Des. Codes Cryptogr. (2014) 73:271–297
DOI 10.1007/s10623-013-9911-7

On low weight codewords of generalized affine and projective Reed–Muller codes

Stéphane Ballet · Robert Rolland

Received: 22 April 2013 / Revised: 30 November 2013 / Accepted: 16 December 2013 /
Published online: 18 January 2014

Abstract We propose new results on low weight codewords of affine and projective generalized Reed–Muller (GRM) codes. In the affine case we prove that if the cardinality of the ground field is large compared to the degree of the code, the low weight codewords are products of affine functions. Then, without this assumption on the cardinality of the field, we study codewords associated to an irreducible but not absolutely irreducible polynomial, and prove that they cannot be second, third or fourth weight depending on the hypothesis. In the projective case the second distance of GRM codes is estimated, namely a lower bound and an upper bound on this weight are given.

Keywords Code · Codeword · Finite field · Generalized Reed–Muller code · Homogeneous polynomial · Hyperplane · Hypersurface · Minimal distance · Next-to-minimal distance · Polynomial · Projective Reed–Muller code · Second weight · Weight

Mathematics Subject Classification 94B27 · 94B65 · 11G25 · 11T71

1 Introduction: notations

1.1 General overview

This article proposes a study on low weight codewords of generalized Reed–Muller (GRM) codes and projective GRM (PGRM) codes of degree d, defined over a finite field $\mathbb{F}_q$, called

This is one of several papers published in *Designs, Codes and Cryptography* comprising the "Special Issue on Coding and Cryptography".

S. Ballet · R. Rolland (✉)
Aix-Marseille University, ERISCS and IML case 930, 13288Marseille Cedex 9, France
e-mail: robert.rolland@acrypta.fr

S. Ballet
e-mail: stephane.ballet@univ-amu.fr

respectively GRM codes and PGRM codes. It includes a focus on their minimum distances as well as the characterization of the codewords reaching these weights. It also includes a study of the second weight, namely the weight which is just above the minimal distance. The second weight is also called the next-to-minimum weight.

Generalized Reed–Muller codes (also known as GRM codes) are evaluation codes obtained from spaces of polynomials in several variables. More precisely, let d be a fixed positive integer, if f is a polynomial function in n variables of degree $\leq d$, the components of the codeword $c(f)$ associated to f are obtained by evaluating the polynomial function f on all the points of $\mathbb{F}_q^n$:

$$c(f) = (f(\mathbf{x}))_{\mathbf{x}\in\mathbb{F}_q^n}.$$

Then, the weight $W_{aff}(f)$ of a codeword $c(f)$ is related to the number of zeros of its associated polynomial, namely the cardinality $\#Z_{aff}(f)$ of the hypersurface $Z_{aff}(f)$ defined by this polynomial, by the following formula:

$$W_{aff}(f) = q^n - \#Z_{aff}(f).$$

Consequently, the study of low weight codewords leads to the study of hypersurfaces with many points. Such a geometric interpretation can be also given in the projective case, for generalized projective Reed–Muller codes (also known as PGRM codes).

Determining the low weights of the Reed–Muller codes as well as the low weight codewords are interesting questions related to various fields. Of course, from the point of view of coding theory, knowing something on the weight distribution of a code, and especially on the low weights is valuable information. From the point of view of algebraic geometry the problem is also related to the computation of the number of rational points of hypersurfaces and in particular hypersurfaces that are arrangements of hyperplanes. By means of incidence matrices, Reed–Muller codes are related to finite geometry codes (see [1, Sects. 5.3, 5.4]). From this point of view, codewords have a geometrical interpretation and can benefit from the numerous results in this area. Consequently there is a wide variety of concepts that may be involved.

We address in the following several questions related to the values of the low weights and to the classes of polynomials reaching these values, or equivalently, to the hypersurfaces with these cardinalities.

Concerning the values of the low weights, the minimal weight is known for the affine case, namely the GRM codes (cf. [11]) and for the projective case, namely the PGRM codes (cf. [30,32]). The next-to-minimal weight is known for GRM codes (partial results can be found in [6,9,10,26,27] and a complete solution in [5]), but it is unknown for PGRM codes except for some special cases (cf. [23,24]). We give a lower bound and an upper bound on this quantity.

Concerning the hypersurfaces related to the codewords of minimum weight we know that they are hyperplane arrangements (cf. [7] for the GRM codes and [25,30] for the PGRM codes). Is it true for the next-to minimal weight? A positive answer is given in [17] for GRM codes and the answer is unknown for PGRM codes except for some special cases (cf. [23,24]). What happens for the codewords which are not products of degree one polynomials? In order to address the problems surrounding this question it is convenient to introduce the three following sets of polynomials classified according to the methods used to study their numbers of zeros:

(1) the class of polynomials which are products of degree one factors; we remark that when we are looking for polynomials of degree $\leq d$ having a lot of distinct zeros, we can require that the degree be exactly d and that the polynomial be without multiple factors,

(2) the class of polynomials which are irreducible but not absolutely irreducible,
(3) the class of absolutely irreducible polynomials.

We study separately the number of zeros of the polynomials of each class, and we compare these numbers for different relative values of d and q.

We give for GRM codes an explicit lower bound on the distance from codewords which are defined by irreducible but not absolutely irreducible polynomials to the next-to-minimal codewords. We study (GRM case), for different relative values of d and q, the codewords which are associated to polynomials which are products of degree one factors (the associated hypersurfaces are hyperplane arrangements). We prove that, when q is greater than a certain value q_0 depending on the degree d, all the weights of the codewords defined by polynomials of degree d which are products of degree one polynomials without multiple factors (the associated hypersurface is an arrangement of d distinct hyperplanes) are lower than the weights of the codewords defined by polynomials which are not products of degree one factors. A similar result was proved in [23] for PGRM codes. We compare for certain relative values of q and d the weights of the codewords associated to polynomials which have an irreducible but not absolutely factor to the four first lower weights of the code.

1.2 Organization of the article

Many results concerning this area are here and there in various articles. In this situation, a comprehensive overview is needed. This is what we do first in Sect. 2.

Section 3 is an overview on the minimal distance both in the affine case as in the projective case. Concerning PGRM codes, the second author characterized in [25] the codewords of minimal weights. But the proof given there is only sketched briefly. We give in this Section a more detailed proof.

In Sect. 4 we study the second weight of GRM codes.

- In Sect. 4.1 we recall some results concerning the second weight and the codewords of a GRM code reaching the second weight. These codewords are now known. They were determined in [9,27] for $1 \leq d \leq \frac{q}{2}$ and in [17] for the general case. It should be noted that these codewords correspond, as do the minimal codewords, to products of affine functions (by an affine function we mean a sum of a constant and a homogeneous linear function, both defined over $\mathbb{F}_q$). Next we give new results on affine low weight codewords and we split the study into the three following parts.
- In Sect. 4.2 we give new results on low weight codewords in the case where q is large compared to d. We prove that any codeword associated to a configuration of d distinct hyperplanes has a weight that is lower than the weight of a codeword associated to a polynomial divisible by an irreducible (absolutely or not) component of degree ≥ 2.
- In Sect. 4.3 we study the general case and we compare the second, third an fourth weights to the weight of a word which is associated to an irreducible but not absolutely irreducible polynomial.
- In Sect. 4.4 we study the important case where $d < q$ and we prove that under some hypotheses, a word which is associated to a polynomial having a factor irreducible but not absolutely irreducible has a weight greater than the third or fourth weight, depending on the hypothesis.

In Sect. 5 we determine an upper bound and a lower bound for the second weight of a PGRM code.

2 Basics

2.1 Polynomials and homogeneous polynomials

Let $\mathbb{F}_q$ be the finite field with q elements and $n \geq 1$ an integer. We denote respectively by $\mathbb{A}^n(q)$ and $\mathbb{P}^n(q)$ the affine space and the projective space of dimension n over $\mathbb{F}_q$.

Let $\mathbb{F}_q[X_1, X_2, \ldots, X_n]$ be the algebra of polynomials in n variables over $\mathbb{F}_q$. If f is in $\mathbb{F}_q[X_1, X_2, \ldots, X_n]$ we denote by $\deg(f)$ its total degree and by $\deg_{X_i}(f)$ its partial degree with respect to the variable X_i.

Denote by $\mathscr{F}(q, n)$ the space of functions from $\mathbb{F}_q^n$ into $\mathbb{F}_q$. It is known that any function in $\mathscr{F}(q, n)$ is a polynomial function. More precisely there is a surjective linear map T from $\mathbb{F}_q[X_1, X_2, \ldots, X_n]$ onto $\mathscr{F}(q, n)$ mapping any polynomial to its associated polynomial function:

$$\begin{array}{ccc} T : \mathbb{F}_q[X_1, X_2, \ldots, X_n] & \to & \mathscr{F}(q, n), \\ f & \mapsto & T(f), \end{array}$$

where $T(f)(\mathbf{x}) = f(\mathbf{x})$ is the evaluation of the polynomial function f at the point $\mathbf{x} = (x_1, x_2, \ldots, x_n)$. The map T is not injective and has for kernel the ideal generated by the n polynomials $X_i^q - X_i$:

$$\mathrm{Ker}(T) = \left\langle X_1^q - X_1, X_2^q - X_2, \ldots, X_n^q - X_n \right\rangle.$$

Any element of the quotient $\mathbb{F}_q[X_1, X_2, \ldots, X_n]/\mathrm{Ker}(T)$ can be represented by a unique reduced polynomial f, namely such that for any variable X_i the following holds:

$$\deg_{X_i}(f) \leq q - 1.$$

We denote by $\mathscr{R}P(q, n)$ the set of reduced polynomials in n variables over $\mathbb{F}_q$. Then, the map T restricted to $\mathscr{R}P(q, n)$ is one to one, namely each function of $\mathscr{F}(q, n)$ can be uniquely represented by a reduced polynomial in $\mathscr{R}P(q, n)$.

Let d be a positive integer. We denote by $\mathscr{R}P(q, n, d)$ the set of reduced polynomials P such that $\deg(P) \leq d$. We remark that if $d \geq n(q-1)$ the set $\mathscr{R}P(q, n, d)$ is the whole set $\mathscr{R}P(q, n)$.

Let $\mathscr{H}(q, n+1, d)$ be the space of homogeneous polynomials in $n+1$ variables over $\mathbb{F}_q$ with total degree d. The decomposition

$$\mathbb{F}_q[X_0, X_1, X_2, \ldots, X_n] = \bigoplus_{d \geq 0} \mathscr{H}(q, n+1, d),$$

provides $\mathbb{F}_q[X_0, X_1, X_2, \ldots, X_n]$ with a graded algebra structure. Let $\mathscr{J}_d$ be the subspace of polynomials f in $\mathscr{H}(q, n+1, d)$ such that $f(\mathbf{x}) = 0$ for any $\mathbf{x} \in \mathbb{F}_q^{n+1}$ and denote by J the homogeneous ideal

$$\mathscr{J} = \bigoplus_{d \geq 0} \mathscr{J}_d.$$

It is known (cf. [21,22]) that the ideal $\mathscr{J}$ is the homogeneous ideal generated by the polynomials $X_i^q X_j - X_i X_j^q$ where $0 \leq i < j \leq n$.

