Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Journal of Pure and Applied Algebra 193 (2004) 251–262
JOURNAL OF PURE AND APPLIED ALGEBRA
www.elsevier.com/locate/jpaa

The number of solutions of the equation $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)+v.x)=b$ and some applications

Dany-Jack Mercier [a,b,*]

[a] *IUFM de Guadeloupe, Morne Ferret, BP399, Pointe-à-Pitre Cedex 97159, France*
[b] *Laboratoire Analyse, Optimisation, Contrôle de l'Université des Antilles-Guyane, France*

Received 6 March 2003; received in revised form 30 January 2004
Communicated by M.-F. Roy

Abstract

We compute the number of solutions of the equation $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)+v.x)=b$ in $\mathbb{F}_t^{2N}$, where f denote a quadratic hermitian form on $\mathbb{F}_t^{2N}$, $v\in\mathbb{F}_t^{2N}$ and $b\in\mathbb{F}_s$, and we deduce the number of hermitian matrices of order N and rank ρ. This number is well-known since the paper of Carlitz and Hodges (Duke Math. J. 22 (1995) 393), but with a more restrictive definition of hermitian matrices and with a rather different proof. Next, we introduce a linear code $\Gamma(N,t,s)$ on $\mathbb{F}_s$ constructed with the same method as Reed–Muller one, and compute its weight distribution. $\Gamma(N,t,s)$ is a generalization of the two codes Γ and C studied in Mercier (J. Pure Appl. Algebra 173 (3) (2003) 273) and the method for obtaining its weight distribution is new and more straightforward. Tools are exponential sums and linear algebra on $\mathbb{F}_t$.

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

1. Introduction

Let $\mathbb{F}_t$ be the finite field with t elements and characteristic p. Let α denote an element in $\mathbb{F}_{t^2}$ such that $\mathbb{F}_{t^2}=\mathbb{F}_t(\alpha)$. Then each element x of $\mathbb{F}_{t^2}$ is uniquely written as $x=a+b\alpha$ with $(a,b)\in\mathbb{F}_t^2$, and we say that $\bar{x}=x^t=a+b\alpha^t$ is the conjugate of x. We say that a matrix $A=(a_{ij})_{i,j}$ with entries a_{ij} in $\mathbb{F}_{t^2}$ is hermitian if it satisfies $\bar{a}_{ji}=a_{ij}$ for all i, j. Hermitian matrices with entries in $\mathbb{F}_{t^2}$, quadratic hermitian forms on $\mathbb{F}_t^{2N}$ and the properties that we shall need are stated in Section 2.

* Corresponding author. IUFM de Guadeloupe, Morne Ferret, BP399, Pointe-à-Pitre Cedex 97159, France.
E-mail address: dany-jack.mercier@univ-ag.fr (D.-J. Mercier).

0022-4049/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.jpaa.2004.02.007

Let f denote a quadratic hermitian form on $\mathbb{F}_t^{2N}$, and $v \in \mathbb{F}_t^{2N}$. Let ψ denote a non-trivial additive character on $\mathbb{F}_t$. The value of the exponential sum $S(f,v) = \sum_{x \in \mathbb{F}_t^{2N}} \psi(f(x) + v.x)$ is well-known (see [4, Proposition 2] or [10, Theorem 1]), and allow us to deduce the number of solutions of the equation $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x) + v.x) = b$ in $\mathbb{F}_t^{2N}$ (Theorem 6). This last result was only known when $b = 0$ [4, Proposition 4] or $v = 0$ [6, Proposition 3]. Then it follows easily that $f(x)$ in $\mathbb{F}_t[x_1, \ldots, x_{2N}]$ is a κ-polynomial in $\mathbb{F}_s[x_1, \ldots, x_{2N}]$ with the terminology of [11], and that the number $M(b)$ of solutions $x = (x_1, \ldots, x_N)$ in $\mathbb{F}_{t^2}^N$ of the equation $x_1^{t+1} + \cdots + x_\rho^{t+1} = b$ is

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

The two last sections give two applications of Theorem 6.

In Section 4, we compute the number of unitary matrices and deduce the number $|H(N,\rho)|$ of hermitian matrices of order N and rank ρ for our involutory automorphism $\bar{x} = x^t$. This number was already computed by Carlitz and Hodges in [3], using results about the number of solutions of quadratic diagonal equations like $\sum_{i=1}^m (\alpha_i^2 - v\beta_i^2) = 1$, but with a more restrictive definition of hermitian matrices using $\alpha \in \mathbb{F}_{t^2}$ with $\alpha^2 = v \in \mathbb{F}_t$ but $\alpha \notin \mathbb{F}_t$, and introducing the involutory automorphism $x \mapsto \bar{x}$ defined by $\bar{x} = a - b\alpha$ as soon as $x = a + b\alpha$ and $(a,b) \in \mathbb{F}_t^2$.

