HAMMING DISTANCES FROM A FUNCTION TO ALL CODEWORDS OF A GENERALIZED REED-MULLER CODE OF ORDER ONE

MIRIAM ABDÓN AND ROBERT ROLLAND

Abstract. For any finite field \( \mathbb{F}_q \) with \( q \) elements, we study the set \( \mathcal{F}_{(q,m)} \) of functions from \( \mathbb{F}_q^m \) into \( \mathbb{F}_q \). We introduce a transformation that allows us to determine a linear system of \( q^m+1 \) equations and \( q^m+1 \) unknowns, which has for solution the Hamming distances of a function in \( \mathcal{F}_{(q,m)} \) to all the affine functions.

1. Introduction

1.1. Generalized Reed-Muller codes of order 1. Let \( \mathbb{F}_q \) be the finite field with \( q \) elements. For any integer \( m \geq 1 \), we will identify \( \mathbb{F}_q^m \) with \( \mathbb{F}_q^m \) as follows: consider a basis \( \{ e_1, \ldots, e_m \} \) of \( \mathbb{F}_q^m \) over \( \mathbb{F}_q \), then an element \( u \in \mathbb{F}_q^m \) will be identified with the vector \( (u_1, \ldots, u_m) \in \mathbb{F}_q^m \) if and only if, \( u = \sum_{i=1}^m u_i e_i \).

If \( u = (u_1, \ldots, u_m) \) and \( v = (v_1, \ldots, v_m) \), are two elements of \( \mathbb{F}_q^m \) we will denote by \( u \cdot v \) their product in the field \( \mathbb{F}_q^m \) and by \( \langle u, v \rangle \) their scalar product

\[
\langle u, v \rangle = \sum_{i=1}^m u_i v_i.
\]

We denote by \( \mathcal{F}_{(q,m)} = \{ f : \mathbb{F}_q^m \to \mathbb{F}_q \} \) the set of functions from \( \mathbb{F}_q^m \) to \( \mathbb{F}_q \). Each function \( f \in \mathcal{F}_{(q,m)} \) can be identified with its image \( \{ f(u) \}_{u \in \mathbb{F}_q^m} \). We know that these functions are polynomial functions of \( m \) variables. The kernel of the map which associates to any polynomial the corresponding polynomial function is the ideal \( I \) generated by the \( m \) polynomials \( X_i^q - X_i \). The reduced polynomials are the polynomials \( P(X_1, \ldots, X_m) \) such that for each \( i \), the partial degree \( \deg_i(P(X_1, \ldots, X_m)) \) of \( P(X_1, \ldots, X_m) \) with respect to the variable \( X_i \) is \( \leq q - 1 \). Then for any \( f \in \mathcal{F}_{(q,m)} \) there exists an unique reduced
polynomial \( P(X_1, \ldots, X_m) \) for which \( f \) is the associated polynomial function. The total degree of \( P(X_1, \ldots, X_m) \) is called the degree of \( f \) and denoted by \( \deg(f) \).

With these notations, the Generalized Reed-Muller code of order 1 is the set
\[
RM^{(1)}_{(q,m)} = \{ (g(u))_{u \in \mathbb{F}_q^m} \mid g \in \mathcal{F}_{(q,m)} \text{ and } \deg(g) \leq 1 \}.
\]

If \( f, g \in \mathcal{F}_{(q,m)} \), the Hamming distance between these two functions is defined by
\[
d(f, g) = \text{card} \left( \{ u \in \mathbb{F}_q^m \mid f(u) \neq g(u) \} \right).
\]

### 1.2. Organization of the article

In this article we study the Hamming distances from a function \( f \in \mathcal{F}_{(q,m)} \) to all the codewords \( g \in \mathcal{R}M^{(1)}_{(q,m)} \).

### 2. An adapted transform

It is known that every codeword \( g \in \mathcal{R}M^{(1)}_{(q,m)} \) can be characterized by a pair \((v, t) \in \mathbb{F}_q^m \times \mathbb{F}_q\) in the following sense:
\[
g(u) = \langle u, v \rangle + t \quad \forall u \in \mathbb{F}_q^m.
\]

If \( f \in \mathcal{F}_{(q,m)} \) and \( g \) as above, we have that
\[
d(f, g) = \text{card} \left( \{ u \in \mathbb{F}_q^m \mid f(u) \neq \langle u, v \rangle + t \} \right) = q^m - N_{v,t}(f),
\]
where \( N_{v,t}(f) = \text{card} \left( \{ u \in \mathbb{F}_q^m \mid f(u) = \langle u, v \rangle + t \} \right) \).

