Hermitian forms, trace equations and application to codes

Dany-Jack Mercier*

November 14th, 2001

Abstract:

We provide a systematic study of sesquilinear hermitian forms and a new proof of the calculus of some exponential sums defined with quadratic hermitian forms. The computation of the number of solutions of equations such as $\text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x) + v.x) = 0$ or $\text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)) = a$ allows us to construct codes and to obtain their parameters.

Key-Words:

Sesquilinear Hermitian Forms, Quadratic Forms, Finite Fields, Traces, Exponential Sums, Codes.

MSC-Class:

94B05, 11T23, 11T71.

Versions:

Minor changes in version 2 (21th April 2003).

1 Introduction

Let $\mathbb{F}_t$ be the finite field with $t$ elements and characteristic $p$. Our first purpose is to adapt the classical hermitian form Theory on $\mathbb{C}$ to the case of the finite field $\mathbb{F}_2$, considering the involution $x \mapsto x^t$ in $\mathbb{F}_{t^2}$ instead of the application $z \mapsto \overline{z}$. Then we introduce exponential sums associated with quadratic hermitian forms and obtain the number of solutions of certain equations on $\mathbb{F}_t$. At this point it is easy to construct two linear codes using the same method as Reed-Muller codes, to get their parameters and to compare them to the classical Reed-Muller construction.

A general introduction to hermitian forms over a finite field is given by Bose and Chakravarti in [1], and the use of those objects in coding Theory has been discussed for instance in [3], [4] or [5].

*NT/0111191 [cco0007] v 1.00 Equipe Applications de l’Algèbre et de l’Arithmétique, Département de Mathématiques & Informatique, Université des Antilles-Guyane, Campus Fouillole, F97159 Pointe-à-Pitre cedex, France, e-mail : dany-jack.mercier@univ-ag.fr.
My first contribution will be to review in details the main results of [1] and [3], giving alternative proofs of some important results in the Theory. It is worth pointing out that the existence of a $H$-orthogonal basis is shown by induction without explicit calculus on rows and columns of a matrix as in [1] (see Theorem 4). Another example is given by a new and straightforward proof of the most precious result of the paper of Cherdieu [3] (see Theorem 14).

Section 10 is devoted to the construction of the code $\Gamma$ of [3], and Section 11 use the same argument to give another example of such a linear code. As this paper wants to remain self-contained, an annex in Section 12 will summarize without proofs the relevant material on characters on a finite group.

2 Sesquilinear hermitian forms on $\mathbb{F}_{t^2}^N$

Let $N$ be an integer $\geq 1$ and let $E$ be the vector space $\mathbb{F}_{t^2}^N$.

**Définition 1** A function $H : \mathbb{F}_{t^2}^N \times \mathbb{F}_{t^2}^N \rightarrow \mathbb{F}_{t^2}$ is a sesquilinear form on $E = \mathbb{F}_{t^2}^N$ if it is semi-linear in the first variable and linear in the second variable, i.e.

1. $\forall \lambda, \mu \in \mathbb{F}_{t^2} \ \forall x, x', y \in E \ \ H(\lambda x + \mu x', y) = \lambda H(x, y) + \mu H(x', y)$,
2. $\forall \lambda, \mu \in \mathbb{F}_{t^2} \ \forall x, y, y' \in E \ \ H(x, \lambda y + \mu y') = \lambda H(x, y) + \mu H(x, y')$.

The sesquilinear form $H$ is called **hermitian** if

3. $\forall x, y \in E \ \ H(x, y) = H(y, x)^t$.

A sesquilinear hermitian form will be called a **hermitian form** on $E$. The vector space of all hermitian forms on $\mathbb{F}_{t^2}^N$ will be denoted by $H(\mathbb{F}_{t^2}^N)$.

Note that properties (2) and (3) give (1), and that $H(x, x) \in \mathbb{F}_t$ for all $x \in E$ as soon as $H$ is a hermitian form.

If $x \in \mathbb{F}_{t^2}$ we put $\overline{x} = x^t$ and we say that $\overline{x}$ is the conjugate of $x$. If $\alpha \in \mathbb{F}_{t^2}$ satisfies $\mathbb{F}_{t^2} = \mathbb{F}_t(\alpha)$, each element $x$ of $\mathbb{F}_{t^2}$ is uniquely written as $x = a + b\alpha$ with $a$ and $b$ in $\mathbb{F}_t$. Then $\overline{x} = (a + b\alpha)^t = a + b\overline{\alpha}$.

**Définition 2** Let $A = (a_{ij})_{i,j}$ be a square matrix with $i, j = 1, ..., N$ and with entries in $\mathbb{F}_{t^2}$. We denote by $\overline{A}$ the matrix $\overline{A} = (\overline{a_{ij}})_{i,j}$ and by $^tA$ the transpose of $A$. The **conjugate** of $A = (a_{ij})_{i,j}$ is the matrix $A^* = ^T(\overline{A}) = (\overline{a_{ji}})_{i,j}$. The matrix $A$ is **hermitian** if $A^* = A$.

If $e = (e_1, ..., e_N)$ is a basis of $E$ and if $H$ is a sesquilinear form on $E$,

$$H(x, y) = H\left(\sum_i x_ie_i, \sum_j y_je_j\right) = \sum_{i,j} \overline{x}_i y_j H(e_i, e_j) = X^*MY$$

where $M = (H(e_i, e_j))_{i,j}$, $X = ^T(x_1, ..., x_N)$ and $Y = ^T(y_1, ..., y_N)$. We say that $M$ is the **matrix of $H$ in the basis $e$**, and we write $M = \text{Mat}(H; e)$.

**Théorème 1** A sesquilinear form $H$ is hermitian if, and only if, its matrix $\text{Mat}(H; e)$ in a basis $e$ is hermitian.
Proof: Let $M$ denotes the matrix $\text{Mat}(H; e)$. If $H$ is a hermitian form, $H(e_i, e_j) = \overline{H(e_j, e_i)}$ implies $M^* = M$. Conversely, $M^* = M$ implies
\[ \forall X,Y \quad H(Y, X) = Y^T M X = T Y^T M X = T (T Y^T M X) = X^* M Y = H(X, Y). \]

Corollaire 1 $\dim_{\mathbb{F}_2} (\mathbb{F}_2^N) = N^2$.

Proof: The matrix $H = (a_{ij})$ of a hermitian form depends on $\frac{N^2 - N}{2}$ coefficients $a_{ij}$ (where $1 \leq j < i \leq N$) in $\mathbb{F}_2$ and $N$ coefficients $a_{ii}$ ($1 \leq i \leq N$) in $\mathbb{F}_2$. Thus we have $2 \times \frac{N^2 - N}{2} + N = N^2$ independent parameters.

Let $P_{e'} = P$ denotes a change of coordinates from a basis $e = (e_1, ..., e_N)$ to another basis $e' = (e'_1, ..., e'_N)$. Let $X = T (x_1, ..., x_N)$ and $X' = T (x'_1, ..., x'_N)$ stands for the $N$-tuplets of coordinates of the same vector in basis $e$ and $e'$. Then
\[ H(X, Y) = X^* M Y = (P X')^* M (P Y') = X'^* (P^* M P) Y' \]
and $\text{Mat}(H; e') = P^* M P$ is the matrix of $H$ in the new basis $e'$.

3 Kernel and rank of $H$

If $x \in E$ and if $H$ denotes a hermitian form, we define the linear application $H(x,.)$ in the dual $E^*$ by:
\[ H(x,.): \quad E \to \mathbb{F}_2 \quad y \mapsto H(x, y). \]

The map:
\[ \tilde{H}: \quad E \to E^* \quad x \mapsto H(x,.). \]

is semi-linear, i.e. satisfies $\tilde{H}(\lambda x + x') = \tilde{H}(x) + \tilde{H}(x')$ for all vectors $x, x'$ and all $\lambda \in \mathbb{F}_2$. The extern law $\bullet$ defined by $\lambda \bullet l = \tilde{H}(\lambda)l$ gives us a new vector space structure on $E^*$.

For convenience, we shall write $E^\#$ instead of $E^*$ when we use this new extern law. The map $\tilde{H}: E \to E^\#$ is semi-linear if, and only if, $\tilde{H}: E \to E^\#$ is linear, and we can introduce the matrix of $\tilde{H}$ in the basis $e = (e_1, ..., e_N)$ in $E$ and the dual basis $e^* = (e'_1, ..., e'_N)$ in $E^\#$. The linearity of $\tilde{H}$ gives us the same results as in the case of symmetric bilinear forms. Namely:

Théorème 2 The equality $\text{Mat}(\tilde{H}; e, e^*) = \text{Mat}(H; e)$ holds for all hermitian form $H$.

Proof: Assume that $\text{Mat}(\tilde{H}; e, e^*) = (a_{ij})$. Then $\tilde{H}(e_j) = \sum_i a_{ij} \bullet e_i^*$ and
\[ \tilde{H}(e_j)(e_k) = H(e_j, e_k) = \overline{a_{kj}}. \]

Thus $\text{Mat}(\tilde{H}; e, e^*) = T \text{Mat}(H; e) = \text{Mat}(H; e)$. ■

Définition 3 The kernel $\text{Ker} H$ (resp. rank $\text{rk} H$) of $H$ is the kernel (resp. rank) of $\tilde{H}$. Thus $\text{Ker} H = \{x \in E \mid \forall y \in E \quad H(x, y) = 0\}$ and $\text{rk} H = \text{rk} (\text{Mat}(H; e))$.
4 Orthogonality

Définition 4 Let $H$ denotes a hermitian form on $E$. Vectors $x$ and $y$ are orthogonal if $H(x, y) = 0$. If $F$ is a subset of $E$, the subspace $F^\perp = \{ x \in E / \forall y \in F \quad H(x, y) = 0 \}$ is called the orthogonal of $F$.