In fact, the definition of Carlitz and Hodges with $\bar{x} = a - b\alpha$ is only a special case of our definition with $\bar{x} = a + b\alpha^t$, as it is easily seen that $\alpha^2 \in \mathbb{F}_t$ and $\alpha \notin \mathbb{F}_t$ imply $\alpha^t = -\alpha$ (indeed, $\alpha^{2t} = \alpha^2$ gives $\alpha^{2(t-1)} = 1$ thus $\alpha^{t-1} = -1$ as we know that $\alpha^{t-1} = 1$ is impossible), and that we can find $\alpha \in \mathbb{F}_{t^2} \setminus \mathbb{F}_t$ such that $\mathbb{F}_{t^2} = \mathbb{F}_t(\alpha)$ and $\alpha^t \neq -\alpha$ (otherwise the polynomial $x^t + x$ of degree t would have $t^2 - t$ distinct roots).

The two important points to note here are that we work with the conjugate $\bar{x} = a + b\alpha^t$, and only use the number $M(b)$ of solutions of the equation $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)) = b$ provided by Theorem 6 (without the help of well-known theorems about the number of solutions of diagonal equations, for instance in [7, Chapter 6]). Therefore we give an alternate proof for computing $|H(N,\rho)|$.

Last section is devoted to the study of a linear code $\Gamma(N,t,s)$ on $\mathbb{F}_s$ defined by the codewords $(\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x) + v.x) + a)_{x \in \mathbb{F}_t^{2N}}$. Theorem 6 enables us to compute its parameters and its weight distribution. The code $\Gamma(N,t,s)$ is a generalization of the hermitian form trace code Γ_H defined by the words $(\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x) + v.x))_{x \in \mathbb{F}_t^{2N}}$ and first introduced in [4]. It is also a generalization of some codes introduced in [5] or [10], but the method for obtaining the weight distribution of $\Gamma(N,t,s)$ and its subcodes seems to be more easier and systematic here.

2. Notations and preliminaries

Let us recall some definitions from [1,6]. Let N be an integer $\geqslant 1$ and let E be the vector space $\mathbb{F}_{t^2}^N$. 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. H is called *hermitian*

if $H(x,y)=H(y,x)^t$ for all vectors x,y. A sesquilinear hermitian form is called a *hermitian form*, and the vector space of hermitian forms on $\mathbb{F}_{t^2}^N$ is denoted by $\mathrm{H}(\mathbb{F}_{t^2}^N)$.

A square matrix $A=(a_{ij})_{i,j}$ $(i,j=1,\dots,N)$ with entries in $\mathbb{F}_{t^2}$ is *hermitian* if $A^*=A$, where A^* denotes the matrix ${}^{\mathrm{T}}(\bar{A}):=(b_{ij})_{i,j}$ with $b_{ij}=a_{ji}^t$ (the transpose of the conjugate of A). If $e=(e_1,\dots,e_N)$ is a basis of E, and if H is a sesquilinear form on E, $M:=(H(e_i,e_j))_{i,j}$ is a matrix that satisfies $H(x,y)=X^*MY$ where $X:={}^{\mathrm{T}}(x_1,\dots,x_N)$ and $Y:={}^{\mathrm{T}}(y_1,\dots,y_N)$ denote the coordinates of x and y in e. We say that M is *the matrix of H in e*, and write $M=\mathrm{Mat}(H;e)$. It is a simple matter to check that H is hermitian if and only if $\mathrm{Mat}(H;e)$ is hermitian, and that $\dim_{\mathbb{F}_t} H(\mathbb{F}_{t^2}^N)=N^2$.

If $x\in E$ and if H is a hermitian form, the map $H(x,.):E\to\mathbb{F}_{t^2};\ y\mapsto H(x,y)$ is linear and allows us to introduce the semi-linear map

$$\widetilde{H}:E\to E^*,$$

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

where E^* is the dual of E. In fact, $\widetilde{H}$ becomes linear for the extern law $\bullet$ defined by $\lambda\bullet l=\bar{\lambda}.l$. With this extern law, the matrix of $\widetilde{H}$ in the basis e in E and the dual basis e^* in E^* satisfies $\mathrm{Mat}(\widetilde{H};e,e^*)=\mathrm{Mat}(H;e)$. We say that the *kernel* $\mathrm{Ker}\ H$ (resp. *rank* $\mathrm{rk}\ H$) of H is the *kernel* (resp. *rank*) of $\widetilde{H}$. Thus $\mathrm{rk}\ H=\mathrm{rk}(\mathrm{Mat}(H;e))$.