Now the problem is to study the integer numbers \( N_{(v,t)}(f) \). In order to do that, we will introduce a transform on the group algebra \( \mathbb{C}F_q \) of the additive group \( \mathbb{F}_q \) over the complex field \( \mathbb{C} \) which is quite similar to a Fourier Transform.

More precisely, \( \mathbb{C}F_q \) is the algebra of formal linear combinations with coefficients in \( \mathbb{C} \)
\[
\sum_{t \in \mathbb{F}_q} \alpha_t Z^t
\]
where the operations are defined by
\[
\sum_{t \in \mathbb{F}_q} \alpha_t Z^t + \sum_{t \in \mathbb{F}_q} \beta_t Z^t = \sum_{t \in \mathbb{F}_q} (\alpha_t + \beta_t) Z^t;
\]
\[
\lambda \left( \sum_{t \in \mathbb{F}_q} \alpha_t Z^t \right) = \sum_{t \in \mathbb{F}_q} (\lambda \alpha_t) Z^t;
\]
\[
(\sum_{t \in \mathbb{F}_q} \alpha_t Z^t)(\sum_{t \in \mathbb{F}_q} \beta_t Z^t) = \sum_{t \in \mathbb{F}_q} \left( \sum_{r+s=t} (\alpha_r \beta_s) \right) Z^t.
\]
Let \( G_{(q,m)} \) be the algebra of functions from \( \mathbb{F}_q^m \) (or from \( \mathbb{F}_q^m \)) into \( \mathbb{C}\mathbb{F}_q \). It is a vector space of dimension \( q^{m+1} \) over \( \mathbb{C} \). Let us define an order on \( \mathbb{F}_q^m \times \mathbb{F}_q \) and define the family \(( e_{u,t} )_{(u,t) \in \mathbb{F}_q^m \times \mathbb{F}_q} \) of elements of \( G_{(q,m)} \) where

\[
e_{u,t}(v) = \begin{cases} 
0 & \text{if } v \neq u \\
Z^t & \text{if } v = u
\end{cases}
\]

This family is a basis of \( G_{(q,m)} \) and has \( q^{m+1} \) elements.

Define the operator \( T_{(q,m)} \) of the \( \mathbb{C} \)-vector space \( G_{(q,m)} \) by

\[
T_{(q,m)}(\phi)(v) = \sum_{u \in \mathbb{F}_q^m} \phi(u)Z^{-\langle u,v \rangle}.
\]

**Remark 2.1.** In the case where the function \( \phi \) is given by \( \phi(v) = Z^f(v) \) for some \( f \in \mathcal{F}_{(q,m)} \), then the transform introduced above is the same that the one introduced by Ashikhmin and Litsyn (see [1]). We recall here some basic properties of this transform, for more details see [2].

**Lemma 2.2.** The transform of \( e_{u,t} \) by \( T_{(q,m)} \) is given by

\[
e_{u,t}(v) = T_{(q,m)}(e_{u,t})(v) = \sum_{w \in \mathbb{F}_q^m} e_{u,t}(w)Z^{-\langle w,v \rangle} = Z^t\delta_{(u,v)},
\]

then

\[
\epsilon_{u,t} = \sum_{(v,\tau) \in E_{-u,t}} \epsilon_{v,\tau},
\]

where \( E_{-u,t} \) is the hyperplane of \( \mathcal{F}_{(q,m)} \times \mathcal{F}_q \) defined by

\[
E_{-u,t} = \{ (v, \tau) \in \mathbb{F}_q^m \times \mathbb{F}_q \mid \tau = t - \langle u, v \rangle \}.
\]

