\phi_2 \in R(2,m)$, its weight is divisible by 2^{ℓ} because

$$\ell = \lceil (m-1)/r \rceil \leq \lfloor (m-1)/2 \rfloor$$

for $r > 2$. It follows that

$$\begin{aligned} \mathrm{wt}\,(f+(\phi_1\phi_2)) &= \mathrm{wt}\,(f) + \mathrm{wt}\,(\phi_1\phi_2) - 2\mathrm{wt}\,(f\phi_1\phi_2) \\ &\equiv \mathrm{wt}\,(f) - 2\mathrm{wt}\,(f\phi_1\phi_2) \bmod 2^{\ell}. \end{aligned}$$

Moreover, Proposition 1 implies that

$$\mathrm{wt}\,(f+(\phi_1\phi_2)) \equiv \mathrm{wt}\,(f) \bmod 2^{\lceil \frac{m-2}{r} \rceil}.$$

Since r is not a divisor of $(m-2)$, $\lceil (m-2)/r \rceil = \lceil (m-1)/r \rceil = \ell$. We deduce that

$$\mathrm{wt}\,(f\phi_1\phi_2) \equiv 0 \bmod 2^{\ell-1}.$$

Equation (1) then implies that

$$\mathrm{wt}\,(f(\phi_1+\phi_2)) \equiv \mathrm{wt}\,(f\phi_1) + \mathrm{wt}\,(f\phi_2) \bmod 2^{\ell}.$$

Ψ is, therefore, a linear mapping. Since it is assumed that $\Psi^{-1}(1) \neq \emptyset$, $E_f = \mathrm{Ker}\Psi$ is a linear subspace of $R(1,m)$ of codimension 1. Since

$$\mathrm{wt}\,(f+1) \equiv -\mathrm{wt}\,(f) \bmod 2^{\ell+1}$$

we obtain that the all-one vector belongs to E_f if and only if $\mathrm{wt}\,(f) \equiv 0 \bmod 2^{\ell}$. □

This result enables us to split a coset $f + R(1,m)$ into two different parts, namely, $f + E_f$ and $f + (R(1,m) \setminus E_f)$. We now suppose that all assumptions of the previous proposition are satisfied and that $f + R(1,m)$ is an almost optimal coset with $\mathrm{wt}\,(f) \equiv 0 \bmod 2^{\ell+1}$. In that case, we deduce some information on the weight distribution of the coset of $R(1,m-1)$ generated by the restriction of f to E_f.

Proposition 3: Let m be an odd integer and let r be such that $2 < r \leq m$ and r does not divide $m-2$. Let $\ell = \lceil (m-1)/r \rceil$ and $f \in R(r,m)$ such that $\mathrm{wt}\,(f) \equiv 0 \bmod 2^{\ell+1}$. Assume that $f + R(1,m)$ is an almost optimal coset and that it contains a word c such that $\mathrm{wt}\,(c) \equiv 2^{\ell} \bmod 2^{\ell+1}$. Then there exists $g \in R(r,m-1)$ such that the weight of any codeword in $g + R(1,m-1)$ belongs to

$$\left\{2^{m-2} \pm \left(2^{\frac{m-1}{2}} - 2^{\ell-1} - i2^{\ell}\right), 0 \leq i \leq 2^{\frac{m+1}{2}-\ell}\right\}.$$

Proof: Since $\mathrm{wt}\,(f) \equiv 0 \bmod 2^{\ell+1}$ and since all hypotheses of Proposition 2 are satisfied

$$E_f = \{\phi \in R(1,m), \mathrm{wt}\,(f+\phi) \equiv 0 \bmod 2^{\ell+1}\}$$

is a linear subspace of $R(1,m)$ of codimension 1 which contains the all-one vector. After a nonsingular affine transformation, we may assume that E_f is spanned by $1, x_1, \ldots, x_{m-1}$. For any Boolean function F with m variables, we denote by $F = (F_1, F_2)$ its decomposition relatively to x_m

$$F = (x_m + 1)F_1 + x_m F_2$$

where F_1 and F_2 are Boolean functions with $(m-1)$ variables. By definition, any function $\phi \in E_f$ can be written as $\phi = (\psi, \psi)$ with $\psi \in R(1,m-1)$. Similarly, any function $\phi \in (R(1,m) \setminus E_f)$ can be decomposed as $\phi = (\psi, \psi+1)$ with $\psi \in R(1,m-1)$. Let $f = (g,h)$ denote the decomposition of f where both g and h belong to $R(r,m-1)$. Then we have, for any $\phi = (\psi,\psi)$ in E_f

$$\begin{aligned} \mathrm{wt}\,(f+\phi) &= \mathrm{wt}\,(g+\psi) + \mathrm{wt}\,(h+\psi) \\ &\equiv 0 \bmod 2^{\ell+1}. \end{aligned}$$

