Cryptogr. Commun. (2013) 5:241–276
DOI 10.1007/s12095-013-0084-z

Second weight codewords of generalized Reed-Muller codes

Elodie Leducq

Received: 4 December 2012 / Accepted: 12 May 2013 / Published online: 5 June 2013

Abstract Recently, the second weight of generalized Reed-Muller codes have been determined (Erickson 1974; Bruen 2010; Geil, Des. Codes Cryptogr. 48(3):323–330, 2008; Rolland, Cryptogr. Commun. 2(1):19–40, 2010). In this paper, we give the second weight codewords of the generalized Reed-Muller codes.

Keywords Generalized Reed-Muller codes · Second weight codewords · Hyperplane · Affine geometry

Mathematics Subject Classifications (2010) 11-T-71

1 Introduction

In this paper, we want to characterize the second weight codewords of generalized Reed-Muller codes.

We first introduce some notations:

Let p be a prime number, n a positive integer, $q = p^n$ and $\mathbb{F}_q$ a finite field with q elements.

If m is a positive integer, we denote by B_m^q the $\mathbb{F}_q$-algebra of the functions from $\mathbb{F}_q^m$ to $\mathbb{F}_q$ and by $\mathbb{F}_q[X_1, \ldots, X_m]$ the $\mathbb{F}_q$-algebra of polynomials in m variables with coefficients in $\mathbb{F}_q$.

We consider the morphism of $\mathbb{F}_q$-algebras $\varphi : \mathbb{F}_q[X_1, \ldots, X_m] \to B_m^q$ which associates to $P \in \mathbb{F}_q[X_1, \ldots, X_m]$ the function $f \in B_m^q$ such that

$$\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m,\ f(x) = P(x_1, \ldots, x_m).$$

The morphism φ is onto and its kernel is the ideal generated by the polynomials $X_1^q - X_1, \ldots, X_m^q - X_m$. So, for each $f \in B_m^q$, there exists a unique polynomial $P \in$

E. Leducq (✉)
Institut de Mathématiques de Jussieu, 175 rue du Chevaleret, 75013 Paris, France
e-mail: elodieleducq@math.jussieu.fr

$\mathbb{F}_q[X_1, \dots, X_m]$ such that the degree of P in each variable is at most $q-1$ and $\varphi(P) = f$. We say that P is the reduced form of f and we define the degree $\deg(f)$ of f as the degree of its reduced form. The support of f is the set $\{x \in \mathbb{F}_q^m : f(x) \neq 0\}$ and we denote by $|f|$ the cardinal of its support (by identifying canonically B_m^q and $\mathbb{F}_q^{q^m}$, $|f|$ is actually the Hamming weight of f).

For $0 \leq r \leq m(q-1)$, the rth order generalized Reed-Muller code of length q^m is

$$R_q(r,m) := \{f \in B_m^q : \deg(f) \leq r\}.$$

For $1 \leq r \leq m(q-1)-2$, the automorphism group of generalized Reed-Muller codes $R_q(r,m)$ is the affine group of $\mathbb{F}_q^m$ (see [2]).

For more results on generalized Reed-Muller codes, we refer to [7].

In the following of the article, we write $r = t(q-1)+s$, $0 \leq t \leq m-1$, $0 \leq s \leq q-2$.

In [10], interpreting generalized Reed-Muller codes in terms of BCH codes, it is proved that the minimal weight of the generalized Reed-Muller code $R_q(r,m)$ is $(q-s)q^{m-t-1}$.

The following theorem gives the minimum weight codewords of generalized Reed-Muller codes and is proved in [7] (see also [12]).

Theorem 1 *Let $r = t(q-1)+s < m(q-1)$, $0 \leq s \leq q-2$. The minimal weight codewords of $R_q(r,m)$ are codewords whose support is the union of $(q-s)$ distinct parallel affine subspaces of codimension $t+1$ included in an affine subspace of codimension t.*

In his Ph.D thesis [8], Erickson proves that if we know the second weight of $R_q(s,2)$, then we know the second weight for all generalized Reed-Muller codes. From a conjecture on blocking sets, Erickson conjectures that the second weight of $R_q(s,2)$ is $(q-s)q+s-1$. Bruen proves the conjecture on blocking set in [5]. Geil also proves this result in [9] using Groebner basis. An altenative approach can be found in [13] where the second weight of most $R_q(r,m)$ is established without using Erickson's results.

Theorem 2 *For $m \geq 3$, $q \geq 3$ and $q \leq r \leq (m-1)(q-1)$ the second weight W_2 of the generalized Reed-Muller codes $R_q(r,m)$ satisfies:*

1. *if $1 \leq t \leq m-1$ and $s = 0$,*

$$W_2 = 2(q-1)q^{m-t-1};$$

2. *if $1 \leq t \leq m-2$ and $s = 1$,*
   (a) *if $q = 3$, $W_2 = 8 \times 3^{m-t-2}$,*
   (b) *if $q \geq 4$, $W_2 = q^{m-t}$,*
3. *if $1 \leq t \leq m-2$ and $2 \leq s \leq q-2$,*

$$W_2 = (q-s+1)(q-1)q^{m-t-2}.$$

In [6], Cherdieu and Rolland prove that the codewords of $R_q(s,m)$ of weight $(q-s+1)(q-1)q^{m-2}$, $2 \leq s \leq q-2$, which are the product of s polynomials of degree 1 are of the following form.

Theorem 3 *Let $m \geq 2$, $2 \leq s \leq q-2$ and $f \in R_q(s,m)$ such that $|f| = (q-s+1)(q-1)q^{m-2}$; we denote by S the support of f. Assume f is the product of s polynomials of degree 1 then either S is the union of $q-s+1$ parallel affine hyperplanes minus their intersection with an affine hyperplane which is not parallel or S is the union of $(q-s+1)$ affine hyperplanes which meet in a common affine subspace of codimension 2 minus this intersection.*

In [14], Sboui proves that the only codewords of $R_q(s,m), 2 \leq s \leq \frac{q}{2}$ whose weight is $(q-s+1)(q-1)q^{m-2}$ are these codewords. The case where $q=2$ is proved in [11]. In [1], Ballet and Rolland prove that a codeword with an irreducible but not absolutely irreducible factor of degree greater than 1 over $\mathbb{F}_q$ is not a second weight codeword.

All the results proved in this paper are summarized in Section 2 and their proofs are in the following sections.

2 Results

2.1 Description of second weight codewords of generalized Reed-Muller codes

The following theorems and propositions describe the second weight codewords of generalized Reed-Muller code $R_q(r,m)$ for $q \geq 3$, $m \geq 2$, and $1 \leq r \leq m(q-1)-1$. We recall that we write $r = t(q-1)+s$ where $0 \leq t \leq m-1$ and $0 \leq s \leq q-2$.

2.1.1 Case where $t = m-1$ and $s \neq 0$

Theorem 4 *Let $m \geq 2$, $q \geq 5$, $1 \leq s \leq q-4$. Up to affine transformation, the second weight codewords of $R_q((m-1)(q-1)+s,m)$ are of the form*

$$\forall x = (x_1,\ldots,x_m) \in \mathbb{F}_q^m \quad f(x) = \alpha \prod_{i=1}^{m-1}\left(1-x_i^{q-1}\right)\prod_{j=1}^{s-1}(x_m - b_j)$$

where $\alpha \in \mathbb{F}_q^*$ and $b_j \in \mathbb{F}_q$ are such that if $j \neq k$, $b_j \neq b_k$.

Proposition 1 *Let $m \geq 2$ and $q \geq 4$. Up to affine transformation, the second weight codewords of $R_q((m-1)(q-1)+q-3,m)$ are either of the form*

$$\forall x = (x_1,\ldots,x_m) \in \mathbb{F}_q^m \quad f(x) = \alpha \prod_{i=1}^{m-1}\left(1-x_i^{q-1}\right)\prod_{i=1}^{q-4}(x_m - b_i)$$

where $\alpha \in \mathbb{F}_q^*$ and $b_j \in \mathbb{F}_q$ are such that if $j \neq k$, $b_j \neq b_k$ or

$$\forall x = (x_1,\ldots,x_m) \in \mathbb{F}_q^m \quad f(x) = \alpha \prod_{i=1}^{m-2}\left(1-x_i^{q-1}\right)\prod_{i=1}^{q-1}(a_i x_{m-1} + b_i x_m)\prod_{i=1}^{q-3}(x_m - c_i)$$

where $\alpha \in \mathbb{F}_q^*$, $(a_j, b_j) \in \mathbb{F}_q^2 \setminus \{(0,0)\}$ *and* $c_j \in \mathbb{F}_q^*$ *are such that if* $j \neq k$ $c_j \neq c_k$ *or of the form* $\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m$

$$f(x) = \alpha \prod_{i=1}^{m-2} \left(1 - x_i^{q-1}\right) \prod_{i=1}^{q-1} (a_i x_{m-1} + b_i x_m) \prod_{i=1}^{q-4} (x_m - c_i)(a x_{m-1} + b x_m + c)$$

where $\alpha \in \mathbb{F}_q^*$, $(a_j, b_j) \in \mathbb{F}_q^2 \setminus \{(0,0)\}$, $c_j \in \mathbb{F}_q^*$ *are such that if* $j \neq k$ $c_j \neq c_k$ *and* $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$, $c \in \mathbb{F}_q^*$

Proposition 2 *Let* $m \geq 2$ *and* $q \geq 3$. *If* $q \geq 3$, *up to affine transformation, the second weight codewords of* $R_q((m-1)(q-1)+q-2, m)$ *are of the form* $\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m$

$$f(x) = \alpha \prod_{i=1}^{m-2} \left(1 - x_i^{q-1}\right) \prod_{i=1}^{q-2} (x_{m-1} - b_i) \prod_{i=1}^{q-2} (x_m - c_i)(a x_{m-1} + b x_m + c)$$

where $\alpha \in \mathbb{F}_q^*$, $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q^*$, $c \in \mathbb{F}_q$ *and* $b_j \in \mathbb{F}_q$, $c_j \in \mathbb{F}_q$ *are such that if* $j \neq k$, $b_j \neq b_k$ *and* $c_j \neq c_k$

2.1.2 Case where $0 \leq t \leq m-2$ *and* $2 \leq s \leq q-2$

Theorem 5 *Let* $q \geq 4$, $m \geq 2$, $0 \leq t \leq m-2$, $2 \leq s \leq q-2$. *Up to affine transformation, the second weight codewords of* $R_q(t(q-1)+s, m)$ *are either of the form*

$$\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m \quad f(x) = \alpha \prod_{i=1}^{t} \left(1 - x_i^{q-1}\right) \prod_{j=1}^{s-1} (x_{t+1} - b_j)(x_{t+2} - c)$$

where $\alpha \in \mathbb{F}_q^*$, $b_j \in \mathbb{F}_q$ *are such that if* $j \neq k$, $b_j \neq b_k$ *and* $c \in \mathbb{F}_q$ *or of the form*

$$\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m \quad f(x) = \alpha \prod_{i=1}^{t} \left(1 - x_i^{q-1}\right) \prod_{j=1}^{s} (a_j x_{t+1} + b_j x_{t+2} + c_j)$$

where $\alpha \in \mathbb{F}_q^*$ *and* $(a_j, b_j) \in \mathbb{F}_q^2 \setminus \{(0,0)\}$, $c_j \in \mathbb{F}_q$ *such that*

$$A = \bigcap_{j=1}^{s} \{(x_{t+1}, x_{t+2}, \ldots, x_m) : a_j x_{t+1} + b_j x_{t+2} + c_j = 0\} \neq \emptyset$$

and $\dim(A) = m - t - 2$.

2.1.3 Case where $s = 0$

Theorem 6 *Let* $m \geq 2$, $q \geq 3$, $1 \leq t \leq m-1$. *Up to affine transformation, the second weight codewords of* $R_q(t(q-1), m)$ *are either of the form*

$$\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m \quad f(x) = \alpha \prod_{i=1}^{t-1} \left(1 - x_i^{q-1}\right) \prod_{j=1}^{q-2} (x_t - b_j)(x_{t+1} - c)$$

where $\alpha \in \mathbb{F}_q^*$, $b_j \in \mathbb{F}_q$ *are such that if* $j \neq k$, $b_j \neq b_k$ *and* $c \in \mathbb{F}_q$ *or of the form*

$$\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m \quad f(x) = \alpha \prod_{i=1}^{t-1} \left(1 - x_i^{q-1}\right) \prod_{j=1}^{q-1} (a_j x_t + b_j x_{t+1} + c_j)$$

where $\alpha \in \mathbb{F}_q^*$ *and* $(a_j, b_j) \in \mathbb{F}_q^2 \setminus \{(0,0)\}$, $c_j \in \mathbb{F}_q$ *such that*

$$A = \bigcap_{j=1}^{q-1} \{(x_t, x_{t+1}, \ldots, x_m) : a_j x_t + b_j x_{t+1} + c_j = 0\} \neq \emptyset$$

and $\dim(A) = m - t - 1$.

2.1.4 Case where $0 \leq t \leq m-2$ and $s = 1$

Theorem 7 *Let* $q \geq 4$, $m \geq 1$, $0 \leq t \leq m-1$. *Up to affine transformation, the second weight codewords of* $R_q(t(q-1)+1, m)$ *are of the form*

$$\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m \quad f(x) = \alpha \prod_{i=1}^{t} \left(1 - x_i^{q-1}\right)$$

where $\alpha \in \mathbb{F}_q^*$.

Proposition 3 *Let* $m \geq 3$, $q = 3$, $1 \leq t \leq m-2$. *Up to affine transformation, the second weight codewords of* $R_3(2t+1, m)$ *are of the form*

$$\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m \quad f(x) = \alpha \prod_{i=1}^{t-1} \left(1 - x_i^2\right) x_t x_{t+1} x_{t+2}$$

where $\alpha \in \mathbb{F}_3^*$.

Remark 1 For $q = 3$, in the case where $r = 1$, the second weight of $R_3(1, m)$ is 3^m and the second weight codewords are degree zero codewords.

Remark 2 From the above theorems, it follows that second weight codewords of generalized Reed-Muller codes are product of degree 1 factors.

2.2 Strategy of proof

In the following, except when another affine space is specified, a hyperplane or a subspace is, respectively, an affine hyperplane or an affine subspace of $\mathbb{F}_q^m$.

It is easy to verify that the codewords described above are second weight codewords. Using the following lemma and its corollary from [7], we deduce that these codewords are exactly the second weight codewords from the results on the structure of the support of second weight codewords below.

Lemma 1 *Let $m \geq 1$, $q \geq 2$, $f \in B_m^q$ and $a \in \mathbb{F}_q$. If for all $(x_2, \ldots, x_m)$ in $\mathbb{F}_q^{m-1}$, $f(a, x_2, \ldots, x_m) = 0$ then for all $(x_1, \ldots, x_m) \in \mathbb{F}_q^m$,*

$$f(x_1, \ldots, x_m) = (x_1 - a)g(x_1, \ldots, x_m)$$

with $\deg_{x_1}(g) \leq \deg_{x_1}(f) - 1$.

Corollary 1 *Let $m \geq 1$, $q \geq 2$, $f \in B_m^q$ and $a \in \mathbb{F}_q$. If for all $(x_1, \ldots, x_m)$ in $\mathbb{F}_q^m$ such that $x_1 \neq a$, $f(x_1, \ldots, x_m) = 0$ then for all $(x_1, \ldots, x_m) \in \mathbb{F}_q^m$, $f(x_1, \ldots, x_m) = (1 - (x_1 - a)^{q-1})g(x_2, \ldots, x_m)$.*

2.2.1 Case where $t = m - 1$ and $s \neq 0$

Theorem 4 comes from

Theorem 8 *Let $m \geq 2$, $q \geq 5$, $1 \leq s \leq q - 4$ and $f \in R_q((m-1)(q-1) + s, m)$ such that $|f| = q - s + 1$. Then the support of f is included in a line.*

Propositions 1 and 2 come from

Proposition 4 *Let $m \geq 2$. If $q \geq 4$ and $f \in R_q((m-1)(q-1) + q - 3, m)$ such that $|f| = 4$ or $q \geq 3$ and $f \in R_q((m-1)(q-1) + q - 2, m)$ such that $|f| = 3$, then the support of f is included in an affine plane.*

Indeed, in both cases, since the support of f is included in an affine plane, up to affine transformation, $\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m$,

$$f(x) = \prod_{i=1}^{m-2} \left(1 - x_i^{q-1}\right) g(x_{m-1}, x_m)$$

where $g \in R_q(u, 2)$, $u \in \{2q - 4, 2q - 3\}$.