**Lemma 2.3.** Let \( \gamma_a \in G_{(q,m)} \) be defined by \( \gamma_a(u) = Z^{(a,u)} \), then the transform of \( \gamma_a \) is given by

\[
T_{(q,m)}(\gamma_a)(v) = \begin{cases} 
q^m Z^0 & \text{if } v = a \\
q^{m-1} \sum_{t \in \mathbb{F}_q} Z^t & \text{if } v \neq a.
\end{cases}
\]

**Proof.** We have successively

\[
T_{(q,m)}(\gamma_a)(v) = \sum_{u \in \mathbb{F}_q^m} \gamma_a(u)Z^{-\langle u,v \rangle}
\]

\[
= \sum_{u \in \mathbb{F}_q^m} Z^{(a,u)}Z^{-\langle u,v \rangle}
\]

\[
= \sum_{u \in \mathbb{F}_q^m} Z^{(a-v,u)}.
\]
If \( v = a \) we have that \( T_{(q,m)}(\gamma_a)(v) = q^m Z^0 \) and then, when \( v \neq a \), for each \( t \in \mathbb{F}_q \), the equation \( \langle a - v, u \rangle = t \) defines a hyperplane and consequently has \( q^{m-1} \) solutions.

Let \( \phi \) be an element of \( \mathcal{G}_{(q,m)} \), we denote by \( \psi = T_{(q,m)}(\phi) \) its transform, and by \( \theta = T_{(q,m)}(\psi) \) its double transform.

**Theorem 2.4.** With the previous notations we have

\[
\theta(w) = q^{m-1} \sum_{t \in \mathbb{F}_q} (Z^0 - Z^t) \phi(-w) + \left( q^{m-1} \sum_{t \in \mathbb{F}_q} Z^t \right) \psi(0).
\]

**Proof.** We have that

\[
\theta(w) = \sum_{v \in \mathbb{F}_q^m} \left( \sum_{u \in \mathbb{F}_q^m} \phi(u) Z^{-(u,v)} \right) Z^{-(v,w)}
\]

\[
= \sum_{v \in \mathbb{F}_q^m} \left( \sum_{u \in \mathbb{F}_q^m} \phi(u) Z^{-(u+w,v)} \right)
\]

\[
= \sum_{u \in \mathbb{F}_q^m} \phi(u) \sum_{v \in \mathbb{F}_q^m} Z^{-(u+w,v)}
\]

From Lemma 2.3 we obtain

\[
\theta(w) = q^m \phi(-w) + \left( q^{m-1} \sum_{t \in \mathbb{F}_q} Z^t \right) \sum_{u \in \mathbb{F}_q^m \setminus \{-w\}} \phi(u).
\]

The Lemma follows from the equality above and from the fact that:

\[
\sum_{u \in \mathbb{F}_q^m \setminus \{-w\}} \phi(u) = \sum_{u \in \mathbb{F}_q^m} \phi(u) - \phi(-w) = \psi(0) - \phi(-w).
\]

We want to characterize the kernel of \( T_{(q,m)} \), in order to do that, we need the following lemma:

**Lemma 2.5.** A function \( \phi \in \mathcal{G}_{(q,m)} \) verifies

\[
\phi(w) \cdot \left( q - \sum_{t \in \mathbb{F}_q} Z^t \right) = 0
\]

for each \( w \in \mathbb{F}_q^m \) if, and only if,

\[
\phi(w) = \lambda(w) \sum_{t \in \mathbb{F}_q} Z^t,
\]
where $\lambda$ is a function from $\mathbb{F}_q^m$ into $\mathbb{C}$.

Proof. Let $\phi$ be given by $\phi(w) = \sum_{t \in \mathbb{F}_q} C_t(\phi)(w)Z^t$, then we have

$$\phi(w) \cdot \left(q - \sum_{t \in \mathbb{F}_q} Z^t\right) = q\phi(w) - \left(\sum_{t \in \mathbb{F}_q} C_t(\phi)(w)\right)\left(\sum_{t \in \mathbb{F}_q} Z^t\right).$$

If this product is equal to zero, then

$$\phi(w) = \left(1/q\right) \left(\sum_{t \in \mathbb{F}_q} C_t(\phi)(w)\right)\left(\sum_{t \in \mathbb{F}_q} Z^t\right).$$

On the other hand a direct computation of

$$\left(\lambda(w) \sum_{t \in \mathbb{F}_q} Z^t\right) \cdot \left(q - \sum_{t \in \mathbb{F}_q} Z^t\right)$$

does the converse.  \hfill \Box

Now we can determine the kernel of $T_{(q,m)}$.

