Caps of order $3q^2$ in affine 4-space in characteristic 2

Yves Edel
Mathematisches Institut der Universität
Im Neuenheimer Feld 288
69120 Heidelberg (Germany)

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

September 2, 2003

Abstract

We prove that a class of q-ary dual BCH-codes in characteristic 2 produce caps in $AG(4,q)$. This is the first family of caps of order $3q^2$ in $PG(4,q)$. It is proved that our caps are complete in $PG(4,q)$. We determine the weight distribution of the codes generated by the caps, via a close link to the binary Kloosterman codes, the dual Mélas codes.

1 Introduction

A **cap** in projective geometry $PG(n,q)$ is a set of points no three of which are collinear.

Theorem 1. *Let $q = 2^f$, where f is odd, and $F = \mathbb{F}_{q^4}$. Identify the points in $AG(4,q)$ with the points $(1,x)$, $x \in F$. The points $(1,x)$ where $x = 0$ or x is a $3(q^2+1)$-th root of unity form a $(3q^2+4)$-cap $\mathcal{K}_q \subset AG(4,q)$.*

The construction of large caps in $PG(4,q)$ or $AG(4,q)$ appears to be a difficult problem. The best known asymptotic result is a family of caps of order $2.5q^2$ in $PG(4,q)$ in odd characteristic (see [3, 10]). Here we speak of order cq^2 if the number of points is a polynomial in q with cq^2 as leading term. In characteristic 2 it had hitherto not been possible to construct families of caps in $PG(4,q)$ of order more than $2q^2$. This asymptotic value is trivial to reach (the union of two ovoids in hyperplanes is a $(2q^2+2)$-cap in $PG(4,q)$). A survey of the problem is in [2], and [7] is a more general survey concerning related questions.

Theorem 1 shows that caps of order $3q^2$ can be constructed in characteristic 2, more precisely in $AG(4,q)$, where $q=2^f,\ f$ odd.

Moreover the cap $\mathcal{K}_q$ constructed in Theorem 1 essentially is a cyclic code. Clearly $\mathcal{K}_q$ admits the cyclic group of order $3(q^2+1)$ as a group of automorphisms, with $(1,0)$ as fixed point and with regular action on the remaining points of $\mathcal{K}_q$. In the language of the theory of cyclic codes we can describe $\mathcal{K}_q \setminus \{(1,0)\}$ as the dual of the q-ary BCH-code of length $3(q^2+1)$ and defining set $A=\{0,1\}$ of exponents (see [1, 8]). The claim that $\mathcal{K}_q \setminus \{(1,0)\}$ is a cap is equivalent to the statement that the BCH-code has minimum distance 4. This will be proved in Section 2. In Section 3 we prove that $\mathcal{K}_q$ is complete in $PG(4,q)$. The maximum hyperplane section, equivalently the minimum distance of the code C_q generated by $\mathcal{K}_q$, will be determined in Section 4.

Theorem 2. *The cap $\mathcal{K}_q$ is complete in $PG(4,q)$. All intersection sizes of $\mathcal{K}_q$ with hyperplanes of $PG(4,q)$ are multiples of 4. Let ι_q be the maximum hyperplane intersection size of $\mathcal{K}_q$. Then $\iota_2=8,\ \iota_8=32,\ \iota_{32}=120$ and, for $q>32,\ \iota_q=3(q+1+t)$, where t is the largest integer smaller than $2\sqrt{q}$, which is congruent to 3 mod 4.*

Let C_q be a $[3q^2+4,5]_q$-code whose generator matrix has as columns representatives of the points of $\mathcal{K}_q$ (the extended dual BCH-code). We exhibit a close link between the weight distribution of C_q and the weight distribution of the $2f$-dimensional binary Kloosterman code, the dual Mélas code. As the weight distribution of the Kloosterman codes is known by [9] we determine the weight distribution of C_q.

The theory of sequences with low crosscorrelation motivated the study of binary cyclic codes with minimum distance 5, see [5] for the link to coding theory and [6] for a survey. Theorem 1 shows that interesting caps may be constructed as duals of BCH-codes. This raises the question to determine which cyclic codes have minimum distance ≥ 4. Another family of cyclic caps was recently constructed in [4].

2 Proof of Theorem 1

Let us fix notation. We have $q = 2^f$, f odd, $F = \mathbb{F}_{q^4}$, $K = \mathbb{F}_{q^2}$. Denote by $Tr_{a,b}$ the trace : $\mathbb{F}_a \longrightarrow \mathbb{F}_b$ and by $N : F \longrightarrow K$ the norm. Let $W \subset F$ be the group of (q^2+1)-st roots of unity ($w \in W \iff N(w) = 1$). Denote the points of $\mathcal{K}_q$ as $P(0) = (1, 0)$ and $P(a, w) = (1, aw)$, where $0 \neq a \in \mathbb{F}_4$ and $w \in W$.

Lemma 1. *The numbers* $3,\ q-1$ *and* q^2+1 *are pairwise coprime.*

The trivial Lemma 1 implies that the points $P(0)$ and $P(a, w)$ are pairwise different. Moreover, if $(a_1, w_1) \neq (a_2, w_2)$ $(0 \neq a_i \in \mathbb{F}_4, w_i \in W)$, then $\dfrac{a_1w_1}{a_2w_2} \notin \mathbb{F}_q$. It follows that $P(0)$ is not collinear with two of the remaining points of $\mathcal{K}_q$. It suffices to show that the $P(a, w)$ form a cap.