For any $\phi = (\psi, \psi+1)$ in $R(1,m) \setminus E_f$, we obtain

$$\begin{aligned} \mathrm{wt}\,(f+\phi) &= \mathrm{wt}\,(g+\psi) + \mathrm{wt}\,(h+\psi+1) \\ &= \mathrm{wt}\,(g+\psi) + 2^{m-1} - \mathrm{wt}\,(h+\psi) \\ &\equiv 2^{\ell} \bmod 2^{\ell+1}. \end{aligned}$$

It follows that, for any $\psi \in R(1,m-1)$

$$\begin{aligned} \mathrm{wt}\,(g+\psi) &\equiv 2^{\ell-1} \bmod 2^{\ell} \\ \mathrm{wt}\,(h+\psi) &\equiv 2^{\ell-1} \bmod 2^{\ell}. \end{aligned}$$

We now prove that the minimum weight of $g + R(1,m-1)$ is at least $2^{m-2} - 2^{(m-1)/2} + 2^{\ell-1}$. Suppose that there exists $\psi \in R(1,m-1)$ such that

$$\mathrm{wt}\,(g+\psi) \leq 2^{m-2} - 2^{\frac{m-1}{2}}. \quad (2)$$

Since $h + R(1,m-1)$ contains no codeword of weight 2^{m-2}, we have that either $\mathrm{wt}\,(h+\psi) < 2^{m-2}$ or $\mathrm{wt}\,(h+1+\psi) < 2^{m-2}$. We deduce that either

$$\begin{aligned} \mathrm{wt}\,(f+(\psi,\psi)) &= \mathrm{wt}\,(g+\psi) + \mathrm{wt}\,(h+\psi) \\ &< 2^{m-1} - 2^{\frac{m-1}{2}} \end{aligned}$$

or

$$\begin{aligned} \mathrm{wt}\,(f+(\psi,\psi+1)) &= \mathrm{wt}\,(g+\phi) + \mathrm{wt}\,(h+1+\phi) \\ &< 2^{m-1} - 2^{\frac{m-1}{2}}. \end{aligned}$$

This would mean that $f + R(1,m)$ is not almost optimal, contradicting the assumption of the proposition. Therefore, ψ satisfying (2) does not exist. □

IV. Cosets of $R(1,m)$ in $R(m-2,m)$

The previous results do not hold when r divides $m-2$. In the special case $r = m-2$, we can nevertheless derive some information on the size of E_f, i.e., on the number of codewords in $f + R(1,m)$ whose weight is divisible by 8.

Lemma 3: Let $f \in R(m-2,m)$ with $m \geq 5$. Let I denote the set of all pairs of indexes (i,j) such that the algebraic normal form of f contains the monomial of degree $m-2$, $\prod_{k\neq(i,j)} x_k$. For any $g \in R(2,m)$, we have

$$\mathrm{wt}\,(fg) \equiv \#\{(i,j) \in I, x_i x_j \in g\} \bmod 2.$$

Proof: Let $g \in R(2,m)$. Using that

$$\mathrm{wt}\,(f+g) = \mathrm{wt}\,(f) + \mathrm{wt}\,(g) - 2\mathrm{wt}\,(fg)$$

and that $\mathrm{wt}\,(g)$ is divisible by 4 if $m \geq 5$, we have $\mathrm{wt}\,(fg) \equiv 0 \bmod 2$ if and only if $\mathrm{wt}\,(f+g) \equiv \mathrm{wt}\,(f) \bmod 4$. Let $(f_1,\ldots,f_{s_1})$ (resp., $(g_1,\ldots,g_{s_2})$) denote the monomials of f (resp., g). The formula given in Lemma 2 leads to

$$\mathrm{wt}\,(f+g) \equiv \mathrm{wt}\,(f) + \sum_{j=1}^{s_2} 2^{m-r(j)} - 2\sum_{1\leq j_1<j_2\leq s_2} 2^{m-r(j_1,j_2)} - 2\sum_{\substack{1\leq i\leq s_1\\ 1\leq j\leq s_2}} 2^{m-r(i,j)} \bmod 4.$$

Since $g \in R(2,m)$, for any $j_1, j_2 \in \{1,\ldots,s_2\}$, we have $r(j_1) \leq 2$ and $r(j_1,j_2) \leq 4$. For $m \geq 5$, we then deduce that

$$\begin{aligned}\mathrm{wt}\,(f+g) &\equiv \mathrm{wt}\,(f) - 2\sum_{\substack{1\leq i\leq s_1\\ 1\leq j\leq s_2}} 2^{m-r(i,j)} \bmod 4\\ &\equiv \mathrm{wt}\,(f) - 2\#\{(i,j)\in I, x_i x_j \in g\} \bmod 4 \qquad \square\end{aligned}$$

Proposition 4: Let $f \in R(m-2,m)\setminus R(m-3,m)$ with $m \geq 5$. Suppose that $\mathrm{wt}\,(f) \equiv 0 \bmod 8$. Then the weight of any codeword in $f + R(1,m)$ is divisible by 4 and

$$\#\{c \in f + R(1,m), \mathrm{wt}\,(c) \equiv 0 \bmod 8\} = 2^m + 2^i \text{ or } 2^m$$

with $\lceil m/2\rceil \leq i \leq m-1$.

