On Low Weight Codewords of Generalized Affine and Projective Reed-Muller Codes (Extended abstract)

Stéphane Ballet · Robert Rolland

Received: date / Accepted: date

Abstract We propose new results on low weight codewords of affine and projective generalized Reed-Muller codes. In the affine case we give some results on codewords that cannot reach the second weight also called the next to minimal distance. In the projective case the second distance of generalized Reed-Muller codes is estimated, namely a lower bound and an upper bound of 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 (2010) 94B27 · 94B65 · 11G25 · 11T71

1 Introduction - Notations

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

For GRM codes, we give some results concerning the next to minimal weight codewords. These codewords are known when \( 1 \leq d \leq \frac{q}{2} \) (cf. [10], [21]). For other values of \( d \) we prove that an irreducible, non-absolutely irreducible polynomial cannot reach the second weight. For \( d < q - 1 \) we improve the previous result. More precisely we show that a polynomial having a factor of degree \( d \geq 2 \) which is irreducible, non-absolutely irreducible, cannot reach the second weight.

For PGRM codes, we determine an upper bound and a lower bound for the second weight of a PGRM code.

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

Stéphane Ballet  
Aix-Marseille University, ERISCS and IML case 930, F13288 Marseille cedex 9, France  
E-mail: stephane.ballet@univ-amu.fr

Robert Rolland  
Aix-Marseille University, ERISCS and IML case 930, F13288 Marseille cedex 9 France  
E-mail: robert.rolland@acrypa.fr
of coding theory, knowing something on the weight distribution of a code, and especially on the low weights is a 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 \cite[5.3 and 5.4]{1}). From this point of view, the 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.

1.1 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 $\mathcal{F}(q, n)$ the space of functions from $\mathbb{F}_q^n$ into $\mathbb{F}_q$. Any function in $\mathcal{F}(q, n)$ 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 $\mathcal{P}(q, n)$ the set of reduced polynomials in $n$ variables over $\mathbb{F}_q$.

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

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

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

provides $\mathbb{F}_q[X_0, X_1, X_2, \ldots, X_n]$ with a graded algebra structure.

1.2 Generalized Reed-Muller codes

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

$$\text{RM}_q(d, n) = \left\{ (f(X))_{X \in \mathbb{F}_q^n} \mid f \in \mathbb{F}_q[X_0, \ldots, X_n] \text{ and } \deg(f) \leq d \right\}.$$  

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 $\mathcal{P}(q, n, d)$.

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

$$W_a(f) = q^n - N_a(f).$$
The code RM$_a(q,d,n)$ has the following parameters (cf. [12], [3, p. 72]) (where the index $a$ stands for “affine code”):

1. length $m_a(q,n,d) = q^n$,
2. dimension

$$k_a(q,n,d) = \sum_{i=0}^{d} \sum_{j=0}^{n} (-1)^j \binom{n}{j} \binom{t-jq+n-1}{t-jq},$$
3. minimum distance $W_a(q,n,d) = (q-b)q^{n-a-1}$, 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 $0 \leq b < q-1$.

We denote by $N_a(q,n,d)$ the maximum number of zeros for a non-null polynomial function of degree $\leq d$ where $1 \leq d < n(q-1)$, namely

$$N_a(q,n,d) = q^n - W_a(q,n,d) = q^n - (q-b)q^{n-a-1}.$$

The minimum distance of RM$_a(q,d,n)$ was given by T. Kasami, S. Lin, W. Peterson in [12]. The words reaching this bound were characterized by P. Delsarte, J. Goethals and F. MacWilliams in [8].