It is easily seen that:

Théorème 3 For all subspaces $F$ and $G$ in $E$,

$$ F \subset (F^\perp)^\perp, \quad (F + G)^\perp = F^\perp \cap G^\perp, \quad (F \cap G)^\perp \supset F^\perp + G^\perp. $$

Définition 5 A basis $e = (e_1, ..., e_N)$ is orthogonal for the hermitian form $H$ (we say $H$-orthogonal) if $H(e_i, e_j) = 0$ when $i \neq j$. This means that the matrix $\text{Mat}(H; e)$ is diagonal.

Lemme 1 Let $H$ denotes a sesquilinear form on $E$. If $t$ is odd and if $q(x) = H(x, x)$, then for all $x, y$ in $E$,

1) $H(x, y) + H(y, x) = \frac{1}{2}[q(x + y) - q(x - y)]$,
2) $H(x, y) - H(y, x) = \frac{1}{2}\alpha [q(x + \alpha y) - q(x + \bar{\alpha}y)]$,
3) $H(x, y) = \frac{1}{4}[q(x + y) - q(x - y)] + \frac{1}{2(\alpha - \bar{\alpha})}[q(x + \alpha y) - q(x + \bar{\alpha}y)].$

Proof: We have

$$ q(x + y) - q(x - y) = q(x) + H(x, y) + H(y, x) + q(y) $$

$$ - [q(x) + H(x, y) + H(y, x) + H(-y, y)] $$

$$ = 2(H(x, y) + H(y, x)). $$

and

$$ q(x + \alpha y) - q(x + \bar{\alpha}y) = q(x) + \alpha H(x, y) + \alpha^t H(y, x) + \alpha^{t+1}q(y) $$

$$ - [q(x) + \alpha^t H(x, y) + \alpha H(y, x) + \alpha^{t+1}q(y)] $$

$$ = (\alpha - \alpha^t)(H(x, y) - H(y, x)). $$

As $\alpha \notin \mathbb{F}_t$, we have $\alpha^t \neq \alpha$ and the Lemma follows.

Lemme 2 The norm application

$$ N_{\mathbb{F}_t/m/\mathbb{F}_t} : \mathbb{F}_t^m \to \mathbb{F}_t^* $$

$$ x \mapsto x^{m-1+...+t+1} $$

is a multiplicative group epimorphism, and $|N_{\mathbb{F}_t/m/\mathbb{F}_t}^{-1}(b)| = \frac{t^m - 1}{t-1}$ for all $b \in \mathbb{F}_t^*$.

Proof: It is obvious that the map $N_{\mathbb{F}_t/m/\mathbb{F}_t}$ is a morphism. Consider a primitive element $\alpha$ in $\mathbb{F}_t^m$. It means that $\alpha$ generates the multiplicative group $\mathbb{F}_t^*$, hence

$$ \mathbb{F}_t^m = \{ 0, 1, \alpha, \alpha^2, ..., \alpha^{m-2} \}. $$
Each element \(x^{m-1+...t+1}\) lies in \(\mathbb{F}_t\) as \((x^{m-1+...t+1})^t = x^{m-1+...t+1}\), and for \(1 \leq u \leq t-1\), all elements \(\alpha^{u(m-1+...t+1)}\) are different. Thus:

\[
\mathbb{F}_t = \left\{0, \alpha^{(m-1+...t+1)}, \alpha^{2(t-1)(m-1+...t+1)}, ..., \alpha^{(t-1)(m-1+...t+1)}\right\}
\]

and \(N_{\mathbb{F}_t}/\mathbb{F}_t\) is surjective. The decomposition of the morphism \(N_{\mathbb{F}_t}/\mathbb{F}_t\) gives:

\[
\mathbb{F}_t^*/\ker(N_{\mathbb{F}_t}/\mathbb{F}_t) \cong \mathbb{F}_t^*,
\]

hence \(|\ker(N_{\mathbb{F}_t}/\mathbb{F}_t)| = \frac{m-1}{t-1}|.\) If \(a \in N_{\mathbb{F}_t}/\mathbb{F}_t\) (b), then:

\[
N_{\mathbb{F}_t}/\mathbb{F}_t (x) = b \iff N_{\mathbb{F}_t}/\mathbb{F}_t (xa^{-1}) = 1 \iff x \in a\ker(N_{\mathbb{F}_t}/\mathbb{F}_t)
\]

and we deduce \(|N_{\mathbb{F}_t}/\mathbb{F}_t (b)| = |\ker N_{\mathbb{F}_t}/\mathbb{F}_t| = \frac{m-1}{t-1}|.\)

**Théorème 4 Existence of \(H\)-orthogonal basis**

If \(t\) is odd and if \(H\) is a hermitian form on \(E = \mathbb{F}_N^t\),

1) We can find a \(H\)-orthogonal basis \(e = (e_1, ..., e_N)\), and assume \(H(e_i, e_i) = 0\) or \(1\) for all \(i\),

2) The number \(r\) of non zero entries in the diagonal of \(\text{Mat}(H; e)\) is an invariant that depends only on \(H\). It is the rank of \(H\).

**Proof :** The proof of 1) is by induction on \(N\). Assume \(N = 1\). The result is obvious if \(H(x, x) = 0\) for all \(x\). If \(x \in E\) satisfies \(H(x, x) = b \in \mathbb{F}_t^*,\) Lemma 2 shows the existence of \(a \in \mathbb{F}_2^t\) such that \(a^{t+1} = b\). Hence \(H(\frac{a}{a}, \frac{a}{a}) = 1\) and we take the basis \(e_1 = \frac{a}{a}\).

Assuming the result holds for \(N\), we will prove it for \(\dim E = N + 1\). We need only consider two cases :

- If \(H(x, x) = 0\) for all \(x\), then all basis are \(H\)-orthogonal by formula 3) in Lemma 4

- If there exists \(x\) with \(H(x, x) \neq 0\), we proceed as in the case \(N = 1\) to show the existence of \(a \in \mathbb{F}_2^s\) such that \(H(\frac{a}{a}, \frac{a}{a}) = 1\). The subspace

\[
F = (Kx)^\perp = \{y \in E / H(x, y) = 0\} = \ker H(x)
\]

is a hyperplane of \(E\) as it is the kernel of a non zero linear form. But \(E = F \oplus \text{Vect}(x)\) since \(x \notin F\), and the induction hypothesis gives a \(H\)-orthogonal basis \((e_1, ..., e_{N-1})\) of \(F\) with \(H(e_i, e_i) = 0\) or \(1\) for all \(i\). We check at once that \((e_1, ..., e_{N-1}, \frac{a}{a})\) is a \(H\)-orthogonal basis of \(E\) and this complete the proof of 1). The second part of the Theorem follows from

\[
\text{rk } H = \text{rk } H = \text{rk } \text{Mat}(H; e).
\]

**Définition 6 A hermitian form \(H\) is non degenerate if \(E^\perp = \{0\}\).**

**Théorème 5 Let \(H\) be a hermitian form. The following conditions are equivalent:**

1) \(H\) is non degenerate,

2) \(\ker H = \{0\}\),

3) \(H\) is an isomorphism from \(E\) to \(E^*\),

4) \(\text{Mat}(H; e)\) is non singular.
**Proof**: From \( E^\perp = \{ x \in E \mid \forall y \in E \quad H(x,y) = 0 \} = \text{Ker} \bar{H} \) we conclude that 1) is equivalent to 2). Since \( \dim E = \dim \overline{E^*} \), the condition \( \text{Ker} \bar{H} = \{ 0 \} \) means that \( \bar{H} \) is an isomorphism from \( E \) to \( \overline{E^*} \), and it suffices to observe that Mat \((H; e)\) is the matrix of \( \bar{H} \) to complete the proof. \( \blacksquare \)

**Théorème 6** Theorem \( \mathbb{3} \) can be improved if \( H \) is non degenerate. We get:

\[
\dim F + \dim F^\perp = n, \quad F = \left( F^\perp \right)^\perp \quad \text{and} \quad (F \cap G)^\perp = F^\perp + G^\perp.
\]

**Proof**: Let \((e_1, \ldots, e_p)\) denotes a basis of \( F \). As \( \bar{H} \) is an isomorphism, the orthogonal

\[
F^\perp = \{ x \in E / \forall i \in \mathbb{N}_p \quad H(x,e_i) = 0 \} = \bigcap_{i=1}^{p} \ker \bar{H}(e_i)
\]

is the intersection of \( p \) kernels of independant linear forms. Hence \( \dim F^\perp = n - p \). The inclusion \( F \subset (F^\perp)^\perp \) and the equality \( \dim (F^\perp)^\perp = n - \dim F^\perp = \dim F \) give us the second result. It is sufficient to write the relation \( (F + G)^\perp = F^\perp \cap G^\perp \) of Theorem \( \mathbb{3} \) with \( F^\perp \) and \( G^\perp \) instead of \( F \) and \( G \) to prove the last result. \( \blacksquare \)

### 4.1 Isotropy

**Définition 7** Let \( H \) be a hermitian form on \( E = \mathbb{F}^N_{\mathbb{C}} \). A subspace \( F \) of \( E \) is called isotropic if \( F \cap F^\perp \neq \{ 0 \} \). A vector \( x \) is isotropic if \( H(x,x) = 0 \).

