Discrete Mathematics 310 (2010) 3162–3167

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Constructions of unitals in Desarguesian planes

A. Aguglia [a,*], L. Giuzzi [b], G. Korchmáros [c]

[a] *Dipartimento di Matematica, Politecnico di Bari, Via Amendola 126/B, I-70126 Bari, Italy*

[b] *Dipartimento di Matematica, Facoltà di Ingegneria, Università degli Studi di Brescia, Via Valotti 9, I-25133 Brescia, Italy*

[c] *Dipartimento di Matematica e Informatica, Università degli Studi della Basilicata, Campus Macchia Romana, Viale dell'Ateneo Lucano, 10, I-85100 Potenza, Italy*

ARTICLE INFO

Article history:
Received 30 September 2008
Received in revised form 23 June 2009
Accepted 24 June 2009
Available online 11 July 2009

Keywords:
Hermitian curve
Unital
Conic

ABSTRACT

We present a new construction of non-classical unitals from a classical unital $\mathcal{U}$ in $\mathrm{PG}(2, q^2)$. The resulting non-classical unitals are B–M unitals. The idea is to find a non-standard model Π of $\mathrm{PG}(2, q^2)$ with the following three properties:

(i) points of Π are those of $\mathrm{PG}(2, q^2)$;
(ii) lines of Π are certain lines and conics of $\mathrm{PG}(2, q^2)$;
(iii) the points in $\mathcal{U}$ form a non-classical B–M unital in Π.

Our construction also works for the B–T unital, provided that conics are replaced by certain algebraic curves of higher degree.

1. Introduction

A classical unital $\mathcal{U}$ in the Desarguesian plane $\mathrm{PG}(2, q^2)$ is the set of all absolute points of a non-degenerate unitary polarity. Up to a projectivity of $\mathrm{PG}(2, q^2)$, $\mathcal{U}$ consists of all the $q^3 + 1$ points of the non-degenerate Hermitian curve $\mathcal{H}$ with equation $y^q + y - x^{q+1} = 0$. The relevant combinatorial property of $\mathcal{U}$, leading to important applications in coding theory, is that $\mathcal{U}$ is a *two-character set* with parameters 1 and $q + 1$, that is, a line in $\mathrm{PG}(2, q^2)$ meets $\mathcal{U}$ in either 1 or $q + 1$ points. A *unital* in $\mathrm{PG}(2, q^2)$ is defined by this combinatorial property, namely it is a two-character set of size $q^3 + 1$ with parameters 1 and $q + 1$.

The known non-classical unitals are the B–M unitals due to Buekenhout and Metz, see [6,21], and the B–T unitals due to Buekenhout; see [6]. They were constructed in the Desarguesian plane by an ingenious idea, relying on the Bruck–Bose representation of $\mathrm{PG}(2, q^2)$ in $\mathrm{PG}(4, q)$ and exploiting properties of spreads and ovoids (in particular, quadrics). For q odd, an alternative construction for special B–M unitals which are the union of q conics sharing a point has been given by Hirschfeld and Szőnyi [16] and independently by Baker and Ebert [3]. Such B–M unitals are called H–Sz type B–M unitals.

In this paper, we present a new construction for non-H–Sz type B–M unitals. The key idea, as described in the abstract, is fully realised within $\mathrm{PG}(2, q^2)$, and it uses only quadratic transformations. This method also works for B–T unitals, provided that quadratic transformations are replaced by certain birational transformations.

Our notation and terminology are standard. For generalities on unitals in projective planes the reader is referred to [5,10,11]. Basic facts on rational transformations of projective planes are found in [15, Section 3.3].

2. A non-standard model of $\mathrm{PG}(2, q^2)$

Fix a projective frame in $\mathrm{PG}(2, q^2)$ with homogeneous coordinates (x_0, x_1, x_2), and consider the affine plane $\mathrm{AG}(2, q^2)$ whose infinite line ℓ_∞ has equation $x_0 = 0$. Then $\mathrm{AG}(2, q^2)$ has affine coordinates (x, y) where $x = x_1/x_0,\ y = x_2/x_0$ so that $X_\infty = (0, 1, 0)$ and $Y_\infty = (0, 0, 1)$ are the infinite points of the horizontal and vertical lines, respectively.

* Corresponding author.
E-mail address: a.aguglia@poliba.it (A. Aguglia).