Lemma 2. *Let $0 \neq \alpha \in K$. The following are equivalent:*

- *There exists $w \in W$ such that $Tr_{q^4,q^2}(w) = \alpha$*
- $Tr_{q^2,4}(1/\alpha) \in \mathbb{F}_4 \setminus \mathbb{F}_2$.
- $Tr_{q^2,2}(1/\alpha) = 1$.

Proof. It is clear that the second and third condition are equivalent, and $Tr_{q^4,q^2}(w) = w + 1/w = \alpha$ is equivalent with $(w/\alpha)^2 + (w/\alpha) + 1/\alpha^2 = 0$. Clearly, $w = 1$ is not a solution. Let $Tr_{q^2,2}(1/\alpha) = 0$. Then the solutions of $x^2 + x + 1/\alpha^2 = 0$ are in K. It follows $w \in K$, contradiction. This shows that there is no solution in this case. As there are $q^2/2$ elements $\alpha \in K$ such that $Tr_{q^2,2}(1/\alpha) = 1$ and each contributes at most two solutions $1 \neq w \in W$, we must have equality. $\square$

Lemma 3. $Tr_{q^2,2}(\mathbb{F}_q) = 0$. *We have $\mathbb{F}_q = \mathbb{F}_q^{\perp}$ with respect to the bilinear form defined by $Tr_{q^2,2}$ on K.*

Lemma 3 is obvious as $\lambda^q = \lambda$ for $\lambda \in \mathbb{F}_q$.

Let $P(a_1, w_1),\ P(a_2, w_2),\ P(a_3, w_3)$ be different points of $\mathcal{K}_q$, which are collinear. Let the coefficients of an affine linear combination be $1, \lambda, \lambda + 1$, where $\lambda \in \mathbb{F}_q \setminus \mathbb{F}_2$. This yields the equation

$$(\lambda + 1)a_1 w_1 = a_2 w_2 + \lambda a_3 w_3.$$

Assume at first $a_i = a_j$ for some $i \neq j$. Using the automorphism group we can assume $a_2 = a_3 = 1$ and $w_3 = 1$. The equation is

$$(\lambda + 1)a_1 w_1 = w_2 + \lambda.$$

As the second and third point are different, it follows $w_2 \neq 1$. Application of the norm ($N(x) = x^{q^2+1}$) to both sides yields $(\lambda^2 + 1)a_1^2 = \lambda^2 + 1 + \lambda\alpha$, where $\alpha = Tr_{q^4,q^2}(w_2)$. We have $\alpha \neq 0$ as $w_2 \neq 1$. It follows $a_1 \neq 1$. The equation

$$\frac{1}{\alpha}(a_1^2 + 1) = \frac{\lambda}{\lambda^2 + 1} = \frac{1}{\lambda + 1} + \frac{1}{(\lambda + 1)^2}$$

shows $(a_1^2 + 1)Tr_{q^2,4}(1/\alpha) = Tr_{q^2,4}(\frac{1}{\lambda+1} + \frac{1}{(\lambda+1)^2}) = Tr_{q^2,2}(\frac{1}{\lambda+1}) = 0$ (see Lemma 3). It follows $Tr_{q^2,4}(1/\alpha) = 0$, contradicting Lemma 2.

Assume now the a_i are pairwise different (and nonzero) elements of $\mathbb{F}_4$. We can choose notation such that

$$(\lambda + 1)w_1 = \omega w_2 + \lambda\overline{\omega}.$$

Here ω and $\overline{\omega} = \omega^2$ are the primitive elements of $\mathbb{F}_4$. Application of N yields $\lambda^2 + 1 = \overline{\omega} + \lambda^2\omega + \lambda\alpha$, where $\alpha = Tr_{q^4,q^2}(w_2)$. We have $\alpha \neq 0$ as otherwise $\lambda \in \mathbb{F}_4$, which is impossible as $\mathbb{F}_q \cap \mathbb{F}_4 = \mathbb{F}_2$. An equivalent form of the equation is $\lambda^2\overline{\omega} + \lambda\alpha + \omega = 0$. Multiplication by $\overline{\omega}/\alpha^2$ yields $x^2 + x + 1/\alpha^2 = 0$, where $x = \lambda\overline{\omega}/\alpha$. This yields $Tr_{q^2,2}(1/\alpha) = 0$, contradicting Lemma 2.

3 Completeness

In this section we prove that $\mathcal{K}_q \subset PG(4, q)$ is a complete cap.

Proposition 1. *Each point in the hyperplane avoided by $\mathcal{K}_q$ is collinear with two points of $\mathcal{K}_q$.*

Proof. Consider point $(0,x)$. We want to find $0 \neq \lambda \in \mathbb{F}_q, 0 \neq a \in \mathbb{F}_4$ and $w_1, w_2 \in W$ such that $(0,x) = \lambda(1, aw_1) + \lambda(1, aw_2)$, equivalently $x = \lambda a(w_1 + w_2)$. Applying the norm we obtain $N(x) = \lambda^2 a^2 Tr_{q^4,q^2}(w)$, where $w = w_1/w_2 \neq 1$. Assume this equation is satisfied. Then x and $\lambda a(w_1 + w_2)$ have the same norm. As the elements of W are precisely those of norm 1, we can find $w' \in W$ such that $x = \lambda a(w_1 w' + w_2 w')$ and are done. We have seen that it suffices to find λ, a, w such that $N(x) = \lambda^2 a^2 Tr_{q^4,q^2}(w)$. We have $Tr_{q^4,q^2}(w) \neq 0$ as $w \neq 1$. Let $\alpha = N(x)/(\lambda^2 a^2)$. By Lemma 2 we need to find α, a such that $Tr_{q^2,2}(1/\alpha) = 1$, where

