Inherited unitals in Moulton planes

Gábor Korchmáros, Angelo Sonnino

Dipartimento di Matematica, Informatica ed Economia
Università degli Studi della Basilicata
Viale dell’Ateneo Lucano 10, 85100 Potenza, Italy

Tamás Szőnyi

ELTE Eötvös Loránd University, Institute of Mathematics and
MTA-ELTE Geometric and Algebraic Combinatorics Research Group
H-1117 Budapest, Pázmány P. s. 1/c, Hungary

Received 11 January 2017, accepted 24 July 2017, published online 4 September 2017

Abstract

We prove that every Moulton plane of odd order—by duality every generalised André plane—contains a unital. We conjecture that such unitals are non-classical, that is, they are not isomorphic, as designs, to the Hermitian unital. We prove our conjecture for Moulton planes which differ from \( \text{PG}(2, q^2) \) by a relatively small number of point-line incidences. Up to duality, our results extend previous analogous results—due to Barwick and Grünig—concerning inherited unitals in Hall planes.

Keywords: Unitals, Moulton planes.

Math. Subj. Class.: 51E20, 05B25

1 Introduction

A unital is a set of \( q^3 + 1 \) points together 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 \( 2-(q^3+1, q+1, 1) \). The classical example of a unital arises from the unitary polarity in the Desarguesian projective plane \( \text{PG}(2, q^2) \) where the points are the absolute points, and the blocks are the non-absolute lines of the unitary polarity. The name of “Hermitian unital” is commonly used for the

---

*This research was carried out within the activities of the GNSAGA of the Italian INdAM.

E-mail address: gabor.korchmaros@unibas.it (Gábor Korchmáros), angelo.sonnino@unibas.it (Angelo Sonnino), szonyi@cs.elte.hu (Tamás Szőnyi)

© Creative Commons This work is licensed under http://creativecommons.org/licenses/by/3.0/
classical example since the absolute points of the unitary polarity are the points of the Hermitian curve defined over GF(q^2).

A unital U is embedded in a projective plane Π of order q^2, if its points are points of Π and its blocks are intersections with lines. As usual, we adopt the term “chord” to indicate a block of U. A line ℓ of Π is either a tangent or a (q + 1)-secant to U according as |ℓ ∩ U| = 1 or |ℓ ∩ U| = q + 1, and in the latter case ℓ ∩ U is a chord. Examples of unitals embedded in PG(2, q^2) other than the Hermitian ones are known to exist.

A unital is classical if it is isomorphic, as a block-design, to a Hermitian unital. Classical unitals contain no O’Nan configurations, and it has been conjectured that any non-classical unital embedded in PG(2, q^2) must contain a O’Nan configuration.

In several families of non-desarguesian planes, the problem of constructing and characterizing unitals has also been investigated; see [1, 2, 5, 6, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 22, 23, 24, 27, 28]. Apart from the examples of unitals arising from a unitary polarity in a commutative semifield plane, the known examples are inherited unitals from the Hermitian unital. In a non-desarguesian plane Π of order q^2 arising from PG(2, q^2) by altering some of the point-line incidences, the adjective “inherited” is used for those pointsets of PG(2, q^2) which keep their intersection properties with lines when moving from PG(2, q^2) to Π.

In this paper we construct inherited unitals in Moulton planes of odd order q^2, and, by duality, in generalised André planes of the same order; see Theorem 3.1. We also investigate the problem whether these unitals are classical; see Theorems 3.5 and 3.6. We show that if such a plane differs from PG(2, q^2) by a relatively small number of incidences only, then the inherited unital is non-classical. Also, we exhibit non-classical inherited unitals in case of many point-line incidence alterations. Such unitals appear to be of interest in coding theory; see [25].

What emerges from our work leads us to conjecture that the inherited unitals constructed in our paper are all non-classical. It should be noticed that our results extend previous analogous results due to Barwick and Grüning concerning inherited unitals in Hall planes which are very special André planes; see [8, 16] and Remark 3.4. The methods used in [8] are mostly geometric and involve Baer subplanes and blocking sets. In this paper, we adopt a more algebraic approach that allows us to exploit results on the number of solutions of systems of polynomial equations over a finite field.

2 Two new results on the Hermitian unital

We establish and prove two theorems on Hermitian unitals that will play a role in our study on unitals in Moulton planes.

Up to a change of the homogeneous coordinate system (X_1, X_2, X_3) in PG(2, q^2), the points of the classical unital U are those satisfying the equation

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

(2.1)

In the affine plane AG(2, q^2) arising from 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 U in AG(2, q^2) are the solutions of the equation

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

(2.2)

Since GF(q^2) is the quadratic extension of GF(q) by adjunction of a root i of the polynomial \( X^2 - s \) with a non-square element s of GF(q), every element u of GF(q^2) can
uniquely be written as \( u = u_1 + iu_2 \) with \( u_1, u_2 \in \text{GF}(q) \). Then \( u^q = u_1 - iu_2 \) and \( \|u\|^q = u_1^q + 1 = u_1^2 - su_2^2 \). Therefore, the points \( P(x, y) \in \mathcal{U} \) lying in \( \text{AG}(2, q^2) \) are those satisfying the equation

\[
x_1^2 - sx_2^2 + y_1^2 - sy_2^2 + 1 = 0.
\]

(2.3)

For a subset \( T \subseteq \text{GF}(q) \setminus \{0\} \), let \( \mathcal{S}_T \) denote the set of points \( \{(x, y) \mid \|x\| = t \in T\} \). Hence the pointset \( \mathcal{S}_T \cap \mathcal{U} \) comprises all points \( P(x, y) \) such that both \( x_1^2 - sx_2^2 = t \) and (2.3) hold. Therefore, a point \( P(x, y) \in \text{AG}(2, q^2) \) is in \( \mathcal{S}_T \cap \mathcal{U} \) if and only if \( P_1(x_1, x_2) \in \text{AG}(2, q) \) lies on the non-degenerate conic \( C_1 : x^2 - sy^2 - t = 0 \) while \( P_2(y_1, y_2) \in \text{AG}(2, q) \) does lie on the conic \( C_2 : x^2 - sy^2 + 1 + t = 0 \). This shows that \( \mathcal{S}_T \cap \mathcal{U} \) has size \((q + 1)^2\) apart from the case \( t = -1 \) when it consists of the \( q + 1 \) points of \( \mathcal{U} \) lying on the \( X \)-axis.