0012-365X/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2009.06.023

Fix a non-zero element $a \in \mathrm{GF}(q^2)$. For $m, d \in \mathrm{GF}(q^2)$ and $a \in \mathrm{GF}(q^2)^*$, let $\mathcal{C}_a(m, d)$ denote the parabola of equation $y = ax^2 + mx + d$. Consider the incidence structure $\mathfrak{A}_a = (\mathcal{P}, \mathcal{L})$ whose points are the points of $\mathrm{AG}(2, q^2)$ and whose lines are the vertical lines of equation $x = k$, together with the parabolas $\mathcal{C}_a(m, d)$ where m, d, k range over $\mathrm{GF}(q^2)$.

Lemma 2.1. *For every non-zero $a \in \mathrm{GF}(q^2)$, the incidence structure $\mathfrak{A}_a = (\mathcal{P}, \mathcal{L})$ is an affine plane isomorphic to $\mathrm{AG}(2, q^2)$.*

Proof. The birational transformation φ given by

$$\varphi : (x, y) \mapsto (x, y - ax^2), \tag{1}$$

transforms vertical lines into themselves, whereas the generic line $y = mx + d$ is mapped into the parabola $\mathcal{C}_a(m, d)$. Therefore, φ determines an isomorphism

$$\mathfrak{A}_a \simeq \mathrm{AG}(2, q^2),$$

and the assertion is proved. □

Completing $\mathfrak{A}_a$ with its points at infinity in the usual way gives a projective plane isomorphic to $\mathrm{PG}(2, q^2)$. Note that the infinite point Y_∞ of the vertical lines of $\mathrm{AG}(2, q^2)$ is also the infinite point of the vertical lines of $\mathfrak{A}_a$.

For q an odd power of 2, a different, yet similar, construction will also be useful in our investigation. The construction depends on some known facts about Galois fields of even characteristic. Let $\varepsilon \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$ such that $\varepsilon^2 + \varepsilon + \delta = 0$, for some $\delta \in \mathrm{GF}(q) \setminus \{1\}$ with $\mathrm{Tr}\,(\delta) = 1$. Here, as usual, Tr stands for the trace function $\mathrm{GF}(q) \to \mathrm{GF}(2)$. Then $\varepsilon^{2q} + \varepsilon^q + \delta = 0$. Therefore, $(\varepsilon^q + \varepsilon)^2 + (\varepsilon^q + \varepsilon) = 0$, whence $\varepsilon^q + \varepsilon + 1 = 0$. Moreover, if q is an odd power of 2, then

$$\sigma : x \mapsto x^{2^{(e+1)/2}}$$

is an automorphism of $\mathrm{GF}(q)$.

For any $m, d \in \mathrm{GF}(q^2)$ let $\mathcal{D}(m, d)$ denote the plane algebraic curve of equation

$$y = [((x^q + x)\varepsilon + x)^{\sigma+2} + (x^q + x)^\sigma + ((x^q + x)\varepsilon + x)(x^q + x)]\varepsilon + bx^{q+1} + mx + d \tag{2}$$

where b is a given element in $\mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$.

Introduce the incidence structure $\mathfrak{A}'_\varepsilon = (\mathcal{P}', \mathcal{L}')$ whose points are the points of $\mathrm{AG}(2, q^2)$ and whose lines are the vertical lines of equation $x = k$, together with the curves $\mathcal{D}(m, d)$ where m, d, k range over $\mathrm{GF}(q^2)$.

Lemma 2.2. *The incidence structure $\mathfrak{A}'_\varepsilon = (\mathcal{P}', \mathcal{L}')$ is an affine plane isomorphic to $\mathrm{AG}(2, q^2)$.*

Proof. The argument in the proof of Lemma 2.1 works also in this case, provided that φ is replaced by the birational transform γ defined by

$$\gamma : (x, y) \mapsto (x, y + [((x^q + x)\varepsilon + x)^{\sigma+2} + (x^q + x)^\sigma + ((x^q + x)\varepsilon + x)(x^q + x)]\varepsilon + bx^{q+1}). \quad \square$$

The idea to use a non-standard model of $PG(2, q^2)$ arising from a quadratic transformation, as in our approach, goes back to [19] where inherited arcs and ovals in non-Desarguesian planes were studied. This idea was also used by Jha and Johnson, see [17,18], in investigating certain translation ovals of generalized André planes.

