Number of points in the intersection of two quadrics defined over finite fields

Frédéric A. B. EDOUKOU
e.mail:abfedoukou@ntu.edu.sg
Nanyang Technological University
SPMS-MAS
Singapore

Carleton Finite Fields Workshop
July 20-23, 2010
Carleton University
Ottawa, (Ontario), Canada

Contents

Notations

I- Some results on intersection of quadrics

II-Intersection of two quadrics in $\mathbb{P}^3(\mathbb{F}_q)$

III-Intersection of two quadrics in $\mathbb{P}^4(\mathbb{F}_q)$

IV-Applications to coding theory

V-Generalization to quadrics in $\mathbb{P}^n(\mathbb{F}_q)$

VI-Conclusion

References

Notations

- $\mathbb{F}_q$: finite field with q elements, ($q = p^a$).
- $V = \mathbb{A}^{m+1}$ aff. sp. of dim. $m+1$ on $\mathbb{F}_q$.
  $\mathbb{P}^m(\mathbb{F}_q)$: proj. space of dim. m.
- $\#\mathbb{P}^m(\mathbb{F}_q) = q^m + q^{m-1} + \ldots + q + 1$
- $\pi_m = q^m + q^{m-1} + \ldots + q + 1$
- $\mathcal{F}_h(V, \mathbb{F}_q)$: forms of degree h on V with coefficients in $\mathbb{F}_q$.

I-Some results on intersection of two quadrics in $\mathbb{P}^n(\mathbb{F}_q)$.

- In 1975, W. M. Schmidt

$$|\mathcal{Q}_1 \cap \mathcal{Q}_2| \leq 2(4q^{n-2} + 4\pi_{n-3}) + \frac{7}{q-1}$$

- In 1992, Y. aubry

$$|\mathcal{Q}_1 \cap \mathcal{Q}_2| \leq 2(4q^{n-2} + \pi_{n-3}) + \frac{1}{q-1}$$

- In 1999, D. B. Leep et L. M. Schueller

Suppose: $w(\mathcal{Q}_1, \mathcal{Q}_2) = n + 1$

If $n + 1 \geq 4$ and even, then:

$$|\mathcal{Q}_1 \cap \mathcal{Q}_2| \leq 2q^{n-2} + \pi_{n-3} + 2q^{\frac{n-1}{2}} - 3q^{\frac{n-3}{2}}$$

If $n + 1 \geq 5$ and odd, then

$$|\mathcal{Q}_1 \cap \mathcal{Q}_2| \leq 2q^{n-2} + \pi_{n-3} + q^{\frac{n}{2}}$$

- In 2006, **Lemma**

Let $1 \leq l \leq n - 1$ and $w(\mathcal{Q}_1, \mathcal{Q}_2) = n - l + 1$.
If $|\mathcal{Q}_1 \cap \mathcal{Q}_2 \cap E| \leq m$ where $E \simeq \mathbb{P}^{n-l}(\mathbb{F}_q)$,
then $|\mathcal{Q}_1 \cap \mathcal{Q}_2| \leq mq^l + \pi_{l-1}$

This bound is the best possible as soon as m is optimal for E.

II-Intersection of two quadrics in $\mathbb{P}^3(\mathbb{F}_q)$
$X : F(x_0, x_1, x_2, x_3) = 0$

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

r($\mathcal{Q}$)	Description	$\|\mathcal{Q}\|$	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	quadric cone $\Pi_0\mathcal{P}_2$	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 de $\#X_{Z(f)}(\mathbb{F}_q)$

$C(q) = 4q + 1$, $C_2(q) = 3q + 1$, $C_3(q) = 3q$
$H(q) = 4q$, $H_2(q) = 3q + 1$, $H_3(q) = 3q$
$E(q) = 2(q + 1)$, $E_2(q) = 2q + 1$, $E_3(q) = 2q$

III-Intersection of two quadrics in $\mathbb{P}^4(\mathbb{F}_q)$

Table 2: Quadrics in $\mathbb{P}^4(\mathbb{F}_q)$.

