ResearchGate

See discussions, stats, and author profiles for this publication at:
https://www.researchgate.net/publication/238849763

Two codes related to hermitian forms

Article *in* Journal of Pure and Applied Algebra · April 2003

DOI: 10.1016/S0022-4049(02)00194-9

CITATIONS
2

READS
9

1 author:

Dany-Jack Mercier
Université des Antilles

27 PUBLICATIONS **30** CITATIONS

SEE PROFILE

All in-text references underlined in blue are linked to publications on ResearchGate, letting you access and read them immediately.

Available from: Dany-Jack Mercier
Retrieved on: 15 October 2016

ELSEVIER

Journal of Pure and Applied Algebra 179 (2003) 273–285

JOURNAL OF PURE AND APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

Two codes related to hermitian forms

Dany-Jack Mercier

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

Received 28 January 2000
Communicated by M.-F. Roy

Abstract

Hermitian forms, exponential sums and linear algebra give us the opportunity to construct two trace-codes and obtain their parameters.
© 2003 Elsevier Science B.V. All rights reserved.

MSC: Primary: 11T71; secondary: 94B60; 11E04

1. Introduction and preliminaries

Let $\mathbb{F}_t$ denote the finite field with t elements and characteristic p. The classical hermitian form theory on $\mathbb{C}$ can be written on $\mathbb{F}_{t^2}$ with the involution $x \mapsto x^t$ in $\mathbb{F}_{t^2}$ instead of the application $z \mapsto \bar{z}$. Then we can define quadratic hermitian forms on $\mathbb{F}_{t^2}^N$ and on $\mathbb{F}_t^{2N}$ and construct two linear codes using the same method as Reed–Muller codes. The aim of this paper is to define two codes, to compute their parameters (Theorems 4 and 5) and to compare them to the classical Reed–Muller one.

A rather complete introduction to hermitian forms over a finite field can be found in [1], and the use of those objects in coding Theory has been discussed in [2,3] or [4].

If α denotes an element in $\mathbb{F}_{t^2}$ such that $\mathbb{F}_{t^2} = \mathbb{F}_t(\alpha)$, each element x of $\mathbb{F}_{t^2}$ is uniquely written as $x = a + b\alpha$ with $(a, b) \in \mathbb{F}_t^2$. We say that $\bar{x} = x^t = a + b\alpha^t$ is the conjugate of x. A matrix $A = (a_{ij})_{i,j}$ with entries a_{ij} in $\mathbb{F}_{t^2}$ is said to be hermitian if it satisfies $\bar{a}_{ji} = a_{ij}$ for all i, j. Let N be an integer $\geqslant 1$. A *sesquilinear form on* $E := \mathbb{F}_{t^2}^N$ is a function $H : \mathbb{F}_{t^2}^N \times \mathbb{F}_{t^2}^N \to \mathbb{F}_{t^2}$ semi-linear in the first variable and linear in the second variable. We know that H is called *hermitian* if it satisfies $H(x, y) = H(y, x)^t$ for all vectors x, y, and that a *hermitian form* is a sesquilinear hermitian form. We will denote by

E-mail address: dany-jack.mercier@univ-ag.fr (D.-J. Mercier).

0022-4049/03/$ - see front matter © 2003 Elsevier Science B.V. All rights reserved.
PII: S0022-4049(02)00194-9

$\mathrm{H}(\mathbb{F}_{t^2}^N)$ the vector space of hermitian forms on $\mathbb{F}_{t^2}^N$. If $x \in E$ and if H is a hermitian form, we can define the semi-linear map

$$\tilde{H} : E \to E^*$$

$$x \mapsto H(x, .),$$

where E^* denotes the dual of E. The map $\tilde{H}$ becomes linear with the external law $\bullet$ defined by $\lambda \bullet l = \bar{\lambda}.l$. We recall that the *kernel* $\operatorname{Ker} H$ (resp. *rank* $\operatorname{rk} H$) of H is the *kernel* (resp. *rank*) of the linear map $\tilde{H}$. The *matrix of* H in a basis $e = (e_1, \ldots, e_N)$ of E is $M := (H(e_i, e_j))_{i,j}$ and satisfies $H(x, y) = X^* M Y$ where $X := {}^{\mathrm{T}}(x_1, \ldots, x_N)$ and $Y := {}^{\mathrm{T}}(y_1, \ldots, y_N)$ are the co-ordinates of x and y in e. We know that M is also the matrix of $\tilde{H}$ in the basis e and its dual basis e^*, and we will write $M = \operatorname{Mat}(H; e)$.