2.2 GRM codes

Let d be an integer such that $1 \leq d < n(q-1)$. The GRM code of order d over $\mathbb{F}_q$ is the following subspace of $\mathbb{F}_q^{(q^n)}$:

$$\mathrm{GRM}_q(d, n) = \left\{ (f(\mathbf{x}))_{\mathbf{x}\in\mathbb{F}_q^n} | f \in \mathbb{F}_q[X_1, \ldots, X_n] \text{ and } \deg(f) \leq d \right\}.$$

It may be remarked that the polynomials f determining this code are viewed as polynomial functions. Hence each codeword is associated with a unique reduced polynomial in $\mathscr{R}P(q, n, d)$.

Remark 1 If $d \geq n(q-1)$, the space of functions given by the polynomials of $\mathscr{R}P(q, n, d)$ is the whole space of functions, hence yielding the trivial code. This is the reason for defining $\mathrm{GRM}_q(d, n)$ for $d < n(q-1)$.

Let us denote by $Z_{aff}(f)$ the set of zeros of f (where the index *aff* stands for "affine"). From a geometrical point of view $Z_{aff}(f)$ is an affine algebraic hypersurface in $\mathbb{F}_q^n$ and the number of points $\#Z_{aff}(f)$ of this hypersurface (the number of zeros of f) is connected to the weight $W_{aff}(f)$ of the associated codeword by the following formula:

$$W_{aff}(f) = q^n - \#Z_{aff}(f).$$

The code $\mathrm{GRM}_q(d, n)$ has the following parameters (cf. [2, p. 72], [11]) (where the index *aff* stands for "affine code"):

(1) length $m_{aff}(q, n, d) = q^n$,
(2) dimension

$$k_{aff}(q, n, d) = \sum_{t=0}^{d} \sum_{j=0}^{n} (-1)^j \binom{n}{j} \binom{t - jq + n - 1}{t - jq},$$

(3) minimum distance $W_{aff}^{(1)}(q, n, d) = (q-b)q^{n-a-1}$, where a and b are the quotient and the remainder in the Euclidean division of d by $q-1$, namely $d = a(q-1) + b$ and $0 \leq b < q-1$.

Remark 2 The code $\mathrm{GRM}_q(d, 1)$ is a MDS code.

Remark 3 Be careful not to confuse symbols. With our notations, the length of the Reed–Muller code of order d is $m_{aff}(q, n, d)$, its dimension is $k_{aff}(q, n, d)$ and its minimum distance is $W_{aff}^{(1)}(q, n, d)$. Namely it is an

$$\left[m_{aff}(q, n, d), k_{aff}(q, n, d), W_{aff}^{(1)}(q, n, d) \right]\text{-code.}$$

The integer n is the number of variables of the polynomials defining the words and the order d is the maximum total degree of these polynomials.

Remark 4 If $d < q-1$ then $a = 0$ and $b = d$. Hence

$$W_{aff}^{(1)}(q, n, d) = (q-d)q^{n-1}.$$

The minimum distance of $\mathrm{GRM}_q(d, n)$ was given by Kasami et al. [11]. The words reaching this bound were characterized by Delsarte et al. [7] and are described in the following theorem:

Theorem 5 (Delsarthe, Goethals, McWilliams) *The maximum number of rational points over $\mathbb{F}_q$, for an algebraic hypersurface V of degree d in the affine space of dimension n which is not the whole space $\mathbb{F}_q^n$ is attained if and only if*:

$$V = \left(\bigcup_{i=1}^{a}\left(\bigcup_{j=1}^{q-1} V_{i,j}\right)\right)\left(\bigcup_{j=1}^{b} W_j\right) \quad \text{where } d = a(q-1)+b,$$

with $0 \leq b < q-1$ and where the $V_{i,j}$ and W_j are d distinct hyperplanes defined on $\mathbb{F}_q$ such that for each fixed i the $V_{i,j}$ are $q-1$ parallel hyperplanes, the W_j are b parallel hyperplanes and the $a+1$ distinct linear forms directing these hyperplanes are linearly independent.

A simpler proof than the original one is given in [18].

2.3 PGRM codes

The case of projective codes is a bit different, because homogeneous polynomials do not define in a natural way functions on the projective space. Let d be an integer such that $1 \leq d \leq n(q-1)$. The PGRM code of order d (PGRM code) was introduced by Lachaud [13]. Let S a subset of $\mathbb{F}_q^{n+1}$ corresponding to the choice of one point on each punctured vector line of $\mathbb{F}_q^{n+1}$. Remark that any point of the projective space $\mathbb{P}^n(q)$ has a unique coordinate representation by an element of S. The projective Reed–Muller code $\mathrm{PGRM}_q(d,\ n)$ of order d over $\mathbb{P}^n(q)$ is constituted by the words $(f(\mathbf{x}))_{\mathbf{x}\in S}$ where $f \in \mathscr{H}(q,\ n+1,\ d)$:

$$\mathrm{PGRM}_q(d,\ n) = \{(f(\mathbf{x}))_{\mathbf{x}\in S} | f \in \mathscr{H}(q,\ n+1,\ d)\}.$$

This code depends on the set S chosen to represent the points of $\mathbb{P}^n(q)$. Nevertheless, different choices of S lead to equivalent codes. Then the main parameters are independent of this choice. Following [13] we can choose

$$S = \cup_{i=0}^{n} S_i,$$

where $S_i = \{(0, \ldots, 0,\ 1,\ x_{i+1}, \ldots, x_n) | x_k \in \mathbb{F}_q\}$. Subsequently, we shall adopt this value of S to define the code $\mathrm{PGRM}_q(d,\ n)$.

Remark 6 For $d > n(q-1)$, the image of $\mathscr{H}(q,\ n+1,\ d)$ fills up the whole of the ambient vector space, hence yielding the trivial code. This is the reason for defining $\mathrm{PGRM}_q(d,\ n)$ for $d \leq n(q-1)$.

For a homogeneous polynomial f let us denote by $Z_{proj}(f)$ the set of zeros of f in the projective space $\mathbb{P}^n(q)$ (where the index *proj* stands for "projective"). From a geometrical point of view, an element $f \in \mathscr{H}(q,\ n+1,\ d)$ defines a projective hypersurface $Z_{proj}(f)$ in the projective space $\mathbb{P}^n(q)$. The number $\#Z_{proj}(f)$ of points of this projective hypersurface is connected to the weight $W_{proj}(f)$ of the corresponding codeword by the following relation:

$$W_{proj}(f) = \frac{q^{n+1}-1}{q-1} - \#Z_{proj}(f).$$

The parameters of $\mathrm{PGRM}_q(d,\ n)$ are the following (cf. [32]) (where the index *proj* stands for "projective code"):

(1) length $m_{proj}(q,\ n,\ d) = \frac{q^{n+1}-1}{q-1}$,

(2) dimension,

$$k_{proj}(q,\ n,\ d) = \sum_{\substack{t = d \bmod q-1 \\ 0 < t \leq d}} \left(\sum_{j=0}^{n+1} (-1)^j \binom{n+1}{j} \times \binom{t - jq + n}{t - jq} \right),$$

(3) minimum distance: $W^{(1)}_{proj}(q,\ n,\ d) = (q-b)q^{n-a-1}$ where a and b are the quotient and the remainder in the Euclidean division of $d-1$ by $q-1$, namely $d-1 = a(q-1)+b$ and $0 \leq b < q-1$.

Remark 7 The code $\mathrm{PGRM}_q(d,\ 1)$ is a MDS code.

3 Minimal distance and corresponding codewords

3.1 The affine case: GRM codes

For the affine case recall that we write the degree d in the following form:

$$d = a(q-1) + b \quad \text{with } 0 \leq b < q-1. \tag{1}$$

The minimum distance of a GRM code was given by Kasami et al. [11]. The words reaching this bound (i.e. the polynomials reaching the maximal number of zeros) were characterized by Delsarte et al. [7]. As indicated in [7] the polynomial functions reaching this bound can be written as:

$$P(\mathbf{x}) = w_0 \prod_{i=1}^{a} \left(1 - (l_i(\mathbf{x}) - w_i)^{q-1}\right) \prod_{j=1}^{b} \left(l_{a+1}(\mathbf{x}) - w'_j\right), \tag{2}$$

where $\mathbf{x} \in \mathbb{F}_q^n$, the w'_j in the last b factors are distinct elements of $\mathbb{F}_q$, the w_i are arbitrary elements of $\mathbb{F}_q$ with $w_0 \neq 0$ and l_i are $a+1$ linearly independent linear forms on $\mathbb{F}_q^n$.

We give here the geometric interpretation of such a polynomial f reaching the maximal number of zeros. The hypersurface defined by f is the following arrangement of hyperplanes:

(1) a blocks of $q-1$ parallel hyperplanes, each of them directed by one of the a first linearly independent linear forms l_i,
(2) one block of b parallel hyperplanes directed by l_{a+1}.

Such a hypersurface will be called a maximal hypersurface and the associated polynomial is called a maximal polynomial. The corresponding weight is the minimal weight.

3.2 The projective case: PGRM codes

Let us denote respectively by $W^{(1)}_{proj}(q,\ n,\ d)$ and $W^{(2)}_{proj}(q,\ n,\ d)$ the first and second weights of the projective Reed–Muller code.

In order to describe the minimal distance in the projective case, write $d-1 = a(q-1)+b$ with $0 \leq b < q-1$. The minimum distance of a PGRM code was given by Serre for $d \leq q$ (cf. [30]), and by Sørensen [32] in the general case. The polynomials reaching the maximal number of zeros (or defining the minimum weighted codewords) are given by J.-P. Serre in the case of $d \leq q$ (cf. [30]) and by the last author (cf. [25]) in the general case. Let us give a detailed proof of the following result stated in [25].

Theorem 8 *Let f be a homogeneous polynomial in $n+1$ variables of total degree d, with coefficients in $\mathbb{F}_q$, which does not vanish on the whole projective space $\mathbb{P}^n(q)$. Then the following holds*:

(1) *The number of $\mathbb{F}_q$-rational points $\#Z_{proj}(f)$ of the projective algebraic set defined by f satisfies the following*:

$$\#Z_{proj}(f) \leq \frac{q^{n+1}-1}{q-1} - W^{(1)}_{proj}(q,\, n,\, d), \tag{3}$$

where

$$W^{(1)}_{proj}(q,\, n,\, d) = \begin{cases} 1 & \text{if } d > n(q-1), \\ (q-b)q^{n-a-1} & \text{if } d \leq n(q-1), \end{cases}$$

with

$$d-1 = a(q-1)+b \quad \text{and} \quad 0 \leq b < q-1.$$

(2) *The bound in (3) is attained. When $d \leq n(q-1)$, the polynomials f attaining this bound are exactly the polynomials defining a hypersurface $V = Z_{proj}(f)$ such that : V contains a hyperplane H (namely f vanishes on H) and V restricted to the affine space $\mathbb{A}^n(q) = \mathbb{P}^n(q) \setminus H$ is a maximal affine hypersurface of $\mathbb{A}^n(q)$.*

Proof The point (1) is proved by Sørensen [32]. However, in order to prove at the same time the point (2), let us rewrite entirely the proof given by Sørensen of the point (1) and let us show that one can deduce the result (2) from this proof.

