On Some Cosets of the First-Order Reed–Muller Code with High Minimum Weight

Caroline Fontaine

Abstract—We study a family of particular cosets of the first-order Reed–Muller code $R(1, m)$; those generated by special codewords, the idempotents. Thus we obtain new almost maximal weight distributions of cosets of $R(1, 7)$ and 84 distinct almost maximal weight distributions of cosets of $R(1, 9)$, that is, with minimum weight 240. This leads to cryptographic applications in the context of stream ciphers.

Index Terms—Boolean function, covering radius, idempotent, Reed–Muller code, stream cipher.

I. INTRODUCTION

The purpose of this correspondence is to study the weight distributions of cosets of the binary first-order Reed–Muller code generated by idempotents. We are particularly interested in the maximal weight distributions, that is, those weight distributions whose minimum weight is equal to the covering radius $\rho(1, m)$ of the first-order Reed–Muller code.

We will often use the correspondence between the binary $r$th-order Reed–Muller code of length $2^n$, denoted by $R(r, m)$, and the Boolean functions of $m$ variables with degree at most $r$. Thus we use both terminologies: the one of the Reed–Muller codes, and the one of the Boolean functions. This correspondence underlines the link between coding theory and cryptography, since $\rho(1, m)$ is the highest nonlinearity of Boolean functions, that is, the greatest distance from the affine functions; this criterion is very important, as well for block ciphers as for stream ciphers.

The weight of a coset $D$ of $R(1, m)$ is the minimum weight of the words of $D$; the coset $D$ is said to be maximal if its weight is equal to $\rho(1, m)$. When $m$ is even we know that $\rho(1, m) = 2^{m-1} - \frac{m}{2}$, and the associated Boolean functions are called bent functions [1]; moreover, there is a unique weight distribution for the maximal cosets. But in the case when $m$ is odd we do not know the exact value of $\rho(1, m)$ for arbitrary $m$; we only know that for all odd $m$ we have

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

More precisely we know that for $m = 3, 5, 7$ we have $\rho(1, m) = 2^{m-1} - 2\frac{m}{2}$ [2], [3] and that for odd $m \geq 15$, $\rho(1, m) > 2^{m-1} - 2\frac{m}{2}$ [4]–[6]. But for $m = 9, 11, 13$ we do not know if $\rho(1, m)$ matches the lower bound $2^{m-1} - 2\frac{m}{2}$ or not.

In Section II we recall some important definitions and we introduce our notation. Section III is entirely devoted to the idempotents: what they are and why they are interesting. In Section IV we recall the knowledge about the maximal weight distributions of cosets of $R(1, m)$; Sections V and VI are devoted to our theoretical and numerical results: we mostly exhibit four distinct maximal weight distributions for $m = 7$, and 84 distinct weight distributions with minimum weight $2^{m-1} - 2\frac{m}{2}$ $\geq 240$ for $m = 9$. At last, we present in Section VII some cryptographic applications of these results.


II. DEFINITIONS AND NOTATION

In this correspondence, we treat binary primitive codes of length $n = 2^m - 1$ or $2^m$. We denote by $F_q$ the Galois field of order $q$. The binary words $x'$ of length $n$ can be regarded as polynomials of $F_2[Z]/(Z^n - 1)$, which is the classical algebra for cyclic codes

$$x'(Z) = \sum_{i=0}^{n-1} x_i Z^i.$$  

From now on, $\alpha$ will be a fixed primitive element of $F_{2^m}$.

Definition 1: The punctured $r$th-order Reed–Muller code of length $n$, denoted by $R(r, m)$, is defined as the cyclic code which has as zeroes $\alpha^i$ for all $i$ satisfying $0 < w_2(i) < m - r$ (where $w_2(i)$ denotes the number of 1’s in the binary expansion of $i$). Then a codeword $x'(Z)$ of $R(r, m)$ is regarded as a polynomial $x'(Z)$ such that $x'(\alpha^i) = 0$ for all $i$ satisfying $0 < w_2(i) < m - r$. The $r$th-order Reed–Muller code of length $2^n$, denoted by $R(r, m)$, is obtained from $R(r, m)$ by adding an overall parity-check symbol: $R(r, m)$ is an extended cyclic code.

Any word $x = (x_0, x_1, \ldots, x_{n-1})$ of length $2^n = n + 1$ can be identified with a Boolean function of $m$ variables, taking $f(0) = x_0$ and $f(\alpha^i) = x_i$ for all $i = 0, \ldots, n - 1$. Let $f$ be such a function; its Algebraic Normal Form (ANF) is the polynomial $Q(f) \in F_2(z_1, \ldots, z_m)$ such that $Q(f)(z_1, \ldots, z_m) = f(z_1, \ldots, z_m)$ for all $(z_1, \ldots, z_m) \in F_2^m$, and the degree of $f$ is the global degree of $Q(f)$.