1.3 Projective generalized Reed-Muller 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 projective generalized Reed-Muller code of order $d$ (PGRM code) was introduced by G. Lachaud in [14]. Let $S$ a subset of $P_{q-1}^n$ constituted by one point on each punctured vector line of $P_{q-1}^n$. Remark that any point of the projective space $P^q$ has a unique coordinate representation by an element of $S$. The projective Reed-Muller code PRM$_a(q,d,n)$ of order $d$ over $P^q$ is constituted by the words $(f(X))_{X \in S}$ where $f \in \mathcal{H}(q,n+1,d)$ and the null word:

$$\text{PRM}_a(n,d) = \left\{ (f(X))_{X \in S} \mid f \in \mathcal{H}(q,n+1,d) \right\} \cup \{0, \ldots, 0\}.$$

This code is dependent on the set $S$ chosen to represent the points of $P^q$. But the main parameters are independent of this choice. Following [14] we can choose

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

where $S_i = \{0, \ldots, 0, X_{i+1}, \ldots, X_n \mid X_i \in \mathbb{F}_q \}$. Subsequently, we shall adopt this value of $S$ to define the code PRM$_a(q,d,n)$.

For a homogeneous polynomial $f$ let us denote by $Z_h(f)$ the set of zeros of $f$ in the projective space $P^q$ (where the index $h$ stands for “projective”). From a geometrical point of view, an element $f \in \mathcal{H}(q,n+1,d)$ defines a projective hypersurface $Z_h(f)$ in the projective space $P^q$. The number $N_h(f) = \#Z_h(f)$ of points of this projective hypersurface is connected to the weight $W_h(f)$ of the corresponding codeword by the following relation:

$$W_h(f) = \frac{d_{2^n-1} - 1}{q-1} - N_h(f).$$

The parameters of PRM$_a(n,d)$ are the following (cf. [23]) (where the index $h$ stands for “projective code”):
1. length \( m_h(q, n, d) = \frac{q^{d+1} - 1}{q-1} \).

2. dimension

\[
k_h(q, n, d) = \sum_{i=1}^{n} a_i^{d+1} \left( \frac{q}{1-q} \right)^i \left( \frac{q^n}{1-q} \right)^{d+1}.
\]

3. minimum distance: \( W_h^{(1)}(q, n, d) = (q-b)q^{n-d-1} \) 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 \( 0 \leq b < q-1 \).

We denote by \( N_h^{(1)}(q, n, d) \) the maximum number of zeros for a non-null homogeneous polynomial function of degree \( d \) where \( 1 \leq d \leq n(q-1) \), namely

\[
N_h^{(1)}(q, n, d) = \frac{q^{d+1} - 1}{q-1} - W_h^{(1)}(q, n, d) = \frac{q^{d+1} - 1}{q-1} - (q-b)q^{n-d-1}.
\]

1.4 Minimal distance and corresponding codewords

1.4.1 The affine case: GRM codes

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

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

The minimum distance of a GRM code was given by T. Kasami, S. Lin, W. Peterson in [12]. The words reaching this bound (i.e. the polynomials reaching the maximal number of zeros) were characterized by P. Delsarte, J. Goethals and F. MacWilliams in [8]. Such a polynomial will be called a maximal polynomial and the associated hypersurface is called a maximal hypersurface. The corresponding weight is the minimal weight.

1.4.2 The projective case: PGRM codes

Let us denote respectively by \( W_h^{(1)}(q, n, d) \) and \( W_h^{(2)}(q, n, d) \) the first and second weight of the projective Reed-Muller code.

In order to describe the minimal distance for 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 J.-P. Serre for \( d \leq q \) (cf. [22]), and by A. Sørensen in [23] for the general case. The polynomials reaching the maximal number of zeros (or defining the minimum weighted codewords) are given by J.-P. Serre for \( d \leq q \) (cf. [22]) and by the last author (cf. [19]) for the general case.

2 The second weight in the affine case

2.1 what is known

Let us denote by \( W_h^{(2)}(q, n, d) \) the second weight of the GRM code \( RM_b(d, n) \), 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 \( W^{(1)}_a(q, n, 1) = q^n - q^{n-1} \) and the second weight \( W^{(2)}_a(q, n, 1) = q^n \). For \( d = 2 \) and
Low Weight Codewords of Reed-Muller Codes

