Hermitian forms, trace equations and application to codes

Dany-Jack Mercier*

November 14^{th}, 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 $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f\,(x)+v.x)=0$ or $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f\,(x))=a$ 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 (21^{th} 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 $\mathbb{F}_{t^2}$, 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 [ccof0007] 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 staightforward 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 Γ 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 ≥ 1 and let E be the vector space $\mathbb{F}_{t^2}^N$.

Définition 1 *A function* $H : \mathbb{F}_{t^2}^N \times \mathbb{F}_{t^2}^N \to \mathbb{F}_{t^2}$ *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.*

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

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

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

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* $\mathrm{H}\left(\mathbb{F}_{t^2}^N\right)$.

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 $\overline{x} = (a + b\alpha)^t = a + b\alpha^t = a + b\overline{\alpha}$.

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* ${}^T A$ *the transpose of* A. *The* ***conjugate*** *of* $A = (a_{ij})_{i,j}$ *is the matrix* $A^* = {}^T\left(\overline{A}\right) = \left(a_{ji}^t\right)_{i,j}$. *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,

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

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 $M = \mathrm{Mat}(H; e)$.

Théorème 1 *A sesquilinear form H is hermitian if, and only if, its matrix* $\mathrm{Mat}(H; e)$ *in a basis e is hermitian.*

Proof : Let M denotes the matrix $\mathrm{Mat}(H;e)$. If H is a hermitian form, $H(e_i,e_j)=\overline{H(e_j,e_i)}$ implies $M^*=M$. Conversely, $M^*=M$ implies

$$\forall X,Y \quad \overline{H(Y,X)}=\overline{Y}^*\overline{M}\,\overline{X}={}^TY\,\overline{M}\,\overline{X}={}^T\left({}^TY\,\overline{M}\,\overline{X}\right)=X^*MY=H(X,Y).\ \blacksquare$$

Corollaire 1 $\dim_{\mathbb{F}_t}\mathrm{H}\left(\mathbb{F}_{t^2}^N\right)=N^2$.

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 $\mathbb{F}_{t^2}$ and N coefficients a_{ii} $(1\leq i\leq N)$ in $\mathbb{F}_t$. Thus we have $2\times\frac{N^2-N}{2}+N=N^2$ independent parameters. ■

Let $P_e^{e'}=P$ 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

$$H(X,Y)=X^*MY=\left(PX'\right)^*M\left(PY'\right)=X'^*\left(P^*MP\right)Y'$$

and $\mathrm{Mat}(H;e')=P^*MP$ 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:

$$\begin{array}{rccc} H(x,.): & E & \longrightarrow & \mathbb{F}_{t^2} \\ & y & \longmapsto & H(x,y). \end{array}$$

The map:

$$\begin{array}{rccc} \widetilde{H}: & E & \longrightarrow & E^* \\ & x & \longmapsto & H(x,.) \end{array}$$

is semi-linear, i.e. satisfies $\widetilde{H}(\lambda x+x')=\overline{\lambda}\widetilde{H}(x)+\widetilde{H}(x')$ for all vectors x, x' and all $\lambda\in\mathbb{F}_{t^2}$. The extern law $\bullet$ defined by $\lambda\bullet l=\overline{\lambda}.l$ gives us a new vector space structure on E^*. For convenience, we shall write $\overline{E^*}$ instead of E^* when we use this new extern law. The map $\widetilde{H}:E\rightarrow E^*$ is semi-linear if, and only if, $\widetilde{H}:E\rightarrow\overline{E^*}$ is linear, and we can introduce the matrix of $\widetilde{H}$ in the basis $e=(e_1,...,e_N)$ in E and the dual basis $e^*=(e_1^*,...,e_N^*)$ in $\overline{E^*}$. The linearity of $\widetilde{H}$ gives us the same results as in the case of symmetric bilinear forms. Namely:

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

Proof : Assume that $\mathrm{Mat}\left(\widetilde{H};e,e^*\right)=(a_{ij})$. Then $\widetilde{H}(e_j)=\sum_i a_{ij}\bullet e_i^*$ and

$$\widetilde{H}(e_j)(e_k)=H(e_j,e_k)=\overline{a}_{kj}.$$

Thus $\mathrm{Mat}\left(\widetilde{H};e,e^*\right)={}^T\overline{\mathrm{Mat}(H;e)}=\mathrm{Mat}(H;e)$. ■

Définition 3 *The* ***kernel*** $\mathrm{Ker}\,H$ *(resp.* ***rank*** $\mathrm{rk}\,H$*) of* H *is the* ***kernel*** *(resp.* ***rank****) of* $\widetilde{H}$. *Thus* $\mathrm{Ker}\,H=\{x\in E\,/\,\forall y\in E\quad H(x,y)=0\}$ *and* $\mathrm{rk}\,H=\mathrm{rk}(\mathrm{Mat}(H;e))$.

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,*

$$\begin{array}{ll} F\subset\left(F^{\perp}\right)^{\perp}, & F\subset G\Rightarrow G^{\perp}\subset F^{\perp}, \\ (F+G)^{\perp}=F^{\perp}\cap G^{\perp}, & (F\cap G)^{\perp}\supset F^{\perp}+G^{\perp}. \end{array}$$

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 $\mathrm{Mat}(H;e)$ 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) $H(x,y)+H(y,x)=\frac{1}{2}\left[q(x+y)-q(x-y)\right]$,
2) $H(x,y)-H(y,x)=\frac{1}{\alpha-\overline{\alpha}}\left[q(x+\alpha y)-q(x+\overline{\alpha}y)\right]$,
3) $H(x,y)=\frac{1}{4}\left[q(x+y)-q(x-y)\right]+\frac{1}{2(\alpha-\overline{\alpha})}\left[q(x+\alpha y)-q(x+\overline{\alpha}y)\right]$.