**Lemma 2.1.** Let \( \ell \) be a non-vertical line in \( \text{AG}(2, q^2) \). Then \( |\ell \cap \mathcal{U} \cap \mathcal{S}_1| \in \{0, 1, 2, q + 1\} \) for every \( t \in T \). If \( q + 1 \) occurs then \( \ell \) is either a horizontal line, or it passes through the origin.

**Proof.** The points \( P(x, 0) \) with \( \|x\| = t \) form a Baer subline. As \( \mathcal{U} \) is classical, \( \ell \cap \mathcal{U} \) is a Baer subline of \( \ell \), and hence the projection of \( \ell \cap \mathcal{U} \) on the \( X \)-axis from \( Y_\infty \) is a Baer-subline, as well. Since two distinct Baer sublines have at most two common points, the first assertion follows. To prove the second one, we need some computation. If \( \ell \) has equation \( Y = Xm + b \), we have to count the roots \( x \) of the polynomial \( f(X) = X^{q+1} + (Xm + b)q+1 + 1 \) whose norm \( \|x\| \) is equal to \( t \). If \( \|x\| = t \), then \( f(x) = bm^2x^q + b^qmx + t(1 + m^q + 1) + b^q + 1 \) and hence

\[
x f(x) = b^qmx^2 + (t(1 + m^q + 1) + b^q + 1)x + bm^qt.
\]

If we have at least three such roots \( x \) then either \( m = 0 \) and \( t + 1 = -b^q + 1 \), or \( b = 0 \) and \( t(1 + m^q + 1) = -1 \).

Take any two distinct non-tangent lines \( \ell_1 \) and \( \ell_2 \) of \( \mathcal{U} \). We are interested in the intersection of the projection of \( \ell_1 \cap \mathcal{U} \) from \( P \) on \( \ell_2 \) with \( \ell_2 \cap \mathcal{U} \). For any point \( P \) outside both \( \ell_1 \) and \( \ell_2 \), the projection of \( \ell_1 \) to \( \ell_2 \) from \( P \) takes the chord \( \ell_1 \cap \mathcal{U} \) to a Baer subline of \( \ell_2 \). Since two Baer sublines of \( \ell_2 \) intersect in \( 0, 1, 2 \) or \( q + 1 \) points, one may want to determine the size of the sets \( \Sigma_i \) \((i = 0, 1, 2, q + 1)\) consisting of all points \( P \) for which this intersection number is equal to \( i \). The points in \( \Sigma_i \) are called elliptic, parabolic, hyperbolic, or full with respect to the pair \( (\ell_1, \ell_2) \), according as \( i = 0 \), \( i = 1 \), \( i = 2 \), or \( i = q + 1 \), respectively; see [21].

We go on to compute the size of \( \Sigma_i \cap \mathcal{U} \). Since the linear collineation group \( G \cong \text{PGU}(3, q) \) of \( \text{PG}(2, q^2) \) preserving \( \mathcal{U} \) acts transitively on the points outside \( \mathcal{U} \), we may assume that \( Y_\infty = \ell_1 \cap \ell_2 \). The stabiliser of \( Y_\infty \) in \( G \) acts on the pencil with center in \( Y_\infty \) as the general projective group \( \text{PGL}(2, q) \) on the projective line \( \text{PG}(1, q^2) \). Therefore, it has two orbits, one consisting of all tangents the other of all chords to \( \mathcal{U} \) through \( Y_\infty \). This allows us to assume without loss of generality that \( \ell_1 \) is the line at infinity. Since \( \ell_2 \) is not a tangent to \( \mathcal{U} \), its equation is of the form \( X = c \) with \( c^{q+1} + 1 \neq 0 \). Therefore, \( c^{q+1} + 1 \) is either a non-zero square or a non-square element of \( \text{GF}(q) \). These two cases occur depending upon whether a linear collineation \( \gamma \in \text{PGL}(2, q) \) taking \( \ell_1 \) to \( \ell_2 \) is in the subgroup isomorphic to the special projective group \( \text{PSL}(2, q) \) or not. Accordingly, \( (\ell_1, \ell_2) \) is called a *special* pair or a *general* pair. Further, since \( P \) is a point outside \( \ell_1 \) and \( \ell_2 \), it is an affine point \( P = (a, b) \) with \( a \neq c \).
Let \( P = (a, b) \) denote a point of \( U \), that is,
\[
a^{q+1} + b^{q+1} + 1 = 0. 
\] (2.4)

Take a line \( r \) of equation \( Y = m(X - a) + b \) through \( P = (a, b) \). A necessary and sufficient condition for \( r \) to meet both \( \ell_1 \) and \( \ell_2 \) in \( U \) is the existence of a solution \( \tau \in \text{GF}(q^2) \) of the system consisting of (2.4) together with
\[
c^{q+1} + \tau^{q+1} + 1 = 0,  
\] (2.5)
\[
m^{q+1} + 1 = 0.  
\] (2.6)

In fact, \( Q(c, \tau) \) with \( \tau = m(c - a) + b \) is the point of \( r \) on \( \ell_2 \). Then (2.5) holds if and only if \( Q \in U \). Furthermore, (2.6) is the necessary and sufficient condition for the infinite point of \( r \) to be in \( U \); see Figure 1.

The above discussion also shows how to count lines through \( P \) meeting both \( \ell_1 \cap U \) and \( \ell_2 \cap U \). Essentially, one has to find the number of solutions in the indeterminate \( \tau \) of the system consisting of the equations (2.4), (2.5), and (2.6). Observe that (2.4), (2.5), (2.6) are equivalent to
\[
a_1^2 - sa_2^2 + b_1^2 - sb_2^2 + 1 = 0,  
\] (2.7)
\[
c_1^2 - sc_2^2 + \tau_1^2 - s\tau_2^2 + 1 = 0,  
\] (2.8)
\[
b_1\tau_1 - sb_2\tau_2 + a_1c_1 - sa_2c_2 + 1 = 0.  
\] (2.9)

From this the following result is obtained.