r($\mathcal{Q}$)	Description	$\vert\mathcal{Q}\vert$	g($\mathcal{Q}$)
1	repeated hyperplane $\Pi_3\mathcal{P}_0$	π_3	3
2	pair of hyperplanes $\Pi_2\mathcal{H}_1$	$2q^3 + \pi_2$	3
2	plane $\Pi_2\mathcal{E}_1$	π_2	2
3	cone $\Pi_1\mathcal{P}_2$	π_3	2
4	cone $\Pi_0\mathcal{H}_3(\mathcal{R}, \mathcal{R}')$	$\pi_3 + q^2$	2
4	cone $\Pi_0\mathcal{E}_3$	$\pi_3 - q^2$	1
5	parabolic quadric $\mathcal{P}_4$	π_3	1

Section of X: g($\mathcal{Q}$)=2

Table 3: Plane quadric curves

r($\mathcal{Q}'$)	Description	$\lvert\mathcal{Q}'\rvert$	g($\mathcal{Q}'$)
1	repeated line $\Pi_1\mathcal{P}_0$	$q+1$	1
2	pair of lines $\Pi_0\mathcal{H}_1$	$2q+1$	1
2	point $\Pi_0\mathcal{E}_1$	1	0
3	parabolic $\mathcal{P}_2$	$q+1$	0

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

Section of X: g($\mathcal{Q}$)=3

a. $\mathcal{Q}$ is a repeated hyperplane

Theorem [Primrose, 1951]
Let $H \subset \mathbb{P}^4(\mathbb{F}_q)$ be an hyperplane

$$\#\mathcal{X}_H(\mathbb{F}_q) = \begin{cases} \pi_2 + q, \pi_2 - q & \text{if H n.-tan. to } \mathcal{X}, \\ \pi_2 & \text{if H is tan. to } \mathcal{X}. \end{cases}$$

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

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

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

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

Theorem [Swinnerton-Dyer, 1964] Let $\tilde{\mathcal{X}}$ be a degenerate quadric 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 quadric variety in Π_{r-1}.

Theorem [Wolfmann, 1975] Let $\tilde{\mathcal{X}} \subset \mathbb{P}^n(\mathbb{F}_q)$ be a non-degenerate quadric variety. A tangent hyperplane meets $\tilde{\mathcal{X}}$ at a denegerate quadric of the same type as $\tilde{\mathcal{X}}$.

b.1 Two tangent hyperplanes to $\mathcal{Q}$

b.2 One tangent and one n-tang. to $\mathcal{Q}$

b.3 Two tangent hyperplanes to $\mathcal{Q}$

Proposition If $\mathcal{Q}$ is a pair of hyperplanes in $\mathbb{P}^4(\mathbb{F}_q)$ and $\mathcal{X}$ the non-degenerate quadric variety in $\mathbb{P}^4(\mathbb{F}_q)$, then

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 2q^2 + 3q + 1,\ 2q^2 + 2q + 1$$

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 2q^2 + q + 1,\ 2q^2 + 1,$$

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 2q^2 - q + 1$$

Section of $\mathcal{X}$: g($\mathcal{Q}$)=1

a. $\mathcal{X} \cap \mathcal{Q}$ contains no line

$$\boxed{\#X_{Z(f)}(\mathbb{F}_q) \leq 2(q^2+1)}$$

b. $\mathcal{X} \cap \mathcal{Q}$ contains some lines

b.1. $\mathcal{Q}$ est degenerate

$$\boxed{\#X_{Z(f)}(\mathbb{F}_q) \leq 2q^2+2q+1}$$

b.2. $\mathcal{Q}$ is non-degenerate

Table 4: Intersection of $\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i$ in $\mathbb{P}^3(\mathbb{F}_q)$

Type	$\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i$
1	(hyperbolic quadric) $\cap$ (quadric cone)
2	(quadric cone) $\cap$ (quadric cone)
3	(hyperbolic quadric) $\cap$ (hyperbolic quadric)

Table 5: Number of points and lines in $\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i$

Types	4 lines	3 lines	2 lines	1 line
1			$3q$	$2q+1$
2	4q+1	3q+1	$2q+1$	$2q+1$
3	$4q$	3q+1	$3q+1$	$2(q+1)$