Proof : We have

$$\begin{aligned} q(x+y)-q(x-y) &= q(x)+H(x,y)+H(y,x)+q(y) \\ &\qquad -\left[q(x)+H(x,-y)+H(-y,x)+H(-y,-y)\right] \\ &= 2\left(H(x,y)+H(y,x)\right) \end{aligned}$$

and

$$\begin{aligned} q(x+\alpha y)-q(x+\overline{\alpha}y) &= q(x)+\alpha H(x,y)+\alpha^{t}H(y,x)+\alpha^{t+1}q(y) \\ &\qquad -\left[q(x)+\alpha^{t}H(x,y)+\alpha H(y,x)+\alpha^{t+1}q(y)\right] \\ &= \left(\alpha-\alpha^{t}\right)\left(H(x,y)-H(y,x)\right). \end{aligned}$$

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

Lemme 2 *The norm application*

$$\begin{array}{cccc} N_{\mathbb{F}_{t^m}/\mathbb{F}_t}: & \mathbb{F}_{t^m}^{*} & \to & \mathbb{F}_t^{*} \\ & x & \mapsto & x^{t^{m-1}+...+t+1} \end{array}$$

is a multiplicative group epimorphism, and $\left|N_{\mathbb{F}_{t^m}/\mathbb{F}_t}^{-1}(b)\right|=\frac{t^m-1}{t-1}$ 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 α in $\mathbb{F}_{t^m}$. It means that α generates the multiplicative group $\mathbb{F}_{t^m}^{*}$, hence

$$\mathbb{F}_{t^m}=\left\{0,1,\alpha,\alpha^2,...,\alpha^{t^m-2}\right\}.$$

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

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

and $N_{\mathbb{F}_{t^m}/\mathbb{F}_t}$ is surjective. The decomposition of the morphism $N_{\mathbb{F}_{t^m}/\mathbb{F}_t}$ gives

$$\mathbb{F}_{t^m}^* / \operatorname{Ker}\left(N_{\mathbb{F}_{t^m}/\mathbb{F}_t}\right) \simeq \mathbb{F}_t^*,$$

hence $\left|\operatorname{Ker}\left(N_{\mathbb{F}_{t^m}/\mathbb{F}_t}\right)\right| = \frac{t^m-1}{t-1}$. If $a \in N_{\mathbb{F}_{t^m}/\mathbb{F}_t}^{-1}(b)$, then

$$N_{\mathbb{F}_{t^m}/\mathbb{F}_t}(x) = b \Leftrightarrow N_{\mathbb{F}_{t^m}/\mathbb{F}_t}\left(xa^{-1}\right) = 1 \Leftrightarrow x \in a \operatorname{Ker}\left(N_{\mathbb{F}_{t^m}/\mathbb{F}_t}\right)$$

and we deduce $\left|N_{\mathbb{F}_{t^m}/\mathbb{F}_t}^{-1}(b)\right| = \left|\operatorname{Ker} N_{\mathbb{F}_{t^m}/\mathbb{F}_t}\right| = \frac{t^m-1}{t-1}$. ■

Théorème 4 ***Existence of H-orthogonal basis***
If t is odd and if H is a hermitian form on $E = \mathbb{F}_{t^2}^N$,
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 $\operatorname{Mat}(H; e)$ 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 $a \in \mathbb{F}_{t^2}^*$ such that $a^{t+1} = b$. Hence $H\left(\frac{x}{a}, \frac{x}{a}\right) = 1$ and we take the basis $e_1 = \frac{x}{a}$.
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 1.
- If there exists x with $H(x,x) \neq 0$, we proceed as in the case $N = 1$ to show the existence of $a \in \mathbb{F}_{t^2}^*$ such that $H\left(\frac{x}{a}, \frac{x}{a}\right) = 1$. The subspace

$$F = (Kx)^{\perp} = \{y \in E \,/\, H(x,y) = 0\} = \operatorname{Ker} \widetilde{H}(x)$$

is an hyperplane of E as it is the kernel of a non zero linear form. But $E = F \oplus \operatorname{Vect}(x)$ 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 $\left(e_1, ..., e_{N-1}, \frac{x}{a}\right)$ is a H-orthogonal basis of E and this complete the proof of 1). The second part of the Theorem follows from

$$\operatorname{rk} H = \operatorname{rk} \widetilde{H} = \operatorname{rk} \operatorname{Mat}(H; e) \,. \blacksquare$$

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) $\operatorname{Ker} \widetilde{H} = \{0\}$,
3) $\widetilde{H}$ is an isomorphism from E to $\overline{E^*}$,
4) $\operatorname{Mat}(H; e)$ is non singular.

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

Théorème 6 *Theorem 3 can be improved if H is non degenerate. We get:*

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

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

$$F^{\perp} = \{x \in E \,/\, \forall i \in \mathbb{N}_p \; H(x, e_i) = 0\} = \bigcap_{i=1}^{p} \ker \widetilde{H}(e_i)$$

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

4.1 Isotropy

Définition 7 *Let H be a hermitian form on $E = \mathbb{F}_{t^2}^N$. 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 $\operatorname{Vect}(x)$ generated by x is isotropic.