$$\frac{1}{\alpha} = \frac{\lambda^2 a^2}{N(x)}.$$

If $Tr_{q^2,4}(\lambda^2/N(x)) \neq 0$ we can choose $a \in \mathbb{F}_4$ appropriately and are done. Assume $Tr_{q^2,4}(\lambda^2/N(x)) = 0$ for all $\lambda \in \mathbb{F}_q$. Then $Tr_{q^2,2}(\lambda^2/N(x)) = 0$, and $1/N(x)$ is in the dual of $\mathbb{F}_q$ in the trace form defined by $Tr_{q^2,2}$ on K. By Lemma 3 this dual is precisely $\mathbb{F}_q$. It follows $N(x) \in \mathbb{F}_q$. Choose $\lambda^2 = N(x)$. Then $Tr_{q^2,4}(\lambda^2/N(x)) = Tr_{q^2,4}(1) \neq 0$, contradiction. □

Proposition 2. *Each point $(1,x) \notin \mathcal{K}_q$, where $y = N(x) = x^{q^2+1}$ either is in $\mathbb{F}_4$ or is not a $(q+1)$-st root of unity, is collinear with two points of $\mathcal{K}_q$.*

Proof. Consider points $(1,x)$. Projection from $P(0)$ shows that we are done if the order of x divides $3(q-1)(q^2+1)$. From now on we assume the order of y does not divide $3(q-1)$. In particular $y \notin \mathbb{F}_q, y \notin \mathbb{F}_4$ and $y^{q+1} \neq 1$.

We want to find $\lambda, \mu \in \mathbb{F}_q, a_i \in \mathbb{F}_4^*, w_i \in W$ such that

$$(1,x) = \lambda(1, a_1 w_1) + \mu(1, a_2 w_2),$$

equivalently $x = \lambda a_1 w_1 + (\lambda+1) a_2 w_2$. Applying the norm we obtain the equivalent condition

$$y = \lambda^2 a_1^2 + (\lambda^2+1) a_2^2 + \lambda(\lambda+1) a_1 a_2 Tr_{q^4,q^2}(w) \tag{1}$$

for some $w \in W$. Let $Tr_{q^4,q^2}(w) = \alpha$. Choose $a_1 = a_2 = a$. We have $\alpha \neq 0$ as otherwise $y \in \mathbb{F}_4$. By Lemma 2 we need to find constants such that $Tr_{q^2,2}(1/\alpha) = 1$, where

$$\frac{1}{\alpha} = \frac{(\lambda^2+\lambda)a^2}{y + a^2}.$$

Assume $Tr_{q^2,2}(1/\alpha) = 0$ for all $\lambda \in \mathbb{F}_q$. Repeated application yields

$$Tr_{q^2,2}(\lambda a^2/(y+a^2)) = Tr_{q^2,2}(\lambda^2 a^2/(y+a^2)) = \cdots = Tr_{q^2,2}(\lambda^{2^{f-1}} a^2/(y+a^2)).$$

As we have an odd number of terms it follows

$$Tr_{q^2,2}(\lambda a^2/(y+a^2)) = Tr_{q^2,2}(la^2/(y+a^2)) = l \cdot Tr_{q^2,2}(a^2/(y+a^2)) \qquad (2)$$

where $l = Tr_{q,2}(\lambda)$.

Assume $Tr_{q^2,2}(a^2/(y+a^2)) = 0$. By equation 2, $Tr_{q^2,2}(\lambda a^2/(y+a^2)) = 0$ for all $\lambda \in \mathbb{F}_q$. Because of Lemma 3 this implies $a^2/(y+a^2) \in \mathbb{F}_q$. We obtain $y/a^2 \in \mathbb{F}_q$. It follows that the order of x divides $3(q-1)(q^2+1)$. This case has been taken care of already.

We can assume $Tr_{q^2,2}(a^2/(y+a^2)) = 1$. Equation 2 says

$$Tr_{q^2,2}(\lambda a^2/(y+a^2)) = Tr_{q,2}(\lambda).$$

Factoring $Tr_{q^2,2}$ over $Tr_{q,2}$ we obtain

$$Tr_{q,2}(\lambda(\frac{a^2}{y+a^2} + \frac{a}{y^q+a} + 1)) = 0$$

for all $\lambda \in \mathbb{F}_q$. The second factor under the trace must vanish. This simplifies to $y^{q+1} = 1$. $\square$

¿From now on we assume $y^{q+1} = 1,\ y \notin \mathbb{F}_4$ and we need to choose $a_1 \neq a_2$. The choice $a_1 = \omega, a_2 = \overline{\omega}$ in equation 1 yields

$$\frac{1}{\alpha} = \frac{\lambda^2 + \lambda}{y + \lambda^2 + \omega}$$

In case $a_1 = \overline{\omega}, a_2 = \omega$ an equivalent expression results, obtained by the substitution $\lambda \mapsto \lambda + 1$. Cases $\{a_1, a_2\} = \{1, \omega\}$ and $\{a_1, a_2\} = \{1, \overline{\omega}\}$ lead to similar expressions, where in the denominator y is replaced by ωy or $\overline{\omega} y$. The choice $\lambda = 0$ or $\lambda = 1$ leads to $y \in \mathbb{F}_4$, a case we have excluded. We can assume $\lambda \notin \mathbb{F}_2$. This implies that the expressions above make sense as $y \neq \lambda^2 + \omega$. In fact, assume $y = \lambda^2 + \omega$. Then $1 = y^{q+1} = (\lambda^2 + \omega)(\lambda^2 + \overline{\omega})$, hence $\lambda^2(\lambda^2 + 1) = 0$. We sum up:

Lemma 4. *The cap $\mathcal{K}_q \subset PG(4,q)$ is complete if and only if for every $y \in K$ such that $y^{q+1} = 1,\ y \notin \mathbb{F}_4$ we can find $\lambda \in \mathbb{F}_q \setminus \mathbb{F}_2$ and $0 \neq a \in \mathbb{F}_4$ such that*

$$Tr_{q^2,2}(\frac{\lambda^2 + \lambda}{ay + \omega + \lambda^2}) = 1.$$

Lemma 4 is a motivation to study the rational function $\rho(X)=\sum_{\lambda\in\mathbb{F}_q}\frac{\lambda^2+\lambda}{X+\lambda^2}$ in the variable X. The common denominator is $\prod_\lambda(X+\lambda)=X^q+X$. The numerator

$$\sum_\lambda(\lambda^2+\lambda)\prod_{\mu\neq\lambda^2}(X+\mu)$$

is a polynomial of degree $\leq q-1$, which maps $\lambda^2\mapsto(\lambda^2+\lambda)$, for all $\lambda\in\mathbb{F}_q$. The polynomial $X^{q/2}+X$ affords the same mapping. Because of the unicity of the interpolating polynomial our numerator is $X^{q/2}+X$. We have seen

$$\rho(X)=\frac{X^{q/2}+X}{X^q+X}.$$

In view of Lemma 4 and replacing y by y^2 (in order to avoid square roots in the formulas) the following is obtained:

Lemma 5. *Let $\rho(X)=(X^{q/2}+X)/(X^q+X)$. In order to prove the completeness of $\mathcal{K}_q$ it is sufficient to show that for every $(q+1)$-st root of unity $y\in K\setminus\mathbb{F}_4$ we have*

$$Tr_{q^2,q}(\sum_{0\neq a\in\mathbb{F}_4}\rho(ay^2+\omega))=1.$$

Proof. In fact, in the contrary case we would have in particular $Tr_{q^2,2}(\rho(ay^2+\omega)=0$ for all $0\neq a\in\mathbb{F}_4$ and therefore also $Tr_{q^2,2}(\sum_{0\neq a\in\mathbb{F}_4}\rho(ay^2+\omega))=0$, which is incompatible with the expression in the statement of the lemma. $\square$

We have

$$\rho(ay^2+\omega)=\frac{ay^2+ay^q}{1+ay^2+a^2y^{2q}}=\frac{ay^2+a/y}{1+ay^2+a^2/y^2}$$

and

$$Tr_{q^2,q}(\rho(ay^2+\omega))=\frac{ay^2+a/y+a^2/y^2+a^2y}{1+ay^2+a^2/y^2}=$$

$$=1+\frac{1+a/y+a^2y}{1+ay^2+a^2/y^2}=1+\frac{1}{1+a^2y+a/y}.$$

Observe that these expressions make sense as the denominator does not vanish. If it vanished, ay^2 would satisfy a quadratic equation with coefficients in $\mathbb{F}_2$, resulting in the contradiction $y\in\mathbb{F}_4$.

We have seen

$$Tr_{q^2,q}(\rho(ay^2+\omega)) = 1 + \frac{1}{1+Tr_{q^2,q}(a^2y)}.$$

Summing up over all a we obtain $1+\sum_a \frac{1}{1+Tr_{q^2,q}(a^2y)}$. It suffices to show that the last sum vanishes. Writing it with the obvious common denominator the numerator is

$$(1+y+\frac{1}{y})(1+\omega y+\overline{\omega}/y)+(1+y+\frac{1}{y})(1+\overline{\omega}y+\omega/y)+(1+\omega y+\overline{\omega}/y)(1+\overline{\omega}y+\omega/y)$$

which simplifies to 0. This completes the proof of completeness, by Lemma 5.

4 Hyperplane sections and codes

In this section we determine ι_q. Moreover we show how to determine the weight distribution of C_q.

Write the points of $AG(4,q)$ as $(1,x),\ x\in F$. Let $\tau = Tr_{q^4,q} : F \longrightarrow \mathbb{F}_q$ be the trace. The hyperplanes of $PG(4,q)$ aside of the hyperplane described by the first coordinate are coordinatized by pairs (u,c), where $0\neq u\in F, c\in\mathbb{F}_q$. Point $(1,x)$ belongs to hyperplane $H=H_{u,c}$ if and only if $\tau(ux)=c$. In particular $P(0)\in H$ if and only if $c=0$, and $P(a,w)\in H$ if and only if $\tau(uaw)=c$. Observe that $H_{u,c}=H_{\lambda u,\lambda c}$ for every $0\neq\lambda\in\mathbb{F}_q$.

A family of 2-weight codes

The following lemma will be used in the proof of Theorem 3 below.

Lemma 6. *Each $0\neq z\in K$ can be written in the form $z=\lambda z_2$, where $\lambda\in\mathbb{F}_q,\ z_2^{q+1}=1$, in a unique way, and $z^{q-1}=1/z_2^2$.*

Let a $(q+1)$-st root of unity z_2 be given. If $z_2\neq 1$, there are $q/2$ elements $\lambda\in\mathbb{F}_q$ such that $Tr_{q^2,2}(\lambda z_2)=1$. If $z_2=1$ there is no such λ.