A) $\mathcal{X} \cap \mathcal{Q}$ contains exactly one line

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

B) $\mathcal{X} \cap \mathcal{Q}$ contains at least two lines:
B-1) $\mathcal{X} \cap \mathcal{Q}$ contains only skew lines

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

B-2) $\mathcal{X} \cap \mathcal{Q}$ contains at least two secant lines:
($\star$)**It exists H_1 and H_2 such that $\hat{\mathcal{X}}_i = \hat{\mathcal{Q}}_i$**

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

($\star\star$) **It exists H_1 such that $\hat{\mathcal{X}}_1 = \hat{\mathcal{Q}}_1$**

$$\#X_{Z(f)}(\mathbb{F}_q) \leq q^2 + 6q + 2$$

($\star\star\star$) **For $i = 1, ..., q+1$ $\hat{\mathcal{X}}_i \neq \hat{\mathcal{Q}}_i$**

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

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

Theorem If $\mathcal{X}$ is a non-degenerate quadric in $\mathbb{P}^4(\mathbb{F}_q)$ and $\mathcal{Q}$ a quadric of $\mathbb{P}^4(\mathbb{F}_q)$ such that $\mathcal{X} \neq \lambda\mathcal{Q}$, then

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 2q^2 + 3q + 1,\ 2q^2 + 2q + 1$$

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 2q^2 + q + 1,\ 2q^2 + 1,$$

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 2q^2 - q + 1$$

Theorem Let $\mathcal{X}$ be a quadric in $\mathbb{P}^4(\mathbb{F}_q)$ and $\mathcal{Q}$ another quadric in $\mathbb{P}^4(\mathbb{F}_q)$. If X is :
–non-degenerate, then

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq 2q^2 + 3q + 1.$$

–degenerate with $r(X) = 3$, then

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq 4q^2 + 3q + 1.$$

–degen. with $r(X) = 4$ and $g(X) = 2$ then,

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) \leq 4q^2 + 1.$$

These bounds are the best possible.

IV- Applications to Coding Theory

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

$$\begin{array}{rcl} c : \mathcal{F}_h(V, \mathbb{F}_q) & \longrightarrow & \mathbb{F}_q^N \\ f & \longmapsto & c(f) = (f(P_1), \ldots, f(P_N)) \end{array}$$

$$C_h(X) = \mathrm{Im}\, c$$

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

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

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

$$\mathrm{dist} C_h(X) = \min_{f \in \mathcal{F}_h} \{w(c(f))\}$$

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

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

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

Weights Distribution of $C_2(\mathcal{H}_3)$

- $\boxed{w_1 = q^2 - 2q + 1}$.
  The codewords $<< w_1 >>$:
  –union of 2 tan planes and l bisecant
  –hyperbolic quadric containing || and = lines of X.

- $\boxed{w_2 = q^2 - q}$.
  The codewords $<< w_2 >>$:
  –hyperbolic quadric containing exactly two lines in distinct regulus and the q other lines of one regulus are bisecants of X.
  –union of two tangent planes of X and the line of intersection is contained in X.
  –union of two planes one is tan., the second is non-tan. to X and the line of intersection intersecting X at a single point.

- $\boxed{w_3 = q^2 - q + 1}$.
  The codewords $<< w_3 >>$:
  union of two planes one tan., the second non-tan. to X and the line of intersection intersecting X at two points.

Weights Distribution of $C_2(\mathcal{E}_3)$

- $\boxed{w_1 = q^2 - 2q - 1}$
  The codewords $<< w_1 >>$:
  –union of two planes non-tan and l disjoint to X.
  –hyperbolic quadrics with all lines of one regulus are bisecants.
  –degenerate quadrics of rank 3 (i.e. $q+1$ lines) with the vertex no contained in X et and all the $q+1$ lines are bisecants.

- $\boxed{w_2 = q^2 - 2q}$
  The codewords $<< w_1 >>$: quadrics which are union of two non-tan. planes to X and the line of intersection intersecting X at two points.

- $\boxed{w_3 = q^2 - 2q + 1}$

Table 6: The first 5 weights of $C_2(X)$.