Consider the case of Proposition 1. If the support of f is included in a line then f is a minimum weight codeword of $R_q((m-1)(q-1) + q - 4, m)$ and we get the first case of the Proposition. Assume that 3 points of the support are included in a line L. We denote by A the point of the support which is not in L and by B, C , D the 3 other points. We define a point E such that $ABDE$ is a parallelogram.

Then considering the lines parallel to (AB) and those parallel to (AD) which do not contain any point of the support, the line parallel to (BD) through E and the line L and L' (see Fig. 1), we get that up to affine transformation g is of the form $\prod_{i=1}^{q-3}(x_{m-1} - b_i) \prod_{i=1}^{q-3}(x_m - c_i) \prod_{i=1}^{3}(\alpha_i x_{m-1} + \beta_i x_m + \gamma_i)$ where $b_i \in \mathbb{F}_q$, $c_i \in \mathbb{F}_q$ are such that if $j \neq k$, $b_j \neq b_k$, $c_j \neq c_k$ and $\alpha_i \in \mathbb{F}_q^*$, $\beta_i \in \mathbb{F}_q^*$, $\gamma_i \in \mathbb{F}_q$. So $f \in R_q((m-1)(q-1) + q - 2, m)$ and this case is not possible.

In the other cases, the four points of the support form a quadrilateral, we denote by M the intersection of the diagonals of this quadrilateral. By applying an affine transformation, we can assume that $M = (0, 0)$.

If at least two of the edges of this quadrilateral are parallel, considering all the lines through M which do not contain any point of the support and all the lines parallel to

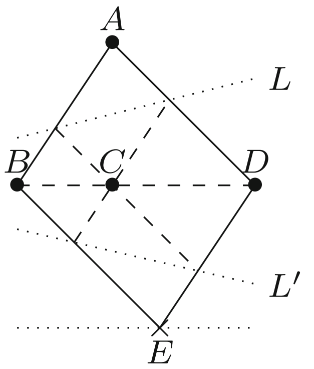

Fig. 1 Proposition 1, case where 3 points of the support are included in a line

these edges which contain neither M nor any point of the support, we get that f is of the second form in Proposition 1.

In the last case, we denote by A, B, C, D the vertices of the quadrilateral and by C' (respectively D') the intersection of the diagonal (BD) (respectively (AC)) with the line parallel to (AB) through C (respectively D). Then considering all the lines through M which do not contain any point of the support, all the lines parallel to (AB) which do not contain any point of the support and the line $(C'D')$, we get that f is of the third form in Proposition 1.

Consider now the case of Proposition 2. Denote by A, B, C the 3 points of the support and define D a point such that $ABCD$ is a parallelogram. Considering the line through D parallel to (AC) we get that f is of the form described in the Proposition.

2.2.2 Case where $0 \leq t \leq m-2$ and $2 \leq s \leq q-2$

Theorem 5 comes from

Theorem 9 *Let $q \geq 4$, $m \geq 2$, $0 \leq t \leq m-2$, $2 \leq s \leq q-2$. The second weight codewords of $R_q(t(q-1)+s, m)$ are codewords whose support S is included in an affine subspace of codimension t and either S is the union of $q-s+1$ parallel affine subspaces of codimension $t+1$ minus their intersection with an affine subspace of codimension $t+1$ which is not parallel or S is the union of $(q-s+1)$ affine subspaces of codimension $t+1$ which meet in an affine subspace of codimension $t+2$ minus this intersection (see Fig. 2).*

2.2.3 Case where $s = 0$

Theorem 6 comes from:

Theorem 10 *Let $m \geq 2$, $q \geq 3$, $1 \leq t \leq m-1$. The second weight codewords of $R_q(t(q-1), m)$ are codewords whose support S is included in an affine subspace of codimension $t-1$ and either S is the union of 2 parallel affine subspaces of codimension t minus their intersection with an affine subspace of codimension t which is not parallel or S is the union of two non parallel affine subspaces of codimension t minus their intersection.*

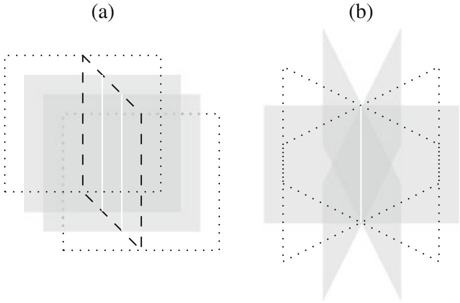

Fig. 2 The possible support for a second weight codeword of $R_4(5, 3)$

2.2.4 Case where $0 \le t \le m-2$ *and* $s = 1$

Theorem 7 comes from

Theorem 11 *For* $q \ge 4$, $m \ge 1$, $0 \le t \le m-1$, *if* $f \in R_q(t(q-1)+1, m)$ *is such that* $|f| = q^{m-t}$, *the support of* f *is an affine subspace of codimension* t.

Proposition 3 comes from

Proposition 5 *Let* $m \ge 3$, $q = 3$, $1 \le t \le m-2$ *and* $f \in R_3(2t+1, m)$ *such that* $|f| = 8.3^{m-t-2}$. *We denote by* S *the support of* f. *Then* S *is included in* A *an affine subspace of dimension* $m-t+1$, S *is the union of two parallel hyperplanes of* A *minus their intersection with two non parallel hyperplanes of* A *(see Fig. 3).*

3 A preliminary lemma

Lemma 2 *Let* $q \ge 3$, $m \ge 3$, *and* S *be a set of points of* $\mathbb{F}_q^m$ *such that* $\#S = u.q^n < q^m$, *with* $u \not\equiv 0 \mod q$. *Assume for all hyperplanes* H *either* $\#(S \cap H) = 0$ *or* $\#(S \cap H) = v.q^{n-1}$, $v < u$ *or* $\#(S \cap H) \ge u.q^{n-1}$ *Then there exists* H *an affine hyperplane such that* S *does not meet* H *or such that* $\#(S \cap H) = vq^{n-1}$.

Proof Assume for all H hyperplane, $S \cap H \ne \emptyset$ and $\#(S \cap H) \ne vq^{n-1}$. Consider an affine hyperplane H; then for all H' hyperplane parallel to H, $\#(S \cap H') \ge u.q^{n-1}$.

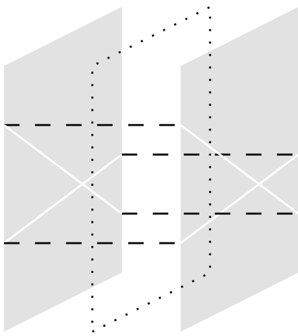

Fig. 3 The support of a second weight codeword of $R_3(3, 3)$

Since $u.q^n = \#S = \sum_{H'//H} \#(S \cap H')$, we get that for all H hyperplane, $\#(S \cap H) = u.q^{n-1}$.

Now consider A an affine subspace of codimension 2 and the $(q+1)$ hyperplanes through A. These hyperplanes intersect only in A and their union is equal to $\mathbb{F}_q^m$. So

$$uq^n = \#S = (q+1)u.q^{n-1} - q\#(S \cap A).$$

Finally we get a contradiction if $n = 1$. Otherwise, $\#(S \cap A) = u.q^{n-2}$. Iterating this argument, we get that for all A affine subspace of codimension $k \leq n$, $\#(S \cap A) = u.q^{n-k}$.

Let A be an affine subspace of codimension $n+1$ and A' an affine subspace of codimension $n-1$ containing A. We consider the $(q+1)$ affine subspace of codimension n containing A and included in A', then

$$u.q = \#(S \cap A') = (q+1)u - q\#(S \cap A)$$

which is absurd since $\#(S \cap A)$ is an integer and $u \not\equiv 0 \mod q$. So there exists H_0 an hyperplane such that $\#(S \cap H_0) = vq^{n-1}$ or S does not meet H_0. □

Remark 3 This lemma applies in particular when S is the support of a second weight codeword and vq^n is the minimal weight.

4 Case where $t = m - 1$ and $s \neq 0$

4.1 Proof of Theorem 8

We recall that S is the support of f. Let $\omega_1, \omega_2 \in S$ and H be an affine hyperplane containing ω_1 and ω_2. Assume $S \cap H \neq S$. We have $\#S = q - s + 1 \leq q$ and $\omega_1, \omega_2 \in S \cap H$, so there exists an affine hyperplane parallel to H which does not meet S. Since the affine group is the automorphism group of generalized Reed-Muller codes, we can apply an affine transformation without changing the weight of a codeword. So, we can assume $x_1 = 0$ is an equation of H and we denote by H_a the affine hyperplane parallel to H of equation $x_1 = a$, $a \in \mathbb{F}_q$. Let $I := \{a \in \mathbb{F}_q : S \cap H_a = \emptyset\}$ and denote by $k := \#I$; $s \leq k \leq q - 2$. Let $c \notin I$, we define

$$\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m,\ \ f_c(x) = f(x) \prod_{a \notin I, a \neq c} (x_1 - a)$$

that is to say f_c is a function in B_m^q such that its support is $S \cap H_c$. Since $c \notin I$, f_c is not identically zero. Then $|f| = \sum_{c \notin I} |f_c|$ and we consider two cases.

- Assume $k > s$.
  Then the reduced form of f_c has degree at most $(m-1)(q-1) + q - 1 + s - k$ and $|f_c| \geq k - s + 1$. Then,

$$(q - s + 1) = |f| = \sum_{c \notin I} |f_c| \geq (q - k)(k - s + 1)$$

which gives

$$1 \geq (q-1-k)(k-s)$$

this is possible if and only if $k = q-2 = s+1$ and we get a contradiction since $s \leq q-4$.

– Assume $k = s$.
Then S meets $(q-s-1)$ affine hyperplanes parallel to H in 1 point and H in 2 points. Consider the function g in B_m^q defined by

$$\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m,\ g(x) = x_1 f(x).$$

The reduced form of g has degree at most $(m-1)(q-1)+s+1$ and

$$|g| = (q-s-1).$$

So g is a minimum weight codeword of $R_q((m-1)(q-1)+s+1, m)$ and its support is included in a line. This line is not included in H. So consider H_1 an affine hyperplane which contains this line but does not contain both ω_1 and ω_2. Then $S \cap H_1 \neq S$ and H_1 contains at least 3 points of S since $s \leq q-4$ which gives a contradiction by applying the previous argument to H_1.

So S is included in all affine hyperplanes through ω_1 and ω_2 which gives the result.

4.2 Proof of Proposition 4

– If $f \in R_q((m-1)(q-1)+q-2, m)$ is such that $|f| = 3$, we have the result since 3 points are always included in an affine plane.

– Assume $f \in R_q((m-1)(q-1)+q-3, m)$ is such that $|f| = 4$. By Corollary 1, there exist $a, b, c, d \in \mathbb{F}_q^*$ and $\omega^{(a)} = (\omega_1^{(a)}, \ldots, \omega_m^{(a)})$, $\omega^{(b)} = (\omega_1^{(b)}, \ldots, \omega_m^{(b)})$, $\omega^{(c)} = (\omega_1^{(c)}, \ldots, \omega_m^{(c)})$, $\omega^{(d)} = (\omega_1^{(d)}, \ldots, \omega_m^{(d)})$ 4 distinct points of $\mathbb{F}_q^m$ such that $\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m$,

$$f(x) = a\prod_{i=1}^{m}\left(1-\left(x_i-\omega_i^{(a)}\right)^{q-1}\right) + b\prod_{i=1}^{m}\left(1-\left(x_i-\omega_i^{(b)}\right)^{q-1}\right)$$
$$+c\prod_{i=1}^{m}\left(1-\left(x_i-\omega_i^{(c)}\right)^{q-1}\right) + d\prod_{i=1}^{m}\left(1-\left(x_i-\omega_i^{(d)}\right)^{q-1}\right).$$

So,

$$f(x) = (-1)^m(a+b+c+d)\prod_{i=1}^{m} x_i^{q-1}$$
$$+(-1)^{m-1}\sum_{i=1}^{m}\left(a\omega_i^{(a)} + b\omega_i^{(b)} + c\omega_i^{(c)} + d\omega_i^{(d)}\right)x_i^{q-2}\prod_{j\neq i} x_j^{q-1} + r$$

with $\deg(r) \leq (m-1)(q-1)+q-3$. Since $f \in R_q((m-1)(q-1)+q-3, m)$,

$$\begin{cases} a+b+c+d = 0 \\ a\omega^{(a)} + b\omega^{(b)} + c\omega^{(c)} + d\omega^{(d)} = 0 \end{cases}.$$

So, $a\overrightarrow{\omega^{(d)}\omega^{(a)}} + b\overrightarrow{\omega^{(d)}\omega^{(b)}} + c\overrightarrow{\omega^{(d)}\omega^{(c)}} = \overrightarrow{0}$ which gives the result.

Remark 4 In both cases we cannot prove that the support of f is included in a line. Indeed,

- Let $\omega_1, \omega_2, \omega_3$ be 3 points of $\mathbb{F}_q^m$ not included in a line. For $q \geq 3$ we can find a, $b \in \mathbb{F}_q^*$ such that $a + b \neq 0$. Let $f = a1_{\omega_1} + b1_{\omega_2} - (a+b)1_{\omega_3}$ where for $\omega \in \mathbb{F}_q^m$, 1_ω is the function from $\mathbb{F}_q^m$ to $\mathbb{F}_q$ such that $1_\omega(\omega) = 1$ and $1_\omega(x) = 0$ for all $x \neq \omega$. Then, since $\sum_{x \in \mathbb{F}_q^m} f(x) = a + b - (a+b) = 0$, $f \in R_q((m-1)(q-1) + q - 2, m)$.
- Let $\omega_1, \omega_2, \omega_3$ be 3 points of $\mathbb{F}_q^m$ not included in a line and set

$$\omega_4 = \omega_1 + \omega_2 - \omega_3.$$

Then $f = 1_{\omega_1} + 1_{\omega_2} - 1_{\omega_3} - 1_{\omega_4} \in R_q((m-1)(q-1) + q - 3, m)$.

5 Case where $0 \leq t \leq m-2$ and $2 \leq s \leq q-2$

5.1 Case where $t = 0$

In this subsection, we write $r = a(q-1) + b$ with $0 \leq a \leq m-1$ and $0 < b \leq q-1$.