3. The construction

Before presenting our construction we recall the equations of B–M unitals and B–T unitals in $\mathrm{PG}(2, q^2)$.

Proposition 3.1 (*Baker and Ebert[4], Ebert [8,10]*)**.** *For $a, b \in \mathrm{GF}(q^2)$, the point-set*

$$U_{a,b} = \{(1, x, ax^2 + bx^{q+1} + r) | x \in \mathrm{GF}(q^2), r \in \mathrm{GF}(q)\} \cup \{Y_\infty\}$$

is a B–M unital in $\mathrm{PG}(2, q^2)$ if and only if Ebert's discriminant condition is satisfied, that is for odd q,

(i) *$4a^{q+1} + (b^q - b)^2$ is a non-square in $\mathrm{GF}(q)$,*

and for q even,

(ii) *$b \notin \mathrm{GF}(q)$ and $\mathrm{Tr}\,(a^{q+1}/(b^q + b)^2) = 0$.*

Conversely, every B–M unital has a representation as $U_{a,b}$.

Proposition 3.2. *With the above notation,*

(i) *$U_{a,b}$ is classical if and only if $a = 0$;*
(ii) *$U_{a,b}$ is a H–Sz type B–M unital if and only if $a^{(q+1)/2} \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$ and $b \in \mathrm{GF}(q)$.*

Proof. This is a direct corollary of [10, Theorems 1 and 12]. □

Proposition 3.3. *Let $q = 2^e$, where $e > 1$ is an odd integer. In the above notation, the point-set*

$$U_\varepsilon = \{(1, x, [((x^q + x)\varepsilon + x)^{\sigma+2} + (x^q + x)^\sigma + ((x^q + x)\varepsilon + x)(x^q + x)]\varepsilon + r) \mid x \in \mathrm{GF}(q^2), r \in \mathrm{GF}(q)\} \cup \{Y_\infty\}, \tag{3}$$

is a B–T unital in $\mathrm{PG}(2, q^2)$. Conversely, every B–T unital may be represented as U_ε for some choice of ε.

Proof. From [9,10], the point-set

$$U_\varepsilon = \{(1, s + t\varepsilon, (s^{\sigma+2} + t^\sigma + st)\varepsilon + r) | r, s, t \in \mathrm{GF}(q)\} \cup \{Y_\infty\} \tag{4}$$

is a B–T unital and, conversely, every B–T unital has such an equation. Let $x = s + t\varepsilon$. Then, $t = x^q + x$ and $s = x + (x^q + x)\varepsilon$. Substituting t and s in (4) gives the result. □

If $b \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$ then, from Proposition 3.2, the point-set

$$\mathcal{U}_b = \{(1, x, bx^{q+1} + r) | x \in \mathrm{GF}(q^2), r \in \mathrm{GF}(q)\} \cup \{Y_\infty\} \tag{5}$$

is a classical unital in $\mathrm{PG}(2, q^2)$. As pointed out in Section 2, $\mathcal{U}_b$ can be regarded as a point-set in the projective closure of $\mathfrak{A}_a$ and, for q even, also as a point-set of the projective closure of $\mathfrak{A}'_\varepsilon$. The question arises whether $\mathcal{U}_b$ is still a unital in these planes. Our main result, stated in the following two theorems, shows that the answer is positive.

Theorem 3.4. *Let $a \in \mathrm{GF}(q^2)^*$, $b \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$. If (a, b) satisfies Ebert's discriminant condition, then $\mathcal{U}_b$ is the non-classical B–M unital $U_{-a,b}$ in the projective closure of $\mathfrak{A}_a$. Conversely, every non-H–Sz type B–M unital is obtained in this way.*

Proof. Let $P = (\xi, \eta)$ an affine point in $\mathfrak{A}_a$. This point, viewed as an element of $\mathrm{AG}(2, q^2)$, has coordinates $x = \xi$ and $y = \eta + a\xi^2$. From (5),

$$\mathcal{U}_b = \{(1, \xi, -a\xi^2 + b\xi^{q+1} + r) \mid \xi \in \mathrm{GF}(q^2), r \in \mathrm{GF}(q)\} \cup \{Y_\infty\}. \tag{6}$$