**Proposition 2.2.** The number of lines through \( P \) meeting both \( \ell_1 \cap U \) and \( \ell_2 \cap U \) equals the number of solutions \((\tau_1, \tau_2)\), with \( \tau_1, \tau_2 \in \text{GF}(q) \), of the system consisting of (2.7), (2.8), (2.9).
In investigating the above system, two cases are distinguished according as \((b_1, b_2)\) is \((0, 0)\) or not.

In the former case, Equations (2.7) and (2.9) read \(a_1^2 - sa_2^2 + 1 = 0\) and \(a_1 c_1 - sa_2 c_2 + 1 = 0\). Geometrically in \(\text{AG}(2, q)\), the point \(U = (a_1, a_2)\) is the intersection of the ellipse \(E\), with equation \(X^2 - sY^2 + 1 = 0\), and the line \(v\) with equation \(c_1X - sc_2Y + 1 = 0\). Since \(c_{q+1}^2 + 1 = c_1^2 - sc_2^2 + 1\) is a non-zero element in \(\text{GF}(q)\), \(v\) must be either a secant, or an external line to \(E\) and this occurs according as \(c_1^2 - sc_2^2 + 1\) is a non-zero square or non-square element in \(\text{GF}(q)\). In fact, from (2.7) and (2.9),

\[
a_1 = \frac{sc_2 a_2 - 1}{c_1}, \quad a_2 = \frac{-sc_2 \pm ic_1 \sqrt{c_1^2 - sc_2^2 + 1}}{s(c_1^2 - sc_2^2)},
\]

Therefore, if \(P\) is on the \(X\)-axis, then \(P\) is elliptic in general, apart from the case where \(c_{q+1}^2 + 1 = c_1^2 - sc_2^2 + 1\) is a non-square element in \(\text{GF}(q)\) and \(P\) is one of the two common points of \(C\) and \(v\), namely \(P = P(a, 0)\) where

\[
a = a_1 + ia_2 = \frac{-1 \pm \sqrt{1 + c_{q+1}^2}}{c_1}.
\]

Further, in the exceptional case, \(P\) is a full point as for any \(c_1, c_2 \in \text{GF}(q)\) with \(c_1^2 - sc_2^2 + 1 \neq 0\), Equation (2.8) always has \(q + 1\) solutions \((\tau_1, \tau_2)\) with \(\tau_1, \tau_2 \in \text{GF}(q)\).

In the latter case, either \(b_1\) or \(b_2\) is not zero. If \(b_1 \neq 0\), retrieving \(\tau_1\) from (2.9) and putting it in (2.8) gives a quadratic equation in the indeterminate \(\tau_2\), namely

\[
(b_1^2 - sb_2^2)\tau_2^2 - 2sb_1 b_2 (a_1 c_1 - sa_2 c_2 + 1)\tau_2 + (a_1 c_1 - sa_2 c_2 + 1)^2 + b_1^2 (1 + c_1^2 - sc_2^2) = 0, \quad (2.10)
\]

whose discriminant is \(\Delta_1 = sb_1^2 \Delta\) with

\[
\Delta = (b_1^2 - sb_2^2)(1 + c_1^2 - sc_2^2) + (a_1 c_1 - sa_2 c_2 + 1)^2
\]

which can also be written by (2.7) as

\[
\Delta = -(1 + c_1^2 - sc_2^2)(a_1^2 - sa_2^2 + 1) + (a_1 c_1 - sa_2 c_2 + 1)^2.
\]

For \(b_2 \neq 0\), retrieving \(\tau_2\) from (2.9) and putting it in (2.8) gives the following quadratic equation in the indeterminate \(\tau_1\):

\[
(-b_1^2 + b_2^2)\tau_1^2 + 2a_1 b_1 c_1 \tau_1 - a_1^2 - s^2 a_2^2 c_2^2 - b_2^2 c_1^2 + sb_1^2 c_2^2 + 2sa_2 c_2 - b_2^2 - 1 = 0 \quad (2.11)
\]

with discriminant \(\Delta_2 = s^3 b_2^2 \Delta\). Since \(\Delta_1\) and \(\Delta_2\) are simultaneously zero, or a square, or a non-square in \(\text{GF}(q)\), each of the equations (2.10) and (2.11) has 2, 1 or zero solutions in \(\text{GF}(q)\), depending upon whether \(\Delta\) is a square element, zero, or a non-square element of \(\text{GF}(q)\), respectively. This leads to the study of the zeroes of the polynomial

\[
F(X, Y, Z) = -(1 + c_1^2 - sc_2^2)(X^2 - sY^2 + 1) + (c_1 X - sc_2 Y + 1)^2 - Z^2. \quad (2.12)
\]

Geometrically, \(F(X, Y, Z) = 0\) is the equation of a quadric \(\mathcal{Q}\) in \(\text{AG}(3, q)\). Actually, \(\mathcal{Q}\)
Table 1: Elliptic, parabolic, hyperbolic and full points.

<table>
<thead>
<tr>
<th></th>
<th>$P(a, 0)$</th>
<th>$P(a, b), b \neq 0$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$1 +</td>
<td></td>
</tr>
<tr>
<td>$N_{E}$</td>
<td>$q + 1$</td>
<td>$q - 1$</td>
</tr>
<tr>
<td>$N_{P}$</td>
<td>$0$</td>
<td>$0$</td>
</tr>
<tr>
<td>$N_{H}$</td>
<td>$0$</td>
<td>$0$</td>
</tr>
<tr>
<td>$N_{F}$</td>
<td>$0$</td>
<td>$2$</td>
</tr>
</tbody>
</table>

is a cone. In fact, the system $F_X = F_Y = F_Z = 0$ has a (unique) solution $(c_1, c_2, 0)$ and hence the point $V(c_1, c_2, 0)$ is the vertex of $\mathcal{Q}$. In particular, the intersection of $\mathcal{Q}$ with the plane $Z = 0$ splits into two lines over $GF(q)$ or its quadratic extension $GF(q^2)$, and this occurs according as the infinite points of the conic with equation

$$-(1 + c_1^2 - sc_2^2)(X^2 - sY^2) + (c_1X - sc_2Y)^2 = 0$$

lie in $PG(2, q)$ or in $PG(2, q^2) \setminus PG(2, q)$. By a direct computation, this condition only depends on $c^{q+1}$, namely whether $1 + c^{q+1}$ is a square or a non-square element of $GF(q)$. Therefore, $\mathcal{Q}$ contains either $2q - 1$ or 1 points in the plane $Z = 0$, and this occurs according as the pair $\{\ell_1, \ell_2\}$ is special or general. Also, in the former case there are exactly $2q - 1$ parabolic points $P$ but in the latter case no point $P$ is parabolic. Therefore, the following result holds.

