Minimal codewords in Reed-Muller codes

J. Schillewaert, L. Storme and J.A. Thas

January 13, 2009

Abstract

Minimal codewords were introduced by Massey [8] for cryptographical purposes. They are used in particular secret sharing schemes, to model the access structures. We study minimal codewords of weight smaller than $3 \cdot 2^{m-r}$ in binary Reed-Muller codes $\mathbf{RM}(r, m)$ and translate our problem into a geometrical one, using a classification result of Kasami, Tokura, and Azumi [5, 6] on Boolean functions. In this geometrical setting, we calculate numbers of non-minimal codewords. So we obtain the number of minimal codewords in the cases where we have information about the weight distribution of the code $\mathbf{RM}(r, m)$.

The presented results improve previous results obtained theoretically by Borissov, Manev, and Nikova [3], and computer aided results of Borissov and Manev [2].

This paper is in fact an extended abstract. Full proofs can be found on the arXiv.

1 Introduction

First we give some definitions and theorems required for a good statement of the problem. We will associate geometrical objects to the codewords. This will allow us to translate the problem into an equivalent geometrical problem.

Definition 1.1 *For any m and r, $0 \leq r \leq m$,* the binary r-th order Reed-Muller code $\mathbf{RM}(r, m)$ *is defined to be the set of all binary vectors f of length $n = 2^m$ associated with Boolean polynomials $f(x_1, x_2, ..., x_m)$ of degree at most r.*

Definition 1.2 *If $f(x_1, ..., x_m)$ is a Boolean function, then $T(f)$ is the collection of vectors $X = (x_1, ..., x_m)$ such that $f(X) = 1$.*

Definition 1.3 *The* support *of a codeword $c \in \mathbf{RM}(r, m)$, denoted by $supp(c)$, is the set of positions in which the non-zero digits appear.*

Definition 1.4 *Let C be a q-ary linear code. A non-zero codeword $c \in C$ is called* minimal *if its leftmost non-zero component is a 1 and if it has a support that does not contain the support of any other non-zero codeword with leftmost component 1 as a proper subset. The support of a minimal codeword $c \in C$ is called* minimal *with respect to C.*

The following properties can be found in [1]; we will use the second one later on.

Lemma 1.5 *Let C be a binary linear $[n, k, d]$-code.*

(i) *Every support of a codeword of weight $\leq 2d-1$ is minimal with respect to C.*

(ii) *The codeword c is a non-minimal codeword in C if and only if there is a pair of non-zero codewords c_1, c_2, with disjoint supports contained in the support of c, such that $c = c_1 + c_2$.*

(iii) *If c is a minimal codeword in C, then $wt(c) \leq n - k + 1$.*

So a naturally arising question is what happens for weights in between the above bounds. The smallest non-trivial case is $wt(c) = 2d$. This was solved by Borissov, Manev, and Nikova for $\mathbf{RM}(r, m)$ [3], by interpreting the non-minimal codewords of weight $2d$ geometrically as a union of two disjoint affine spaces $\mathbf{AG}(m-r, 2)$. To state their result, we first introduce some notations.

Definition 1.6 *The quantity known as* q-ary Gaussian coefficient *is defined by:* $\begin{bmatrix} m \\ i \end{bmatrix} = \prod_{j=0}^{i-1} \frac{q^m - q^j}{q^i - q^j}$, $\begin{bmatrix} m \\ 0 \end{bmatrix} = 1$, *for* $i = 1, 2, \ldots, m$.

Furthermore, we use the following notations:

$$A_{r,m} = 2^{r-1} \begin{bmatrix} m \\ m-r+1 \end{bmatrix}.$$

$$B_{r,m} = \frac{2^{r+1}-4}{4} \begin{pmatrix} 2^{r+1} \\ 3 \end{pmatrix} \begin{bmatrix} m \\ m-r-1 \end{bmatrix}.$$

$$S_{r,m} = (2^{m-r+1}-1)A_{r,m} + 3B_{r,m}.$$

$$P_{r,m} = 2^{r-1} \begin{bmatrix} m \\ m-r \end{bmatrix} (2^r \begin{bmatrix} m \\ m-r \end{bmatrix} - \sum_{k=\max\{0,m-2r\}}^{m-r} 2^{(m-r-k)(m-r-k+1)} \begin{bmatrix} m-r \\ k \end{bmatrix} \begin{bmatrix} r \\ m-r-k \end{bmatrix}).$$

Now we can state their main theorem.

Theorem 1.7 *The number of non-minimal codewords of weight $2d = 2^{m-r+1}$ in $RM(r, m)$ is $A_{r,m} + B_{r,m} + P_{r,m} - S_{r,m}$.*

We translate the problem for larger values $wt(c)$ into a geometrical one, making use of the following result of Kasami, Tokura, and Azumi [5, 6].

Theorem 1.8 *Let $f(x_1, ..., x_m)$ be a Boolean function of degree at most r, where $r \geq 2$, such that $|T(f)| < 2^{m-r+1}$. Then f can be transformed by an affine transformation into either*

$$f = x_1 \cdots x_{r-2}(x_{r-1}x_r + \cdots + x_{r+2\mu-3}x_{r+2\mu-2}),\ 2 \leq 2\mu \leq m-r+2,\ \textit{or}$$

$$f = x_1 \cdots x_{r-\mu}(x_{r-\mu+1} \cdots x_r + x_{r+1} \cdots x_{r+\mu}),\ 3 \leq \mu \leq r, \mu \leq m-r.$$

We call codewords of the forms above *codewords of first and second type* respectively. It is not hard to determine the weight of these codewords. As is well-known, the smallest weight vectors in $\mathbf{RM}(r,m)$ are the ones of weight 2^{m-r} which can be interpreted as the incidence vectors of $(m-r)$-dimensional affine spaces, see [7].

We need the following lemma which can be found in [7].

Lemma 1.9 *The number of values $(x_1,...,x_{2h})$ for which*

$$\sum_{i=1}^{h} x_{2i-1}x_{2i} = 0$$

is equal to $2^{2h-1}+2^{h-1}$.

From this it is easy to deduce the following.