This shows that $\mathcal{U}_b$ and $U_{-a,b}$ coincide in $\mathfrak{A}_a$. Since $(-a, b)$ also satisfies Ebert's discriminant condition, $U_{-a,b}$ is a B–M unital in the projective closure of $\mathfrak{A}_a$. By Proposition 3.2, $U_{-a,b}$ is a non-H–Sz type B–M unital. □

Theorem 3.5. *Let $q = 2^e$, with $e > 1$ an odd integer. Then $\mathcal{U}_\varepsilon$ is a non-classical B–T unital in the projective closure of $\mathfrak{A}'_\varepsilon$.*

Proof. We use the same argument as in the preceding proof. The point $P = (\xi, \eta)$ of $\mathfrak{A}'_\varepsilon$, viewed as an element of $\mathrm{AG}(2, q^2)$, has coordinates $x = \xi$ and

$$y = \eta + [((\xi^q + \xi)\varepsilon + \xi)^{\sigma+2} + (\xi^q + \xi)^\sigma + ((\xi^q + \xi)\varepsilon + \xi)(\xi^q + \xi)]\varepsilon + b\xi^{q+1}.$$

From (5),

$$\mathcal{U}_b = \{(1, \xi, [((\xi^q + \xi)\varepsilon + \xi)^{\sigma+2} + (\xi^q + \xi)^\sigma + ((\xi^q + \xi)\varepsilon + \xi)(\xi^q + \xi)]\varepsilon + r) \mid \xi \in \mathrm{GF}(q^2), r \in \mathrm{GF}(q)\} \cup \{Y_\infty\}.$$

By Proposition 3.3 we have that $\mathcal{U}_b$ and $\mathcal{U}_\varepsilon$ coincide in $\mathfrak{A}'_\varepsilon$ and the assertion follows. □

3.1. An alternative proof of Theorem 3.4

The above proofs of Theorems 3.4 and 3.5 depend on the explicit equations for B–M and B–T unitals, as given in Propositions 3.1 and 3.3. Here we provide a direct proof of Theorem 3.4. Without loss of generality, we assume that $q \geq 3$.

Let $\mathcal{H}$ be the set of all points in $\mathrm{AG}(2, q^2)$ of the affine Hermitian curve $\mathcal{C}$ of equation

$$y^q - y + (b - b^q)x^{q+1} = 0, \quad b \notin \mathrm{GF}(q), \tag{7}$$

Then, $\mathcal{H} \cup \{Y_\infty\}$ is a classical unital in $\mathrm{PG}(2, q^2)$. We prove that $\mathcal{H} \cup \{Y_\infty\}$ is also a unital in the projective closure of $\mathfrak{A}_a$.

We first need the following lemma.

Lemma 3.6. *For every $m, d \in \mathrm{GF}(q^2)$, the parabola $\mathcal{C}_a(m, d)$ and $\mathcal{H}$ have either 1 or $q + 1$ points in $\mathrm{AG}(2, q^2)$.*

Proof. The number of solutions $(x, y) \in \mathrm{GF}(q^2) \times \mathrm{GF}(q^2)$ of the system

$$\begin{cases} y^q - y + (b - b^q)x^{q+1} = 0 \\ y - ax^2 - mx - d = 0 \end{cases} \tag{8}$$

gives the number of points in common of $\mathcal{H}$ and $\mathcal{C}_a(m, d)$. To solve this system, recover the value of y from the second equation and substitute it in the first. The result is

$$a^q x^{2q} + (b - b^q)x^{q+1} + m^q x^q - ax^2 - mx + d^q - d = 0. \tag{9}$$

Consider now $\mathrm{GF}(q^2)$ as a vector space over $\mathrm{GF}(q)$, fix a basis $\{1, \varepsilon\}$ with $\varepsilon \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$, and write the elements in $\mathrm{GF}(q^2)$ as a linear combination with respect to this basis, that is, $z = z_0 + z_1\varepsilon$, with $z \in \mathrm{GF}(q^2)$ and $z_0, z_1 \in \mathrm{GF}(q)$. Thus, (9) becomes an equation over $\mathrm{GF}(q)$. We investigate separately the even q and odd q cases.