Let us introduce the orthogonality with respect to H in a usual way. The main result concerning H-orthogonality is the existence of H-orthogonal basis ([1, Theorem 4.1, p. 1165]): If t is odd, we can find a H-orthogonal basis $e = (e_1, \ldots, e_N)$, and assume $H(e_i, e_i) = 0$ or 1 for all i. Moreover the number r of non zero entries in the diagonal of Mat $(H; e)$ is an invariant that depends only on H. The number r is the *rank* of H, and the last result means that we can always assume that H is given in the standard form $H(x, y) = x_1^t y_1 + \cdots + x_r^t y_r$ in some basis.

The map $q : E \to \mathbb{F}_t$ defined by $q(x) = H(x, x)$ is called the *quadratic hermitian form* on E associated to H, and we write $\mathrm{QH}(\mathbb{F}_{t^2}^N)$ for the space of all quadratic hermitian form on E. If $q \in \mathrm{QH}(\mathbb{F}_{t^2}^N)$, there exists a unique hermitian form H such that $\Psi(H) = q$, and it is called the *polar form* of q. The *kernel* and the *rank* of q will be those of the associated polar form H. In a H-orthogonal basis of E we certainly get $q(x) = \sum_{i=1}^r x_i^{t+1}$.

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

From now on, t is odd, $H : \mathbb{F}_{t^2}^N \times \mathbb{F}_{t^2}^N \to \mathbb{F}_{t^2}$ denotes a sesquilinear form, and $\mathbb{F}_{t^2} = \mathbb{F}_t(\alpha)$. The map $\imath : \mathbb{F}_t^{2N} \to \mathbb{F}_{t^2}^N$ defined by $\imath(x_1, \ldots, x_{2N}) = (x_1 + \alpha x_2, \ldots, x_{2N-1} + \alpha x_{2N})$ is an $\mathbb{F}_t$- vector space isomorphism. The map $\mathbb{F}_t^{2N} \times \mathbb{F}_t^{2N} \to \mathbb{F}_{t^2}; (x, y) \mapsto H(\imath x, \imath y)$ will be $\mathbb{F}_t$- linear but with values in $\mathbb{F}_{t^2}$. As we want to work with functions with values in $\mathbb{F}_t$, it is convenient to define the *quadratic hermitian form* f *on* $\mathbb{F}_t^{2N}$ *associated with* H by

$$f : \mathbb{F}_t^{2N} \to \mathbb{F}_t$$

$$x \mapsto H(\imath x, \imath x).$$

If $\mathrm{QH}(\mathbb{F}_t^{2N})$ denotes the vector space of all quadratic hermitian forms on $\mathbb{F}_t^{2N}$, the function

$$\mathrm{QH}(\mathbb{F}_{t^2}^N) \to \mathrm{QH}(\mathbb{F}_t^{2N})$$

$$q(x) = H(x, x) \mapsto f(x) := H(\imath x, \imath x)$$

will be a $\mathbb{F}_t$-isomorphism. From this point of view, a hermitian form H, a quadratic hermitian form q on $\mathbb{F}_{t^2}^N$ and a quadratic hermitian form f on $\mathbb{F}_t^{2N}$ are all the same.

Proposition 1. *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*

$$B : \mathbb{F}_t^{2N} \times \mathbb{F}_t^{2N} \to \mathbb{F}_t$$

$$(x, y) \mapsto f(x + y) - f(x) - f(y).$$

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

Proof. In a H-orthogonal basis of $\mathbb{F}_{t^2}^N$, we get $q(x) = \sum_{i=1}^r x_i^{t+1}$ for all $x \in E$, thus