Note that a non null vector \( x \) is isotropic if and only if the subspace \( \text{Vect}(x) \) generated by \( x \) is isotropic.

**Théorème 7** Let \( H \) denote a hermitian form on \( E = \mathbb{F}^N_{\mathbb{C}} \), and \( F \) a subspace of \( E \). The following conditions are equivalent:

(i) The restriction \( H|_{F \times F} \) of \( H \) to \( F \) is non degenerate,

(ii) \( F \) is non isotropic,

(iii) \( E = F \oplus F^\perp \).

**Preuve**: Equivalence between (i) and (ii) follows from:

\[
(i) \iff \forall x \in F \quad ((\forall y \in F \quad H(x,y) = 0) \Rightarrow x = 0)
\]
\[
\iff \forall x \in F \quad (x \in F^\perp \Rightarrow x = 0) \iff F \cap F^\perp = \{ 0 \} \iff (ii).
\]

We see at once that (iii) implies (ii). Let us show that (i) implies (iii). If \( H|_{F \times F} \) is non degenerate, we already have \( F \cap F^\perp = \{ 0 \} \), and it only remains to prove that \( E = F + F^\perp \). Let \( x \in E \). Let \( l \) be the linear form \( F \to \mathbb{F}_{\mathbb{C}} : z \mapsto H(x,z) \). Since \( H|_{F \times F} \) is non degenerate, we can find \( y \in F \) such that \( l = H|_{F \times F}(y,.) \), and it shows that

\[
\forall z \in F \quad l(z) = H(x,z) = H(y,z).
\]

Thus \( H(x - y,z) = 0 \) for all \( z \) in \( F \), and we conclude that

\[
\forall x \in E \quad \exists y \in F \quad x = (x - y) + y \text{ et } x - y \in F^\perp. \blacksquare
\]
5 Quadratic hermitian forms on $\mathbb{F}_t^N$

Définition 8 If $H$ denotes a hermitian form, the application

$$q : \ E \rightarrow \mathbb{F}_t$$

$$x \mapsto q(x) = H(x,x)$$

is called the **quadratic hermitian form** on $E$ associated to $H$. We denote by $QH(\mathbb{F}_t^N)$ the space of all quadratic hermitian forms on $E$.

With this Definition:

1. $\forall \lambda \in \mathbb{F}_t^2 \ \forall x \in E \quad q(\lambda x) = \lambda^{t+1}q(x) = N(\lambda)q(x)$,
2. $\forall \lambda \in \mathbb{F}_t \ \forall x \in E \quad q(\lambda x) = \lambda^2q(x)$.

Result (1') explain the name "quadratic" when we restrict our attention on $\mathbb{F}_t$. Result (2) is true when $t$ is odd (see Lemma IV). From now on we assume that $t$ is odd.

Théorème 8 Let $\mathbb{F}_t^E$ denotes the $\mathbb{F}_t$-vector space of all applications from $E$ to $\mathbb{F}_t$. The function

$$\Psi : \ H(\mathbb{F}_t^N) \rightarrow \mathbb{F}_t^E$$

$$H \mapsto q \text{ such that } q(x) = H(x,x)$$

is $\mathbb{F}_t$-linear and one to one. We have $\text{Im} \Psi = QH(\mathbb{F}_t^N)$ and $\Psi$ induces an isomorphism from $H(\mathbb{F}_t^N)$ onto $QH(\mathbb{F}_t^N)$. Hence $\dim_{\mathbb{F}_t} QH(\mathbb{F}_t^N) = N^2$.

Proof : Result (2) shows that $\Psi$ is one to one. ■

Définition 9 Let $q \in QH(\mathbb{F}_t^N)$. The unique hermitian form $H$ satisfying $\Psi(H) = q$ is called the **polar form** of $q$, and is given by result (2). The isomorphism $QH(\mathbb{F}_t^N) \cong H(\mathbb{F}_t^N)$ allows us to construct the same objects from a quadratic hermitian form or from a hermitian form. For instance, the **kernel** and the **rank** of $q$ will be those of the associated polar form.

Let $M = (a_{ij})$ denotes the matrix of a hermitian form $H$ in a basis of $E$. Then

$$H(x,x) = \sum_{i,j} a_{ij}x_i\overline{x}_j = \sum_{i=1}^N a_{ii}x_i^{t+1} + \sum_{1 \leq i < j \leq N} (a_{ij}x_i\overline{x}_j + a_{ji}\overline{x}_i x_j)$$

$$= \sum_{i=1}^N a_{ii}x_i^{t+1} + \sum_{1 \leq i < j \leq N} (a_{ij}x_i\overline{x}_j + (a_{ij}\overline{x}_i x_j)^t).$$

We can say that a quadratic hermitian form $q$ on $E$ is an application from $E$ to $\mathbb{F}_t$ defined by

$$\forall x \in E \quad q(x) = \sum_{i=1}^N a_{ii} N_{\mathbb{F}_t^2/\mathbb{F}_t}(x_i) + \sum_{1 \leq i < j \leq N} \text{Tr}_{\mathbb{F}_t^2/\mathbb{F}_t}(a_{ij}\overline{x}_i x_j)$$

where $(x_1, ..., x_N)$ are the coordinates of $x$ in a basis, $a_{ii} \in \mathbb{F}_t$ and $a_{ij} \in \mathbb{F}_t$ for all $i \neq j$.

In fact Theorem IV ensures us the existence of a $H$-orthogonal basis of $E$. In such a basis

$$q(x) = \sum_{i=1}^r x_i^{t+1} \text{ for all } x \in E.$$
Théorème 9 If \( q \in \mathbb{F}_t^E \) satisfies (1) and if \( H \) defined by (2) is sesquilinear, then \( q \) is the quadratic hermitian form associated with the hermitian form \( H \).

Proof: (1) and (2) show that

\[
H(x, x) = \frac{1}{4} [q(2x) - q(0)] + \frac{1}{2(\alpha - \overline{\alpha})} [q((1 + \alpha)x) - q((1 + \overline{\alpha})x)]
\]

\[
= \frac{1}{4} [2^{t+1}q(x)] + \frac{1}{2(\alpha - \overline{\alpha})} [(1 + \alpha)^{t+1} - (1 + \overline{\alpha})^{t+1}] q(x)
\]

\[
= q(x) + \frac{1}{2(\alpha - \overline{\alpha})} [(1 + \alpha^t)(1 + \alpha) - (1 + \overline{\alpha}^t)(1 + \overline{\alpha})] q(x) = q(x).
\]

By hypothesis, the form \( H \) is sesquilinear, and it remains to prove the hermitian symmetry. We have

\[
H(y, x) = \frac{1}{4} [q(y + x) - q(y - x)] + \frac{1}{2(\alpha - \overline{\alpha})} [q(y + \alpha x) - q(y + \overline{\alpha} x)].
\]

Condition 2) of Lemma \( \square \) yields

\[
q(y + \alpha x) - q(y + \overline{\alpha} x) = q(x + \overline{\alpha} y) - q(x + \alpha y)
\]

hence

\[
H(y, x) = \frac{1}{4} [q(x + y) - q(x - y)] - \frac{1}{2(\alpha - \overline{\alpha})} [q(x + \alpha y) - q(x + \overline{\alpha} y)].
\]

As \( q \) takes its values in \( \mathbb{F}_t \), we conclude that \( H(y, x) = \overline{H(x, y)} \).

Remark: The proof above also gives that a sesquilinear form \( H \) is hermitian if and only if \( H(x, x) \in \mathbb{F}_t \) for all \( x \in E \).

6 Equivalence between quadratic hermitian forms

Définition 10 Two hermitian forms (resp. quadratic hermitian forms) \( \varphi_1 \) and \( \varphi_2 \) (resp. \( q_1 \) and \( q_2 \)) are called equivalent, and we note \( \varphi_1 \sim \varphi_2 \) (resp. \( q_1 \sim q_2 \)), if there exists an automorphism \( u \) of \( E \) such that

\[
\forall x, y \in E \quad \varphi_2(x, y) = \varphi_1(u(x), u(y)) \quad (\text{resp. } \forall x \in E \quad q_2(x) = q_1(u(x))).
\]

Théorème 10 Let \( q_1 \) and \( q_2 \) denote two quadratic hermitian forms whose polar forms are \( \varphi_1 \) and \( \varphi_2 \). The following conditions are equivalent:

i) \( q_1 \) and \( q_2 \) are equivalent,

ii) \( q_1 \) and \( q_2 \) have the same matrix but in different basis,

iii) \( q_1 \) and \( q_2 \) have same rank.

Proof: i) \( \iff \) ii): Let \( e = (e_1, ..., e_N) \) denote a basis of \( E \). We have

\[
(\varphi_1 \sim \varphi_2) \iff \exists u \in \text{GL}(E) \quad \forall x, y \in E \quad \varphi_2(x, y) = \varphi_1(u(x), u(y))
\]

\[
\iff \exists u \in \text{GL}(E) \quad \forall i, j \in \mathbb{N}_n \quad \varphi_2(e_i, e_j) = \varphi_1(u(e_i), u(e_j))
\]

\[
\iff \exists u \in \text{GL}(E) \quad \text{Mat}(\varphi_2; e) = \text{Mat}(\varphi_1; u(e)),
\]

8
We denote by \( QH \) therefore i) implies ii).

Conversely, if there are two basis \( e \) and \( e' \) such that \( \text{Mat} (\varphi_2;e) = \text{Mat} (\varphi_1;e') \), we can define an automorphism \( u \) in \( E \) with \( u(e) = e' \), and use the above equivalences to obtain \( \varphi_1 \sim \varphi_2 \).