Lemma 1.10 *The weight of codewords of first type is equal to*

$$2^{m-r-2\mu+2}(2^{2\mu-1}-2^{\mu-1}) = 2^{m-r-\mu+1}(2^{\mu}-1).$$

The weight of codewords of second type is equal to

$$2^{m-\mu-r+1}(2^{\mu}-1).$$

These weight functions are both increasing in μ, so the smallest weights are found for the smallest values of μ.

The second smallest weight of the code $\mathbf{RM}(r,m)$ is $3\cdot\frac{2^{m-r}}{2}$. We will count the number of non-minimal codewords $c=c_1+c_2$ of weight smaller than $3\cdot 2^{m-r}$. This implies that either c_1 or c_2 can be interpreted as an affine $(m-r)$-dimensional space.

We can regard vectors $(x_1,...,x_m)$ as points of the affine space $\mathbf{AG}(m,2)$. So by adding an extra variable X_0, we can consider the problem in the projective space $\mathbf{PG}(m,2)$; this means we set $x_i=\frac{X_i}{X_0}$ and hence we are working in a projective space where $X_0=0$ denotes the space at infinity. For $\mu=1$, the set $T(f)$ of a codeword of first type is defined by the equations

$$X_1 = X_0, \ldots, \ X_0 = X_r,$$

so represents an $(m-r)$-dimensional space. So let $\mu>1$. The first object then can be considered as the incidence vector of the geometrical object defined by the following equations:

$$X_1 = X_0, \ ..., \ X_{r-2} = X_0, \ X_0^2 = X_{r-1}X_r + \cdots + X_{r+2\mu-3}X_{r+2\mu-2}.$$

The first $r-2$ equations all describe hyperplanes, so their intersection is a $\mathbf{PG}(m-r+2,2)$. The remaining equation is the standard equation of a non-singular parabolic quadric in 2μ dimensions. If we look at the intersection with infinity, we get

$$X_0 = 0,$$

$$X_{r-1}X_r + \cdots + X_{r+2\mu-3}X_{r+2\mu-2} = 0.$$

This is the standard equation of a non-singular hyperbolic quadric in $2\mu-1$ dimensions. Furthermore we see that the coordinates $X_{r+2\mu-1}, \ldots, X_m$ can be chosen freely, so in the $\mathbf{PG}(m-r+2,2)$ defined by $X_1 = X_0, \ldots, X_{r-2} = X_0$, this codeword defines a cone Ψ with as vertex a $\mathbf{PG}(m-r+1-2\mu,2)$ at infinity, and base a non-singular parabolic quadric $Q(2\mu,2)$ in 2μ dimensions having a non-singular hyperbolic quadric at infinity. We must also keep in mind that the codeword defines the affine part of this cone Ψ.

The object of second type is easily seen to define all affine points lying inside the union of two $(m-r)$-dimensional affine spaces α and β, but not in the $(m-r-\mu)$-dimensional affine intersection space $\alpha \cap \beta$; we will call this kind of object a *symmetric difference*.

A codeword c of $\mathbf{RM}(r,m)$ is non-minimal if and only if $c = c_1 + c_2$, where c_1 and c_2 are non-zero codewords having disjoint supports. Since we are interested in counting the number of non-minimal codewords of weight less than $3 \cdot 2^{m-r}$, we take c_1 to be a non-zero codeword of smallest weight, namely 2^{m-r}, and c_2 to be a codeword of first or second type with small μ. We don't take weight 2^{m-r} for both codewords since this case has already been solved by Borissov, Manev, and Nikova [3]; their result is stated here in Theorem 1.7. So a non-minimal codeword corresponds to a pair (c_1, c_2) of geometric objects having no affine intersection points, where c_1 is an $(m-r)$-dimensional space, and where c_2 is a quadric or a symmetric difference. Call such a pair a *skew pair*. This geometrical problem of counting the number of skew pairs will be solved more generally over $\mathbf{GF}(q)$ than over $\mathbf{GF}(2)$.

2 Counting the number of objects

In this section, we first determine how many basic objects of each type, namely quadrics and symmetric differences, there are. From now on, we work more generally over $\mathbf{GF}(q)$ instead of over $\mathbf{GF}(2)$. Hence, we will no longer use the term codeword, since only for $q = 2$ do the geometric objects correspond to codewords.

However, we will still use sentences like "the projective space defined by c_1", and such sentences will be used to indicate that we are talking about the generalization over $\mathbf{GF}(q)$ of the geometric object over $\mathbf{GF}(2)$ that corresponds to the codeword c_1.

Denote the number of m-dimensional spaces $\mathbf{PG}(m,q)$ lying inside an n-dimensional space $\mathbf{PG}(n,q)$ by $\phi(m;n,q)$, the number of non-singular hyperbolic quadrics $Q^+(2\mu-1,q)$ inside a $(2\mu-1)$-dimensional space $\mathbf{PG}(2\mu-1,q)$ by $O(Q^+(2\mu-1,q))$, and the number of non-singular parabolic quadrics $Q(2\mu,q)$ inside a 2μ-dimensional space $\mathbf{PG}(2\mu,q)$ by $O(Q(2\mu,q))$.

These numbers can be found in [4].

If we denote

$$\frac{q^{r-2}\phi(m-r+1;m-1,q)\phi(m-r+1-2\mu;m-r+1,q)}{\phi(2\mu-1;2\mu,q)}$$

by F_h, then we get for the number F of cones Ψ with as vertex a $\mathbf{PG}(m-r+1-2\mu,q)$

at infinity, and base a non-singular parabolic quadric $Q(2\mu, q)$ in 2μ dimensions having a non-singular hyperbolic quadric at infinity the following.

$$F = F_h|O(Q(2\mu, q))||Q^+(2\mu - 1, q) \text{ on a given } Q(2\mu, q)|$$

Since for $q = 2$, the weight distribution for the codewords of $\mathbf{RM}(r, m)$ of weight less than $2.5d = \frac{5}{2}2^{m-r}$ is known [6], we also have the number S of symmetric difference objects in this case, but not for general q.