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

with $x = (u_1, v_1, \ldots, u_N, v_N) \in \mathbb{F}_t^{2N}$ and $\alpha^{t+1} \in \mathbb{F}_t$. It follows that $f(x)$ is an homogeneous polynomial of degree 2 in the coordinates of x and with coefficients in $\mathbb{F}_t$, i.e. a $\mathbb{F}_t$ -quadratic form. Then it is easy to check that $f(x + y) = f(x) + f(y) + H(\imath x, \imath y) + H(\imath x, \imath y)^t$. □

The kernel of B is

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

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

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

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

Proposition 2. (1) *We have* $\imath(\mathrm{Ker}\, B) = \mathrm{Ker}\, H$. *Thus* $\imath$ *induces a* $\mathbb{F}_t$*-isomorphism from* $\mathrm{Ker}\, B$ *onto* $\mathrm{Ker}\, H$ *and* $\mathrm{rk}\, f = \mathrm{rk}\, B = 2\,\mathrm{rk}\, H$.

(2) *There is an endomorphism T of $\mathbb{F}_t^{2N}$ with $B(x, y) = T(x).y$ for all $(x, y) \in \mathbb{F}_t^{2N} \times \mathbb{F}_t^{2N}$.*

(3) *We have* $\mathrm{Ker}\, T = \mathrm{Ker}\, B$, $\mathrm{Im}\, T = (\mathrm{Ker}\, B)^\perp$ *and* $\mathrm{Ker}\, T \subset f^{-1}(0)$.

Proof. (1) Let ψ denote a non trivial additive character on $\mathbb{F}_t$. The map $\psi' = \psi \circ \mathrm{Tr}_{\mathbb{F}_{t^2}/\mathbb{F}_t}$ is a non trivial additive character on $\mathbb{F}_{t^2}$ and Lemma 1 gives:

$$(x \in \mathrm{Ker}\, B) \Leftrightarrow \forall y \in \mathbb{F}_t^{2N} \quad B(x, y) = \mathrm{Tr}_{\mathbb{F}_{t^2}/\mathbb{F}_t}(H(\imath x, \imath y)) = 0$$

$$\Leftrightarrow \sum_{y \in \mathbb{F}_t^{2N}} \psi(\mathrm{Tr}_{\mathbb{F}_{t^2}/\mathbb{F}_t}(H(\imath x, \imath y))) \neq 0$$

$$\Leftrightarrow \sum_{z \in \mathbb{F}_{t^2}^N} \psi(\mathrm{Tr}_{\mathbb{F}_{t^2}/\mathbb{F}_t}(H(\imath x, z))) \neq 0$$

$$\Leftrightarrow \sum_{z \in \mathbb{F}_{t^2}^N} \psi'(H(\imath x, z)) \neq 0$$

$$\Leftrightarrow \forall z \in \mathbb{F}_{t^2}^N \ H(\imath x, z) = 0 \ \Leftrightarrow \ \imath x \in \mathrm{Ker}\, H.$$

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

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

(2) 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 $T(\lambda x + x') - \lambda T(x) - T(x') = 0$ and the linearity of T follows.

(3) The first equality is a consequence of

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

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

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

If $x \in \operatorname{Ker} T = \operatorname{Ker} B$ then $f(x) = H(\imath x, \imath x) = 0$ from 1, hence $\operatorname{Ker} T \subset f^{-1}(0)$. □

3. Exponential sums S(*f*, *v*)

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

$$\psi(x) = \exp\left(\frac{\mathrm{i}2\pi}{p} \operatorname{Tr}_{\mathbb{F}_t/\mathbb{F}_p}(x)\right).$$

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

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

Lemma 1. *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 ([6, Theorem 5.4, p. 188]). □

Lemma 2.

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

Proof. The norm $\mathrm{N}_{\mathbb{F}_{t^m}/\mathbb{F}_t}: \mathbb{F}_{t^m}^* \to \mathbb{F}_t^*$ is a multiplicative group epimorphism and that $|\mathrm{N}^{-1}_{\mathbb{F}_{t^m}/\mathbb{F}_t}(b)| = (t^m-1)/(t-1)$ for all $b\in\mathbb{F}_t^*$. Hence

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

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

We are now ready to give another proof of the main result in [2]. In fact, a small mistake occurred in Proposition 3 of [2] 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.