\( ii) \iff iii) \) : If \( \text{Mat} (\varphi_2;e) = \text{Mat} (\varphi_1;e') \) then \( \varphi_1 \) and \( \varphi_2 \) have same rank. Conversely, if \( \varphi_1 \) and \( \varphi_2 \) have same rank \( r \), Theorem 4 provides two basis \( e \) and \( e' \) such that \( \text{Mat} (\varphi_2;e) \) and \( \text{Mat} (\varphi_1;e') \) are equal to the diagonal matrix \( \text{Diag} (1, ..., 1, 0, ..., 0) \) with \( r \) numbers 1, ■

7 Quadratic hermitian forms on \( \mathbb{F}_t^{2N} \)

Suppose \( t \) odd. Let \( H : \mathbb{F}_t^N \times \mathbb{F}_t^N \to \mathbb{F}_t^2 \) be a sesquilinear form and \( \alpha \) denotes an element of \( \mathbb{F}_t^2 \) with \( \mathbb{F}_t^2 = \mathbb{F}_t (\alpha) \). The application \( \iota : \mathbb{F}_t^{2N} \to \mathbb{F}_t^2 \) defined by

\[
\iota (x_1, ..., x_{2N}) = (x_1 + \alpha x_2, ..., x_{2N-1} + \alpha x_{2N})
\]

is an \( \mathbb{F}_t \)-vector space isomorphism. Since \( H : \mathbb{F}_t^N \times \mathbb{F}_t^N \to \mathbb{F}_t^2 \) is \( \mathbb{F}_t \)-bilinear, it will be the same with \( \mathbb{F}_t^{2N} \times \mathbb{F}_t^{2N} \to \mathbb{F}_t^2 ; (x, y) \mapsto H (\iota x, \iota y) \). Roughly speaking, we want to work with functions with values in \( \mathbb{F}_t \), thus it is convenient to define:

\textbf{Définition 11} The quadratic hermitian form \( f \) on \( \mathbb{F}_t^{2N} \) associated with \( H \) is

\[
f : \mathbb{F}_t^{2N} \to \mathbb{F}_t \quad x \mapsto H (\iota x, \iota x).
\]

We denote by \( QH (\mathbb{F}_t^{2N}) \) the vector space of all quadratic hermitian forms \( f \) on \( \mathbb{F}_t^{2N} \).

It is clear that the function

\[
QH (\mathbb{F}_t^N) \to QH (\mathbb{F}_t^{2N})
\]

\[
q \mapsto f
\]

where \( f(x) = H (\iota x, \iota x) \) when \( q(x) = H (x, x) \), is an isomorphism between \( \mathbb{F}_t \)-vector spaces, hence \( \dim_{\mathbb{F}_t} QH (\mathbb{F}_t^{2N}) = N^2 \).

\textbf{Théorème 11} Suppose \( t \) odd. The quadratic hermitian form \( f \) on \( \mathbb{F}_t^{2N} \) associated with \( H \) is a \( \mathbb{F}_t \)-quadratic form associated with the bilinear form \( \frac{1}{2}B \), where

\[
B : \mathbb{F}_t^{2N} \times \mathbb{F}_t^{2N} \to \mathbb{F}_t \quad (x, y) \mapsto f(x + y) - f(x) - f(y).
\]

We have \( B(x, y) = H (\iota x, \iota y) + H (\iota x, \iota y)^\dagger = \text{Tr}_{\mathbb{F}_t^2 / \mathbb{F}_t} (H (\iota x, \iota y)) \).

\textbf{Proof} : It is a simple matter to see that \( f \) is a \( \mathbb{F}_t \)-quadratic form because \( f(x) \) is a homogeneous polynomial of degree 2 in the coordinates of \( x \) and with coefficients in \( \mathbb{F}_t \). Indeed, it suffices to use a \( H \)-orthogonal basis of \( \mathbb{F}_t^N \) to get \( q(x) = \sum_{i=1}^r x_i t^{i+1} \) for all \( x \in E \) (Theorem 4) and

\[
f(x) = q(\iota x) = \sum_{i=1}^r (u_i + \alpha v_i)^{t+1} = \sum_{i=1}^r u_i^2 + \alpha^{t+1} u_i^2 + (\alpha + \alpha^t) u_i v_i
\]

with \( x = (u_1, v_1, ..., u_N, v_N) \in \mathbb{F}_t^{2N} \) and \( \alpha^{t+1} \in \mathbb{F}_t \).

Then it is easy to check that \( f(x + y) = f(x) + f(y) + H (\iota x, \iota y) + H (\iota x, \iota y)^\dagger \), ■

9
Hence inclusion. To complete the proof, we write $F$ as a non-trivial additive character on $Ker B$. Theorem 12 will never be the bilinear form associated with $B$ as $dim Ker B + dim (Ker B)^\perp = 2N$ but we can’t say that $F^2_t = Ker B \oplus (Ker B)^\perp$. With these notations:

**Theorem 12** We have $\iota (Ker B) = Ker H$. Thus $\iota$ induces a $F_t$-isomorphism from Ker $B$ onto Ker $H$ and $rk f = rk B = 2rk H$.

**Proof**: Let $\psi$ denotes a non trivial additive character on $F_t$. The map $\psi' = \psi \circ Tr_{F_t^2/F_t}$ is a non trivial additive character on $F_t^2$ and Lemma 8 gives:

$$
\{(x \in Ker B) \iff \forall y \in F^2_t, B(x,y) = Tr_{F_t^2/F_t}(H(\iota x, ty)) = 0 \\
\iff \sum_{y \in F^2_t} \psi(Tr_{F_t^2/F_t}(H(\iota x, ty))) = 0 \iff \sum_{z \in F^2_t} \psi'(H(\iota x, z)) = 0 \iff \forall z \in F^2_t, H(\iota x, z) = 0 \iff \iota x \in Ker H.
$$

Hence $\iota (Ker B) \subset Ker H$. Since $\iota$ is a $F_t$-isomorphism, the above equivalences imply the inverse inclusion. To complete the proof, we write

$$
rk f = rk B = 2N - \dim F_t, Ker B = 2N - 2 \dim F_t^2, Ker H = 2rk H. \blacksquare
$$

**Theorem 13** 1) There is an endomorphism $T$ of $F^2_t$ such that $B(x,y) = T(x).y$ for all $(x,y) \in F^2_t \times F^2_t$.

2) We have $Ker T = Ker B$, $Im T = (Ker B)^\perp$ and $Ker T \subset f^{-1}(0)$.
**Proof**: 1) Since the inner product is non-degenerate, for all \( x \in \mathbb{F}_t^{2N} \) we can find \( T(x) \in \mathbb{F}_t^{2N} \) such that \( B(x, y) = T(x) \cdot y \) for all \( y \in \mathbb{F}_t^{2N} \). From \( B(\lambda x + x', y) = \lambda B(x, y) + B(x', y) \) we deduce \( [T(\lambda x + x') - \lambda T(x) - T(x')] \cdot y = 0 \) for all \( y \in \mathbb{F}_t^{2N} \), hence

\[
T(\lambda x + x') - \lambda T(x) - T(x') = 0
\]

and the linearity of \( T \) follows.

2) The first equality is a consequence of \( x \in \ker T \leftrightarrow (\forall y \in \mathbb{F}_t^{2N} \ T(x) \cdot y = 0) \leftrightarrow (\forall y \in \mathbb{F}_t^{2N} \ B(x, y) = 0) \leftrightarrow x \in \ker B. \)

If \( z \in \mathbb{F}_t^{2N} \) and if \( u \in \ker B, \) then \( T(z) \cdot u = B(z, u) = 0, \) hence \( \text{Im} T \subset (\ker B)^\perp. \) This inclusion is an equality because

\[
\dim (\text{Im} T) = 2N - \dim (\ker T) = 2N - \dim (\ker B) = \dim \left((\ker B)^\perp\right).
\]

If \( x \in \ker T = \ker B \) then \( f(x) = H(lx, lx) = 0 \) from Theorem 12, thus \( \ker T \subset f^{-1}(0). \)

8 **Exponential sums S(f, v)**

Let us denote by \( \psi \) the additive character on \( \mathbb{F}_t \) defined by

\[
\psi(x) = \exp \left( \frac{i2\pi}{p} \text{Tr}_{\mathbb{F}_t/\mathbb{F}_p}(x) \right).
\]

If \( v \in \mathbb{F}_t^{2N} \), we consider the exponential sum associated to \( f \) and \( v \):

\[
S(f, v) = \sum_{x \in \mathbb{F}_t^{2N}} \psi(f(x) + v \cdot x).
\]

**Lemme 3** Let \( \psi \) denotes a non-trivial additive character on \( \mathbb{F}_t \), \( V \) a \( \mathbb{F}_t \)-vector space of finite dimension \( m \), and \( l : V \rightarrow \mathbb{F}_t \) a linear form on \( V \). Then

\[
\sum_{y \in V} \psi(l(y)) = \begin{cases} 
1 & \text{if } l = 0, \\
0 & \text{if } l \neq 0.
\end{cases}
\]

**Proof**: The map \( \psi \circ l \) is an additive character on \( V \simeq \mathbb{F}_t^m \) and we can apply the orthogonality relation (Theorem 19).