In the following, the correspondence between a word and the associated Boolean function will be often used, and both terminologies equivalently employed.

Since the codewords of $R(r, m)$ are the Boolean functions of degree at most $r$ the codewords of $R(1, m)$ are the affine functions.

For a given word $x$, we denote by $wt(x)$ its Hamming weight, and define the weight of the coset $x \oplus R(1, m)$ as the minimum weight...
for a word lying in this coset, that is, the minimal distance between the Boolean function \( f \) corresponding to \( x \) and the set of the affine functions. It measures the nonlinearity of \( f \), and this criterion is very important in cryptography, for example if \( f \) is designed to combine the outputs of some linear feedback shift registers and produce a running-key in the context of a stream cipher.

We can define the covering radius of \( R(1,m) \), denoted by \( \rho(1,m) \), as the maximum weight of a coset of \( R(1,m) \). Notice that \( \rho(1,m) \) is the highest nonlinearity for Boolean functions of \( m \) variables.

The weight distribution of the coset \( x \oplus R(1,m) \) is the set \( \{ W_i \}_{0 \leq i \leq 2^m} \) where \( W_i \) denotes the number of words of Hamming weight \( i \) lying in this coset.

We know that \( R(1,m) \) can be obtained from \( R(1,m) \) by deleting the first coordinate. But another important remark is that we can obtain the Simplex code \( S(m) \) of length \( n \) from \( R(1,m) \) by removing the all-one vector from the set of the generating vectors. We recall that \( S(m) \) is the dual of the Hamming code of length \( n \). We can recover the weight distribution \( \{ W_i \}_{0 \leq i \leq 2^m} \) of a coset \( \{ x \oplus R(1,m) \} \) from the weight distribution \( \{ W_i \}_{0 \leq i \leq 2^m} \) of \( x \oplus S(m) \): we have \( W_0 = W_{2^m} = w_0 \), and for all \( 1 \leq i \leq 2^n - 1 \), \( W_i = W_{2^m-i} = w_i + w_{2^m-i} \).

At last we introduce another representation for words of length \( n \) by means of their Mattson-Solomon polynomial [11].

**Definition 2:** Let \( x^* \) be a binary vector of length \( n \), It's Mattson-Solomon (MS) polynomial, denoted by \( MS_{x^*}(Z) \), belongs to \( F_{2^m}[Z] \) and is given by

\[
MS_{x^*}(Z) = \sum_{j=1}^{n} A_j Z^{-j}, \quad \text{with} \quad A_j = x^*(\alpha^j).
\]

\( MS_{x^*}(Z) \) is in fact a discrete Fourier transform of \( x^* \), and we can recover the coefficients of \( x^*(Z) \) by inverting this transformation: \( x_k = MS_{x^*}(\alpha^k) \).

**Proposition 1 [10]:** If \( x^* \) and \( y^* \) are binary vectors of length \( n \), then we have \( MS_{x^* \oplus y^*}(Z) = MS_{x^*}(Z) + MS_{y^*}(Z) \). Moreover, the coefficient \( A_n \) of \( MS_{x^*}(Z) \) is equal to \( wt(x^*) \mod 2 \).

### III. The Idempotents

Here we are interested in some particular cosets of \( R(1,m) \); those generated by idempotents. This study is motivated by the following points: first, the best nonlinearity obtained by picking idempotents at random is higher than the one obtained by picking regular Boolean functions; moreover, the only examples we know for cosets of \( R(1,m) \) whose minimum weight is greater than \( 2^{m-1} - 2^{m-3} \), when \( m \) is odd, are given by N. J. Patterson and D. H. Wiedemann in [4], [5] and are generated by idempotents.

We give here the definition and some well-known properties of idempotents [12].

**Definition 3:** The codeword \( x^* \) of length \( n \) is an idempotent if and only if

\[
x^*(Z) = \sum_{i=0}^{n-1} x_i Z^{-i}, \quad \text{with} \quad x_{2i} = x_i \text{ for all } i.
\]

Moreover, a word \( x = (0, x_0, \ldots, x_{m-1}) \) of length \( 2^m \) such that \( (x_0, \ldots, x_{m-1}) \) is an idempotent of length \( n \) is called here an idempotent too.

Notice that we are not interested here in the words \( x = (1, x_0, \ldots, x_{m-1}) \) such that \( (x_0, \ldots, x_{m-1}) \) is an idempotent of length \( n \); actually, this word is in the same coset of \( R(1,m) \) as \( (0, 1 + x_0, \ldots, 1 + x_{m-1}) \) (since \( R(1,m) \) contains the all-one vector) which is an idempotent in our definition. So, considering both \( (0, x^*) \) and \( (1, y^*) \), where \( x^* \) and \( y^* \) range in the set of the idempotents of length \( n \), would give each coset of \( R(1,m) \) twice.