Proof: Let I denote the set of all pairs (i,j) such that f contains the monomial of degree $m-2, \prod_{k\neq(i,j)} x_k$. Let

$$\hat{f}(x) = \sum_{(i,j)\in I} x_i x_j.$$

From Dickson's theorem [21, p. 197] there exists a function in the general affine group $AGL_m(\boldsymbol{F}_2)$ which transforms $\hat{f}$ into $\sum_{i=1}^{h} x_{2i-1}x_{2i}$ with $1 \leq h \leq \lfloor m/2\rfloor$. f can then be written as

$$f = \sum_{i=1}^{h}\left(\prod_{k\neq 2i-1,2i} x_k\right) + g, \qquad \text{with } g \in R(m-3,m).$$

We now decompose $R(1,m)$ as the direct sum $V_0 \oplus V_1 \cdots \oplus V_h \oplus \{1\}$ where V_0 is the subspace spanned by the linear functions $x_{2h+1},\ldots,x_m$ and, for $1 \leq i \leq h$, V_i is the subspace spanned by x_{2i-1} and x_{2i}. Let

$$E_i = \{\phi \in V_0 \oplus \cdots \oplus V_i, \mathrm{wt}\,(f\phi) \equiv 0 \bmod 4\}.$$

Assume that $m \neq 2h$, i.e., $V_0 \neq \emptyset$. For any $\phi_1, \phi_2 \in V_0$, we have

$$\mathrm{wt}\,(f(\phi_1+\phi_2)) = \mathrm{wt}\,(f\phi_1) + \mathrm{wt}\,(f\phi_2) - 2\mathrm{wt}\,(f\phi_1\phi_2).$$

Since the quadratic function $\phi_1\phi_2$ does not contain any monomial $x_{2k-1}x_{2k}$ with $1 \leq k \leq h$, we have from Lemma 3

$$\mathrm{wt}\,(f(\phi_1+\phi_2)) \equiv \mathrm{wt}\,(f\phi_1) + \mathrm{wt}\,(f\phi_2) \bmod 4.$$

It follows that either $E_0 = V_0$ or E_0 is a linear subspace of V_0 of codimension 1. Therefore, $|E_0| \in \{2^{m-2h-1}, 2^{m-2h}\}$. Let us now determine the size of E_{i+1} as a function of $|E_i|$. Let us decompose $\phi \in V_0 \oplus \cdots \oplus V_{i+1}$ as $\phi = \phi_1 + \phi_2$ with $\phi_1 \in V_0 \oplus \cdots \oplus V_i$ and $\phi_2 \in V_{i+1}$. From Lemma 3, we similarly have

$$\begin{aligned}\mathrm{wt}\,(f\phi) &= \mathrm{wt}\,(f(\phi_1+\phi_2))\\ &= \mathrm{wt}\,(f\phi_1) + \mathrm{wt}\,(f\phi_2) - 2\mathrm{wt}\,(f\phi_1\phi_2)\\ &\equiv \mathrm{wt}\,(f\phi_1) + \mathrm{wt}\,(f\phi_2) \bmod 4\end{aligned}$$

since the quadratic function $\phi_1\phi_2$ contains no monomial $x_{2k-1}x_{2k}$ with $1 \leq k \leq h$. It follows that $(\phi_2 + E_i) \subset E_{i+1}$ if and only if $\mathrm{wt}\,(f\phi_2) \equiv 0 \bmod 4$ and $(\phi_2 + \bar{E}_i) \subset E_{i+1}$ otherwise, where $\bar{E}_i = (V_0 \oplus \cdots \oplus V_i) \setminus E_i$. Using Lemma 3 we also obtain

$$\mathrm{wt}\,(f(x_{2i+1}+x_{2i+2})) \equiv \mathrm{wt}\,(fx_{2i+1}) + \mathrm{wt}\,(fx_{2i+2}) + 2 \bmod 4.$$

We then deduce that the three nonzero elements of V_{i+1}, namely, x_{2i+1}, x_{2i+2}, and $x_{2i+1}+x_{2i+2}$ do not lie all together in E_{i+1} or in $\bar{E}_{i+1}$: among these three functions, only one or two belong to E_{i+1}. By adding the zero vector, we obtain that two or three elements of V_{i+1} belong to E_{i+1}. It follows that

$$|E_{i+1}| = 2|E_i| + 2|\bar{E}_i| \text{ or } |E_{i+1}| = 3|E_i| + |\bar{E}_i|.$$