If $d > n(q-1)$, as f does not vanish on the whole projective space $\mathbb{P}^n(q)$, then

$$\#Z_{proj}(f) \leq \frac{q^{n+1}-1}{q-1} - 1.$$

Remark 6 proves that this bound is attained.

If $d \leq n(q-1)$ and $V = Z_{proj}(f)$ contains a hyperplane H, we can suppose that this hyperplane is given by $X_0 = 0$, so that $f = x_0 f_1$, where f_1 is a homogeneous polynomial of degree $d-1$. The complement of H is the affine space

$$\mathbb{A}^n(q) = \left\{ \mathbf{x} \in \mathbb{P}^n(q) | x_0 = 1 \right\}.$$

Let $\widetilde{f}_1$ be the polynomial in n variables obtained from f_1 by setting $x_0 = 1$. This polynomial is defined on $\mathbb{A}^n(q)$ and does not vanish on the whole affine space $\mathbb{A}^n(q)$. Hence, using the result of Kasami et al. [11], we obtain:

$$\#Z_{aff}\left(\widetilde{f}_1\right) \leq q^n - (q-b)q^{n-a-1},$$

and consequently

$$\#Z_{proj}(f) = \#H + \#Z_{aff}\left(\widetilde{f}_1\right) \leq \frac{q^n-1}{q-1} + q^n - (q-b)q^{n-a-1},$$

$$\#Z_{proj}(f) \leq \frac{q^{n+1}-1}{q-1} - (q-b)q^{n-a-1},$$

where the symbol # denotes the cardinality. The bound is attained if and only if the polynomial $\widetilde{f}_1$ verifies the conditions of maximality given in [7].

If $d \leq n(q-1)$ and $V = Z_{proj}(f)$ does not contain any hyperplane, we give a proof of (3) by induction on n. If $n = 1$ and $d > q-1$ the result is a consequence of Remark 6. If $d \leq q-1$ the homogeneous polynomial f in two variables of degree d can be written as:

$$f(X_0,\ X_1) = kX_1^d + lX_0 g(X_0,\ X_1),$$

where $k \neq 0$ and $l \neq 0$ (because V does not contain any hyperplane) and where g is a nonzero homogeneous polynomial function of degree $d-1$. The point at infinity $x_0 = 0,\ x_1 = 1$ of the projective line is not a zero, the only zeros are points such that $x_0 = 1$ and x_1 is a solution of a polynomial equation in one variable of degree d. Then $\#Z_{proj}(f) \leq d$ and the induction property is verified.

Next suppose that the property is true for $n-1$ and $Z_{proj}(f)$ does not contain any hyperplane. Then for any hyperplane H we have

$$\#\left(Z_{proj}(f) \cap H\right) \leq \frac{q^n-1}{q-1} - W^{(1)}_{proj}(q,\ n-1,\ d),$$
$$\#\left(H \backslash Z_{proj}(f) \cap H\right) \geq W^{(1)}_{proj}(q,\ n-1,\ d).$$

Let us count the number $\mathcal{N}$ of couples $(M,\ H)$ where H is a hyperplane and M a point in $(\mathbb{P}^n(q) \backslash Z_{proj}(f)) \cap H$. We know that the number of hyperplanes containing a given point is $\frac{q^n-1}{q-1}$. Then

$$\mathcal{N} = \frac{q^n-1}{q-1} \#\left(\mathbb{P}^n(q) \backslash Z_{proj}(f)\right).$$

This number is also the following sum on the $\frac{q^{n+1}-1}{q-1}$ hyperplanes of the space $\mathbb{P}^n(q)$

$$\mathcal{N} = \sum_H \#\left(H \setminus Z_{proj}(f) \cap H\right) \geq \frac{q^{n+1}-1}{q-1} W^{(1)}_{proj}(q,\ n-1,\ d).$$

Then

$$W_{proj}(f) \geq \frac{q^{n+1}-1}{q^n-1} W^{(1)}_{proj}(q,\ n-1,\ d),$$
$$W_{proj}(f) > q W^{(1)}_{proj}(q,\ n-1,\ d).$$

As $d \leq n(q-1)$ we have two cases:

(1) $d \leq (n-1)(q-1)$ and then $W^{(1)}_{proj}(q,\ n-1,\ d) = (q-b)q^{n-a-2}$. Hence $q W^{(1)}_{proj}(q,\ n-1,\ d) = (q-b)q^{n-a-1} = W^{(1)}_{proj}(q,\ n,\ d)$. In this case we conclude

$$W_{proj}(f) > W^{(1)}_{proj}(q,\ n,\ d),$$

which proves that the induction property is verified and also that the bound cannot be reached by a hypersurface which does not contain any hyperplane.

(2) $(n-1)(q-1) < d \leq n(q-1)$ and in this case we have $W^{(1)}_{proj}(q,\ n-1,\ d) = 1,\ a = n-1$ and $W^{(1)}_{proj}(q,\ n,\ d) = q-b$. Then

$$W_{proj}(f) > q W^{(1)}_{proj}(q,\ n-1,\ d) = q \geq q-b,$$
$$W_{proj}(f) > W^{(1)}_{proj}(q,\ n,\ d),$$

which proves that the induction property is verified and also that the bound cannot be reached by a hypersurface which does not contain any hyperplane.
The point (2) is a consequence of the above reasoning.

□

4 Low weight codewords in the affine case

4.1 The second weight in the affine case

Let us denote by $W^{(2)}_{aff}(q, n, d)$ the second weight of the GRM code $RM_q(d, n)$, namely the weight which is just above the minimum distance. Several simple cases can be easily described. If $d = 1$, we know that the code has only three weights: 0, the minimum distance $W^{(1)}_{aff}(q, n, 1) = q^n - q^{n-1}$ and the second weight $W^{(2)}_{aff}(q, n, 1) = q^n$. For $d = 2$ and $q = 2$ the weight distribution is more or less a consequence of the investigation of quadratic forms done by Dickson [8] and was also done by E. Berlekamp and N. Sloane in an unpublished paper. For $d = 2$ and any q (including $q = 2$) the weight distribution was given by McEliece [20]. For $q = 2$, for any n and any d, the weight distribution is known in the range $[W^{(1)}_{aff}(2, n, d), 2.5W^{(1)}_{aff}(2, n, d)]$ by a result of Kasami et al. [12]. In particular, the second weight is $W^{(2)}_{aff}(2, n, d) = 3 \times 2^{n-d-1}$ if $1 < d < n - 1$ and $W^{(2)}_{aff}(2, n, d) = 2^{n-d+1}$ if $d = n - 1$ or $d = 1$. For $d \geq n(q - 1)$ the code $\mathrm{GRM}_q(d, n)$ is trivial, namely it is the whole of $\mathscr{F}(q, d, n)$, hence any integer $0 \leq t \leq q^n$ is a weight.

The general problem of the second weight was tackled by Erickson in his thesis [9, 1974] and was partly solved. Unfortunately this very good piece of work was not published and remained virtually unknown. Meanwhile several authors became interested in the problem independently of the work of D. Erickson. The second weight was first studied by Cherdieu and Rolland [6] who proved that when $q > 2$ is fixed, for $d < q$ sufficiently small the second weight is

$$W^{(2)}_{aff}(q, n, d) = q^n - dq^{n-1} + (d - 1)q^{n-2}.$$

Their result was improved by Sboui [27], who proved the formula for $d \leq q/2$. The methods in [6,27] are of a geometric nature by means of which the codewords reaching this weight were determined. These codewords are hyperplane arrangements. Then Geil [10], using Gröbner basis methods, proved the formula for $d < q$. Moreover as an application of his method, he gave a new proof of the Kasami–Lin–Peterson minimum distance formula and determined, when $d > (n - 1)(q - 1)$, the first $d + 1 - (n - 1)(q - 1)$ weights. In particular for $n = 2$ the problem is completely solved in his work, and this case is particularly important as we shall see later. Finally, the last author in [26], using a mix of Geil's method and geometrical considerations found the second weight for all cases except when $d = a(q - 1) + 1$. However the Gröbner basis method does not determine all the codewords reaching the second weight.

Recently, Bruen [5] exhumed the work of Erickson and completed the proof, solving the problem of the second weight for the GRM code. Let us describe a little more the result of Erickson. First, in order to present his result introduce the following notation used in [9]: s and t are integers such that

$$d = s(q - 1) + t, \quad \text{with} \quad 0 < t \leq q - 1.$$

Theorem 9 *The second weight* $W^{(2)}_{aff}(q,\ n,\ d)$ *is*

$$W^{(2)}_{aff}(q,\ n,\ d) = W^{(1)}_{aff}(q,\ n,\ d) + cq^{n-s-2},$$

where $W^{(1)}_{aff}(q,\ n,\ d) = (q-t)q^{n-s-1}$ *is the minimal distance and* c *is*

$$c = \begin{cases} q & \text{if } s = n-1, \\ t-1 & \text{if } s < n-1 \text{ and } 1 < t \leq \frac{q+1}{2}, \\ & \text{or } s < n-1 \text{ and } t = q-1 \neq 1, \\ q & \text{if } s = 0 \text{ and } t = 1, \\ q-1 & \text{if } q < 4,\ s < n-2 \text{ and } t = 1, \\ q-1 & \text{if } q = 3,\ s = n-2 \text{ and } t = 1, \\ q & \text{if } q = 2,\ s = n-2 \text{ and } t = 1, \\ q & \text{if } q \geq 4,\ 0 < s \leq n-2 \text{ and } t = 1, \\ c_t & \text{if } q \geq 4,\ s \leq n-2 \text{ and } \frac{q+1}{2} < t. \end{cases}$$

The number c_t *is such that* $c_t + (q-t)q$ *is the second weight for the code* $\mathrm{GRM}_q(2,\ t)$.

It follows from the previous theorem that if one could compute the second weight for a case where $c = c_t$, the problem would be completely solved. Alternatively, Erickson [9, Conjecture 4.14, p. 76]conjectured that $c_t = t - 1$ and reduced this conjecture to a conjecture on blocking sets. Recently in Bruen [3–5] proved that this conjecture follows from two of his articles. To summarize the state of the art on the problem of determining the next-to-minimal weights of the GRM codes, say that the problem is now solved by the combination of the results in [5,9]. It is also solved by combining the results of [9,10] (the important case $n = 2$ is completely solved in [10] and this leads to the conclusion as noted above) or by combining the results of [9,26] (the case not solved in [9] are explicitly resolved in [26]). More precisely the following theorem holds.