We present now some useful properties of the MS polynomials of idempotents. Notice that we can immediately deduce from (2) that a codeword \( x^* \) is an idempotent if and only if \( x^*(Z) \) is of the form

\[
x^*(Z) = \sum_{x \in S} \sum_{z \in C_x} Z^i
\]

where \( C_s = \{ s, 2s, \ldots, 2^{m-1}s \} \). Moreover, (2) also implies the following results.

**Proposition 2:** The codeword \( x^* \) is an idempotent if and only if for all \( i \) we have \( x^*(\alpha^i)^2 = x^*(\alpha^i) \).

**Proof:** Consider \( x^* \) in \( F_{2^m}[Z]/(Z^n - 1) \). It is an idempotent if and only if we have for all \( i \) in \( [0 \cdots n - 1] \)

\[
x^*(\alpha^i)^2 = \left( \sum_{j=0}^{n-1} x_j \alpha^{2^j} \right)^2 = \sum_{j=0}^{n-1} x_j \alpha^{2^{2j}} = \sum_{j=0}^{n-1} x_j \alpha^{2^j} = x^*(\alpha^i).
\]

**Proposition 3:** The codeword \( x^* \) is an idempotent if and only if \( MS_{x^*}(Z) \) is an idempotent.

**Proof:** Consider \( x^* \) in \( F_{2^m}[Z]/(Z^n - 1) \). By Proposition 2, \( x^* \) is an idempotent if and only if the coefficients of \( MS_{x^*}(Z) \) belong to \( F_2 \) and are constant on each 2-cyclotomic coset modulo \( n \)—that is, \( x^*(\alpha) = x^*(\alpha') \) for all \( j \) in \( C_1 \). In other words, \( x^* \) is an idempotent if and only if its Mattson-Solomon polynomial is an idempotent.

We can use this result to represent an idempotent by a short MS polynomial, keeping only the index of one nonzero term of the MS polynomial for each class of nonzero coefficients.

**Example 1:** Take \( m = 3 \), and consider the idempotent \( x^* \) whose support is \( \{ \alpha^0, \alpha^1, \alpha^2, \alpha^4 \} \), where \( \alpha \) is a root of \( X^3 + X + 1 \): Its MS polynomial is \( Z^3 + Z^5 + Z^8 \). The nonzero coefficients are \( x^*(\alpha^1), x^*(\alpha^2), \) and \( x^*(\alpha^4) \). But 1, 2, 4 are all in the cyclotomic coset containing 1; so the short MS polynomial of \( x^* \) has only one nonzero coefficient—\( x^*(\alpha) \)—and is equal to \( Z^6 \).

Another important point concerning idempotents is that every cyclic code contains an idempotent which generates it entirely: its primitive idempotent. The Simplex code \( S(m) \) contains only one primitive idempotent: its MS polynomial is \( T_m(Z) = Z + Z^2 + \cdots + Z^{2^{m-1}} \).

### IV. The Weight Distributions: What Is Known

Before presenting our results let us recall what is known about the weight distributions of the cosets of \( R(1,m) \).

From now on, a coset \( D \) of \( R(1,m) \) will be called maximal if \( \rho(D) \) is known and \( wt(D) = \rho(D) \), and almost maximal if \( \rho(D) \) is unknown and \( wt(D) \geq 2^{m-1} - 2^{m-2} \).

For any \( m \), the weight distributions of the cosets \( x \oplus R(1,m) \) with \( x \in R(2,m) \backslash R(1,m) \) are known. Those with the highest minimum weight are

- for even \( m \):

<table>
<thead>
<tr>
<th>Weight</th>
<th>Number of Words</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2^{m-1} \pm 2^{m-1} )</td>
<td>( 2^m )</td>
</tr>
</tbody>
</table>

- for odd \( m \):

<table>
<thead>
<tr>
<th>Weight</th>
<th>Number of Words</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2^{m-1} \pm 2^{m-2} )</td>
<td>( 2^{m-1} )</td>
</tr>
</tbody>
</table>

These weight distributions are called the maximal quadratic weight distributions.
Proposition 4: The Boolean functions generating cosets with the maximal quadratic weight distribution are of degree at most $\frac{m}{2}$, for even $m \geq 4$, and $\frac{m+1}{2}$ for odd $m$.

Proof: The proof for even $m$ can be found in [1], [10]. For odd $m$, the functions $f$ which generate cosets with the maximal quadratic weight distribution satisfy
\[ \sum_{u \in F_{2}^{m}} (-1)^{f(u)+a.u} \in \{0, 2^{\frac{m+1}{2}}, -2^{\frac{m+1}{2}}\} \]
for all $a \in F_{2}^{m}$ [10, p. 415], and the final result is obtained by applying [13, Lemma 3].