Proof. The first statements follow from the fact that the multiplicative group of K is the direct product of the multiplicative group of $\mathbb{F}_q$ and of the cyclic subgroup of order $q+1$. Let $z_2\neq 1$. Assume $Tr_{q^2,2}(\lambda z_2)=0$ for all $\lambda\in\mathbb{F}_q$. By Lemma 3, $z_2\in\mathbb{F}_q^{\perp}=\mathbb{F}_q$, which is a contradiction. □

Theorem 3. *Let A be a set of $(q+1)$-st roots of unity in K, $|A| = d$. Let $D(A)$ be the 4-dimensional q-ary code of length $d(q^2+1)$ defined by its generator matrix whose columns are the points $Q(a,w), a \in A, w^{q^2+1} = 1$, where $Q(a,w)$ is the point in $PG(3,q)$ generated by $aw \in F$. Then $D(A)$ is a 2-weight code with weights $dq^2-(d-1)q$ and $d(q^2-q)$. There are $d(q-1)(q^2+1)$ words of weight $dq^2-(d-1)q$ and $(q+1-d)(q-1)(q^2+1)$ words of weight $d(q^2-q)$.*

Proof. Consider intersections with hyperplane $H' = H'_{\langle u\rangle}$ of $PG(3,q)$, where $Q(a,w) \in H'$ if and only if $\tau(uaw) = 0$. The number of points $Q(a,w) \in H'$ remains unchanged if we multiply u by an element of W. It can therefore be assumed that $u \in K$. Factorize the trace:

$$\tau(uaw) = Tr_{q^2,q}(ua\alpha) = ua\alpha + u^q a^q \alpha^q = 0,$$

where $\alpha = Tr_{q^4,q^2}(w)$. If $\alpha = 0$, then $w = 1$ and $0 \neq a \in A$ arbitrary. This gives us d points on H'. Let now $\alpha \neq 0$. We have to count solutions of the equation

$$(1/\alpha)^{q-1} = a^{q-1}v = v/a^2,$$

where $v = u^{q-1}$ and $Tr_{q^2,2}(1/\alpha) = 1$ (see Lemma 2). Observe $v^{q+1} = a^{q+1} = 1$. We distinguish two cases. Assume at first $v = a_0^2$ for $a_0 \in A$. The choice $a = a_0$ gives no solution α such that $Tr_{q^2,2}(1/\alpha) = 1$. In each of the remaining $d-1$ choices for a we obtain $q/2$ solutions for α (see Lemma 6), each of which contributes 2 solutions for w. The hyperplane intersection size is $d+0+(d-1)\cdot 2\cdot q/2 = (d-1)q+d$ in this case.

Assume $v \notin A^2$. This time each of the d choices for a yields $q/2$ choices for $\alpha \neq 0$ and therefore q solutions for w. The size of the hyperplane intersection is $d + dq$ in this case. □

Corollary 1. *Let D_q be the q-ary cyclic code of length $3(q^2+1)$ with defining set $\{1\}$. Then D_q is the shortened code of C_q with respect to the coordinate indexed by $P(0)$ (the 4-dimensional subcode of C_q consisting of all codewords of C_q which vanish in that coordinate, with this coordinate removed).*

Further $D_q, q > 2$ is a 2-weight code with weights $3q^2-3q$ and $3q^2-2q$. In particular D_q is a $[3(q^2+1), 4, 3q(q-1)]_q$-code.

In case $q = 2$ the second case in the proof of Theorem 3 does not occur. It follows that D_2 is a constant-weight code. Clearly D_2 is the Simplex code $[15, 4, 8]_2$.

Factorize τ over $K : \tau(x) = Tr_{q^2,q}(Tr_{q^4,q^2}(x))$. As in the proof of Theorem 3 we can assume $u \in K$, and $Tr_{q^4,q^2}(uaw) = uaw + ua/w = ua\alpha$, where $\alpha = Tr_{q^4,q^2}(w) = w + 1/w$.

We wish to count the number of points of $\mathcal{K}_q$ on hyperplanes $H = H_{u,c}$, where $P(a, w) \in H$ if and only if $\tau(uaw) = c$. Case $c = 0$ is covered by Corollary 1. Let $c \neq 0$. Upon multiplying u by a suitable factor from $\mathbb{F}_q$ we can assume $c = 1$.

Lemma 7. *Let $x \in K$. Then the following are equivalent:*

- $Tr_{q^2,q}(x) = 1$,
- $x = \dfrac{1}{z+1}$, *where* $z \neq 1,\ z^{q+1} = 1$.

Lemma 7 follows from a direct calculation. It implies that $P(a, w) \in H$ if and only if $ua\alpha = 1/(z + 1)$, where $z^{q+1} = 1$ and $Tr_{q^2,2}(1/\alpha) = Tr_{q^2,2}(u(z + 1)a) = 1$. For given $1 \neq z, z^{q+1} = 1$ the number of solutions a is either 0 or 2. It is 0 if $u(z+1) \in \mathbb{F}_4^\perp$ with respect to the bilinear form defined by $Tr_{q^2,2}$ on K, it is 2 otherwise. Each value of α contributes precisely two solutions w. We see that each z contributes either 0 or 4 to the intersection with hyperplane H. The contribution is 4 if and only if $u(z+1) \notin \mathbb{F}_4^\perp$ (with respect to $Tr_{q^2,2}$). In particular all of these hyperplane section sizes are multiples of 4 and at most $4q$. Let $|\mathcal{K}_q \cap H| = 4s$.