Orthogonality with respect to H is defined in a usual way, and we have:

Theorem 1 (Bose and Chakravarti [1, Theorem 4.1, p. 1165], Existence of H-orthogonal basis). *If t is odd and if H is a hermitian form on $E=\mathbb{F}_{t^2}^N$, then we can find a H-orthogonal basis $e=(e_1,\dots,e_N)$, and assume $H(e_i,e_i)=0$ or 1 for all i. Moreover the number r of nonzero entries in the diagonal of* $\mathrm{Mat}(H;e)$ *is an invariant that depends only on H.*

The number r in the previous Theorem is the rank of H. A hermitian form H is *nondegenerate* if $E^\perp=\{0\}$, and this means that $\widetilde{H}$ is an isomorphism from E to E^*, or that $\mathrm{Mat}(H;e)$ is nonsingular. If H is nondegenerate, then $\dim F+\dim F^\perp=n$ and $F=(F^\perp)^\perp$ for all subspaces F, but we have no reason to say that the sum $E=F+F^\perp$ is direct. As usual, we say that a subspace F of E is *isotropic* if $F\cap F^\perp\neq\{0\}$, and that a vector x is *isotropic* if $H(x,x)=0$. Next Theorem is well-known:

Theorem 2 (Mercier [9], Theorem 7). *The following conditions are equivalent*:

(i) *The restriction $H|_{F\times F}$ of H to F is nondegenerate*,
(ii) *F is nonisotropic*,
(iii) $E=F\oplus F^\perp$.

If H denotes a hermitian form, 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. Let $\mathrm{QH}(\mathbb{F}_{t^2}^N)$ be the space of all quadratic hermitian form on E. We have $H(\mathbb{F}_{t^2}^N)\simeq\mathrm{QH}(\mathbb{F}_{t^2}^N)$, thus $\dim_{\mathbb{F}_t}\mathrm{QH}(\mathbb{F}_{t^2}^N)=N^2$. If $q\in\mathrm{QH}(\mathbb{F}_{t^2}^N)$, the unique hermitian form H satisfying $\Psi(H)=q$ is called the *polar form* of q. By definition the *kernel* and the *rank* of q will be those of the associated

polar form H. If $M=(a_{ij})$ denotes the matrix of H in a basis of E, then $q(x)=H(x,x)=\sum_{i,j} a_{ij}\bar{x}_i x_j$ for all $x\in E$. In a H-orthogonal basis we only get $q(x)=\sum_{i=1}^{r} x_i^{t+1}$.

From now on, t is odd, $H:\mathbb{F}_{t^2}^N\times\mathbb{F}_{t^2}^N\to\mathbb{F}_{t^2}$ is a sesquilinear form, and $\alpha\in\mathbb{F}_{t^2}$ satisfies $\mathbb{F}_{t^2}=\mathbb{F}_t(\alpha)$. 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. We say that the map

$$f:\mathbb{F}_t^{2N}\to\mathbb{F}_t,$$
$$x\mapsto H(\imath x,\imath x).$$

is the *quadratic hermitian form f on $\mathbb{F}_t^{2N}$ associated with H*. Let $\mathrm{QH}(\mathbb{F}_t^{2N})$ denote the space of quadratic hermitian forms on $\mathbb{F}_t^{2N}$. One can check that the map

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

where $f(x)=H(\imath x,\imath x)$ when $q(x)=H(x,x)$, is an isomorphism between $\mathbb{F}_t$-vector spaces, and deduce $\dim_{\mathbb{F}_t}\mathrm{QH}(\mathbb{F}_t^{2N})=N^2$. We refer to [10] for the two next results:

Theorem 3 (Cherdieu [4, Theorem 1] or Mercier [10, 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 $B(x,y)=H(\imath x,\imath y)+H(\imath x,\imath y)^t=\mathrm{Tr}_{\mathbb{F}_{t^2}/\mathbb{F}_t}(H(\imath x,\imath y))$.

We shall say that B is also a bilinear form associated with f.

Remark. If $t=2^\zeta$ the map B defined in Theorem 3 can never be the bilinear form associated with f because $B(x,x)=f(2x)-2f(x)=0$ (for more details we refer the reader to [6]).

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

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

Theorem 4 (Mercier [10, 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* $\mathbb{F}_t^{2N}$ *such that* $B(x,y)=T(x).y$ *for all* $(x,y)\in \mathbb{F}_t^{2N}\times\mathbb{F}_t^{2N}$. *We have* $\operatorname{Ker} T=\operatorname{Ker} B$, $\operatorname{Im} T=(\operatorname{Ker} B)^{\perp}$ *and* $\operatorname{Ker} T\subset f^{-1}(0)$.

3. A trace equation

Following Cherdieu [4], we define the exponential sum associated to f and $v\in\mathbb{F}_t^{2N}$ by

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

where ψ denotes the additive character on $\mathbb{F}_t$ defined by $\psi(x)=\exp((\mathrm{i}2\pi/p)\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_p}(x))$. We recall the main result of Cherdieu ([4, Theorem 2 and Proposition 3i] or [10, Theorem 1]):

Theorem 5. *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* $v\in(\operatorname{Ker} B)^{\perp}=\operatorname{Im} T$, *we can find* $u\in\mathbb{F}_t^{2N}$ *such that* $v=T(u)$. *Then*

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

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

An improvement of both Proposition 4 in [4], Proposition 3 in [6] and Theorems 2 and 3 in [10] is given by next theorem.