Lemma 3 *Let $q \geq 3$, $m \geq 2$, $0 \leq a \leq m-2$, $2 \leq b \leq q-1$ and $f \in R_q(a(q-1) + b, m)$ such that $|f| = (q-b+1)(q-1)q^{m-a-2}$; we denote by S the support of f. If H is an affine hyperplane of $\mathbb{F}_q^m$ such that $S \cap H \neq \emptyset$ and $S \cap H \neq S$ then either S meets all affine hyperplanes parallel to H or S meets $q-b+1$ affine hyperplanes parallel to H in $(q-1)q^{m-a-2}$ points or S meets $q-1$ affine hyperplanes parallel to H in $(q-b+1)q^{m-a-2}$ points.*

Proof By applying an affine transformation, we can assume $x_1 = 0$ is an equation of H and consider the q affine hyperplanes H_w of equation $x_1 = w$, $w \in \mathbb{F}_q$, parallel to H. Let $I := \{w \in \mathbb{F}_q : S \cap H_w = \emptyset\}$ and denote by $k := \#I$. Assume $k \geq 1$. Since $S \cap H \neq \emptyset$ and $S \cap H \neq S$, $k \leq q-2$. For all $c \in \mathbb{F}_q$, $c \notin I$, we define

$$\forall x = (x_1, \ldots, x_n) \in \mathbb{F}_q^m,\ \ f_c(x) = f(x) \prod_{w \in \mathbb{F}_q, w \neq c, w \notin I} (x_1 - w).$$

- Assume $b < k$.
  Then $2 \leq q - 1 + b - k \leq q-2$ and for all $c \notin I$, the reduced form of f_c has degree at most $a(q-1) + q - 1 + b - k$. So $|f_c| \geq (k-b+1)q^{m-a-1}$. Hence

$$(q-1)(q-b+1)q^{m-a-2} \geq (q-k)(k-b+1)q^{m-a-1}$$

  which means that $(b-k)q(q-k-1) + b - 1 \geq 0$. However $(b-k) \leq -1$ and $q - k - 1 \geq 1$ so $(b-k)q(q-k-1) + b - 1 < 0$ which gives a contradiction.
- Assume $b \geq k$.
  Then $0 \leq b - k \leq q-2$ and for all $c \notin I$, the reduced form of f_c has degree at most $(a+1)(q-1) + b - k$. So $|f_c| \geq (q-b+k)q^{m-a-2}$. Hence

$$(q-1)(q-b+1)q^{m-a-2} \geq (q-k)(q-b+k)q^{m-a-2}$$

  with equality if and only if for all $c \notin I$, $|f_c| = (q-b+k)q^{m-a-2}$. Finally, we obtain that $(k-1)(k-b+1) \geq 0$ which is possible if and only if $k = 1$ or $1 \geq$

$b - k \geq 0$. Now, we have to show that $k = s$ is impossible to prove the lemma. If $b = q - 1$, since $k \leq q - 2$, we have the result. Assume $b \leq q - 2$ and $b = k$. Then, for all $c \notin I$, $f_c \in R_q((a+1)(q-1), m)$. The minimum weight of $R_q((a+1)(q-1), m)$ is q^{m-a-1} and its second weight is $2(q-1)q^{m-a-2}$. We denote by $N_1 := \#\{c \notin I : |f_c| = q^{m-a-1}\}$. Since $k = b$, $N_1 \leq q - b$. Furthermore, we have

$$(q-b+1)(q-1)q^{m-a-2} \geq N_1 q^{m-a-1} + (q-b-N_1)2(q-1)q^{m-a-2}$$

which means that $N_1 \geq \frac{(q-1)(q-b-1)}{q-2} > q - b - 1$. Finally, $N_1 = q - b$ and for all $c \notin I$, $|f_c| = q^{m-a-1}$. However $(q-1)(q-b+1)q^{m-a-2} > (q-b)q^{m-a-1}$ which gives a contradiction. □

Lemma 4 *For $m = 2$, $q \geq 3$, $2 \leq b \leq q-1$. The second weight codewords of $R_q(b, 2)$ are codewords of $R_q(b, 2)$ whose support S is the union of $q - b + 1$ parallel lines minus their intersection with a line which is not parallel or S is the union of $(q - b + 1)$ lines which meet in a point minus this point.*

Proof To prove this lemma, we use some results on blocking sets proved by Erickson in [8] and Bruen in [5]. All these results are recalled in the Appendix of this paper. By Theorem 3, which is also true for $b = q - 1$ (see [8, Lemma 3.12]), it is sufficient to prove that $f \in R_q(b, 2)$ such that $|f| = (q - b + 1)(q - 1)$ is the product of linear factors.

Let $f \in R_q(b, 2)$ such that $|f| \leq (q - b + 1)(q - 1) = q(q - b) + b - 1$. We denote by S its support. Then, S is not a blocking set of order $(q - b)$ of $\mathbb{F}_q^2$ (Theorem 13) and f has a linear factor (Lemma 10).

We proceed by induction on b. If $b = 2$ and $f \in R_q(b, 2)$ is such that $|f| \leq (q - b + 1)(q - 1)$, then f has a linear factor and by Lemma 1 f is the product of two linear factors. Assume if $f \in R_q(b - 1, 2)$ is such that $|f| \leq (q - b + 2)(q - 1)$ then f is a product of linear factors. Let $f \in R_q(b, 2)$ such that $|f| \leq (q - b + 1)(q - 1)$; then f has a linear factor. By applying an affine transformation, we can assume for all $(x, y) \in \mathbb{F}_q^2$, $f(x, y) = y\widetilde{f}(x, y)$ with $\deg(\widetilde{f}) \leq b - 1$. So, L the line of equation $y = 0$ does not meet S the support of f. Since $(q - b + 1)(q - 1) > q$, S is not included in a line and by Lemma 3, either S meets $(q - b + 1)$ lines parallel to L in $(q - 1)$ points or S meets $(q - 1)$ lines parallel to L in $(q - b + 1)$ points.

In the first case, by Lemma 1, we can write for all $(x, y) \in \mathbb{F}_q^2$,

$$f(x, y) = y(y - a_1)\dots(y - a_{b-2})g(x, y)$$

where a_i, $1 \leq i \leq q - 2$ are $q - 2$ distinct elements of $\mathbb{F}_q^*$ and $\deg(g) \leq 1$ which gives the result.

In the second case, we denote by $a \in \mathbb{F}_q$ the coefficient of x^{s-1} in $\widetilde{f}$. Then for any $\lambda \in \mathbb{F}_q^*$, since S meets all lines parallel to L but L in $q - s + 1$ points, we get for all $x \in \mathbb{F}_q$,

$$f(x, \lambda) = a\lambda(x - a_1(\lambda))\dots(x - a_{b-1}(\lambda))$$

So there exists $a_1, \dots a_{b-1} \in \mathbb{F}_q[Y]$ of degree at most $q - 1$ such that for all $(x, y) \in \mathbb{F}_q^2$,

$$f(x, y) = ay(x - a_1(y))\dots(x - a_{b-1}(y)).$$

Then for all $x \in \mathbb{F}_q$,

$$\widetilde{f}_0(x) = \widetilde{f}(x, 0) = a(x - a_1(0)) \ldots (x - a_{b-1}(0))$$

and $|\widetilde{f}_0| \leq q - 1$. So,

$$|\widetilde{f}| \leq |f| + |\widetilde{f}_0| \leq (q - b + 2)(q - 1).$$

By induction hypothesis, $\widetilde{f}$ is the product of linear factors which finishes the proof of Lemma 4. □

Proposition 6 *For $m \geq 2$, $q \geq 3$, $2 \leq b \leq q - 1$. The second weight codewords of $R_q(b, m)$ are codewords of $R_q(b, m)$ whose support S is the union of $q - b + 1$ parallel hyperplanes minus their intersection with an affine hyperplane which is not parallel or S is the union of $(q - b + 1)$ hyperplanes which meet in an affine subspace of codimension 2 minus this intersection.*

Proof We say that we are in configuration A if S is the union of $q - b + 1$ parallel hyperplanes minus their intersection with an affine hyperplane which is not parallel (see Fig. 2a) and that we are in configuration B if S is the union of $(q - b + 1)$ hyperplanes which meet in an affine subspace of codimension 2 minus this intersection (see Fig. 2b).

We prove this proposition by induction on m. The Lemma 4 proves the case where $m = 2$. Assume $m \geq 3$ and that second weight codeword of $R_q(b, m - 1)$, $2 \leq b \leq q - 1$ are of type A or type B. Let $f \in R_q(b, m)$ such that $|f| = (q - 1)(q - b + 1)q^{m-2}$ and we denote by S its support.

- Assume S meets all affine hyperplanes.
  Then, by Lemma 2, there exists an affine hyperplane H such that $\#(S \cap H) = (q - b)q^{m-2}$. By applying an affine transformation, we can assume $x_1 = 0$ is an equation of H. We denote by 1_H the function in B_m^q such that

  $$\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m,\ 1_H(x) = 1 - x_1^{q-1}$$

  then the reduced form $f.1_H$ has degree at most $(t + 1)(q - 1) + s$ and the support of $f.1_H$ is $S \cap H$ so $S \cap H$ is the support of a minimal weight codeword of $R_q(q - 1 + b, m)$ and $S \cap H$ is the union of $(q - b)$ parallel affine subspaces of codimension 2. Consider P an affine subspace of codimension 2 included in H such that $\#(S \cap P) = (q - b)q^{m-3}$. Assume there are at least two hyperplanes through P which meet S in $(q - b)q^{m-2}$ points. Then, there exists H_1 an affine hyperplane through P different from H such that $\#(S \cap H_1) = (q - b)q^{m-2}$. So, $S \cap H_1$ is the union of $(q - b)$ parallel affine subspaces of codimension 2. Consider G an affine hyperplane which contains Q an affine subspace of codimension 2 included in H which does not meet S and the affine subspace of codimension 2 included in H_1 which meets Q but not S (see Fig. 4).

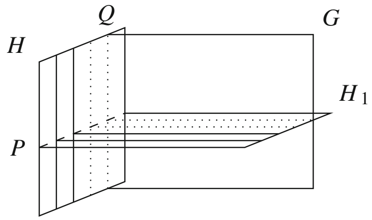

Fig. 4 Proposition 6, case where S meets all affine hyperplanes, construction of G

By applying an affine transformation, we can assume $x_m = \lambda$, $\lambda \in \mathbb{F}_q$ is an equation of an hyperplane parallel to G. For all $\lambda \in \mathbb{F}_q$, we define $f_\lambda \in B^q_{m-1}$ by

$$\forall (x_1, \ldots, x_{m-1}) \in \mathbb{F}_q^{m-1}, \qquad f_\lambda(x_1, \ldots, x_{m-1}) = f(x_1, \ldots, x_{m-1}, \lambda).$$

If all hyperplanes parallel to G meets S in $(q-b+1)(q-1)q^{m-3}$ then for all $\lambda \in \mathbb{F}_q$, f_λ is a second weight codeword of $R_q(b, m-1)$ and its support is of type A or B. We get a contradiction if we consider an hyperplane parallel to G which meets $S \cap H$ and $S \cap H_1$. So, there exits G_1 an hyperplane parallel to G which meets S in $(q-b)q^{m-2}$ points and $S \cap G_1$ is the union of $(q-b)$ parallel affine subspaces of codimension 2 which is a contradiction. Then for all H' hyperplane through P different from H $\#(S \cap H') \geq (q-1)(q-b+1)q^{m-3}$. Furthermore, since

$$(q-b)q^{m-2} + q.(q-1)(q-b+1)q^{m-3}$$
$$-q.(q-b)q^{m-3} = (q-1)(q-b+1)q^{m-2},$$

$\#(S \cap H') = (q-1)(q-b+1)q^{m-3}$. Finally, by applying the same argument to all affine subspaces of codimension 2 included in H parallel to P, we get that all hyperplanes through an affine subspace of codimension 2 parallel to P but H meet S in $(q-1)(q-b+1)q^{m-3}$. Choosing q such hyperplanes, we get q parallel hyperplanes $(G_i)_{1 \leq i \leq q}$ such that for all $1 \leq i \leq q$, $\#(S \cap G_i) = (q-b+1)(q-1)q^{m-3}$ and $\#(S \cap G_i \cap H) = (q-b)q^{m-3}$. Then by induction hypothesis, $S \cap G_i$ is either of type A or of type B.

If there exists i_0 such that $S \cap G_{i_0}$ is of type A. Consider F an affine hyperplane containing R an affine subspace of codimension 2 included in H which does not meet S and the affine subspace of codimension 2 included in G_{i_0} which does not meets S but meets R. If for all F' hyperplane parallel to F, $\#(S \cap F') > (q-b)q^{m-2}$ then $\#(S \cap F') = (q-1)(q-b+1)q^{m-3}$. So $S \cap F'$ is the support of a second weight codeword of $R_q(b, m-1)$ and is either of type A or of type B which is absurd is we consider an hyperplane parallel to F which meets $S \cap H$. So there exits F_1 an affine hyperplane parallel to F which meets S in $(q-b)q^{m-2}$ points. So $S \cap F_1$ is the union of $(q-s)$ parallel affine subspaces of codimension 2 which is absurd since $S \cap G_{i_0}$ is of type A (see Fig. 5).

If for all $1 \leq i \leq q$, $S \cap G_i$ is of type B. Let H_1 be the affine hyperplane parallel to H which contains the affine subspace of codimension 3 intersection of the affine subspaces of codimension 2 of $S \cap G_1$. We consider R an affine subspace of codimension 2 included in H which does not meet S. Then there is $(q-b+1)$ affine hyperplanes through R which meet $S \cap G_1$ in $(q-b)q^{m-3}$. However, if we

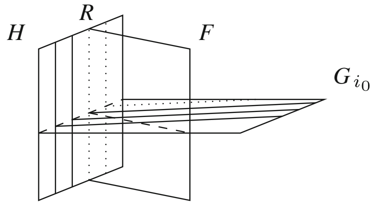

Fig. 5 Proposition 6, case where S meets all affine hyperplanes, there exists G_{i_0} such that $S \cap G_{i_0}$ is of type A

denote by k the number of hyperplanes through R which meet S in $(q-b)q^{m-2}$ points, we have

$$k(q-b)q^{m-2} + (q+1-k)(q-1)(q-b+1)q^{m-3} \leq (q-1)(q-b+1)q^{m-2}$$

which implies that $k \geq q-b+2$. For all H' hyperplane through R such that $\#(S \cap H') = (q-b)q^{m-2}$, $S \cap H'$ is the union of $(q-b)$ affine subspaces of codimension 2 parallel to R and then $\#(S \cap H' \cap G_1) = (q-b)q^{m-3}$ which is absurd (see Fig. 6).