The first case leads to $|E_{i+1}| = 2^{m-2h+2i+1}$ and the second one to $|E_{i+1}| = 2^{m-2h+2i-1} + 2|E_i|$, i.e.,

$$|E_{i+1}| - 2^{m-2h+2i+1} = 2(|E_i| - 2^{m-2h+2i-1}).$$

By induction, we obtain that either $|E_h| = 2^{m-1}$ or

$$|E_h| = 2^{m-1} + 2^h(|E_0| - 2^{m-2h-1}).$$

We then conclude that

$$|E_h| = 2^{m-1} \text{ or } |E_h| = 2^{m-1} + 2^{m-h-1}.$$

Note that this result also holds when $m = 2h$. In this case, we start from E_1: we have $|E_1| \in \{2,3\}$ and we similarly obtain

$$|E_h| = 2^{m-1} \text{ or } |E_h| = 2^{m-1} + 2^{h-1}(|E_1| - 2).$$

The expected result can then be deduced from

$$\#\{\phi \in R(1,m), \mathrm{wt}\,(f+\phi) \equiv 0 \bmod 8\} = 2|E_h|. \qquad \square$$

V. Weight Distribution of Some Almost Optimal Cosets of $R(1,7)$ and $R(1,9)$

When the assumptions of Proposition 2 are satisfied, the decomposition of $f + R(1,m)$ into two parts makes the determination of the weight distribution easier: the weight distributions of both parts can be studied independently. This decomposition enables us to restrict the number of possible weight distributions for (almost) optimal cosets of $R(1,m)$ in $R(r,m)$ when $m \in \{5,7,9\}$ in some particular cases.

Proposition 5: Let $f \in R(r,m)$ such that $f + R(1,m)$ is an (almost) optimal coset. If $m \in \{5,7\}$ and $r = 4$ or if $m = 9$ and $r = 3$, $f + R(1,m)$ has either the three-weight almost optimal distribution or the following five-weight distribution:

weight	$2^{m-1} \pm 2^{\frac{m-1}{2}}$	$2^{m-1} \pm 2^{\frac{m-3}{2}}$	2^{m-1}
number of words	3.2^{m-3}	2^{m-1}	2^{m-2}

Proof: Let $(A_0,\ldots,A_{2^m})$ denote the weight distribution of $f + R(1,m)$. From Corollary 2, we know that $A_w = 0$ except for

$$w \in \{2^{m-1} \pm 2^{\frac{m-1}{2}}, 2^{m-1} \pm 2^{\frac{m-3}{2}}, 2^{m-1}\}.$$

Moreover, we may assume without loss of generality that $\mathrm{wt}\,(f) = 2^{m-1} - 2^{(m-1)/2}$. Suppose that $f + R(1,m)$ does not have the three-weight almost-optimal distribution. Since all hypotheses of Proposition 2 are satisfied

$$E_f = \left\{\phi \in R(1,m), \mathrm{wt}\,(f\phi) \equiv 0 \bmod 2^{\frac{m-1}{2}}\right\}$$

is a linear subspace of $R(1,m)$ which contains the all-one vector. After a nonsingular affine transformation, we may assume that E_f is spanned by $1, x_1, \ldots, x_{m-1}$. We now consider the $[2^m, m+1]$-linear codes

$$\mathcal{C}_1 = (f + E_f) \cup E_f$$

and

$$\mathcal{C}_2 = (f + (R(1,m) \setminus E_f)) \cup E_f.$$

We denote by $f = (g,h)$ the decomposition of f relatively to x_m. Using the same technique as in the proof of Proposition 3, we have that

$$\begin{aligned}\mathcal{C}_1 &= \{(g+\psi, h+\psi), \psi \in R(1,m-1)\}\\ &\quad \cup \{(\psi,\psi), \psi \in R(1,m-1)\},\\ \mathcal{C}_2 &= \{(g+\psi, h+1+\psi), \psi \in R(1,m-1)\}\\ &\quad \cup \{(\psi,\psi), \psi \in R(1,m-1)\}.\end{aligned}$$

Let $(\eta_0, \ldots, \eta_{2^m})$ and $(\nu_0, \ldots, \nu_{2^m})$ denote the weight distributions of these codes and $(\eta_0^\perp, \ldots, \eta_{2^m}^\perp)$ and $(\nu_0^\perp, \ldots, \nu_{2^m}^\perp)$ the weight distributions of their duals. By definition of E_f, $\mathcal{C}_2$ is a five-weight code whose weight distribution is given by

$$\begin{aligned}\nu_0 = \nu_{2^m} &= 1\\ \nu_{2^{m-1}-2^{\frac{m-3}{2}}} = \nu_{2^{m-1}+2^{\frac{m-3}{2}}} &= 2^{m-1}\\ \nu_{2^{m-1}} &= 2^m - 2.\end{aligned}$$

The second Pless power moment identity [22] applied to this code then leads to

$$\begin{aligned}\sum_{w=0}^{2^m} w^2 \nu_w &= 2^{3m-1} + 2^{2m-1} + 2^{2m-3}\\ &= 2^{2m-1}(2^m+1) + 2^{2m}\nu_1^\perp + 2^m \nu_2^\perp.\end{aligned}$$