Theorem 6. *Let* $v\in\mathbb{F}_t^{2N}$ *and* $b\in\mathbb{F}_s$. *Let* ρ *denote a positive integer such that* $1\leqslant\rho\leqslant N$, *and* f *denote a quadratic hermitian form of rank* 2ρ *on* $\mathbb{F}_t^{2N}$. *The number* M *of solutions of the equation* $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)+v.x)=b$ *in* $\mathbb{F}_t^{2N}$ *is*

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

where

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

and where $u\in\mathbb{F}_t^{2N}$ *satisfies* $v=T(u)$.

Proof. Let $b=\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(b')$ where $b'\in\mathbb{F}_t$. The map $\psi'(x)=\exp((\mathrm{i}2\pi/p)\mathrm{Tr}_{\mathbb{F}_s/\mathbb{F}_p}(x))$ is a nontrivial additive character on $\mathbb{F}_s$, and we have (see remark below Theorem 5.5 in [8]):

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

It is easily seen that $\psi'(c\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(z)) = \psi(cz)$, hence

$$sM = \sum_{c\in\mathbb{F}_s}\sum_{x\in\mathbb{F}_t^{2N}} \psi(c(f(x)+v.x-b'))$$

$$= t^{2N} + \sum_{c\in\mathbb{F}_s^*} \psi(-cb') \sum_{x\in\mathbb{F}_t^{2N}} \psi(cf(x)+cv.x).$$

If $c \neq 0$, then

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

thus

$$sM = t^{2N} + \sum_{c\in\mathbb{F}_s^*} \psi(-cb')S(c^{-1}f, v).$$

Theorem 5 shows that $sM = t^{2N}$ when $v \notin \mathrm{Im}\, T$. If $v = T(u) \in \mathrm{Im}\, T$, Theorem 5 yields $S(c^{-1}f, v) = (-1)^\rho t^{2N-\rho}\psi(-cf(u))$, thus

$$sM = t^{2N} + (-1)^\rho t^{2N-\rho} \sum_{c\in\mathbb{F}_s^*} \psi(c(-f(u)-b'))$$

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

Since the elements of the set of additive characters on $\mathbb{F}_s$ are the maps $z \mapsto \psi'(cz)$ where $c \in \mathbb{F}_s$, the theorem will follow from the above formula and the orthogonality relation. □

Remark. The constant $A(s, v)$ in Theorem 6 is well defined and does not depend on the choice of u such that $v = T(u)$. Indeed, if $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u)) = -b$ and $v = T(u) = T(u')$, we get $w := u - u' \in \mathrm{Ker}\, T$. Then $B(w, u') = f(u) - f(w) - f(u')$, with $B(w, u') = T(w).u' = 0$ and $f(w) = \frac{1}{2}B(w, w) = \frac{1}{2}T(w).w = 0$, whence $f(u) = f(u')$ and $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u')) = -b$.

Following [2,11] we say that a polynomial f in $\mathbb{F}_t[x_1, \ldots, x_N]$ is a *κ-polynomial* if the number of solutions of $f(x) = b$ in $\mathbb{F}_t^N$ is $A + \kappa(b)B$, where A and B are integers and

$$\kappa(b) = \begin{cases} t-1 & \text{if } b = 0, \\ -1 & \text{else.} \end{cases}$$

Every map from $\mathbb{F}_t^{2N}$ to $\mathbb{F}_t$ is polynomial, and, from Theorem 6, the equation $f(x) = b$ has only two kinds of numbers of solutions whether $b = 0$ or not. Hence:

Corollary 7. *$f(x)$ is a κ-polynomial in $\mathbb{F}_t[x_1, \ldots, x_{2N}]$.*

If $x=(x_1,\dots,x_N)\in\mathbb{F}_{t^2}^N$ and $x_i=u_i+\alpha v_i$ with $(u_i,v_i)\in\mathbb{F}_t^2$, we have $x=\imath z$ if we write $z=(u_1,v_1,\dots,u_N,v_N)\in\mathbb{F}_t^{2N}$. Then

$$f(z)=q(\imath z)=\sum_{i=1}^{\rho}(u_i+\alpha v_i)^{t+1}=\sum_{i=1}^{\rho}x_i^{t+1}$$

in a H-orthogonal basis of $\mathbb{F}_{t^2}^N$ (1). With $v=0$ and $s=t$, Theorem 6 gives:

Corollary 8. *Let $b\in\mathbb{F}_t$. The number $M(b)$ of solutions $x=(x_1,\dots,x_N)$ in $\mathbb{F}_{t^2}^N$ of the diagonal equation $x_1^{t+1}+\cdots+x_\rho^{t+1}=b$ is*

$$M(b)=\begin{cases}t^{2N-1}+(-1)^\rho(t-1)t^{2N-\rho-1} & if\ \ b=0,\\ t^{2N-1}-(-1)^\rho t^{2N-\rho-1} & else.\end{cases}$$

4. Number of hermitian matrices of order N and rank ρ

Let $\mathrm{GL}(N,\mathbb{F}_{t^2})$ denote the set of nonsingular matrices of order N with entries in $\mathbb{F}_{t^2}$, and $H(N,\rho)$ denote the set of hermitian matrices of order N and rank ρ, with entries in $\mathbb{F}_{t^2}$. We know that $M\in H(N,\rho)$ if and only if $M^*=M$ and M is equivalent to the diagonal matrix $D_\rho:=\mathrm{Diag}(1,\dots,1,0,\dots,0)$ with ρ digits 1. This last assertion means that there exists a matrix P in $\mathrm{GL}(N,\mathbb{F}_{t^2})$ such that $M=P^*D_\rho P$.

