ON THE HERMITIAN TRACE BASIS OF $GF(q^{2m})$ OVER $GF(q)$

S. NDJEYA

Department of Mathematics
Higher Teachers Training College of Yaounde
University of Yaoundé I
P. O. Box 47, Yaounde
Cameroon
e-mail: ndjeyas@yahoo.fr

Abstract

This article handles a particular type of trace σ -basis of order m , which has been studied in [3]. These basis were introduced for the first time by Wolfmann in [6] and we call them Hermitian trace basis of order m of $GF(q^{2m})$ on $GF(q)$. We give the existence theorem and the exact number of such bases on $GF(q^2)$.

1. Introduction

Let K be a commutative field and σ be an automorphism of K .

Definition 1. Let E be a vector space over K . A σ -sesquilinear form on E , is any mapping $f : E \times E \rightarrow K$ satisfying the following properties:

- (a) For $y \in E$ fixed, the mapping $f_y : x \mapsto f(x, y)$ is linear.

2010 Mathematics Subject Classification: 11E39, 12E20, 16R30, 47A07.

Keywords and phrases: Galois fields, trace mapping, Hermitian trace basis.

Received May 20, 2017; Revised May 26, 2017

(b) For $x \in E$ fixed, the mapping $f_x : y \mapsto f(x, y)$ is σ -semilinear (i.e., the mapping f_x is additive and for any $y \in E, \lambda \in K : f(x, \lambda y) = \sigma(\lambda)f(x, y)$).

When $\sigma := Id_K$, we say that f is a bilinear form. A sesquilinear form f is symmetry if for all $x, y \in E : f(x, y) = f(y, x)$. However, if $\mathcal{B} = \{e_1, e_2, \dots, e_n\}$ is a basis of E over K , the coefficients are $a_{ij} := f(e_i, e_j)$ define a square matrix $M_{f, \mathcal{B}}$ of order n with coefficients in K called matrix associated f and the determinant of $M_{f, \mathcal{B}}$ is called discriminant of f on K .

Definition 2. Let $f : E \times E \rightarrow K$ be a symmetry sesquilinear form. The mapping $q : E \rightarrow K$ defined by $q(x) := f(x, x)$ for all $x \in E$ is called quadratic form associated to f and vice versa. f is polar form of q .

Remark 3. When the characteristic of K is different from 2, we define an equivalence relation between sesquilinear form on E as follows: if $GL(E)$ is the group of linear automorphisms of E over K . If f and f' are sesquilinear forms on E , we say that f and f' are equivalent if there exists $u \in GL(E)$ such that for all $x, y \in E, f'(x, y) = f(u(x), u(y))$.

Remark 4 ([4]). Let $K := GF(q)$ be a finite field of characteristic different from 2. Let E be a vector space over K of dimension n and $\alpha \in K(\alpha \neq 0)$, where α is not a square. Then there are two equivalence classes of non degenerate quadratic forms on E of matrices:

$$I_n \quad \text{or} \quad \begin{pmatrix} I_{n-1} & 0_{n-1,1} \\ 0_{1,n-1} & \alpha \end{pmatrix}.$$

A quadratic form Q is one or the other type depending on whether discriminant is a square or not of $K \setminus \{0_K\}$.

Remark 5 ([1]). Let E be a vector space of dimension n over K . If the characteristic of K is different from 2 and f is a symmetric bilinear form on E , then there exists an orthogonal basis for f .

Notation 6. In the remainder of this paper, we adopt the following notations:

q is a power of a prime integer p ;

m is a nonzero integer;

$F := GF(q^{2m})$;

for all $x \in F$, $\bar{x} = x^{q^m}$.

2. Hermitian Trace Basis

Let $\mathcal{B} := \{b_0, \dots, b_{2m-1}\}$ be an $GF(q)$ -basis of F , where $b_i \in F$ for all $i = 0, \dots, 2m-1$.

Definition 7. $\mathcal{B}$ is called a Hermitian trace-base of F over $GF(q)$ of the order m if $\text{tr}_{F/GF(q)}(b_i b_j) = \delta_{ij}$ for all integers i and j with $0 \leq i, j \leq 2m-1$. δ_{ij} is the Kronecker's symbol and $\text{tr}_{F/GF(q)}(x) = x + x^q + \dots + x^{q^{2m-1}}$.