**Theorem 2.3.** Let $\ell_1, \ell_2$ be any two distinct non-tangent lines of the classical unital $\mathcal{U}$ in $PG(2, q^2)$ whose common point is off $\mathcal{U}$. The number $N_{E}, N_{P}, N_{H}, N_{S}$ of elliptic, parabolic, hyperbolic and full points of $\mathcal{U}$ with respect to the pair $\{\ell_1, \ell_2\}$ is given in Table 1.

We state a corollary of Theorem 2.3 that will be used in Section 3. For $i = 1, 2$ let $\Lambda_i$ be a subset of $\ell_i \cap \mathcal{U}$ such that $|\Lambda_1| = |\Lambda_2| = \lambda$.

**Theorem 2.4.** If

$$\lambda > \sqrt{(q + 1)(q + 3)}$$

(2.13)

there exists a non-degenerate quadrangle $A_1B_1A_2B_2$ with vertices $A_i, B_i \in \Lambda_i$ for $i = 1, 2$ such that its diagonal point $A_1B_2 \cap B_1A_2$ lies in $\mathcal{U}$.

**Proof.** We prove the existence of a hyperbolic point $D$ in $\mathcal{U}$ such that the projection of $\Lambda_1$ from $D$ on $\ell_2$ share two points with $\Lambda_2$. From Theorem 2.3, we have at least $\frac{1}{2}(q - 1)^2(q + 1)$ hyperbolic points in $\mathcal{U}$. We omit those hyperbolic points projecting $\overline{\Lambda_1} = (\ell_1 \cap \mathcal{U}) \setminus \Lambda_1$ to a pointset of $\ell_2$ meeting $\ell_2 \cap \mathcal{U}$ nontrivially. The number of such hyperbolic points is
Similarly we omit all hyperbolic points projecting $\Lambda_2 = (\ell_2 \cap U) \setminus \Lambda_2$ to a pointset of $\ell_1$ meeting $\ell_1 \cap U$ nontrivially. Therefore, the total number of omitted hyperbolic points is $2\bar{\lambda}(q^2 - 1) - \bar{\lambda}^2(q - 1) = (q - 1)\bar{\lambda}(2q + 2 - \bar{\lambda}(q - 1))$.

From Theorem 2.3, this number is smaller than the total number of hyperbolic points as far as (2.13) holds.

To state the other new result on the classical unital a couple of ad hoc notation in $AG(2, q^2)$ will be useful: For a non-vertical line $\ell$ with equation $Y = Xm + b$, $\bar{\ell}$ denotes the non-vertical line with equation $Y = Xm^q + b$. Given a point $P(a, b)$ outside $U$, two lines $\ell_1$ and $\ell_2$ are said to be a good line-pair whenever the lines $\bar{\ell}_1$ and $\bar{\ell}_2$ meet in a point of $U$. Our goal is to show that if $a \neq 0$ then there exist many good pairs.

For $i = 1, 2$, write the equations of $\ell_i$ in the form $Y = (X - a)m_i + b$. Then $\bar{\ell}_i$ has equation $Y = Xm_i^q - am_i + b$. Hence $\bar{P}(x, y) = \bar{\ell}_1 \cap \bar{\ell}_2$ where

$$x = \frac{a(m_1 - m_2)}{m_1^q - m_2^q},$$

and hence

$$y = \frac{a(m_1 - m_2)}{m_1^q - m_2^q}m_1^q - am_1 + b.$$

Note that

$$\|x\| = x^{q + 1} = a^{q + 1}\left(\frac{1}{(m_1 - m_2)^{q - 1}}\right)^{q + 1} = \frac{\|a\|}{(m_1 - m_2)^{q^2 - 1}} = \|a\| \neq 0.$$

The condition for $\bar{P}(x, y)$ to lie in $U$ is

$$x^{q + 1} + y^{q + 1} + 1 = a^{q + 1} + a^{q + 1}\left(\frac{1}{(m_1 - m_2)^{q - 1}}\right)^{q + 1} = 0.$$

Let

$$\xi = -\frac{a^{q + 1} + 1}{a^{q + 1}} \in GF(q).$$

Then the last equation reads

$$\left(\frac{m_1^q - m_1 + \frac{b}{a}}{(m_1 - m_2)^q}\right)^{q + 1} = \xi.$$ (2.14)

Henceforth we assume that

$$\|a\| \neq -1.$$

With

$$m_1 = \alpha + i\beta, \quad m_2 = \gamma + i\delta, \quad \frac{b}{a} = u + iv,$$

(2.14) reads

$$\left(\frac{(\alpha - \gamma) + i(\beta - \delta)}{(\alpha - \gamma) - i(\beta - \delta)}(\alpha - i\beta) - (\alpha + i\beta) + u + iv\right)^{q + 1} = \xi.$$
The above coefficients are related by the following equations:

\[ (u\alpha - u\gamma - sv\beta + sv\delta)^2 - s(2\beta\gamma - 2\alpha\delta - u(\beta - \delta) + v(\alpha - \gamma))^2 - \xi((\alpha - \gamma)^2 - s(\beta - \delta)^2) = 0, \]

that is,

\[ (u(\alpha - \gamma) - sv(\beta - \delta))^2 - s(2\beta\gamma - 2\alpha\delta - u(\beta - \delta) + v(\alpha - \gamma))^2 - \xi((\alpha - \gamma)^2 - s(\beta - \delta)^2) = 0. \]  \hspace{1cm} (2.15)

With \( \gamma = \alpha - \overline{\gamma}, \quad \delta = \beta - \overline{\delta}, \)