Theorem 10 *The coefficient* c_t *used in the previous Theorem 9 is*

$$c_t = t - 1.$$

Remark 11 The values s and t are connected to the values a and b of the formula (1) in the following way: $a = s$ and $b = t$ unless $t = q - 1$ and in this case $a = s + 1$ and $b = 0$. Let us also express the second weight with the writing (1) of Euclidean division (cf. [26]). Let us define γ to be such that

$$W^{(2)}_{aff}(q,\ n,\ d) = W^{(1)}_{aff}(q,\ n,\ d) + \gamma q^{n-a-2}. \tag{4}$$

The second weight is given by the following:

(I) $n = 1$ (and then $q > 2$):

$$W^{(2)}_{aff}(q,\ n,\ d) = q - d + 1; \quad \gamma = q;$$

(II) $n \geq 2$

(A) $d = 1$:

$$W^{(2)}_{aff}(q,\ n,\ d) = q^n; \quad \gamma = q;$$

(B) $d \geq 2$

(1) $q = 2$

(a) $2 \leq d < n-1$:

$$W_{aff}^{(2)}(q,\, n,\, d) = 3 \times 2^{n-d-1}; \quad \gamma = q = 2;$$

(b) $d = n-1$:

$$W_{aff}^{(2)}(q,\, n,\, d) = 4; \quad \gamma = q^2 = 4;$$

(2) $q \geq 3$

(a) $2 \leq d < q-1$:

$$W_{aff}^{(2)}(q,\, n,\, d) = q^n - dq^{n-1} + (d-1)q^{n-2}; \quad \gamma = b-1 = d-1;$$

(b) $(n-1)(q-1) < d < n(q-1)$:

$$W_{aff}^{(2)}(q,\, n,\, d) = q - b + 1; \quad \gamma = q;$$

(c) $q-1 \leq d \leq (n-1)(q-1)$

(i) $b = 0$:

$$W_{aff}^{(2)}(q,\, n,\, d) = 2q^{n-a-1}(q-1); \quad \gamma = q(q-2);$$

(ii) $b = 1$

(α) $q = 3$

$$W_{aff}^{(2)}(3,\, n,\, d) = 8 \times 3^{n-a-2}; \quad \gamma = q-1;$$

(β) $q \geq 4$:

$$W_{aff}^{(2)}(q,\, n,\, d) = q^{n-a}; \quad \gamma = q;$$

(iii) $2 \leq b < q-1$:

$$W_{aff}^{(2)}(q,\, n,\, d) = q^{n-a-2}(q-1)(q-b+1); \quad \gamma = b-1.$$

Finally let us remark that we now have several approaches to find the next-to-minimal distance, close to each other, but nevertheless different. The first one (cf. [5,9]) is mainly based on combinatorics of finite geometries, the second one (cf. [6,26,27]) is mainly based on geometry and hyperplane arrangements, the third (cf. [10,26]) is mainly based on polynomial study by means of commutative algebra and Gröbner basis. All these approaches can be fruitful for the study of similar problems, in particular for the similar codes based on incidence structures, finite geometry and incidence matrices (see [14–16,33]).

The polynomials reaching the second weight are known (cf. [9, Theorem 3.13, p. 60], [27] for $2d \leq q$ and [17] for any d).

4.2 Low weight codewords for large q

The dimension n of the ambient space and the degree d are fixed. As we make a study of low weight codewords for large values of q, we suppose first that $q > d$. Let us denote by $\mathscr{LW}(q,\, d,\, n)$ the set of words f (where f is a reduced polynomial) of the Reed–Muller code $\mathrm{GRM}_q(d,\, n)$ such that the set $Z_{aff}(f)$ of zeros of f is an union of d distinct hyperplanes.

Lemma 12 *Let f be a reduced polynomial function in $\mathscr{F}(q,\, n)$ which is in $\mathscr{LW}(q,\, d,\, n)$. Then the number $\#Z_{aff}(f)$ of zeros in $\mathbb{F}_q^n$ is such that*

$$\#Z_{aff}(f) \geq dq^{n-1} - \frac{d(d-1)}{2}q^{n-2}. \tag{5}$$

Proof The set $Z_{aff}(f)$ of zeros of f is the union of the d distinct hyperplanes H_i. Then

$$\#Z_{aff}(f) = \#Z_{aff}(f) \geq \sum_{i=1}^{d} \#H_i - \sum_{i \neq j} \#\left(H_i \cap H_j\right).$$

But

$$\sum_{i \neq j} \#\left(H_i \cap H_j\right) = \frac{d(d-1)}{2} q^{n-2}.$$

Then

$$\#Z_{aff}(f) \geq dq^{n-1} - \frac{d(d-1)}{2} q^{n-2}.$$

□

The two following lemmas are useful for the study of irreducible but not absolutely irreducible polynomial functions. The first one is a key lemma which can be found in [31].The second one is a slight modification of [25, Theorem 2.1].

Lemma 13 *Let f be a nonzero irreducible but not absolutely irreducible polynomial over the finite field $\mathbb{F}_q$, in n variables and of degree d. Then one can find a finite extension $\mathbb{F}_{q'}$ such that there exists a unique polynomial g absolutely irreducible over the finite field $\mathbb{F}_{q'}$, in n variables and of degree d', satisfying*:

$$f = \lambda \prod_{\sigma \in G} g^{\sigma},$$

where $G = Gal(\mathbb{F}_{q'}/\mathbb{F}_q)$ is the Galois group of $\mathbb{F}_{q'}$ over $\mathbb{F}_q$,

$$deg(f) = \left[\mathbb{F}_{q'} : \mathbb{F}_q\right] deg(g),$$

λ is a constant in $\mathbb{F}_q$ and the g^{σ} are conjugated.

Lemma 14 *Let $f \in \mathscr{R}P(q, n, d)$ be an irreducible but not absolutely irreducible polynomial of degree $d > 1$. Let us set a and b such that $d = a(q-1) + b$ and $0 \leq b < q-1$. Denote by u the smallest prime factor of d. Then the number $\#Z_{aff}(f)$ of zeros of f over $\mathbb{F}_q$ satisfies*:

$$\#Z_{aff}(f) < q^n - 2q^{n - \left\lfloor \frac{d}{u(q-1)} \right\rfloor - 1}. \tag{6}$$

Moreover if $a = 0$

$$\#Z_{aff}(f) < \frac{d}{u} q^{n-1}. \tag{7}$$

Proof Using the Lemma 13 we get:

$$f = \prod_{\sigma \in G} g^{\sigma}.$$

where $g \in \mathbb{F}_{q'}[X_1, \ldots, X_n]$. Let us write the polynomial g as

$$g\left(X_1, \ldots, X_n\right) = \sum_{(u_1, \ldots, u_n) \in D} c_{(u_1, \ldots, u_n)} X_1^{u_1}, \ldots, X_n^{u_n},$$

where D is a finite set of multiple indexes. Hence

$$g^{\sigma}\left(X_1,\ldots,X_n\right)=\sum_{(u_1,\ldots,u_n)\in D}\sigma\left(c_{(u_1,\ldots,u_n)}\right)X_1^{u_1},\ldots,X_n^{u_n}.$$

Let us denote by s the cardinality of the Galois group G. The number s is also the dimension $[\mathbb{F}_{q'}:\mathbb{F}_q]$ of the vector space $\mathbb{F}_{q'}$ over the field $\mathbb{F}_q$. The total degree d of f and the total degree d' of g are related by the following formula:

$$d=deg(f)=s\,deg(g)=sd'.$$

Let δ_i be the partial degree of g with respect to the variable X_i. Then the partial degree of f with respect to the variable X_i is $s\delta_i$. As f is reduced, all the partial degrees of the polynomials g are $\leq q-1$.

From the previous writing of f we get:

$$Z_{aff}(f)=\bigcup_{\sigma\in G}Z_{aff}\left(g^{\sigma}_{|\mathbb{F}_q^n}\right),$$

where $g^{\sigma}_{|\mathbb{F}_q^n}$ is the restriction to $\mathbb{F}_q^n$ of g^{σ}. However all the conjugate polynomials g^{σ} have the same zeros in $\mathbb{F}_q^n$. Hence $Z_{aff}(f)=Z_{aff}(g_{|\mathbb{F}_q^n})$.

Let $(w_1,\ldots,w_s)$ be a basis of the vector space $\mathbb{F}_{q'}$ over $\mathbb{F}_q$ and h_j the following polynomial in $\mathbb{F}_q[X_1,\ldots,X_n]$:

$$h_j\left(X_1,\ldots,X_n\right)=\sum_{(u_1,\ldots,u_n)\in D}c_{j\,(u_1,\ldots,u_n)}X_1^{u_1},\ldots,X_n^{u_n},$$

where $c_{j\,(u_1,\ldots,u_n)}\in\mathbb{F}_q$ is the component of $c_{(u_1,\ldots,u_n)}$ on w_j. Then h_j is a reduced polynomial in $\mathbb{F}_q[X_1,\ldots,X_n]$. Now we can write g as:

$$g\left(X_1,\ldots,X_n\right)=\sum_{j=1}^{s}h_j\left(X_1,\ldots,X_n\right)w_j,$$

where $h_j\in\mathscr{R}P(q,\,d',\,n)$ and are not all zero.

Hence,

$$Z_{aff}(f)=\bigcap_{j=1}^{s}Z_{aff}\left(h_j\right).$$

The nonzero h_j cannot all be equal to the same product of d' distinct (up to a constant multiplier) degree one polynomials because in this case, g would be proportional to a polynomial over $\mathbb{F}_q$. Then the h_j are such that:

(1) there is a j such that h_j is of degree $< d'$ or has a multiple factor; or
(2) all the h_j are of degree d' but there is a j such that h_j is not the product of degree one polynomials; or
(3) all the h_j are products of d' distinct degree one polynomials, but there are two indexes i and j such that at least one factor of h_i is not (up to a constant multiplier) a factor of h_j (and consequently a factor of h_j which is not a factor of h_i).

In the two first cases, there is a j such that h_j cannot have the maximum number of zeros (see Theorem 5). In the third case $Z_{aff}(h_i)\cap Z_{aff}(h_j)$ is strictly included both in $Z_{aff}(h_i)$

and $Z_{aff}(h_j)$ (a factor of h_i which is not in h_j defines a hyperplane not included in the hypersurface defined by h_j). Hence $\#(Z_{aff}(h_i) \cap Z_{aff}(h_j))$ cannot be maximum.

