A Collection of
MTA–ELTE GAC manuscripts

Gábor Korchnáros, Alessandro Siciliano,
Tamás Szőnyi

Embedding of Classical Polar Unitals in
$PG(2; q^2)$

2017

MTA–ELTE Geometric and Algebraic
Combinatorics Research Group

Hungarian Academy of Sciences
Eötvös University, Budapest

MANUSCRIPTS
Embedding of Classical Polar Unital in PG(2, q^2)

Gábor Korchmáros* Alessandro Siciliano*
Tamás Szőnyi†

Abstract
A unital, that is, a block-design 2 − (q^3 + 1, q + 1, 1) is embedded in a projective plane Π of order q^2 if its points and blocks are points and lines of Π. A unital embedded in PG(2, q^2) is Hermitian if its points and blocks are the absolute points and lines of a unitary polarity of PG(2, q^2). A classical polar unital is a unital isomorphic, as a block-design, to a Hermitian unital. We prove that there exists only one embedding of the classical polar unital in PG(2, q^2), namely the Hermitian unital.

1 Introduction
A unital is defined to be a set of q^3 + 1 points equipped with a family of subsets, each of size q + 1, such that every pair of distinct points are contained in exactly one subset of the family. Such subsets are usually called blocks so that unitals are block-designs 2 − (q^3 + 1, q + 1, 1). A unital is embedded in a projective plane Π of order q^2, if its points are points of Π and its blocks are lines of Π. Sufficient conditions for a unital to be embeddable in a projective

*Gábor Korchmáros: gabor.korchmaros@unibas.it
Alessandro Siciliano: alessandro.siciliano@unibas.it
Dipartimento di Matematica, Informatica ed Economia - Università degli Studi della Basilicata - Viale dell’Ateneo Lucano 10 - 85100 Potenza (Italy).
†Tamás Szőnyi: szonyi@cs.elte.hu
Department of Computer Science - Eötvös Loránd University - Pázmány Péter sétány 1/C - 1117 Budapest (Hungary).
plane are given in [8]. Computer aided searches suggest that there should be plenty of unitals, especially for small values of \( q \), but those embeddable in a projective plane are quite rare, see [1, 3, 10]. In the Desarguesian projective plane \( \text{PG}(2, q^2) \), a unital arises from a unitary polarity in \( \text{PG}(2, q^2) \): the points of the unital are the absolute points, and the blocks are the non-absolute lines of the polarity. The name of “Hermitian unital” is commonly used for such a unital since its points are the points of the Hermitian curve defined over \( \text{GF}(q^2) \). A classical polar unital is a unital isomorphic, as a block-design, to a Hermitian unital. By definition, the classical polar unital can be embedded in \( \text{PG}(2, q^2) \) as the Hermitian unital, and it has been conjectured for a long time that this is the unique embedding of the classical polar unital in \( \text{PG}(2, q^2) \). Our goal is to prove this conjecture. Our notation and terminology are standard. The principal references on unitals are [2, 6].

2 Projections and Hermitian unital

Let \( \mathcal{H} \) be a Hermitian unital in the Desarguesian plane \( \text{PG}(2, q^2) \). Any non-absolute line intersects \( \mathcal{H} \) in a Baer subline, that is a set of \( q + 1 \) points isomorphic to \( \text{PG}(1, q) \). Take any two distinct non-absolute lines \( \ell \) and \( \ell' \). For any point \( Q \) outside both \( \ell \) and \( \ell' \), the projection of \( \ell \) to \( \ell' \) from \( Q \) takes \( \ell \cap \mathcal{H} \) to a Baer subline of \( \ell' \). We say that \( Q \) is a full point with respect to the line pair \((\ell, \ell')\) if the projection from \( Q \) takes \( \ell \cap \mathcal{H} \) to \( \ell' \cap \mathcal{H} \).

From now on, we assume that \( \ell \) and \( \ell' \) meet in a point \( P \) of \( \text{PG}(2, q^2) \) not lying in \( \mathcal{H} \). We denote the polar line of \( P \) with respect to the unitary polarity associated to \( \mathcal{H} \) by \( P^\perp \). Then \( P^\perp \) is a non-absolute line. We will prove that if \( q \) is even then \( P^\perp \cap \mathcal{H} \) contains a unique full point. This does not hold true for odd \( q \). In fact, we will prove that for odd \( q \), \( P^\perp \cap \mathcal{H} \) contains zero or two full points depending on the mutual position of \( \ell \) and \( \ell' \).

