Codes correcteurs d'erreurs sur des surfaces Hermitiennes

Frédéric Aka-Bilé EDOUKOU
e.mail: edoukou@iml.univ-mrs.fr
Institut de Mathématiques de Luminy
Marseille, France

JNCF 2008: Journées Nationales de Calcul Formel
Lundi 20 Octobre 2008
CIRM, Luminy, Marseille, France

Contents

I-Notations

- $\mathbb{F}_q$: finite field with q elements ($q = p^a$).

- $V = \mathbb{A}^{m+1}$ the affine space of dimension $m+1$ on $\mathbb{F}_q$.
  $\mathbb{P}^m(\mathbb{F}_q)$:the corresponding projective space of dimension m.

- $\#\mathbb{P}^m(\mathbb{F}_q) = \pi_m = q^m + q^{m-1} + ... + q + 1$

- $\mathcal{F}_h(V, \mathbb{F}_q)$: vector space of forms of degree h on V with coefficients in $\mathbb{F}_q$.

- Si $f \in \mathcal{F}_h(V, \mathbb{F}_q)$,
  $Z(f)$: the set of zeros of f in $\mathbb{P}^m(\mathbb{F}_q)$.

- Let $X \subset \mathbb{P}^m(\mathbb{F}_q)$ a variety in $\mathbb{P}^m(\mathbb{F}_q)$,

  $X_{Z(f)}(\mathbb{F}_q)$: the set of rational points on $\mathbb{F}_q$ of the algebraic set $X \cap Z(f)$.

II- Construction of $C_h(X)$

- Let $X \subset \mathbb{P}^m(\overline{\mathbb{F}}_q)$ and $N = \#X(\mathbb{F}_q)$

$$c : \mathcal{F}_h(V, \mathbb{F}_q) \longrightarrow \mathbb{F}_q^N$$

$$f \longmapsto c(f) = (f(P_1), \ldots, f(P_N))$$

$C_h(X) = \text{Im}c$

- **definition** Let $c(f)$ be a codeword

$$cw(f) = \#\{P \in X \quad | \quad f(P) = 0\}$$

$$w(c(f)) = \#X(\mathbb{F}_q) - cw(f)$$

$$\text{dist}C_h(X) = \#X(\mathbb{F}_q) - \max_{f \in \mathcal{F}_h} cw(f)$$

- **Proposition** The parameters of $C_h(X)$:
length $C_h(X) = \#X(\mathbb{F}_q)$,

$$\dim C_h(X) = \dim \mathcal{F}_h - \dim \ker c,$$

$$\text{dist}C_h(X) = \#X(\mathbb{F}_q) - \max_{f \in \mathcal{F}_h} \#X_{Z(f)}(\mathbb{F}_q)$$

If c injective $\Rightarrow$ $\dim C_h(X) = \binom{m+h}{h}$

III-The study of $C_2(X)$ (X n-degenerate Hermit. surf. in $\mathbb{P}^3(\mathbb{F}_q)$)

$X : x_0^{t+1} + x_1^{t+1} + x_2^{t+1} + x_3^{t+1} = 0$

- 3.1 Number of points of X

$\#X(\mathbb{F}_q) = (t^2+1)(t^3+1)$, 1966

- 3.2 Injectivity of the application c

Tsfasman-Serre-Sørensen Bound $\Rightarrow$ $h \leq t$.

- 3.3 History of $C_h(X)$

$h = 2, t = 2$ | R. Tobias, 1985 | P. Spurr, 1986

$h = 2, t = 2$ A. B. Sørensen, 1991

Conjecture: $\#X_{Z(f)}(\mathbb{F}_q) \leq h(t^3 + t^2 - t) + t + 1$

G. Lachaud, A.G.C.T-4, 1993

$\#X_{Z(f)}(\mathbb{F}_q) \leq h(t^3 + t^2 + t + 1)$

S. H. Hansen, G. Lachaud, J. B. Little, F. Rodier

Weight Distribution of the code $C_2(X)$ over $\mathbb{F}_4$ (i.e. $h = 2, t = 2$)