For q even, ε may be chosen as in Section 2. With this choice of ε, (9) becomes

$$(a_1 + b_1)x_0^2 + [(a_0 + a_1) + \nu(a_1 + b_1)]x_1^2 + b_1 x_0 x_1 + m_1 x_0 + (m_0 + m_1)x_1 + d_1 = 0. \tag{10}$$

We shall represent the the solutions (x_0, x_1) of (10) as points of the affine plane $\mathrm{AG}(2, q)$ over $\mathrm{GF}(q)$ arising from the vector space $\mathrm{GF}(q^2)$. In fact, (10) turns out to be the equation of a (possibly degenerate) affine conic Ξ of $\mathrm{AG}(2, q)$. Actually, Ξ is either an ellipse or is a single point. To prove this, we have to show that it has no point at infinity; that is, we need to prove that the points $P=(x_0,x_1,0)$ with

$$(a_1+b_1)x_0^2+[(a_0+a_1)+\nu(a_1+b_1)]x_1^2+b_1x_0x_1=0, \tag{11}$$

do not lie in PG$(2,q)$. This is the case if and only if (11) admits only the trivial solution over GF(q). A necessary a sufficient condition for this is

$$\mathrm{Tr}\left(\frac{(a_1+b_1)[(a_0+a_1)+\nu(a_1+b_1)]}{b_1^2}\right)=1. \tag{12}$$

In our case, (12) holds as it follows directly from Ebert's discriminant condition; see [5, page 83]. Therefore, Ξ is either an ellipse or it consists of a single point; hence, $\mathcal{C}_a(m,d)$ meets $\mathcal{H}$ in either 1 or $q+1$ points.

For q odd, an analogous argument is used. For this purpose, as in [10], choose a primitive element β of GF(q^2) and let $\varepsilon=\beta^{(q+1)/2}$. Then, $\varepsilon^q=-\varepsilon$ and ε^2 is a primitive element of GF(q). With this choice of ε, (9) becomes

$$(b_1+a_1)\varepsilon^2x_1^2+2a_0x_0x_1+(a_1-b_1)x_0^2+m_0x_1+m_1x_0+d_1=0. \tag{13}$$

The discussion of the (possibly degenerate) affine conic Ξ of Eq. (13) may be carried out exactly as in the even order case. The points $P=(x_0,x_1,0)$ of Ξ at infinity are determined by

$$(b_1+a_1)\varepsilon^2x_1^2+2a_0x_0x_1+(a_1-b_1)x_0^2=0,$$

and this equation has only the trivial solution over GF(q), since Ebert's discriminant condition implies that $4a^q+(b^q-b)^2$ is non-square in GF(q). □

Lemma 3.6 together with [14, Theorem 12.16] have the following corollary.

Theorem 3.7. *The point-set $\mathcal{H}\cup\{Y_\infty\}$ is a unital in the projective closure of $\mathfrak{A}_a$.*

To show that $\mathcal{H}\cup\{Y_\infty\}$ is a non-classical unital in the projective closure of $\mathfrak{A}$, we rely on some elementary facts on algebraic curves.

Lemma 3.8. *The points of $\mathcal{H}$ in $\mathfrak{A}_a$ lie on the absolutely irreducible affine plane curve $\mathcal{C}'$ of equation*

$$\eta^q-\eta+(b-b^q)\xi+a^q\xi^{2q}-a\xi^2=0.$$

Proof. The plane curve $\mathcal{C}'$ is absolutely irreducible, see [15, Lemma 12.1]. If $P=(\xi,\eta)$ is a point of $\mathcal{H}$ in $\mathfrak{A}_a$, then P, regarded as a point of AG$(2,q^2)$, has coordinates x,y with $x=\xi,\ y=\eta+a\xi^2$. Since (x,y) satisfies (7),

$$(\eta+a\xi^2)^q-\eta-a\xi^2+(b-b^q)\xi=0$$

holds. This implies that $P=(\xi,\eta)$ is a point of $\mathcal{C}'$. □

Theorem 3.9. *The point-set $\mathcal{H}\cup\{Y_\infty\}$ is a non-classical unital in the projective closure of $\mathfrak{A}_a$.*