– So, there exists H an affine hyperplane such that H does not meet S.
Then, by Lemma 3, either S meets $(q-1)$ hyperplanes parallel to H in $(q-b+1)q^{m-2}$ points or S meets $(q-b+1)$ hyperplanes parallel to H in $(q-1)q^{m-2}$ points.
If S meets $(q-b+1)$ hyperplanes parallel to H in $(q-1)q^{m-2}$ points, then , for all H' hyperplane parallel to H such that $S \cap H' \neq \emptyset$, $S \cap H'$ is the support of a minimal weight codeword of $R_q(q,m)$ and is the union of $(q-1)$ parallel affine subspaces of codimension 2. Let H' be an affine hyperplane parallel to H such that $S \cap H' \neq \emptyset$. We denote by P the affine subspace of codimension 2 of H' which does not meet S. Consider H_1 an affine hyperplane which contains P and a point not in S of an affine hyperplane H" parallel to H which meets S. Then

$$\#(H_1 \setminus S) \geq bq^{m-2} + 1.$$

However, if $S \cap H_1 \neq \emptyset$, $\#(H_1 \setminus S) \leq bq^{m-2}$. So, $S \cap H_1 = \emptyset$ and we are in configuration A.
If S meets $(q-1)$ hyperplanes parallel to H in $(q-b+1)q^{m-2}$ points. Then for all H' parallel to H different from H, $S \cap H'$ is the support of a minimal weight codeword of $R_q((q-1)+b-1,m)$ and is the union of $(q-b+1)$ parallel affine subspaces of codimension 2. Let H_1 be an affine hyperplane parallel to H

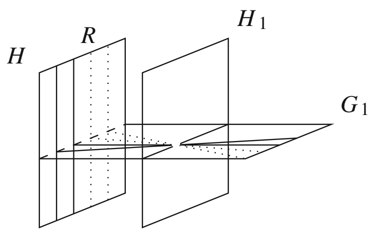

Fig. 6 Proposition 6, case where S meets all affine hyperplanes, for all G_i, $S \cap G_i$ is of type B

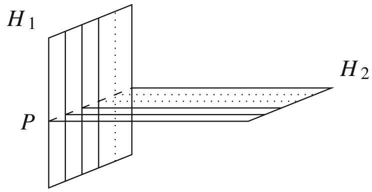

Fig. 7 Proposition 6, case where there exists an affine hyperplane which does not meet S, contruction of (G_i)

different from H and consider P an affine subspace of codimension 2 included in H_1 such that

$$\#(S \cap P) = (q - b + 1)q^{m-3}.$$

Assume there exists H_2 an affine hyperplane through P such that $\#(S \cap H_2) = (q-b)q^{m-2}$. Then $S \cap H_2$ is the support of a minimal weight codeword of $R_q(q-1+b, m)$ and is the union of $(q-b)$ parallel affine subspaces of codimension 2 which is absurd since $S \cap H_2$ meets H_1 in $S \cap P$ (see Fig. 7).
Then, for all H' through P $\#(S \cap H') \geq (q-1)(q-b+1)q^{m-3}$. Furthermore,

$$(q-b+1)q^{m-2} + q.(q-1)(q-b+1)q^{m-3} - q.(q-b+1)q^{m-3}$$
$$= (q-1)(q-b+1)q^{m-2}.$$

So for all H' hyperplane through P different from H_1,

$$\#(S \cap H') = (q-1)(q-b+1)q^{m-3}.$$

By applying the same argument to all affine subspaces of codimension 2 included in H_1 parallel to P, we get q parallel hyperplanes $(G_i)_{1 \leq i \leq q}$ such that for all $1 \leq i \leq q$, $\#(S \cap G_i) = (q-b+1)(q-1)q^{m-3}$ and $\#(S \cap G_i \cap H_1) = (q-s+1)q^{m-3}$. By induction hypothesis, for all $1 \leq i \leq q$, either $S \cap G_i$ is of type A or $S \cap G_i$ is of type B.
Assume there exists i_0 such that $S \cap G_{i_0}$ is of type A. Consider F an affine hyperplane containing Q an affine subspace of codimension 2 included in H_1 which does not meet S and the affine subspace of codimension 2 included in G_{i_0} which does not meets S but meets Q. Assume S meets all hyperplanes parallel to F in at least $(q-b)q^{m-t-2}$. If for all F' parallel to F, $\#(S \cap F') > (q-b)q^{m-2}$ then

$$\#(S \cap F') \geq (q-1)(q-b+1)q^{m-3}.$$

So $S \cap F'$ is the support of a second weight codeword of $R_q(b, m-1)$ and is either of type A or of type B which is absurd is we consider an hyperplane parallel to F which meets $S \cap H_1$ and $S \cap G_{i_0}$. So, there exits F_1 an affine hyperplane parallel to F such that $\#(S \cap F_1) = (q-b)q^{m-2}$. Then, $S \cap F_1$ is the union of $(q-b)$ parallel affine subspaces of codimension 2, which is absurd. Finally, there exists an affine hyperplane parallel to F which does not meet S. By Lemma 3, either S meets $(q-b+1)$ hyperplanes parallel to F in $(q-1)q^{m-2}$ points and we have already seen that in this case S is of type A or S meets $(q-1)$ hyperplanes parallel to F in $(q-b+1)q^{m-2}$ points. In this case, for all F' parallel to F such that $S \cap F' \neq \emptyset$, $S \cap F'$ is the support of a minimal weight codeword of

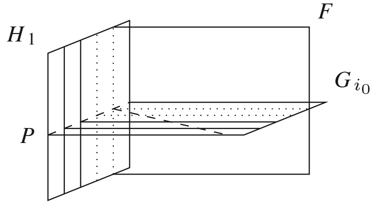

Fig. 8 Proposition 6, case where there exists an affine hyperplane which does not meet S, there exists G_{i_0} such that $S \cap G_{i_0}$ is of type A

$R_q(q-1+b-1, m)$ and is the union of $q-b+1$ parallel affine subspaces of codimension 2, which is absurd since $S \cap G_{i_0}$ is of type A (see Fig. 8).

Now, assume for all $1 \le i \le q$, $G_i \cap S$ is of type B. Let Q be an affine subspace of codimension 2 included in H_1 which does not meets S. Assume S meets all affine hyperplanes through Q and denote by k the number of these hyperplanes which meet S in $(q-b)q^{m-2}$ points. Then,

$$k(q-b)q^{m-2} + (q+1-k)(q-1)(q-b+1)q^{m-3} \le (q-1)(q-b+1)q^{m-2}$$

which means that $k \ge q-b+2$. These $(q-b+2)$ hyperplanes are minimal weight codewords of $R_q(q-1+b, m)$. So, they meet S in $(q-b)$ affine subspaces of codimension 2 parallel to Q, that is to say, they meet $S \cap G_1$ in $(q-b)q^{m-3}$ points. This is absurd since $S \cap G_1$ is of type B and so there are at most $(q-b+1)$ affine hyperplanes through Q which meet $S \cap G_1$ in $(q-b)q^{m-3}$ points (see Fig. 9). So there exists an affine hyperplane through Q which does not meet S.

By applying the same argument to all affine subspaces of codimension 2 included in H_1 which does not meet S, since $S \cap G_i$ is of type B for all i, we get that S is of type B. □

5.2 The support is included in an affine subspace of codimension t.

The two following lemmas are proved in [8].

Lemma 5 *Let $m \ge 2$, $q \ge 3$, $1 \le t \le m-1$, $1 \le s \le q-2$. Assume $f \in R_q(t(q-1)+s, m)$ is such that $\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m$,*

$$f(x) = (1 - x_1^{q-1})\widetilde{f}(x_2, \ldots, x_m)$$

and that $g \in R_q(t(q-1)+s-k)$, $1 \le k \le q-1$, is such that $(1-x_1^{q-1})$ does not divide g. Then, if $h = f+g$, either $|h| \ge (q-s+k)q^{m-t-1}$ or $k = 1$.

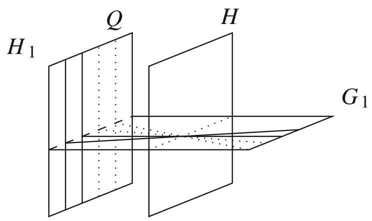

Fig. 9 Proposition 6, case where there exists an affine hyperplane which does not meet S, for all G_i, $S \cap G_i$ is of type B

Lemma 6 *Let $m \geq 2$, $q \geq 3$, $1 \leq t \leq m-1$, $1 \leq s \leq q-2$ and $f \in R_q(t(q-1)+s, m)$. For $a \in \mathbb{F}_q$, the function f_a of B^q_{m-1} defined for all $(x_2, \dots, x_m) \in \mathbb{F}_q^m$ by $f_a(x_2, \dots, x_m) = f(a, x_2, \dots, x_m)$. Assume for a, $b \in \mathbb{F}_q$ f_a is different from the zero function and $(1 - x_2^{q-1})$ divides f_a and that*

$$0 < |f_b| < (q-s+1)q^{m-t-2}.$$

Then there exists T an affine transformation, fixing x_i for $i \neq 2$ such that $(1 - x_2^{q-1})$ divides $(f \circ T)_a$ and $(f \circ T)_b$.

Lemma 7 *Let $m \geq 3$, $q \geq 4$, $1 \leq t \leq m-2$ and $2 \leq s \leq q-2$. If $f \in R_q(t(q-1)+s, m)$ is such that $|f| = (q-s+1)(q-1)q^{m-t-2}$, then the support of f is included in an affine hyperplane of $\mathbb{F}_q^m$.*

Proof We denote by S the support of f. Assume S is not included in an affine hyperplane. Then, by Lemma 2, there exists an affine hyperplane H such that either H does not meet S or H meets S in $(q-s)q^{m-t-2}$. Now, by Lemma 3, since S is not included in an affine hyperplane, either S meets all affine hyperplanes parallel to H or S meets $(q-1)$ affine hyperplanes parallel to H in $(q-s+1)q^{m-t-2}$ or S meets $(q-s+1)$ affine hyperplanes parallel to H in $(q-1)q^{m-t-2}$ points. By applying an affine transformation, we can assume $x_1 = \lambda$, $\lambda \in \mathbb{F}_q$ is an equation of H. We define $f_\lambda \in B^q_{m-1}$ by

$$\forall (x_2, \dots, x_m) \in \mathbb{F}_q^{m-1}, \qquad f_\lambda(x_2, \dots, x_m) = f(\lambda, x_2, \dots, x_m).$$

We set an order $\lambda_1, \dots, \lambda_q$ on the elements of $\mathbb{F}_q$ such that

$$|f_{\lambda_1}| \leq \dots \leq |f_{\lambda_q}|.$$

Then either $|f_{\lambda_1}| = 0$ or $|f_{\lambda_1}| = (q-s)q^{m-t-2}$, that is to say either f_{λ_1} is null or f_{λ_1} is the minimal weight codeword of $R_q(t(q-1)+s, m-1)$ and its support is included in an affine subspace of codimension $t+1$. Since $t \geq 1$, in both cases, the support of f_{λ_1} is included in an affine hyperplane of $\mathbb{F}_q^m$ different from the hyperplane parallel to H of equation $x_1 = \lambda_1$. By applying an affine transformation that fixes x_1, we can assume $(1 - x_2^{q-1})$ divides f_{λ_1}. Since S is not included in an affine hyperplane, there exists $2 \leq k \leq q$ such that $1 - x_2^{q-1}$ does not divide f_{λ_k}. We denote by k_0 the smallest such k.

Assume S meets all affine hyperplanes parallel to H and that

$$|f_{\lambda_{k_0}}| \geq (q-s+k_0-1)q^{m-t-2}.$$

Then

$$\begin{aligned}
|f| &= \sum_{k=1}^{q} |f_{\lambda_k}| \\
&\geq (q-s)q^{m-t-2}(k_0-1) + (q-k_0+1)(q-s+k_0-1)q^{m-t-2} \\
&= (q-s)q^{m-t-1} + (k_0-1)(q-k_0+1)q^{m-t-2} \\
&> (q-s)q^{m-t-1} + (s-1)q^{m-t-2}
\end{aligned}$$

which gives a contradiction. In the cases where S meets $(q-s')$, $s'=1$ or $s'=s-1$, for $1 \leq i \leq s'$, $|f_{\lambda_i}|=0$ and the support of $f_{\lambda_{s'+1}}$ is $S \cap H_{\lambda_{s'+1}}$, where $H_{\lambda_{s'+1}}$ is the hyperplane of equation $x_1=\lambda_{s'+1}$. Since $S \cap H_{\lambda_{s'+1}}$ is the support of a minimum weight codeword of $R_q((t+1)(q-1)+s', m)$, it is included in affine subspace of codimension $t+1$. So in those cases, we can assume $k_0 \geq s'+2$. Finally, $|f_{\lambda_{k_0}}| < (q-s+k_0-1)q^{m-t-2}$.

We write

$$f(x_1, x_2, x_3, \ldots, x_m) = \sum_{i=0}^{q-1} x_2^i g_i(x_1, x_3, \ldots, x_m)$$

$$= h(x_1, x_2, x_3, \ldots, x_m) + (1-x_2^{q-1}) g(x_1, x_3, \ldots, x_m).$$

Since for all $1 \leq i \leq k_0-1$, $1-x_2^{q-1}$ divides f_{λ_i}, for all $(x_2, \ldots, x_m) \in \mathbb{F}_q^{m-1}$, for all $1 \leq i \leq k_0-1$, $h(\lambda_i, x_2, \ldots, x_m)=0$. So, by Lemma 1,

$$f(x_1, x_2, x_3, \ldots, x_m) = (x_1-\lambda_1)\ldots(x_1-\lambda_{k_0-1})\widetilde{h}(x_1, x_2, x_3, \ldots, x_m)$$
$$+(1-x_2^{q-1}) g(x_1, x_3, \ldots, x_m)$$

with $\deg(\widetilde{h}) \leq r-k_0+1$. Then by applying Lemma 5 to $f_{\lambda_{k_0}}$, since

$$|f_{\lambda_{k_0}}| < (q-s+k_0-1)q^{m-t-2},$$

$k_0=2$. This gives a contradiction in the cases where S does not meet all hyperplanes parallel to H. In the case where S meets all hyperplanes parallel to H, by applying Lemma 6, there exists T an affine transformation which fixes x_1 such that $(1-x_2^{q-1})$ divides $(f \circ T)_{\lambda_1}$ and $(f \circ T)_{\lambda_2}$, we set k'_0 the smallest k such that $(1-x_2^{q-1})$ does not divide $(f \circ T)_{\lambda_k}$. Then $k'_0 \geq 3$ and by applying the previous argument to $f \circ T$, we get a contradiction. □

Proposition 7 *Let $m \geq 3$, $q \geq 4$, $1 \leq t \leq m-2$ and $2 \leq s \leq q-2$. If $f \in R_q(t(q-1)+s, m)$ is such that $|f| = (q-1)(q-s+1)q^{m-t-2}$, then the support of f is included in an affine subspace of codimension t.*

Proof We denote by S the support of f. By Lemma 7, S is included in H an affine hyperplane. By applying an affine transformation, we can assume $x_1=0$ is an equation of H. Let $g \in B_{m-1}^q$ defined by

$$\forall x = (x_2, \ldots, x_m) \in \mathbb{F}_q^{m-1}, g(x) = f(0, x_2, \ldots, x_m)$$

and denote by $P \in \mathbb{F}_q[X_2, \ldots, X_m]$ its reduced form. Since

$$\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m,\ f(x) = \left(1-x_1^{q-1}\right) P(x_2, \ldots, x_m),$$

the reduced form of $f \in R_q(t(q-1)+s, m)$ is

$$\left(1-X_1^{q-1}\right) P(X_2, \ldots, X_m).$$

Then $g \in R_q((t-1)(q-1)+s, m-1)$ and

$$|g| = |f| = (q-s+1)(q-1)q^{m-t-2} = (q-1)(q-s+1)q^{m-1-(t-1)-2}.$$

Then, by Lemma 7, if $t \geq 2$, the support of g is included in an affine hyperplane of $\mathbb{F}_q^{m-1}$. By iterating this argument, we get that S is included in an affine subspace of codimension t. □

5.3 Proof of Theorem 9

Let $0 \leq t \leq m-2$, $2 \leq s \leq q-2$ and $f \in R_q(t(q-1)+s, m)$ such that

$$|f| = (q-s+1)(q-1)q^{m-t-2};$$

we denote by S the support of f. Assume $t \geq 1$. By Proposition 7, S is included in an affine subspace G of codimension t. By applying an affine transformation, we can assume

$$G = \{x = (x_1, \dots, x_m) \in \mathbb{F}_q^m : x_i = 0 \text{ for } 1 \leq i \leq t\}.$$

Let $g \in B_{m-t}^q$ defined for all $x = (x_{t+1}, \dots, x_m) \in \mathbb{F}_q^{m-t}$ by

$$g(x) = f(0, \dots, 0, x_{t+1}, \dots, x_m)$$

and denote by $P \in \mathbb{F}_q[X_{t+1}, \dots, X_m]$ its reduced form. Since

$$\forall x = (x_1, \dots, x_m) \in \mathbb{F}_q^m,\ f(x) = \left(1 - x_1^{q-1}\right) \dots \left(1 - x_t^{q-1}\right) P(x_{t+1}, \dots, x_m),$$

the reduced form of $f \in R_q(t(q-1)+s, m)$ is

$$\left(1 - X_1^{q-1}\right) \dots \left(1 - X_t^{q-1}\right) P(X_{t+1}, \dots, X_m).$$

Then $g \in R_q(s, m-t)$ and $|g| = |f| = (q-s+1)(q-1)q^{m-t-2}$. Thus, using the case where $t = 0$, we finish the proof of Theorem 9.