For even $m$, all maximal cosets have the maximal quadratic weight distribution. The Boolean functions generating them are called bent functions and their degree is at most $\frac{m}{2}$ (see the preceding proposition).

For odd $m$, we must distinguish two cases.

- For $m = 3, 5, 7$ we know that $\rho(1,m) = 2^{m-1} - 2^{\frac{m+1}{2}}$ [2], [3], and all the weight distributions of the maximal cosets are known for $m = 3, 5$; E. R. Berlekamp and L. R. Welch have shown in [2] that for $m = 5$ there are two maximal weight distributions: the quadratic one and another one. We will show that for $m = 7$ there are also several maximal weight distributions.

- For $m \geq 9$ we do not know the exact value of $\rho(1,m)$. It is conjectured that the almost maximal cosets $D = x \oplus R(1,m)$ with $x \in R(3,m) \cap R(2,m)$ have the maximal quadratic weight distribution. X.-D. Hou has proved in [14] that for $m = 9, 11, 13$ the weight of $D$ cannot exceed $2^{m-1} - 2^{\frac{m+1}{2}}$ (see also the result of P. Langevin in [15] for $m = 9$). He has also shown in [16] that for $m = 9$ the weight of a coset $x \oplus R(1,m)$ with $x \in R(4,m) \setminus R(3,m)$ can not exceed $2^{m-1} - 2^{\frac{m+1}{2}}$.

Even if we know some theoretical results, it is still an important problem to exhibit some generators of maximal cosets. We will give in the next two sections our results, showing that idempotents enable us to obtain quite easily (almost) maximal cosets and new (almost) maximal weight distributions.

V. THE WEIGHT DISTRIBUTIONS: NEW THEORETICAL RESULTS

We present here two kinds of theoretical results: first we analyze the weight distributions of some particular cosets of $R(1,m)$; the second and third paragraphs deal with some constructions of new good cosets, that is, with a high minimum weight, from other ones.

A. Cosets $x \oplus R(1,m)$, Where $x \equiv (0,x')^T$ and $MS_{x'} = T_m(\lambda Z^{n-m})$

We describe here a general result on cosets whose generators have an MS polynomial of the form $T_m(\lambda Z^{n-m})$, where $\lambda$ lies in $F_{2^m}$ and $T_m$ denotes the trace function over $F_{2^m}$. Our proof is based on a result of T. Kasami [17].

Theorem 1: Let $m$ be odd and $x' \not\equiv S(m)$ be such that its MS polynomial is equal to $T_m(\lambda Z^{n-m})$, with $\lambda$ in $F_{2^m}$, and $t$ prime to $m$. $t \not\equiv -1 \mod n$. If $x$ is the word of length $2^m$ such that $x = (0,x')$, then $wt(x \oplus R(1,m)) \leq 2^{m-1} - 2^{\frac{m+1}{2}}$, and if the equality holds, then the weight distribution of $x \oplus R(1,m)$ is the following one:

<table>
<thead>
<tr>
<th>weight</th>
<th>$2^{m-1} \pm 2^{\frac{m+1}{2}}$</th>
<th>$2^{m-1}$</th>
<th>$2^m$</th>
</tr>
</thead>
</table>

Proof: We denote by $C$ the cyclic code of length $n$ and nonzeros $\alpha^{n-1}$ and $\alpha^t$ (and their conjugates). Since $t$ is prime to $n$, $t \not\equiv -1 \mod n$, $C$ has dimension 2m. The codewords of $C$ have an MS polynomial of the form $T_m(\mu Z^{n-m}) + T_m(\nu Z)$, with $\mu$ and $\nu$ in $F_{2^m}$. The set of words of the MS polynomial $T_m(\nu Z)$, with $\nu$ ranging in $F_{2^m}$, is the simplex code $S(m)$. Then $C$ contains $S(m)$ and $x^t \oplus S(m)$; thus $C^t$ is contained in $S(m)^t = H(m)$, the $[n, n - m, 3]$ Hamming code, and then has no word of weight 1 nor 2. So we can apply Theorem 13 of T. Kasami [17] (see a proof in [18, Theorem 3.30]): let $a_w$ denote the number of codewords of $C$ with Hamming weight $w$, and $w_0$ the smallest integer $0 < w < 2^{m-1}$ such that $a_w + 2w_0w_0 = 0$; then we have $w_0 \leq 2^{m-1} - 2^{\frac{m+1}{2}}$, and if the equality holds, the weight distribution of $C$ is the same as the one of the dual code of a double-error-correcting Bose–Chaudhuri–Hocquenghem (BCH) code, i.e., the only nonzero values of $a_w$ are

\[
\begin{array}{c|c}
\hline
w & a_w \\
\hline
0 & 1 \\
2^{m-1} - 2^{\frac{m+1}{2}} & (2^m - 1)(2^{m-2} + 2^{\frac{m+1}{2}}) \\
2^{m-1} & (2^m - 1)(2^{m-1} + 1) \\
2^m & (2^m - 1)(2^{m-2} - 2^{\frac{m+1}{2}}) \\
\hline
\end{array}
\]