The map

$$\Psi:\ \mathrm{GL}(N,\mathbb{F}_{t^2})\to H(N,\rho),$$
$$P\mapsto P^*D_\rho P$$

is onto, and

$$\Psi(P)=\Psi(Q)\Leftrightarrow D_\rho=(QP^{-1})^*D_\rho(QP^{-1})\Leftrightarrow QP^{-1}\in D(N,\rho),$$

where $D(N,\rho):=\{X\in\mathrm{GL}(N,\mathbb{F}_{t^2})/X^*D_\rho X=D_\rho\}$. Therefore, if $|V|$ denotes the cardinal of V,

$$|H(N,\rho)|=\frac{|\mathrm{GL}(N,\mathbb{F}_{t^2})|}{|D(N,\rho)|}. \tag{1}$$

The number $|\mathrm{GL}(N,\mathbb{F}_{t^2})|$ is well known, and we only have to compute $|D(N,\rho)|$. Let

$$X=\begin{pmatrix}A & C\\ B & D\end{pmatrix}$$

denote a square matrix of order N, where A is a square matrix of order ρ. Let I_ρ denote the unit matrix of order ρ. Since

$$X^*D_\rho X=\begin{pmatrix}A^* & B^*\\ C^* & D^*\end{pmatrix}\begin{pmatrix}I_\rho & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}A & C\\ B & D\end{pmatrix}=\begin{pmatrix}A^*A & A^*C\\ C^*A & C^*C\end{pmatrix},$$

it follows that

$$X^*D_\rho X = D_\rho \Leftrightarrow \begin{cases} A^*A = I_\rho, \\ C = 0. \end{cases}$$

A matrix A of order ρ, with entries in $\mathbb{F}_{t^2}$, and such that $A^*A = I_\rho$, is said to be *unitary*, and we shall denote by $U(\rho, \mathbb{F}_{t^2})$ the set of such unitary matrices. Thus

$$U(\rho, \mathbb{F}_{t^2}) = \{A \in \mathrm{GL}(\rho, \mathbb{F}_{t^2}) / A^*A = I_\rho\} = D(\rho, \rho).$$

From above, it follows that $D(N, \rho)$ is the set of all matrices

$$\begin{pmatrix} A & 0 \\ B & D \end{pmatrix}$$

with $A \in U(\rho, \mathbb{F}_{t^2})$, $D \in \mathrm{GL}(N-\rho, \mathbb{F}_{t^2})$, and with no condition on B. Consequently,

$$|D(N, \rho)| = t^{2\rho(N-\rho)} \times |\mathrm{GL}(N-\rho, \mathbb{F}_{t^2})| \times |U(\rho, \mathbb{F}_{t^2})|. \tag{2}$$

Now we need to compute the cardinal $|U(\rho, \mathbb{F}_{t^2})|$. It is easy to check that a square matrix $A = (a_{ij})$ of order ρ is unitary if and only if the image of an orthonormal basis of $\mathbb{F}_{t^2}^\rho$ (for the nondegenerated hermitian form $(x, y) \mapsto (x|y) = x_1^t y_1 + \cdots + x_\rho^t y_\rho$) by A is again an orthonormal basis. Thus

$$A \in U(\rho, \mathbb{F}_{t^2}) \Leftrightarrow \begin{cases} \forall i & a_{1i}^{t+1} + \cdots + a_{\rho i}^{t+1} = 1, \\ \forall i < j & a_{1i}^t a_{1j} + \cdots + a_{\rho i}^t a_{\rho j} = 0 \end{cases}$$

and the number of unitary matrices will be the number of orthonormal basis in $\mathbb{F}_{t^2}^\rho$. Let $E := \mathbb{F}_{t^2}^\rho$. To construct an orthonormal basis in $\mathbb{F}_{t^2}^\rho$, we have only to choose one vector $u_1 = (x_1, \ldots, x_\rho)$ with "norm" 1, i.e. such that $(u_1|u_1) = x_1^{t+1} + \cdots + x_\rho^{t+1} = 1$, and complete u_1 with any orthonormal basis of the orthogonal space $E' = (\mathbb{F}_{t^2} u_1)^\perp$. As u_1 is nonisotropic, we have $E = E' \oplus (\mathbb{F}_{t^2} u_1)$, and E' is nonisotropic from Theorem 2. Therefore, the same theorem shows that the restriction of the "scalar product" $(x|y)$ to E' is nondegenerate, i.e. of rank $\rho - 1$. From Theorem 1 it follows that the number of orthonormal basis of E' with respect to the restriction of the "scalar product" $(x|y)$ is the same as the number of orthonormal basis of E' with respect to the "canonical scalar product" $(x, y) \mapsto (x|y) = x_1^t y_1 + \cdots + x_{\rho-1}^t y_{\rho-1}$, written in an orthonormal basis. If $v(\rho)$ denotes the number of vectors with "norm" 1 in $\mathbb{F}_{t^2}^\rho$, we obtain $|U(\rho, \mathbb{F}_{t^2})| = v(\rho) \times |U(\rho-1, \mathbb{F}_{t^2})|$, hence $|U(\rho, \mathbb{F}_{t^2})| = v(\rho) \times v(\rho-1) \times \cdots \times v(1)$.