Théorème 7 *Let H denote a hermitian form on $E = \mathbb{F}_{t^2}^N$, 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:

$$\begin{aligned}(i) &\Leftrightarrow \forall x \in F \quad ((\forall y \in F \quad H(x,y) = 0) \Rightarrow x = 0) \\ &\Leftrightarrow \forall x \in F \quad \left(x \in F^{\perp} \Rightarrow x = 0\right) \Leftrightarrow F \cap F^{\perp} = \{0\} \Leftrightarrow (ii).\end{aligned}$$

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 $F \to \mathbb{F}_{t^2}\,;\, z \mapsto H(x,z)$. 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 $\mathbb{F}_{t^2}^N$

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

$$\begin{array}{rccc} q: & E & \longrightarrow & \mathbb{F}_t \\ & x & \longmapsto & q(x) = H(x,x) \end{array}$$

is called the ***quadratic hermitian form*** *on E associated to H. We denote by $\mathrm{QH}\left(\mathbb{F}_{t^2}^N\right)$ the space of all quadratic hermitian forms on E.*

With this Definition:

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

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

(2) $\forall x, y \in E\ H(x,y) = \frac{1}{4}\left[q(x+y) - q(x-y)\right] + \frac{1}{2(\alpha - \overline{\alpha})}\left[q(x+\alpha y) - q(x + \overline{\alpha} y)\right].$

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 1). 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*

$$\begin{array}{rccc} \Psi: & \mathrm{H}\left(\mathbb{F}_{t^2}^N\right) & \longrightarrow & \mathbb{F}_t^E \\ & H & \longmapsto & q \text{ such that } q(x) = H(x,x) \end{array}$$

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

Proof : Result (2) shows that Ψ is one to one. ∎

Définition 9 *Let $q \in \mathrm{QH}\left(\mathbb{F}_{t^2}^N\right)$. The unique hermitian form H satisfying $\Psi(H) = q$ is called the* ***polar form*** *of q, and is given by result (2). The isomorphism $\mathrm{QH}\left(\mathbb{F}_{t^2}^N\right) \simeq \mathrm{H}\left(\mathbb{F}_{t^2}^N\right)$ 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

$$\begin{aligned} H(x,x) = \sum_{i,j} a_{ij} \overline{x}_i x_j &= \sum_{i=1}^N a_{ii} x_i^{t+1} + \sum_{1 \le i < j \le N} \left(a_{ij}\overline{x}_i x_j + a_{ji} \overline{x}_j x_i\right) \\ &= \sum_{i=1}^N a_{ii} x_i^{t+1} + \sum_{1 \le i < j \le N} \left(a_{ij}\overline{x}_i x_j + \left(a_{ij}\overline{x}_i x_j\right)^t\right). \end{aligned}$$

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

$$\forall x \in E \quad q(x) = \sum_{i=1}^N a_{ii}\, \mathrm{N}_{\mathbb{F}_{t^2}/\mathbb{F}_t}(x_i) + \sum_{1 \le i < j \le N} \mathrm{Tr}_{\mathbb{F}_{t^2}/\mathbb{F}_t}\left(a_{ij}\overline{x}_i x_j\right)$$

where $(x_1, ..., x_N)$ are the coordinates of x in a basis, $a_{ii} \in \mathbb{F}_t$ and $a_{ij} \in \mathbb{F}_{t^2}$ for all $i \neq j$. In fact Theorem 4 ensures us the existence of a H-orthogonal basis of E. In such a basis $q(x) = \sum_{i=1}^r x_i^{t+1}$ for all $x \in E$.
Next Theorem provides another criterion for q:

Théorème 9 *If* $q \in \mathbb{F}_t^E$ *satisfies (1) and if* H *defined by (2) is sesquilinear, then* q *is the quadratric hermitian form associated with the hermitian form* H*.*

Proof : (1) and (2) show that

$$\begin{aligned} H(x,x) &= \frac{1}{4}\left[q(2x) - q(0)\right] + \frac{1}{2(\alpha - \overline{\alpha})}\left[q((1+\alpha)x) - q((1+\overline{\alpha})x)\right] \\ &= \frac{1}{4}\left[2^{t+1}q(x)\right] + \frac{1}{2(\alpha - \overline{\alpha})}\left[(1+\alpha)^{t+1} - (1+\overline{\alpha})^{t+1}\right]q(x) \\ &= q(x) + \frac{1}{2(\alpha - \overline{\alpha})}\left[\left(1+\alpha^t\right)(1+\alpha) - \left(1+\overline{\alpha}^t\right)(1+\overline{\alpha})\right]q(x) = q(x). \end{aligned}$$

By hypothesis, the form H is sesquilinear, and it remains to prove the hermitian symetry. We have

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

Condition 2) of Lemma 1 yields

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

hence

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

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)* φ_1 *and* φ_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*

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

Théorème 10 *Let* q_1 *and* q_2 *denote two quadratic hermitian forms whose polar forms are* φ_1 *and* φ_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) $\Leftrightarrow$ ii) : Let $e = (e_1, ..., e_N)$ denote a basis of E. We have

$$\begin{aligned} (\varphi_1 \sim \varphi_2) &\Leftrightarrow \exists u \in \mathrm{GL}(E) \quad \forall x,y \in E \quad \varphi_2(x,y) = \varphi_1(u(x),u(y)) \\ &\Leftrightarrow \exists u \in \mathrm{GL}(E) \quad \forall i,j \in \mathbb{N}_n \quad \varphi_2(e_i,e_j) = \varphi_1(u(e_i),u(e_j)) \\ &\Leftrightarrow \exists u \in \mathrm{GL}(E) \quad \mathrm{Mat}(\varphi_2;e) = \mathrm{Mat}(\varphi_1;u(e)), \end{aligned}$$