Lemma 8. *Let $l \in K$. Then l is orthogonal to $\mathbb{F}_4$ with respect to the trace form defined by $Tr_{q^2,2}$ if and only if $Tr_{q^2,4}(l) = 0$.*

Proof. Orthogonality means $Tr_{q^2,2}(l) = Tr_{q^2,2}(\omega l) = 0$. Assume $Tr_{q^2,2}(l) = 0$. Then $Tr_{q^2,2}(\omega l) = \omega Tr_{q^2,4}(l) + \overline{\omega} Tr_{q^2,4}(l) = Tr_{q^2,4}(l)$. □

By Lemma 8, z contributes to the hyperplane section size if and only if $Tr_{q^2,4}(u(z+1)) \neq 0$. It follows that s equals the number of $z,\ z^{q+1} = 1$ such that $Tr_{q^2,4}(u(z + 1)) \neq 0$. Equivalently $q + 1 - s$ is the number of such z satisfying $Tr_{q^2,4}(u(z+1)) = 0$.

Let $u(z + 1) = c_1\omega + c_2$. Here $c_1, c_2 \in \mathbb{F}_q$ are uniquely determined as $1, \omega$ form a basis of K over $\mathbb{F}_q$. The last trace condition is equivalent with $Tr_{q,2}(c_1) = Tr_{q,2}(c_2) = 0$. We count such c_1, c_2 satisfying

$$(\frac{c_1\omega + c_2}{u} + 1)^{q+1} = 1.$$

This is equivalent with

$$c_1^2 + c_1c_2 + c_2^2 + u^q(c_1\omega + c_2) + u(c_1\overline{\omega} + c_2) = 0.$$

With $u = u_1\omega + u_2$ this becomes

$$c_1^2 + c_1c_2 + c_2^2 + c_1u_2 + c_2u_1 = 0.$$

Let $x = c_1 + u_1, y = c_2 + u_2$. The main condition is

$$x^2 + xy + y^2 + (u_1^2 + u_1u_2 + u_2^2) = 0,$$

the side conditions are $Tr_{q,2}(x) = Tr_{q,2}(u_1),\ Tr_{q,2}(y) = Tr_{q,2}(u_2)$. Let $v^2 = u_1^2 + u_1u_2 + u_2^2 \neq 0$.

4.1 Kloosterman and Mélas codes

In the sequel the trace $Tr_{q,2}$ will often be used. We abbreviate it by tr_0.

Definition 1. *For $0 \neq v \in \mathbb{F}_q$ let p_v be the number of $0 \neq x \in \mathbb{F}_q$ such that*

$$tr_0(x) = tr_0(v/x) = 1.$$

Also let m_i be the number of v such that $p_v = i$.

The curve with affine equation

$$y^2 + y = x + \frac{v}{x}$$

defined over $\mathbb{F}_q$ is elliptic and has $4p_v$ rational points. The Hasse inequality implies

$$\frac{q+1-2\sqrt{q}}{4} < p_v < \frac{q+1+2\sqrt{q}}{4}.$$

The Kloosterman code L_q or dual Mélas code is a binary code of length $q-1$ and dimension $2f$. Codeword $c(a,b)$, where $a, b \in \mathbb{F}_q$, has entry

$$tr_0(ax + b/x).$$

Clearly $wt(c(a,b)) = wt(c(1,ab))$ for $ab \neq 0$, and

$$wt(c(1,v)) = q - 2p_v.$$

A detailed analysis is in [9], where the weight distribution of L_q is determined. In particular $m_i > 0$ for every integer i contained in the interval. Knowledge of the weight distribution of L_q is equivalent with knowledge of the numbers m_i in Definition 1.

In order to avoid confusion let us sum up. Consider the hyperplane $H = H_{u,1}$, where $u = u_1\omega + u_2 \in K,\ v^2 = u_1^2 + u_1u_2 + u_2^2$. The parameters $u_1, u_2 \in \mathbb{F}_q$ and their absolute traces $tr_0(u_1),\ tr_0(u_2)$ are given, as well as $0 \neq v \in \mathbb{F}_q$. The intersection size $|\mathcal{K}_q \cap H| = 4s$ is determined by the number of pairs $x, y \in \mathbb{F}_q$ which satisfy $tr_0(x) = tr_0(u_1),\ tr_0(y) = tr_0(u_2)$ and the quadratic equation

$$x^2 + xy + y^2 = v^2. \tag{3}$$

The number of such pairs x, y is $q + 1 - s$.

Let $tr_0(u_2) = 1$. We have to choose y (automatically $\neq 0$) such that $tr_0(y) = 1$. Dividing equation 3 by y^2 yields the equivalent equation

$$(x/y)^2 + (x/y) + 1 + (v/y)^2 = 0.$$

This has solutions if and only if $tr_0(v/y) = 1$. If this is satisfied there are two solutions x, which have different absolute traces. Exactly one will satisfy $tr_0(x) = tr_0(u_1)$. We conclude $q + 1 - s = p_v$, or

$$s = q + 1 - p_v.$$

By symmetry the same is true when $tr_0(u_1) = 1$. It remains to consider the cases when $tr_0(u_1) = tr_0(u_2) = 0$. Let r be the number of pairs (x, y) such that $tr_0(x) = 0$ and equation 3 is satisfied. The only solution for $x = 0$ has $y = v$. In all other cases we must have $tr_0(v/x) = 1, tr_0(x) = 0$, and in each such case we count two choices for y. This yields $r = 1+2(\frac{q}{2}-p_v) = q+1-2p_v$. The number of pairs (x, y) satisfying $tr_0(x) = 0,\ tr_0(y) = 1$ and equation 3 is p_v. We obtain

$$s = 3p_v.$$

In case $s = q + 1 - p_v$ we have

$$4s \leq 4(q + 1) - (q + 1) + 2\sqrt{q}.$$

This is smaller than in the second case, where $s = 3p_v$ and therefore

$$s \leq 3(q + 1 + t).$$

Here t is as in Theorem 2.