Now, if we remove from $C$ all the words of $S(m)$, we obtain the set of words whose MS polynomials are of the form $T_m(\mu Z^{n-m}) + T_m(\nu Z)$, with $\mu \neq 0$. Since $t$ is prime to $n$, $t \not\equiv -1 \mod n$, this set is in fact \{shift$(x') \oplus S(m)$\} where shift$(x')$ denotes all the possible vectors obtained by shifting the vector $x'$: it is a union of cosets of $S(m)$ which have all the same weight distribution. The one of $x \oplus R(1,m)$ is obtained from it by adding for each $i$ the number of words of weight $i$ and the number of words of weight $2^m - i$.

B. Constructing New Good Orphan Cosets from Other Ones

The notion of “orphan cosets” has been introduced by T. Helleseth and H. F. Mattson Jr. in [19] with the “urocosets” terminology, and then studied by R. A. Brualdi and V. S. Pless in [20], [6] with the “orphan cosets” terminology. We call a minimum-weight word in some coset a leader of that coset. Let $C'$ and $C''$ be two cosets of a binary linear code. We use the notation $C' \prec C''$ if and only if there exists leaders $x'$ of $C'$ and $x''$ of $C''$ such that $x''$ covers $x'$ (i.e., $x' \equiv 1$ implies $x'' \equiv 1$), $C'$ is a child of $C''$ if and only if $C' \prec C''$ and there does not exist $D$ such that $C' \prec D \prec C''$; then we also say that $C''$ is a parent of $C'$. The coset $C'$ is called an orphan if and only if it has no parent. We can remark that $C' \prec C''$ implies that $wt(C'(t)) \leq wt(C''(t))$. Another important property is that all maximal cosets are orphans, but in general the converse is not true. In [6], the authors give a construction of orphan cosets of $R(1,m)$, and they show the following fact: if for a given odd $m$ there exist an orphan coset of weight greater than $2^{m-1} - 2^{\frac{m+1}{2}}$, then for any odd $m' > m$ there exists an orphan coset of $R(1,m')$ of weight greater than $2^{m'-1} - 2^{\frac{m'+1}{2}}$; in their proof they construct the second coset from the first one, and from this construction we can deduce the following.

Theorem 2: Let $m$ be an integer, and $C_1 = f \oplus R(1,m)$ be an orphan coset with weight distribution $\{W_{i}\}_{0 \leq i \leq 2^{m-1}}$. Thus for any integer $m'$ which is of the form $m' = m + 2u$, with $u > 0$, the coset $C_1' = g \oplus R(1,m')$, where the ANF of $g$ is obtained from the one of $f$ by
\[
g(z_1, \ldots, z_m) = f(z_1, \ldots, z_m) + z_{m+1}z_{m+2} + \cdots + z_{m+u}z_m,
\]
\[\text{is orphan, and its weight distribution } \{W_{i}\}_{0 \leq i \leq 2^{m'-1}} \text{ satisfy}
\]
\[
W_{2^m-1+i}(2^{m'-1-i} - 2^u) = 2^{2u} \times W_{i},
\]
for all $0 \leq i \leq 2^{m'-1}$, which is equivalent to
\[
W_{2^m-1+i}(2^{m'-1-i} - 2^u) = 2^{2u} \times W_{2^m-1-i},
\]
for all $0 \leq i \leq 2^{m'-1}$, the other $W_{i}'$'s being all zero.
This result enables us to deduce some weight distributions of cosets of $R(1, m')$ from the ones of cosets of $R(1, m)$, and to construct these cosets.

**Example 2:** According to the results presented by E. R. Berlekamp and L. R. Welch in [2], and to the preceding theorem, we can construct, for any odd $m \geq 5,208,320$ orphan cosets of $R(1, m)$, with minimum weight $2^{m-1} - 2\frac{m-1}{2}$, and with the following weight distribution:

<table>
<thead>
<tr>
<th>weight</th>
<th>$2^{m-1} \pm 2\frac{m-1}{2}$</th>
<th>$2^{m-1} \pm 2\frac{m-1}{2}$</th>
<th>$2^{m-1}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>number of words</td>
<td>$2^{m-5} \times 12$</td>
<td>$2^{m-5} \times 16$</td>
<td>$2^{m-5} \times 8$</td>
</tr>
</tbody>
</table>

**C. Constructing New Good Idempotents from Other Ones**

Now let us look at the action of the Linear Group on our idempotents and on the cosets of $R(1, m)$ generated by them. We will call 2-permutation polynomial a polynomial

$$P(X) = \sum_{i=0}^{m-1} p_i X^{2^i} \in F_2[X]$$

such that the mapping $e \mapsto P(e)$ is a permutation on $F_{2m}$ (since it is a linear mapping, this means that its kernel is $\{0\}$).