Proof. Assume, on the contrary, that $\mathcal{H}$ coincides in $\mathfrak{A}_a$ with the point-set of a non-degenerate affine Hermitian curve $\mathcal{D}'$. Then, $\mathcal{C}'$ and $\mathcal{D}'$ have at least q^3 common points. Since $\deg\mathcal{C}'=2q$ and $\deg\mathcal{D}'=q+1$ and $2q(q+1)<q^3$, Bézout's theorem, see [15, Theorem 3.13], implies that $\mathcal{C}'$ and $\mathcal{D}'$ share a common component. This contradicts Lemma 3.8. □

Finally, we prove that $\mathcal{H}\cup\{Y_\infty\}$ is a B–M unital in the projective closure of $\mathfrak{A}_a$. Our proof relies on the Ebert–Wantz group-theoretic characterization of B–M unitals of a Desarguesian plane: A unital $\mathcal{U}$ of PG$(2,q^2)$ is a B–M unital if, and only if, $\mathcal{U}$ is preserved by a linear collineation group of order $q^3(q-1)$ which is the semidirect product of a subgroup S of order q^3 by a subgroup R of order $q-1$. Moreover, S is Abelian if, and only if, $\mathcal{U}$ is a H–Sz type B–M unital; see [12] and [10, Theorem 12]. For more results on the collineation group of a B–M unital, see [1,2].

Theorem 3.10. *In the projective closure of $\mathfrak{A}_a$, the point-set $\mathcal{H}\cup\{Y_\infty\}$ is a non-Sz–H type B–M unital.*

Proof. A straightforward computation shows that for any point $P=(u,v)\in\mathcal{H}$ in $\mathfrak{A}_a$ and for any $\lambda\in$ GF$(q)^*$, the affinities

$$\begin{aligned}\alpha_{u,v}:(\xi,\eta)\ &\rightarrow\ (\xi+u,\eta-2au\xi+u^q(b-b^q)\xi+v),\\ \beta_\lambda:(\xi,\eta)\ &\rightarrow\ (\lambda\xi,\lambda^2\eta)\end{aligned} \tag{14}$$

of $\mathfrak{A}_a$ preserve $\mathcal{H}$. The group S of the linear collineations $\alpha_{u,v}$ with $P=(u,v)$ ranging over $\mathcal{H}$ is a non-Abelian group of order q^3. Write R for the group of the linear collineations β_λ as λ ranges on GF$(q)^*$. It turns out that the group G generated by all these collineations has order $q^3(q-1)$ and is the semidirect product $S\rtimes R$, and the assertion follows from the Ebert–Wantz characterization. □

Remark 3.11. Theorem 3.9 may also be proved without using algebraic geometry. The idea is to write the equation of the tangent parabolas $\mathcal{C}_a(m,d)$ at the points of the classical unital $\mathcal{H}\cup\{Y_\infty\}$ and use Thas' characterization [23] involving the feet of a point on a unital. If $P=(w,z)\in\mathcal{H}$ then the unique tangent parabola to $\mathcal{H}$ at P has equation

$$y=ax^2+\left(-2aw+(b-b^q)w^q\right)x-z^q+aw^2. \tag{15}$$

For q odd, Theorem 3.10 can also be shown by replacing group theoretic arguments with some geometric characterizations results depending on Baer sublines, due to Casse, O'Keefe, Penttila and Quinn; see [7,22] and [10, Theorem 11].

4. Absolutely irreducible curves containing all points of a B–M unital in PG$(2, q^2)$

Let $a \in GF(q^2)^*$ and $b \in \mathrm{GF}(q^2) \setminus GF(q)$. If (a, b) satisfies Ebert's discriminant condition, then the absolutely irreducible plane curve $\Gamma_{a,b}$ of PG$(2, q^2)$ with affine equation

$$y^q - y - a^q x^{2q} + ax^2 + (b - b^q)x^{q+1} = 0 \tag{16}$$

contains all points of the B–M unital $U_{-a,b}$. We prove some properties of $\Gamma_{a,b}$.

Theorem 4.1. *The curve $\Gamma_{a,b}$ is birationally equivalent over $GF(q^2)$ to a non-degenerate Hermitian curve.*

Proof. The birational map $(x, y) \to (x, y - ax^2)$ transforms $\Gamma_{a,b}$ into the Hermitian curve $\mathcal{C}$ of equation (7). $\square$

Theorem 4.2. *$\Gamma_{a,b}$ is the unique plane curve of minimum degree which contains all the points of the B–M unital $U_{-a,b}$ in* PG$(2, q^2)$.