Lemma 8. Let n be integer such that $n \geq 2$. The matrix

$$\begin{pmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^{n-1} \end{pmatrix},$$

(where a_i are elements of a finite field or no) is called matrix of Vandermonde. His determinant denoted $\det(V)$ is given by:

$$\det(V) = \prod_{1 \leq i < j \leq n} (a_i - a_j).$$

Thus, $\det(V) \neq 0$ if and only if $a_i \neq a_j$ as soon as $i \neq j$.

Notation 9. In the sequel, unless otherwise stated, we denote by: $K = GF(q^m)$, $F_1 = GF(q^2)$, and $F_0 = GF(q)$.

Theorem 10. *In characteristic 2, there is no Hermitian trace basis of order m of F on F_0 .*

Proof. It is immediate and follows from the transitivity of the trace mapping. $\square$

Remark 11. We have the following properties:

- (i) For all $x \in F$, $\text{tr}_{F/F_0}(\bar{x}) = \text{tr}_{F/F_0}(x)$.
- (ii) The mapping $f : F \times F \rightarrow F_0$ definite by: for all $x, y \in F$, $f(x, y) = \text{tr}_{F/F_0}(xy)$ is the symmetry bilinear form and no degenerate.

Remark 12 ([1]). Let q be a power of an integer p and n is a nonzero integer. Let $L = GF(q^n) = GF(q)(\gamma)$, where γ is a primitive element of L . If V is the matrix given by: $V = (\gamma^{iq^j})_{0 \leq i, j \leq n-1}$ and we denote by $|V|$ the determinant of V , then $|V|^q = (-1)^{n-1}|V|$.

Remark 13 ([5]). Let q be a power of an odd prime integer. Then a is a square in $GF(q) \setminus \{0\}$ if and only if $a^{\frac{q-1}{2}} = 1$.

Theorem 14. *Let q be an integer power of odd prime p and an integer m nonzero. The following properties are equivalent:*

- (i) F admits an Hermitian $GF(q)$ -trace-basis of m order.
- (ii) $q \equiv 3 \pmod{4}$ and m odd.

Proof. Show that (i) implies (ii).

Indeed, suppose that F admits an Hermitian $GF(q)$ -trace-basis of order m . Let $\mathcal{B} := \{b_0, \dots, b_{2m-1}\}$ be such a basis, and let $f(x, y) =$

$\text{tr}_{F/F_0}(xy)$ for all $x, y \in F$ be the map defined in Remark 11. We know that if the discriminant of f is a square, the quadratic form Q associated to f with respect to $\mathcal{B}$ is the matrix $M_Q = I_{2m}$ (see Remark 4) and this is true regardless of the base F chosen. In particular, choose the base $\mathcal{B}' := \{1, \gamma, \dots, \gamma^{2m-1}\}$ be the canonical basis of F over $GF(q)$. That is, according to Remark 11 (ii), if we put $A = (a_{ij})_{0 \leq i, j \leq n-1}$, where the following equation: $A = V \times W$, where $V = (\gamma^{iq^j})_{0 \leq i, j \leq n-1}$ and $W^t = V^{q^m}$.

So $|A| = |V| \times |W| = |V^{q^m}|$, where $|A|$ denotes the determinant of A . according to the Remark 4, $|A|$ is a square of $GF(q) \setminus \{0\}$ or still:
 $|A|^{\frac{q-1}{2}} = |V|^{\frac{q-1}{2}} (q^m - 1) = 1$ (see Remark 11), i.e., $(-1)^{\frac{q^m+1}{2}} = 1$ (see Remark 13)
 $\frac{q^m+1}{2} \equiv 0 \pmod{2}$ still or: $q^m + 1 \equiv 0 \pmod{4}$ or and finally: $q \equiv 3 \pmod{4}$ and m is odd. Then (i) implies (ii).

Show that (ii) implies (i).