Let us denote by $\mathcal{P}$ the set of such polynomials. Let $\beta \in F_{2m}$. By class $(\beta)$ we will denote the set $\{\beta, \beta^2, \cdots, \beta^{2^{m-1}}\}$, that is, the conjugacy class of $\beta$.

**Lemma 1:** Let $P$ be in $\mathcal{P}$ and let $(\gamma, \gamma^2, \cdots, \gamma^{2^{m-1}})$ be a normal basis of $F_{2m}$. Then its image by $P$ is also a normal basis of $F_{2m}$.

**Proof:** First we will show that the image of $(\gamma, \gamma^2, \cdots, \gamma^{2^{m-1}})$ by $P$ is of the form $(\delta, \delta^2, \cdots, \delta^{2^{m-1}})$ with $\delta = P(\gamma)$: for all $j = 0, \cdots, m-1$ we have

$$P(\gamma^{2^j}) = \sum_{i=0}^{m-1} p_i(\gamma^{2^j})^{2^i} = \sum_{i=0}^{m-1} p_i(\gamma^i)^{2^j} = \left(\sum_{i=0}^{m-1} p_i \gamma^i\right)^{2^j} = P(\gamma)^{2^j}$$

and thus

$$\{P(y), y \in \text{class}(\gamma)\} = \{P(\gamma^{2^j}), j = 0, \cdots, m-1\} = \{P(\gamma)^{2^j}, j = 0, \cdots, m-1\} = \text{class}(P(\gamma)).$$

Now, since $P$ is an $F_2$-linear permutation polynomial, the image of a basis is also a basis. This concludes the proof. \hfill \Box

In the following we will denote by $\log(\beta)$, where $\beta$ is an element of $F_{2m}$, the unique integer of $[0 \cdots 2^m - 2]$ such that $\alpha^{\log(\beta)} = \beta$.

**Proposition 5:** Let $x$ be an idempotent. Let $\mathcal{P}_x$ be the function

$$\mathcal{P}_x : \sum_{i=0}^{n-1} x_i Z^{i} \mapsto \sum_{i=0}^{n-1} x_i Z^{\log(P(\alpha^i))}.$$

If $P$ belongs to $\mathcal{P}$, then $\mathcal{P}_x(x)$ is an idempotent too, and the Boolean functions associated with these idempotents have the same degree. Moreover, the cosets $\mathcal{P}_x(x) \oplus R(1, m)$ and $x \oplus R(1, m)$ have the same weight distributions.

**Proof:** Since $x$ is an idempotent, it can be written as $\sum_{s \in S} \sum_{e \in C_{S}} Z^i$ for some set $S$ of representatives of some 2-cyclic cosets modulo $n$. So $\mathcal{P}_x(x)$ is equal to

$$\sum_{s \in S} \sum_{e \in C_{S}} Z^{\log(P(\alpha^i))} = \sum_{x \in \{\log(P(\alpha^i)), i \in S\}} \sum_{e \in C_{S}} Z^i$$

and $\mathcal{P}_x(x)$ is an idempotent.

We know that the automorphism group of $R(1, m)$ is the general affine group [10, p. 399], thus since $P$ is a linear permutation, $x \oplus R(1, m)$ and $\mathcal{P}_x(x) \oplus R(1, m)$ have the same weight distribution. The remark concerning the degree of the Boolean functions also comes from the linearity of $P$. \hfill \Box

The set of the 2-permutation polynomials is then a subset of the automorphism group of the idempotents. But actually we do not know if it is the whole group. This defines a kind of equivalence between idempotents and enables us to construct, from one coset, a lot of cosets with the same weight distribution.

**Example 3:** When $m = 15$ we can construct from each of the two cosets given by N. J. Patterson and D. H. Wiedemann in [4] and [5] 675 other cosets with the same weight distribution.

**VI. THE WEIGHT DISTRIBUTIONS: NUMERICAL RESULTS**

After some explanations on our algorithm, we present new numerical results, distinguishing between the cases when $\rho(1, m)$ is known and the cases when it is not already known.

**A. Algorithm**

We present here our algorithm, which generates idempotents whose MS polynomials have all the same number of terms. This enables us to compute all the idempotents for small values of $m$, and to study a complete sublist of idempotents for large values of $m$. This approach is motivated by the fact that the short MS polynomials of the idempotents given by N. J. Paterson and D. H. Wiedemann are sparse, since they have, respectively, three and five terms.