Complete Computer Search

- The code $C_2(X)$ defined over $\mathbb{F}_4$ is a $[45, 10, 22]_4$-code.
  And it is a even-weight code.
  We have the following formula:

$$w_i = (10 + i) \times 2 \quad i = 1, ..., 12$$

- $\boxed{A_{w_1} = 2.160}$, $\boxed{A_{w_2} = 2.970,\ A_{w_3} = 4.320,}$ $A_{w_4} = 40.500$, $A_{w_5} = 122.976$, $A_{w_6} = 233.415$, $A_{w_7} = 285.120$, $A_{w_8} = 233.400$, $A_{w_9} = 97.200$, $A_{w_{10}} = 20.574$, $A_{w_{11}} = 4.320$, $A_{w_{12}} = 1.620$

• 3.4 Resolution of Sørensen's conjecture ($h \leq 2$ et $t = p^a$) and some consequences

$h = 1$: Bose and Chark., 1966 | Chark., 1971
$h = 2$

Table 1: Quadrics in PG(3,q).

r($\mathcal{Q}$)	Description	$\lvert\mathcal{Q}\rvert$	g($\mathcal{Q}$)
1	repeated plane $\Pi_2\mathcal{P}_0$	π_2	2
2	pair of distinct planes $\Pi_2\mathcal{H}_1$	$2q^2 + \pi_1$	2
2	line $\Pi_1\mathcal{E}_1$	π_1	1
3	cone quadric $\Pi_0\mathcal{P}_2$	π_2	1
4	hyperbolic quadric $\mathcal{H}_3(\mathcal{R}, \mathcal{R}')$	$\pi_2 + q$	1
4	elliptic quadric $\mathcal{E}_3$	$\pi_2 - q$	0

Some values of $\#X_{Z(f)}(\mathbb{F}_q)$

$s(t) = 2t^3 + 2t^2 - t + 1$, $s_2(t) = 2t^3 + t^2 + 1$, $s_3(t) = 2t^3 + t^2 - t + 1$, $s_4(t) = 2t^3 + 1$, $s_5(t) = 2t^3 - t + 1$

a. $\mathcal{Q}$ is a pair of planes: $\mathcal{Q} = H_1 \cup H_2$

$$\hat{\mathcal{X}}_1 = H_1 \cap \mathcal{X},\ \hat{\mathcal{X}}_2 = H_2 \cap \mathcal{X} \text{ et } \mathcal{L} = H_1 \cap H_2$$

$$|\mathcal{Q} \cap \mathcal{X}| = |H_1 \cap \mathcal{X}| + |H_2 \cap \mathcal{X}| - |\mathcal{L} \cap \mathcal{X}|. \quad (1)$$

$$\mathcal{P} \cap \mathcal{X} = \mathcal{L} \cap \hat{\mathcal{X}}_1 = \mathcal{L} \cap \hat{\mathcal{X}}_2. \quad (2)$$

a.1 Two tan planes to $\mathcal{Q}$

a.2 One tan and the second n-tan to $\mathcal{Q}$

a.3 Two n-tan planes to $\mathcal{Q}$

Theorem Bose-Chakravarti,1966 Let $\tilde{\mathcal{X}}$ be a degenerate Hermitian variety of rank $r < n+1$ in $\mathbb{P}^n(\mathbb{F}_q)$ and Π_{r-1} a linear projective space of dimension $r-1$ disjoint from the singular space Π_{n-r} of $\tilde{\mathcal{X}}$. Then $\Pi_{r-1} \cap \tilde{\mathcal{X}}$ is a non-degenerate Hermitian variety in Π_{r-1}.

b. $\mathcal{Q}$ is an elliptic quadric.