Proof. Let Ψ be a plane curve of PG$(2, q^2)$ of degree $d \leq 2q$ that is not necessarily absolutely irreducible and which contains all points of $U_{-a,b}$. Obviously, $\Gamma_{a,b}$ and Ψ have at least $q^3 + 1$ common points. From Bézout's theorem [15, Theorem 3.13], $\Gamma_{a,b}$ is a component of Ψ. Since deg $\Gamma_{a,b} \geq$ deg Ψ, this is only possible when they coincide. $\square$

Remark 4.3. In 1982, Goppa introduced a general construction technique for linear codes from algebraic curves defined over a finite field; see [13]. In the current literature, these codes are called *algebraic geometry*.

The parameters of linear codes arising from a Hermitian curve by Goppa's method were computed in [20]. These codes turn out to perform very well, when compared with Reed-Solomon codes of similar length and dimension.

In [10], Ebert raised the question whether the parameters of the codes arising from $\Gamma_{a,b}$ by Goppa's construction were close to maximum distance separable codes.

Since the algebraic-geometric codes are determined by the function fields of the related algebraic curves and the function fields of two birationally equivalent plane curves are isomorphic, Theorem 4.1 implies that the algebraic-geometry codes arising from the Hermitian curve $\mathcal{C}$ and those arising from the curve $\Gamma_{a,b}$ are the same.

5. B–M unitals and cones of PG$(3, q^2)$

We present another way to construct a non-classical B–M unital using a Hermitian curve and a suitable cone of PG$(3, q^2)$.

Let x_0, x_1, x_2, x_3 denote homogeneous coordinates in PG$(3, q^2)$. Consider the Hermitian curve $\mathcal{H} = \{(1, t, bt^{q+1} + r) | t \in \mathrm{GF}(q^2), r \in \mathrm{GF}(q)\} \cup \{Y_\infty\}$ and the map $\phi : \mathcal{H} \mapsto \mathrm{PG}(3, q^2)$ which transforms the point $P(1, t, bt^{q+1} + r)$ into the point $\phi(P) = (1, t, t^2, bt^{q+1} + r)$ and $Y_\infty = (0, 0, 1)$ into $\phi(Y_\infty) = (0, 0, 0, 1)$.

The map ϕ is injective; thus, the set $\phi(\mathcal{H})$ consists of $q^3 + 1$ points lying on the cone $\mathfrak{C}$ represented by $x_0x_2 = x_1^2$. The point $Q(0, 0, 1, -a)$, where $a \in GF(q^2)^*$, does not lie on the cone $\mathfrak{C}$; hence, the projection ρ from Q to the plane $\pi : x_2 = 0$ is well defined. The point $\phi(Y_\infty)$ is on π thus we get $\rho(0, 0, 0, 1) = (0, 0, 0, 1)$.

For any $(t, r) \in \mathrm{GF}(q^2) \times \mathrm{GF}(q)$, set $P_{t,r} = (1, t, bt^{q+1} + r)$. The line $P_{t,r}Q$ has point-set

$$\{(1, t, t^2 + \lambda, bt^{q+1} + r - \lambda a) | \lambda \in \mathrm{GF}(q^2)\} \cup \{(0, 0, 0, 1)\}$$

and intersects the plane π at $\rho(P_{t,r}) = (1, t, 0, at^2 + bt^{q+1} + r)$. We are going to show that no 2-secant lines of $\phi(\mathcal{H})$ pass through Q. Let $P_{t_1,r_1}(1, t_1, t_1^2, bt_1^{q+1} + r_1)$ and $P_{t_2,r_2}(1, t_2, t_2^2, bt_2^{q+1} + r_2)$ be two distinct points of $\phi(\mathcal{H})$. The line $P_{t_1,r_1}P_{t_2,r_2}$ is the point-set

$$\{(\lambda + 1, t_1 + \lambda t_2, t_1^2 + \lambda t_2^2, b(t_1^{q+1} + \lambda t_2^{q+1}) + r_1 + \lambda r_2) | \lambda \in \mathrm{GF}(q^2)\} \cup \{P_{t_2,r_2}\}.$$

If the point Q were on the line $P_{t_1,r_1}P_{t_2,r_2}$ then $\lambda = -1$, $t_1 - t_2 = 0$ and $t_1^2 - t_2^2 \neq 0$, which is impossible. Therefore, $|\rho(\phi(\mathcal{H}))| = q^3 + 1$ and it is possible to choose homogeneous coordinates for the plane π in such a way as $\rho(\phi(\mathcal{H}))$ turns out to be the set

$$\{(1, t, at^2 + bt^{q+1} + r) | t \in \mathrm{GF}(q^2), r \in \mathrm{GF}(q)\} \cup \{P_\infty\};$$

that is, $\rho(\phi(\mathcal{H}))$ is a non-classical B–M unital in π.