**Lemme 4**

\[
\sum_{x \in \mathbb{F}_t^{2m}} \psi(N_{\mathbb{F}_t/\mathbb{F}_t}(x)) = \frac{t - t^m}{t - 1}.
\]

**Proof**: From Lemma 2 it follows that \( N_{\mathbb{F}_t/\mathbb{F}_t} : \mathbb{F}_t^{2m} \rightarrow \mathbb{F}_t^* \) is a multiplicative group epimorphism and that \( |N_{\mathbb{F}_t/\mathbb{F}_t}^{-1}(b)| = \frac{t^m - 1}{t - 1} \) for all \( b \in \mathbb{F}_t^* \). Hence

\[
\sum_{x \in \mathbb{F}_t^{2m}} \psi(N_{\mathbb{F}_t/\mathbb{F}_t}(x)) = 1 + \sum_{x \in \mathbb{F}_t^{2m}} \psi(N_{\mathbb{F}_t/\mathbb{F}_t}(x)) = 1 + \frac{t^m - 1}{t - 1} \sum_{z \in \mathbb{F}_t^*} \psi(z).
\]
The use of the orthogonality relation $\sum_{z \in \mathbb{F}_t^2} \psi (z) = -1$ completes the proof. ■

We are now ready to give another proof of the main result in [3]. In fact, a small mistake occurred in Proposition 3 of [3] as $A(s,v)$ do not depends on $f(u)$ but on $\text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u))$, as we shall see below.

**Théorème 14** ([3], Th. 2 and Prop. 3) Let $v \in \mathbb{F}_t^{2N}$ and let $f$ denote a quadratic hermitian form of rank $2\rho$ in $\mathbb{F}_t^{2N}$. Consider the extensions $\mathbb{F}_p \subset \mathbb{F}_s \subset \mathbb{F}_t \subset \mathbb{F}_{t2}$ and let $a \in \mathbb{F}_s$.

1) If $v \in (\text{Ker } B)^{\perp} = \text{Im } T$, we can find $u \in \mathbb{F}_t^{2N}$ such that $v = T(u)$. Then

$$S(af,v) = (-1)^{\rho} t^{2N-\rho} \psi (-a^{-1} f(u))$$

and $\sum_{a \in \mathbb{F}_s^2} S(af,v) = (-1)^{\rho} t^{2N-\rho} A(s,v)$ where

$$A(s,v) = \begin{cases} s - 1 & \text{if } \text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u)) = 0, \\ -1 & \text{else}. \end{cases}$$

2) If $v \notin (\text{Ker } B)^{\perp}$ then $S(af,v) = 0$.

**Proof**: Without loss of generality, we can assume that $f$ is given in the standard form $f(x) = H(y,y) = q(y) = y_1^{t+1} + \ldots + y_{\rho}^{t+1}$ where $y = t(x) \in \mathbb{F}_{t2}^{N}$.

1) a) We first compute $S(f,v)$. Since $v = T(u)$,

$$f(x) + v.x = f(x) + T(u).x = f(x) + B(u,x) = f(u + x) - f(u)$$

and

$$S(f,v) = \sum_{x \in \mathbb{F}_t^{2N}} \psi (f(x) + v.x) = \sum_{x \in \mathbb{F}_t^{2N}} \psi (f(u + x) - f(u)).$$

Define $z = tu$. Then

$$f(u + x) - f(u) = q(z + y) - q(z) = \sum_{k=1}^{\rho} \left[ (z_k + y_k)^{t+1} - z_k^{t+1} \right]$$

and

$$S(f,v) = \sum_{y_1,\ldots,y_N \in \mathbb{F}_{t2}} \prod_{k=1}^{\rho} \psi \left( (z_k + y_k)^{t+1} - z_k^{t+1} \right)$$

$$= t^{2(N-\rho)} \sum_{y_1,\ldots,y_N \in \mathbb{F}_{t2}} \prod_{k=1}^{\rho} \psi \left( (z_k + y_k)^{t+1} - z_k^{t+1} \right)$$

$$= t^{2(N-\rho)} \xi \prod_{k=1}^{\rho} \psi \left( -z_k^{t+1} \right)$$

where $\xi = \sum_{y_1,\ldots,y_\rho \in \mathbb{F}_{t2}} \prod_{k=1}^{\rho} \psi \left( (z_k + y_k)^{t+1} \right)$. We have

$$\xi = \sum_{y_1,\ldots,y_{\rho-1} \in \mathbb{F}_{t2}} \left( \prod_{k=1}^{\rho-1} \psi \left( (z_k + y_k)^{t+1} \right) \right) \left( \sum_{y_\rho \in \mathbb{F}_{t2}} \psi \left( (z_\rho + y_\rho)^{t+1} \right) \right).$$

12
Lemma \[\text{1}\] gives \[\sum_{y_{\rho} \in \mathbb{F}_{i}^2} \psi((z_{\rho} + y_{\rho})^{t+1}) = \sum_{y \in \mathbb{F}_{i}^2} \psi(y^{t+1}) = -t, \text{ hence} \]

\[\xi = (-t) \sum_{y_{1}, \ldots, y_{t-1} \in \mathbb{F}_{i}^2} \left( \prod_{k=1}^{t-1} \psi((z_k + y_k)^{t+1}) \right).\]

We proceed to obtain \(\xi = (-t)^{\rho}\), and so

\[S(f, v) = (-1)^{\rho} t^{2N-\rho} \prod_{k=1}^{\rho} \psi(-z_{k}^{t+1}) = (-1)^{\rho} t^{2N-\rho} \psi(-z_{1}^{t+1} - \ldots - z_{\rho}^{t+1}) = (-1)^{\rho} t^{2N-\rho} \psi(-q(z)).\]

Since \(q(z) = H(\iota u, \iota u) = f(u)\), we see that \(S(f, v) = (-1)^{\rho} t^{2N-\rho} \psi(-f(u)).\)

\(\beta)\) Let us compute \(S(af, v)\). By the above applied with \(f_a = af\) instead of \(f\), we obtain \(S(af, v) = (-1)^{\rho} t^{2N-\rho} \psi(-af(u_a))\) where \(u_a\) satisfies \(v = T_a u_a\) and \(T_a\) is defined by

\[T_a(x).y = f_a(x + y) - f_a(x) - f_a(y) = a(f(x + y) - f(x) - f(y)) = a(T(x).y).\]

Hence \(T_a = aT\). We have \(v = T_a u_a\) and the bilinear \(s\) and the bilinear \(f\) gives

\[\gamma)\) By the above

\[\sum_{a \in \mathbb{F}^*_{s}} S(af, v) = (-1)^{\rho} t^{2N-\rho} \sum_{a \in \mathbb{F}^*_{s}} \psi(-a^{-1} f(u)) = (-1)^{\rho} t^{2N-\rho} \sum_{a \in \mathbb{F}^*_{s}} \psi'(a^{-1} \text{Tr}_{\mathbb{F}_s/\mathbb{F}_p}(f(u)))\]

where \(\psi'\) is the additive character \(\psi'(x) = \exp\left(\frac{12\pi}{p} \text{Tr}_{\mathbb{F}_s/\mathbb{F}_p}(x)\right)\) on \(\mathbb{F}_s\). The map \(z \mapsto \psi'(cz)\) describes the set of additive characters on \(\mathbb{F}_s\) when \(c\) describes \(\mathbb{F}_s\), consequently the orthogonality relation (Theorem \[\text{19}\]) yields

\[\sum_{a \in \mathbb{F}^*_{s}} S(af, v) = (-1)^{\rho} t^{2N-\rho} \left(1 + \sum_{\chi \in \mathbb{F}^*_{s}} \chi(\text{Tr}_{\mathbb{F}_s/\mathbb{F}_p}(f(u)))\right) = (-1)^{\rho} t^{2N-\rho} A(s, v).\]

2) Define \(f_a = af\). Since \(a \in \mathbb{F}_s\), \(f_a\) is a hermitian quadratic form on \(\mathbb{F}_s^2\) and the bilinear form \(B_a(x, y) = f_a(x + y) - f_a(x) - f_a(y)\) associated to \(f_a\) satisfies \(\text{Ker} B_a = \text{Ker} B\). Hence we can assume that \(a = 1\) without loss of generality. Let \(v \notin (\text{Ker} B)^{\perp}\). The first part of the Theorem gives \(S(f, 0) = (-1)^{\rho} t^{2N-\rho}\) hence \(S(f, 0) \neq 0\). Therefore \(S(f, v) = 0\) if and only if
Let us introduce the additive character \( \psi \)

\[
S (f, v) S (f, 0) = 0.
\]

We have:

\[
\begin{align*}
S (f, v) S (f, 0) &= \sum_{x, y \in \mathbb{F}_t^{2N}} \psi \left( (f (x) - f (y) + v.x) \right) \\
&= \sum_{x, y \in \mathbb{F}_t^{2N}} \psi \left( (f (x + y) - f (y) + v.x + v.y) \right) \\
&= \sum_{x, y \in \mathbb{F}_t^{2N}} \psi \left( (f (x) + B (x, y) + v.x + v.y) \right) \\
&= \sum_{x \in \mathbb{F}_t^{2N}} \psi \left( (f (x) + v.x) \right) \sum_{y \in \mathbb{F}_t^{2N}} \psi \left( (T (x) + v).y \right).
\end{align*}
\]