Equation (2.15) becomes

\[ (u\gamma - sv\delta)^2 - s(-2\beta\gamma - 2\alpha\delta - u\beta + v\alpha)^2 - \xi(\gamma^2 - s\delta^2) = 0, \]  \hspace{1cm} (2.16)

which can be viewed as a quadratic form in \( \gamma \) and \( \delta \):

\[ F(\gamma, \delta) = (u^2 - v^2 s + 4v\beta s - 4\beta^2 s - \xi)\gamma^2 + 2(-2u\beta s + 2v\alpha s - 4u\beta s)\gamma\delta + (-u^2 s - 4u\alpha s + v^2 s^2 - 4\alpha^2 s + s\xi)\delta^2 \]  \hspace{1cm} (2.17)

with discriminant

\[ \Delta = -u^4 s + 2u^2 v^2 s^2 + 2u^2 s\xi - v^4 s^3 - 2v^2 s^2 \xi - s\xi^2 + (-4u^3 s + 4uv^2 s^2 + 4us\xi)\alpha + (-4u^2 v s^2 + 4v^3 s^3 + 4v^2 s^2 \xi)\beta - 8uv s^2 \alpha\beta + (-4u^2 s + 4s\xi)\alpha^2 + (-4v^2 s^3 - 4s^2 \xi)\beta^2. \]

Note that \( \overline{F}(x, y) \in \mathcal{U} \) if and only if \( \Delta = \lambda^2 \) for some \( \lambda \in GF(q) \). This leads us to consider the quadric \( Q \) in \( AG(3, q) \) of equation

\[ a_{00} + a_{01} X + a_{02} Y + a_{12} XY + a_{11} X^2 + a_{22} Y^2 - Z^2 = 0, \]

where

\[
\begin{align*}
  a_{00} &= -u^4 s + 2u^2 v^2 s^2 + 2u^2 s\xi - v^4 s^3 - 2v^2 s^2 \xi - s\xi^2, \\
  a_{01} &= -4u^3 s + 4uv^2 s^2 + 4us\xi, \\
  a_{02} &= 4u^2 v s^2 + 4v^3 s^3 + 4v^2 s^2 \xi, \\
  a_{12} &= -8uv s^2, \\
  a_{11} &= -4u^2 s + 4s\xi, \\
  a_{22} &= -4v^2 s^3 - 4s^2 \xi.
\end{align*}
\]

The above coefficients are related by the following equations:

(i) \( a_{00} - \frac{1}{2}(\frac{1}{2}a_{01}u - \frac{1}{2}a_{02}v) = s\xi(u^2 - sv^2 - \xi); \)

(ii) \( \frac{1}{2}a_{01} - \frac{1}{2}(a_{11}u - \frac{1}{2}a_{12}v) = 0; \)
Therefore, the determinant $D$ of the $4 \times 4$ matrix associated with $Q$ is equal to $-s\xi(u^2 - sv^2 - \xi)$ multiplied by the determinant of the cofactor of $a_{00}$. The latter determinant $a_{11}a_{22} - \frac{1}{4}a_{12}^2$ is equal to

$$D_0 = s^3\xi(u^2 - sv^2 - \xi) = s^3(a^{q+1} + b^{q+1} + 1)(a^{q+1} + 1).$$

(2.18)

It turns out that

$$D = -(s^2\xi(u^2 - sv^2 - \xi))^2.$$

Observe that $\xi = 0$ if and only if $a^{q+1} = -1$, while

$$u^2 - sv^2 - \xi = \frac{b^{q+1}}{a^{q+1}} + \frac{a^{q+1} + 1}{a^{q+1}} = \frac{a^{q+1} + b^{q+1} + 1}{a^{q+1}}$$

vanishes only for $P(a, b) \in \mathcal{U}$. Therefore, $Q$ is non-degenerate. More precisely, the quadric $Q$ is either elliptic or hyperbolic according as $q \equiv -1 \mod 4$ or $q \equiv 1 \mod 4$. The plane at infinity cuts out from $Q$ a conic $C$ with homogeneous equation $a_{11}X^2 + a_{12}XY + a_{22}Y^2 - Z^2 = 0$. Observe that $C$ is non-degenerate by $D_0 \neq 0$. Thus, the number of points of $Q$ in $AG(3, q)$ is $q^2 \pm q$ with $q \equiv \pm 1 \mod 4$. Furthermore, the point at infinity $Z_\infty$ on the $Z$-axis does not lie on $Q$, and it is an external point or an internal point to $C$ according as $-D_0$ is a non-zero square or a non-square in $GF(q)$. Therefore, the number of tangents to $Q$ through $Z_\infty$ in $AG(3, q)$ is equal to $q - 1$ or $q + 1$ according as $-D_0$ is a (non-zero) square or a non-square in $GF(q)$. From the above discussion, the numbers $N_s$ and $N_t$ of secants and tangents to $Q$ through $Z_\infty$ are those given in the following lemma:

**Lemma 2.5.** For $q \equiv -1 \mod 4$, either $N_t = q + 1$, $N_s = \frac{1}{2}q^2$, or $N_t = q - 1$, $N_s = \frac{1}{2}(q^2 - 2q - 1)$, according as $D_0$ is a (non-zero) square or a non-square in $GF(q)$. For $q \equiv 1 \mod 4$, either $N_t = q - 1$, $N_s = \frac{1}{2}(q^2 + 1)$, or $N_t = q + 1$, $N_s = \frac{1}{2}(q^2 - 1)$, according as $D_0$ is a (non-zero) square or a non-square in $GF(q)$.

Going back to the discriminant $\Delta$, we see that $\Delta$ vanishes for $N_s + N_t$ ordered pairs $(\alpha, \beta)$, that is, $N_s + N_t$ is the number of lines $\ell_1$ through $P(a, b)$ for which there exists a line $\ell_2$ such that $(\ell_1, \ell_2)$ is a good line-pair. For each $\ell_1$ counted in $N_t$ (resp. $N_s$), we have $q - 1$ (resp. $2(q - 1)$) such lines $\ell_2$, since if (2.17) has a non-trivial solution $(\gamma, \delta)$ in $GF(q) \times GF(q)$ then it has exactly $q - 1$ solutions, the multiples of $(\gamma, \delta)$ by the non-zero elements of $GF(q)$.