**Theorem 2.6.** The kernel of $T_{q,m}$ is the subspace of the functions $\phi$ such that for each $w \in \mathbb{F}_q^m$ \n
$$\phi(w) = \lambda(w) \sum_{t \in \mathbb{F}_q} Z^t$$

where $\lambda$ is any function from $\mathbb{F}_q^m$ into $\mathbb{C}$ verifying \n
$$\sum_{u \in \mathbb{F}_q^m} \lambda(u) = 0.$$

The dimension of the kernel is $q^m - 1$.

Proof. Note that if the transform of $\phi$ is the zero function, then using the Proposition 2.4 we get

$$\phi(w) \cdot \left(q - \sum_{t \in \mathbb{F}_q} Z^t\right) = 0,$$

and by Lemma 2.5

$$\phi(w) = \lambda(w) \sum_{t \in \mathbb{F}_q} Z^t.$$

Hence, for each $t \in \mathbb{F}_q$ we must have

$$C_t(\phi)(w) = \lambda(w).$$
If we denote by $\psi$ the transform of $\phi$ we know that

$$C_t(\psi)(w) = \sum_{u \in \mathbb{F}_q^m} C_{(u,w)+t}(\phi)(u)$$

$$= \sum_{u \in \mathbb{F}_q^m} \lambda(u)$$

The result follows. Let us remark that the functions $\lambda$ such that

$$\sum_{u \in \mathbb{F}_q^m} \lambda(u) = 0,$$

defines an hyperplane of the space of functions from $\mathbb{F}_q^m$ into $\mathbb{C}$ and then, the dimension of the kernel is $q^m - 1$. □

**Proposition 2.7.** The functions

$$\delta_a = \sum_{t \in \mathbb{F}_q} (e_{0,t} - e_{a,t})$$

with $a \in \mathbb{F}_q^m \setminus \{0\}$ are a basis of the kernel $\text{Ker}(T_{(q,m)})$, where

$$e_{u,t}(v) = \begin{cases} Z^t & \text{if } v = u \\ 0 & \text{otherwise} \end{cases}$$

The functions $e_{a,t}$ with

$$(a \neq 0 \text{ and } t \neq 0) \text{ or } (a = 0)$$

is a basis of a complement of $\text{Ker}(T_{q,m})$.

**Proof.** For any $a \in \mathbb{F}_q^m \setminus \{0\}$ the following holds:

$$\delta_a(v) = \lambda(v) \sum_{t \in \mathbb{F}_q} Z^t,$$

with $\lambda(0) = 1$, $\lambda(a) = -1$ and $\lambda(v) = 0$ for the other values of $v$, then by Theorem 2.6 $\delta_a$ is in the kernel of $T_{(q,m)}$. As the $e_{a,t}$ are linearly independent, the $\delta_a$ are linearly independent. We conclude that the $\delta_a$ constitute a basis of $\text{Ker}(T_{q,m})$.

Let $I$ be the set

$$I = \{(v, t) \mid (v \neq 0 \text{ and } t \neq 0) \text{ or } (v = 0)\}$$

and $\phi$ the function

$$\phi = \sum_{(v,t) \in I} \lambda_{v,t} e_{v,t}.$$
The following holds:

\[ T_{(q,m)}(\phi)(v) = \sum_{\{t|(v,t)\in I\}} \lambda_{v,t} Z^t. \]

If \( v \neq 0 \) then

\[ T_{(q,m)}(\phi)(v) = \sum_{t \in \mathbb{F}_q} \lambda_{v,t} Z^t. \]

Then \( T_{(q,m)}(\phi)(v) \) cannot be a multiple of \( \sum_{t \in \mathbb{F}_q} Z^t \) unless all the \( \lambda_{v,t} \)
are zero for \( v \neq 0 \) and in this case the coefficient of \( \sum_{t \in \mathbb{F}_q} Z^t \) is 0. Now if \( v = 0 \) then

\[ T_{(q,m)}(\phi)(0) = \sum_{t \in \mathbb{F}_q} \lambda_{0,t} Z^t. \]