Since E_f contains the all-one vector, $\nu_1^\perp = 0$. We deduce that $\nu_2^\perp = 2^{m-3}$. The definition of $\mathcal{C}_2$ also implies that

$$\nu_2^\perp = \#\left\{x \in \boldsymbol{F}_2^{m-1},\ g(x) = h(x) + 1\right\} = \mathrm{wt}\,(g+h).$$

Now, the five-weight code $\mathcal{C}_1$ has the following weight distribution:

$$\begin{aligned}\eta_0 = \eta_{2^m} &= 1\\ \eta_{2^{m-1}-2^{\frac{m-1}{2}}} = \eta_{2^{m-1}+2^{\frac{m-1}{2}}} &= A_{2^{m-1}-2^{\frac{m-1}{2}}}\\ \eta_{2^{m-1}} &= A_{2^{m-1}} + 2^m - 2.\end{aligned}$$

Here, the Pless second-power moment identity gives

$$\begin{aligned}\sum_{w=0}^{2^m} w^2 \eta_w &= (2^{2m-1} + 2^m) A_{2^{m-1}-2^{\frac{m-1}{2}}}\\ &\quad + 2^{2m-2} A_{2^{m-1}} + 2^{3m-2} + 2^{2m-1}\\ &= 2^{2m-1}(2^m+1) + 2^{2m}\eta_1^\perp + 2^m \eta_2^\perp.\end{aligned}$$

Exactly as for $\mathcal{C}_2$, we have $\eta_1^\perp = 0$ and

$$\eta_2^\perp = \#\{x \in \boldsymbol{F}_2^{m-1},\ g(x) = h(x)\} = 2^{m-1} - \nu_2^\perp.$$

It follows that

$$A_{2^{m-1}-2^{\frac{m-1}{2}}} + 2^{2m-2} A_{2^{m-1}} = 2^{3m-2} + 3 \cdot 2^{2m-3}.$$

By combining this relation with $2A_{2^{m-1}-2^{\frac{m-1}{2}}} + A_{2^{m-1}} = 2^m$, we deduce that

$$A_{2^{m-1}-2^{\frac{m-1}{2}}} = 3 \cdot 2^{m-3} \text{ and } A_{2^{m-1}} = 2^{m-2}. \qquad \square$$

We notably recover the weight distributions of optimal cosets of $R(1,5)$ found by simulations in [4].

Corollary 3: Let $f + R(1,5)$ be an optimal coset of $R(1,5)$. If $f \in R(3,5)$, this coset has the three-weight optimal distribution; otherwise, it has the five-weight distribution described in Proposition 5.

Proof: Since $\rho(1,5)$ is even, any optimal coset of $R(1,5)$ is generated by a function of degree at most 4. From Corollary 2, we have that $f + R(1,5)$ is a three-weight optimal coset when $f \in R(3,5)$. When f has degree 4, this weight distribution can not appear since $\deg(f) > (m+1)/2 = 3$. In this case, the five-weight distribution given in Proposition 5 is the only possible weight distribution for $f + R(1,5)$. $\square$

A. Optimal Cosets of $R(1,7)$ in $R(5,7)$

We now focus on optimal cosets of $R(1,7)$ in $R(5,7)$. We have proved that there are only two possible weight distributions for optimal cosets of $R(1,7)$ in $R(4,7)$. We now show that, if $f \in R(3,7)$, then $f + R(1,7)$ has the three-weight optimal distribution.

Theorem 1: Let $f \in R(3,7)$ such that $f + R(1,7)$ is optimal. Then $f + R(1,7)$ has the three-weight optimal distribution.

Proof: We may assume that $\mathrm{wt}\,(f) = 2^{m-1} - 2^{(m-1)/2} = 56$. Suppose that $f + R(1,7)$ does not have the three-weight optimal distribution. It then contains a word of weight 60. Proposition 3 then implies the existence of $g \in R(1,6)$ such that the weights of $g + R(1,6)$ belong to $\{26, 30, 34, 38\}$. Let $\mathcal{C}$ be the $[64,8]$-linear code $(g + R(1,6)) \cup R(1,6)$ and let $A_0, \ldots, A_{64}$ denote its weight distribution. We obviously have $A_0 = A_{64} = 1$, $A_{32} = 126, A_{26} = A_{38}$, and $A_{30} = A_{34} = 64 - A_{26}$. Since $\mathcal{C} \subset R(1,6)$, we have that $\mathcal{C}^\perp \subset R(4,6)$. It follows that the minimum distance of $\mathcal{C}^\perp$ is at least 4. The Pless second-power moment identity applied to $\mathcal{C}$ then leads to

$$\begin{aligned}\sum_{w=0}^{64} w^2 A_w &= (26^2+38^2)A_{26} + (30^2+34^2)(64-A_{26}) + 32^2 \cdot 126 + 64^2\\ &= 2^{12} \cdot 65.\end{aligned}$$