However, it is not hard to calculate this number S in general. The number of choices for the first affine space forming the symmetric difference is

$$F_1(m, r, \mu, q) = \frac{q^m(q^m - 1)(q^m - q)\cdots(q^m - q^{m-r-\mu-1})}{q^{m-r-\mu}(q^{m-r-\mu} - 1)(q^{m-r-\mu} - q)\cdots(q^{m-r-\mu} - q^{m-r-\mu-1})}.$$

The number of choices for the second affine space forming the symmetric difference is then

$$F_2(m, r, \mu, q) = \frac{(q^m - q^{m-r})(q^m - q^{m-r+1})\cdots(q^m - q^{(m-r)+(\mu-1)})}{(q^{m-r} - q^{m-r-\mu})(q^{m-r} - q^{m-r-\mu+1})\cdots(q^{m-r} - q^{m-r-1})}.$$

Hence, we get

$$S = \frac{\phi(r-1; \mu - 1 + r, q)F_1(m, r, \mu, q)F_2(m, r, \mu, q)}{2}.$$

for the number of symmetric differences defined by two affine $(m - r)$-dimensional spaces α and β having an $(m - r - \mu)$-dimensional intersection.

Next, we will count the number of skew pairs (c_1, c_2), c_1 an affine $(m-r)$-dimensional space in $\mathbf{AG}(m, q)$ and c_2 a cone or a symmetric difference as counted for the determination of F and S.

2.1 The second codeword c_2 is a quadric Ψ

Suppose that we have fixed a quadric Ψ in $\mathbf{AG}(m, q)$, where Ψ is a cone having an $(m - r - 2\mu + 1)$-dimensional vertex Γ at infinity and having as base B a non-singular parabolic quadric $Q(2\mu, q)$, and that we wish to determine how many $(m-r)$-dimensional affine spaces $\mathbf{AG}(m - r, q)$ are skew to the affine part of the quadric Ψ.

Let Π be the $(m - r + 2)$-dimensional projective space containing the quadric Ψ and let α be the projective completion of the $(m - r)$-dimensional affine space corresponding to the codeword c_1 of smallest weight. The intersection of Π with the space at infinity is denoted by Π_∞. We describe the different situations in $\mathbf{AG}(m, q)$ which occur if we want to count the pairs (Ψ, α) having no affine points in common, where Ψ is the quadric and where α is a projective space $\mathbf{PG}(m - r, q)$ not lying at infinity. Note that in the case $q = 2$, the affine part of α defines the codeword c_1 and the affine part of Ψ defines the codeword c_2.

Case (1) The spaces α and Π have no affine points in common. So α certainly does not have affine points in common with Ψ.

Denote the number of c-dimensional projective spaces lying inside an a-dimensional projective space Π_a that are skew to a given b-dimensional projective space of Π_a by $Skew(a, b, c)$.

Lemma 2.1 *The number $Skew(a, b, c)$ is equal to*

$$\prod_{k=-1}^{c-1} \frac{q^{a-k} - q^{b+1}}{q^{k+2} - 1}.$$

Hence, in this case, we get

Lemma 2.2 *The number P of $\mathbf{AG}(m-r, q)$ skew to a given space $\mathbf{AG}(m-r+2, q)$ in $\mathbf{AG}(m, q)$ is equal to*

$$P = \sum_{x=-1}^{m-r-1} \phi(x; m-r+1, q)T(x),$$

where

$$T(x) = Skew(m-x-1, m-r+1-x, m-r-x-1) - Skew(m-x-2, m-r-x, m-r-x-1).$$

Case (2) The spaces α and Π intersect in an l-dimensional space Π_l, $l \geq 0$, not lying completely in Π_∞. If $l = 0$, we count how many $(m-r)$-dimensional affine spaces have a projective completion that intersects Π exactly in an affine point not lying on Ψ. If $l > 0$, we will start from a given intersection at infinity.

The following lemma severely restricts the number of possibilities for this intersection with Π_∞.

Lemma 2.3 *Let α be an $(m-r)$-dimensional affine space in $\mathbf{AG}(m, q)$ having a non-empty intersection with the $(m-r+2)$-dimensional affine space Π containing the quadric Ψ. Assume that $\alpha \cap \Pi$ is skew to Ψ, then $\alpha \cap \Pi_\infty$ is either contained in $\Psi \cap \Pi_\infty$ or $\alpha \cap \Pi_\infty \cap \Psi$ is a hyperplane of $\alpha \cap \Pi_\infty$.*

Terminology. *For the rest of the paper, we refer to these two cases as the cases "hyperplane" and "hyperplane in the hyperplane".*

Call an $(s+k+1)$-dimensional space Π_{s+k+1} at infinity, lying on Ψ and intersecting the vertex Γ of Ψ in an s-dimensional space and the base $Q^+(2\mu-1, q)$ of $\Pi_\infty \cap \Psi$ in a k-dimensional space, a *starting configuration* from now on.

Case (2.a) The "hyperplane case".

We count in how many ways we can extend a starting configuration to an affine space Π_{s+k+2} lying in $\Pi = \mathbf{PG}(m-r+2, q)$ and skew to the affine part of Ψ, and intersecting Π_∞ in this given starting configuration Π_{s+k+1}.

Lemma 2.4 *Through an $(s+k+1)$-dimensional space Π_{s+k+1} at infinity, completely lying on Ψ, that intersects the vertex Γ in an s-dimensional space Π_s, there pass*

$$H(s,k) = \frac{q^{m-r+2-2\mu}(q^{2\mu-2k-2} - q^{2\mu-2k-3} + q^{\mu-k-2})}{q^{s+1}}$$

affine $(s+k+2)$-dimensional spaces of Π skew to the affine part of the quadric Ψ.

Case (2.b) The case "hyperplane in the hyperplane".

We count in how many ways we can extend a starting configuration to an affine space Π_{s+k+3} lying in $\Pi = \mathbf{PG}(m-r+2,q)$ and skew to the affine part of Ψ, and intersecting Π_∞ in an $(s+k+2)$-dimensional space only sharing Π_{s+k+1} with Ψ.