Taking into account that $Z_{aff}(f) = \bigcap_{j=1}^{s} Z_{aff}(h_j)$ we conclude that $\#Z_{aff}(f)$ cannot attain the maximum number of zeros for a polynomial of degree $\leq d'$ given by the formula of Kasami et al. [11]:

$$\#Z_{aff}(f) < q^n - (q - b')q^{n-a'-1}, \tag{8}$$

where $d' = a'(q-1) + b'$ and $0 \leq b' < q-1$. But a' is the integer part of $d'/(q-1)$, namely:

$$a' = \left\lfloor \frac{d'}{q-1} \right\rfloor = \left\lfloor \frac{d}{s(q-1)} \right\rfloor.$$

In any case:

$$\#Z_{aff}(f) < q^n - (q - (q-2))q^{n-\left\lfloor \frac{d}{s(q-1)} \right\rfloor - 1}.$$

As s divides d we have $u \leq s$ and consequently

$$\#Z_{aff}(f) < q^n - 2q^{n-\left\lfloor \frac{d}{u(q-1)} \right\rfloor - 1}.$$

Now, if $a = 0$ then $a' = 0$ and we can improve the previous estimate. In this case we know that $b' = d' = d/s$, so that, from (8) we get:

$$\#Z_{aff}(f) < q^n - (q - d/s)q^{n-1} = (d/s)q^{n-1}.$$

As s divides d we have $u \leq s$ and consequently the following inequality holds:

$$\#Z_{aff}(f) < \frac{d}{s}q^{n-1} \leq \frac{d}{u}q^{n-1}.$$

Let us remark that $2 \leq u$ so that if we replace u by 2, the formulas are still valid. □

Lemma 15 *Let $g \in \mathscr{F}(q, n)$ such that $\deg(g) \leq d < q-1$. Suppose that $g = g_1 g_2$ where g_1 is an irreducible but not absolutely irreducible polynomial of degree $d' \geq 2$. Then*

$$\#Z_{aff}(g) < \left(d - \frac{d'}{2}\right) q^{n-1} \leq (d-1)q^{n-1}.$$

Proof By Lemma 14 we know that

$$\#Z_{aff}\,(g_1) < \frac{d'}{2}q^{n-1}.$$

On the other hand, as g_2 is not the zero polynomial and is of degree $\leq (d - d') < q - 1$, by Remark 4 we get

$$\#Z_{aff}\,(g_2) \leq (d - d')q^{n-1}.$$

Then

$$\#Z_{aff}(g) \leq \#Z_{aff}\,(g_1) + \#Z_{aff}\,(g_2) < \left(d - d' + \frac{d'}{2}\right) q^{n-1} = \left(d - \frac{d'}{2}\right) q^{n-1}.$$

As $d' \geq 2$, we have

$$\#Z_{aff}(g) < (d-1)q^{n-1}.$$

□

Proposition 16 *Let $g \in \mathscr{F}(q, n)$ such that* $\deg(g) \leq d < q-1$. *Suppose that $g = g_1 g_2$ where g_1 is an irreducible but not absolutely irreducible polynomial of degree $d' \geq 2$. Then if $q \geq \frac{d(d-1)}{2}$, for any $f \in \mathscr{LW}(q, d, n)$, the following inequality holds*:

$$\#Z_{aff}(f) > \#Z_{aff}(g).$$

Proof We know by Lemma 12 that

$$\#Z_{aff}(f) \geq dq^{n-1} - \frac{d(d-1)}{2} q^{n-2},$$

and by Lemma 15 that

$$\#Z_{aff}(g) < (d-1)q^{n-1}.$$

Then

$$\#Z_{aff}(f) - \#Z_{aff}(g) > q^{n-1} - \frac{d(d-1)}{2} q^{n-2}.$$

Hence if

$$q \geq \frac{d(d-1)}{2},$$

we have

$$\#Z_{aff}(f) - \#Z_{aff}(g) > 0.$$

□

Lemma 17 *For any absolutely irreducible polynomial function h in $\mathscr{F}(q, n)$ of degree $\leq d$ the following inequality holds*:

$$\left|\#Z_{aff}(h) - q^{n-1}\right| \leq A(d) q^{n-\frac{3}{2}} + B(d) q^{n-2},$$

where

$$A(d) = \sqrt{2} d^{\frac{5}{2}} \quad \text{and} \quad B(d) = 4d^2 k^{2^k} \quad \text{with } k = \frac{d(d+1)}{2}.$$

Proof See [29, Theorem 5A, p. 210]. □

Lemma 18 *Let $g \in \mathscr{F}(q, n)$ such that* $\deg(g) \leq d$. *Suppose that $g = g_1 g_2$ where g_1 is an absolutely irreducible polynomial of degree $d' \geq 2$. Then*

$$\#Z_{aff}(g) \leq (d-1)q^{n-1} + A(d) q^{n-\frac{3}{2}} + B(d) q^{n-2}.$$

Proof

$$\#Z_{aff}(g) \leq \#Z_{aff}(g_1) + \#Z_{aff}(g_2).$$

Lemma 17 gives an upper bound for $\#Z_{aff}(g_1)$ and as g_2 is not zero, $\#Z_{aff}(g_2)$ is bounded by $(d-d')q^{n-1}$. Then

$$\#Z_{aff}(g) \leq (d-d')q^{n-1} + q^{n-1} + A(d') q^{n-\frac{3}{2}} + B(d') q^{n-2},$$
$$\#Z_{aff}(g) \leq (d+1-d')q^{n-1} + A(d') q^{n-\frac{3}{2}} + B(d') q^{n-2},$$

and as $d' \geq 2$ and $A(d)$, $B(d)$ are increasing functions

$$\#Z_{aff}(g) \leq (d-1)q^{n-1} + A(d) q^{n-\frac{3}{2}} + B(d) q^{n-2}.$$

□

Proposition 19 *Let $g \in \mathscr{F}(q,\ n)$ such that* $\deg(g) \leq d$. *Suppose that $g = g_1 g_2$ where g_1 is an absolutely irreducible polynomial of degree $d' \geq 2$. Then if $q > q_0(d)$, where*

$$q_0(d) = \left(\frac{A(d) + \sqrt{A(d)^2 + 4C(d)}}{2} \right)^2 \quad \textit{with} \quad C(d) = B(d) + \frac{d(d-1)}{2},$$

for any $f \in \mathscr{LW}(q,\ d,\ n)$ the following inequality holds:

$$\#Z_{aff}(f) > \#Z_{aff}(g).$$

Proof We know by Lemma 12 that

$$\#Z_{aff}(f) \geq dq^{n-1} - \frac{d(d-1)}{2} q^{n-2},$$

and by Lemma 18 that

$$\#Z_{aff}(g) \leq (d-1)q^{n-1} + A(d)q^{n-\frac{3}{2}} + B(d)q^{n-2}.$$

Then we have

$$\#Z_{aff}(f) - \#Z_{aff}(g) \geq q^{n-1} - A(d)q^{n-\frac{3}{2}} - C(d)q^{n-2},$$
$$\#Z_{aff}(f) - \#Z_{aff}(g) \geq q^{n-2}(q - A(d)\sqrt{q} - C(d)).$$

As $q - A(d)\sqrt{q} - C(d)$ is a quadratic polynomial in $\sqrt{q}$ we can conclude that if $q > q_0(d)$ then

$$\#Z_{aff}(f) - \#Z_{aff}(g) > 0.$$

□

Theorem 20 *Let $n \geq 2$ and $d \geq 2$ be integers. For any prime power $q > q_0(d)$, for any polynomial function g of degree $\leq d$ which is not the product of affine factors and for any polynomial function f of degree d which is the product of d affine factors $l_i(x) + a_i$ pairwise non-proportional the following holds*:

$$\#Z_{aff}(f) > \#Z_{aff}(g). \tag{9}$$

Proof Note that

$$\frac{d(d-1)}{2} < q_0(d).$$

Then the result is a consequence of Propositions 16 and 19. □

Remark 21 Theorem 20 can be also expressed in term of weights of codewords. If $q > q_0(d)$ then any word in $\mathscr{LW}(q,\ d,\ n)$ has a weight which is strictly lower than any word which is not a product of degree one factors.

Remark 22 Presumably, the value $q_0(d)$ must be improved. Rodier and Sboui proved a similar result by geometric techniques for PGRM codes with $q_0(d) = d(d-1)/2$ (cf. [23,28]).

Remark 23 Let us give as examples of codewords in $\mathscr{LW}(q,\ d,\ n)$ the codewords associated to hyperplane arrangements $\mathscr{L}$ defined in [26, Sect. 2] in the following way. Let $d = d_1 + d_2 + \cdots + d_k$ where

$$\begin{cases} 1 \leq d_1 \leq d_2 \cdots \leq d_k \leq q-1, \\ 1 \leq k \leq n. \end{cases} \tag{10}$$

Let us denote by $f_1, f_2, \ldots, f_k$, k linearly independent linear forms on $\mathbb{F}_q^n$ and let us consider the following hyperplane arrangement: for each f_i we have d_i distinct parallel hyperplanes defined by

$$f_i(x) = u_{i,j} \quad \text{with} \quad 1 \leq j \leq d_i,$$

where, when j varies, $u_{i,j}$ yields d_i distinct values. This arrangement of d hyperplanes consists of k blocks of parallel hyperplanes, the k directions of the blocks being linearly independent. The corresponding codeword

$$f(x) = \prod_{i=1}^{k} \prod_{j=1}^{d_i} \left(f_i(x) - u_{i,j}\right),$$

is in $\mathscr{LW}(q, d, n)$ and has the following number of zeros (see [26, Theorem 2.1]):

$$\#Z_{aff}(f) = q^n - q^{n-k} \prod_{i=1}^{k} (q - d_i).$$

From the point of view of weight distribution, there are a lot of different values $W_{aff}(f)$ for different f in this class. For example with $k = 2$, all the different pairs (d_1, d_2) with $d_1 + d_2 = d$ and $d_1 \leq d_2$ give different $W_{aff}(f)$.

4.3 Low weight codewords in the general case

From [17] all the next-to-minimal words are known. So the main interest of the following theorem is to give an estimate of the distance from codewords corresponding to the third or higher weight to the next-to-minimal ones.

Theorem 24 *If $f \in \mathscr{R}P(q, n, d)$ is an irreducible polynomial but not absolutely irreducible, in n variables over $\mathbb{F}_q$, of degree $d > 1$ then the weight $W_{aff}(f)$ of the corresponding codeword in $\mathrm{GRM}_q(d, n)$ is such that $W_{aff}(f) > W_{aff}^{(2)}(q, n, d)$.*

Remark 25 In the proof of the previous theorem we will determine a strictly positive exact lower bound for $W_{aff}(f) - W_{aff}^{(2)}(q, n, d)$ in most of the cases appearing.

Proof (of Theorem 24) By Lemma 14 the weight $W_{aff}(f)$ of the codeword associated to f is such that

$$W_{aff}(f) > 2q^{n - \left\lfloor \frac{d}{u(q-1)} \right\rfloor - 1}. \tag{11}$$

Moreover when $a = 0$ the following holds:

$$W_{aff}(f) > q^n - \frac{d}{u} q^{n-1}. \tag{12}$$

All the previous inequalities remain valid if u is replaced by a lower value in particular by 2. Thus, in general we shall apply this result with $u = 2$ unless we have more information on d and if we need a more accurate inequality. In the following we compare for each case $W_{aff}(f)$ to $W_{aff}^{(2)}(q, n, d)$ and we prove that $W_{aff}(f) > W_{aff}^{(2)}(q, n, d)$ and compute a lower bound for $W_{aff}(f) - W_{aff}^{(2)}(q, n, d)$. This lower bound will be useful later.

For $n = 1$ the result is trivial (f does not have any zeros). We suppose now that $n \geq 2$. Subsequently a_2 is defined by:

$$a_2 = \left\lfloor \frac{d}{u(q-1)} \right\rfloor,$$

with $u = 2$ unless we specify another value.

(1) The case $q = 2$.