This implies that $A_{26} = 24$ and $A_{30} = 40$. Without loss of generality, we can suppose that $\mathrm{wt}\,(g) = 26$. By Proposition 2 we now deduce that

$$E_g = \{\phi \in R(1,6), \mathrm{wt}\,(g+\phi) \equiv 2 \bmod 8\}$$

is a linear subspace of $R(1,6)$ of codimension 1 which does not contain the all-one vector. E_g is then the set of all linear functions with six variables. Let $\mathcal{C}' = (g + E_g) \cup E_g$ and let $(B_0, \ldots, B_{64})$ denote its weight distribution. By definition, the weight of any codeword in $\mathcal{C}'$ belongs to $\{0, 26, 32, 34\}$. Moreover, we have

$$B_0 = 1, B_{32} = 63, B_{26} = 24, \text{ and } B_{34} = 40.$$

By applying the Pless first-power moment identity on $\mathcal{C}'$, we obtain

$$\sum_{w=0}^{64} w B_w = 4000 = 2^6(2^6 - B_1^\perp)$$

where $B_1^\perp$ denotes the number of codewords of weight 1 in $(\mathcal{C}')^\perp$. Since E_g corresponds to the set of all linear functions with six variables, we have that $B_1^\perp = 1$ if $g(0) = 0$ and $B_1^\perp = 0$ otherwise. It follows that the previous identity is not satisfied and therefore that $g +$

$R(1,6)$ cannot have the expected weight distribution. So $f + R(1,7)$ has the three-weight optimal distribution. □

Using Proposition 4 we are now able to restrict the number of possible weight distributions for optimal cosets of $R(1,7)$ in $R(5,7) \setminus R(4,7)$.

Proposition 6: Let $f \in R(5,7) \setminus R(4,7)$ such that $f + R(1,7)$ is optimal. Then $f+R(1,7)$ has one of the following weight distributions.

weight	56 72	60 68	64
number of words	48	64	32
	50	56	44
	52	48	56
	56	32	80

Proof: From Corollary 2, the weight of any word in $f + R(1,7)$ belongs to $\{56, 60, 64, 68, 72\}$. Let $(A_0, \ldots, A_{128})$ denote the weight distribution of $f + R(1,7)$. Proposition 4 implies that

$$|R(1,7) \setminus E_f| = A_{60} + A_{68} = 2A_{60} = 2^7 - 2^i \text{ or } 2^7$$

where $i \in \{4,5,6\}$. The weight distribution $(B_0, \ldots, B_{128})$ of the $[128,9]$-linear code $\mathcal{C} = (f + R(1,7)) \cup R(1,7)$ then satisfies

$$B_0 = B_{128} = 1$$
$$B_{56} = B_{72} = A_{56}$$
$$B_{60} = B_{68} = A_{60}$$

and

$$B_{64} = 254 + A_{64} = 510 - 2A_{56} - 2A_{60}.$$

The Pless second-power moment identity here gives

$$(56^2+72^2)A_{56}+(60^2+68^2)A_{60}+64^2(510-2A_{56}-2A_{60})+128^2 = 2^{14}(2^7+1).$$

It follows that $A_{56} = 64 - A_{60}/4$. We then deduce the complete weight distribution of $f + R(1,7)$ corresponding to each one of the four possible values of A_{60}. □

It follows that there are at most five different weight distributions for all optimal cosets of $R(1,7)$ in $R(5,7)$. These results are summed up in the following table.

weight	56 72	60 68	64	degree of f	
number of words	64		128	3 or 4	(I)
	48	64	32	4 or 5	(II)
	50	56	44	5	(III)
	52	48	56	5	(IV)
	56	32	80	5	(V)

Moreover, we can exhibit a coset having anyone of these weight distributions. Optimal cosets with weight distributions (I) and (III) have been found by Fontaine [18] (note that weight distribution (I) was obtained both for functions of degree 3 and 4). Distribution (II) appears for the following function of degree 4, $f_{(\mathrm{II})}$, which is derived from the five-weight optimal coset of $R(1,5)$ found in [4]

$$f_{(\mathrm{II})} = x_2x_3x_4x_5 + x_1x_2x_3 + x_2x_4 + x_3x_5 + x_6x_7.$$

We obtained by simulations some functions of degree 5 providing distributions (IV) and (V)

$$f_{(\mathrm{IV})} = x_1x_2x_3x_4x_5 + x_1x_2x_3x_6x_7 + x_1x_2x_4x_5 + x_1x_2x_7 + x_1x_4 + x_2x_5 + x_3x_6,$$
$$f_{(\mathrm{V})} = x_1x_2x_3x_4x_5 + x_1x_3x_7 + x_1x_2 + x_3x_4 + x_5x_6.$$

As pointed out in [23] and [18], the existence of a coset of $R(1,m)$ in $R(r,m)$ with weight distribution $(A_0, \ldots, A_{2^m})$ implies the existence of a coset of $R(1,m')$ in $R(r,m')$ with a "similar" weight distribution $(B_0, \ldots, B_{2^{m'}})$ for any $m' = m + 2i, i \geq 0$

$$B_{2^{m'-1} \pm 2^i u} = 2^{2i} A_{2^{m-1} \pm u}, \qquad \text{for all } 0 \leq u \leq 2^{m-1}$$

the other B_j's being zero. Using this construction we conclude.