**Algorithm 1 (Inputs: $m, T, b$):** Generate all the short MS polynomials $MS_{\rho}(Z)^T$ with $T$ nonzero coefficients, and such that $A_{2^{m-1}-1} = 0$ (to obtain each coset only once). For each of them

1) compute the weight distribution of $(0, x^*) \oplus R(1, m)$. If there is a word of weight less than $b$, then go directly to the next short MS polynomial;
2) display $MS_{\rho}(Z)^T$ and the weight distribution of $(0, x^*) \oplus R(1, m)$.

**Remark 1:** We know that the idempotents $x^*$ and $x^* \oplus s^*$ (where $s^*$ denotes the idempotent which generates the Simplex code $S(m)$) are in the same coset. Since the short MS polynomial of $s^*$ has only one nonzero coefficient—$s^*(\alpha^{m-1}-1)$—we will look only at idempotents such that $x^*(\alpha^{m-1}-1) = 0$. Then we are sure not to obtain the same coset twice.

**Remark 2:** In our computations we looked only at the proper cosets of $R(1, m)$, that is, those which are distinct from $R(1, m)$. This means that if there are $j$ 2-cyclic cosets, there are $2^{m-1} - 1$ proper cosets of $R(1, m)$ generated by the $2^j - 2$ idempotents.

**Remark 3:** When $m$ is odd and the short MS polynomial of the idempotent $x^*$ is $Z^{2^{m-1}}$ with $t$ prime to $n$, $t \not\equiv -1 \mod n$, the weight of the coset $x \oplus R(1, m)$ (where $x \equiv (0, x^*)$) is at most $2^{m-1} - 2\frac{2^{m-1}}{2}$, and if the equality holds, its weight distribution is the maximal quadratic one (see Theorem 1). This enables us to find...
very easily some idempotents, generating cosets with the maximal quadratic weight distribution.

Remark 4: When $m$ is odd, the major part of the almost maximal nonquadratic weight distributions corresponds to idempotents of degree at least $\frac{m-1}{2} + 1$ (see Proposition 4). So the short MS polynomial of such idempotents must have at least one nonzero coefficient $x^r(z_j)$ with $w_2(i) \geq \frac{m-1}{2}$. It is now easy to think that when the number of classes of nonzero coefficients we choose increases, thus the chance of obtaining an idempotent of high degree increases also, and then the chance of getting an almost maximal weight distribution which is not the maximal quadratic one.

B. When $\rho(1,m)$ Is Known

$m = 5$: E. R. Berlekamp and L. R. Welch give in their paper [2] all the weight distributions of the cosets of $R(1,5)$, and they show that there are two maximal weight distributions.

In computing the weight distributions of the $2^5 - 1$ proper cosets of $R(1,5)$ generated by idempotents, we found the quadratic maximal one for nine of the cosets, but never the other maximal distribution.

Here are some examples of short MS polynomials of idempotents which generate maximal cosets: $Z_2^{74} + Z_2^{120} + Z_2^{16}$ (degree 2), $Z_2^{80} + Z_2^{124} + Z_2^{16}$ (degree 3).

$m = 6$: We computed all weight distributions of the $2^{12} - 1$ proper cosets of $R(1,6)$ generated by idempotents. We found 12 maximal cosets corresponding to the bent functions, classified by O. S. Rothaus in [1].

Here are some examples of the short MS polynomials of idempotents generating them: $Z_2^{18} + Z_2^{10} + Z_2^{30} + Z_2^{12}$ (degree 2), $Z_2^{36} + Z_2^{12} + Z_2^{30}$ (degree 3).

$m = 7$: We computed all the $2^{18} - 1$ proper cosets generated by idempotents. 2947 of them are maximal, and we observed four different maximal weight distributions, which are listed in Table I. The links between these weight distributions according to the number of words of weight 1 of the functions lying in these cosets.

We summarize our results in Table III, giving new almost maximal weight distributions, sorted according to the number of words of weight 2, 4, 8, 16, 32, 64, 128, 256, 512 for each of them we give the number of cosets we found and for some of them, as an index, the degree of the functions lying in these cosets.

When we look at this table, we can see that there are 83 almost maximal nonquadratic weight distributions. And each time we increase the number of classes of nonzero coefficients, we obtain new ones (see Remark 4). Some of these weight distributions are just obtained a few times, but it is possible by applying the 2-permutation polynomials on their idempotent generators to construct a lot of other cosets with the same weight distributions.