To work out our proofs we need some notation and known results regarding \( \mathcal{H} \) and the projective unitary group \( \text{PGU}(3, q) \) preserving \( \mathcal{H} \).

Up to a change of the homogeneous coordinate system \((X_1, X_2, X_3)\) in \( \text{PG}(2, q^2) \), the points of \( \mathcal{H} \) are those satisfying the equation

\[ X_1^{q+1} + X_2^{q+1} + X_3^{q+1} = 0. \] (1)

Since the unitary group \( \text{PGU}(3, q) \) preserving \( \mathcal{H} \) acts transitively on the points of \( \text{PG}(2, q^2) \) not lying in \( \mathcal{H} \), we may assume \( P = (0, 1, 0) \). Then \( P^\perp \) has equation \( X_2 = 0 \). Also, since the stabilizer of \( P \) in \( \text{PGU}(3, q) \) acts
transitively on the non-absolute lines through \( P \), \( \ell \) may be assumed to be the line of equation \( X_3 = 0 \).

In the affine plane \( \text{AG}(2, q^2) \) arising from \( \text{PG}(2, q^2) \) with respect to the line \( X_3 = 0 \), we use the coordinates \( (X, Y) \) where \( X = X_1/X_3 \) and \( Y = X_2/X_3 \). Then the points of \( \mathcal{H} \) in \( \text{AG}(2, q^2) \) have affine coordinates \( (X, Y) \) that satisfy the equation

\[
X^{q+1} + Y^{q+1} + 1 = 0,
\]

whereas the points of \( \mathcal{H} \) at infinity are the \( q + 1 \) points \( M = (1, m, 0) \) with \( m^{q+1} + 1 = 0 \). In this setting the line \( \ell' \) is a vertical line and hence it has equation \( X - c = 0 \) where \( c^{q+1} + 1 \neq 0 \) as \( \ell' \) is a non-absolute line. In the following, we will use \( \ell_c \) to denote the line with equation \( X - c = 0 \).

Fix a point \( Q \) of \( \mathcal{H} \) lying on \( P^\perp \). Then \( Q = Q(a, 0) \) with \( a^{q+1} + 1 = 0 \). Take a point \( M = (1, m, 0) \) at infinity lying in \( \mathcal{H} \), and project it to \( \ell_c \) from \( Q \). If the point \( T = (c, t) \) is the result of the projection then \( t = (c - a)m \). Therefore, \( T \) lies on \( \mathcal{H} \) if and only if \( ca^q + ac^q + 2 = 0 \).

### 2.1 The case \( q \) odd

Let \( q \) be an odd prime power. As \( a^2 = -a^{-1} \), \( ca^q + ac^q + 2 = 0 \) can also be written in the form

\[
a^2c^q + 2a - c = 0.
\]

By abuse of notation, let \( \sqrt{1 + c^{q+1}} \) and \( -\sqrt{1 + c^{q+1}} \) denote the roots of the equation \( Z^2 = 1 + c^{q+1} \). Then the solutions of (2) are

\[
a_{1,2} = \frac{-1 \pm \sqrt{1 + c^{q+1}}}{c^q}.
\]

Here, \( \sqrt{1 + c^{q+1}} \in \text{GF}(q) \) if and only if \( 1 + c^{q+1} \) is a (non-zero) square element in \( \text{GF}(q) \). Actually, this case cannot occur. In fact, (2) together with \( \sqrt{1 + c^{q+1}} \in \text{GF}(q) \) yield \( c^q a + 1 = \pm \sqrt{1 + c^{q+1}} \) whence

\[
(c^q a + 1)^{q+1} = (\sqrt{1 + c^{q+1}})^{q+1} = (\sqrt{1 + c^{q+1}})^2 = 1 + c^{q+1}.
\]

Expanding the left hand side and using \( a^{q+1} = -1 \) we obtain \( ca^q + ca^q = 2c^{q+1} \) whence \( -c + c^q a^2 - 2ac^{q+1} = 0 \). Subtracting (2) gives either \( 1 + c^{q+1} = 0 \), or \( a = 0 \). The former case cannot occur by the choice of \( \ell_c \). In the latter case, \( Q = (0, 0) \) but the origin does not lie in \( \mathcal{H} \).