6 Case where $s = 0$

6.1 The support is included in an affine subspace of dimension $m-t+1$

Proposition 8 *Let $q \geq 3$, $m \geq 2$ and $f \in R_q((m-1)(q-1), m)$ such that $|f| = 2(q-1)$. Then, the support of f is included in an affine plane.*

In order to prove this proposition, we need the following lemma.

Lemma 8 *Let $m \geq 3$, $q \geq 4$ and $f \in R_q((m-1)(q-1), m)$ such that $|f| = 2(q-1)$. If H is an affine hyperplane of $\mathbb{F}_q^m$ such that $S \cap H \neq S$, $\#(S \cap H) = N$, $3 \leq N \leq q-1$ and $S \cap H$ is not included in a line then there exists H_1 an affine hyperplane of $\mathbb{F}_q^m$ such that $S \cap H_1 \neq S$, $\#(S \cap H_1) \geq N+1$ and $S \cap H_1$ is not included in a line*

Proof Since $S \cap H \neq S$, by Lemma 3, either S meets $(q-1)$ hyperplanes parallel to H or S meets two hyperplanes parallel to H or S meets all affine hyperplanes parallel to H. If S does not meet all affine hyperplanes parallel to H then $S \cap H$ is the support of a minimal weight codeword of $R_q((m-1)(q-1)+s', m)$, $s' = 1$ or

$s' = q - 2$. In both cases, $S \cap H$ is included in a line which is absurd. So, S meets all affine hyperplanes parallel to H.

By applying an affine transformation, we can assume $x_1 = 0$ is an equation of H. Let $I := \{a \in \mathbb{F}_q : \#(\{x_1 = a\} \cap S) = 1\}$ and $k := \#I$. Since $\#S = 2(q-1)$ and $\#(S \cap H) = N$, $k \geq N$. We define

$$\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m, \quad g(x) = f(x) \prod_{a \notin I} (x_1 - a).$$

Then, $\deg(g) \leq (m-1)(q-1) + q - k$ and $|g| = k$. So, g is a minimal weight codewords of $R_q((m-1)(q-1) + q - k, m)$ and its support is included in a line L which is not included in H. We denote by $\overrightarrow{u}$ a directing vector of L. Let b be the intersection point of H and L and ω_1, ω_2, ω_3 3 points of $S \cap H$ which are not included in a line. Then there exists $\overrightarrow{v}$ and $\overrightarrow{w} \in \{\overrightarrow{b\omega_1}, \overrightarrow{b\omega_2}, \overrightarrow{b\omega_3}\}$ which are linearly independent. Since L is not included in H, $\{\overrightarrow{u}, \overrightarrow{v}, \overrightarrow{w}\}$ are linearly independent. We choose H_1 an affine hyperplane such that $b \in H_1$, $b + \overrightarrow{v} \in H_1$, $L \subset H_1$ but $b + \overrightarrow{w} \notin H_1$. □

Now we can prove the proposition

Proof If $m = 2$, we have the result. Assume $m \geq 3$. Let S be the support of f. Since $\#S = 2(q-1) > q$, S is not included in a line. Let ω_1, ω_2, ω_3 be 3 points of S not included in a line. Let H be an hyperplane such that $\omega_1, \omega_2, \omega_3 \in H$. Assume $S \cap H \neq S$. Then there exists an affine hyperplane H_1 such that $\#(S \cap H_1) \geq q$, $S \cap H_1$ is not included in a line and $S \cap H_1 \neq S$. Indeed, if $q = 3$, we take $H_1 = H$ and for $q \geq 4$, we proceed by induction using the previous Lemma. Then by Lemma 3 either S meets two hyperplanes parallel to H_1 in 2 points or S meets two hyperplanes parallel to H_1 in $q - 1$ points or S meets all affine hyperplanes parallel to H_1. Since $\#(S \cap H_1) \geq q$, S meets all hyperplanes parallel to H_1. Then, we must have

$$q + q - 1 \leq 2(q-1)$$

which is absurd. □

The two following lemmas are proved in [8].

Lemma 9 *Let $m \geq 2$, $q \geq 3$, $1 \leq t \leq m$ and $f \in R_q(t(q-1), m)$ such that $|f| = q^{m-t}$ and $g \in R_q((t(q-1) - k, m)$, $1 \leq k \leq q - 1$, such that $g \neq 0$. If $h = f + g$ then either $|h| = kq^{m-t}$ or $|h| \geq (k+1)q^{m-t}$.*

Lemma 10 *Let $m \geq 2$, $q \geq 3$, $1 \leq t \leq m - 1$ and $f \in R_q(t(q-1), m)$. For $a \in \mathbb{F}_q$, we define the function f_a of B^q_{m-1} by for all $(x_2, \ldots, x_m) \in \mathbb{F}_q^m$, $f_a(x_2, \ldots, x_m) = f(a, x_2, \ldots, x_m)$. If for some a, $b \in \mathbb{F}_q$, $|f_a| = |f_b| = q^{m-t-1}$, then there exists T an affine transformation fixing x_1 such that*

$$(f \circ T)_a = (f \circ T)_b.$$

Proposition 9 *Let $q \geq 3$, $m \geq 2$, $1 \leq t \leq m - 1$. If $f \in R_q(t(q-1), m)$ is such that $|f| = 2(q-1)q^{m-t-1}$ then the support of f is included in an affine subspace of dimension $m - t + 1$.*

Proof For $t = 1$, this is obvious. For the other cases we proceed by recursion on t. Proposition 8 gives the case where $t = m - 1$.

If $m \leq 3$ we have considered all cases. Assume $m \geq 4$. Let $2 \leq t \leq m - 2$. Assume for $f \in R_q((t+1)(q-1), m)$ such that $|f| = 2(q-1)q^{m-t-2}$ the support of f is included in an affine subspace of dimension $m - t$. Let $f \in R_q(t(q-1), m)$ such that $|f| = 2(q-1)q^{m-t-1}$. We denote by S the support of f.

Assume S is not included in an affine subspace of dimension $m - t + 1$. Then there exists H an affine hyperplane of $\mathbb{F}_q^m$ such that $S \cap H \neq S$ and $S \cap H$ is not included in an affine space of dimension $m - t$. By Lemma 3, either S meets all affine hyperplanes parallel to H or S meets $(q-1)$ affine hyperplanes parallel to H in $2q^{m-t-1}$ or S meets two affine hyperplanes parallel to H in $(q-1)q^{m-t-1}$ points.

If S does not meet all hyperplanes parallel to H then $S \cap H$ is the support of a minimal weight codeword of $R_q(t(q-1) + s', m)$, $s' = 1$ or $s' = q - 2$. So $S \cap H$ is included in an affine subspace of dimension $m - t$ which gives a contradiction.

So, S meets all affine hyperplanes parallel to H in at least q^{m-t-1} points. If for all H' parallel to H, $\#(S \cap H') > q^{m-t-1}$ then for all H' parallel to H, $\#(S \cap H') \geq 2(q-1)q^{m-t-2}$. So, for reason of cardinality, $S \cap H$ is the support of a second weight codeword of $R_q((t+1)(q-1), m)$ and by recursion hypothesis $S \cap H$ is included in an affine subspace of dimension $m - t$ which gives a contradiction. So, there exists H_1 an affine hyperplane parallel to H such that $\#(S \cap H_1) = q^{m-t-1}$.

By applying an affine transformation, we can assume $x_1 = \lambda$, $\lambda \in \mathbb{F}_q$ is an equation of H. For $\lambda \in \mathbb{F}_q$, we define $f_\lambda \in B_{m-1}^q$ by

$$\forall (x_2, \ldots, x_m) \in \mathbb{F}_q^{m-1}, \qquad f_\lambda(x_2, \ldots, x_m) = f(\lambda, x_2, \ldots, x_m).$$

We set an order $\lambda_1, \ldots, \lambda_q$ on the elements of $\mathbb{F}_q$ such that

$$|f_{\lambda_1}| \leq \ldots \leq |f_{\lambda_q}|.$$

Since $\#(S \cap H_1) = q^{m-t-1}$ and S meets all hyperplanes parallel to H,

$$|f_{\lambda_1}| = q^{m-t-1}$$

and f_{λ_1} is a minimum weight codeword of $R_q(t(q-1), m-1)$. Let k_0 be the smallest integer such that $|f_{\lambda_{k_0}}| > q^{m-t-1}$. Since $|f| > q^{m-t}$, $k_0 \leq q$. Then by Lemma 10 and applying an affine transformation that fixes x_1, we can assume for all $2 \leq i \leq k_0 - 1$, $f_{\lambda_i} = f_{\lambda_1}$. If we write for all $x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m$,

$$f(x) = f_{\lambda_1}(x_2, \ldots, x_m) + (x_1 - \lambda_1)\widehat{f}(x_1, \ldots, x_m).$$

Then for all $2 \leq i \leq k_0 - 1$, for all $\overline{x} = (x_2, \ldots, x_m) \in \mathbb{F}_q^{m-1}$,

$$f_{\lambda_i}(\overline{x}) = f_{\lambda_1}(\overline{x}) + (\lambda_i - \lambda_1)\widehat{f_{\lambda_i}}(\overline{x}).$$

Since for all $2 \leq i \leq k_0 - 1$, $f_{\lambda_i} = f_{\lambda_1}$, by Lemma 1, we can write for all $x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m$,

$$f(x) = f_{\lambda_1}(x_2, \ldots, x_m) + (x_1 - \lambda_1)\ldots(x_1 - \lambda_{k_0-1})\overline{f}(x_1, \ldots, x_m)$$

with $\deg(\overline{f}) \leq t(q-1) - k_0 + 1$. Now, we have $f_{\lambda_{k_0}} = f_{\lambda_1} + \lambda' \overline{f}_{\lambda_{k_0}}$, $\lambda' \in \mathbb{F}_q^*$. Then, by Lemma 9, either $|f_{\lambda_{k_0}}| \geq k_0 q^{m-t-1}$ or $|f_{\lambda_{k_0}}| = (k_0 - 1)q^{m-t-1}$. Assume $|f_{\lambda_{k_0}}| \geq k_0 q^{m-t-1}$. Then

$$\begin{aligned} |f| &= \sum_{i=1}^{q} |f_{\lambda_i}| \\ &\geq (k_0 - 1)q^{m-t-1} + (q + 1 - k_0)k_0 q^{m-t-1} \\ &= q^{m-t} + (k_0 - 1)(q - k_0 + 1)q^{m-t-1} \\ &> 2(q-1)q^{m-t-1}. \end{aligned}$$

So, $|f_{\lambda_{k_0}}| = (k_0 - 1)q^{m-t-1}$. Since $|f_{\lambda_{k_0}}| > q^{m-t-1}$, $k_0 \geq 3$. Now, we have

$$|f| \geq (k_0 - 1)q^{m-t-1} + (q + 1 - k_0)(k_0 - 1)q^{m-t-1} = (k_0 - 1)(q - k_0 + 2)q^{m-t-1}.$$

So either $k_0 = q$ or $k_0 = 3$.

- Assume $k_0 = q$.
  Since $f_{\lambda_1} = \ldots = f_{\lambda_{q-1}}$ are minimum weight codeword of $R_q(t(q-1), m-1)$, there exists A an affine subspace of dimension $m-t$ of $\mathbb{F}_q^m$ such that for all $1 \leq i \leq q-1$, $S \cap H_i \subset A$, where H_i is the hyperplane parallel to H of equation $x_1 = \lambda_i$. Since S is not included in an affine subspace of dimension $m-t+1$ and $t \geq 2$, there exists an affine hyperplane G containing A such that $S \cap G \neq S$ and there exists $x \in S \cap G$, $x \notin A$. Then $\#(S \cap G) \geq (q-1)q^{m-t-1} + 1$, $S \cap G \neq S$ and $S \cap G$ is not included in an affine subspace of dimension $m-t$. Applying to G the same argument than to H, we get a contradiction.
- So, $k_0 = 3$.
  Then $f_{\lambda_1} = f_{\lambda_2}$ are minimum weight codeword of $R_q(t(q-1), m-1)$ and for reason of cardinality, for all $3 \leq i \leq q$, $|f_{\lambda_i}| = 2q^{m-t-1}$. So, there exists A an affine subspace of dimension $m-t$ of $\mathbb{F}_q^m$ such that for all $1 \leq i \leq 2$, $S \cap H_i \subset A$, where H_i is the hyperplane parallel to H of equation $x_1 = \lambda_i$. Since S is not included in an affine subspace of dimension $m-t+1$ and $t \geq 2$, there exists an affine hyperplane G containing A such that $S \cap G \neq S$ and there exists $x \in S \cap G$, $x \notin A$. Then $\#(S \cap G) \geq 2q^{m-t-1} + 1$, $S \cap G \neq S$ and $S \cap G$ is not included in an affine subspace of dimension $m-t$. Applying to G the same argument than to H, we get a contradiction.

Finally, S is included in an affine subspace of dimension $m-t+1$. □

6.2 Proof of Theorem 10

Let $1 \leq t \leq m-1$ and $f \in R_q(t(q-1), m)$ such that

$$|f| = 2(q-1)q^{m-t-1};$$

we denote by S the support of f. Assume $t \geq 2$. By Proposition 9, S is included in an affine subspace G of codimension $t-1$. By applying an affine transformation, we can assume

$$G = \{x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m : x_i = 0 \text{ for } 1 \leq i \leq t-1\}.$$

Let $g \in B^q_{m-t+1}$ defined for all $x = (x_t, \dots, x_m) \in \mathbb{F}_q^{m-t+1}$ by

$$g(x) = f(0, \dots, 0, x_t, \dots, x_m)$$

and denote by $P \in \mathbb{F}_q[X_t, \dots, X_m]$ its reduced form. Since

$$\forall x = (x_1, \dots, x_m) \in \mathbb{F}_q^m,\ f(x) = \left(1 - x_1^{q-1}\right) \dots \left(1 - x_{t-1}^{q-1}\right) P(x_t, \dots, x_m),$$

the reduced form of $f \in R_q(t(q-1) + s, m)$ is

$$\left(1 - X_1^{q-1}\right) \dots \left(1 - X_{t-1}^{q-1}\right) P(X_t, \dots, X_m).$$

Then $g \in R_q(q-1, m-t+1)$ and $|g| = |f| = 2(q-1)q^{m-t-1}$. Thus, using the case where $t = 1$, we finish the proof of Theorem 10.

7 Case where $0 \leq t \leq m-2$ and $s = 1$

7.1 Case where $q \geq 4$

Lemma 11 *Let $m \geq 2$, $q \geq 4$, $0 \leq t \leq m-2$ and $f \in R_q(t(q-1)+1, m)$ such that $|f| = q^{m-t}$. We denote by S the support of f. Then, if H is an affine hyperplane of $\mathbb{F}_q^m$ such that $S \cap H \neq \emptyset$ and $S \cap H \neq S$, S meets all affine hyperplanes parallel to H.*

Proof By applying an affine transformation, we can assume $x_1 = 0$ is an equation of H. Let H_a be the q affine hyperplanes parallel to H of equation $x_1 = a$, $a \in \mathbb{F}_q$. We denote by $I := \{a \in \mathbb{F}_q : S \cap H_a = \emptyset\}$. Let $k := \#I$ and assume $k \geq 1$. Since $S \cap H \neq \emptyset$ and $S \cap H \neq S$, $k \leq q-2$. For all $c \notin I$ we define

$$\forall x = (x_1, \dots, x_m) \in \mathbb{F}_q^m, \quad g_c(x) = f(x) \prod_{a \in \mathbb{F}_q \setminus I, a \neq c} (x_1 - a).$$

Then $|f| = \sum_{c \notin I} |g_c|$.