4.2 The weight distribution of C_q

Consider the hyperplane $H = H_{u,1}$, where $u = u_1\omega + u_2 \in K$, $v^2 = u_1^2 + u_1u_2 + u_2^2$. Let $p_v = i$. We have seen that $|\mathcal{K}_q \cap H| = 4s$ and $4s = 4(q + 1 - i)$ if $(tr_0(u_1), tr_0(u_2)) \neq (0,0)$, whereas $4s = 12i$ if $(tr_0(u_1), tr_0(u_2)) = (0,0)$. For fixed v the number of (u_1, u_2) such that $v^2 = u_1^2 + u_1u_2 + u_2^2$ and $(tr_0(u_1), tr_0(u_2)) \neq (0,0)$ is $3p_v = 3i$, and consequently the number of (u_1, u_2) such that $v^2 = u_1^2 + u_1u_2 + u_2^2$ and $(tr_0(u_1), tr_0(u_2)) = (0,0)$ is $q + 1 - 3i$.

It follows that each of the m_i elements $v \in \mathbb{F}_q$ such that $p_v = i$ contributes $3im_i$ hyperplanes $H_{u,1}$ with intersection size $4(q + 1 - i)$ and $(q + 1 - 3i)m_i$ such hyperplanes with intersection size $12i$. Recall that by [9] we have $m_i > 0$ for all i in the Hasse interval. In particular $\iota_q \leq 3(q + 1 + t)$ with equality if and only if $t < (q + 1)/3$. This is satisfied for $q > 32$.

In case $q = 32$ we have $t = 11$. Clearly $\iota_{32} = 3(q+1+7) = 120$. For $q = 8$ we have $i \in \{1, 2, 3\}$ and $\iota_8 = 4(9 - 1) = 32$.

Multiplication by $(q - 1)(q^2 + 1)$ yields the weight distribution of C'_q, the subset of codewords of C_q, which do not belong to D_q or to $\langle 1 \rangle$.

Theorem 4. *Let $n = 3q^2 + 4$ and $A_w(C'_q)$ the number of codewords of C'_q of weight w. Then*

$$A_w(C'_q) = (q - 1)(q^2 + 1)(q + 1 - (n - w)/4)\{3m_{q+1-(n-w)/4} + m_{(n-w)/12}\}$$

with the proviso that $m_i = 0$ if i is not a positive integer.

As the m_i have been determined in [9] we know the weight distribution of C'_q. As all elements of $C_q \setminus C'_q$ belong either to $\langle 1 \rangle$ or to the 2-weight code D_q (see Corollary 1) this determines the weight distribution of C_q.

5 An example: C_8

As $\iota_8 = 32$, code C_8 is a $[196, 5, 164]_8$-code. Represent $\mathbb{F}_8$ as $\mathbb{F}_2(\epsilon)$ where $\epsilon^3 + \epsilon^2 + 1 = 0$. The numbers p_v from Definition 1 are

$$p_1 = 1,\ p_\epsilon = p_{\epsilon^2} = p_{\epsilon^4} = 3,\ p_{\epsilon^3} = p_{\epsilon^5} = p_{\epsilon^6} = 2,$$

hence

$$m_1 = 1,\ m_2 = 3,\ m_3 = 3.$$

By Subsection 4.2 this yields 3 hyperplanes $H_{u,1}, u \in K$ of intersection size 32, 18 such hyperplanes of intersection size 28, 27 of intersection size 24, 6 of intersection size 12, 9 more of intersection size 24 and finally 0 hyperplanes of intersection size 36. The weight distribution of C'_8 is therefore

$$A_{184}(C'_8) = 2730,\ A_{172}(C'_8) = 16380,\ A_{168}(C'_8) = 8190,\ A_{164}(C'_8) = 1365.$$

Together with the repetition code $\langle 1\rangle$ and the weights of the 2-weight subcode D_8 this leads to the following weight distribution for C_8 :

$$A_0 = 1,\ A_{164} = 1365,\ A_{168} = 10920,\ A_{172} = 16380,$$

$$A_{176} = 1365,\ A_{184} = 2730,\ A_{196} = 7.$$

In particular $C_8 \supset D_8$ form a chain of codes with parameters $[196, 5, 164]_8 \supset [196, 4, 168]_8$. Application of construction X from coding theory (see [8]) with $[4, 1, 4]_8$ as auxiliary code yields a code $[200, 5, 168]_8$.

6 The quadratic structure

In this section we describe how the points $\neq P_0$ of the cap $\mathcal{K}_q$ are distributed on three parabolic quadrics.

Lemma 2 shows that we can find $w_0 \in W$ such that $Tr_{q^4,q^2}(w_0) = \omega$. As $1, w_0$ form a basis of F over K, each $y \in F$ can be expressed as $y = c_1 + c_2 w_0$, where $c_1, c_2 \in K$ are uniquely determined.

We have $N(y) = (c_1 + c_2 w_0)(c_1 + c_2/w_0) = c_1^2 + c_2^2 + \omega c_1 c_2$. In particular $y \in W$ if and only if $c_1^2 + c_2^2 + \omega c_1 c_2 + 1 = 0$.