Therefore, \( \sqrt{1 + c^{q+1}} \in \text{GF}(q^2) \setminus \text{GF}(q) \). Hence \( \sqrt{1 + c^{q+1}} = iu \), with \( u \in \text{GF}(q) \) where \( \text{GF}(q^2) \) is considered as the quadratic extension of \( \text{GF}(q) \).
by adjunction of a root $i$ of the polynomial $X^2 - s$ with a fixed non-square element $s \in \mathbb{GF}(q)$. From $i^q = -i$, we get $(\sqrt{1 + c^{q+1}})^q = -\sqrt{1 + c^{q+1}}$. Hence

$$a_1^{q+1} = a_1^q a_1 = -a_1 a_2 = -(\frac{\sqrt{1 + c^{q+1} - 1}}{\sqrt{1 + c^{q+1} + 1}}) = -1.$$  

This shows that $Q_1 = (a_1, 0)$ lies in $\mathcal{H}$. Similarly, $Q_2 = (a_2, 0) \in \mathcal{H}$.

Since $a_1$ and $a_2$ do not depend on the choice of $M$, both points $Q_1$ and $Q_2$ are full points with respect to the line pair $(\ell, \ell_c)$. The projection $\varphi$ with center $Q_1$ which maps $\ell$ to $\ell_c$ takes the point $M = (1, m, 0)$ to the point $T' = (c, m(c - a_1))$, and the projection $\varphi'$ with center $Q_2$ mapping $\ell_c$ to $\ell$ takes the point $T = (c, t)$ to the point $M' = (1, m', 0)$ with $m' = t(c - a_2)^{-1}$. Therefore, the product $\psi = \varphi' \circ \varphi$ is the automorphism of the line $\ell_c$ with equation

$$M' = d M,$$  

where $d = \frac{c - a_1}{c - a_2} = -\frac{1 - \sqrt{1 + c^{q+1}}}{1 + \sqrt{1 + c^{q+1}}}$. We show that $\psi^q$ is the identity automorphism of $\ell$. From (4), $\psi^q$ takes the point $M = (1, m, 0)$ to the point $M(1, \bar{m}, 0)$, where $\bar{m} = d^{q+1} m$ with

$$d^{q+1} = \left(-\frac{1 - \sqrt{1 + c^{q+1}}}{1 + \sqrt{1 + c^{q+1}}} \right)^q \left(-\frac{1 - \sqrt{1 + c^{q+1}}}{1 + \sqrt{1 + c^{q+1}}} \right)^q = \left(-\frac{1 - \sqrt{1 + c^{q+1}}}{1 + \sqrt{1 + c^{q+1}}} \right)^{q+1}.$$  

Since $\sqrt{1 + c^{q+1}} = -\sqrt{1 + c^{q+1}}$ this yields $d = 1$.

Now we count the automorphisms $\psi$ when $c$ ranges over $\mathbb{GF}(q^2)$.

We show that each $u \in \mathbb{GF}(q^2)$ produces such an automorphism. Observe that $(iu)^2 = su^2$ is a non-square element in $\mathbb{GF}(q)$. As the norm function $x \mapsto x^{q+1}$ from $\mathbb{GF}(q^2)$ in $\mathbb{GF}(q)$ is surjective, $\mathbb{GF}(q^2)$ contains an nonzero element $c$ such that $su^2 = 1 + c^{q+1}$. Therefore, either $iu = \sqrt{1 + c^{q+1}}$, or $iu = -\sqrt{1 + c^{q+1}}$. With this notation,

$$M' = -\frac{1 - iu}{1 + iu} M.$$  

Any two different choices of $u$ in $\mathbb{GF}(q^2)$ produce two different automorphisms of $\ell$. In fact, if $u, v \in \mathbb{GF}(q)$,

$$-\frac{1 - iu}{1 + iu} = -\frac{1 - iv}{1 + iv}$$  

then $u = v$.