- Assume $k \geq 2$.
  Then for all $c \notin I$, $\deg(g_c) \leq t(q-1) + q - k$ and $2 \leq q-k \leq q-2$. So, $|g_c| \geq kq^{m-t-1}$. Let $N = \#\{c \notin I : |g_c| = kq^{m-t-1}\}$. If $|g_c| > kq^{m-t-1}$, $|g_c| \geq (k+1)(q-1)q^{m-t-2}$. Hence

  $$q^{m-t} \geq Nkq^{m-t-1} + (q-k-N)(k+1)(q-1)q^{m-t-2}.$$

  Since $k \geq 2$, we get that $N \geq q-k$. Since $(q-k)kq^{m-t-1} \neq q^{m-t}$, we get a contradiction.
- Assume $k = 1$.
  Then, for all $c \notin I$, $\deg(g_c) \leq t(q-1) + 1 + q - 2 = (t+1)(q-1)$. So $|g_c| \geq q^{m-t-1}$. Let $N = \#\{c \notin I : |g_c| = q^{m-t-1}\}$. If $|g_c| > q^{m-t-1}$, $|g_c| \geq 2(q-1)q^{m-t-2}$. Since for $q \geq 4$, $2(q-1)^2 q^{m-t-2} > q^{m-t}$, $N \geq 1$. Furthermore, since $(q-1)q^{m-t-1} < q^{m-t}$, $N \leq q-2$. For $\lambda \in \mathbb{F}_q$, we define $f_\lambda \in B^q_{m-1}$ by

  $$\forall (x_2, \dots, x_m) \in \mathbb{F}_q^{m-1}, \qquad f_\lambda(x_2, \dots, x_m) = f(\lambda, x_2, \dots, x_m).$$

We set $\lambda_1, \ldots, \lambda_q$ an order on the elements of $\mathbb{F}_q$ such that for all $i \leq N$, $|f_{\lambda_i}| = q^{m-t-1}$, $|f_{\lambda_{N+1}}| = 0$ and $q^{m-t-1} < |f_{\lambda_{N+2}}| \leq \ldots \leq |f_{\lambda_q}|$.
Since $f_{\lambda_{N+1}} = 0$, we can write for all $(x_1, \ldots, x_m) \in \mathbb{F}_q^m$,

$$f(x_1, \ldots, x_m) = (x_1 - \lambda_{N+1})h(x_1, \ldots, x_m)$$

with $\deg(h) \leq t(q-1)$. Then, for all $1 \leq i \leq q$, $i \neq N+1$ and $(x_2, \ldots, x_m) \in \mathbb{F}_q^{m-1}$,

$$f_{\lambda_i}(x_2, \ldots, x_m) = (\lambda_i - \lambda_{N+1})h_{\lambda_i}(x_2, \ldots, x_m).$$

So $\deg(f_{\lambda_i}) \leq t(q-1)$ and $h_{\lambda_i} = \frac{f_{\lambda_i}}{\lambda_i - \lambda_{N+1}}$.
Since $h \in R_q(t(q-1), m)$, by Lemma 10, there exists an affine transformation such that for all $i \leq N$, $h_{\lambda_i} = h_{\lambda_1}$. Then, for all $(x_1, \ldots, x_m) \in \mathbb{F}_q^m$,

$$h(x_1, \ldots, x_m) = h_{\lambda_1}(x_2, \ldots, x_m) + (x_1 - \lambda_1) \ldots (x_1 - \lambda_N)\widetilde{h}(x_1, \ldots, x_m)$$

with $\deg(\widetilde{h}) \leq t(q-1) - N$. Hence, for all $(x_1, \ldots, x_m) \in \mathbb{F}_q^m$,

$$f(x_1, \ldots, x_m) = \frac{x_1 - \lambda_{N+1}}{\lambda_1 - \lambda_{N+1}} f_{\lambda_1}(x_2 \ldots, x_m) + (x_1 - \lambda_1) \ldots (x_1 - \lambda_{N+1})\widetilde{h}(x_1, \ldots, x_m).$$

Then, for all $(x_2, \ldots, x_m) \in \mathbb{F}_q^{m-1}$,

$$f_{\lambda_{N+2}}(x_2, \ldots, x_m) = \lambda f_{\lambda_1}(x_2 \ldots, x_m) + \lambda' \widetilde{h}_{\lambda_{n+2}}(x_2, \ldots, x_m)$$

with $\lambda, \lambda' \in \mathbb{F}_q^*$.
Since $f_{\lambda_1} \in R_q(t(q-1), m-1)$ and $\widetilde{h}_{\lambda_{n+2}} \in R_q(t(q-1)-N, m-1)$, by Lemma 9, either $|f_{\lambda_{N+2}}| = Nq^{m-t-1}$ or $|f_{\lambda_{N+2}}| \geq (N+1)q^{m-t-1}$.
If $N = 1$, since $|f_{\lambda_{N+2}}| > q^{m-t-1}$, we get

$$q^{m-t-1} + (q-2)2q^{m-t-1} \leq q^{m-t}$$

which means that $q \leq 3$. So $N \geq 2$. Then,

$$Nq^{m-t-1} + (q-1-N)Nq^{m-t-1} \leq q^{m-t}.$$

Since $N(q-N) \geq 2(q-2)$, we get that $q \leq 4$. So, the only possibility is $q = 4$ and $N = q - 2 = 2$.
If $t = 0$, H_{λ_4} contains 2.4^{m-1} points which is absurd. Assume $t \geq 1$. Since $h_{\lambda_1} = h_{\lambda_2}$ and for $i \in \{1, 2\}$, $f_{\lambda_i} = (\lambda_i - \lambda_3)h_{\lambda_i}$, $S \cap H_{\lambda_1}$ and $S \cap H_{\lambda_2}$ are both included in A an affine subspace of dimension $m - t$. If $t = 1$, by applying an affine transformation which fixes x_1, we can assume $x_2 = 0$ is an equation of A. If S is included in A, then

$$\#(S \cap H_{\lambda_4} \cap A) = 2.4^{m-2}$$

which is absurd since $H_{\lambda_4} \cap A$ is an affine subspace of codimension 2. So there exists an affine hyperplane H' containing A but not S. By applying an affine transformation which fixes x_1, we can assume $x_2 = 0$ is an equation of H'. Now, consider g defined for all $(x_1, \ldots, x_m) \in \mathbb{F}_q^m$ by $g(x_1, \ldots, x_m) = x_2 f(x_1, \ldots, x_m)$. Then $|g| \leq 2.4^{m-t-1}$. Furthermore, since S is not included in H' and $\deg(g) \leq 3t + 2$, $|g| \geq 2.4^{m-t-1}$. So g is a minimum weight codeword of $R_4(3t + 2, m)$ and its support is the union of two parallel affine subspace of codimension $t + 1$

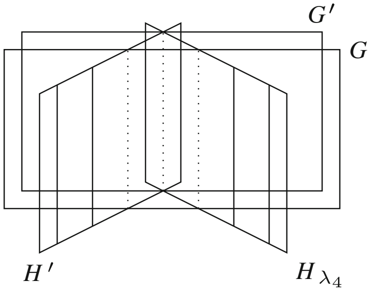

Fig. 10 Lemma 11, case where $k = 1$

included in an affine subspace of codimension t. Then, since $H' \cap H_{\lambda_4} = \emptyset$, there exists H'_1 an hyperplane parallel to H' such that $S \cap H'_1 = \emptyset$. Now, consider G the hyperplane through $H_{\lambda_4} \cap H'_1$ and $H' \cap H_{\lambda_3}$ and G' the hyperplane through $H' \cap H_{\lambda_4}$ parallel to G (see Fig. 10).
Then G and G' does not meet S but S is not included in an hyperplane parallel to G which is absurd by the previous case. □

Lemma 12 *For $m \geq 3$, if $f \in R_4(3(m-2)+1, m)$ is such that $|f| = 16$, the support of f is an affine plane.*

Proof We denote by S the support of f.

First, we prove the case where $m = 3$. To prove this case, by Lemma 11, we only have to prove that there exists an affine hyperplane which does not meet S.

Assume S meets all affine hyperplanes. Let H be an affine hyperplane. Then for all H' affine hyperplane parallel to H, $\#(S \cap H') \geq 3$. Assume for all H' hyperplane parallel to H, $\#(S \cap H') \geq 4$. For reason of cardinality , for all H' parallel to H $\#(S \cap H') = 4$. Since $q = 4$, there exists a line in H which does not meet S. Since $3.4 + 4 = 16$, S meets four hyperplanes through this line in 3 points and the last one in 4 points. So, there exists H_1 an affine hyperplane such that $\#(S \cap H_1) = 3$. We denote by H_2, H_3, H_4 the hyperplanes parallel to H_1. Then, $S \cap H_1$ is the support of a minimal weight codeword of $R_4(3(m-1)+1, m)$ so $S \cap H_1$ is included in L a line. Consider L' a line in H_1 parallel to L. Then there is four hyperplanes through L' which meets S in 3 points and one H'_1 which meets S in 4 points. Let H' be an affine hyperplane through L' which meets S in 3 points; $S \cap H'$ is minimum weight codeword of $R_4(3(m-1)+1, m)$ which does not meet H_1. So either $S \cap H'$ is included in an affine hyperplane parallel to H_1 or $S \cap H'$ meets all affine hyperplane parallel to H_1 but H_1 in 1 point. Then we consider four cases:

1. H_1 is the only hyperplane through L' such that $\#(S \cap H_1) = 3$ and $S \cap H_1$ is included in one of the affine hyperplane parallel to H_1.
   Since $S \cap H_1 \cap H'_1 = \emptyset$ there exists an affine hyperplane parallel to H_1 which meets $S \cap H'_1$ in at least 2 points. Assume for example it is H_2. Since $m = 3$, these 2 points are included in L_1 a line which is a translation of L. Consider H the hyperplane containing L_1 and L. Then, H meets $S \cap H_3$ and $S \cap H_4$ in 1 point (see Fig. 11a). So $\#(S \cap H) = 7$

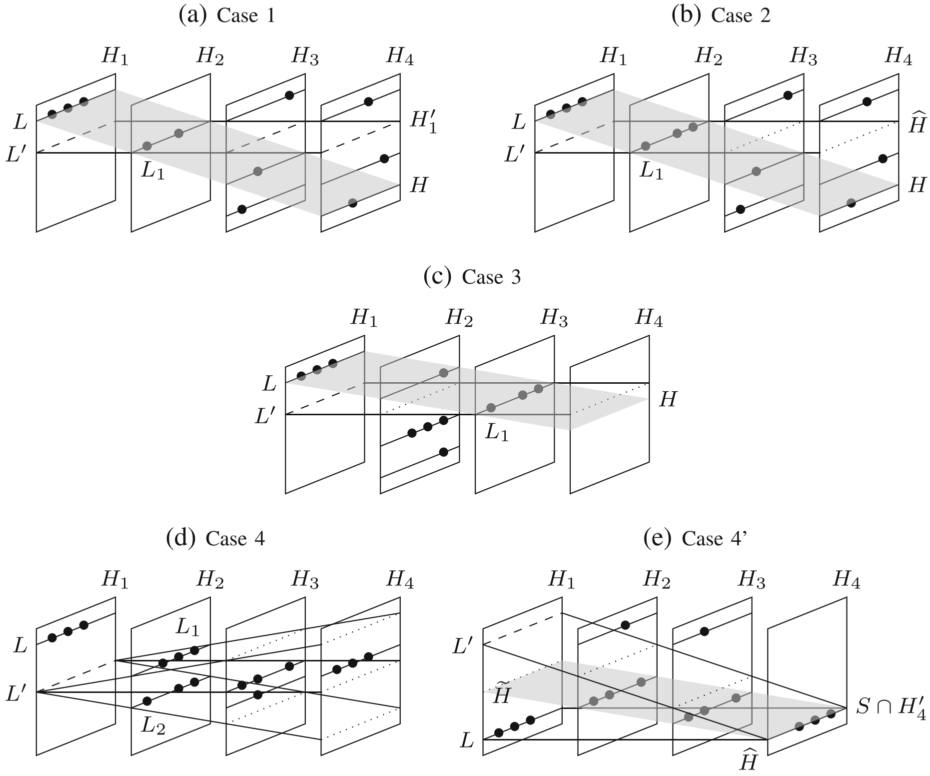

Fig. 11 Lemma 12, case where $m = 3$

2. There are exactly two hyperplanes through L' which meets S in 3 points and such that its intersection with S is included in one of the affine hyperplane parallel to H_1.
   Assume H_2 contains $S \cap \widehat{H}$ where $\widehat{H}$ is the hyperplane through L' different from H_1 such that $\#(S \cap \widehat{H}) = 3$ and $S \cap \widehat{H}$ is included in an hyperplane parallel to H_1, say H_2. We denote by $L_1 = \widehat{H} \cap H_2$. Since for all H' hyperplane $\#(S \cap H') \geq 3$, $S \cap H'_1$ meets H_3 and H_4 in at least one point. Then consider H the hyperplane through L and L_1. Since H is different from the hyperplane through L' and L_1, H meets H_3 and H_4 in at least 1 point each (see Fig. 11b). So $\#(S \cap H) \geq 7$.
3. There are exactly three hyperplanes through L' which meets S in 3 points and such that its intersection with S is included in one of the affine hyperplane parallel to H_1.
   If two such hyperplanes have their intersection with S included in the same hyperplane parallel to H_1, say H_2, then $\#(S \cap H_2) \geq 7$. Now, assume they are included in two different hyperplanes, H_2 and H_3. If $S \cap H'_1$ is included in H_4 then we consider H the hyperplane through L and $S \cap H'_1$ and $\#(S \cap H) \geq 7$. Otherwise, we can assume $S \cap H'_1$ meets H_2 in at least 1 point. Let H be the hyperplane through L and L_1 the line containing the minimum weight codeword included in H_3. Since H is different from the hyperplane through L' and L_1, H meets $S \cap H_2$ in at least 1 point and $\#(S \cap H) \geq 7$ (see Fig. 11c).

4. There are four hyperplanes through L' which meets S in 3 points and such that its intersection with S is included in one of the affine hyperplane parallel to H_1. If three such hyperplanes have their intersection with S included in the same hyperplane parallel to H_1, say H_2, then $\#(S \cap H_2) \geq 7$. Assume two such hyperplanes have their intersection included in the same hyperplane parallel to H_1, say H_2 and the last one has its intersection with S included in H_3. Then, since $\#(S \cap H_4) \geq 3$, $\#(S \cap H'_1 \cap H_4) \geq 3$.
If $\#(S \cap H_4 \cap H'_1) = 4$, we consider H the hyperplane through L and $S \cap H'_1$ and $\#(S \cap H) \geq 7$. Otherwise, there is one point of $S \cap H_4$ included in H_2 or H_3. If this point is included in H_2 then $\#(S \cap H_2) \geq 7$. If it is included in H_3, we consider L_1 and L_2 the two lines in H_2 containing S which are a translation of L. Then either the hyperplane through L and L_1 or the hyperplane through L and L_2 meets $S \cap H_3$ or $S \cap H_4$ (see Fig. 11d). So there is an hyperplane H such that $\#(S \cap H) \geq 7$.
Now assume for each hyperplane H' parallel to H_1, there is only one hyperplane through L' which meets S in 3 points such that its intersection with S included in H'. If $S \cap H'_1$ is included in an affine hyperplane parallel to H_1 then we consider H the hyperplane through L and $S \cap H'_1$ and $\#(S \cap H) \geq 7$. Otherwise, $S \cap H'_1$ meets at least two hyperplanes parallel to H_1, say H_2 and H_3 in at least 1 point. For $i \in \{2, 3, 4\}$, we denote by H'_i the hyperplane through L' such that $S \cap H'_i \subset H_i$. If $\widehat{H}$ the hyperplane through L and $S \cap H'_4$ does not meet $S \cap H_2$ and $S \cap H_3$, then $\widetilde{H}$ the hyperplane through $S \cap H'_4$ and $S \cap H'_3$ meets $S \cap H_2$. Indeed, if $\widehat{H}$ does not meet $S \cap H_2$ we consider four hyperplanes through $S \cap H'_4$ different from H_4, which intersect H_2 in 4 distinct parallel lines. However two of these lines meet S (see Fig. 11e). So there is an hyperplane H such that $\#(S \cap H) \geq 7$.