Corollary 4: For any odd $m \geq 7$, there exists some almost optimal cosets of $R(1,m)$ in $R(5,m)$, $f+R(1,m)$, having the following weight distributions:

weight distribution of $f + R(1,m)$			
$2^{m-1} \pm 2^{\frac{m-1}{2}}$	$2^{m-1} \pm 2^{\frac{m-3}{2}}$	2^{m-1}	$\deg(f)$
$3 \cdot 2^{m-3}$	2^{m-1}	2^{m-2}	4
$25 \cdot 2^{m-6}$	$7 \cdot 2^{m-4}$	$11 \cdot 2^{m-5}$	5
$13 \cdot 2^{m-5}$	$3 \cdot 2^{m-3}$	$7 \cdot 2^{m-4}$	5
$7 \cdot 2^{m-4}$	2^{m-2}	$5 \cdot 2^{m-3}$	5

B. Optimal Cosets of $R(1,9)$ in $R(3,9)$

We have pointed out that, for $m = 7$, the existence of an optimal weight distribution is strongly related to the degree of the considered Boolean function. Finding how these parameters are related in the general case appears as an interesting problem. It is known, for instance, that, for any odd $m \geq 5$, there exists some almost-optimal cosets of $R(1,m)$ in $R(4,m)$ whose weight distributions differ from the three-weight almost-optimal distribution. But we conversely proved that any optimal coset of $R(1,7)$ in $R(3,7)$ has the three-weight optimal distribution. The following problem then immediately arises: do there exist almost-optimal cubic cosets of $R(1,m)$, m odd, whose weights take on more than three values?

If such a coset exists for $m = 9$, it has the five-weight distribution described in Proposition 5. Proposition 3 then implies that it is generated by a cubic function which is equivalent under the action of the general affine group to

$$(1 + x_9)g_1(x_1, \ldots, x_8) + x_9 g_2(x_1, \ldots, x_8) \tag{3}$$

where g_1 and g_2 are some elements of $R(3,8)$ such that the weights of $g_1 + R(1,8)$ and $g_2 + R(1,8)$ lie in $\{116, 124, 132, 140\}$.

We then determine by computer all cubic cosets of $R(1,8)$ having that property, up to $AGL_8(\boldsymbol{F}_2)$-equivalence. Since representatives F_i of the 32 $GL_8(\boldsymbol{F}_2)$-orbits of $R(3,8)/R(2,8)$ are known, we only have to examine the cubic functions $g \in F_i + R(2,8)$, $1 \leq i \leq 32$, where all F_i are given in [24, Table 2]. Cosets whose weights lie in $\{116, 124, 132, 140\}$ were found for $F_i = F_{14}, F_{26}, F_{27}$. An example is

$$g = x_1x_2x_3 + x_4x_5x_6 + x_1x_7x_8 + x_4x_7x_8 + x_1x_5 + x_1x_6 + x_1x_7 + x_1x_8 + x_2x_4 + x_2x_5 + x_2x_7 + x_3x_4 + x_5x_6 + x_5x_7.$$

For some pairs of such functions, construction (3) provides almost optimal cubic cosets of $R(1,9)$ having a five-weight distribution. An example is

$$f = x_1x_2x_3 + x_4x_5x_6 + x_1x_7x_8 + x_4x_7x_8 + x_9x_1x_4 + x_1x_5 + x_1x_6 + x_1x_7 + x_1x_8 + x_2x_4 + x_2x_5 + x_2x_7 + x_3x_4 + x_5x_6 + x_5x_7 + x_9x_1.$$

We then deduce the following theorem.

Theorem 2: For any odd $m \geq 9$, there exists almost optimal cosets of $R(1,m)$ in $R(3,m)$ having the following weight distribution:

weight	$2^{m-1} \pm 2^{\frac{m-1}{2}}$	$2^{m-1} \pm 2^{\frac{m-3}{2}}$	2^{m-1}
number of words	3.2^{m-3}	2^{m-1}	2^{m-2}

ACKNOWLEDGMENT

The author wishes to thank Pascale Charpin, Claude Carlet, Caroline Fontaine, and Simon Litsyn for many helpful discussions.

REFERENCES

[1] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, "Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions," in *Advances in Cryptology—EUROCRYPT 2000 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2000, vol. 1807, pp. 507–522.

[2] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, "On cryptographic properties of the cosets of $R(1,m)$," *IEEE Trans. Inform. Theory*, to be published.