Therefore, we have produced as many as $q - 1$ pairwise distinct nontrivial automorphisms $\psi_u$. A further nontrivial automorphism of $\ell$ preserving $\ell \cap \mathcal{H}$ is
\(\psi_0\) of equation \(m' = -m\) which is the restriction on \(\ell\) of the linear collineation \((X_1, X_2, X_3) \mapsto (X_1, -X_2, X_3)\) belonging to \(\text{PGU}(3, q)\). In fact, \(\psi_0\) occurs for \(u = 0\) in (5). Furthermore, \(\psi_0\) is an involution, and hence its \(q + 1\)-st power is the identity. All these automorphisms together with the identity \(\psi_\infty\) form a set of \(q + 1\) automorphisms of \(\ell\) which preserve \(\ell \cap \mathcal{H}\). To show that they form a group \(\Psi\), replace \(u\) with \(v/s\) in (5). Then (5) reads

\[
m' = \frac{1 - uv}{1 + uv} m, \tag{6}\]

and the claim follows from the fact that the product of two such maps takes \(m\) to

\[
\frac{1 - uv}{1 + uv} \frac{1 - iw}{1 + iw} m = \frac{1 - iz}{1 + iz} m
\]

with

\[
z = \frac{v + w}{1 + vw}.
\]

On other hand, the cyclic automorphism group of \(\ell\) consisting of all maps of equation \(m' = hm\) with \(h \in GF(q^2)^*\) fixes \(P = (0, 1, 0)\) and \(R = (1, 0, 0)\). Therefore its subgroup \(\Psi\) is also cyclic, and leaves \(\ell \cap \mathcal{H}\) invariant acting on it regularly.

### 2.2 The case \(q\) even

Let \(q = 2^r \geq 4\). From \(a^{q+1} + 1 = 0\) and \(t = (a + c)m\), we have \(a = \sqrt{\frac{-1}{c}}\). Therefore, \(T \in \mathcal{H}\) if and only if \(a = \sqrt{\frac{-1}{c}}\). This shows that \(a\) is independent of the choice of \(M\) on \(\ell\). Thus, \(Q\) is a full point for the line pair \((\ell, \ell_c)\). It is easily seen that \(Q\) is also a full point for the pair \((\ell_c, \ell)\).

Take two distinct non-absolute lines \(\ell_{c_1}\) and \(\ell_{c_2}\) through \(P\) with \(c_1 \neq 0 \neq c_2\), and let

\[
\gamma(c_1, c_2) = c_2(1 + c_1^{q+1}) + c_1(1 + c_2^{q+1}).
\]

A straightforward computation shows that \(Q = (a, 0)\) with \(a^{q+1} + 1 = 0\) is the full point for the line pair \((\ell_{c_1}, \ell_{c_2})\) if and only if

\[
a = \sqrt[2]{\frac{\gamma(c_1, c_2)}{\gamma(c_1, c_2)^2}}. \tag{7}\]

Furthermore, the projection with center \(Q\) which maps \(\ell_{c_1}\) to \(\ell_{c_2}\), takes the point \(M = (c_1, m)\) to the point \(T = (c_2, m(a + c_1)/(a + c_2))\).
Lemma 2.1. For any given $c_1 \in \text{GF}(q^2)^*$, with $c_1^{q+1} \neq 1$, there exists only one further $c_2 \in \text{GF}(q^2)^*$, with $c_2^{q+1} \neq 1$ such that

$$\gamma(c_1, c_2) = c_2(1 + c_1^{q+1}) + c_1(1 + c_2^{q+1}) = 0.$$  \hspace{1cm} (8)

In particular, $c_2 = c_1 t$, for some $t \in \text{GF}(q)^*$.

Proof. Let $c_1 = x_1 + iy_1$ and $c_2 = x_2 + iy_2$. Then, $c_1^{q+1} = x_1^2 + x_1 y_1 + sy_1^2$ and $c_2^{q+1} = x_2^2 + x_2 y_2 + sy_2^2$.