In all cases, there exists an affine hyperplane H such that $\#(S \cap H) \geq 7$. If $\#(S \cap H) > 7$, since S meets all affine hyperplanes in at least 3 points, $\#S > 7 + 3.3 = 16$ which gives a contradiction. If $\#(S \cap H) = 7$, then for all H' parallel to H different form H $\#(S \cap H') = 3$. By applying an affine transformation, we can assume $x_1 = 0$ is an equation of H. Then $g = x_1 f \in R_4(3(m-2)+2, m)$ and $|g| = 9$. So, g is a second weight codeword of $R_4(3(m-2)+2, m)$ and by Theorem 9, the support of g is included in a plane P. Since S meets all hyperplanes, S is not included in P. Then, S meets all hyperplanes parallel to P in at least 3 points. However $3.3 + 9 = 18 > 16$ which is absurd.

Now, assume $m \geq 4$. Assume S is not included in an affine subspace of dimension 3. Then there exists H an affine hyperplane such that $S \cap H$ is not included in a plane and S is not included in H. So, by Lemma 11, S meets all affine hyperplanes parallel to H in at least 3 points.

Assume for all H' parallel to H, $\#(S \cap H') \geq 4$, then for reason of cardinality, $\#(S \cap H) = 4$. So $S \cap H$ is the support of a second weight codeword of $R_4(3(m-1)+1, m)$ and is included in a plane which is absurd. So there exists H_1 an affine hyperplane parallel to H such that $\#(S \cap H_1) = 3$. Then, $S \cap H_1$ is the support of the minimum weight codeword of $R_4(3(m-1)+1, m)$ and is included in a line L. We denote by $\overrightarrow{u}$ a directing vector of L and a the point of L which is not in S.

Let w_1, w_2, w_3 be 3 points of $S \cap H$ which are not included in a line. Then, there are at least 2 vectors of $\{\overrightarrow{w_1w_2}, \overrightarrow{w_1w_3}, \overrightarrow{w_2w_3}\}$ which are not collinear to $\overrightarrow{u}$. Assume they are $\overrightarrow{w_1w_2}$ and $\overrightarrow{w_1w_3}$. Let a be an affine subspace of codimension 2 included in H_1 which contains a, $a + \overrightarrow{w_1w_2}$, $a + \overrightarrow{w_1w_3}$ but not $a + \overrightarrow{u}$. Then S does not meet A.

Assume S does not meet one hyperplane through A. Then S is included in an affine hyperplane parallel to this hyperplane which is absurd by definition of A. So, S meets all hyperplanes through A and since $3.4 + 4 = 16$, There exists H_2 an hyperplane through A such that $\#(S \cap H_2) = 4$ and $S \cap H_2$ is included in a plane. For all H' hyperplane through A different from H_2, $\#(S \cap H') = 3$ and $S \cap H'$ is included in a line. Consider H_2' the hyperplane through A such that $w_1 \in H_2'$. Then $w_1, w_2, w_3 \in H_2'$. Since for all H' hyperplane through A different from H_2, $S \cap H'$ is included in a line and w_1, w_2, w_3 are not included in a line $H_2' = H_2$. Further more $S \cap H_2$ is included in a plane, so $S \cap H_2' \subset H$.

For all H' hyperplane through A different from H_2, $S \cap H'$ is the support of a minimum weight codeword of $R_4(3(m-1)+1, m)$ which does not meet H_1, so either $S \cap H'$ is included an affine hyperplane parallel to H_1 or $S \cap H'$ meets all affine hyperplanes parallel to H but H_1 in 1 point. Since $S \cap H_2$ is included in H and all hyperplanes parallel to H meets S in at least 3 points, there are only three possibilities:

1. For all H_2' hyperplane through A, $S \cap H_2'$ is included in an affine hyperplane parallel to H.
2. For H_2' hyperplane through A different from H_2 and H_1, $S \cap H_2'$ meets all affine hyperplanes parallel to H different from H_1 in 1 points.
3. There is four hyperplanes through A such that their intersection with S is included in an affine hyperplane parallel to H and one hyperplane through A which meets all hyperplanes parallel to H but H_1 in 1.

In the two first cases, since $S \cap H$ is not included in a plane and S meets all hyperplanes parallel to H in at least 3 points, $\#(S \cap H) = 7$ and for all H' parallel to H different form H, $\#(S \cap H') = 3$. By applying an affine transformation, we can assume $x_1 = 0$ is an equation of H. Then $g = x_1 f \in R_4(3(m-2)+2, m)$ and $|g| = 9$. So, g is a second weight codeword of $R_4(3(m-2)+2, m)$ and by Theorem 9, the support of g is included in a plane P. Since S is not included in P, there exists H_1' an affine hyperplane which contains P but not S. Then, S meets all hyperplanes parallel to H_1' in at least 3 points. However $3.3 + 9 = 18 > 16$ which is absurd.

Assume we are in the third case. Since $S \cap H$ is the union of a point and $S \cap H_2$ which is included in a plane and $m \geq 4$, there exist B an affine subspace of codimension 2 included in H such that S does not meet B and $S \cap H$ is not included in affine hyperplane parallel to B. Then S meets all affine hyperplanes through B in at most 4 points which is a contradiction since $\#(S \cap H) = 5$.

So S is included in G an affine subspace of dimension 3. By applying an affine transformation, we can assume

$$G := \{(x_1, \dots, x_m) \in \mathbb{F}_q^m : x_4 = \dots = x_m = 0\}.$$

Let $g \in B_3^q$ defined for all $x = (x_1, x_2, x_3) \in \mathbb{F}_q^3$ by

$$g(x) = f(x_1, x_2, x_3, 0, \dots, 0)$$

and denote by $P \in \mathbb{F}_q[X_1, X_2, X_3]$ its reduced form. Since

$$\forall x = (x_1, \dots, x_m) \in \mathbb{F}_q^m,\ f(x) = (1 - x_4^{q-1}) \dots (1 - x_m^{q-1}) P(x_1, x_2, x_3),$$

the reduced form of $f \in R_q(3(m-2)+1, m)$ is

$$(1 - X_4^{q-1}) \dots (1 - X_m^{q-1}) P(X_1, X_2, X_3).$$

Then $g \in R_q(4, 3)$ and $|g| = |f| = 16$. Thus, using the case where $m = 3$, we finish the proof of Lemma 12. □

Theorem 12 *For $q \geq 4$, $m \geq 2$, $0 \leq t \leq m-2$, if $f \in R_q(t(q-1)+1, m)$ is such that $|f| = q^{m-t}$, the support of f is an affine subspace of codimension t.*

Proof If $t = 0$, the second weight is q^m and we have the result.

For other cases, we proceed by recursion on t.

If $q \geq 5$, we have already proved the case where $t = m-1$ (Theorem 8); if $m = 2$ and $t = m-2 = 0$, we have the result. Assume $m \geq 3$.

For $q = 4$, if $m = 2$, $t = m-2 = 0$ and we have the result. If $m \geq 3$, we have already proved the case $t = m-2$ (Lemma 12). Furthermore, if $m = 3$ we have considered all cases. Assume $m \geq 4$

Let $1 \leq t \leq m-2$ (or for $q = 4$, $1 \leq t \leq m-3$). Assume the support of $f \in R_q((t+1)(q-1)+1, m)$ such that $|f| = q^{m-t-1}$ is an affine subspace of codimension $t+1$.

Let $f \in R_q(t(q-1)+1, m)$ such that $|f| = q^{m-t}$. We denote by S its support. Assume S is not included in an affine subspace of codimension t. Then there exists H an affine hyperplane such that $S \cap H$ is not included in an affine subspace of codimension $t+1$ and $S \cap H \neq S$. Then, by Lemma 11, S meets all affine hyperplanes parallel to H and for all H' hyperplane parallel to H,

$$\#(S \cap H') \geq (q-1)q^{m-t-2}.$$

If for all H' hyperplane parallel to H, $\#(S \cap H') > (q-1)q^{m-t-2}$ then, for reason of cardinality, $\#(S \cap H) = q^{m-t-1}$. So $S \cap H$ is the support of a second weight codeword of $R_q((t+1)(q-1)+1, m)$ and is included in an affine subspace of codimension $t+1$ which is a contradiction.

So there exists H_1 parallel to H such that $\#(S \cap H_1) = (q-1)q^{m-t-2}$. Then $S \cap H_1$ is the support of a minimal weight codeword of $R_q((t+1)(q-1)+1, m)$. Hence, $S \cap H_1$ is the union of $q-1$ affine subspaces of codimension $t+2$ included in an affine subspace of codimension $t+1$.

Let A be an affine subspace of codimension 2 included in H_1 such that A meets the affine subspace of codimension $t+1$ which contains $S \cap H_1$ in the affine subspace of codimension $t+2$ which does not meet S. Assume there is an affine hyperplane through A which does not meet S. Then, by Lemma 11, S is included in an affine hyperplane parallel to this hyperplane which is absurd by construction of A. So, S meets all hyperplanes through A. Furthermore,

$$q^{m-t} = q^{m-t-1} + q(q-1)q^{m-t-2}.$$

So S meets one of the hyperplane through A in q^{m-t-1} points, say H_2, and all the others in $(q-1)q^{m-t-2}$ points.

Since $H_2 \neq H_1$, $H_2 \cap H_1 = A$ and $S \cap H_2 \cap H_1 = \emptyset$. So, $S \cap H_2$ is the support of a second weight codewords of $R_q((t+1)(q-1)+1, m)$ which does not meet H_1. Hence, $S \cap H_2$ is included in one of the affine hyperplanes parallel to H.

Furthermore, for all H_2' hyperplane through A different from H_2 and H_1, $S \cap H_2'$ is the support of a minimum weight codeword of $R_q((t+1)(q-1)+1, m)$ which does not meet H_1, so it meets all affine hyperplanes parallel to H_1 different from H_1 in q^{m-t-2} points or is included in an affine hyperplane parallel to H_1. Since $S \cap H_2$ is included in one of the affine hyperplanes parallel to H and all hyperplanes parallel to H meets S in at least $(q-1)q^{m-t-2}$ points, there are only three possibilities:

1. For all H_2' hyperplane through A, $S \cap H_2'$ is included in an affine hyperplane parallel to H.
2. For H_2' hyperplane through A different from H_2 and H_1, $S \cap H_2'$ meets all affine hyperplanes parallel to H different from H_1 in q^{m-t-2} points.
3. There is q hyperplanes through A such that their intersection with S is included in an affine hyperplane parallel to H and one hyperplane through A which meets all hyperplanes parallel to H but H_1 in q^{m-t-2}.

In the two first cases, if $S \cap H_2$ is not included in H' parallel to H, $\#(S \cap H') = (q-1)q^{m-t-2}$ and $S \cap H'$ is the support of a minimum weight codewords of $R_q((t+1)(q-1)+1, m)$. So $S \cap H'$ is included in an affine subspace of codimension $t+1$. Then, necessarily, $S \cap H_2$ is included in H. For all H' parallel to H but H, $\#(S \cap H') = (q-1)q^{m-t-2}$. In the third case, for all H' hyperplane parallel to H different from H_1 which does not contain $S \cap H_2$, $\#(S \cap H') = q^{m-t-1}$. So $S \cap H'$ is the support of a second weight codeword of $R_q((t+1)(q-1)+1, m)$ and is an affine subspace of dimension $m-t-1$. Then, $S \cap H_2 \subset H$ and $\#(S \cap H) = q^{m-t-2} + q^{m-t-1}$, $\#(S \cap H_1) = (q-1)q^{m-t-2}$. So if we are in the last case for reason of cardinality, for all A' affine subspace of codimension 2 included in H_1 such that A' meets the affine subspace of codimension $t+1$ which contains $S \cap H_1$ in the affine subspace of codimension $t+2$ which does not meet S we are also in case 3. Then S is the union of affine subspaces of dimension $m-t-2$ which are a translation of the affine subspace of codimension $t+2$ which does not meet S in $S \cap H_1$. Then, since $S \cap H_2$ is the support of a second weight codeword of $R_q((t+1)(q-1)+1, m)$, it is an affine subspace of dimension $m-t-1$. So $S \cap H$ is the union of an affine subspace of dimension $m-t-1$ and an affine subspace of dimension $m-t-2$. Since S is the union of affine subspaces of dimension $m-t-2$ which are a translation of an affine subspace of codimension $t+2$, there exists B an affine subspace of codimension 2 such that B does not meet S and $S \cap H$ is not included in an affine subspace of codimension 2 parallel to B. Now, we consider all affine hyperplanes through B. Assume there exists G an affine hyperplane through B which does not meet S. Then, S is included in an affine hyperplane parallel to G which is absurd by construction of B. So, S meets all hyperplanes through B and there exists G_1 hyperplane through B such that $\#(S \cap G_1) = q^{m-t-1}$ and for all G through B but G_1, $\#(S \cap G) = (q-1)q^{m-t-2}$ which is absurd since $\#(S \cap H) = q^{m-t-1} + q^{m-t-2}$. Finally, we are in case 1 or 2.

By applying an affine transformation, we can assume $x_1 = 0$ is an equation of H. Now, consider g the function defined by

$$\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m \quad g(x) = x_1 f(x).$$

Then $\deg(g) \leq t(q-1)+2$ and $|g| = (q-1)^2 q^{m-t-2}$. So, g is a second weight codeword of $R_q(t(q-1)+2, m)$ and by Theorem 9, the support of g is included in an affine subspace of codimension t.

Let H_3 be an affine hyperplane containing the support of g but not S. Then, $\#(S \cap H_3) \geq (q-1)^2 q^{m-t-2}$. Furthermore, since $S \not\subset H_3$, S meets all affine hyperplanes parallel to H_3 in at least $(q-1)q^{m-t-2}$. Finally,

$$\#S \geq 2(q-1)^2 q^{m-t-2} > q^{m-t}.$$

We get a contradiction. So S is included in an affine subspace of codimension t. For reason of cardinality, S is an affine subspace of codimension t. □

7.2 Case where $q = 3$, proof of Theorem 5

Lemma 13 *Let $m \geq 2$, $0 \leq t \leq m-2$, $f \in R_3(2t+1, m)$ such that $|f| = 8.3^{m-t-2}$. If H is an affine hyperplane of $\mathbb{F}_q^m$ such that $S \cap H \neq \emptyset$ and $S \cap H \neq S$ then either S meets two hyperplanes parallel to H in 4.3^{m-t-2}points or S meets all affine hyperplanes parallel to H.*

Proof By applying an affine transformation, we can assume $x_1 = 0$ is an equation of H. We denote by H_a the affine hyperplanes parallel to H of equation $x_1 = a$, $a \in \mathbb{F}_q$. Let $I := \{a \in \mathbb{F}_q : S \cap H_a = \emptyset\}$ and $k := \#I$. Since $S \cap H \neq \emptyset$ and $S \cap H \neq S$, $k \leq q-2 = 1$. Assume $k = 1$. For all $c \notin I$ we define

$$\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m, \quad f_c(x) = f(x) \prod_{a \notin I, a \neq c} (x_1 - a).$$

Then $\deg(f_c) = (t+1)2$ and $|f_c| \geq 3^{m-t-1}$. Assume there exists H' an affine hyperplane parallel to H such that $\#(S \cap H') = 3^{m-t-1}$ and $S \cap H'$ is the support of a minimal weight codeword of $R_3(2(t+1), m)$. Then consider A an affine subspace of codimension 2 included in H' containing $S \cap H'$ and A' an affine subspace of codimension 2 included in H' parallel to A. We denote by k the number of hyperplanes through A which meet S and by k' the number of affine hyperplanes through A' which meet S in 3^{m-t-1} points. Then

$$k' 3^{m-t-1} + (k-k') 4.3^{m-t-2} \leq 8.3^{m-t-2}.$$

Since $\#S > \#(S \cap H')$ and $k' \leq k$, we get $k = 2$. Then, if we denote by H'' the other hyperplane parallel to H' which meets S, $S \cap H''$ is included in an affine subspace of codimension 2 which is a translation of A. By applying this argument to all affine subspaces of codimension 2 included in H' and containing $S \cap H'$, we get that $S \cap H''$ is included in a an affine subspace of dimension $m-t-1$. For reason of cardinality this is absurd. If $|f_c| > 3^{m-t-1}$ then $|f_c| \geq 4.3^{m-t-2}$. For reason of cardinality, we have the result. □

Now, we prove Proposition 5.