Use $1, \omega$ as basis of K over $\mathbb{F}_q$, write $c_1 = x_1 + \omega x_2,\ c_2 = x_3 + \omega x_4$. Represent (x_0, y) by the tuple $(x_0, x_1, x_2, x_3, x_4) \in \mathbb{F}_q^5$. Using these bases we can use any of the following representations for an element $x \in \mathbb{F}_q^5$:

$$x = (x_0, y) = (c_0, c_1, c_2) = (x_0, x_1, x_2, x_3, x_4),\ \text{where}$$

$$y \in F,\ c_0 = x_0 \in \mathbb{F}_q,\ c_1, c_2 \in K,\ x_i \in \mathbb{F}_q.$$

We have

$$N(y) = x_1^2 + \overline{\omega} x_2^2 + x_3^2 + \overline{\omega} x_4^2 + x_2 x_4 + \omega x_1 x_3 + \overline{\omega}(x_1 x_4 + x_2 x_3),$$

equivalently $N(y) = u_1 + \omega u_2$, where

$$u_1 = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_2 x_4 + x_1 x_4 + x_2 x_3,$$

$$u_2 = x_2^2 + x_4^2 + x_1 x_3 + x_1 x_4 + x_2 x_3.$$

Definition 2. *Consider the following quadratic forms in* 5 *variables:*

$$Q_2(x_0, x_1, x_2, x_3, x_4) = \sum_{i=0}^{4} x_i^2 + x_2x_4 + x_1x_4 + x_2x_3,$$

$$Q_3(x_0, x_1, x_2, x_3, x_4) = x_0^2 + x_1^2 + x_3^2 + x_1x_3 + x_2x_4.$$

It follows

$$N(y) = x_0^2 + Q_2(x) + \omega(Q_2(x) + Q_3(x)), \text{ where } x = (x_0, y).$$

Both Q_2 and Q_3 are non-degenerate, hence parabolic. They share the radical P_0 of the associated symplectic bilinear form.

Definition 3. *Consider the symmetry ρ defined by $\rho(c_0, c_1, c_2) = (c_0, \omega c_1, \omega c_2)$, equivalently $\rho(x) = (x_0, x_2, x_1 + x_2, x_4, x_3 + x_4)$. Clearly ρ has order* 3*. It implies an action on quadratic forms by*

$$(\rho Q)(x) = Q(\rho(x)).$$

Our quadratic forms are related by $Q_3 = \rho(Q_2)$. Let Q_1 be the third quadratic form in this ρ-orbit, so $Q_1 = \rho(Q_3)$.

Definition 4. *Let K_1 consist of the points $(1 : y)$, where $N(y) = 1$. Likewise K_2 is defined by $N(y) = \omega$ and K_3 by $N(y) = \overline{\omega}$.*

The points $\neq P_0$ of $\mathcal{K}_q$ form the union $K_1 \cup K_2 \cup K_3$. Observe that K_1 consists of the points $(1, w), K_2$ of the points $(1, \overline{\omega}w)$ and K_3 of the points $(1, \omega w)$ (where $N(w) = 1$). The formula in Definition 2 shows that $N(y) = 1$ if and only if $x = (1, y)$ satisfies $Q_2(x) = Q_3(x) = 0$. The same formula shows that a vector $x = (0, y)$ where $y \neq 0$ cannot satisfy $Q_2(x) = Q_3(x) = 0$ as otherwise we would have $N(y) = 0$. This shows $Q_2 \cap Q_3 = K_1$. The symmetry ρ shows that $Q_i \cap Q_j = K_k$ for $\{i, j, k\} = \{1, 2, 3\}$.

Theorem 5. *The points $\neq P_0$ of our cap form the union $K_1 \cup K_2 \cup K_3$. Each such point is on two of the quadrics Q_1, Q_2, Q_3, more exactly*

$$Q_i \cap Q_j = K_k \textit{ whenever } \{i, j, k\} = \{1, 2, 3\}.$$

References

[1] J. Bierbrauer: *The theory of cyclic codes and a generalization to additive codes, Designs, Codes and Cryptography* **25** (2002), 189-206.

[2] J. Bierbrauer: *Large caps, Combinatorics 2002, Topics in Combinatorics: geometry, graph theory and designs, Maratea (Potenza), Italy, 2-8 June, G.Korchmaros, editor,* pp.7-38.

[3] J. Bierbrauer and Y. Edel: *A family of caps in projective* 4*-space in odd characteristic, Finite Fields and Their Applications* **6** (2000),283-293.

[4] J. Bierbrauer, A. Cossidente and Y. Edel: *Caps on classical varieties and their projections, European Journal of Combinatorics* **22** (2001), 135-143.

[5] A. Carlet, P. Charpin and V. Zinoviev: *Codes, bent functions, and permutations suitable for DES-like cryptosystems, Designs, Codes and Cryptography* **15** (1998), 125-156.

[6] T. Helleseth and V. Kumar: *Sequences with low correlation,* in *Handbook of Coding Theory,* edited by V.Pless and C.Huffman, Elsevier Science Publishers, 1998.

[7] J.W.P. Hirschfeld and L. Storme: *The packing problem in statistics, coding theory and finite projective spaces: update 2001, Developments in Mathematics Vol. 3, Kluwer Academic Publishers. Finite Geometries, Proceedings of the Fourth Isle of Thorns Conference (Chelwood Gate, July 16-21, 2000) (Eds. A. Blokhuis, J.W.P. Hirschfeld, D. Jungnickel and J.A. Thas),* pp. 201-246.

[8] F. J. MacWilliams and N. J. A. Sloane.
The Theory of Error-Correcting Codes, North-Holland, 1977.

[9] R. Schoof and M. van der Vlugt: *Hecke operators and the weight distribution of certain codes, Journal of Combinatorial Theory A* **57** (1991), 163-186.

[10] B. Segre: *Le geometrie di Galois, Annali di Matematica Pura ed Applicata* **48** (1959),1-97.