Since \( v \notin (\text{Ker } B)^\perp \), the sum \( T (x) + v \) is never null and the map \( l (y) = (T (x) + v).y \) is a non trivial linear form on \( \mathbb{F}_t^{2N} \). We conclude from Lemma \( 3 \) that \( \sum_{y \in \mathbb{F}_t^{2N}} \psi (l (y)) = 0 \), and finally that \( S (f, v) S (f, 0) = 0 \). \( \blacksquare \)

**Remark:** The constant \( A (s, v) \) in Theorem \( 14 \) depends whether \( \text{Tr}_{\mathbb{F}_t/\mathbb{F}_s} (f (u)) = 0 \) or not. It has a meaning if we check that \( v = T (u) = T (u') \) and \( \text{Tr}_{\mathbb{F}_t/\mathbb{F}_s} (f (u)) = 0 \) imply \( \text{Tr}_{\mathbb{F}_t/\mathbb{F}_s} (f (u')) = 0 \). Let \( v = T (u) = T (u') \). Then \( u - u' := w \in \text{Ker } T \) and \( B (w, u') = f (u) - f (w) - f (u') \). From \( B (w, u') = T (w).u' = 0 \) and \( f (w) = \frac{1}{2} B (w, w) = \frac{1}{2} T (w).w = 0 \) it follows that \( f (u) = f (u') \), which gives the desired conclusion.

## 9 Number of solutions of some trace equations

**Théorème 15** Let \( v \in \mathbb{F}_t^{2N} \), let \( \rho \) be a positive integer such that \( 1 \leq \rho \leq N \), and \( f \) be a quadratic hermitian form of rank \( 2 \rho \) on \( \mathbb{F}_t^{2N} \). The number \( M \) of solutions of the equation \( \text{Tr}_{\mathbb{F}_t/\mathbb{F}_s} (f (x) + v.x) = 0 \) in \( \mathbb{F}_t^{2N} \) is

\[
M = \begin{cases} 
\frac{1}{2} (t^{2N} + (-1)^\rho A (s, v) t^{2N-\rho}) & \text{if } v \in (\text{Ker } B)^\perp = \text{Im } T, \\
\text{else}. 
\end{cases}
\]

**Proof:** Let us introduce the additive character \( \psi' (x) = \exp \left( \frac{i2\pi}{p} \text{Tr}_{\mathbb{F}_s/\mathbb{F}_p} (x) \right) \) on \( \mathbb{F}_s \). Theorem \( 21 \) gives

\[
sM = \sum_{c \in \mathbb{F}_s} \sum_{x \in \mathbb{F}_t^{2N}} \psi' (c \text{Tr}_{\mathbb{F}_t/\mathbb{F}_s} (f (x) + v.x)).
\]

Since

\[
\psi' (c \text{Tr}_{\mathbb{F}_t/\mathbb{F}_s} (f (x) + v.x)) = \exp \left( \frac{i2\pi}{p} \text{Tr}_{\mathbb{F}_s/\mathbb{F}_p} (c \text{Tr}_{\mathbb{F}_t/\mathbb{F}_s} (f (x) + v.x)) \right) \\
= \exp \left( \frac{i2\pi}{p} \text{Tr}_{\mathbb{F}_s/\mathbb{F}_p} (cf (x) + cv.x) \right) \\
= \psi (cf (x) + cv.x),
\]

we have

\[
\psi' (c \text{Tr}_{\mathbb{F}_t/\mathbb{F}_s} (f (x) + v.x)) = \psi (cfs (x) + cv.s) = \psi (cf (x) + cv.x).
\]

Therefore

\[
\sum_{c \in \mathbb{F}_s} \sum_{x \in \mathbb{F}_t^{2N}} \psi' (c \text{Tr}_{\mathbb{F}_t/\mathbb{F}_s} (f (x) + v.x)) = \sum_{x \in \mathbb{F}_t^{2N}} \sum_{c \in \mathbb{F}_s} \psi' (cf (x) + cv.x) = \sum_{x \in \mathbb{F}_t^{2N}} \psi (cf (x) + cv.x) = \psi (S (f (v))).
\]
we deduce
\[
    sM = \sum_{c \in \mathbb{F}_s} \sum_{x \in \mathbb{F}_s^2} \psi(cf(x) + cv.x) = t^{2N} + \sum_{c \in \mathbb{F}_s^*} \sum_{x \in \mathbb{F}_s^2} \psi(e^{-1}f(cx) + v(cx))
\]
\[
    = t^{2N} + \sum_{c \in \mathbb{F}_s^*} S(e^{-1}f, v).
\]

Now the assertion follows from Theorem 14.

**Théorème 16** \{8, Prop. 3\} Let \(a\) be an element of \(\mathbb{F}_s\), \(\rho\) be a positive integer with \(1 \leq \rho \leq N\), and \(f\) be a quadratic hermitian form of rank \(2\rho\) on \(\mathbb{F}_t^{2N}\). The number \(M\) of solutions of the equation \(\text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)) = a\) in \(\mathbb{F}_t^{2N}\) is
\[
    M = \begin{cases} 
        \frac{1}{s}(t^{2N} - (-1)^\rho t^{2N-\rho}) & \text{if } a \neq 0, \\
        \frac{1}{s}(t^{2N} + (-1)^\rho (s - 1) t^{2N-\rho}) & \text{if } a = 0.
    \end{cases}
\]

**Proof**: We can assume that \(f\) is given in the standard form \(f(x) = H(y, y) = y_1^t + \ldots + y_{\rho}^t\) where \(y = t(x) \in \mathbb{F}_s^N\). If \(\mathbb{F}_s\) denotes the set of additive characters on \(\mathbb{F}_s\), then (Theorem 24)
\[
    sM = \sum_{\psi \in \mathbb{F}_s^*} \sum_{x \in \mathbb{F}_t^{2N}} \psi(\text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)) - a).
\]

Hence
\[
    sM = t^{2N} + \sum_{\psi \neq 1} \underbrace{\psi(a)}_{y \in \mathbb{F}_t} \sum_{y \in \mathbb{F}_s^N} \psi(\text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(y_1^{t+1} + \ldots + y_{\rho}^{t+1})).
\]

We have
\[
    A_\psi = \sum_{y \in \mathbb{F}_s^N} \psi(\text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(y_1^{t+1})) \ldots \psi(\text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(y_{\rho}^{t+1}))
\]
\[
    = t^{2(N-\rho)} \left( \sum_{y \in \mathbb{F}_s^N} \psi(\text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(y^{t+1})) \right)^\rho = t^{2(N-\rho)} B_\psi
\]

where \(B_\psi = \sum_{y \in \mathbb{F}_s^N} \psi(\text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(y^{t+1}))\). Since the norm \(N : \mathbb{F}_{t^2}^* \to \mathbb{F}_t^*\) is surjective and satisfies \(|N^{-1}(z)| = t + 1\) for all \(z \in \mathbb{F}_t^*\) (Lemma 2), we get
\[
    B_\psi = 1 + (t + 1) \sum_{z \in \mathbb{F}_t^*} \psi(\text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(z)) = -t.
\]

Therefore
\[
    sM = t^{2N} + (-1)^\rho t^{2N-\rho} \sum_{\psi \neq 1} \underbrace{\psi(a)}_{y \in \mathbb{F}_t} = t^{2N} + (-1)^\rho t^{2N-\rho} \left( -1 + \sum_{\psi \in \mathbb{F}_s^*} \overrightarrow{\psi}(a) \right)
\]

and the usual orthogonality relation establishes the formula.

**Remark**: Theorem 16 follows from Theorem 15 when \(a = 0\). A generalization of these two results would be to compute the number of solutions of \(\text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x) + v.x) = a\) in \(\mathbb{F}_t^{2N}\).
10 The code $\Gamma$

Remember that $\text{QH} \left( \mathbb{F}_t^{2N} \right)$ denotes the $\mathbb{F}_t$-vector space of quadratic hermitian forms on $\mathbb{F}_t^{2N}$. The image of the linear map

\[
\gamma : \text{QH} \left( \mathbb{F}_t^{2N} \right) \times \mathbb{F}_t^{2N} \rightarrow \mathbb{F}_s^{2N}
\]

\[
(f, v) \mapsto \left( \text{Tr}_{\mathbb{F}_t/\mathbb{F}_s} \left( f(x) + v.x \right) \right)_{x \in \mathbb{F}_t^{2N}}
\]

is a code $\Gamma$ in $\mathbb{F}_s^{2N}$. This code was first introduced by J.-P. Cherdieu in [3] and next Theorem provides us with its parameters. Let us denote by $w(c)$ the weight of a non null code-word in a code $C$. If $d \leq w(c) \leq D$ and if the bounds of these inequalities are reached, we say that $d$ is the minimal distance of $C$, and that $r = \frac{D - d}{2}$ is the disparity of $C$.