By Corollary 8,

$$v(\rho) = |\{x = (x_1, \ldots, x_\rho) \in \mathbb{F}_{t^2}^\rho / x_1^{t+1} + \cdots + x_\rho^{t+1} = 1\}| = t^{\rho-1}(t^\rho - (-1)^\rho)$$

and so

$$|U(\rho, \mathbb{F}_{t^2})| = t^{\rho(\rho-1)/2} \prod_{k=1}^{\rho} (t^k - (-1)^k). \tag{3}$$

It is now a simple matter to use the well-known formula

$$|\mathrm{GL}(N,\mathbb{F}_{t^2})| = \prod_{k=0}^{N-1} (t^{2N} - t^{2k})$$

together with (1)–(3) to get:

Theorem 9. *The number of hermitian matrices of order N and rank ρ with entries in $\mathbb{F}_{t^2}$ is*

$$|H(N,\rho)| = t^{\rho(\rho-1)/2} \prod_{k=1}^{\rho} \frac{t^{2N-2(k-1)} - 1}{t^k - (-1)^k}.$$

Remark. As N^2 is the dimension of the $\mathbb{F}_t$-space $H(N)$ of hermitian matrices of order N and entries in $\mathbb{F}_{t^2}$, we have $|H(N)| = t^{N^2}$ and we can check that $\sum_{\rho=0}^{N} |H(N,\rho)| = t^{N^2}$.

5. The code $\Gamma(N, t, s)$ and its weight distribution

The image $\Gamma(N,t,s)$ (or Γ to shorten notation) of the linear map

$$\gamma : \mathrm{QH}(\mathbb{F}_t^{2N}) \times \mathbb{F}_t^{2N} \times \mathbb{F}_s \to \mathbb{F}_s^{t^{2N}},$$

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

defines a linear code on $\mathbb{F}_s$ of length $N_\Gamma = t^{2N}$. From now on, $M(f,v,a)$ denotes the number of solutions of the equation $\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x) + v.x) + a = 0$ in $\mathbb{F}_t^{2N}$.

Lemma 10. *$M(f,v,a) = t^{2N}$ if and only if $(f,v,a) = (0,0,0)$.*

Proof. $M(f,v,a)$ is provided by Theorem 6 and takes only three values.

- If $M = (1/s)(t^{2N} + (-1)^\rho A(s,v) t^{2N-\rho})$, then

  $$M = t^{2N} \Leftrightarrow (-1)^\rho A(s,v) t^{2N-\rho} = (s-1)t^{2N}.$$

  If $A(s,v) = s-1$ then $\rho = 0$. If $A(s,v) = -1$, then ρ must be odd and satisfy $1 = (s-1)t^\rho$, hence $\rho = 0$. It follows that $\rho = 0$ and $f = 0$ in both cases. Finally $T = 0$ and $v \in \mathrm{Im}\, T$ give $v = 0$, and $a = 0$.
- If $M = t^{2N}/s$, then $M = t^{2N}$ if and only if $s = 1$, which is impossible. □

The Lemma shows that γ is one to one, hence the dimension of Γ (on $\mathbb{F}_s$) is

$$K_\Gamma = \dim_{\mathbb{F}_s} \Gamma = (N^2 + 2N) \log_s t + 1.$$

The weight $\mathrm{w}(\gamma(f,v,a))$ of the codeword $c = \gamma(f,v,a)$ is $\mathrm{w}(\gamma(f,v,a)) = t^{2N} - M(f,v,a)$. Define $\alpha = t^{2N} - t^{2N}/s$, and for $\rho = 0,\ldots,N$, let $\beta(\rho) = t^{2N} - (1/s)(t^{2N} + (-1)^\rho (s-1) t^{2N-\rho})$

and $\gamma(\rho) = t^{2N} - (1/s)(t^{2N} + (-1)^{\rho+1}t^{2N-\rho})$. From Theorem 6 it follows that the set $\mathscr{P}_\Gamma$ of the weights of codewords in Γ is $\mathscr{P}_\Gamma = \{\alpha\} \cup \{\beta(\rho)/\rho = 0,\dots,N\} \cup \{\gamma(\rho)/\rho = 0,\dots,N\}$. It is as simple matter to check that α, $\beta(\rho)$, $\gamma(\rho)$ are distinct numbers when $\rho \in \{0,\dots,N\}$, to notice that $\beta(0) = 0$ is the weight of the null codeword, and to get $\mathrm{Min}(\mathscr{P}_\Gamma \setminus \{0\}) = \gamma(1)$. Therefore:

Theorem 11. *The parameters of $\Gamma(N,t,s)$ are*

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

From now on, if $\zeta \in \mathscr{P}_\Gamma$, we denote by E_ζ the set of all codewords c in Γ with weight $\mathrm{w}(c) = \zeta$. When the rank of f is 2ρ and when H and T are associated to f, we have

$$\dim_{\mathbb{F}_t} \mathrm{Ker}\, T = \dim_{\mathbb{F}_t} \mathrm{Ker}\, H = 2\dim_{\mathbb{F}_{t^2}} \mathrm{Ker}\, H = 2(N - \mathrm{rk}\, H) = 2N - 2\rho$$

thus $\dim_{\mathbb{F}_t} \mathrm{Im}\, T = 2\rho$. If $f \in \mathrm{QH}(\mathbb{F}_t^{2N})$, define

$$E_{\zeta,f} = \{(v,a) \in \mathbb{F}_t^{2N} \times \mathbb{F}_s / \mathrm{w}(\gamma(f,v,a)) = \zeta\}.$$

We have the disjoint union $E_\zeta = \bigcup_{f \in \mathrm{QH}(\mathbb{F}_t^{2N})} (\{f\} \times E_{\zeta,f})$. From Theorem 6, it follows

$$(v,a) \in E_{\alpha,f} \Leftrightarrow v \notin \mathrm{Im}\, T.$$

Since $|\mathrm{Im}\, T| = t^{2\rho}$, we deduce $|E_{\alpha,f}| = s(t^{2N} - t^{2\rho})$ and

$$|E_\alpha| = s\sum_{\rho=0}^{N} |H(N,\rho)| \times (t^{2N} - t^{2\rho}).$$

If $\rho \in \{0,\dots,N\}$, then $E_{\beta(\rho),f} = \emptyset$ and $E_{\gamma(\rho),f} = \emptyset$ as soon as $\mathrm{rk}(f) \neq 2\rho$. Let f denote a quadratic hermitian form f of rank 2ρ. We have

$$E_{\beta(\rho),f} = \{(v,a) \in \mathbb{F}_t^{2N} \times \mathbb{F}_s / v = T(u) \in \mathrm{Im}\, T \text{ and } \mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u)) = a\}.$$

The map $(v,a) \mapsto v$ defines a bijection between $E_{\beta(\rho),f}$ and $\mathrm{Im}\, T$, thus $|E_{\beta(\rho),f}| = t^{2\rho}$ and $|E_{\beta(\rho)}| = |H(N,\rho)| \times t^{2\rho}$. We next write

$$E_{\gamma(\rho),f} = \{(v,a) \in \mathbb{F}_t^{2N} \times \mathbb{F}_s / v = T(u) \in \mathrm{Im}\, T \text{ and } \mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u)) \neq a\}$$

The map $T : \mathbb{F}_t^{2N} \to \mathrm{Im}\, T$ is linear and onto, thus $|T^{-1}(v)| = |\mathrm{Ker}\, T| = t^{2N-2\rho}$ for all v in $\mathrm{Im}\, T$, and

$$|E_{\gamma(\rho),f}| = \sum_{a \in \mathbb{F}_s} \frac{|\{u \in \mathbb{F}_t^{2N} / \mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u)) \neq a\}|}{|\mathrm{Ker}\, T|}.$$

Theorem 6 gives

$$|\{u \in \mathbb{F}_t^{2N} / \mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(u)) = a\}| = \begin{cases} \dfrac{1}{s}(t^{2N} + (-1)^\rho(s-1)t^{2N-\rho}) & \text{if } a = 0, \\ \dfrac{1}{s}(t^{2N} - (-1)^\rho t^{2N-\rho}) & \text{else,} \end{cases}$$

hence $|E_{\gamma(\rho),f}| = (s-1)t^{2\rho}$ and $|E_{\gamma(\rho)}| = |H(N,\rho)| \times (s-1)t^{2\rho}$. We obtain:

Theorem 12. *The weight distribution of Γ is*

Weights:	*Number of codewords in Γ*:
α	$s\sum_{\rho=0}^{N} \lvert H(N,\rho)\rvert \times (t^{2N} - t^{2\rho})$
$\beta(\rho)$ (*where* $0 \leqslant \rho \leqslant N$)	$\lvert H(N,\rho)\rvert \times t^{2\rho}$
$\gamma(\rho)$ (*where* $0 \leqslant \rho \leqslant N$)	$\lvert H(N,\rho)\rvert \times (s-1)t^{2\rho}$

where $|H(N,\rho)|$ is given by Theorem 9.