$q = 2$ the weight distribution is more or less a consequence of the investigation of quadratic forms done by L. Dickson in [9] 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 R. McEliece in [18]. For $q = 2$, for any $n$ and any $d$, the weight distribution is known in the range $[W_a^{(1)}(2, n, d), 2.5W_a^{(1)}(2, n, d)]$ by a result of Kasami, Tokura, Azumi [13]. In particular, the second weight is $W_a^{(2)}(2, n, d) = 3 \times 2^{n-d-1}$ if $1 < d < n - 1$ and $W_a^{(2)}(2, n, d) = 2^{n-d+1}$ if $d = n-1$ or $d = 1$. For $d \geq n(q-1)$ the code $RM_q(d, n)$ is trivial, namely it is the whole $\mathcal{F}(q, d, n)$, hence any integer $0 \leq t \leq q^d$ is a weight. Let us remark also that if $q = p$ is a prime, GRM codes (and also PGRM codes) are the finite geometry codes, and in this case the next to minimal distance is known as well as the geometrical nature of the corresponding codewords.

The general problem of the second weight was tackled by D. Erickson in his thesis [10, 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. The second weight was first studied by J.-P. Cherdieu and R. Rolland in [7] who proved that when $q > 2$ is fixed, for $d < q$ sufficiently small the second weight is

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

Their result was improved by A. Sboui in [21], who proved the formula for $d \leq q/2$. The methods in [7] and [21] are of a geometric nature by means of which the codewords reaching this weight were determined. These codewords are hyperplane arrangements. Then O. Geil in [11], using Gröbner basis methods, proved the formula for $d < q$ and solved the problem for $n = 2$. This case is particularly important as we shall see later. Finally, the last author in [20], using a mix of Geil’s method and geometrical considerations found the second weight for all cases except when $d = a(q-1) + 1$.

Recently, A. Bruen ([6]) exhume the work of Erickson and completed the proof, solving the problem of the second weight for Generalized Reed-Muller code. Let us describe more precisely the result of Erickson. First, in order to present his result let us introduce the following notation used in [10]: $s$ and $t$ are integers such that

$$d = s(q-1) + t,$$  

with $0 < t \leq q-1$.

**Theorem 1** The second weight $W_a^{(2)}(q, n, d)$ is

$$W_a^{(2)}(q, n, d) = W_a^{(1)}(q, n, d) + cq^{n-t-2}$$  

where $W_a^{(1)}(q, n, d) = (q-t)q^{n-t-1}$ is the minimal distance and $c$ is

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

The number $c_t$ is such that $c_t + (q-t)q$ is the second weight for the code $RM_q(2, t)$. 

Unfortunately the number \( c \) is not determined in the work of Erickson. But, it results from the previous theorem that if someone could calculate the second weight for a case where \( c = c_t \), the problem would be fully resolved. Alternatively, Erickson conjectured that \( c_t = t - 1 \) and reduced this conjecture to a conjecture on blocking sets [10, Conjecture 4.14 p. 76]. Recently in [6] A. Bruen proved that this conjecture follows from two of his papers [4], [5]. Then the problem is now solved by [10]+[6]. It is also solved by [10]+[11] (the important case \( n = 2 \) is completely solved in [11] and this leads to the conclusion as noted above) or by [10]+[20] (the cases not solved in [10] are explicitly resolved in [20]).

**Remark 2** 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 \( b = 0 \). Then we can also express the second weight with the classical writing for the Euclidean quotient as in [20].

Finally let us remark that we now have several approaches, close to each other, but nevertheless different. The first one [10],[6] is mainly based on combinatorics of finite geometries, the second one [7],[21], [20] is mainly based on geometry and hyperplane arrangements, the third [11], [20] 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 [24], [16], [17], [15]).

2.2 New results on the codewords reaching the second weight

The polynomials reaching the second weight are known for \( 2d \leq q \) (cf. [10, Theorem 3.13, p. 60], [21]). For the other values of \( d \) the result is not known. However we can say that:

**Theorem 3** If \( f \in \mathbb{R}P(q, n, d) \) is an irreducible polynomial but not absolutely irreducible, in \( n \) variables over \( \mathbb{F}_q \), of degree \( d > 1 \) then the weight \( W_a(f) \) of the corresponding codeword in \( RM_q(n, d) \) is such that \( W_a(f) > W_a^{(2)}(q, n, d) \). Namely such a polynomial cannot reach the next to minimal weight.