[3] E. Filiol and C. Fontaine, "Highly nonlinear balanced Boolean functions with a good correlation-immunity," in *Advances in Cryptology—EUROCRYPT'98 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1998, vol. 1403, pp. 475–488.

[4] E. R. Berlekamp and L. R. Welch, "Weight distributions of the cosets of the (32,6) Reed-Muller code," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 203–207, Jan. 1972.

[5] N. Katz, "On a theorem of Ax," *Amer. J. Math.*, vol. 93, pp. 485–499, 1971.

[6] A. E. Brouwer, "The linear programming bound for binary linear codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 677–680, Mar. 1993.

[7] J. Simonis, "Restrictions on the weight distribution of binary linear codes imposed by the structure of Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 194–196, Jan. 1994.

[8] X.-D. Hou, "On the covering radius of $R(1,m)$ in $R(3,m)$," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1035–1037, May 1996.

[9] X.-D. Hou, "The covering radius of $R(1,9)$ in $R(4,9)$," *Des. Codes Cryptogr.*, vol. 8, pp. 285–292, 1996.

[10] O. S. Rothaus, "On bent functions," *J. Combin. Theory Ser. A*, vol. 20, pp. 300–305, 1976.

[11] T. Helleseth, T. Kløve, and J. Mykkeltveit, "On the covering radius of binary codes," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 627–628, Sept. 1978.

[12] J. Mykkeltveit, "The covering radius of the $(128,8)$ Reed–Muller code is 56," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 359–362, May 1980.

[13] X.-D. Hou, "Covering radius of the Reed-Muller code $R(1,7)$—A simpler proof," *J. Combin. Theory Ser. A*, no. 74, pp. 337–341, 1996.

[14] N. J. Patterson and D. H. Wiedemann, "The covering radius of the $[2^{15},16]$ Reed–Muller code is at least 16276," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 354–356, May. 1983.

[15] ——, "Correction to 'The covering radius of the $[2^{15},16]$ Reed–Muller code is at least 16276'," *IEEE Trans. Inform. Theory*, vol. 36, p. 443, Mar. 1990.

[16] P. Langevin, "Covering radius of $RM(1,9)$ in $RM(3,9)$," in *Eurocode'90 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1991, vol. 514, pp. 51–59.

[17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[18] C. Fontaine, "On some cosets of the first-order Reed-Muller code with high minimum weight," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1237–1243, May 1999.

[19] O. Moreno and J. C. Moreno, "The MacWilliams–Sloane conjecture on the tightness of the Carlitz–Uchiyama bound and the weights of duals of BCH codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1894–1907, Nov. 1994.

[20] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*. Amsterdam, The Netherlands: North-Holland, 1997.

[21] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*. New York: Dover, 1958.

[22] V. Pless, "Power moment identities on weight distributions in error-correcting codes," *Inform. Contr.*, vol. 3, pp. 147–152, 1963.

[23] R. A. Brualdi, N. Cai, and V. S. Pless, "Orphan structure of the first-order Reed-Muller codes," *Discr. Math.*, no. 102, pp. 239–247, 1992.

[24] X.-D. Hou, "$GL(m,2)$ acting on $R(r,m)/R(r-1,m)$," *Discr. Math.*, no. 149, pp. 99–122, 1996.

On the Covering Radius of Ternary Negacyclic Codes with Length up to 26

Tsonka S. Baicheva

***Abstract*—The covering radius of all ternary negacyclic codes of even length up to 26 is given. The minimum distances and weight distributions of all codes were recalculated. Seven of the open cases for the least covering radius of ternary linear codes were solved and for the other three cases upper bounds were improved.**

***Index Terms*—Covering radius, least covering radius, ternary linear codes, ternary negacyclic codes.**

I. INTRODUCTION

Covering radius is an important code parameter. If the code is used to correct errors and decoding to the nearest codeword is performed, then error vectors of weight greater than the covering radius are uncorrectable. If the code is used to compress data, its covering radius is a measure of maximum distortion. The covering radius also shows if a code is maximal, i.e., no more new codewords can be added to the code without decreasing its minimum distance.

There are now many papers concerning covering radius (see [1]) and many upper and lower bounds have been derived. Not much is known, however, about the exact values of the covering radii of basic families of codes and especially of codes over fields of more than two elements. One such example is ternary negacyclic codes whose covering radii are unknown. The aim of this work is to calculate the covering radii of all nonequivalent ternary negacyclic codes of length up to 26. Using the results obtained, open cases for the least covering radius of ternary linear codes are solved or upper bounds improved.

Manuscript received March 23, 2000; revised October 5, 2000. This work was supported under a DFG Contract. The material in this correspondence was presented in part at the 2000 IEEE International Symposium on Information Theory, Sorento, Italy, June 25–30, 2000.

The author is with the Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 5000 Veliko Tarnovo, Bulgaria (e-mail: lpmivt@vt.bia-bg.com).

Communicated by A. Barg, Asociate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(01)00595-8.