Numb	$\mathcal{Q}$	$\mathcal{P} \cap \mathcal{X}$	w_i
1	2 n-tan $\mathcal{H}$	n-sin. conic	$q^3 - q^2 - 2q$
2	2 n-tan	sin. cve (r=2)	$q^3 - q^2 - q$
3	1t+1n-tan	$\Pi_0\mathcal{H}_1$	$q^3 - q^2$
4	1t+1n-tan	sin. cve (r=2)	$q^3 - q^2 + q$
	2tan	$\Pi_0\mathcal{H}_1$	
5	2 n-tan $\mathcal{E}$	n-sin. conic	$q^3 - q^2 + 2q$

Tuesday 02/27/2007 (Seminar of GRIM, Toulon)

Theorem [Ax, 1964]

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

V-Generalization to quadrics in $\mathbb{P}^n(\mathbb{F}_q)$

Theorem[E., Hallez, Rodier, Storme]
Let X be a quadric in $\mathbb{P}^n(\mathbb{F}_q)$ with $n \geq 5$, If

$$|X \cap Q| \geq q^{n-2} + 3q^{n-3} + 3q^{n-4} + 2q^{n-5} + ... + 2q + 1,$$

then there exist a quadric consisting of two hyperplanes.

• 5.1 X is a non-degenerate quadric in $\mathbb{P}^{2l+1}(\mathbb{F}_q)$

$$|X \cap Q| \leq 2q^{n-2} + \pi_{n-3} + 2q^{\frac{n-1}{2}} - q^{\frac{n-3}{2}}$$

Weights Distribution of $C_2(\mathcal{H}_{2l+1})$

dist$C_h(X)$: D. Leep, in 1999, FFA (7).

$$\text{dist}C_h(X) \geq q^{2l} - q^{2l-1} - q^l + q^{l-1}$$

Table 6: The first 6 weights of $C_2(X)$.

Numb	$\mathcal{Q}$	$\Pi_{2l-1} \cap \mathcal{X}$	w_i
1	2 tan.	$\mathcal{H}_{2l-1}$	$q^{2l} - q^{2l-1} - q^l + q^{l-1}$
2	1t+1n-tan	$\Pi_0 \mathcal{P}_{2l-2}$	$q^{2l} - q^{2l-1}$
	2tan	$\Pi_1 \mathcal{H}_{2l-3}$	
3	1t+1n-tan	$\mathcal{H}_{2l-1}$	$q^{2l} - q^{2l-1} + q^{l-1}$
4	2 n-tan.	$\mathcal{E}_{2l-1}$	$q^{2l} - q^{2l-1} + q^l - q^{l-1}$
5	2 n-tan	$\Pi_0 \mathcal{P}_{2l-2}$	$q^{2l} - q^{2l-1} + q^l$
6	2 n-tan	$\mathcal{H}_{2l-1}$	$q^{2l} - q^{2l-1} + q^l + q^{l-1}$

Weights distribution of $C_2(\mathcal{E}_{2l+1})$

dist$C_h(X)$: D. Leep, in 1999, FFA (7).

$$\text{dist}C_h(X) \geq q^{2l} - q^{2l-1} - 3q^l + 3q^{l-1}$$

Table 7: The first 7 weights of $C_2(\mathcal{E}_{2l+1})$.

Numb	$\mathcal{Q}$	$\Pi_{2l-1} \cap \mathcal{X}$	w_i
1	2 n-tan.	$\mathcal{E}_{2l-1}$	$q^{2l} - q^{2l-1} - q^l - q^{l-1}$
2	2 n-tan	$\Pi_0\mathcal{P}_{2l-2}$	$q^{2l} - q^{2l-1} - q^l$
3	1t+1n-tan	$\mathcal{H}_{2l-1}$	$q^{2l} - q^{2l-1} - q^l + q^{l-1}$
4	2 n-tan.	$\mathcal{E}_{2l-1}$	$q^{2l} - q^{2l-1} - q^{l-1}$
5	1t+1n-tan	$\Pi_0\mathcal{P}_{2l-2}$	$q^{2l} - q^{2l-1}$
	2tan	$\Pi_1\mathcal{E}_{2l-3}$	
6	2 tan	$\mathcal{E}_{2l-1}$	$q^{2l} - q^{2l-1} + q^l - q^{l-1}$
7	2 tan	$\Pi_0\mathcal{P}_{2l-2}$	$q^{2l} - q^{2l-1} + q^l$

Theorem [E. Hanja, Rodier Storme]
Let $\mathcal{X}$ be a non-degenerate quadric in $\mathbb{P}^{2l+1}(\mathbb{F}_q)$ with $l \in \mathbb{N}^\star$. Then all the weights of the code $C_2(X)$ defined on X are divisible by q^{l-1}.