Théorème 17 The weights $w(\gamma(f, v))$ of the non null code-word $\gamma(f, v)$ of the code $\Gamma$ satisfy:

\[
t^{2N} - \frac{1}{2} \left( t^{2N} + t^{2N-1} \right) \leq w(\gamma(f, v)) \leq t^{2N} - \frac{1}{2} \left( t^{2N} - (s - 1) t^{2N-1} \right)
\]

and the bounds of these inequalities are reached. The parameters and the disparity of $\Gamma$ are:

\[
[N_\Gamma, K_\Gamma, D_\Gamma] = \left[ t^{2N}, (N^2 + 2N) \log_s t, t^{2N} - \frac{1}{2} \left( t^{2N} + t^{2N-1} \right) \right] \quad \text{and} \quad r(\Gamma) = \frac{(s - 1) (t + 1)}{st - t - 1}.
\]

Proof: The length of $\Gamma$ is $N_\Gamma = t^{2N}$. It follows immediately from Theorem 15 that the equation $\text{Tr}_{\mathbb{F}_t/\mathbb{F}_s} \left( f(x) + v.x \right) = 0$ have $t^{2N}$ solutions in $\mathbb{F}_t^{2N}$ if and only if $(f, v) = (0, 0)$. Consequently the map $\gamma$ is injective and

\[
K_\Gamma = \text{dim}_\mathbb{F}_s \Gamma = \text{dim}_\mathbb{F}_s \left( \text{QH} \left( \mathbb{F}_t^{2N} \right) \times \mathbb{F}_t^{2N} \right) = (N^2 + 2N) \log_s t.
\]

We have $w(\gamma(f, v)) = t^{2N} - M(f, v)$ where the number $M(f, v)$ of solutions of the equation $\text{Tr}_{\mathbb{F}_t/\mathbb{F}_s} \left( f(x) + v.x \right) = 0$ in $\mathbb{F}_t^{2N}$ is provided by Theorem 15:

\[
M(f, v) = \begin{cases} 
\frac{1}{s} \left( t^{2N} + (-1)^{\rho} A(s, v) t^{2N-\rho} \right) & \text{if } v \in (\text{Ker } B)^\perp = \text{Im } T, \\
\frac{1}{s} \left( t^{2N} - (s - 1) t^{2N-2} \right) & \text{else}.
\end{cases}
\]

We consider several cases:

1. If $v = 0$, then $f \neq 0$, and
   
   1.1. If $\rho$ is even, then $2 \leq \rho \leq 2 \left[ \frac{N}{2} \right]$ and
   
   \[
   \frac{1}{s} \left( t^{2N} + (s - 1) t^{2N-2} \left[ \frac{N}{2} \right] \right) \leq M(f, 0) \leq \frac{1}{s} \left( t^{2N} + (s - 1) t^{2N-2} \right). \tag{1}
   \]
   
   1.2. If $\rho$ is odd, then $1 \leq \rho \leq 2 \left[ \frac{N-1}{2} \right] + 1$ and
   
   \[
   \frac{1}{s} \left( t^{2N} - (s - 1) t^{2N-2} \right) \leq M(f, 0) \leq \frac{1}{s} \left( t^{2N} - (s - 1) t^{2N-2} \left[ \frac{N}{2} \right] \right). \tag{2}
   \]

2. If $v \neq 0$,
2.1. If \( \rho \) is even and \( v \in (\text{Ker} B)^\perp \), then \( \rho \neq 0 \). We get

\[
2 \leq \rho \leq 2 \left\lfloor \frac{N}{2} \right\rfloor \quad \text{et} \quad M(f, v) = \frac{1}{s} \left( t^{2N} + A(s, v) t^{2N-\rho} \right).
\]

We can find a vector \( u \) such that \( \text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u)) \neq 0 \) (indeed \( f(u) = y_1^{t+1} + \ldots + y_\rho^{t+1} \) in a convenient basis, and the map \( y \mapsto \text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(y^{t+1}) \) is surjective since \( \text{Tr}_{\mathbb{F}_t/\mathbb{F}_s} \) are surjective) thus there will be 2 possible cases:

2.1.1. If \( v = T(u) \) with \( \text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u)) = 0 \), then \( M(f, v) = \frac{1}{s} \left( t^{2N} + (s - 1) t^{2N-\rho} \right) \)

\[
\frac{1}{s} \left( t^{2N} + s - 1 \right) t^{2N-2} \left( \frac{N}{2} \right) \leq M(f, v) \leq \frac{1}{s} \left( t^{2N} + (s - 1) t^{2N-2} \right).
\]

(3)

2.1.2. If \( v = T(u) \) with \( \text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u)) \neq 0 \), then \( M(f, v) = \frac{1}{s} \left( t^{2N} - t^{2N-\rho} \right) \) and

\[
\frac{1}{s} \left( t^{2N} - t^{2N-2} \right) \leq M(f, v) \leq \frac{1}{s} \left( t^{2N} - t^{2N-2} \right)
\]

(4)

2.2. If \( \rho \) is even and \( v \notin (\text{Ker} B)^\perp \), then \( M(f, v) = \frac{t^{2N}}{s} \) belongs to one of the intervals defined by (3) or (4).

2.3. If \( \rho \) is odd and \( v \in (\text{Ker} B)^\perp \), then \( M(f, v) = \frac{1}{s} \left( t^{2N} - A(s, v) t^{2N-\rho} \right) \).

2.3.1. If \( v = T(u) \) with \( \text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u)) = 0 \), then \( M(f, v) = \frac{1}{s} \left( t^{2N} - (s - 1) t^{2N-\rho} \right) \)

and

\[
\frac{1}{s} \left( t^{2N} - s - 1 \right) t^{2N-1} \leq M(f, v) \leq \frac{1}{s} \left( t^{2N} - (s - 1) t^{2N-1} \right)
\]

(5)

2.3.2. If \( v = T(u) \) with \( \text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u)) \neq 0 \), then \( M(f, v) = \frac{1}{s} \left( t^{2N} + t^{2N-\rho} \right) \) and

\[
\frac{1}{s} \left( t^{2N} + t^{2N-2} \left( \frac{N-1}{2} \right) \right) \leq M(f, v) \leq \frac{1}{s} \left( t^{2N} + t^{2N-1} \right)
\]

(6)

2.4. If \( \rho \) is odd and \( v \notin (\text{Ker} B)^\perp \), then \( M(f, v) = \frac{t^{2N}}{s} \) belongs to one of the intervals defined by (3) or (4).

It is sufficient to consider the bounds (1) à (6) to deduce

\[
\frac{1}{s} \left( t^{2N} - (s - 1) t^{2N-1} \right) \leq M(f, v) \leq \frac{1}{s} \left( t^{2N} + t^{2N-1} \right)
\]

for all \( (f, v) \in (\text{OH} (\mathbb{F}_t^{2N}) \times \mathbb{F}_t^{2N}) \setminus \{(0, 0)\} \). Hence we obtain the bounds of the weights \( w(\gamma, f, v) \). ■

Let \( C \) denote a code \([N_C, K_C, D_C]\). The ratio \( \frac{K_C}{N_C} \) is called the transmission rate, and the ratio \( \frac{D_C}{N_C} \) represents the reliability of \( C \). Note that \( C \) can correct \( \left\lfloor \frac{D_C - 1}{2} \right\rfloor \) errors and that

\[
\lambda(C) = \frac{K_C}{N_C} + \frac{D_C}{N_C}
\]

is less than \( 1 + \frac{1}{N_C} \) and must be as great as possible.

The generalized Reed-Muller code \( R(r, m) \) of order \( r \) on \( \mathbb{F}_t^m \) is described by the code-words \( (f(x))_{x \in \mathbb{F}_t^m} \) where \( f \) are polynomials in \( \mathbb{F}_t[X_1, \ldots, X_m] \) of total degree less than \( r \). The dimension of \( R(r, m) \) is \( C_{m+r}^r \) if \( r < t \), and the parameters of \( R(2, 2N) \) are

\[
[N_R, K_R, D_R] = [t^{2N}, 2N^2 + 3N + 1, t^{2N} - 2t^{2N-1}].
\]
Let us compare $R(2,2N)$ to the code $\Gamma$ with same length $t^{2N}$ obtained with $s = t$. The code $R(2,2N)$ have a better transmission rate since
\[
\frac{K_R}{N_R} - \frac{K_{\Gamma}}{N_{\Gamma}} = \frac{1}{t^{2N}} (N^2 + N + 1)
\]
is always positive, but the numbers of corrected errors is better with $\Gamma$ since
\[
D_{\Gamma} - D_R = t^{2N-1} - t^{2N-2}
\]
is always positive. One can also check that the difference
\[
\lambda(\Gamma) - \lambda(R) = \frac{t^2}{t^{2N}} (t^{2N-1} - t^{2N-2} - N^2 - N - 1)
\]
is positive or null as soon as $N \geq 2$ or $t \geq 4$. In this sens, $\Gamma$ have better parameters than $R(2,2N)$.

11 The code $C$

The parameters of the code $\Gamma$ in Section 10 are computed from Theorem 15. We can apply the same construction to use Theorem 16. The image of the linear map
\[
c : \text{QH} \left( \mathbb{F}_t^{2N} \right) \times \mathbb{F}_s \rightarrow \mathbb{F}_s^{2N}
\]
\[
(f,a) \mapsto \left( \text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)) - a \right) x \in \mathbb{F}_t^{2N}
\]
is a code $C$ with length $N_C = t^{2N}$ on $\mathbb{F}_s$. The map $c$ is one to one. Indeed, if the non null quadratic form $f$ satisfies $\text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)) = a$ for all $x \in \mathbb{F}_t^{2N}$, and if $\rho$ denotes the rank of $f$, then $f(x) = y_1^{t+1} + \ldots + y_{\rho}^{t+1}$ where $y = \iota x$ and $1 \leq \rho \leq N$, and the assumption on $f$ implies $\text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(y_1^{t+1}) = a$ for all $y_1 \in \mathbb{F}_t^{\rho}$. This is a contradiction of the fact that the map $\text{Tr}_{\mathbb{F}_t/\mathbb{F}_s} \circ N_{\mathbb{F}_t/\mathbb{F}_s} : \mathbb{F}_t^{\rho} \rightarrow \mathbb{F}_s$ is onto.