References

[1] V. Abatangelo, On Buekenhout-Metz unitals in PG$(2, q^2)$, q even, Arch. Math. 59 (1992) 197–203.
[2] V. Abatangelo, B. Larato, A group theoretic characterization of parabolic Buekenhout-Metz unitals, Boll. Unione Mat. Ital. 5-A 7, 195–206.
[3] R.D. Baker, G.L. Ebert, Intersection of unitals in the Desarguesian plane, in: Proceedings of the Twentieth Southeastern Conference on Combinatorics, Graph Theory, and Computing (Boca Raton, FL, 1989), in: Congr. Numer, vol. 70, 1990, pp. 87–94.

[4] R.D. Baker, G.L. Ebert, On Buekenhout-Metz unitals of odd order, J. Combin. Theory Ser. A 60 (1992) 67–84.
[5] S.G. Barwick, G.L. Ebert, Unitals in Projective Planes, in: Monographs in Mathematics, Springer, New York, 2008.
[6] F. Buekenhout, Existence of unitals in finite translation planes of order q^2 with a kernel of order q, Geom., Dedicata 5 (1976) 189–194.
[7] L.R.A. Casse, C.M. O'Keefe, T. Pentilla, Characterizations of Buekenhout–Metz unitals, Geom., Dedicata 59 (1996) 29–42.
[8] G.L. Ebert, On Buekenhout-Metz unitals of even order, European J. Combin. 13 (1992) 109–117.
[9] G.L. Ebert, Buekenhout-Tits unitals, J. Algebraic Combin. 6 (1997) 133–140.
[10] G.L. Ebert, Hermitian arcs, Rend. Circ. Mat. Palermo (2) Suppl. 51 (1998) 87–105.
[11] G.L. Ebert, Buekenhout unitals, Discrete Math. 208/209 (1999) 247–260.
[12] G.L. Ebert, K. Wantz, A group theoretic characterization of Buekenhout-Metz unitals, J. Combin. Designs 4 (1996) 143–152.
[13] V.D. Goppa, Algebraic-geometric codes, Izv. Akad. Nauk SSSR Ser. Mat. 46 (1982) 762–781.
[14] J.W.P. Hirschfeld, Projective geometries over finite fields, in: Oxford Mathematical Monographs, Second ed., The Clarendon Press, Oxford University Press, New York, 1998.
[15] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves over a Finite Field, in: Princeton Series in Applied Mathematics, Princeton University Press, Princeton, NJ, 2008.
[16] J.W.P. Hirschfeld, T. Szőnyi, Sets in a finite plane with few intersection numbers and a distinguished point, Discrete Math. 97 (1991) 229–242.
[17] V. Jha, N.L. Johnson, On the ubiquity of Denniston-type translation ovals in generalized André planes, in: Combinatorics '90 (Gaeta, 1990), in: Annals of Discrete Math, vol. 52, North-Holland, Amsterdam, 1992, pp. 279–296.
[18] V. Jha, N.L. Johnson, A characterisation of spreads ovally-derived from Desarguesian spreads, Combinatorica 14 (1994) 51–61.
[19] G. Korchmáros, Inherited arcs in finite affine planes, J. Combin. Theory Ser. A 42 (1986) 140–143.
[20] J.H. van Lint, Y.A. Springer, Generalized Reed Solomon codes from algebraic geometry, IEEE Trans. Inform. Theory 33 (1987) 305–309.
[21] R. Metz, On a class of unitals, Geom., Dedicata 8 (1979) 125–126.
[22] C.T. Quinn, L.R.A Casse, Concerning a characterization of Buekenhout-Metz unitals, J. Geometry 52 (1995) 159–167.
[23] J.A. Thas, A combinatorial characterization of Hermitian curves, J. Algebraic Combin. 1 (1992) 97–102.