Lemma 2.5 *Through an $(s+k+1)$-dimensional space Π_{s+k+1} at infinity, lying completely on Ψ, that intersects the vertex Γ of Ψ in an s-dimensional space Π_s, there are in Π*

$$HIH(s,k) = \frac{q^{2m-2r-3\mu-2s-k}(q^{\mu-k-1}-1)((q-1)q^{2\mu-2k-4} + q^{\mu-k-2})}{2}$$

affine $(s+k+3)$-dimensional spaces Π_{s+k+3} skew to the affine part of the quadric Ψ, and intersecting Π_∞ in an $(s+k+2)$-dimensional space only intersecting Ψ in Π_{s+k+1}.

We now determine how many starting configurations there are. In the lemma below, the following notation is used:

$$[r,s]_+ = (q^r+1)(q^{r+1}+1)\cdots(q^s+1) \text{ if } s \geq r,$$

$$[r,s]_- = (q^r-1)(q^{r+1}-1)\cdots(q^s-1) \text{ if } s \geq r.$$

If $s < r$, then $[r,s]_+ = [r,s]_- = 1$.

Lemma 2.6 *The number of $(s+k+1)$-dimensional spaces Π_{s+k+1} at infinity lying on the quadric $\Gamma Q^+(2\mu-1,q)$ and intersecting the vertex Γ in some s-dimensional space Π_s is equal to*

$$S(s,k) = \phi(s;v,q)q^{(k+1)(v-s)}\frac{[\mu-1-k,\mu-1]_+[\mu-k,\mu]_-}{[1,k+1]_-}, \text{ with } v = m-r-2\mu+1.$$

The remaining problem consists of determining the number of ways the extended starting configurations $\Pi_{x'}$, $x' \geq 0$, $x' = s+k+2$ or $x' = s+k+3$, can be extended to $(m-r)$-dimensional affine spaces in the space $\mathbf{AG}(m,q)$, that intersect the affine part $\mathbf{AG}(m-r+2,q)$ of Π exactly in the space $\Pi_{x'}$, and determining the number of spaces $\mathbf{AG}(m-r,q)$ that are affinely completely skew to the $\mathbf{AG}(m-r+2,q)$. The number of ways to extend $\Pi_{x'}$ to an $(m-r)$-dimensional space intersecting $\mathbf{AG}(m-r+2,q)$ in $\Pi_{x'}$ is

$$Ext_Q(x') = \frac{(q^m - q^{m-r+2})\cdots(q^m - q^{(m-r+2)+m-r-x'-1})}{(q^{m-r}-q^{x'})\cdots(q^{m-r}-q^{m-r-1})}.$$

Since we have determined for all dimensions x how many affine spaces $\mathbf{AG}(m-r,q)$ intersect $\mathbf{AG}(m-r+2,q)$ in a given x-dimensional affine space, $x \geq 0$, and since we know the number of $\mathbf{AG}(m-r,q)$ skew to $\mathbf{AG}(m-r+2,q)$, the number of affine $(m-r)$-dimensional subspaces of $\mathbf{AG}(m,q)$ skew to the affine part of Ψ can be counted.

Theorem 2.7 *The number of affine $(m-r)$-dimensional subspaces of* $\mathbf{AG}(m,q)$ *skew to the affine part of a given cone $\Psi = \Gamma Q(2\mu, q)$, where Γ is the $(m-r-2\mu+1)$-dimensional vertex at infinity of Ψ, is equal to*

$$A_1 = P + \sum_{(s,k)\in R(s,k)} S(s,k)(H(s,k)Ext_Q(s+k+2) + HIH(s,k)Ext_Q(s+k+3)),$$

where

$$R(s,k) = \{(s,k)| -1 \leq s \leq m-r+1-2\mu,\ -1 \leq k \leq \mu-1\},$$

and where P is defined in Lemma 2.2.

Proof First of all, by Lemma 2.2, we have P distinct $(m-r)$-dimensional affine spaces that have no affine points in common with $\Pi = AG(m-r+2,q)$. By Lemma 2.6, the number of $(s+k+1)$-dimensional spaces at infinity Π_{s+k+1} lying on the quadric $\Gamma Q^+(2\mu-1,q)$ and intersecting the vertex Γ in some s-dimensional space Π_s is equal to $S(s,k)$. We recall Lemma 2.4. Through an $(s+k+1)$-dimensional space Π_{s+k+1} at infinity that intersects the vertex Γ in an s-dimensional space Π_s, and supposing that we are in the case hyperplane, there pass $H(s,k)$ affine $(s+k+2)$-dimensional spaces in Π skew to the affine part of the quadric Ψ. Another case is treated in Lemma 2.5. Through an $(s+k+1)$-dimensional space Π_{s+k+1} at infinity that intersects the vertex Γ in an s-dimensional space Π_s, and supposing that we are in the case hyperplane in the hyperplane, there are $HIH(s,k)$ affine $(s+k+3)$-dimensional affine spaces in Π skew to the affine part of the quadric Ψ.

So suppose that we already have such an $(s+k+2)$- or $(s+k+3)$-dimensional affine space Π_x in Π. A given space Π_x, $x \geq 0$, can be extended to $(m-r)$-dimensional affine spaces in the space $AG(m,q)$, that intersect the affine part $AG(m-r+2,q)$ of Π exactly in the space Π_x, in $Ext_Q(x)$ ways. □

2.2 The second codeword c_2 is a symmetric difference

We are going to count the number of $(m-r)$-dimensional affine spaces $AG(m-r,q)$ having no affine points in common with a fixed symmetric difference. We repeat that a symmetric difference is equal to $(\alpha \cup \beta) \setminus (\alpha \cap \beta)$, with α and β two affine $(m-r)$-dimensional spaces, intersecting in an $(m-r-\mu)$-dimensional affine space, where $3 \leq \mu \leq r, \mu \leq m-r$ (Theorem 1.8).

We look at the projective completion Π_{m-r} of such an $(m-r)$-dimensional affine space. Denote the $(m-r)$-dimensional projective spaces forming the symmetric difference by α and β.

Since Π_{m-r} is allowed to contain affine points lying in $\alpha \cap \beta$, we have to distinguish between two cases.

Case (1) The $(m-r)$-dimensional space Π_{m-r} has affine points in common with $\alpha \cap \beta$.