- $2 \le d < n-1$. We know that $W^{(2)}_{aff}(q,\, n,\, d) = 3 \times 2^{n-d-1}$. As $d \ge 2$, we have $a_2 = \left\lfloor \frac{d}{2(q-1)} \right\rfloor \ge 1$. If d is even then $2a_2 = d$ and the following holds:

$$W^{(2)}_{aff}(q,\, n,\, d) = 3 \times 2^{n-2a_2-1} \le 3 \times 2^{n-a_2-2} \le \frac{3}{4} \times 2^{n-a_2} < \frac{3}{4} W_{aff}(f).$$

  If d is odd, then $a_2 = \frac{d-1}{2}$ and $d = 2a_2+1$. It follows that $W_{aff}(f) > 4 \times 2^{n-a_2-2} > 3 \times 2^{n-2a_2-2} = W^{(2)}_{aff}(q,\, n,\, d)$.
- $d = n-1$. Then $W^{(2)}_{aff}(q,\, n,\, d) = 4$. As $d \ge 2$ we conclude that $n \ge 3$ and $a_2 = \left\lfloor \frac{n-1}{2} \right\rfloor \le \frac{n-1}{2}$. Then

$$W_{aff}(f) > 2^{n-a_2} \ge 2^{\frac{n+1}{2}} \ge 4 = W^{(2)}_{aff}(q,\, n,\, d).$$

(2) The case $q \ge 3$ and $2 \le d < q$.

- $2 \le d < q-1$. Here $a = 0$. Then $W_{aff}(f) > q^n - \frac{d}{2} q^{n-1}$. On the other hand we have $W^{(2)}_{aff}(q,\, n,\, d) = q^n - dq^{n-1} + (d-1)q^{n-2}$. Then

$$W_{aff}(f) - W^{(2)}_{aff}(q,\, n,\, d) > \frac{d}{2} q^{n-1} - (d-1)q^{n-2},$$

$$W_{aff}(f) - W^{(2)}_{aff}(q, n, d) > q^{n-2} \left(\frac{qd}{2} - d + 1 \right).$$

  But $q \ge 3$ then $\frac{qd}{2} \ge \frac{3}{2} d$ and

$$W_{aff}(f) - W^{(2)}_{aff}(q,\, n,\, d) > 2q^{n-2}.$$

- $d = q-1$. In this case $W^{(2)}_{aff}(q,\, n,\, d) = 2q^{n-1} - 2q^{n-2}$ while $a_2 = \left\lfloor \frac{1}{2} \right\rfloor = 0$ and $W_{aff}(f) > 2q^{n-1}$. Hence

$$W_{aff}(f) - W^{(2)}_{aff}(q,\, n,\, d) > 2q^{n-2}.$$

(3) The case $q \ge 3$ and $(n-1)(q-1) < d < n(q-1)$.
In this case $a_2 < \frac{n}{2}$, $W^{(2)}_{aff}(q,\, n,\, d) = (q - b + 1)$. On the other hand, $W_{aff}(f) > 2q^{n-a_2-1}$.
If $n = 2$ then $a_2 = 0$ and $W_{aff}(f) > 2q > W^{(2)}_{aff}(q,\, n,\, d)$.
If $n = 3$ then $a_2 = 1$ and $W_{aff}(f) > 2q^{n-2} \ge 2q > W^{(2)}_{aff}(q,\, n,\, d)$.
If $n \ge 4$ then $W_{aff}(f) > q^{\frac{n-2}{2}} \ge 2q > W^{(2)}_{aff}(q,\, n,\, d)$.

(4) The case $q \ge 3$ and $q \le d \le (n-1)(q-1)$.

- $b = 0$. In this case $W^{(2)}_{aff}(q,\, n,\, d) = 2q^{n-a-1}(q-1)$ and $a_2 = \left\lfloor \frac{a}{2} \right\rfloor$. If a is even then $a = 2a_2 \ge 1$. Then $W^{(2)}_{aff}(q,\, n,\, d) = 2q^{n-2a_2} - 2q^{n-2a_2-1}$ and $W_{aff}(f) > 2q^{n-a_2-1}$. Hence,

$$W_{aff}(f) - W^{(2)}_{aff}(q,\, n,\, d) > 2q^{n-2a_2} \left(q^{a_2-1} - 1 \right) + 2q^{n-2a_2-1}.$$

As $q^{a_2-1}-1 \geq 0$ we conclude that

$$W_{aff}(f) - W^{(2)}_{aff}(q,\, n,\, d) > 2q^{n-a-1}.$$

If a is odd then $a = 2a_2 + 1$ and $W^{(2)}_{aff}(q,\, n,\, d) = 2q^{n-2a_2-1} - 2q^{n-2a_2-2}$ the following formulas hold:

$$W_{aff}(f) - W^{(2)}_{aff}(q,\, n,\, d) > 2q^{n-2a_2-1}\left(q^{a_2}-1\right) + 2q^{n-2a_2-2}.$$

As $q^{a_2}-1 \geq 0$ we conclude that

$$W_{aff}(f) - W^{(2)}_{aff}(q,\, n,\, d) > 2q^{n-a-1}.$$

- $b = 1$.

– $q = 3$. In this case $d = 2a+1$, and consequently the lowest prime factor of d is ≥ 3. Then we shall take $u = 3$ for this case. Hence $a_2 = \left\lfloor \frac{d}{3(q-1)} \right\rfloor = \left\lfloor \frac{d}{6} \right\rfloor < \frac{d}{6}$, namely $a_2 < \frac{a}{3} + \frac{1}{6}$. Moreover $W^{(2)}_{aff}(q,\, n,\, d) = 8 \times 3^{n-a-2}$ and $W_{aff}(f) > 2 \times 3^{n-\frac{a}{3}-\frac{1}{6}-1}$. Then

$$W_{aff}(f) - W^{(2)}_{aff}(q,\, n,\, d) > 2 \times 3^{n-a-2}\left(3^{\frac{2a}{3}+\frac{5}{6}} - 4\right),$$

and as $a \geq 1$

$$W_{aff}(f) - W^{(2)}_{aff}(q,\, n,\, d) > 2 \times 3^{n-a-2}\left(3^{\frac{3}{2}} - 4\right) > 2 \times 3^{n-a-2}.$$

– $q \geq 4$. We know that $W^{(2)}_{aff}(q,\, n,\, d) = q^{n-a}$ and $W_{aff}(f) > 2q^{n-a-1}$. If $a_2 = 0$ then

$$W_{aff}(f) - W^{(2)}_{aff}(q,\, n,\, d) > 2q^{n-1} - q^{n-a} \geq q^{n-1}.$$

If $a = 1$ then $d = q \geq 4$ and $a_2 \leq \frac{q}{2(q-1)} \leq \frac{2}{3} < 1$. Then $a_2 = 0$. Hence, if $a_2 = 1$ then $a \geq 2$. Then $W_{aff}(f) > q^{n-2}$ and $W^{(2)}_{aff}(q,\, n,\, d) \leq q^{n-2}$. We conclude that

$$W_{aff}(f) - W^{(2)}_{aff}(q,\, n,\, d) > 0.$$

If $a_2 \geq 2$, we know that $a_2 = \left\lfloor \frac{a(q-1)+1}{2(q-1)} \right\rfloor$ and then $a_2 \leq \frac{a}{2} + \frac{1}{6}$ or $a > 2a_2 - \frac{1}{3}$. Consequently $W^{(2)}_{aff}(q,\, n,\, d) < q^{n-2a_2+\frac{1}{3}}$ while $W_{aff}(f) > 2q^{n-a_2-1}$, hence

$$W_{aff}(f) - W^{(2)}_{aff}(q,\, n,\, d) > q^{n-2a_2+\frac{1}{3}}\left(2q^{a_2-\frac{4}{3}} - 1\right) > 0.$$

- $2 \leq b < q-1$. We know that $W^{(2)}_{aff}(q,\, n,\, d) = q^{n-a-2}(q-1)(q-b+1)$. From the definitions we get the two following inequalities:

$$\frac{d}{q-1} - 1 < a \leq \frac{d}{q-1},$$
$$\frac{d}{2(q-1)} - 1 < a_2 \leq \frac{d}{2(q-1)},$$

then

$$0 \leq a - 2a_2 \leq 1.$$

If a is even then $a = 2a_2 \geq 2$ and

$$W_{aff}^{(2)}(q,\, n,\, d) = q^{n-2a_2-2}(q-1)(q-b+1) < q^{n-2a_2}.$$

Hence:

$$W_{aff}(f) - W_{aff}^{(2)}(q,\, n,\, d) > 2q^{n-a_2-1} - q^{n-2a_2},$$
$$W_{aff}(f) - W_{aff}^{(2)}(q,\, n,\, d) > q^{n-2a_2}\left(2q^{a_2-1} - 1\right),$$

and as $a_2 \geq 1$ we conclude that

$$W_{aff}(f) - W_{aff}^{(2)}(q,\, n,\, d) > q^{n-2a_2} = q^{n-a}.$$

If a is odd, $a = 2a_2 + 1,\ a \geq 1,\ a_2 \geq 0$. Moreover

$$W_{aff}^{(2)}(q,\, n,\, d) = q^{n-2a_2-3}(q-1)(q-b+1) < q^{n-2a_2-1},$$

and

$$W_{aff}(f) > 2q^{n-a_2-1}.$$

Then

$$W_{aff}(f) - W_{aff}^{(2)}(q,\, n,\, d) > q^{n-2a_2-1}\left(2q^{a_2} - 1\right),$$

and as $2q^{a_2} - 1 \geq 1$ we obtain

$$W_{aff}(f) - W_{aff}^{(2)}(q,\, n,\, d) > q^{n-2a_2-1} = q^{n-a}.$$

□

From the computations done in the proof of the previous theorem and examples of hyperplane arrangements introduced in [26, Sect. 2] we can deduce the following:

Theorem 26 *Suppose that d is such that $d = a(q-1) + b$ with $1 \leq a < n-1$ and $2 \leq b < q-1$ (hence $q \geq 4$). If $f \in \mathscr{R}P(q,\, n,\, d)$ is an irreducible polynomial but not absolutely irreducible, in n variables over $\mathbb{F}_q$, of degree d then the weight $W_{aff}(f)$ of the corresponding codeword in $\mathrm{GRM}_q(d,\, n)$ is such that $W_{aff}(f) > W_{aff}^{(4)}(q,\, n,\, d)$.*

Proof Recall that to each hyperplane is associated up to a multiplicative nonzero constant a affine polynomial. To a hyperplane configuration is associated the product of these affine polynomials. Let us consider T_1, the type 1 hyperplane configuration, T_2, the type 2 hyperplane configuration and T_3, the type 3 hyperplane configuration given in [26, Sect. 2.2]. The following inequalities hold (cf. [26, Propositions 2.6, 2.8]):

$$\#Z_{aff}\,(T_3) > \#Z_{aff}\,(T_1) > \#Z_{aff}\,(T_2)\,.$$

Note that T_3 defines codewords which have the second weight. We have computed in the proof of the previous theorem that

$$W_{aff}(f) - W_{aff}^{(2)}(q,\, n,\, d) \geq q^{n-a}.$$

But by [26, Proposition 2.9]

$$W_{aff}(T_2) - W_{aff}(T_3) = W_{aff}(T_2) - W^{(2)}_{aff}(q, n, d) = q^{n-a-2}(q-1).$$

Then

$$W_{aff}(f) > W_{aff}(T_2) > W_{aff}(T_1) > W_{aff}(T_3) = W^{(2)}_{aff}(q, n, d),$$

hence

$$W_{aff}(f) > W^{(4)}_{aff}(q, n, d).$$

□

4.4 Low weight codeword for the important case $d < q$

In the following, for GRM codes, we study when $d < q$ the case of an irreducible but not absolutely irreducible factor.