Theorem 1 (Cherdieu [3, Theorem 2 and Proposition 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*

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

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 $f(x) = H(y,y) = q(y) = y_1^{t+1}+\cdots+y_\rho^{t+1}$ where $y=\imath(x)\in\mathbb{F}_{t^2}^N$.

(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 $z=\imath u$. Then

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

and

$$S(f,v)=\sum_{y_1,\dots,y_N\in\mathbb{F}_{t^2}}\prod_{k=1}^{\rho}\psi((z_k+y_k)^{t+1}-z_k^{t+1})$$

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

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

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

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

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

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

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

$$S(f,v)=(-1)^\rho t^{2N-\rho}\prod_{k=1}^{\rho}\psi(-z_k^{t+1})=(-1)^\rho t^{2N-\rho}\psi(-z_1^{t+1}-\cdots-z_\rho^{t+1})$$

$$=(-1)^\rho t^{2N-\rho}\psi(-q(z)).$$

Since $q(z)=H(u,u)=f(u)$, 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 $v=T_au_a$ 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 $v=T_au_a=aT(u_a)=T(au_a)$, and we can take $u=au_a$. This gives $S(af,v)=(-1)^\rho t^{2N-\rho}\psi(-af(a^{-1}u))=(-1)^\rho t^{2N-\rho}\psi(-a^{-1}f(u))$.

(γ) By the above

$$\sum_{a\in\mathbb{F}_s^*}S(af,v)=(-1)^\rho t^{2N-\rho}\sum_{a\in\mathbb{F}_s^*}\psi(-a^{-1}f(u))$$

$$=(-1)^\rho t^{2N-\rho}\sum_{a\in\mathbb{F}_s^*}\psi'(-a^{-1}\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u))),$$

where ψ' is the additive character $\psi'(x)=\exp((\mathrm{i}2\pi/p)\,\mathrm{Tr}_{\mathbb{F}_s/\mathbb{F}_p}(x))$ on $\mathbb{F}_s$. Since the map $z\mapsto\psi'(cz)$ describes the set of additive characters on $\mathbb{F}_s$ when c describes $\mathbb{F}_s$, the

orthogonality relation yields

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

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

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

Since $v\notin(\mathrm{Ker}\, B)^\perp$, 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 1 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 1 depends whether $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u))=0$ or not. It has a meaning if we check that $v=T(u)=T(u')$ and $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u))=0$ imply $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u'))=0$. Let $v=T(u)=T(u')$. Then $u-u' := w\in\mathrm{Ker}\, T$ and $B(w,u')=f(u)-f(w)-f(u')$. From $B(w,u')=T(w).u'=0$ and $f(w)=\frac{1}{2}B(w,w)=\frac{1}{2}T(w).w=0$ if follows that $f(u)=f(u')$, which gives the desired conclusion.

4. Number of solutions of two trace equations

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

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

Proof. Let us introduce the additive character $\psi'(x) = \exp((\mathrm{i}2\pi/p)\,\mathrm{Tr}_{\mathbb{F}_s/\mathbb{F}_p}(x))$ on $\mathbb{F}_s$. Then (see remark below Theorem 5.5 in [6]):

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

Since

$$\begin{aligned}\psi'(c\,\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)+v.x)) &= \exp\left(\frac{\mathrm{i}2\pi}{p}\,\mathrm{Tr}_{\mathbb{F}_s/\mathbb{F}_p}(c\,\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)+v.x))\right)\\ &= \exp\left(\frac{\mathrm{i}2\pi}{p}\,\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_p}(cf(x)+cv.x)\right)\\ &= \psi(cf(x)+cv.x),\end{aligned}$$

we deduce

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

Now the assertion follows from Theorem 1. □

Theorem 3 (Cherdieu et al. [5, Proposition 3]). *Let $a\in\mathbb{F}_s$, ρ be a positive integer with $1\leqslant\rho\leqslant N$, 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*

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

Proof. We can assume that f is given in the standard form $f(x) = H(y,y) = y_1^{t+1} + \cdots + y_\rho^{t+1}$ where $y = \imath(x)\in\mathbb{F}_{t^2}^N$. If $\mathbb{F}_s^\wedge$ denotes the set of additive characters on $\mathbb{F}_s$, then (see remark below Theorem 5.5 in [6])

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

Hence

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

We have

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

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

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

Therefore

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

and the usual orthogonality relation establishes the formula. □

Remark. Theorem 3 follows from Theorem 2 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 $\mathbb{F}_t^{2N}$.