If we do not count the $q + 1$ tangents to $\mathcal{U}$ through $P(a, b)$, each of the lines through $P(a, b)$ counted in $N_s$ is in at least $2(q - 1) - (q + 1) = q - 3$ good line-pairs. Therefore, Lemma 2.5 has the following corollary.

**Theorem 2.6.** Let $P(a, b)$ be a point of $AG(2, q^2)$ outside $\mathcal{U}$. If $a \neq 0$, $||a|| \neq -1$ and $q > 3$, then there exist at least two non-tangent lines $\ell_1, \ell_2$ of $\mathcal{U}$ through $P$, such that the non-tangent lines $\bar{\ell}_1$ and $\bar{\ell}_2$ meet in a point of $\mathcal{U}$. Further, if $q > 5$ then $\ell_1$ and $\ell_2$ may be chosen among the lines through $P(a, b)$ other than the horizontal lines and those passing through the origin.
3 Unitals in Moulton planes

Let $T$ be a non-empty subset of the multiplicative group of $\text{GF}(q)$. The (affine) Moulton plane $\mathfrak{M}_T(q^2)$ which is considered in our paper is the affine plane coordinatized by the left quasifield $\text{GF}(q^2)(+, \circ)$ where

$$x \circ y = \begin{cases} xy & \text{if } \|x\| \notin T, \\ xy^q & \text{if } \|x\| \in T, \end{cases}$$

with $\|x\| = x^{q+1}$ being the norm of $x \in \text{GF}(q^2)$ over $\text{GF}(q)$. Geometrically, $\mathfrak{M}_T(q^2)$ is constructed on $\text{AG}(2, q^2)$ by replacing the non-vertical lines with the graphs of the functions

$$Y = X \circ m + b.$$  

(3.1)

This also shows that to the non-vertical line $\ell$ of equation $Y = Xm + b$ there corresponds the line of equation $\tilde{\ell}$ of equation $Y = X \circ m + b$ in $\mathfrak{M}_T(q^2)$, and viceversa. It is useful to look at the partition of the points outside the $Y$-axis into $q - 1$ subsets $S_i$, called stripes, where $P(x, y) \in S_i$ if and only if $\|x\| = \omega^i$ with $\omega$ a fixed primitive element of $\text{GF}(q)$. Such stripes were already defined in Section 2; here we just abbreviate the subscript $\omega^i$ by $i$. In fact, moving to $\mathfrak{M}_T(q^2)$ the point-line incidences $P \in \ell$ in $\text{AG}(2, q^2)$ do not alter as long as $P \in S_i$ with $\omega^i \notin T$. The projective Moulton plane is the projective closure of $\mathfrak{M}_T(q^2)$ and it has the same points at infinity as $\text{AG}(2, q^2)$. For a similar description of Moulton planes see also [3, 4, 26].

The dual of the Moulton plane is the André plane $\mathfrak{A}_T(q^2)$ coordinatized by the right quasifield $\text{GF}(q^2)(+, \ast)$ where

$$x \ast y = \begin{cases} xy & \text{if } \|x\| \notin T, \\ x^qy & \text{if } \|x\| \in T. \end{cases}$$

In this duality, the correspondence occurs between the point $(u, v)$ of $\mathfrak{M}_T(q^2)$ and the line of equation $Y = u \ast X - v$, as well as between the line of equation $Y = X \circ m + b$ and the point $(m, -b)$ of $\mathfrak{A}_T(q^2)$. The correspondence between points at infinity and lines through $Y_\infty$, and viceversa, is the same as the canonical duality between $\text{PG}(2, q^2)$ and its dual plane $\text{PG}^*(2, q^2)$. If $T$ consists of just one element, then the arising André planes are pairwise isomorphic and they are also known as Hall planes.

Let $\mathcal{U}$ be the classical unital in $\text{PG}(2, q^2)$ given in its canonical form (2.1). We prove that $\mathcal{U}$ is an inherited unital in the Moulton plane, that is, the point-set of $\mathcal{U}$ is a unital in $\mathfrak{M}_T(q^2)$ as well.

**Theorem 3.1.** Let $\mathcal{U}$ be the classical unital in $\text{PG}(2, q^2)$ given in its canonical form (2.1). Then, for any $T$, $\mathcal{U}$ is a unital in the projective Moulton plane $\mathfrak{M}_T(q^2)$ as well.

**Proof.** In the very special case $T = \{−1\}$, the proof is straightforward. It is enough to show that if a non-vertical line $\ell$ of equation $Y = Xm + b$ meets $\mathcal{U}$ in a point $P(x, y)$ with $\|x\| = −1$ then $y = 0$ and $x = −b/m$ with $−(b/m)^{q+1} = 1$. In fact, the corresponding line $\tilde{\ell}$ in $\mathfrak{M}_T(q^2)$ has the same property: if $P(x, y) \in \tilde{\ell} \cap \mathcal{U}$ then $y = 0$ and $x = ((−b/m)^q)^{q+1}$. Since $((−b/m)^q)^{q+1} = ((b/m^q)^q)^{q+1}$, the assertion follows for $T = \{−1\}$.

In the general case, it suffices to exhibit a bijective map from $\ell \cap \mathcal{U}$ to $\tilde{\ell} \cap \mathcal{U}$ for every line $\ell$ of $\text{AG}(2, q^2)$. We may limit ourselves to non-vertical lines with non zero slopes. Let
\[ Y = Xm + b \]
be the equation of such a line \( \ell \) and take any point \( P(x, y) \) lying in \( \ell \cap U \). Then \( m \neq 0 \) and \( x = (y - b)m^{-1} \). Define the map \( \varphi : \ell \mapsto \ell \) by
\[
\varphi(P) = \begin{cases} 
\overrightarrow{P}((y - b)m^{-1}, y) & \text{for } \|x\| \not\in T, \\
\overrightarrow{P}((y - b)m^{-q}, y) & \text{for } \|x\| \in T.
\end{cases}
\]

Obviously, \( \varphi(P) = P \) whenever \( \|x\| \not\in T \).