Suppose that Π_{m-r} has a k-dimensional projective intersection space Π_k, $\Pi_k \not\subset \Pi_\infty$, in common with $\alpha \cap \beta$, which is a space of dimension $m-r-\mu$. There are

$$N(k) = \frac{q^{m-r-\mu}(q^{m-r-\mu}-1)\cdots(q^{m-r-\mu}-q^{k-1})}{q^k(q^k-1)\cdots(q^k-q^{k-1})}$$

choices for such a space Π_k.

Suppose that we have fixed such a k-dimensional intersection space Π_k. We are going to extend it to an $(m-r)$-dimensional affine space without adding any point of $\alpha \cup \beta$ to it. We do this inductively on the dimension and we work in the projective space $\mathbf{PG}(m,q)$. Such an $(m-r)$-dimensional space has a t-dimensional intersection space with the space generated by α and β, further denoted by $\langle \alpha, \beta \rangle$. Here we explain the method of projection and induction. At other places we just mention the results.

We start from a given k-dimensional intersection space Π_k and we first construct the t-dimensional intersection spaces $\Pi_{k,t}$ with $\langle \alpha, \beta \rangle$ that intersect $\alpha \cup \beta$ exactly in $\Pi_k \subset \alpha \cap \beta$. Suppose that we have already constructed all a-dimensional affine spaces in $\langle \alpha, \beta \rangle$ through Π_k that have exactly Π_k in common with $\alpha \cup \beta$. Let γ be an a-dimensional space through Π_k, having only Π_k in common with $\alpha \cup \beta$. We project from γ onto a complementary space of γ in the m-dimensional projective space $\mathbf{PG}(m,q)$; this complementary space γ^* has dimension $m-a-1$. Denote the projections on γ^* of α, β, and $\langle \alpha, \beta \rangle$ from γ by α^*, β^*, and $\langle \alpha, \beta \rangle^*$ respectively. These spaces have dimension $m-r-k-1$, $m-r-k-1$, and $m-r+\mu-a-1$ respectively, and $\alpha^* \cap \beta^*$ has dimension $m-r-\mu-2k+a-1$. So in order to have an extension of γ to an $(a+1)$-dimensional space lying in $\langle \alpha, \beta \rangle$, such that the intersection space with $\alpha \cup \beta$ remains Π_k, we must choose points in $\langle \alpha, \beta \rangle^*$, but outside of $\alpha^* \cup \beta^*$. In this way, we get

$$Q(a,k) = \frac{q^{m-r+\mu-a}-1}{q-1} - 2\frac{q^{m-r-k}-1}{q-1} + \frac{q^{m-r-\mu-2k+a}-1}{q-1}$$

choices for an extension of this a-dimensional space γ to an $(a+1)$-dimensional space in $\langle \alpha, \beta \rangle$, intersecting $\alpha \cup \beta$ in Π_k.

Denote the number of a-dimensional affine spaces in $\langle \alpha, \beta \rangle$ that intersect $\alpha \cup \beta$ exactly in $\Pi_k \subset \alpha \cap \beta$ by $\psi(a,k)$. Then we have $\psi(k,k) = 1$, namely the k-dimensional space Π_k itself. This yields the induction formula

$$\psi(a+1,k) = \frac{Q(a,k)\psi(a,k)}{\phi(0;a-k,q)}.$$

The number of t-dimensional affine spaces lying in $\langle \alpha, \beta \rangle$ that intersect $\alpha \cup \beta$ exactly in a given affine space Π_k of dimension k contained in $\alpha \cap \beta$ is thus equal to $\psi(t,k)$, and the number of t-dimensional affine spaces that intersect $\alpha \cup \beta$ exactly in some k-dimensional space lying in $\alpha \cap \beta$, but not in Π_∞, is equal to $N(k)\psi(t,k)$.

Next we are going to count in how many ways we can extend a given t-dimensional space Π_t lying in $\langle \alpha, \beta \rangle$, which intersects $\alpha \cup \beta$ in a given k-dimensional affine space Π_k lying in $\alpha \cap \beta$, with Π_k not lying completely in Π_∞, to an $(m-r)$-dimensional affine space without changing the intersection with $\langle \alpha, \beta \rangle$. Let

$$R(a,k,t) = \frac{q^{m-a}-1}{q-1} - \frac{q^{m-r+\mu-t}-1}{q-1}.$$

Denote the number of a-dimensional affine spaces γ that intersect $\langle \alpha, \beta \rangle$ exactly in Π_t, and $\alpha \cap \beta$ exactly in a k-dimensional space, $k \geq 0$, not lying at infinity, by $\rho(a,k,t)$. Then we have $\rho(t,k,t) = 1$, namely the t-dimensional space Π_t itself. We get the

following induction formula

$$\rho(a+1,k,t) = \frac{R(a,k,t)\rho(a,k,t)}{\phi(0;a-t,q)}.$$

The number of $(m-r)$-dimensional affine spaces intersecting $\langle \alpha, \beta \rangle$ in a given t-dimensional affine space Π_t, where $\Pi_t \cap \alpha \cap \beta = \Pi_k$, $k \geq 0$, is thus equal to $\rho(m-r,k,t)$.

In order to find the total number of such $(m-r)$-dimensional spaces, we must sum over all possible dimensions k and t, which yields the following theorem.

Theorem 2.8 *The number of $(m-r)$-dimensional affine spaces in $\mathbf{AG}(m,q)$ having no affine points in common with a fixed symmetric difference formed by two affine $(m-r)$-dimensional spaces α and β, but having at least one affine intersection point with the $(m-r-\mu)$-dimensional space $\alpha \cap \beta$, is equal to*

$$\sum_{k=0}^{m-r-\mu} \sum_{t=k}^{m-r} N(k)\psi(t,k)\rho(m-r,k,t).$$

Case (2) Now suppose that all intersection points of Π_{m-r} and $\alpha \cup \beta$ lie at infinity.

We start from such an intersection at infinity. Denote the intersections of α and β with the space at infinity by α_∞ and β_∞ respectively. These are $(m-r-1)$-dimensional spaces intersecting in an $(m-r-\mu-1)$-dimensional space.