Table 3: Plane Hermitian curves.

r($\mathcal{V}$)	Description	$\lvert\mathcal{V}\rvert$	g($\mathcal{V}$)
1	repeated line $\Pi_1\mathcal{U}_0$	t^2+1	1
2	cone $\Pi_0\mathcal{U}_1$	t^3+t^2+1	1
3	non-sing. Herm. curve $\mathcal{U}_2$	t^3+1	0

Table 4: Plane Quadrics.

r($\mathcal{V}$)	Description	$\lvert\mathcal{V}\rvert$	g($\mathcal{V}$)
1	repeated line $\Pi_1\mathcal{P}_0$	$q+1$	1
2	cone $\Pi_0\mathcal{H}_1$	$2q+1$	1
2	point $\Pi_0\mathcal{E}_1$	1	0
3	conic $\mathcal{P}_2$	$q+1$	0

Rank	Type	$\#X_{Z(\mathcal{Q})}(\mathbb{F}_q)$	F_4	w_i $\mathbb{F}_q$
1 (plane)	1	t^3+t^2+1	13	t^5
	2	t^3+1	9	t^5+t^2
2 (line)	3	1	1	$t^5+t^3+t^2$
	4	$t+1$	3	$t^5+t^3+t^2-t$
	5	t^2+1	5	t^5+t^3
2 (pair of planes)	6	$s_4(t)$	17	$t^5-t^3+t^2$
		$s_5(t)$	15	$t^5-t^3+t^2+t$
	7	$s_3(t)$	19	t^5-t^3+t
		$s_2(t)$	21	t^5-t^3
	8	$s(t)$	23	$t^5-t^3-t^2+t$
		$s_2(t)$	21	t^5-t^3
3 (cone)	9	$\leq t^3+t^2+t+1 < s_4(t)$	≤ 15	$\geq t^5-t$
	10	t^3+t^2+1	13	t^5
		t^3+2t^2-t+1	15	t^5-t^2+t
4 (hyper.) $\mathcal{H}(\mathcal{R},\mathcal{R}')$	11	$s_2(t)$	21	t^5-t^3
	12	$\leq t^3+3t^2-t+1 \leq s_3(t)$	≤ 19	$\geq t^5-t^3$
	13	$\leq t^3+2t^2+1 \leq s_4(t)$	≤ 17	$\geq t^5-t^2$
	14	$\leq t^3+t^2+t+1 < s_4(t)$	≤ 15	$\geq t^5-t$
4 (ellip.)	15	$\leq 2t^3+2t+2 < s_2(t)$	≤ 17	$\geq t^5-t^3+t^2-2t-1$

Weight Distribution (w_i, A_{w_i}) of $C_2(X)$ $(\mathbb{F}_{t^2})$

- $\boxed{w_1 = t^5 - t^3 - t^2 + t}$

  The codewords $<< w_1 >>$: union of 2 tan planes to X and $l \cap X = (t+1)$ points.

  $\boxed{A_{w_1} = (t^2-1)[\frac{1}{2}(t^5 + t^3 + t^2 + 1)t^5]}$

- $\boxed{w_2 = t^5 - t^3}$

  The codewords $<< w_2 >>$ are given by:
  –hyperbolic containing III of X.
  –union of 2 planes tan of X and $l \subset X$.
  –union of 2 planes one tan, the second n-tan to X and $l \cap X = 1$ point.

$A_{w_2} = \boxed{(t^2-1)[\frac{1}{2}(t^5 + t^3 + t^2 + 1)(3t^2 - t + 1)t^2]}$

- $\boxed{w_3 = t^5 - t^3 + t}$
  The codewords $<< w_3 >>$: quadrics which are union of 2 planes one tan, the second non-tan to X and $l \cap X = (t+1)$ points.
  $\boxed{A_{w_3} = (t^2-1)(t^5+t^3+t^2+1)(t^6-t^5)}$

Conjecture on w_4 and w_5

- $\boxed{w_4 = t^5 - t^3 + t^2}$
  The codewords $<< w_4 >>$ are given by quadrics which are union of 2 planes tan to X and $l \cap X = 1$ point and particular elliptic quadrics.

- $\boxed{w_5 = t^5 - t^3 + t^2 + t}$
  The codewords $<< w_5 >>$:union of 2 planes non-tan to X and $l \cap X = (t+1)$ pts, and particular elliptic quadrics.

F. A. B. Edoukou, Codes defined by forms of degree 2 on Hermitian Surface and Sørensen's conjecture. Finite Fields and Their Applications, Volume 13, Issue 3, (2007), 616-627.