Another remark is that we obtained some idempotents of degree $\frac{m+1}{2}$ which give an almost maximal nonquadratic weight distribution. So we can say that even if the elements giving the maximal quadratic weight distribution are necessarily of degree at most $\frac{m+1}{2}$, the converse does not hold. But our numerical results make us think that the maximal elements of degree at most $\frac{m-1}{2}$ always give the quadratic weight distribution.

Concerning the notion of “orphan cosets,” all the almost maximal cosets we checked are orphans, and we can construct from Theorem 2 cosets of $R(1,m)$ with “these” weight distributions for all odd $m > 7$.

VII. CRYPTOGRAPHIC APPLICATIONS

Let us consider a stream cipher. The running-key, which will be added to the plaintext is given by a pseudorandom generator, generally based on Linear Feedback Shift Registers (LFSR’s) which are combined, or filtered by a Boolean function $f$. In order to
resist cryptanalysis, $f$ must satisfy some criteria; first, it must be balanced—this means that its weight must be $2^{m-1}$ (where $m$ is the number of variables); moreover, if $f$ is combining the outputs of the LFSR's, it must also have a high degree (in order to resist Berlekamp–Massey's attack [21], [22]), have a high order of correlation immunity (in order to resist Siegenthaler's attack [23]), and be highly nonlinear (in order to resist fast correlation attacks [24], [25]).

Let us recall that a Boolean function $f$ of $m$ variables is $t$th order correlation-immune if, for any subset $T \subseteq \{1, 2, \ldots, m\}$ of size $t$, the probability distribution of its output is unaltered when the $x_i$ are fixed, for $i \in T$. Moreover a balanced $t$th-order correlation-immune function is said to be $t$-resilient.

In general, the balanced functions we obtained with the best known nonlinearity are not correlation-immune, and it is actually very difficult to find a balanced function which has a high order of correlation immunity and a high nonlinearity.
In 1991, P. Camion, C. Carlet, P. Charpin, and N. Sendrier have presented in [26] a construction of \( t \)-resilient functions: let \( f \) be a \( t \)-resilient function of \( m \) variables, and \( g \) the function of \( m + 1 \) variables defined by (the ANF’s are expressed in the canonical basis)

\[
g(z_1, \ldots , z_{m}, z_{m+1}) = f(z_1, \ldots , z_m) + z_{m+1}.
\]

Then \( g \) is \((t + 1)\)-resilient.

We will apply it to our balanced highly nonlinear functions in order to construct balanced highly nonlinear functions with a good order of correlation immunity.

**Theorem 3:** The degree and nonlinearity of \( g \) can be deduced from the ones of \( f \) by

\[
\deg(g) = \deg(f), \quad \text{wt}(g + R(1, m + 1)) = 2\text{wt}(f + R(1, m)).
\]

Then if we use a \( 0 \)-correlation-immune balanced function of \( m \) variables with nonlinearity \( nl \), we obtain by iterating \( t \) times this construction a \( t \)-resilient function of \( m + t \) variables with nonlinearity \( 2^{2nl} \).

For \( m = 7 \) we obtained 700 balanced functions of degree 6, and 51,744 balanced functions of degree 5, all with the best nonlinearity, that is 56. So by applying the construction twice, we obtain 700 (resp., 51,744) \( 2 \)-resilient functions of nine variables with degree 6 (resp., 5) and nonlinearity \( 2^{2} + 56 = 224 \). Notice that those of degree 6 satisfy the best possible tradeoff between the resilience order and the degree, according to the inequality given by Siegenthaler in [23]: if \( t \neq m - 1 \), then \( \deg(f) + t \leq m - 1 \).

Here we obtained balanced Boolean functions with the best known nonlinearity for \( m = 5, 6, 7, 8, 9, 11, 13, 15 \), and this construction can be applied to get balanced functions with a high nonlinearity and a sufficient order of correlation immunity to resist Siegenthaler’s attack [27].

VIII. CONCLUSION

We have presented a new approach to the study of the weight distributions of cosets of the first-order Reed–Muller code \( R(1, m) \), looking at the cosets generated by idempotents. We thus obtained new maximal-weight distributions of cosets of \( R(1, 7) \), and new almost maximal-weight distributions of cosets of \( R(1, 9) \), that is, with minimal weight \( 2^{2m-1} - 2^{m-1} = 240 \). The diversity of these weight distributions incline us to conclude that cosets generated by idempotents give a good overview of the general corpus of cosets; and so it could be conjectured that the covering radius of \( R(1, 9) \) is 240. Moreover, these results lead to cryptographic applications, in the context of stream ciphers.

ACKNOWLEDGMENT

We are very grateful to P. Charpin and C. Carlet for their motivating discussions and N. Sendrier for valuable improvements concerning the implementation. We wish to thank H. F. Mattson and E. F. Assmus for their enriching discussions and valuable suggestions.

REFERENCES