Since \( \varphi \) is bijective, it suffices to show that \( P \in U \) yields \( \varphi(P) \in \mathcal{U} \), and the converse also holds. \( P(x, y) = ((y - b)m^{-1}, y) \in \mathcal{U} \) if and only if
\[
((y - b)m^{-1})^q + y^{q+1} - 1 = (y - b)^{q+1}(m^{-1})^q + y^{q+1} - 1 = 0.
\]

By \( (m^q)^{q+1} = m^{q+1} \), the latter equation is equivalent to
\[
((y - b)^{q+1}(m^{-q})^{q+1} + y^{q+1} - 1 = ((y - b)m^{-q})^{q+1} + y^{q+1} - 1 = 0,
\]
whence the claim follows.

Theorem 3.1 and its proof also show that if \( \ell \) is a tangent to \( U \) in \( AG(2, q^2) \) then the corresponding line \( \ell' \) is a tangent to \( \mathcal{U} \) in the projective Moulton plane, and the converse also holds. In particular, the tangent to \( U \) at a point outside the \( X \)-axis is the line \( \ell \) of equation \( Y = X(-cd^{-1})^q - d^{-q} \) with tangency point \( P(c, d) \). Therefore, the corresponding line \( \ell' \) of equation \( Y = X \circ (-cd^{-1})^q - d^{-q} \) is a tangent to \( \mathcal{U} \) at the point \( \varphi(P) = \overrightarrow{P}(c, d) \) with \( \overrightarrow{c} = c \) or \( \overrightarrow{c} = c(cd^{-1})^{q-1} \) according as \( \|c\| \not\in T \) or \( \|c\| \in T \). Since \( \|\overrightarrow{c}\| = \|c\| \), the tangency points of \( \ell \) and \( \ell' \) lie in the same stripe. The tangents of \( \mathcal{U} \) with tangency point at infinity contain the origin and each of them has equation \( Y = Xm \) with \( m^{q+1} + 1 = 0 \). By the proof of Theorem 3.1, the corresponding lines \( Y = X \circ m \) are the tangents of \( \mathcal{U} \) in the projective Moulton plane.

Now look at dual plane of the projective Moulton plane \( \mathfrak{M}_T(q^2) \) which is the projective André plane \( \mathfrak{A}_T(q^2) \). In this duality, the tangent line \( \ell \) of \( U \) with equation \( Y = X \circ (-cd^{-1})^q - d^{-q} \) corresponds to the point \( P^*(u^*, v^*) \in \mathfrak{A}_T(q^2) \) where \( u^* = -(cd^{-1})^q \) and \( v^* = d^{-q} \). Since \( ((-cd^{-1})^q)^{q+1} + (d^{-q})^{q+1} + 1 = 0 \), we have \( u^*v^* + v^* + 1 = 0 \). Similarly, the tangent line \( \ell' \) of \( U \) with equation \( Y = X \circ m, m^{q+1} + 1 = 0 \), corresponds to the point \( P^*(u^*, v^*) \in \mathfrak{A}_T(q^2) \) where \( u^* = u \) and \( v^* = 0 \). Therefore \( u^*v^* + v^* + 1 = 0 \). In terms of \( \text{PG}^*(2, q^2) \), the Desarguesian plane which gives rise to the projective André plane \( \mathfrak{A}_T(q^2) \), the points \( P^*(u^*, v^*) \) lie on the classical unital \( U^* \) given in its canonical form. This shows that \( U^* \) can be viewed as an inherited unital in the projective André plane \( \mathfrak{A}_T(q^2) \).

Remark 3.2. If \( T = \{-1\} \) then the unique stripe where incidence are altered meets \( U \) in \( q + 1 \) points lying on the \( X \)-axis. The unital \( U^* \) in the Hall plane is the Grüning unital [16] while for \( T = \{i\} \) with \( \omega^i \neq -1 \), \( U^* \) in the Hall plane is the Barwick unital [7].

A O’Nan configuration of a unital consists of four blocks \( b_1, b_2, b_3 \) and \( b_4 \) intersecting in six points \( P_1, P_2, P_3, P_4, P_5 \) and \( P_6 \) as in Figure 2. As mentioned in the introduction, the Hermitian unital contains no O’Nan configuration. This fundamental result due to O’Nan dates back to 1972, see [22] and [9, Section 4.2].

Lemma 3.3. If \( T = \{-1\} \) then the unital \( U \) of \( \mathfrak{M}_T(q^2) \) is non-classical.
Proof. We show that the unital $U$ in $\mathcal{M}_T(q^2)$ with $T = \{-1\}$ contains a O’Nan configuration. Take $\alpha \in GF(q^2)$ such that $\|\alpha\| = -1$. The line $\ell_1$ of equation $Y = X - \alpha$ meets $U$ in $Q(\alpha, 0)$ and $q$ more points. Take $m \in GF(q^2)$ such that $m^{-1} = -1$. The line $\ell_2$ of equation $Y = Xm + \alpha m$ meets $U$ in $R(-\alpha, 0)$ and $q$ more points. Further, the common point of $\ell_1$ and $\ell_2$ is

$$S = \left( \frac{-\alpha(m + 1)}{(m - 1)}, \frac{-2\alpha m}{(m - 1)} \right).$$

Since

$$\left\| \frac{-\alpha(m + 1)}{(m - 1)} \right\| = -\alpha^{q + 1} \frac{(m + 1)^{q + 1}}{(m - 1)^{q + 1}} = -\frac{m^{q + 1} + m^q + m + 1}{m^{q + 1} - m^q - m + 1} = -\frac{-m^2 - m + m + 1}{-m^2 + m - m + 1} = -1,$$

the point $S$ is outside $U$. Further, in the Moulton plane $\mathcal{M}_T(q^2)$ with $T = \{-1\}$, the corresponding lines $\bar{\ell}_1$ and $\bar{\ell}_2$ meet in $Q(\alpha, 0)$ which is a point of $U$.