F. A. B. Edoukou,The Weight distribution of the functional codes defined by forms of degree 2. To appear in J.T.N.B 2008.

Divisibility by t of the weights ???

Theorem of Ax (1964)
Let r polynomials $f_i(x_1, ..., x_n)$ and deg $(f_i) = d_i$ on $\mathbb{F}_q$ then: if $n > b\sum_{i=1}^{r} d_i \Rightarrow q^b | \#Z(f_1, ..., f_n)$.

Theorem
All the weights w_i are divisible by t.

Consequence: The conjecture on w_4 and w_5 is true.

• 3.5 Resolution of Sørensen's conjecture ($h \geq 3$ and $t = p^a$)

• A) There is no line in Hermitian surface ∩ hypersurface of degree h.

$$\#X_{Z(f)}(\mathbb{F}_q) \leq h(t^3 + t^2 - t) + h + 2t(h - t)$$ (E.)

$$\#X_{Z(f)}(\mathbb{F}_q) \leq h(t^3 + t^2 - t) + t + 1$$ (Sørensen)

• B) There is a line in Hermitian surface ∩ hypersurface of degree h ???

- B-1) Cubic Surface
  1,519.708.182.382.116 $\times 10^{18}$ Tests ($\mathbb{F}_9$)
  Singular (Univ. of Kaiserlautern, July 2008)
  Magma (IML, Luminy, October 2008)
  Sage ???

- B-2) Surface of degree $h > 3$???

IV- The study of the code $C_2(X)$ for X a non-degenerate Hermitian variety in $\mathbb{P}^4(\mathbb{F}_q)$

• $\mathbb{P}^4(\mathbb{F}_q)$: F. A. B. Edoukou,Codes defined by forms of degree 2 on non-degenerate Hermitian varieties in $\mathbb{P}^4(\mathbb{F}_q)$.
To appear in DCC 2008.

Poids	$\mathcal{Q}$	$\mathcal{P} \cap \mathcal{X}$	w_i
1	2 n-tan $\mathcal{H}$	n-sin. Herm	$t^7 - t^5 - t^3 - t^2$
2	2 n-tan	sin. Herm (r=2)	$t^7 - t^5 - t^3$
3	1t+1n-tan	n-sin Herm	$t^7 - t^5 - t^2$
4	1t+1n-tan	sin. Herm (r=2)	$t^7 - t^5$
	2tan	line	
5	2 tan	n-sin. Herm	$t^7 - t^5 + t^3 - t^2$

• Conjecture:

For $h \leq t$ $\#\mathcal{X}_{Z(f)}(\mathbb{F}_q) \leq h(t^5+t^2)+t^3+1$.

The min weight codewords correspond to:
–hypers. reaching the Tsfasman-Serre-Sørensen's upper bound.
–each hyperplane H_i is non-tangent to $\mathcal{X}$
–and the plane $\mathcal{P}$ of intersection of the h hyperplanes intersecting $\mathcal{X}$ at a non-sing Herm plane curve.

V-Generalisation: The study of the code $C_2(X)$ for X a non-degenerate Hermitian variety in $\mathbb{P}^{2l+1}(\mathbb{F}_q)$, $\mathbb{P}^{2l+2}(\mathbb{F}_q)$

• $\mathbb{P}^{2l+1}(\mathbb{F}_q)$, $\mathbb{P}^{2l+2}(\mathbb{F}_q)$: F. A. B. Edoukou, A. Hallez, F. Rodier and L. Storme, Codes defined by forms of degree 2 on non-degenerate Hermitian varieties.
In preparation.

• $\mathbb{P}^{2l+1}(\mathbb{F}_q)$, $\mathbb{P}^{2l+2}(\mathbb{F}_q)$: F. A. B. Edoukou, A. Hallez, F. Rodier and L. Storme, On the small weight codewords of the functional codes $C_h(X)$, X a non-singular Hermitian variety.
In preparation.

F. A. B. Edoukou, Codes defined by forms of degree 2 on quadric Surfaces. I.E.E.E Trans. Inf. Theo., Vo. 54, Issue 2, Pages 860-864, (2008)