As $c$ is one to one, the dimension of $C$ will be:
\[
K_C = \dim_{\mathbb{F}_s} \left( \text{QH} \left( \mathbb{F}_t^{2N} \right) \times \mathbb{F}_s \right) = 1 + N^2 \log_s t.
\]

\textbf{Théorème 18} The weights $w(c(f,a))$ of the non null code-words $c(f,a)$ in $C$ satisfy:
\[
t^{2N} - \frac{1}{s} \left( t^{2N} + t^{2N-1} \right) \leq w(c(f,a)) \leq t^{2N}
\]
and the bounds are reached. The parameters and the disparity of $C$ are:
\[
[N_C, K_C, D_C] = \left[ t^{2N}, 1 + N^2 \log_s t, t^{2N} - \frac{1}{s} \left( t^{2N} + t^{2N-1} \right) \right]
\text{ and } r(C) = \frac{st}{st - t - 1}.
\]

\textbf{Proof} : It suffices to bound the weights $w(c(f,a))$. We certainly have
\[
w(c(f,a)) = t^{2N} - M(f,a)
\]
where $M(f,a)$, which denotes the number of solutions of the equation $\text{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)) = a$ in $\mathbb{F}_t^{2N}$, is given by Theorem 16.
1. If \( a = 0 \), we know that \( \rho \neq 0 \).

1.1. If \( \rho \) is even, then \( 2 \leq \rho \leq 2 \left[ \frac{N}{2} \right] \) and

\[
\frac{1}{s} \left( t^{2N} + (s - 1) t^{2N-2} \left[ \frac{N}{2} \right] \right) \leq M(f,0) \leq \frac{1}{s} \left( t^{2N} + (s - 1) t^{2N-2} \right). \tag{1}
\]

1.2. If \( \rho \) is odd, then \( 1 \leq \rho \leq 2 \left[ \frac{N-1}{2} \right] + 1 \) and

\[
\frac{1}{s} \left( t^{2N} - (s - 1) t^{2N-1} \right) \leq M(f,0) \leq \frac{1}{s} \left( t^{2N} - (s - 1) t^{2N-2} \left[ \frac{N-1}{2} \right] - 1 \right). \tag{2}
\]

2. If \( a \neq 0 \),

2.1. If \( \rho \) is even,

\[
0 \leq M(f,a) \leq \frac{1}{s} \left( t^{2N} - t^{2N-2} \left[ \frac{N}{2} \right] \right). \tag{3}
\]

2.2. If \( \rho \) is odd,

\[
\frac{1}{s} \left( t^{2N} - t^{2N-2} \left[ \frac{N-1}{2} \right] - 1 \right) \leq M(f,a) \leq \frac{1}{s} \left( t^{2N} + t^{2N-1} \right). \tag{4}
\]

The bounds (1) to (4) imply

\[
\forall (f,a) \in (QH (F^2_N) \times F_s) \setminus \{(0,0)\} \quad 0 \leq M(f,a) \leq \frac{1}{s} \left( t^{2N} + t^{2N-1} \right). \tag*{\blacksquare}
\]

Let us compare \( C \) with \( \Gamma \) and \( R(2,2N) \). The codes \( C \) and \( \Gamma \) have same length and same minimal distance, thus will correct the same amount of errors. Nevertheless the dimension of \( \Gamma \) is greater than those of \( C \), hence \( \Gamma \) is better at this point of view. But \( C \) can be compared with the Reed-Muller code \( R(2,2N) \) when \( s = t \). Since

\[
D_C - D_R = t^{2N-2} (t - 1) > 0
\]

we find that \( C \) can correct more errors than \( R(2,2N) \). But the transmission rate is not so good because

\[
\frac{K_R}{N_R} - \frac{K_C}{N_C} = \frac{N^2 + 3N}{t2N} > 0.
\]

We can check that \( \lim_{t \to +\infty} (\lambda(C) - \lambda(R)) = 0 \) when \( N \) is chosen. In this sens, \( C \) can be compared with \( R(2,2N) \) for large values of \( t \). In the same manner \( \lim_{t \to +\infty} \left( \frac{K_R}{N_R} - \frac{K_C}{N_C} \right) = 0 \) and the transmission rates of \( C \) and \( R(2,2N) \) can be compared for large values of \( t \).

12 Annex: Group characters

Let \((G,+)\) be a finite abelian group of order \(|G|\). A character \( \psi \) on \( G \) is a homomorphism from \((G,+)\) to the multiplicative group \((\mathbb{C}^*,.)\) of non null complex numbers. It is easily seen that all \( z \) in \( \text{Im } \psi \) has absolute value 1, that \( \psi(0) = 1 \) and \( \psi(-x) = \psi(x)^{-1} = \overline{\psi(x)} \) for all \( x \in G \). The trivial character \( 1 \) is defined by \( 1(x) = 1 \) for all \( x \in G \). The set \( G^\wedge \) of all characters defined on \( G \) is a multiplicative group of order \(|G|\), with the natural law \((\psi \chi)(x) = \psi(x) \chi(x)\). We have:
Théorème 19 \{[7], Theorem 5.4\} Orthogonality relations (I).

If $\psi \in G^\wedge$, 
\[
\sum_{x \in G} \psi(x) = \begin{cases} 
0 & \text{if } \psi \neq 1, \\
|G| & \text{else.}
\end{cases}
\]

If $x \in G$, 
\[
\sum_{\psi \in G^\wedge} \psi(x) = \begin{cases} 
0 & \text{if } x \neq 0, \\
|G| & \text{else.}
\end{cases}
\]

Theorem 19 immediately gives us two useful results:

Théorème 20 Orthogonality relations (II).

If $\psi, \chi \in G^\wedge$, then 
\[
\sum_{x \in G} \psi(x) \overline{\chi(x)} = \begin{cases} 
0 & \text{if } \psi \neq \chi, \\
|G| & \text{else.}
\end{cases}
\]

If $x, y \in G$, then 
\[
\sum_{\psi \in G^\wedge} \psi(x) \overline{\psi(y)} = \begin{cases} 
0 & \text{if } x \neq y, \\
|G| & \text{else.}
\end{cases}
\]

Proof : We notice that $\psi(x) \overline{\chi(x)} = (\overline{\psi\chi^{-1}})(x)$ and $\psi(x) \overline{\psi(y)} = \psi(x - y)$, and we apply Theorem 19.

Théorème 21 Let $f : E \to G$ be a map from a set $E$ to a finite abelian group $G$, and let $a \in G$. The number $M$ of solutions of the equation $f(x) = a$ is 
\[
M = \frac{1}{|G|} \sum_{\psi \in G^\wedge} \sum_{x \in E} \psi(f(x) - a).
\]

Proof : 
\[
\sum_{\psi \in G^\wedge} \sum_{x \in E} \psi(f(x) - a) = \sum_{x \in f^{-1}(a)} \sum_{\psi \in G^\wedge} \psi(0) + \sum_{x \notin f^{-1}(a)} \sum_{\psi \in G^\wedge} \psi(f(x) - a) = M |G|.
\]

When $G$ is cyclic of order $n$ and generated by $g$, we can check that $G^\wedge$ is cyclic and 
\[
G^\wedge = \{\psi_j / j \in \{0, 1, ..., n\}\} \text{ with } \psi_j \left(g^k\right) = \exp\left(\frac{ijk2\pi}{n}\right).
\]

An additive character on $\mathbb{F}_t$ is a character of the additive group $(\mathbb{F}_t, +)$. One can prove that 
\[
\psi(x) = \exp\left(\frac{i2\pi}{p} \text{ Tr}_{\mathbb{F}_t/\mathbb{F}_p}(x)\right)
\]
declare a non trivial additive character on $\mathbb{F}_t$, and that all others additive characters are given by $\psi_a(x) = \psi(ax)$ where $a \in \mathbb{F}_t$. 

20
References

[1] R.C. Bose, I.M. Chakravarti, Hermitian varieties in a finite projective space PG(N,q^2), Canadian journal of Math. 18, p.1161-1182, 1966.

[2] L. Carlitz & J.H. Hodges, Representations by hermitian forms in a finite field, Duke Math. Journal (22), pp. 393-405, 1955.

[3] J.-P. Cherdieu, Exponential sums, codes and hermitian forms, IEEE Transactions on Information Theory, vol. 41, n°5, September 1995.

[4] J.-P. Cherdieu, A. Delcroix, J-C. Mado & D.-J. Mercier, Weight distribution of the hermitian Reed-Muller code, Applicable Algebra in Engineering, Communication and Computing, AAECC 8, 1997.

[5] J.-P. Cherdieu, D.-J. Mercier & T. Narayaninsamy, On the generalized weights of a class of trace codes, Finite Fields and Their Applications, Vol. 7, pp. 355-371, 2001.

[6] G. Lachaud & S. Vladut, Les codes correcteurs d’erreurs, La Recherche, Hors Série n°2, Août 1999.

[7] R. Lidl & H. Niederreiter, Finite fields, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley Publishing Company, 1983.