Then \( T_{(q,m)}(\phi)(0) \) cannot be a multiple of \( \sum_{t \in \mathbb{F}_q} Z^t \) unless all the \( \lambda_{0,t} \) have the same value \( \lambda_0 \) and in this case the coefficient of \( \sum_{t \in \mathbb{F}_q} Z^t \) is \( \lambda_0 \). Hence, if \( T_{(q,m)}(\phi)(v) \) can be written \( \lambda(v) \sum_{t \in \mathbb{F}_q} Z^t \), we have \( \sum_{v \in \mathbb{F}_q} \lambda(v) = \lambda_0 \). Then, if \( \phi \in \text{Ker}(T_{(q,m)}) \), for any \( (v,t) \in I \) we have \( \lambda_{v,t} = 0 \). We conclude that the \( q^{m+1} - (q^m - 1) \) linearly independent vectors \( (e_{v,t})_{(v,t)\in I} \) constitute a basis of a complement of \( \text{Ker}(T_{(q,m)}) \).

**Corollary 2.8.** The vectors \( \epsilon_{v,t} = T_{(q,m)}(e_{v,t}) \) with \( (v,t) \in I \) are linearly independent. They constitute a basis of the image \( T_{(q,m)}(G_{(q,m)}) \).

3. **Application to the Hamming distances from a function to all codewords of a Generalized Reed-Muller code of order 1**

3.1. **System of equations satisfied by the distances of a function to all codewords.** Coming back to our problem, if \( f \in \mathcal{F}_{(q,m)} \) let us associate to it the function \( F \in \mathcal{G}_{(q,m)} \) defined by

\[ F(u) = Z^{f(u)}. \]

The transform \( T_{(q,m)}(F) \) is given by

\[ T_{(q,m)}(F)(v) = \sum_{u \in \mathbb{F}_q^m} Z^{f(u)-\langle u,v \rangle} = \sum_{t \in \mathbb{F}_q} N_{v,t}(f) Z^t, \]

where \( N_{v,t}(f) = \# \{ u \in \mathbb{F}_q^m | f(u) - \langle u, v \rangle = t \} \) as defined before.

**Lemma 3.1.** Pour any \( v \in \mathbb{F}_q^m \) the following formula holds:

\[ \sum_{t \in \mathbb{F}_q} N_{v,t}(f) = q^m. \]
Proof. It is a direct consequence of the equalities (2). Indeed the total sum of coefficients in the first expression is $q^m$ and in the second one it is $\sum N_{v,t}$.

As one can see, the numbers $N_{v,t}(f)$ are exactly the coefficients of $T_{(q,m)}(F)$ where $F$ is associated to $f$ as above.

For each $w \in \mathbb{F}_{q^m}$ we consider the linear form $L_w$ defined over $\mathbb{F}_{q^m} \times \mathbb{F}_q$ by

$$L_w(v, t) = -\langle w, v \rangle + t,$$

and for each $w \in \mathbb{F}_{q^m}$ and each $\tau \in \mathbb{F}_q$ we consider the hyperplane $E_{w,\tau}$ of $\mathbb{F}_{q^m} \times \mathbb{F}_q$ defined by

$$E_{w,\tau} = \{ (v, t) \in \mathbb{F}_{q^m} \times \mathbb{F}_q \mid L_w(v, t) = \tau \}.$$

Theorem 3.2. Let $f \in \mathcal{F}_{(q,m)}$, then $N_{v,t}(f)$ are solutions of the following linear system with $q^m + 1$ equations on $q^m + 1$ variables where the equation numbered $(w, \tau)$ is:

$$(w, \tau) \sum_{(v, t) \in E_{w,\tau}} x_{v, t} = \begin{cases} q^{2m-1} - q^{m-1} & \text{if } f(-w) \neq \tau \\ q^{2m-1} - q^{m-1} + q^m & \text{if } f(-w) = \tau \end{cases}$$