To show that $U$ is not a classical unital in our Moulton plane $\mathcal{M}_T(q^2)$, it suffices to exhibit a O’Nan configuration $\{P_0, P_1, P_2, P_3, P_4, P_5\}$ lying in $U$. The idea is to start off with $P_0 = Q(\alpha, 0)$, and to find four more affine points $P_1, P_2 \in \bar{\ell}_1$ and $P_3, P_4 \in \bar{\ell}_2$ each lying in $U$, so that $U$ also contains one of the two diagonal points $P_5$ of the quadrangle $P_1P_2P_3P_4$ that are different from $P_0$. First we show that $P_1 \in \bar{\ell}_1$. Let $P_1 = P_1(x_1, y_1)$. Then, $\|x_1\| \neq -1$. In fact, otherwise, we would have $y_1^{q + 1} = 0$ and hence $y_1 = 0$, contradicting $P_0 \neq P_1$. Similarly, $P_2 \in \bar{\ell}_1$ and $P_3, P_4 \in \bar{\ell}_2$. Now we use a counting argument in $PG(2, q^2)$ to show that the quadrangle $P_1P_2P_3P_4$ can be chosen in such a way that $P_5 \in U$. Since $S = \ell_1 \cap \ell_2$ is outside $U$, the lines of $U$ joining a point of $\bar{\ell}_1$ with a point of $\bar{\ell}_2$ cover $(q + 1)^2(q - 1)$ points of $U$ other than those lying in $\bar{\ell}_1 \cup \bar{\ell}_2$. From $(q + 1)^2(q - 1) > q^3 + 1 - 2q$, there exists a quadrangle $P_1P_2P_3P_4$ in $PG(2, q^2)$ such that

$$P_1, P_2 \in \ell_1 \cap U, P_3, P_4 \in \ell_2 \cap U, P_5 = P_1P_3 \cap P_2P_4 \in U.$$
Since \((q+1)^2(q-1) > q^3 + 1 - 2q + (q+1)\) we may also assume that either \(P_5 \in \ell \cap U\), or \(P_5 = (x_5, y_5)\) with \(\|x_5\| \neq -1\). In particular, \(P_5\) is not on the X-axis.

If \(P_1, P_2 \neq Q\) and \(P_3, P_4 \neq R\) then \(P_5\) remains a diagonal point of the quadrangle \(P_1P_2P_3P_4\) in \(\mathcal{M}_T(q^2)\), and we are done.

Otherwise, take the cyclic subgroup \(G\) of \(PGU(3, q)\) of order \(q + 1\) fixing the point \(S\) and preserving each line through \(S\). Since \(|G| \geq 4\), \(G\) contains an element \(g\) such that \(Q \notin \{g(P_1), g(P_2)\}\) and \(R \notin \{g(P_3), g(P_4)\}\). Then, \(g\) takes the quadrangle \(P_1P_2P_3P_4\) to another one, whose vertices are different from both \(Q\) and \(R\). The image \(g(P_5)\) is on the line \(r\) through \(S\) and \(P_5\). Since \(r \cap U\) has at most one point on the X-axis, there exists at most one \(g \in G\) such that \(g(P_5)\) lies on the X-axis. Therefore, if \(|G| \geq 5\), some \(g \in G\) also takes \(P_5\) either to a point of infinity or a point \((x'_5, y'_5)\) with \(\|x'_5\| \neq -1\). In the Moulton plane \(\mathcal{M}_T(q^2)\), the O’Nan configuration \(P_0, g(P_1), g(P_2), g(P_3), g(P_4), g(P_5)\) arising from the quadrangle \(g(P_1)g(P_2)g(P_3)g(P_4)\) lying in \(U\) has also two diagonal points, namely \(P_0\) and \(g(P_5)\), belonging to \(U\).

Remark 3.4. Lemma 3.3 can also be obtained from Grüning’s work. In fact, if \(T = \{-1\}\) then \(U\) is isomorphic to its dual, see [16, Theorem 4.2], and the dual of \(U\) contains some O’Nan configuration, see [16, Lemma 5.4c].

We conjecture that Lemma 3.3 holds true for any \(T\). Theorem 3.5 proves this as long as \(T\) is small enough. On the other end, Theorem 3.6 provides Moulton planes with large \(T\) for which the conjecture holds.

Theorem 3.5. If \(q > 5\) and

\[
|T| < \frac{1}{2} \left( (q + 1) - \sqrt{\frac{1}{2}(q + 1)(q + 3)} \right),
\]

then \(U\) in the Moulton plane \(\mathcal{M}_T(q^2)\) is a non-classical unital.

Proof. As in the proof of Lemma 3.3, we show the existence of a O’Nan-configuration \(\{P_0, P_1, P_2, P_3, P_4, P_5\}\) lying in \(U\). For a point \(P(a, b) \in AG(2, q^2)\) with \(a \neq 0\) and \(\|a\| \in T \setminus \{-1\}\), Theorem 2.6 ensures the existence of two non-vertical lines \(\ell_1\) and \(\ell_2\) through \(P\) such that

(i) neither \(\ell_1\) nor \(\ell_2\) is horizontal or passes through the origin,

(ii) \(P_0 = \ell_1 \cap \ell_2 \in U\).

From Lemma 2.1, there exist at least \(q + 1 - 2|T|\) points \(P(x, y)\) lying on \(\ell_1 \cap U\) such that \(\|x\| \notin T\), and the same holds for \(\ell_2 \cap U\). Therefore, Theorem 2.4 applies with \(\lambda = q + 1 - 2|T|\) showing that if (3.2) is assumed, then the unital \(U\) in \(\mathcal{M}_T(q^2)\) contains an O’Nan configuration.

Theorem 3.6. If \(q > 5\), then there exists a \(T\) with \(|T| > q - 4\) such that \(U\) is a non-classical unital in \(\mathcal{M}_T(q^2)\).

Proof. From the proof of Theorem 3.5, some Moulton plane \(\mathcal{M}_T(q^2)\) contains O’Nan configurations lying in \(U\). If \(\{P_0, P_1, P_2, P_3, P_4, P_5\}\) one of them, add each non-zero element \(s \in GF(q)\) to \(T\) which satisfies the condition \(s \neq \|x_i\|\) for \(P_i = P_i(x_i, y_i)\) with \(1 \leq i \leq 5\). Then \(T\) expands and its size becomes at least \(q - 4\). In the resulting Moulton plane \(\mathcal{M}_T(q^2)\), the above hexagon \(\{P_0, P_1, P_2, P_3, P_4, P_5\}\) is still an O’Nan configuration lying in the unital \(U\).
References


[25] A. Sonnino, Non-classical unitals may be code words, submitted.