Since

$$c_2(1 + c_1^{q+1}) = x_2(1 + x_1^2 + x_1 y_1 + sy_1^2) + iy_2(1 + x_1^2 + x_1 y_1 + sy_1^2)$$

and

$$c_1(1 + c_2^{q+1}) = x_1(1 + x_2^2 + x_2 y_2 + sy_2^2) + iy_1(1 + x_2^2 + x_2 y_2 + sy_2^2),$$

equation (8) holds if and only if

$$\begin{cases} x_2(1 + x_1^2 + x_1 y_1 + sy_1^2) + x_1(1 + x_2^2 + x_2 y_2 + sy_2^2) = 0 \\ y_2(1 + x_1^2 + x_1 y_1 + sy_1^2) + y_1(1 + x_2^2 + x_2 y_2 + sy_2^2) = 0. \end{cases}$$

If $x_1 = 0$ then $c_1 = iy_1$ with $y_1 \neq 1$, and from the above equations, $x_2 = 0$ and $y_2$ is a root of the polynomial in $\xi$

$$sy_1 \xi^2 + (1 + sy_1^2) \xi + y + 1.$$  \hspace{1cm} (9)

Since $y_1$ is also a root of (9), $y_1$ and $y_2$ are the two roots and the assertion is proven in this case. If $y_1 = 0$, a similar argument can be used to prove the assertion.

Therefore $x_1 \neq 0 \neq y_1$ may be assumed. From

$$\begin{cases} y_1 x_2(1 + x_1^2 + x_1 y_1 + sy_1^2) + y_1 x_1(1 + x_2^2 + x_2 y_2 + sy_2^2) = 0 \\ x_1 y_2(1 + x_1^2 + x_1 y_1 + sy_1^2) + x_1 y_1(1 + x_2^2 + x_2 y_2 + sy_2^2) = 0 \end{cases}$$  \hspace{1cm} (10)
we infer \( y_1 x_2 = x_1 y_2 \), that is, \( y_2 = y_1 x_2 x_1^{-1} \). Replacing \( y_2 \) by \( y_1 x_2 x_1^{-1} \) in the first equation of (10) shows that \( x_2 \) is a root of the polynomial in \( \xi \)

\[
(x_1^2 + y_1 x_1 + sy_1^2)x_1^{-1} \xi^2 + (1 + x_1^2 + x_1 y_1 + sy_1^2) \xi + x_1 = 0. \tag{11}
\]

Since \( x_1 \) is another root of (11), \( x_1 \) and \( x_2 \) are the roots, and the assertion is proven.

For the rest of this section, let

\[
a_i = \sqrt{\frac{c_i}{c_i^q}}, \quad i = 1, 2.
\]

Project \( \ell \) to \( \ell_{c_1} \) from \( Q_1(a_1, 0) \), then project \( \ell_{c_1} \) to \( \ell_{c_2} \) from \( Q = (a, 0) \), and finally project \( \ell_{c_2} \) to \( \ell \). The result is the automorphism \( \psi_{c_1,c_2} \) of the line \( \ell \), viewed as \( \text{PG}(1, q^2) \), defined by the equation

\[
\psi_{c_1,c_2}((1, m, 0)) = (1, d(c_1, c_2)m, 0)
\]

where

\[
d(c_1, c_2) = \frac{(a + c_2)(a_1 + c_1)}{(a + c_1)(a_2 + c_2)}.
\]

Using the definition of \( a, a_1, a_2 \), a straightforward computation gives \( d(c_1, c_2)^2 \) as a rational function of \( c_1 \) and \( c_2 \):

\[
d(c_1, c_2)^2 = \frac{c_1 c_2^q (1 + c_1^q c_2)}{c_1 c_2 (1 + c_1 c_2^q)},
\]

whence

\[
d(c_1, c_2) = \sqrt{\frac{c_1 c_2^q (1 + c_1^q c_2)}{c_1 c_2 (1 + c_1 c_2^q)}}.
\]

This also shows that \( d(c_1, c_2) \) is of the form \( \alpha^q / \alpha = \alpha^{q-1} \) for some \( \alpha \in \text{GF}(q^2) \). Hence \( d^{q+1} = 1 \).

**Lemma 2.2.** Let \( \alpha, \beta \in \text{GF}(q^2)^* \) with \( \alpha + \alpha^{q+1} \neq 0 \neq \beta + \beta^{q+1} \). Then there exists \( \delta \in \text{GF}(q^2)^* \) such that

\[
\frac{\alpha^q + \alpha^{q+1}}{\alpha + \alpha^{q+1}} \cdot \frac{\beta^q + \beta^{q+1}}{\beta + \beta^{q+1}} = \frac{\delta^q + \delta^{q+1}}{\delta + \delta^{q+1}}.
\]