Proof. Computing $T^2_{(q,m)}(F)$, where $F = Z^f$ and by using the result of Theorem 2.4 we obtain

$$T^2_{(q,m)}(F)(w) = q^{m-1}(q - \sum_{t \in \mathbb{F}_q} Z^t)F(-w) + q^{m-1} \sum_{t \in \mathbb{F}_q} Z^t \sum_{u \in \mathbb{F}_{q^m}} F(u).$$

Denoting $K(Z) = \sum_{t \in \mathbb{F}_q} Z^t$ and observing that

$$K(Z) \sum_{t \in \mathbb{F}_q} \alpha_t Z^t = (\sum_{t \in \mathbb{F}_q} \alpha_t)K(Z),$$

we obtain

$$T^2_{(q,m)}(F)(w) = q^m Z f(-w) + K(Z)(q^{2m-1} - q^{m-1})$$

$$= (q^{2m-1} - q^{m-1} + q^m) Z f(-w)$$

$$+ (q^{2m-1} - q^{m-1}) \sum_{t \neq f(-w)} Z^t.$$

On the other hand, if we compute $T^2_{(q,m)}(F)$ using that

$$T_{(q,m)}(F)(v) = \sum_{t \in \mathbb{F}_{q^m}} N_{v,t} Z^t,$$
we obtain

\[ T_{(q,m)}^2(F)(w) = \sum_{\tau \in F_q} \left( \sum_{(v,t) \in E_{w,\tau}} N_{v,t} \right) Z^\tau. \]

The theorem follows by comparing the two expressions obtained for \( T_{(q,m)}^2(F) \).

**Remark 3.3.** The system presented in Theorem 3.2 has the following structure: it is constituted by \( q^m \) blocks \( B_w \) of \( q \) equations. The block \( B_w \) contains the \( q \) equations numbered \((w,\tau)\) where \( w \) is fixed and \( \tau \) takes the \( q \) possible values in \( F_q \). Each equation of a block involves \( q^m \) variables, namely the variables indexed by the points \((v,t)\) of the hyperplane \( E_{w,\tau} \) of \( F_q^m \times F_q \). The \( q \) hyperplanes \( E_{w,\tau} \) (\( w \) fixed, \( \tau \in F_q \)) are parallel, then each variable \( x_{v,t} \) is in one and only one equation of each block \( B_w \).

Let us consider the basis defined in section 2 by (1). Remark that the matrix of the system (3.2) is the matrix \( T_{(q,m)} \) of \( T_{(q,m)} \) with respect to the considered basis. Namely by construction (see the proof of Theorem 3.2), the system can be written

\[ T_{(q,m)}X = B, \]

where \( X \) is the column

\[ X = \begin{pmatrix} \vdots & \vdots & \vdots & \vdots & x_{v,t} & \vdots \end{pmatrix}, \]

and \( B \) the column

\[ B = \begin{pmatrix} \vdots & \vdots & \vdots & \vdots & b_{w,\tau} & \vdots \end{pmatrix}, \]

where

\[ b_{w,\tau} = \begin{cases} q^{2m-1} - q^{m-1} & \text{if } f(-w) \neq \tau \\ q^{2m-1} - q^{m-1} + q^m & \text{if } f(-w) = \tau \end{cases}. \]

The system has a solution because we know that the values \( N_{v,t}(f) \) constitute a solution. But, as the linear map \( T_{(q,m)} \) has a kernel, the system has not a unique solution. However, if we add some “normalization” conditions we obtain the desired solution.
Theorem 3.4. The numbers $N_{v,t}(f)$ are the unique solution of the system that appears on the Theorem 3.2 if we join the following $q^m$ equations

$$\sum_{t \in \mathbb{F}_q} x_{v,t} = q^m , \quad \forall v \in \mathbb{F}_{q^m}.$$ 

Proof. We know that any other solution is obtained from the previous solution $(N_{v,t})_{v,t}$ by adding an element in the kernel of the transformation, that is any other solution has the form $(N_{v,t} + \lambda(v))_{v,t}$ with $\sum v \lambda(v) = 0$. For any $v$ fix, we have that $\sum_{t \in \mathbb{F}_q} N_{v,t} = q^m$ and the result follows from it. \qed

3.2. Transformation into a Cramer linear system.

Theorem 3.5. The system $(S)$ constructed in the following way:

1. suppress from the system (3.2) the $q^m - 1$ lines numbered $(w,0)$ with $w \neq 0$,
2. replace these equations by the $q^m - 1$ equations $\sum_{t \in \mathbb{F}_q} x_{w,t} = q^m$, where $w \neq 0$,

is a Cramer linear system and has $(N_{v,t}(f))_{v,t}$ for unique solution.