In fact, Theorem 6 may be handled in much the same way to obtain the weight distribution of several linear subcodes of $\Gamma(N,t,s)$. For instance, the hermitian form trace code Γ_H defined by the words $(\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)+v.x))_{x\in\mathbb{F}_t^{2N}}$ was first introduced in [4], and is a subcode of $\Gamma(N,t,s)$. Another example is given by the code Γ_0 studied in [5] and which codewords are $(\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)))_{x\in\mathbb{F}_t^{2N}}$. Next table shows three such subcodes of $\Gamma(N,t,s)$.

Code:	Codewords:
$\Gamma(N,t,s)$	$(\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)+v.x)+a)_{x\in\mathbb{F}_t^{2N}}$
$\Gamma_H = \gamma(\mathrm{QH}(\mathbb{F}_t^{2N}) \times \mathbb{F}_t^{2N} \times \{0\})$	$(\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)+v.x))_{x\in\mathbb{F}_t^{2N}}$
$C = \gamma(\mathrm{QH}(\mathbb{F}_t^{2N}) \times \{0\} \times \mathbb{F}_s)$	$(\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x))+a)_{x\in\mathbb{F}_t^{2N}}$
$\Gamma_0 = \gamma(\mathrm{QH}(\mathbb{F}_t^{2N}) \times \{0\} \times \{0\})$	$(\mathrm{Tr}_{\mathbb{F}_t/\mathbb{F}_s}(f(x)))_{x\in\mathbb{F}_t^{2N}}$

Let $\mathscr{P}_D$ denotes the set of weights of codewords in D. The same reasoning applies to each of these subcodes and lead us to three similar results (notice that $\gamma(0)$ never occurs when $D = \Gamma_H$):

Theorem 13. *Γ_H is a linear code on $\mathbb{F}_s$ with parameters*

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

and weight distribution

Weights:	*Number of codewords in Γ_H*:
α	$\sum_{\rho=0}^{N} \lvert H(N,\rho)\rvert \times (t^{2N} - t^{2\rho})$
$\beta(\rho)$ (*where* $0 \leqslant \rho \leqslant N$)	$\lvert H(N,\rho)\rvert \times \frac{1}{s}(t^{2\rho} + (-1)^{\rho}(s-1)t^{\rho})$
$\gamma(\rho)$ (*where* $1 \leqslant \rho \leqslant N$)	$\lvert H(N,\rho)\rvert \times \frac{(s-1)t^{\rho}}{s}(t^{\rho} - (-1)^{\rho})$

Theorem 14. *C is a linear code on* $\mathbb{F}_s$ *with parameters*

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

and weight distribution

Weights:	*Number of codewords in C*:
$\beta(\rho)$ (*where* $0 \leqslant \rho \leqslant N$)	$\lvert H(N,\rho)\rvert \times (s-1)$
$\gamma(\rho)$ (*where* $0 \leqslant \rho \leqslant N$)	$\lvert H(N,\rho)\rvert$

Theorem 15. *Γ_0 is a linear code on* $\mathbb{F}_s$ *with parameters*

$$[N_{\Gamma_0}, K_{\Gamma_0}, D_{\Gamma_0}] = \left[t^{2N}, N^2 \log_s t, \frac{(s-1)t^{2N-2}}{s}(t^2-1)\right]$$

and weight distribution

Weights:	*Number of codewords in* Γ_0:
$\beta(\rho)$ (*where* $0 \leqslant \rho \leqslant N$)	$\lvert H(N,\rho)\rvert$

Remark. As $\gamma(1) < \beta(2)$, the code Γ_0 corrects more errors than the three previous codes.

References

[1] R.C. Bose, I.M. Chakravarti, Hermitian varieties in a finite projective space PG(N, q^2), Canad. J. Math. 18 (1966) 1161–1182.
[2] L. Carlitz, The Number of solutions of some special equations in a finite field, Pacific J. Math. 4 (1954) 207–217.
[3] L. Carlitz, J.H. Hodges, Representations by hermitian forms in a finite field, Duke Math. J. (22) (1955) 393–405.
[4] J.-P. Cherdieu, Exponential sums, codes and hermitian forms, IEEE Trans. Inform. Theory 41 (5) September 1995.
[5] J.-P. Cherdieu, A. Delcroix, J.-C. Mado, D.-J. Mercier, Weight distribution of the hermitian Reed–Muller code, Appl. Algebra Engrg. Commun. and Comput. AAECC 8 (1997) 304–314.
[6] 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.
[7] J.-R. Joly, Equations et variétés algébriques sur un corps fini, Enseign. Math. 19 (1973) 1–117.
[8] R. Lidl, H. Niederreiter, Finite fields, Encyclopedia of Mathematics and its Applications, Vol. 20, Addison-Wesley Publishing Company, Reading, MA, 1983.
[9] D.-J. Mercier, Hermitian forms, trace equations and application to codes, arXiv: math.NT/0111191, http://www.arxiv.org/, 2001.
[10] D.-J. Mercier, Two codes related to hermitian forms, J. Pure Appl. Algebra 179 (3) (2003) 273–285.
[11] R.G. Van Meter, Generalized k-linear equations over a finite field, Math. Nachr. 53 (H.1-6) (1972) 63–67.