– First, we prove the case where $t = 1$. Obviously, S is included in an affine subspace of dimension m. Assume S meets all affine hyperplanes of $\mathbb{F}_q^m$. Then for all H' affine hyperplane of $\mathbb{F}_q^m$, $\#(S \cap H') \geq 2.3^{m-3}$ and by Lemma 2, there exists H an affine hyperplane such that

$$\#(S \cap H) = 2.3^{m-3}.$$

Then $S \cap H$ is the support of a minimum weight codeword of $R_3(5, m)$. So it is the union of P_1, P_2 2 parallel affine subspaces of dimension $m-3$ included in an affine subspace of dimension $m-2$. Let A be an affine subspace of codimension 2 included in H, containing P_1 and different from the affine subspace of codimension 2 containing $S \cap H$. Then there exists A' an affine hyperplane of codimension 2 included in H parallel to A which does not meet S. We denote by k the number of affine hyperplanes through A' which meet S in 2.3^{m-3} points. Then, if $m \geq 4$,

$$k2.3^{m-3} + (4-k)8.3^{m-4} \leq 8.3^{m-3}$$

which means that $k \geq 4$. If $m = 3$, $2k + (4-k)3 \leq 8$ which also means that $k \geq 4$. Then for all H' hyperplane through A different from H, $S \cap H'$ is a minimal weight codeword of $R_3(5, m)$ which does not meet H and either $S \cap H'$ is included in one of the hyperplanes parallel to H or $S \cap H'$ meets the two hyperplanes parallel to H different from H. In all cases, S is the union of eight affine subspace of dimension $m-3$. By applying this argument to all affine subspaces of codimension 2 included in H, containing P_1 and different from the affine subspace of codimension 2 containing $S \cap H$, we get that these 8 affine subspaces are a translation of P_1.
Choose H_1 one of the hyperplanes through A' and consider H_2 and H_3 the two hyperplanes parallel to H_1. Since $\#(S \cap H_1) = 2.3^{m-3}$ and S meets all hyperplanes in at least 2.3^{m-3} points, either $\#(S \cap H_2) = 3.3^{m-3}$ and $\#(S \cap H_3) = 3.3^{m-3}$ or $\#(S \cap H_2) = 2.3^{m-3}$ and $\#(S \cap H_3) = 4.3^{m-3}$.
First consider the case where $\#(S \cap H_2) = 3.3^{m-3}$ and $\#(S \cap H_3) = 3.3^{m-3}$. Then there exists an affine subspace of codimension 2 in H_2 which does not meet S. We denote by k' the number of hyperplanes through A which meet S in 2.3^{m-3} points. Then , we have $k' \geq 4$ which is absurd since $\#(S \cap H_2) = 3.3^{m-3}$.
Now, consider the case where $\#(S \cap H_2) = 2.3^{m-3}$ and $\#(S \cap H_3) = 4.3^{m-3}$. By applying an affine transformation, we can assume $x_1 = 0$ is an equation of H_3. Then $x_1.f$ is a codeword of $R_3(4, m)$ and $|x_1.f| = 4.3^{m-3}$. So, by Theorem 10, its support is included in an affine hyperplane H_1' and $S \cap H_1' \cap H_3 = \emptyset$. So S is included H_1' and H_3 and there exists an affine hyperplane through $H_1' \cap H_3$ which does not meet S which is absurd.
Finally there exists an affine hyperplane G_1 which does not meet S. So, by Lemma 13, S meets G_2 and G_3 the two hyperplanes parallel to G_1 in 4.3^{m-3} points. Then, Theorem 10, $G_2 \setminus S$ and $G_3 \setminus S$ are the union of two non parallel affine subspaces of codimension 2. Consider A one of the affine subspaces of codimension 2 in $G_2 \setminus S$. Assume all hyperplanes through A meet S. So for all G' hyperplane through A, $\#(G' \setminus S) \leq 7.3^{m-3}$. Furthermore, one of the hyperplanes through A, say G, meets $G_3 \setminus S$ in at least 2.3^{m-3}, then $\#(G \setminus S) \geq 2.3^{m-2} + 2.3^{m-3}$ which is absurd (see Fig. 12). So there exists G' through A which does not meet S. By applying the same argument to the other affine subspace of dimension 2 of $G_2 \setminus S$, we get the result for $t = 1$.

– We prove by recursion on t that S is included in an affine subspace of dimension $m-t+1$. Consider first the case where $t = m-2$. If $m = 3$ then $t = 1$ and we have already considered this case. Assume $m \geq 4$. Let $f \in R_3(2(m-2)+1, m)$ such that $|f| = 8$. Assume S is not included in an affine subspace of dimension 3. Let w_1, w_2, w_3, w_4 be 4 points of S which are not included in a plane. Since

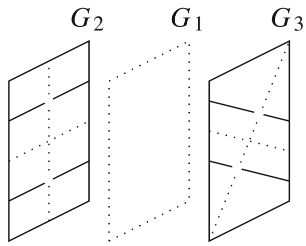

Fig. 12 Proposition 5, case where $t = 1$

S is not included in an affine subspace of dimension 3, there exists H an affine hyperplane such that H contains w_1, w_2, w_3, w_4 but S is not included in H. Then by Lemma 13 either S meets two hyperplanes parallel to H in 4 points or S meets all hyperplanes parallel to H.
If S meets two hyperplanes parallel to H then $S \cap H$ is the support of a second weight codeword of $R_3(2(m-1), m)$ so is included in a plane which is absurd since $w_1, w_2, w_3, w_4 \in S \cap H$. So S meets all hyperplanes parallel to H and for all H' hyperplane parallel to H, $\#(S \cap H') \geq 2$. Since $\#S = 8$ and $\#(S \cap H) \geq 4$, for all H' hyperplane parallel to H different from H $\#(S \cap H') = 2$ and $\#(S \cap H) = 4$.
By applying an affine transformation, we can assume $x_1 = 0$ is an equation of H. Then $x_1.f \in R_3(2(m-1), m)$ and $|x_1.f| = 4$ so $x_1.f$ is a second weight codeword of $R_3(2(m-1), m)$ and its support is included in a plane P not included in H. Let H' be an affine hyperplane which contains P and a point of $(S \cap H) \setminus P$ but not all the points of $S \cap H$. Then, $\#(S \cap H') \geq 5$ and $S \cap H' \neq S$. By applying the same argument to H' than to H we get a contradiction for reason of cardinality.

– If $m \leq 4$, we have already considered all the possible values for t. Assume $m \geq 5$. Let $2 \leq t \leq m-3$. Assume if $f \in R_3(2(t+1)+1, m)$ is such that $|f| = 8.3^{m-t-3}$ then its support is included in an affine subspace of dimension $m-t$. Let $f \in R_3(2t+1, m)$ such that $|f| = 8.3^{m-t-2}$ and denote by S its support. Assume S is not included in an affine subspace of dimension $m-t+1$. Then, there exists H an affine hyperplane such that $S \cap H \neq S$ and $S \cap H$ is not included in an affine subspace of dimension $m-t$. So, by Lemma 13, either S meets two affine hyperplanes parallel to H in 4.3^{m-t-2} points or S meets all affine hyperplanes parallel to H.
If S meets two affine hyperplanes in 4.3^{m-t-2} points, $S \cap H$ is the support of a second weight codeword of $R_3(2(t+1), m)$ and is included in an affine subspace of dimension $m-t$ which is absurd. So S meets all affine hyperplanes parallel to H and for all H' hyperplane parallel to H,

$$\#(S \cap H') \geq 2.3^{m-t-2}.$$

Assume for all H' parallel to H, $\#(S \cap H') > 2.3^{m-t-2}$. Then, for reason of cardinality $\#(S \cap H) = 8.3^{m-t-3}$ and $S \cap H$ is the support of a second weight codeword of $R_3(2(t+1)+1, m)$ which is absurd since $S \cap H$ is not included in an affine subspace of dimension $m-t$. So there exists H_1 parallel to H such that $\#(S \cap H_1) = 2.3^{m-t-2}$ and $S \cap H_1$ is the support of a minimal weight codeword of $R_3(2(t+1)+1, m)$ so $S \cap H_1$ is the union of P_1 and P_2 2 parallel affine subspaces of dimension $m-t-2$ included in an affine subspace of dimension $m-t-1$.

Let A be an affine subspace of codimension 2 included in H_1 and containing P_1 and such that $A \cap P_2 = \emptyset$. Let A' be an affine subspace of codimension 2 included in H_1 parallel to A which does not meet S. Assume there exists H'_1 an affine hyperplane through A' which does not meet S. Then, S meets H'_2 and H'_3 the two hyperplanes parallel to H'_1 different from H'_1 in 4.3^{m-t-2} points. For example, we can assume $A \subset H'_2$. Then, $S \cap H'_3$ is the support of a second weight codeword of $R_3(2(t+1), m)$. So $S \cap H'_3$ meets H in $0, 3^{m-t-2}, 2.3^{m-t-2}$ or 4.3^{m-t-2} points. Since S meets all hyperplanes parallel to H in at least 2.3^{m-t-2} points, if

$$\#(S \cap H \cap H'_3) = 4.3^{m-t-2},$$

$S \cap H \cap H'_2 = \emptyset$. So $S \cap H$ is included in an affine subspace of dimension $m-t$ which is absurd. So $S \cap H'_2$ and $S \cap H'_3$ are the support of second weight codewords of $R_3(2(t+1), m)$ not included in H, then their intersection with H is the union of at most two disjoint affine subspaces of dimension $m-t-2$.
Now assume S meets all hyperplanes through A'. We denote by k the number of the hyperplanes through A which meet S in 2.3^{m-t-2} points. Then

$$k2.3^{m-t-2} + (4-k)8.3^{m-t-3} \leq 8.3^{m-t-2}$$

which means that $k \geq 4$. So for all H' affine hyperplane through A' different from H_1, $S \cap H'$ is the support of minimum weight codeword of $R_3(2(t+1)+1, m)$ which does not meet H_1. So either $S \cap H'$ is included in H or $S \cap H'$ meets S in an affine subspace of dimension $m-t-2$. In both cases , $S \cap H$ is the union of at most four disjoint affine subspaces of dimension $m-t-2$. By applying this argument to all affine subspaces of dimension 2 included in H_1 containing P_1 but not P_2, we get that $S \cap H$ is the union of four affine subspaces of dimension $m-t-2$ which are a translation of P_1. This gives a contradiction since $S \cap H$ is not included in an affine subspace of dimension $m-t$. So S is included in an affine subspace of dimension $m-t+1$.

– Let $f \in R_3(2t+1, m)$ such that $|f| = 8.3^{m-t-2}$ and A the affine subspace of dimension $m-t+1$ containing S. By applying an affine transformation, we can assume

$$A := \{(x_1, \ldots, x_m) \in \mathbb{F}_q^m : x_1 = \ldots = x_{t-1} = 0\}.$$

Let $g \in B^3_{m-t+1}$ defined for all $x = (x_t, \ldots, x_m) \in \mathbb{F}_3^{m-t+1}$ by

$$g(x) = f(0, \ldots, 0, x_t, \ldots, x_m)$$

and denote by $P \in \mathbb{F}_3[X_t, \ldots, X_m]$ its reduced form. Since

$$\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_3^m,\ \ f(x) = \left(1 - x_1^2\right) \ldots \left(1 - x_{t-1}^2\right) P(x_t, \ldots, x_m),$$

the reduced form of $f \in R_3(t(q-1)+s, m)$ is

$$\left(1 - X_1^2\right) \ldots \left(1 - X_{t-1}^2\right) P(X_t, \ldots, X_m).$$

Then $g \in R_3(3, m-t+1)$ and $|g| = |f| = 8.3^{m-t-2}$. Thus, using the case where $t = 1$, we finish the proof of Proposition 5.

Appendix: Blocking sets

Blocking sets have been studied by Erickson in [8] in the case of affine planes and by Bruen in [3–5] in the case of projective planes.

Definition 1 Let S be a subset of the affine space $\mathbb{F}_q^2$. We say that S is a blocking set of order n of $\mathbb{F}_q^2$ if for all line L in $\mathbb{F}_q^2$, $\#(S \cap L) \geq n$ and $\#((\mathbb{F}_q^2 \setminus S) \cap L) \geq n$.

Proposition 10 (Lemma 4.2 in [8]) *Let $q \geq 3$, $1 \leq b \leq q-1$ and $f \in R_q(b, 2)$. If f has no linear factor and $|f| \leq (q-b+1)(q-1)$, then the support of f is a blocking set of order $(q-b)$ of $\mathbb{F}_q^2$.*

In [8] Erickson make the following conjecture. It has been proved by Bruen in [5].

Theorem 13 (Conjecture 4.14 in [8]) *If S is a blocking set of order n in $\mathbb{F}_q^2$, then $\#S \geq nq + q - n$.*

References

1. Ballet, S., Rolland, Robert.: Remarks on low weight codewords of generalized affine and projective reed-muller codes. In: Proceedings of the International Workshop on Coding and Cryptography (2013)
2. Berger, T., Charpin, P.: The automorphism group of generalized Reed-Muller codes. Discrete Math. **117**(1–3), 1–17 (1993)
3. Bruen, A.: Baer subplanes and blocking sets. Bull. Amer. Math. Soc. **76**, 342–344 (1970)
4. Bruen, A.: Blocking sets in finite projective planes. SIAM J. Appl. Math. **21**, 380–392 (1971)
5. Bruen, A.A.: Blocking sets and low-weight codewords in the generalized Reed-Muller codes. In: Error-Correcting Codes, Finite Geometries and Cryptography, Contemp. Math., vol. 523, pp. 161–164. Amer. Math. Soc., Providence, RI (2010)
6. Cherdieu, J.P., Rolland, R.: On the number of points of some hypersurfaces in $\mathbf{F}_q^n$. Finite Fields Appl. **2**(2), 214–224 (1996)
7. Delsarte, P., Goethals, J.-M., MacWilliams, F.J.: On generalized Reed-Muller codes and their relatives. Inform. Control **16**, 403–442 (1970)
8. Erickson, D.E.: Mathematics california institute of technology. Division of Physics, and Astronomy. Counting Zeros of Polynomials Over Finite Fields. CIT theses. California Institute of Technology (1974)
9. Geil, O.: On the second weight of generalized Reed-Muller codes. Des. Codes Cryptogr. **48**(3), 323–330 (2008)
10. Kasami, T., Lin, S., Wesley Peterson, W.: New generalizations of the Reed-Muller codes. I. Primitive codes. IEEE Trans. Inform. Theory **IT-14**, 189–199 (1968)
11. Kasami, T., Tokura, N.: On the weight structure of Reed-Muller codes. IEEE Trans. Inform. Theory **IT-16**, 752–759 (1970)
12. Leducq, E.: A new proof of Delsarte, Goethals and Mac Williams theorem on minimal weight codewords of generalized Reed-Muller codes. Finite Fields Appl. **18**(3), 581–586 (2012)
13. Rolland, R.: The second weight of generalized Reed-Muller codes in most cases. Cryptogr. Commun. **2**(1), 19–40 (2010)
14. Sboui, A.: Second highest number of points of hypersurfaces in $\mathbb{F}_q^n$. Finite Fields Appl. **13**(3), 444–449 (2007)