Proof. Let $T_{(q,m)}$ the matrix of the original system. The columns are the vectors $T_{(q,m)}(e_{v,t}) = e_{v,t}$ decomposed on the basis $(e_{v,t})_{(v,t) \in \mathbb{F}_q \times \mathbb{F}_q}$.

Let us consider the columns $(v,t)$ for which one of the two following conditions holds:

1. $v = 0$;
2. $v \neq 0$ and $t \neq 0$.

Denote by $I$ these indexes. We know by Lemma 2.8 that these $q^{m+1} - (q^m - 1)$ columns are linearly independent.

Denote by $a_{(w,\tau),(v,t)}$ the coefficient of $T_{(q,m)}$ which is at the line indexed by $(w,\tau)$ and the column indexed by $(v,t)$. This coefficient is the component of $\delta_{v,t}$ on $e_{w,\tau}$, namely by Lemma 2.2

$$a_{(w,\tau),(v,t)} = \begin{cases} 1 & \text{if } (w, \tau) \in E_{v,t} \\ 0 & \text{if } (w, \tau) \notin E_{v,t} \end{cases}.$$ 

But as the relation $(w, \tau) \in E_{v,t}$ is equivalent to $(v,t) \in E_{w,\tau}$ we have

$$a_{(w,\tau),(v,t)} = a_{(v,t),(-w,\tau)}.$$ 

Then the elements of line $((w, \tau)$ are the elements of the column $(-w, \tau)$ By Proposition 2.7 the $q^{m+1} - (q^m - 1)$ lines indexed by $(w, \tau)$ where $w \neq 0$ and $t \neq 0$, or $w = 0$, are linearly independent.
Remark that the original system has a vector space of dimension $q^m - 1$ of solutions $(x_{v,t})_{(v,t) \in \mathbb{F}_q^m \times \mathbb{F}_q}$. Adding all equations of the system gives the following equality:

$$\sum_{v,t} x_{v,t} = q^{2m}.$$ 

Then if we suppose that the $q^m - 1$ conditions

$$\sum_{t \in \mathbb{F}_q} x_{v,t} = q^m,$$

where $v \neq 0$, are satisfied, the last condition

$$\sum_{t \in \mathbb{F}_q} x_{0,t} = q^m$$

is also satisfied. Now, using Theorem 3.4, we conclude that $(S)$ is a Cramer linear System. □

**Remark 3.6.** From the definition it follows that

$$N_{v,t} = \text{card}\left( \{ w \in \mathbb{F}_q^m \mid (v,t) \in E_{w,f(-w)} \} \right).$$

So, it would be interesting to consider the arrangement of hyperplanes $A(f)$, consisting of the $q^m$ hyperplanes $E_{w,f(-w)}$ and to relate the geometric and combinatorial properties of $A(f)$ to the properties of the distance between $f$ and the affine functions. A very simple example is the following: if the arrangement $A(f)$ is centered, then there is a $(v,t)$ such that $N_{v,t} = q^m$ and consequently the function $f$ is affine.

**REFERENCES**

[1] Alexei Ashikhmin and Simon Litsyn. Fast decoding of non-binary first order reed-muller codes. AAECC, 7:299–308, 1996.

[2] Robert Rolland. Fonction maximalement non linéaires sur un corps fini. Technical Report 25, Institut de Mathématiques de Luminy, 2000.

IME, UNIV. FEDERAL FLUMINENSE, RUA MARIO SANTOS BRAGA S/N, CEP 24.020-140, NITEROI, BRAZIL

E-mail address: miriam@mat.uff.br

Université d’AIX-MARSEILLE, INSTITUT DE MATHEMATIQUES DE MARSEILLE, case 907, F13288 MARSEILLE CEDEX 9, FRANCE

E-mail address: robert.rolland@acrypta.fr