therefore i) implies ii).
Conversely, if there are two basis e and e' such that $\mathrm{Mat}(\varphi_2; e) = \mathrm{Mat}(\varphi_1; e')$, 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) $\Leftrightarrow$ iii) : If $\mathrm{Mat}(\varphi_2; e) = \mathrm{Mat}(\varphi_1; e')$ then φ_1 and φ_2 have same rank. Conversely, if φ_1 and φ_2 have same rank r, Theorem 4 provides two basis e and e' such that $\mathrm{Mat}(\varphi_2; e)$ and $\mathrm{Mat}(\varphi_1; e')$ are equal to the diagonal matrix $\mathrm{Diag}(1, ..., 1, 0, ..., 0)$ with r numbers 1. ■

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

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

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

$$\begin{array}{cccc} f: & \mathbb{F}_t^{2N} & \to & \mathbb{F}_t \\ & x & \mapsto & H(\iota x, \iota x). \end{array}$$

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

It is clear that the function

$$\begin{array}{ccc} \mathrm{QH}\left(\mathbb{F}_{t^2}^N\right) & \to & \mathrm{QH}\left(\mathbb{F}_t^{2N}\right) \\ q & \mapsto & f \end{array}$$

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

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*

$$\begin{array}{cccc} B: & \mathbb{F}_t^{2N} \times \mathbb{F}_t^{2N} & \to & \mathbb{F}_t \\ & (x, y) & \mapsto & f(x + y) - f(x) - f(y). \end{array}$$

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

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 coodinates of x and with coefficients in $\mathbb{F}_t$. Indeed, it suffices to use a H-orthogonal basis of $\mathbb{F}_{t^2}^N$ to get $q(x) = \sum_{i=1}^r x_i^{t+1}$ for all $x \in E$ (Theorem 4) and

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

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 $f(x + y) = f(x) + f(y) + H(\iota x, \iota y) + H(\iota x, \iota y)^t$. ■

Définition 12 *For simplicity, we also say that B is a bilinear form associated with f.*

Remark : If t is even, say $t = 2^{\zeta}$, a symmetric bilinear form on $\mathbb{F}_t^{2N}$ is

$$B(x,y) = \sum_i a_{ii} x_i y_i + \sum_{i<j} a_{ij} (x_i y_j + x_j y_i) \qquad (*)$$

and the quadratic form associated to B is $f(x) = B(x,x) = \sum_i a_{ii} x_i^2$. A quadratic form on $\mathbb{F}_{2^{\zeta}}^{2N}$ will be an homogeneous polynomial of degree 2 in the coordinates $x_1, ..., x_{2N}$ with no diagonal term $a_{ij} x_i x_j$. Conversely, if $f(x) = \sum_i a_{ii} x_i^2$ is a quadratic form on $\mathbb{F}_t^{2N}$, there exists an infinity of symmetric bilinear forms $B(x,y)$ such that $B(x,x) = f(x)$, and this is different from the usual case. Indeed, it suffices to choose any coefficients a_{ij} ($i<j$) in $\mathbb{F}_{2^{\zeta}}$ and to define $B(x,y)$ by $(*)$ to get $B(x,x) = f(x)$. In this case, the map $B(x,y) = f(x+y) - f(x) - f(y)$ of Theorem 11 will never be the bilinear form associated with f as $B(x,x) = f(2x) - 2f(x) = 0$.

The kernel of B is

$$\operatorname{Ker} B = \left\{ x \in \mathbb{F}_t^{2N} \,/\, \forall y \in \mathbb{F}_t^{2N} \; B(x,y) = 0 \right\},$$

and the orthogonal of $\operatorname{Ker} B$ for the usual inner product in $\mathbb{F}_t^{2N}$ is

$$(\operatorname{Ker} B)^{\perp} = \left\{ x \in \mathbb{F}_t^{2N} \,/\, \forall y \in \operatorname{Ker} B \; x.y = x_1.y_1 + ... + x_{2N}.y_{2N} = 0 \right\}.$$

Since the usual inner product $x.y$ is only a non degenerate bilinear form on $\mathbb{F}_t^{2N}$, we have $\dim \operatorname{Ker} B + \dim (\operatorname{Ker} B)^{\perp} = 2N$ but we can't say that $\mathbb{F}_t^{2N} = \operatorname{Ker} B \oplus (\operatorname{Ker} B)^{\perp}$. With these notations :

Théorème 12 *We have $\iota(\operatorname{Ker} B) = \operatorname{Ker} H$. Thus ι induces a $\mathbb{F}_t$-isomorphism from $\operatorname{Ker} B$ onto $\operatorname{Ker} H$ and $\operatorname{rk} f = \operatorname{rk} B = 2 \operatorname{rk} H$.*