Suppose that the affine space Π_{m-r} intersects α_∞ in a k-dimensional space Π_k, β_∞ in an l-dimensional space Π_l, and $\alpha_\infty \cap \beta_\infty$ in an u-dimensional space Π_u. If these intersection spaces are given, we call this a (k,l,u)-*starting configuration*. We denote the number of a-dimensional spaces contained in Π_∞, and intersecting α_∞, β_∞, $\alpha_\infty \cap \beta_\infty$, and $\langle \alpha_\infty, \beta_\infty \rangle$ in a k-dimensional, l-dimensional, u-dimensional, and f-dimensional space, respectively, by $\psi(a,k,l,u,f)$.

The number $S(k,l,u)$ of (k,l,u)-starting configurations is equal to

$$\psi(k+l-u,k,l,u,k+l-u) = \phi(u;m-r-\mu-1,q)E_1(k,u)E_1(l,u),$$

where

$$E_1(x,y) = \prod_{a=u}^{x-1} \frac{(q^{m-r-a-1} - q^{m-r-\mu-y-1})}{q^{a-y+1}-1}.$$

So suppose that we now have a certain (k,l,u)-starting configuration and we look at the $(k+l-u)$-dimensional space Π_{k+l-u} generated by the spaces of this configuration. Denote the $(m-1)$-dimensional space at infinity of $\mathbf{AG}(m,q)$ by $\tilde{\Pi}_\infty$. Similarly to the previous case, we will inductively Π_{k+l-u} in $\tilde{\Pi}_\infty$ to larger spaces without changing the intersection spaces with α and β. We will do this in two steps: first we extend this space to an f-dimensional space Π_f lying completely in $\langle \alpha_\infty, \beta_\infty \rangle$, then we extend Π_f to an $(m-r-1)$-dimensional space in $\tilde{\Pi}_\infty$ without changing the intersection space Π_f with $\langle \alpha_\infty, \beta_\infty \rangle$.

Denote by $\lambda(k,l,u,s)$ the number of s-dimensional spaces lying completely in $\langle \alpha_\infty, \beta_\infty \rangle$ which intersect α_∞, β_∞, and $\alpha_\infty \cap \beta_\infty$ in a given k-, l-, and u-dimensional

space respectively. We can calculate $\lambda(k,l,u,s)$ by induction, with $\lambda(k,l,u,k+l-u) = 1$, and we find

$$\lambda(k,l,u,s+1) = \frac{\lambda(k,l,u,s)Ext_S(k,l,u,s)}{\phi(0;s-(k+l-u),q)},$$

where

$$Ext_S(k,l,u,s) = \frac{q^{m-r+\mu-s-1}-1}{q-1} - \frac{q^{m-r-k-1}-1}{q-1} - \frac{q^{m-r-l-1}-1}{q-1} + \frac{q^{m-r-k-l-\mu+s-1}-1}{q-1}.$$

We call an f-dimensional space constructed in this way a (k,l,u,f)-*space*. For each (k,l,u,f)-space Π_f we want to extend Π_f without changing the intersection with $\langle \alpha_\infty, \beta_\infty \rangle$. At infinity each Π_f can be extended to an $(m-r-1)$-dimensional space Π_{m-r-1} intersecting $\langle \alpha_\infty, \beta_\infty \rangle$ in Π_f in $\psi(m-r-1,k,l,u,f)$ ways. Since $\lambda(k,l,u,f)$ is the number of (k,l,u,f)-spaces we have as starting formula $\psi(f,k,l,u,f) = \lambda(k,l,u,f)$. The induction formula is

$$\psi(a+1,k,l,u,f) = \frac{\psi(a,k,l,u,f)Q(a,k,l,u,f)}{\phi(a-f-1;a-f,q)}.$$

where

$$Q(a,k,l,u,f) = \frac{q^{m-1-a}-1}{q-1} - \frac{q^{m-r+\mu-f-1}-1}{q-1}.$$

Suppose that we have an $(m-r-1)$-dimensional space Δ lying at infinity, which is the extension of a (k,l,u,f)-space. We still have to extend Δ to an $(m-r)$-dimensional space, not lying at infinity. This yields the following number of extensions:

$$E(k,l,u,f) = q^r - q^{m-r-1-k} - q^{m-r-1-l} + q^{m-r-k-l-\mu+f-1}.$$

The total number of affine $(m-r)$-dimensional spaces intersecting a given symmetric difference only at infinity is found by summing over all possible (k,l,u)-starting configurations and the corresponding (k,l,u,f)-spaces. We collect the restrictions on k, l, u, and f by introducing the following set:

$$Res(k,l,u,f) = \{(k,l,u,f) | -1 \leq k,\ l \leq m-r-1;\ -1 \leq u \leq m-r-\mu-1;$$

$$\max(k-\mu, l-\mu, -1) \leq u \leq k,l;\ k+l-u \leq f \leq m-r-1\}.$$

With the above introduced notations, we get the following theorem.

Theorem 2.9 *The number of $(m-r)$-dimensional affine spaces having no affine points in common with fixed $(m-r)$-dimensional affine spaces α and β, which intersect in an affine $(m-r-\mu)$-dimensional space and together form a symmetric difference is equal to*

$$\sum_{(k,l,u,f) \in Res(k,l,u,f)} S(k,l,u)\psi(m-r-1,k,l,u,f)E(k,l,u,f).$$

Proof We have $S(k,l,u)$ possibilities to obtain a (k,l,u)-starting configuration Π_{k+l-u}. We have $\lambda(k,l,u,f)$ ways to extend a given (k,l,u)-starting configuration to an f-dimensional space Π_f contained in $\langle \alpha_\infty, \beta_\infty \rangle$ which intersects $\alpha_\infty \cup \beta_\infty$ in the given (k,l,u)-starting configuration. A given space Π_f can be extended at infinity to an $(m-r-1)$-dimensional space Π_{m-r-1} intersecting $\langle \alpha_\infty, \beta_\infty \rangle$ in Π_f in $\psi(m-r-1,k,l,u,f)$ ways. A given space Π_{m-r-1} can be extended to an affine space Π_{m-r} having no affine points in common with $\alpha \cup \beta$ in $E(k,l,u,f)$ ways. □

The previous two theorems together yield the following theorem.