Theorem 27 *If $f \in \mathscr{R}P(q, n, d)$ is a product of two polynomials $f = g \cdot h$ such that*

(1) $2 \leq d' = \deg(g) \leq d = \deg(f) < q - 1$;
(2) *g is irreducible but not absolutely irreducible*;

then $W_{aff}(f) > W^{(2)}_{aff}(q, n, d)$. Moreover if $b \geq 3$ and $q \geq 2d - 4$ then $W_{aff}(f) > W^{(3)}_{aff}(q, n, d)$ else if $b \geq 3$ and $q \geq 2d - 3$ then $W_{aff}(f) > W^{(4)}_{aff}(q, n, d)$.

Proof We know by Lemma 15 that

$$\#Z_{aff}(f) < (d-1)q^{n-1}.$$

On the other hand,

$$W^{(2)}_{aff}(q, n, d) = q^n - dq^{n-1} + (d-1)q^{n-2}.$$

Then

$$W_{aff}(f) - W^{(2)}_{aff}(q, n, d) > q^{n-1} - (d-1)q^{n-2} > 0.$$

Consider now the two following hyperplane configurations S and T. The configuration S is given by two blocks of parallel hyperplanes directed by two linearly independent linear forms. The first block contains $b - 2$ parallel hyperplanes and the second block contains two parallel hyperplanes. The number of points of this configuration is (using for example [26, Theorem 2.1]):

$$\#Z_{aff}(S) = q^n - q^{n-2}(q-d+2)(q-2) = dq^{n-1} - (2d-4)q^{n-2} < q^n - W^{(2)}_{aff}(q, n, d).$$

The configuration T is given by three blocks of parallel hyperplanes directed by three linearly independent linear forms. The first block contains $b-2$ parallel hyperplanes, the second block and the third blocks contain a unique hyperplane. The number of points of this configuration is

$$\#Z_{aff}(T) = dq^{n-1} - (2d-3)q^{n-2}q^{n-3} < \#Z_{aff}(S).$$

If $q \geq 2d - 4$, we have

$$\#Z_{aff}(S) = dq^{n-1} - (2d-4)q^{n-2} \geq (d-1)q^{n-1} > \#Z_{aff}(f).$$

Then $W_{aff}(f) > W_{aff}(S)$. Moreover

$$\#Z_{aff}(S) < q^n - W_{aff}^{(2)}(q,\, n,\, d),$$

then

$$W_{aff}(S) = q^n - \#Z_{aff}(S) > W_{aff}^{(2)}(q,\, n,\, d).$$

Consequently

$$W_{aff}^{(2)}(q,\, n,\, d) < W_{aff}(S) < W_{aff}(f),$$

and then $W_{aff}(f) > W_{aff}^{(3)}(q,\, n,\, d)$. Now if $q \geq 2d - 3$, $W_{aff}(f) > \#Z_{aff}(T)$ and consequently

$$W_{aff}^{(2)}(q,\, n,\, d) < W_{aff}(S) < W_{aff}(T) < W_{aff}(f).$$

Then $W_{aff}(f) > W_{aff}^{(4)}(q,\, n,\, d)$. □

Remark 28 In the case of PGRM codes, there are results on the third weight codewords given by Rodier and Sboui [24]. They proved that for $q \geq 3d - 6$ the first three weights are given by hyperplane arrangements and by nothing else. Moreover they proved that this is no longer the case for

$$\frac{q}{2} + \frac{5}{2} \leq d < q,$$

in which case the third weight can be obtained also by some hypersurfaces containing an irreducible quadric.

5 The second weight in the projective case

In this section we tackle the unsolved problem of finding the second weight $W_{proj}^{(2)}(q,\, n,\, d)$ for PGRM codes. The following remark addresses the particular case where $n = 1$.

Remark 29 The code $\mathrm{PGRM}_q(d,\, 1)$ is MDS (cf. Remark 7). Then the weight distribution can be studied using the formulas given in [19, Theorem 6, p. 320]. In particular when $n = 1$ the minimal distance and the next-to-minimal distance are respectively:

$$W_h^{(1)}(q,\, 1,\, d) = q - d + 1, \tag{13}$$

$$W_h^{(2)}(q,\, 1,\, d) = q - d + 2. \tag{14}$$

Lemma 30 *Let f be a homogeneous polynomial in $n + 1$ variables of total degree d, with coefficients in $\mathbb{F}_q$, which does not vanish on the whole projective space $\mathbb{P}^n(q)$.*

(1) *If there exists a projective hyperplane H such that the affine hypersurface $(\mathbb{P}^n(q) \setminus H) \cap Z_{proj}(f)$ contains an affine hyperplane of the affine space $\mathbb{A}^n(q) = \mathbb{P}^n(q) \setminus H$ then the projective hypersurface $Z_{proj}(f)$ contains a projective hyperplane.*
(2) *If there exists a projective hyperplane H such that the affine hypersurface $(\mathbb{P}^n(q) \setminus H) \cap Z_{proj}(f)$ is an affine arrangement of hyperplanes then $Z_{proj}(f)$ is a projective arrangement of hyperplanes.*

(3) *If there exists a projective hyperplane H such that f restricted to the affine space $(\mathbb{P}^n(q) \setminus H)$ defines a minimal word or a next-to-minimal word then $Z_{proj}(f)$ is a projective arrangement of hyperplanes.*

Proof (1) Suppose that

$$f\,(1,\ X_1, \ldots, X_n) = (l\,(X_1, \ldots, X_n) - \alpha)\ f_1\,(X_1, \ldots, X_n)\,,$$

where $l(X_1, \ldots, X_n)$ is linear, then

$$f\,(X_0,\ X_1, \ldots, X_n) = (l\,(X_1, \ldots, X_n) - \alpha X_0)\ \widetilde{f_1}\,(X_0,\ X_1, \ldots, X_n)\,,$$

where $\widetilde{f_1}(X_0,\ X_1, \ldots, X_n)$ is the homogeneous polynomial obtained by homogenization of $f_1(X_1, \ldots, X_n)$. We conclude that f defines a hypersurface containing a hyperplane.

(3) Using the same argument factor by factor we obtain the second statement.

(4) As minimal words and next-to-minimal words are always given by products of degree one factors [7,17], the third statement is a consequence of the second statement.

□

Lemma 31 *For $n \geq 2$ and $d \geq 2$ the following holds*

$$W^{(1)}_{proj}(q,\ n-1,\ d) + W^{(2)}_{aff}(q,\ n,\ d) \leq W^{(2)}_{aff}(q,\ n,\ d-1).$$

Proof Let us introduce the following notations:

$$\begin{aligned} d-1 &= a_{d-1}(q-1) + b_{d-1} \quad \text{with} \quad 0 \leq b_{d-1} \leq q-2, \\ d &= a_d(q-1) + b_d \quad \text{with} \quad 0 \leq b_d \leq q-2. \end{aligned}$$

Define γ_{d-1} and γ_d as in (4). Then we have

$$\begin{aligned} W^{(1)}_{proj}(q,\ n-1,\ d) &= (q - b_{d-1})\, q^{n-a_{d-1}-2}, \\ W^{(2)}_{aff}(q,\ n,\ d) &= (q - b_d)\, q^{n-a_d-1} + \gamma_d q^{n-a_d-2}, \\ W^{(2)}_{aff}(q,\ n,\ d-1) &= (q - b_{d-1})\, q^{n-a_{d-1}-1} + \gamma_{d-1} q^{n-a_{d-1}-2}. \end{aligned}$$

Denote by Δ the difference

$$\Delta = W^{(2)}_{aff}(q,\ n,\ d-1) - \left(W^{(1)}_{proj}(q,\ n-1,\ d) + W^{(2)}_{aff}(q,\ n,\ d)\right).$$

(1) If $0 \leq b_{d-1} \leq q-3$ then $q > 2$, $b_d = b_{d-1} + 1$ and $a_d = a_{d-1}$. In this case let us denote by a the common value of a_d and a_{d-1}. Hence

$$\Delta = q^{n-a-2}\,(b_{d-1} + \gamma_{d-1} - \gamma_d)\,.$$

- If $a = n-1$ and $b_{d-1} = 0$ then $\gamma_{d-1} = q(q-2)$, $\gamma_d = q$ and $\Delta = q^{n-a-1}(q-3)$.
- If $a = n-1$ and $b_{d-1} > 0$ then $\gamma_{d-1} = \gamma_d = q$ and $\Delta = q^{n-a-2} b_{d-1}$.
- If $a < n-1$, $b_{d-1} = 0$ and $q = 3$ then $\gamma_{d-1} = 3$, $\gamma_d = 2$ and $\Delta = q^{n-a-1}$.
- If $a < n-1$, $b_{d-1} = 0$ and $q \geq 4$ then $\gamma_{d-1} = q(q-2)$, $\gamma_d = q$ and $\Delta = q^{n-a-1}(q-3)$.
- If $a < n-1$, $b_{d-1} = 1$, and $q = 3$ then $\gamma_{d-1} = 2$, $\gamma_d = 1$ and $\Delta = 2q^{n-a-2}$.
- If $a < n-1$, $b_{d-1} = 1$, and $q \geq 4$ then $\gamma_{d-1} = q$, $\gamma_d = 1$ and $\Delta = q^{n-a-1}$.
- If $a < n-1$ and $b_{d-1} \geq 2$ then $\gamma_{d-1} - \gamma_d = -1$ and $\Delta = q^{n-a-2}(b_{d-1} - 1)$.

(2) If $b_{d-1} = q-2$ then $a_d = a_{d-1} + 1$ and $b_d = 0$. In this case

- If $a_{d-1} = n-1$ then $W^{(2)}_{aff}(q,\ n,\ d-1)=3,\ W^{(2)}_{aff}(q,\ n,\ d)=2,\ W^{(1)}_{proj}(q,\ n-1,\ d) = 1$. Then $\Delta = 0$.
- If $a_{d-1} < n-1$ then

$$\Delta = 2q^{n-a_{d-1}-1} + \gamma_{d-1}q^{n-a_{d-1}-2} - 2q^{n-a_{d-1}-2} - q^{n-a_{d-1}-1} - \gamma_d q^{n-a_{d-1}-3},$$

$$\Delta = q^{n-a_{d-1}-2}\left(q - 2 + \gamma_{d-1} - \frac{\gamma_d}{q}\right).$$

- If $a_{d-1} = n-2$ and $q = 2$ then $\gamma_{d-1} = 2,\ \gamma_d = 4$ and $\Delta = 0$.
- If $a_{d-1} < n-2$ and $q = 2$ then $\gamma_{d-1} = \gamma_d = 2$ and $\Delta = q^{n-a_{d-1}-2}$.
- If $q = 3$ then $\gamma_{d-1} = 2,\ \gamma_d = 3$ and $\Delta = 2 \times 3^{n-a_{d-1}-2}$.
- If $q \geq 4$ then $\gamma_{d-1} = q-3,\ \gamma_d = q(q-2)$ and $\Delta = q^{n-a_{d-1}-2}(q-3)$.