Proof : Let ψ denotes a non trivial additive character on $\mathbb{F}_t$. The map $\psi' = \psi \circ \operatorname{Tr}_{\mathbb{F}_{t^2}/\mathbb{F}_t}$ is a non trivial additive character on $\mathbb{F}_{t^2}$ and Lemma 3 gives:

$$\begin{aligned}(x \in \operatorname{Ker} B) &\Leftrightarrow \forall y \in \mathbb{F}_t^{2N} \quad B(x,y) = \operatorname{Tr}_{\mathbb{F}_{t^2}/\mathbb{F}_t}(H(\iota x, \iota y)) = 0 \\ &\Leftrightarrow \sum_{y \in \mathbb{F}_t^{2N}} \psi\left(\operatorname{Tr}_{\mathbb{F}_{t^2}/\mathbb{F}_t}(H(\iota x, \iota y))\right) \neq 0 \Leftrightarrow \sum_{z \in \mathbb{F}_{t^2}^N} \psi\left(\operatorname{Tr}_{\mathbb{F}_{t^2}/\mathbb{F}_t}(H(\iota x, z))\right) \neq 0 \\ &\Leftrightarrow \sum_{z \in \mathbb{F}_{t^2}^N} \psi'(H(\iota x, z)) \neq 0 \Leftrightarrow \forall z \in \mathbb{F}_{t^2}^N \quad H(\iota x, z) = 0 \Leftrightarrow \iota x \in \operatorname{Ker} H.\end{aligned}$$

Hence $\iota(\operatorname{Ker} B) \subset \operatorname{Ker} H$. Since ι is a $\mathbb{F}_t$-isomorphism, the above equivalences imply the inverse inclusion. To complete the proof, we write

$$\operatorname{rk} f = \operatorname{rk} B = 2N - \dim_{\mathbb{F}_t} \operatorname{Ker} B = 2N - 2\dim_{\mathbb{F}_{t^2}} \operatorname{Ker} H = 2 \operatorname{rk} H. \blacksquare$$

Théorème 13 *1) There is an endomorphism T of $\mathbb{F}_t^{2N}$ such that $B(x,y) = T(x).y$ for all $(x,y) \in \mathbb{F}_t^{2N} \times \mathbb{F}_t^{2N}$.*
2) We have $\operatorname{Ker} T = \operatorname{Ker} B$, $\operatorname{Im} T = (\operatorname{Ker} B)^{\perp}$ and $\operatorname{Ker} T \subset f^{-1}(0)$.

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 $B(x,y) = T(x).y$ for all $y \in \mathbb{F}_t^{2N}$. From $B(\lambda x + x', y) = \lambda B(x,y) + B(x',y)$ we deduce $[T(\lambda x + x') - \lambda T(x) - T(x')].y = 0$ for all $y \in \mathbb{F}_t^{2N}$, hence

$$T\left(\lambda x + x'\right) - \lambda T(x) - T\left(x'\right) = 0$$

and the linearity of T follows.
2) The first equality is a consequence of

$$x \in \operatorname{Ker} T \Leftrightarrow \left(\forall y \in \mathbb{F}_t^{2N} \quad T(x).y = 0\right) \Leftrightarrow \left(\forall y \in \mathbb{F}_t^{2N} \quad B(x,y) = 0\right) \Leftrightarrow x \in \operatorname{Ker} B.$$

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

$$\dim(\operatorname{Im} T) = 2N - \dim(\operatorname{Ker} T) = 2N - \dim(\operatorname{Ker} B) = \dim\left((\operatorname{Ker} B)^{\perp}\right).$$

If $x \in \operatorname{Ker} T = \operatorname{Ker} B$ then $f(x) = H(\iota x, \iota x) = 0$ from Theorem 12, thus $\operatorname{Ker} T \subset f^{-1}(0)$. ∎

8 Exponential sums $\mathbf{S}(f,v)$

Let us denote by ψ the additive character on $\mathbb{F}_t$ defined by

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

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

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

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

$$\sum_{y \in V} \psi(l(y)) = \begin{cases} t^m & \text{if } l = 0, \\ 0 & \text{if } l \neq 0. \end{cases}$$

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

$$\sum_{x \in \mathbb{F}_{t^m}} \psi\left(\mathrm{N}_{\mathbb{F}_{t^m}/\mathbb{F}_t}(x)\right) = \frac{t - t^m}{t-1}.$$

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

$$\sum_{x \in \mathbb{F}_{t^m}} \psi\left(\mathrm{N}_{\mathbb{F}_{t^m}/\mathbb{F}_t}(x)\right) = 1 + \sum_{x \in \mathbb{F}_{t^m}^*} \psi\left(\mathrm{N}_{\mathbb{F}_{t^m}/\mathbb{F}_t}(x)\right) = 1 + \frac{t^m - 1}{t-1} \sum_{z \in \mathbb{F}_t^*} \psi(z).$$

The use of the orthogonality relation $\sum_{z\in\mathbb{F}_t^*}\psi(z)=-1$ completes the proof. ■

We are now ready to give another proof of the main result in [3]. In fact, a small mistake occured in Proposition 3 of [3] as $A(s,v)$ do not depends on $f(u)$ but on $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u))$, 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 2ρ in $\mathbb{F}_t^{2N}$. Consider the extensions $\mathbb{F}_p\subset\mathbb{F}_s\subset\mathbb{F}_t\subset\mathbb{F}_{t^2}$ and let $a\in\mathbb{F}_s^*$.*
1) If $v\in(\mathrm{Ker}\,B)^{\perp}=\mathrm{Im}\,T$, we can find $u\in\mathbb{F}_t^{2N}$ such that $v=T(u)$. Then

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

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

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

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

Proof : Without loss of generality, we can assume that f is given in the standard form $f(x)=H(y,y)=q(y)=y_1^{t+1}+...+y_\rho^{t+1}$ where $y=\iota(x)\in\mathbb{F}_{t^2}^N$.