Theorem 2.10 *The number A_2 of $(m-r)$-dimensional affine spaces having no affine points in common with a fixed symmetric difference, formed by two $(m-r)$-dimensional affine spaces α and β which intersect in an affine $(m-r-\mu)$-dimensional space, is equal to*

$$\sum_{k=0}^{m-r-\mu} \sum_{t=k}^{m-r} N(k)\psi(t,k)\rho(m-r,k,t) + \sum_{(k,l,u,f)\in Res(k,l,u,f)} S(k,l,u)\psi(m-r-1,k,l,u,f)E(k,l,u,f).$$

3 Interchange

We want to obtain the number of minimal codewords in the coding-theoretical setting corresponding with the case $q = 2$. In the geometrical translation of the problem, we count the number of non-minimal codewords; geometrically they correspond to two geometrical objects of $\mathbf{AG}(m,q)$ which have no affine points in common. The non-minimal codeword then corresponds to the union of the affine point sets of the two objects. It might happen however that a given affine point set corresponding to a non-minimal codeword can be split in several ways into two disjoint affine point sets forming the correct geometrical objects. Then we have counted these objects more than once. With a slight abuse of terminology we will say that the pair (c_1, c_2) is counted several times. In which cases this happens, is investigated in this section.

3.1 Interchange with the symmetric difference

Suppose that $c_1 \cup c_2 = c_3 \cup c_4$ considered as affine point sets, where c_1 and c_3 are two $(m-r)$-dimensional affine spaces and where c_2 is a symmetric difference, formed by two $(m-r)$-dimensional spaces α and β.

Our arguments show that in case of an interchange $c_1 + c_2 = c_3 + c_4$, there is never a swap from a sum $c_1 + c_2$ consisting of an $(m-r)$-dimensional space $c_1 = \mathbf{AG}(m-r,q)$ and a symmetric difference c_2, to a sum $c_3 + c_4$ consisting of an $(m-r)$-dimensional space $c_3 = \mathbf{AG}(m-r,q)$ and a quadric c_4.

The intersections $c_1 \cap c_3$ and $c_2 \cap c_3$ are investigated. First it is shown that $c_1 \neq c_3$ and that $c_1 \cap c_3$ cannot be empty. If $c_1 \cap c_3$ is a t-dimensional space,$0 \leq t < m-r$, then we get,

$$|c_2 \cap c_3| = q^{m-r} - q^t.$$

Next, we consider the intersections of c_3 with α, β, and $\alpha \cap \beta$. Then $|c_2 \cap c_3|$ can also be expressed in terms of the dimensions of these intersections. Up to a few exceptions, this always yields a contradiction.

We obtain the following theorem.

Theorem 3.1 *Let S be the number of symmetric differences counted in Section 2. There are*

$$A_3 = \sum_{t=m-r-\mu}^{m-r} \psi(t, m-r-\mu)\rho(m-r, m-r-\mu, t)S$$

pairs (c_1, c_2), where c_1 is an affine $(m-r)$-dimensional space and where c_2 is a symmetric difference, which are counted three times.

Furthermore, if $q = 2$, there are an extra

$$A_4 = 2 \cdot (2^\mu - 1)((2^\mu - 1)(2^r - 2^\mu) + (2^\mu - 1)(2^r - 2^{\mu-1} - 1) + (2^{r+1} - 2^{\mu+1})(2^r - 2^\mu - 1))S$$

pairs (c_1, c_2), where c_1 is an affine $(m-r)$-dimensional space and where c_2 is a symmetric difference, which are counted three times.

Finally, if $q = 2$, there are an extra

$$A_5 = 2 \cdot (2^r - 2^\mu)A$$

pairs (c_1, c_2), where c_1 is an affine $(m-r)$-dimensional space and where c_2 is a symmetric difference, which are counted $2 \cdot (2^\mu - 1) + 1$ times.

3.2 Interchange with quadrics

Suppose that $c_1 \cup c_2 = c_3 \cup c_4$ as affine point sets, where c_1 and c_3 are $(m-r)$-dimensional affine spaces and where c_2 is a quadratic cone. Recall that $c_1 \cap c_2 = \emptyset$ and $c_3 \cap c_4 = \emptyset$, if they are considered as affine point sets. From the previous section, it follows that if this interchange effectively occurs, then also c_4 is a quadric.

First it is shown that $c_1 \cap c_3$ cannot be empty and that $c_1 \neq c_3$. Hence, we may suppose that $|c_1 \cap c_3| = q^t$, with $0 \leq t < m-r$ and $|c_2 \cap c_3| = q^{m-r} - q^t$.

Suppose that c_3 intersects the projective completion Π of the $(m-r+2)$-dimensional affine space spanned by the cone $c_2 = \Gamma Q(2\mu, q)$ in an l-dimensional space Π_l. Furthermore, suppose that c_3 shares a k-dimensional space Π_k with the vertex Γ of the cone $c_2 = \Gamma Q(2\mu, q)$. Consider a space complementary to the space Π_k in Π_l; this is an $(l-k-1)$-dimensional space Π_{l-k-1} chosen in such a way that $c_2 \cap \Pi_{l-k-1}$ is maximal. Suppose that c_3 intersects $c_2 \cap \Pi_{l-k-1}$ in z affine points. This means that $|c_2 \cap c_3| = zq^{k+1}$. Take a space Π_b complementary to the vertex space of c_2 in Π and containing Π_{l-k-1}. We will call this space the *base space*.

Comparing the two equations above for the number of affine intersection points of c_2 and c_3, and rewriting them, yields the following equation,

$$q^{m-r-t} = 1 + zq^{k+1-t}.$$

An extended case-by-case analysis yields severe restrictions on the number of possibilities, described in the following theorem.

Theorem 3.2 *If $\mu > 2$, then an interchange with a quadric Ψ is impossible. For $\mu = 2$, an interchange can only occur if the vertex of Ψ is contained in c_3. If interchange is possible for $\mu = 2$, we have $q = 2, t = m-r-2, z = 3$, or $q = 3, t = m-r-1, z = 6$, or $q = 2,\ t = m-r-1,\ z = 2$.*

The remaining cases are treated below.

(a) First, the case $q = 2$. The base of Ψ is a non-singular parabolic quadric $Q(4, 2)$ and the vertex Γ is of dimension $k = m - r - 3$. First we show that if we have a given quadric c_2, then in order to have an interchange, c_1 always has to contain Γ. The rest depends on the number of affine points of c_1 contained in Π_b.