□

Remark 32 In the previous lemma, $\Delta \geq 0$ is zero in the following cases:

- $q = 3,\ a_{d-1} = n-1$ and $b_{d-1} = 0$, namely $d = 2(n-1)+1$.
- $q = 2,\ a_{d-1} = n-2$, namely $d = n-1$.
- $a_{d-1} = n-1,\ b_{d-1} = q-2$, namely $d = n(q-1)$.

Theorem 33 *Let $W^{(2)}_{proj}(q,\ n,\ d)$ be the second weight for a homogeneous polynomial f in $n+1$ variables ($n \geq 2$) of total degree d ($2 \leq d \leq n(q-1)$), with coefficients in $\mathbb{F}_q$, which is not maximal. Then the following holds*:

$$W^{(1)}_{proj}(q,\ n-1,\ d) + W^{(2)}_{aff}(q,\ n,\ d) \leq W^{(2)}_{proj}(q,\ n,\ d) \leq W^{(2)}_{aff}(q,\ n,\ d-1).$$

Moreover

$$W^{(2)}_{proj}(q,\ n,\ d) \geq \min\left(W^{(1)}_{proj}(q,\ n-1,\ d) + W^{(3)}_{aff}(q,\ n,\ d),\ W^{(2)}_{aff}(q,\ n,\ d-1)\right).$$

Proof Remark first that by Lemma 31

$$W^{(1)}_{proj}(q,\ n-1,\ d) + W^{(2)}_{aff}(q,\ n,\ d) \leq W^{(2)}_{aff}(q,\ n,\ d-1).$$

Let f be such that $Z_{proj}(f)$ is not maximal. Suppose first that there is a hyperplane H in $Z_{proj}(f)$. Then we can suppose that

$$f\left(X_0,\ X_1, \ldots, X_n\right) = X_0 g\left(X_0,\ X_1, \ldots, X_n\right),$$

where g is a homogeneous polynomial of degree $d-1$. The function

$$f_1\left(X_1, \ldots, X_n\right) = g\left(1,\ X_1, \ldots, X_n\right),$$

defined on the affine space $\mathbb{A}^n(q) = \mathbb{P}^n(q) \setminus H$ is a polynomial function in n variables of total degree $d-1$. If it was maximum, by Theorem 8, the function f would also be maximum.

Then $\#Z_{aff}(f_1) \leq q^n - W^{(2)}_{aff}(q,\ n,\ d-1)$. Hence the following holds:

$$\#Z_{proj}(f) \leq \frac{q^n - 1}{q-1} + q^n - W^{(2)}_{aff}(q,\ n,\ d-1),$$

$$\#Z_{proj}(f) \leq \frac{q^{n+1} - 1}{q-1} - W^{(2)}_{aff}(q,\ n,\ d-1),$$

and the equality holds if and only if f_1 reaches the second weight on the affine space $\mathbb{A}^n(q)$. This case actually occurs. Hence for such a word, in general we have

$$W_{proj}(f) \geq W^{(2)}_{aff}(q,\ n,\ d-1),$$

and as the equality occurs, the following holds for the second distance: $W^{(2)}_{proj}(q,\, n,\, d) \leq W^{(2)}_{aff}(q,\, n,\, d-1)$.

Suppose now that there is not any hyperplane in the hypersurface $Z_{proj}(f)$. Let H be a hyperplane and $\mathbb{A}^n(q) = \mathbb{P}^n(q) \setminus H$. Then as $H \cap Z_{proj}(f) \neq H$

$$\#\left(H \cap Z_{proj}(f)\right) \leq \frac{q^n-1}{q-1} - W^{(1)}_{proj}(q,\, n-1,\, d).$$

We know that the first and second weight of a GRM code are arrangements of hyperplanes, then by Lemma 30

$$\#\left(Z_{proj}(f) \cap \mathbb{A}^n(q)\right) \leq q^n - W^{(3)}_{aff}(q,\, n,\, d).$$

Now we can write

$$\begin{aligned}\#Z_{proj}(f) &\leq \frac{q^n-1}{q-1} - W^{(1)}_{proj}(q,\, n-1,\, d) + q^n - W^{(3)}_{aff}(q,\, n,\, d),\\ &\leq \frac{q^{n+1}-1}{q-1} - \left(W^{(1)}_{proj}(q,\, n-1,\, d) + W^{(3)}_{aff}(q,\, n,\, d)\right),\end{aligned}$$

and consequently

$$W_{proj}(f) \geq W^{(1)}_{proj}(q,\, n-1,\, d) + W^{(3)}_{aff}(q,\, n,\, d) > W^{(1)}_{proj}(q,\, n-1,\, d) + W^{(2)}_{aff}(q,\, n,\, d).$$

Then, for the second distance the conclusion of the theorem holds. □

Remark 34 When $q \geq 2(d-1)$ we know by [28] that

$$W^{(2)}_{proj}(q,\, n,\, d) = W^{(2)}_{aff}(q,\, n,\, d-1) = q^n - (d-1)q^{n-1} + (d-2)q^{n-2}.$$

Unfortunately for the general case we don't know the value of $W^{(3)}_{aff}(q,\, n,\, d)$ and we don't know if the value of the sum $W^{(1)}_{proj}(q,\, n-1,\, d) + W^{(3)}_{aff}(q,\, n,\, d)$ is greater than $W^{(2)}_{aff}(q,\, n,\, d-1)$ or not. What is the exact value of $W^{(2)}_{proj}(q,\, n,\, d)$? This question remains open.

References

1. Assmus E., Key J.: Designs and their codes. In: Cambridge Tracts in Mathematics, vol. 103. Cambridge University Press, Cambridge (1992).
2. Blake I., Mullin R.: The Mathematical Theory of Coding. Academic Press, New York (1975).
3. Bruen A.: Polynomial multiplicities over finite fields and intersection sets. J. Comb. Theory **60**(1), 19–33 (1992).
4. Bruen A.: Applications of finite fields to combinatorics and finite geometries. Acta Appl. Math. **93**(1–3), 179–196 (2006).
5. Bruen A.: Blocking sets and low-weight codewords in the generalized Reed–Muller codes. In: Bruen A., Wehlau D., Society C.M. (eds.) Error-Correcting Codes, Finite Geometries, and Cryptography, Contemporary Mathematics, vol. 525, pp. 161–164. American Mathematical Society (2010).
6. Cherdieu J.P., Rolland R.: On the number of points of some hypersurfaces in $\mathbb{F}_q^n$. Finite Field Appl. **2**, 214–224 (1996).
7. Delsarte P., Goethals J., MacWilliams F.: On generalized Reed–Muller codes and their relatives. Inform. Control **16**, 403–442 (1970).
8. Dickson L.: Linear Groups. Dover Publications, New York (1958).
9. Erickson D.: Counting zeros of polynomials over finite fields. PhD Thesis, California Institute of Technology, Pasadena (1974).

10. Geil O.: On the second weight of generalized Reed–Muller codes. Des. Codes Cryptogr. **48**(3), 323–330 (2008).
11. Kasami T., Lin S., Peterson W.: New generalizations of the Reed–Muller codes. Part I: primitive codes. IEEE Trans. Inform. Theory **IT-14**(2), 189–199 (1968).
12. Kasami T., Tokura N., Azumi S.: On the weight enumeration of weights less than 2.5d of Reed–Muller codes. Inform. Control **30**(4), 380–395 (1976).
13. Lachaud G.: Projective Reed–Muller codes. In: Coding Theory and Applications. Lecture Notes in Computer Science, vol. 311, pp. 125–129. Springer, Berlin (1988).
14. Lavrauw M., Storme L., Van de Voorde G.: On the code generated by the incidence matrix of points and hyperplanes in $PG(n, q)$ and its dual. Des. Codes Cryptogr. **48**, 231–245 (2008a).
15. Lavrauw M., Storme L., Van de Voorde G.: On the code generated by the incidence matrix of points and k-spaces in $PG(n, q)$ and its dual. Finite Fields Appl. **14**, 1020–1038 (2008b).
16. Lavrauw M., Storme L., Sziklai P., Van de Voorde G.: An empty interval in the spectrum of small weight codewords in the code from points and k-spaces in $PG(n, q)$. J. Comb. Theory **116**(4), 996–1001 (2009).
17. Leducq E.: Second weight codewords of generalized Reed–Muller codes. Cryptogr. Commun. **5**, 241–276 (2012).
18. Leducq E.: A new proof of Delsarte, Goethals and MacWilliams theorem on minimal weight codewords of generalized Reed–Muller codes. Finite Fields Appl. **18**(3), 581–586 (2013).
19. MacWilliams F., Sloane N.: The theory of error-correcting codes. In: Mathematical Library, vol. 16. North Holland, Amsterdam (1977).
20. McEliece R.: Quadratic Forms Over Finite Fields and Second-Order Reed–Muller Codes. Technical Report, JPL Space Programs Summary III (1969).
21. Mercier D.J., Rolland R.: Polynômes homogènes qui s'annulent sur l'espace projectif $\mathbb{P}^m(\mathbb{F}_q)$. J. Pure Appl. Algebra **124**, 227–240 (1998).
22. Rentería C., Tapia-Recillas H.: Reed–Muller codes: an ideal theory approach. Commun. Algebra **25**(2), 401–413 (1997).
23. Rodier F., Sboui A.: Les arrangements minimaux et maximaux d'hyperplans dans $\mathbb{P}^n(\mathbb{F}_q)$. C. R. Math. Acad. Sci. Paris **344**(5), 287–290 (2007).
24. Rodier F., Sboui A.: Highest numbers of points of hypersurfaces over finite fields and generalized Reed–Muller codes. Finite Fields Appl. **14**(3), 816–822 (2008).
25. Rolland R.: Number of points of non-absolutely irreducible hypersurfaces. In: Algebraic Geometry and Its Applications, Number Theory and Its Applications, Proceedings of the First SAGA Conference, 7–11 May 2007, Papeete, vol. 5, pp. 481–487. World Scientific, Singapore (2008).
26. Rolland R.: The second weight of generalized Reed–Muller codes in most cases. Cryptogr. Commun. Discret. Struct. Boolean Funct. Seq. **2**(1), 19–40 (2010).
27. Sboui A.: Second highest number of points of hypersurfaces in $\mathbb{F}_q^n$. Finite Fields Appl. **13**(3), 444–449 (2007).
28. Sboui A.: Special numbers of rational points on hypersurfaces in the n-dimensional projective space over a finite field. Discret. Math. **309**(16), 5048–5059 (2009).
29. Schmidt W.: Equations Over Finite Fields: An Elementary Approach. Lecture Notes in Mathematics, vol. 536. Springer, Berlin (1976).
30. Serre J.P.: Lettre à M. Tsfasman du 24 Juillet 1989. In: Journées arithmétiques de Luminy 17–21 Juillet 1989, Astérisque, pp. 198–200. Société Mathématique de France (1991).
31. Sørensen A.: A Note on Algorithms Deciding Rationality and Absolutely Irreducibility Based on the Number of Rational Solutions. RISC-Linz Series 91-37.0 (1991a).
32. Sørensen A.: Projective Reed–Muller codes. Trans. Inform. Theory **IT-37**(6), 1567–1576 (1991b).
33. Van de Voorde G.: Blocking sets in finite projective spaces and coding theory. PhD Thesis, Thesis Faculteit Wetenschappen Vakgroep Zuivere Wiskunde en Computeralgebra (2010).