1) α) 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 $z=\iota u$. 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

$$\begin{aligned}S(f,v)&=\sum_{y_1,\dots,y_N\in\mathbb{F}_{t^2}}\prod_{k=1}^{\rho}\psi\left((z_k+y_k)^{t+1}-z_k^{t+1}\right)\\&=t^{2(N-\rho)}\sum_{y_1,\dots,y_\rho\in\mathbb{F}_{t^2}}\prod_{k=1}^{\rho}\psi\left((z_k+y_k)^{t+1}-z_k^{t+1}\right)\\&=t^{2(N-\rho)}\xi\prod_{k=1}^{\rho}\psi\left(-z_k^{t+1}\right)\end{aligned}$$

where $\xi=\sum_{y_1,\dots,y_\rho\in\mathbb{F}_{t^2}}\prod_{k=1}^{\rho}\psi\left((z_k+y_k)^{t+1}\right)$. We have

$$\xi=\sum_{y_1,\dots,y_{\rho-1}\in\mathbb{F}_{t^2}}\left(\prod_{k=1}^{\rho-1}\psi\left((z_k+y_k)^{t+1}\right)\right)\left(\sum_{y_\rho\in\mathbb{F}_{t^2}}\psi\left((z_\rho+y_\rho)^{t+1}\right)\right).$$

Lemma 4 gives $\sum_{y_\rho\in\mathbb{F}_{t^2}} \psi\left((z_\rho+y_\rho)^{t+1}\right) = \sum_{y\in\mathbb{F}_{t^2}} \psi\left(y^{t+1}\right) = -t$, hence

$$\xi = (-t) \sum_{y_1,\dots,y_{\rho-1}\in\mathbb{F}_{t^2}} \left(\prod_{k=1}^{\rho-1} \psi\left((z_k+y_k)^{t+1}\right)\right).$$

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

$$\begin{aligned} S(f,v) &= (-1)^\rho\, t^{2N-\rho} \prod_{k=1}^{\rho} \psi\left(-z_k^{t+1}\right) = (-1)^\rho\, t^{2N-\rho} \psi\left(-z_1^{t+1} - \dots - z_\rho^{t+1}\right) \\ &= (-1)^\rho\, t^{2N-\rho} \psi\left(-q(z)\right). \end{aligned}$$

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

β) 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

$$T_a(x).y = f_a(x+y) - f_a(x) - f_a(y) = a\left(f(x+y) - f(x) - f(y)\right) = a\left(T(x).y\right).$$

Hence $T_a = aT$. We have $v = T_a u_a = aT(u_a) = T(au_a)$, and we can take $u = au_a$. This gives $S(af,v) = (-1)^\rho\, t^{2N-\rho}\psi\left(-af\left(a^{-1}u\right)\right) = (-1)^\rho\, t^{2N-\rho}\psi\left(-a^{-1}f(u)\right)$.

γ) By the above

$$\begin{aligned} \sum_{a\in\mathbb{F}_s^*} S(af,v) &= (-1)^\rho\, t^{2N-\rho} \sum_{a\in\mathbb{F}_s^*} \psi\left(-a^{-1}f(u)\right) \\ &= (-1)^\rho\, t^{2N-\rho} \sum_{a\in\mathbb{F}_s^*} \psi'\left(-a^{-1}\operatorname{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u))\right) \end{aligned}$$

where ψ' is the additive character $\psi'(x) = \exp\left(\frac{i2\pi}{p}\operatorname{Tr}_{\mathbb{F}_s/\mathbb{F}_p}(x)\right)$ 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 19) yields

$$\begin{aligned} \sum_{a\in\mathbb{F}_s^*} S(af,v) &= (-1)^\rho\, t^{2N-\rho} \left(-1 + \sum_{\chi\in\mathbb{F}_s^\wedge} \chi\left(\operatorname{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u))\right)\right) \\ &= (-1)^\rho\, t^{2N-\rho} A(s,v). \end{aligned}$$

2) Define $f_a = af$. Since $a \in \mathbb{F}_s$, f_a is a hermitian quadratic form on $\mathbb{F}_t^{2N}$ and the bilinear form $B_a(x,y) = f_a(x+y) - f_a(x) - f_a(y)$ associated to f_a satisfies $\operatorname{Ker} B_a = \operatorname{Ker} B$. Hence we can assume that $a = 1$ without loss of generality. Let $v \notin (\operatorname{Ker} B)^\perp$. 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

$S(f,v)\overline{S(f,0)}=0$. We have:

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

Since $v\notin(\operatorname{Ker}B)^{\perp}$, 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 $S(f,v)\overline{S(f,0)}=0$. ■

Remark: The constant $A(s,v)$ in Theorem 14 depends wether $\operatorname{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u))=0$ or not. It has a meaning if we check that $v=T(u)=T(u')$ and $\operatorname{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u))=0$ imply $\operatorname{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u'))=0$. Let $v=T(u)=T(u')$. Then $u-u':=w\in\operatorname{Ker}T$ 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 ρ be a positive integer such that $1\leq\rho\leq N$, and f be a quadratic hermitian form of rank 2ρ on ${\mathbb{F}_t}^{2N}$. The number M of solutions of the equation $\operatorname{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)+v.x)=0$ in $\mathbb{F}_t^{2N}$ is*

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

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

$$sM=\sum_{c\in\mathbb{F}_s}\sum_{x\in\mathbb{F}_t^{2N}}\psi'\left(c\operatorname{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)+v.x)\right).$$