**Theorem 4** If \( f \in \mathbb{R}P(q, n, d) \) 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 \( W_a(f) > W_a^{(2)}(q, n, d) \). Namely such a polynomial cannot reach the next to minimal weight.

The proofs of these two theorems will be given in the full paper and can be found in the preprint [2].

**Remark 5** In any case, among the words reaching the second distance, there are hyperplane configurations. For example the hyperplane configurations given in [20].
3 The second weight in the projective case

In this section we tackle the problem of finding the second weight \( W^{(2)}_h(q, n, d) \) for GPRM codes. Note that if \( q \) is a prime \( p \).

Lemma 6 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 \( \mathbb{P}^n(q) \). If there exists a projective hyperplane \( H \) such that the affine hypersurface \( (\mathbb{P}^n(q) \setminus H) \cap Z_h(f) \) contains an affine hyperplane of the affine space \( \mathbb{A}^n(q) = \mathbb{P}^n(q) \setminus H \) then the projective hypersurface \( Z_h(f) \) contains a projective hyperplane. In particular if \( f \) restricted to the affine space \( \mathbb{A}^n(q) \) defines a maximal affine hypersurface then \( Z_h(f) \) contains a hyperplane.

Lemma 7 For \( n \geq 2 \) the following holds

\[
W^{(1)}_h(q, n-1, d) + W^{(2)}_a(q, n, d) \leq W^{(2)}_a(q, n, d-1).
\]

Proof Let us introduce the following notations:

\[
d - 1 = s_{d-1}(q-1) + t_{d-1}, \quad \text{where} \quad 1 \leq t_{d-1} \leq q - 1;
\]

\[
d = s_d(q-1) + t_d \quad \text{where} \quad 1 \leq t_d \leq q - 1.
\]

The values \( c(d-1) \) and \( c(d) \) are the values of the coefficient \( c \) which occurs in Theorem 1, with respect to \( d - 1 \) and \( d \). Then we have

\[
W^{(1)}_h(q, n-1, d) = (q - t_{d-1})q^{n-s_{d-1}-2},
\]

\[
W^{(2)}_a(q, n, d) = (q - t_d)q^{n-s_1-1} + c(d)q^{n-s_{d-2}-2},
\]

\[
W^{(2)}_a(q, n, d-1) = (q - t_{d-1})q^{n-s_{d-2}-1} + c(d-1)q^{n-s_{d-3}-2}.
\]

Denote by \( \Delta \) the difference

\[
\Delta = W^{(2)}_a(q, n, d-1) - \left( W^{(1)}_h(q, n-1, d) + W^{(2)}_a(q, n, d) \right).
\]

- If \( 1 \leq t_{d-1} \leq q - 2 \) then \( q > 2 \), \( t_d = t_{d-1} + 1 \) and \( s_d = s_{d-1} \). In this case let us denote by \( s \) the common value of \( s_d \) and \( s_{d-1} \). Hence

\[
\Delta = q^{n-s_1-2} (t_{d-1} + c(d-1) - c(d)),
\]

- If \( s = s_{n-1} \) then \( c(d-1) = c(d) \) and \( \Delta > 0 \).
- If \( s < s_{n-1} \) and \( 1 < t_{d-1} \leq \frac{s_{d-1}}{2} - 1 \) then \( q \geq 4 \) and \( c(d-1) - c(d) = -1 \). Hence \( \Delta > 0 \).
- If \( s < s_{n-1} \) and \( \frac{s_{d-1}}{2} - 1 < t_{d-1} \leq \frac{s_{d-1}}{2} \) then \( q \geq 4 \) and \( c(d-1) - c(d) = -1 \). Hence \( \Delta > 0 \).
- If \( s < s_{n-1} \), \( q \geq 4 \) and \( t_{d-1} = 1 \) then \( c(d-1) - c(d) = q - t_{d-1} \). Hence \( \Delta > 0 \).
- If \( s < s_{n-1} \), \( q = 3 \) and \( t_{d-1} = 1 \) then \( c(d-1) - c(d) = 1 \). Hence \( \Delta > 0 \).
- If \( t_{d-1} = q - 1 \) then \( t_d = 1 \) and \( s_d = s_{d-1} + 1 \). Hence