• 5.2 X is a non-degenerate quadric in $\mathbb{P}^{2l+2}(\mathbb{F}_q)$

dist$C_h(X)$: D. Leep, in 1999, FFA (7).

$$\text{dist}C_h(X) \geq q^{2l+1} - q^{2l} - q^{l+1}$$

Table 8: the first 5 weights of $C_2(\mathcal{P}_{2l+2})$.

Numb	$\mathcal{Q}$	$\Pi_{2l} \cap \mathcal{X}$	w_i
1	2 n-tan. $\mathcal{H}$	$\mathcal{P}_{2l}$	$q^{2l+1} - q^{2l} - 2q^l$
2	2 n-tan	$\Pi_0\mathcal{H}_{2l-1}$	$q^{2l+1} - q^{2l} - q^l$
	1tan+1n-tan	$\mathcal{P}_{2l}$	
	2 tan	$\Pi_0\mathcal{E}_{2l-1}$	
3	2 n-tan	$\mathcal{P}_{2l}$	$q^{2l+1} - q^{2l}$
	1tan+1n-tan	$\Pi_0\mathcal{H}_{2l-1}$	
	1tan+1n-tan.	$\Pi_0\mathcal{E}_{2l-1}$	
	2 tan	$\Pi_1\mathcal{P}_{2l-2}$	
4	2 n-tan. $\mathcal{H}$	$\Pi_0\mathcal{E}_{2l-1}$	$q^{2l+1} - q^{2l} + q^l$
	1tan+1n-tan	$\mathcal{P}_{2l}$	
	2 tan	$\Pi_0\mathcal{H}_{2l-1}$	
5	2 n-tan $\mathcal{E}$	$\mathcal{P}_{2l}$	$q^{2l+1} - q^{2l} + 2q^l$

Theorem [E., Hanja, Rodier, Storme]
Let $\mathcal{X}$ be a non-degenerate quadric in $\mathbb{P}^{2l+2}(\mathbb{F}_q)$ and $l \in \mathbb{N}^\star$. Then all the weights of the code $C_2(X)$ defined on X are divisible by q^l.

VII-Conclusion

Theorem [E., San, Xing]
Let $\mathcal{Q}_1$ and $\mathcal{Q}_2$ be two quadrics in $\mathbb{P}^n(\mathbb{F}_q)$ with no common d'hyperplane.
Then:

$$\boxed{|\mathcal{Q}_1 \cap \mathcal{Q}_2| \leq 4q^{n-2} + \pi_{n-3}}$$

Conjecture [E., San, Xing]
Let $X \subset \mathbb{P}^n(\mathbb{F}_q)$ be an arbitrary algebraic set of dimension s and degree d. Then the number of X is such that:

$$\boxed{\#X(\mathbb{F}_q) \leq dq^s + \pi_{s-1}.}.$$

References

E. J. F. Primrose, Quadrics in finite geometries. Proc. Camb. Phil. Soc., (1951), 299-304.

F. A. B. Edoukou, Codes defined by forms of degree 2 on quadric surfaces. IEEE, Trans. Inf. Theory, Vo. 54, (2), (2008), 860-864.

F. A. B. Edoukou,Codes defined by forms of degree 2 on quadric varieties in $\mathbb{P}^4(\mathbb{F}_q)$. Contemp. Mathematics 487, (2009), 21-32.

F. A. B. Edoukou, A. Hallez, F. Rodier and L. Storme, A study of intersections of quadrics having applications on the small weight codewords of the functional codes. $C_2(\mathcal{Q})$, $\mathcal{Q}$ a non-singular quadric. J.P.A.A, 214, (2010), 1729-1939.

F. A. B. Edoukou, S. Ling and C. Xing, Intersection of two quadrics with no common on hyperplanes. Submitted.

Thank you for your attention