Since

$$\begin{aligned}
\psi'\left(c\operatorname{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)+v.x)\right) &= \exp\left(\frac{i2\pi}{p}\operatorname{Tr}_{\mathbb{F}_s/\mathbb{F}_p}\left(c\operatorname{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)+v.x)\right)\right)\\
&= \exp\left(\frac{i2\pi}{p}\operatorname{Tr}_{\mathbb{F}_t/\mathbb{F}_p}(cf(x)+cv.x)\right)\\
&= \psi(cf(x)+cv.x),
\end{aligned}$$

we deduce

$$sM = \sum_{c\in\mathbb{F}_s}\sum_{x\in\mathbb{F}_t^{2N}} \psi\left(cf\left(x\right)+cv.x\right) = t^{2N} + \sum_{c\in\mathbb{F}_s^*}\sum_{x\in\mathbb{F}_t^{2N}} \psi\left(c^{-1}f\left(cx\right)+v.\left(cx\right)\right)$$
$$= t^{2N} + \sum_{c\in\mathbb{F}_s^*} S\left(c^{-1}f, v\right).$$

Now the assertion follows from Theorem 14. ■

Théorème 16 *{[5], Prop. 3} Let a be an element of* $\mathbb{F}_s$, ρ *be a positive integer with* $1\le\rho\le N$, *and f be a quadratic hermitian form of rank* 2ρ *on* ${\mathbb{F}_t}^{2N}$. *The number M of solutions of the equation* $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)) = a$ *in* $\mathbb{F}_t^{2N}$ *is*

$$M = \begin{cases} \frac{1}{s}\left(t^{2N} - (-1)^{\rho}\, t^{2N-\rho}\right) & \text{if } a\neq 0, \\ \frac{1}{s}\left(t^{2N} + (-1)^{\rho}\,(s-1)\, t^{2N-\rho}\right) & \text{if } a = 0. \end{cases}$$

Proof : We can assume that f is given in the standard form $f(x) = H(y,y) = y_1^{t+1}+...+y_\rho^{t+1}$ where $y = \iota(x)\in\mathbb{F}_{t^2}^N$. If $\hat{\mathbb{F}_s}$ denotes the set of additive characters on $\mathbb{F}_s$, then (Theorem 21)

$$sM = \sum_{\psi\in\hat{\mathbb{F}_s}}\sum_{x\in\mathbb{F}_t^{2N}} \psi\left(\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}\left(f\left(x\right)\right)-a\right).$$

Hence

$$sM = t^{2N} + \sum_{\psi\neq\mathbf{1}}\overline{\psi\left(a\right)}\sum_{y\in\mathbb{F}_{t^2}^N}\psi\left(\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}\left(y_1^{t+1}+...+y_\rho^{t+1}\right)\right).$$

We have

$$A_\psi = \sum_{y\in\mathbb{F}_{t^2}^N}\psi\left(\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}\left(y_1^{t+1}\right)\right)...\psi\left(\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}\left(y_\rho^{t+1}\right)\right)$$
$$= t^{2(N-\rho)}\left(\sum_{y\in\mathbb{F}_{t^2}}\psi\left(\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}\left(y^{t+1}\right)\right)\right)^{\rho} = t^{2(N-\rho)}B_\psi^{\rho}$$

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

$$B_\psi = 1 + (t+1)\sum_{z\in\mathbb{F}_t^*}\psi\left(\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}\left(z\right)\right) = -t.$$

Therefore

$$sM = t^{2N} + (-1)^{\rho}\, t^{2N-\rho}\sum_{\psi\neq\mathbf{1}}\overline{\psi\left(a\right)} = t^{2N} + (-1)^{\rho}\, t^{2N-\rho}\left(-1+\sum_{\psi\in\hat{\mathbb{F}_s}}\overline{\psi}\left(a\right)\right)$$

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 $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)+v.x) = a$ in $\mathbb{F}_t^{2N}$.

10 The code Γ

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

$$\begin{array}{rccc} \gamma: & \mathrm{QH}\left(\mathbb{F}_t^{2N}\right)\times\mathbb{F}_t^{2N} & \rightarrow & \mathbb{F}_s^{t^{2N}} \\ & (f,v) & \mapsto & \left(\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)+v.x)\right)_{x\in\mathbb{F}_t^{2N}} \end{array}$$

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

Théorème 17 *The weights* $\mathrm{w}(\gamma(f,v))$ *of the non null code-word* $\gamma(f,v)$ *of the code* Γ *satisfy:*

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

and the bounds of these inequalities are reached. The parameters and the disparity of Γ *are:*

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

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

$$K_\Gamma=\dim_{\mathbb{F}_s}\Gamma=\dim_{\mathbb{F}_s}\left(\mathrm{QH}\left(\mathbb{F}_t^{2N}\right)\times\mathbb{F}_t^{2N}\right)=\left(N^2+2N\right)\log_s t.$$

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

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

We consider several cases:

1. If $v=0$, then $f\neq 0$, and

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

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

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

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

2. If $v\neq 0$,

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

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

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

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

$$\frac{1}{s}\left(t^{2N} + (s-1)\, t^{2N-2\left[\frac{N}{2}\right]}\right) \leq \mathrm{M}(f,v) \leq \frac{1}{s}\left(t^{2N} + (s-1)\, t^{2N-2}\right). \qquad (3)$$

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

$$\frac{1}{s}\left(t^{2N} - t^{2N-2}\right) \leq \mathrm{M}(f,v) \leq \frac{1}{s}\left(t^{2N} - t^{2N-2\left[\frac{N}{2}\right]}\right). \qquad (4)$$

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

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

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

$$\frac{1}{s}\left(t^{2N} - (s-1)\, t^{2N-1}\right) \leq \mathrm{M}(f,v) \leq \frac{1}{s}\left(t^{2N} - (s-1)\, t^{2N-2\left[\frac{N-1}{2}\right]-1}\right). \qquad (5)$$