Assume that $q \equiv 3 \pmod{4}$ and m is odd. It remains to show that F admits an Hermitian $GF(q)$ -trace-basis of order m . Indeed, the hypothesis implies that the discriminant of f is a square, so after equivalence, the matrix denoted M_Q of the quadratic form associated with f is the identity matrix or $M_Q = I_{2m}$. Note that : for all $x, y \in F$, $f(x, y) = \text{tr}_{F/F_0}(xy)$. On the other hand, $p > 2$ and f is a symmetric bilinear form. Then by Remark 5, there is an orthogonal basis $\mathcal{B} := \{b_0, b_1, \dots, b_{2m-1}\}$ for f . Thus: $Q(c_i) = 1$ for $i = 0, \dots, 2m-1$ and $f(b_i, b_j) = 0$ if $i \neq j$, where $\text{tr}_{F/F_0}(b_i b_j) = \delta_{ij}$ for all i and j integers. In the other words, $\mathcal{B}$ is a Hermitian $GF(q)$ -trace-basis of order m of F , where (ii) implies (i).

□

Example 15. Let $E = GF(3^2)(\alpha)$, where $\alpha^2 = \alpha + 1$. Then E admits Hermitian trace basis of order 1 on $GF(3)$. It is given by: $\mathcal{B}_1 = (\alpha, \alpha^3)$, $\mathcal{B}_2 = (\alpha, \alpha^7)$, $\mathcal{B}_3 = (\alpha^9, \alpha^5)$, and $\mathcal{B}_4 = (\alpha^5, \alpha^7)$.

Proposition 16. Let q be a power of a prime integer p with $q \equiv 3 \pmod{4}$ and m odd integer and $E = GF(q^{2m})$. If $\mathcal{B} = \{b_0, b_1, \dots, b_{2m-1}\}$ and $\bar{\mathcal{B}} = \{\bar{b}_0, \bar{b}_1, \dots, \bar{b}_{2m-1}\}$, then the following conditions are equivalents:

- (i) $\mathcal{B}$ is a Hermitian $GF(q)$ -trace basis of order m of E .
- (ii) $\bar{\mathcal{B}}$ is a Hermitian $GF(q)$ -trace basis of order m of E .

Proof. It is immediate and follows from the Definition 7. $\square$

3. Counting of Hermitian Trace Basis

Theorem 17. Let q be a power of a prime integer p with $q \equiv 3 \pmod{4}$ and m nonzero integer. If $\mathcal{B}$ denotes the set of Hermitian trace basis of order m of E on F_0 all distinct, then $0 < |\mathcal{B}| \leq C_{q^{2m-1}+q^{m-1}}^{2m}$.

Proof. In fact, look for a Hermitian trace basis of order m of F on F_0 returns to seek $2m$ -tuples solutions of the equation (S) defined by: $\text{tr}_{F/F_0}(x\bar{x}) = 1$. We must also have : $\text{tr}_{F/F_0}(x_i\bar{x}_j) = 0$ for $i \neq j$, where $x = (c_1, \dots, c_{2m})$ is the $2m$ -tuple solution of (S). $\square$

Remark 18. For $E = GF(3^6) = GF(3)(\alpha)$, where $\alpha^6 = 1 + 2\alpha^5$, there are exactly 36288 Hermitian trace basis of order 3 of E over $GF(3)$.

Remark 19. Let q be a power of an integer p with the first $q \equiv 3 \pmod{4}$. Let $F_1 = GF(q^2)$. Consider the set A as follows:

$$A = \{(i, j) \in \mathbb{N}^2 : 0 \leq i \leq j \leq q \text{ and } j - i = \frac{k(q+1)}{4}, k \text{ integer}\}.$$

Then, there exists a bijection between the set $\mathcal{B}$ of Hermitian trace basis of order 1 on $GF(q)$ and the set A .

Theorem 20. *Let q be a power of a prime integer p with $q \equiv 3 \pmod{4}$ and $F = GF(q^2)$. If $\mathcal{B}$ is the set of Hermitian $GF(q)$ -trace basis of order 1 and distinct from F , then $|\mathcal{B}| = q + 1$.*

Proof. Having the same assumptions as the Remark 19, we get $|\mathcal{B}| = |A|$ (where $|X|$ denote the cardinality of the set X). A being together referred to the Remark 19. It is now the set A .

$$(1) \text{ For } j = 0, \text{ let } E_0 = \left\{ k \in \mathbb{N}^* / 0 + \frac{k(q+1)}{4} \leq q \right\}, \text{ but } 0 \leq \frac{k(q+1)}{4} \leq q$$

implies that $i \leq k \leq \frac{4q}{q-1}$. So $|E_0| = N_0 = \left\lceil \frac{4q}{q+1} \right\rceil$, where $[X]$ is the integral part of X .