Once we have determined in which cases there is an actual interchange and how many times we have counted the same affine point set $c_1 \cup c_2$ in these cases, the only thing left to do is to count how many times these cases effectively occur. This yields the following theorem concerning pairs (c_1, c_2) which are counted several times, where c_2 is a quadric $\Gamma Q(4, 2)$ with Γ an $(m-r-3)$-dimensional space at infinity and $Q(4, 2)$ a 4-dimensional parabolic quadric not lying completely at infinity and with c_1 an affine $(m - r)$-dimensional space.

Theorem 3.3 *Denote the number of quadrics c_2, where c_2 is a quadric $\Gamma Q(4, 2)$, with Γ an $(m - r - 3)$-dimensional space at infinity, which we calculated in Section 2, by the same notation F. Let c_1 be an affine $(m - r)$-dimensional space skew to c_2. Then there are*

$$A_6 = (15 \cdot 2^6(2^{r-2} - 1)(2^{r-3} - 1) + 10 \cdot \frac{2^8(2^{r-2} - 1)(2^{r-3} - 1)}{3})F$$

pairs (c_1, c_2) which are counted 3 times. The following number of pairs (c_1, c_2) are counted 7 times

$$A_7 = (35 \cdot (2^r - 2^2) + 45 \cdot 2^3 \cdot (2^{r-2} - 1))F.$$

Finally, $A_8 = 15F$ pairs (c_1, c_2) are counted 15 times.

(b) Next, the case $q = 3$.

In this case of possible interchange of Theorem 3.2, the base of the quadric Ψ is a non-singular parabolic quadric $Q(4, 3)$ and the vertex Γ at infinity has dimension $k = m-r-3$. In the case $q = 3$, we cannot apply Theorem 1.8 directly, so we still have to check that the affine point set formed by the affine points belonging to $(c_1 \cup c_2)\backslash c_3$ forms a singular quadric c_4 with base a parabolic quadric $Q'(4, 3)$. This turns out to be the case.

Theorem 3.4 *Denote the number of quadrics c_2, where c_2 is a quadric $\Gamma Q(4, 2)$, with Γ an $(m - r - 3)$-dimensional space at infinity, which we calculated in Section 2, by the same notation F. Let c_1 be an affine $(m - r)$-dimensional space skew to c_2. Then the number of distinct unions $c_1 \cup c_2$ for the case $q = 3, \mu = 2$, is equal to*

$$F \cdot (A_1 - 8).$$

This completes the proof of the main theorem stated below. We impose $\mu \geq 2$, since the case $\mu = 1$ reduces to the results of Borissov, Manev, and Nikova.

Theorem 3.5 (Main Theorem) *The number of affine point sets formed by two disjoint affine point sets c_1 and c_2, where c_1 is the point set of an $(m-r)$-dimensional affine space and where c_2 is the point set of either a quadric $\Gamma Q(2\mu, q)$, $4 \leq 2\mu \leq m-r+2$, with an $(m-r-2\mu+1)$-dimensional vertex Γ at infinity, or a symmetric difference defined by two affine $(m-r)$-dimensional spaces intersecting in an affine $(m-r-\mu)$-dimensional space, $3 \leq \mu \leq r$, $\mu \leq m-r$, is equal to A_1F if $q > 3$, $\mu = 2$.*

This number is equal to $A_1F + A_2S - A_3 + \frac{A_3}{3}$ if $q > 2$, $\mu > 2$.

If $q = 2, \mu > 2$, we get

$$A_1F + A_2S - (A_3 + A_4 + A_5) + \frac{A_3}{3} + \frac{A_4}{3} + \frac{A_5}{2(2^\mu - 1) + 1},$$

such sets. If $q = 2, \mu = 2$, there are

$$(A_1F + A_2S - \sum_{i=3}^{8} A_i) + \frac{A_3}{3} + \frac{A_4}{3} + \frac{A_5}{2(2^\mu - 1) + 1} + \frac{A_6}{3} + \frac{A_7}{7} + \frac{A_8}{15}.$$

such sets. Finally, if $q = 3, \mu = 2$, we obtain

$$(A_1 - 8)F,$$

such sets.

Acknowledgement This research takes place within the project "Linear codes and cryptography" of the Fund for Scientific Research Flanders (FWO-Vlaanderen) (Project nr. G.0317.06), and is supported by the Interuniversitary Attraction Poles Programme-Belgian State-Belgian Science Policy: project P6/26-BCrypt.

Address of the authors:

Mathematics and Statistics Department, University of Canterbury, Private Bag 4800, Christchurch 8140, New-Zealand
J. Schillewaert: Jeroen.Schillewaert@canterbury.ac.nz

Ghent University, Dept. of Pure Mathematics and Computer Algebra, Krijgslaan 281-S22, 9000 Ghent, Belgium
L. Storme: ls@cage.ugent.be, `http://cage.ugent.be/~ls`
J.A. Thas: jat@cage.ugent.be, `http://cage.ugent.be/~jat`

References

[1] A. Ashikhmin and A. Barg. Minimal vectors in linear codes. *IEEE Trans. Inform. Theory*, 44(5):2010–2017, 1998.

[2] Y. Borissov and N. Manev. Minimal codewords in linear codes. *Serdica Math. J.*, 30(2-3):303–324, 2004.

[3] Y. Borissov, N. Manev, and S. Nikova. On the non-minimal codewords in binary Reed-Muller codes. *Discrete Appl. Math.*, 128(1):65–74, 2003. International Workshop on Coding and Cryptography (WCC 2001) (Paris).

[4] J. W. P. Hirschfeld. *Projective geometries over finite fields.* Oxford University Press, New York, 1998.

[5] T. Kasami and N. Tokura. On the weight structure of Reed-Muller codes. *IEEE Trans. Information Theory*, IT-16:752–759, 1970.

[6] T. Kasami, N. Tokura, and S. Azumi. On the weight enumeration of weights less than 2.5d of Reed-Muller codes. *Information and Control*, 30(4):380–395, 1976.

[7] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. I+II.* North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[8] J. L. Massey. Minimal codewords and secret sharing. *Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory*, pages 276–279, 1993.