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

$$\frac{1}{s}\left(t^{2N} + t^{2N-2\left[\frac{N-1}{2}\right]-1}\right) \leq \mathrm{M}(f,v) \leq \frac{1}{s}\left(t^{2N} + t^{2N-1}\right). \qquad (6)$$

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

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

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

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

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 $\left[\frac{D_C-1}{2}\right]$ 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

$$[N_R, K_R, D_R] = \left[t^{2N}, 2N^2 + 3N + 1, t^{2N} - 2t^{2N-1}\right].$$

Let us compare $R(2,2N)$ to the code Γ with same length t^{2N} obtained with $s=t$. The code $R(2,2N)$ have a better transmission rate since

$$\frac{K_R}{N_R}-\frac{K_\Gamma}{N_\Gamma}=\frac{1}{t^{2N}}\left(N^2+N+1\right)$$

is always positive, but the numbers of corrected errors is better with Γ since

$$D_\Gamma-D_R=t^{2N-1}-t^{2N-2}$$

is always positive. One can also check that the difference

$$\lambda(\Gamma)-\lambda(R)=\frac{1}{t^{2N}}\left(t^{2N-1}-t^{2N-2}-N^2-N-1\right)$$

is positive or null as soon as $N\geq 2$ or $t\geq 4$. In this sens, Γ have better parameters than $R(2,2N)$.

11 The code C

The parameters of the code Γ in Section 10 are computed from Theorem 15. We can apply the same construction to use Theorem 16. The image of the linear map

$$\begin{array}{rccc} c: & \mathrm{QH}\left(\mathbb{F}_t^{2N}\right)\times\mathbb{F}_s & \to & \mathbb{F}_s^{t^{2N}} \\ & (f,a) & \mapsto & \left(\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x))-a\right)_{x\in\mathbb{F}_t^{2N}} \end{array}$$

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 $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x))=a$ for all $x\in\mathbb{F}_t^{2N}$, and if ρ denotes the rank of f, then $f(x)=y_1^{t+1}+...+y_\rho^{t+1}$ where $y=\iota x$ and $1\leq\rho\leq N$, and the assumpion on f implies $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(y_1^{t+1})=a$ for all $y_1\in\mathbb{F}_{t^2}$. This is a contradiction of the fact that the map $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}\circ\mathrm{N}_{\mathbb{F}_{t^2}/\mathbb{F}_t}:\mathbb{F}_{t^2}\to\mathbb{F}_s$ is onto.
As c is one to one, the dimension of C will be:

$$K_C=\dim_{\mathbb{F}_s}\left(\mathrm{QH}\left(\mathbb{F}_t^{2N}\right)\times\mathbb{F}_s\right)=1+N^2\log_s t.$$

Théorème 18 *The weights* $\mathrm{w}(c(f,a))$ *of the non null code-words* $c(f,a)$ *in* C *satisfy:*

$$t^{2N}-\frac{1}{s}\left(t^{2N}+t^{2N-1}\right)\leq\mathrm{w}(c(f,a))\leq t^{2N}$$

and the bounds are reached. The parameters and the disparity of C *are:*

$$[N_C,K_C,D_C]=\left[t^{2N},1+N^2\log_s t,t^{2N}-\frac{1}{s}\left(t^{2N}+t^{2N-1}\right)\right]\ \textit{and}\ r(C)=\frac{st}{st-t-1}.$$

Proof : It suffices to bound the weights $\mathrm{w}(c(f,a))$. We certainly have

$$\mathrm{w}(c(f,a))=t^{2N}-\mathrm{M}(f,a)$$

where $\mathrm{M}(f,a)$, which denotes the number of solutions of the equation $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x))=a$ in $\mathbb{F}_t^{2N}$, is given by Theorem 16.

1. If $a=0$, we know that $\rho \neq 0$.

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

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

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

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

2. If $a \neq 0$,

2.1. If ρ is even,

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

2.2. If ρ is odd,

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

The bounds (1) to (4) imply

$$\forall (f,a) \in \left(\mathrm{QH}\left(\mathbb{F}_t^{2N}\right) \times \mathbb{F}_s\right) \setminus \{(0,0)\} \qquad 0 \leq \mathrm{M}(f,a) \leq \frac{1}{s}\left(t^{2N}+t^{2N-1}\right). \blacksquare$$

Let us compare C with Γ and $R(2,2N)$. The codes C and Γ have same length and same minimal distance, thus will correct the same amount of errors. Nevertheless the dimension of Γ is greater than those of C, hence Γ 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

$$\frac{K_R}{N_R} - \frac{K_C}{N_C} = \frac{N^2+3N}{t^{2N}} > 0.$$

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 ψ 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 $\mathrm{Im}\,\psi$ 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 $\mathbf{1}$ is defined by $\mathbf{1}(x)=1$ 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 $\psi \in G^\wedge$,

$$\sum_{x \in G} \psi(x) = \begin{cases} 0 \text{ if } \psi \neq \mathbf{1}, \\ |G| \text{ else.} \end{cases}$$

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).***

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

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

Proof : We notice that $\psi(x)\overline{\chi(x)} = \left(\psi\chi^{-1}\right)(x)$ 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 :

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

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

$$\psi(x) = \exp\left(\frac{i2\pi}{p} \operatorname{Tr}_{\mathbb{F}_t/\mathbb{F}_p}(x)\right)$$

define a non trivial additive character on $\mathbb{F}_t$, and that all others additive characters are given by $\psi_a(x) = \psi(ax)$ where $a \in \mathbb{F}_t$.

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 Pubblishing Company, 1983.