$$E_0 = \{1, \dots, N_0\}. \text{ For } j = 1, \text{ let } E_1 = \left\{ k \in \mathbb{N}^* / 1 + \frac{k(q+1)}{4} \leq q \right\},$$

$$|E_1| = N_1 = \left\lceil \frac{4q}{q+1} \right\rceil. E_1 = \{1, \dots, N_1\}.$$

We do this to j denoted $j_{\max}$. The number $j_{\max}$ is the largest integer such that: $q-1 < j_{\max} + \frac{q+1}{4} \leq q$, so $j_{\max} \leq q - \frac{q+1}{4} = \frac{1q-1}{4}$.

Therefore $j_{\max} = \left\lceil \frac{3q-1}{4} \right\rceil$ and $E_{j_{\max}} = \{k \in \mathbb{N}^* / j_{\max} + k(q+1) \leq q\} = \{1\}$.

We have $|E_{j_{\max}}| = N_{j_{\max}} = 1$.

$$(2) \text{ Now, let } E'_0 = \left\{ k \in \mathbb{N}^* / 0 + \frac{k(q+1)}{4} \leq q \right\}. \text{ Then, } |E'_0| = N'_0 = 1 +$$

$$\left\lceil \frac{N_1-1}{2} \right\rceil. \text{ The same for } E'_0 = \left\{ k \in \mathbb{N}^* / 1 + \frac{k(q+1)}{4} \leq q \right\}. |E'_1| = N'_1 = 1$$

$$+ \left\lceil \frac{N_1-1}{2} \right\rceil. \text{ So on until } E'_{j_{\max}}, \text{ where } |E_{j_{\max}}| = 1. \text{ We obtain}$$

$$A = \sum_{i=0}^{j_{\max}} N'_i = j_{\max} + 1 + \sum_{i=0}^{j_{\max}} \left\lceil \frac{N'_i-1}{2} \right\rceil. \quad (*)$$

(3) But for any $i = 0, \dots, j_{\max}$, $N_i = \left\lfloor \frac{4(q-i)}{2q+1} \right\rfloor$. As $\left\lfloor \frac{4(q-1)}{q+1} \right\rfloor = 4 - \frac{4i+4}{q-1}$, it deduces that for any $i = 0, \dots, j_{\max}$, $N_i \leq 3$. Since we know that $q \geq 3$, the terms no null of the sum (*) are such that $N_i = 3 \Leftrightarrow \left\lfloor 4 - \frac{4i+4}{q+1} \right\rfloor = 3$, or still to $0 < \frac{4i+4}{q+1} \leq 1$ or finally to $0 \leq i \leq \frac{q-3}{4} = \frac{q+1}{4} - 1$. Then $\left\lfloor \frac{N_1-1}{2} \right\rfloor = 1$ and if on the other hand $\frac{q-3}{4} < i < j_{\max}$, then $\left\lfloor \frac{N_1-1}{2} \right\rfloor = 0$. Therefore

$$|A| = j_{\max} + 1 + \sum_{i=0}^{\frac{q-3}{4}}, \quad (1)$$

or $j_{\max} = \left\lfloor \frac{3q-1}{q+1} \right\rfloor = \left\lfloor q - \frac{q+1}{4} \right\rfloor = q - \frac{q+1}{4}$ because $q \equiv 3 \pmod{4}$

and $\frac{q+1}{4}$ integer. Later on, $|A| = q - \frac{q+1}{4} + 1 + \frac{q+1}{4} - 1 + 1$, i.e., $|\mathcal{B}| = |A| = q - 1$. □

References

- [1] R. Lidl and H. Niederreiter, Finite Fields Encyclopedia of Mathematics and its Applications, New-York, USA, 1984.
- [2] F. J. Mac Williams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North Holland Publishing Company, 1983.
- [3] S. Ndjeya, Hermitian Codes, Ph.D. Thesis, University of Marseille II, France, 1988.
- [4] Daniel Perrin, Algebraic Courses Editions-ellipses, no 18, France, 1998.
- [5] A. Warusfel, Finite Algebraic Structures, Hachette University, Paris, France, 1971.
- [6] J. Wolfmann, Different aspects of the q -ary image codes, Treatment of the signal, France 1(2) (1984).