\[
\Delta = q^{n-s_{d-1}-3} (c(d-1)q - c(d)) \geq 0.
\]
Theorem 8 Let $W_h^{(2)}(q, n, d)$ be the second weight for a homogeneous polynomial $f$ in $n + 1$ variables ($n \geq 2$) of total degree $d$, with coefficients in $\mathbb{F}_q$, which is not maximal. Let us define $V^{(2)}_h(q, n, d)$ by:
\[ V^{(2)}_h(q, n, d) = 2 \text{ if } d > n(q-1) \]
and
\[ V^{(2)}_h(q, n, d) = W_h^{(1)}(q, n-1, d) + W_a^{(2)}(q, n, d) \text{ if } d \leq n(q-1). \] (2)

Then the following holds:
\[ V^{(2)}_h(q, n, d) \leq W_h^{(2)}(q, n, d) \leq W_a^{(2)}(q, n, d-1). \]

Proof Let us remark first that by Lemma 7
\[ V^{(2)}_h(q, n, d) \leq W_a^{(2)}(q, n, d-1). \]

If $d > n(q-1)$, as $f$ does not vanish on the whole projective space $\mathbb{P}^n(q)$, and $f$ is not maximal then $N_h(f) \leq \frac{q^{d+1}-1}{q-1} - 2$. This bound is attained. Then in this case $W_h^{(2)}(q, n, d) = 2$.

Suppose now that $2 \leq d \leq n(q-1)$. Let $f$ such that $Z_h(f)$ is not maximal. Suppose first that there is an hyperplane $H$ in $Z_h(f)$. Then we can suppose that
\[ f(X_0, X_1, \ldots, X_n) = X_0g(X_0, X_1, \ldots, X_n) \]
where $g$ is an homogeneous polynomial of degree $d-1$. The function
\[ f_1(X_1, \ldots, X_n) = g(1, X_1, \ldots, X_n) \]
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 $d-1$.

Then $\#Z_h(f_1) \leq q^n - W_a^{(2)}(q, n, d-1)$. Hence the following holds:
\[ \#Z_h(f) \leq \frac{q^n - 1}{q-1} + q^n - W_a^{(2)}(q, n, d-1), \]
\[ \#Z_h(f) \leq \frac{q^{n+1} - 1}{q-1} - W_a^{(2)}(q, n, d-1), \]
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
\[ W_h(f) \geq W_a^{(2)}(q, n, d-1), \]
and as the equality occurs, the following holds for the second distance:
\[ W_h^{(2)}(q, n, d) \leq W_a^{(2)}(q, n, d-1). \]

Suppose now that there is not any hyperplane in the hypersurface $Z_h(f)$. Let $H$ be a hyperplane and $\mathbb{A}^n(q) = \mathbb{P}^n(q) \setminus H$. Then as $H \cap Z_h(f) \neq H$
\[ \#(H \cap Z_h(f)) \leq \frac{q^n - 1}{q-1} - W_h^{(1)}(q, n-1, d), \]
and by Lemma 6

\[ \#(Z_h(f) \cap A^n(q)) \leq q^n - W_a^{(2)}(q, n, d). \]

Then

\[ \#Z_h(f) \leq \frac{q^n - 1}{q - 1} - W_h^{(1)}(q, n - 1, d) + q^n - W_a^{(2)}(q, n, d) \]
\[ \leq \frac{q^{n+1} - 1}{q - 1} - \left(W_h^{(1)}(q, n - 1, d) + W_a^{(2)}(q, n, d)\right) \]

and consequently

\[ \quad W_h(f) \geq W_h^{(1)}(q, n - 1, d) + W_a^{(2)}(q, n, d). \]

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

References