5. The code Γ

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

$$\gamma:\ \mathrm{QH}(\mathbb{F}_t^{2N}) \times \mathbb{F}_t^{2N} \to \mathbb{F}_s^{t^{2N}}$$
$$(f,v) \mapsto (\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)+v.x))_{x\in\mathbb{F}_t^{2N}}$$

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

Theorem 4. *The weights* $\mathrm{w}(\gamma(f,v))$ *of the non null code-word* $\gamma(f,v)$ *of the code* Γ *satisfy*:

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

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

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

$$r(\Gamma) = \frac{(s-1)(t+1)}{st-t-1}.$$

Proof. The length of Γ is $N_\Gamma = t^{2N}$. If follows immediately from Theorem 2 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

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

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 2:

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

We consider several cases:

1. If $v=0$, then $f \neq 0$, and
   1.1. If ρ is even, then $2 \leqslant \rho \leqslant 2[N/2]$ and
   $$\frac{1}{s}(t^{2N} + (s-1)t^{2N-2[N/2]}) \leqslant \mathrm{M}(f,0) \leqslant \frac{1}{s}(t^{2N} + (s-1)t^{2N-2}). \tag{1}$$
   1.2. If ρ is odd, then $1 \leqslant \rho \leqslant 2[(N-1)/2]+1$ and
   $$\frac{1}{s}(t^{2N} - (s-1)t^{2N-2}) \leqslant \mathrm{M}(f,0) \leqslant \frac{1}{s}(t^{2N} - (s-1)t^{2N-2[N/2]}). \tag{2}$$
2. If $v \neq 0$,
   2.1. If ρ is even and $v \in (\mathrm{Ker}\, B)^\perp$, then $\rho \neq 0$. We get
   $$2 \leqslant \rho \leqslant 2\left[\frac{N}{2}\right] \text{ et } \mathrm{M}(f,v) = \frac{1}{s}(t^{2N} + A(s,v)t^{2N-\rho}).$$
   We can find a vector u such that $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u)) \neq 0$ (indeed $f(u) = y_1^{t+1} + \cdots + y_\rho^{t+1}$ in a convenient basis, and the map $y \mapsto \mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(y^{t+1})$ is surjective since $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}$ 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 $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u)) = 0$, then $\mathrm{M}(f,v) = 1/s(t^{2N} + (s-1)t^{2N-\rho})$ and
   $$\frac{1}{s}(t^{2N} + (s-1)t^{2N-2[N/2]}) \leqslant \mathrm{M}(f,v) \leqslant \frac{1}{s}(t^{2N} + (s-1)t^{2N-2}). \tag{3}$$
   2.1.2. If $v = T(u)$ with $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u)) \neq 0$, then $\mathrm{M}(f,v) = 1/s(t^{2N} - t^{2N-\rho})$ and
   $$\frac{1}{s}(t^{2N} - t^{2N-2}) \leqslant \mathrm{M}(f,v) \leqslant \frac{1}{s}(t^{2N} - t^{2N-2[N/2]}). \tag{4}$$
   2.2. If ρ is even and $v \notin (\mathrm{Ker}\, B)^\perp$, then $\mathrm{M}(f,v) = t^{2N}/s$ belongs to one of the intervals defined by (3) or (4).
   2.3. If ρ is odd and $v \in (\mathrm{Ker}\, B)^\perp$, then $\mathrm{M}(f,v) = 1/s(t^{2N} - A(s,v)t^{2N-\rho})$.
   2.3.1. If $v = T(u)$ with $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u)) = 0$, then $\mathrm{M}(f,v) = 1/s(t^{2N} - (s-1)t^{2N-\rho})$ and
   $$\frac{1}{s}(t^{2N} - (s-1)t^{2N-1}) \leqslant \mathrm{M}(f,v) \leqslant \frac{1}{s}(t^{2N} - (s-1)t^{2N-2[(N-1)/2]-1}). \tag{5}$$