7
Proof. If $\delta = a + ib$, then there exist $c, d \in \text{GF}(q)$ such that

$$
\frac{\delta^q + \delta^{q+1}}{\delta + \delta^{q+1}} = \frac{c + d + id}{c + id}.
$$

Let $\alpha = x + iy$ and $\beta = u + iv$, with $x, y, u, v \in \text{GF}(q)$. Then

$$
(a^q + a^{q+1})(\beta^q + \beta^{q+1}) = (x + y + x^2 + xy + sy^2)(u + v + u^2 + uv + sv^2) + svy \\
i[(x + x^2 + xy + sy^2)v + (u + u^2 + uv + sv^2)y + yv]
$$

and the expression on the right hand side is equal to

$$
(x + x^2 + xy + sy^2)(u + u^2 + uv + sv^2) + svy \\
i[(x + x^2 + xy + sy^2)v + (u + u^2 + uv + sv^2)y + yv].
$$

Therefore,

$$
(x + x^2 + xy + sy^2)(u + u^2 + uv + sv^2) + svy \\
+ (x + x^2 + xy + sy^2)v + (u + u^2 + uv + sv^2)y + yv = \\
(x + x^2 + xy + sy^2)(u + vu^2 + uv + sv^2)y(u + u^2 + uv + sv^2) + svy = \\
(x + x^2 + xy + sy^2)v + (u + vu^2 + uv + sv^2)y + svy.
$$

Therefore, in the group $\text{PGL}(2, q^2)$ of all automorphisms of $\ell$, the maps

$$
\psi_{c_1, c_2}, \quad \text{with } c_1^{q+1} \neq 1 \neq c_2^{q+1}, \quad \gamma(c_1, c_2) \neq 0
$$

form an abelian subgroup $\Psi$ and the order of each automorphism in $\Psi$ is divisible by $q + 1$.

A good choice for $c_1, c_2$ is $c_1 = s$ and $c_2 = is^{-1}$. In this case, $\gamma(c_1, c_2) = i^{q-1}$ and $d(c_1, c_2) = i^{q-1}$. Hence $\psi_{c_1, c_2}(1, m, 0) = (1, i^{q-1}m, 0)$. Since $i^{q-1}$ is a primitive $(q + 1)$-st root of unity, $\Psi$ contains a cyclic subgroup of order $q + 1$. Since $\Psi$ leaves $\mathcal{H} \cap \ell$ invariant, this shows that $\Psi$ acts on $\mathcal{H} \cap \ell$ regularly, and $\Psi$ is a cyclic group of order $q + 1$.

3 Embedding of the polar classical unital in $\text{PG}(2, q^2)$

Let $\mathcal{U}$ be a classical polar unital isomorphic, as design, to a Hermitian unital of $\text{PG}(2, q^2)$. Assume that $\mathcal{U}$ is embedded in $\text{PG}(2, q^2)$. Take any point $P$ is outside $\mathcal{U}$. Since the arguments used in Section 2 only involve points, secants
and their incidences, all assertions stated there for a Hermitian unital remains true for $\mathcal{U}$. This together with the results proven in Section 2 show that there is a cyclic automorphism group $C_{q+1}$ of the line $\ell$ which preserves $\ell \cap \mathcal{U}$. We are not claiming that $C_{q+1}$ extends to a collineation group of $\text{PG}(2, q^2)$. We only use the facts that $C_{q+1}$ consists of automorphisms leaving $\ell \cap \mathcal{U}$ invariant and that $C_{q+1}$ acts on it regularly. By Dickson’s classification of subgroups of $\text{PGL}(2, q^2)$, see [12] or [7, Theorem A.8], the automorphism group of $\ell$, we have that $C_{q+1}$ is conjugate to the subgroup $\Sigma$ consisting of all maps $m' = wm$ where $w^{q+1} = 1$. In other words, we can change the projective frame so that $\ell \cap \mathcal{U}$ becomes a (nontrivial) $\Sigma$-orbit. Since each nontrivial $\Sigma$-orbit is a Baer subline of $\ell$, so is $\ell \cap \mathcal{U}$. As the unitary group $\text{PGU}(3, q)$ acts transitively on the block of $\mathcal{U}$, we get that each block is a Baer subline, giving $\mathcal{U}$ is projectively equivalent to a Hermitian unital in $\text{PG}(2, q^2)$, see [4, 9].

References