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

$$\frac{1}{s}(t^{2N} + t^{2N-2[(N-1)/2]-1}) \leqslant \mathrm{M}(f,v) \leqslant \frac{1}{s}(t^{2N} + t^{2N-1}). \tag{6}$$

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

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

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

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

6. The code C

The parameters of the code Γ in Section 5 are computed from Theorem 2. We can apply the same construction to use Theorem 3. The image of the linear map

$$c\colon \mathrm{QH}(\mathbb{F}_t^{2N}) \times \mathbb{F}_s \to \mathbb{F}_s^{t^{2N}}$$

$$(f,a) \mapsto (\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)) - a)_{x \in \mathbb{F}_t^{2N}}$$

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 $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)) = a$ for all $x \in \mathbb{F}_t^{2N}$, and if ρ denotes the rank of f, then $f(x) = y_1^{t+1} + \cdots + y_\rho^{t+1}$ where $y = \imath x$ and $1 \leqslant \rho \leqslant N$, and the assumption 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:

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

Theorem 5. *The weights* $\mathrm{w}(c(f,a))$ *of the non null code-words* $c(f,a)$ *in* C *satisfy:*

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

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

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

$$r(C) = \frac{st}{st - t - 1}.$$

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 3.

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

1.1. If ρ is even, then $2 \leqslant \rho \leqslant 2[N/2]$ and

$$\frac{1}{s}(t^{2N} + (s-1)t^{2N-2[N/2]}) \leqslant \mathrm{M}(f,0) \leqslant \frac{1}{s}(t^{2N} + (s-1)t^{2N-2}). \tag{1}$$

1.2. If ρ is odd, then $1 \leqslant \rho \leqslant 2[(N-1)/2] + 1$ and

$$\frac{1}{s}(t^{2N} - (s-1)t^{2N-1}) \leqslant \mathrm{M}(f,0) \leqslant \frac{1}{s}(t^{2N} - (s-1)t^{2N-2[(N-1)/2]-1}). \tag{2}$$

2. If $a \neq 0$,

2.1. If ρ is even,

$$0 \leqslant \mathrm{M}(f,a) \leqslant \frac{1}{s}(t^{2N} - t^{2N-2[N/2]}). \tag{3}$$

2.2. If ρ is odd,

$$\frac{1}{s}(t^{2N} - t^{2N-2[(N-1)/2]-1}) \leqslant \mathrm{M}(f,a) \leqslant \frac{1}{s}(t^{2N} + t^{2N-1}). \tag{4}$$

The bounds (1) to (4) imply

$$\forall (f,a) \in (\mathrm{QH}(\mathbb{F}_t^{2N}) \times \mathbb{F}_s) \setminus \{(0,0)\}$$

$$0 \leqslant \mathrm{M}(f,a) \leqslant \frac{1}{s}(t^{2N} + t^{2N-1}). \qquad \square$$

7. Comparison of Γ and C to Reed–Muller codes

Let C denote a code $[N_C, K_C, D_C]$. The ratio K_C/N_C is called the transmission rate, and the ratio D_C/N_C represents the reliability of C. Note that C can correct $[(D_C-1)/2]$ errors and that

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

is less than $1 + 1/N_C$ and must be as great as possible [5].

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

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

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

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

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

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 sense, C can be compared with $R(2, 2N)$ for large values of t. In the same manner $\lim_{t\to+\infty}((K_R/N_R) - (K_C/N_C)) = 0$ and the transmission rates of C and $R(2, 2N)$ can be compared for large values of t.

References

[1] R.C. Bose, I.M. Chakravarti, Hermitian varieties in a finite projective space PG(N, q^2), Can. J. Math. 18 (1966) 1161–1182.
[2] J.-P. Cherdieu, Exponential sums, codes and hermitian forms, IEEE Trans. Inform. Theory 41 (5), September 1995.
[3] 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.
[4] J.-P. Cherdieu, D.-J. Mercier, T. Narayaninsamy, On the Generalized Weights of a Class of Trace Codes, Finite Fields Appl. 7 (2001) 355–371.
[5] G. Lachaud, S. Vladut, Les codes Correcteurs d'Erreurs, La Recherche, Hors Série no. 2, Août 1999.
[6] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications, Vol. 20, Addison-Wesley Publishing Company, Reading, MA, 1983.