J Algebr Comb (2012) 36:33–43
DOI 10.1007/s10801-011-0322-4

A group theoretic characterization of classical unitals

Giorgio Donati · Nicola Durante

Received: 18 January 2011 / Accepted: 22 September 2011 / Published online: 13 October 2011

Abstract Let G be the group of projectivities stabilizing a unital $\mathcal{U}$ in $\mathrm{PG}(2,q^2)$. In this paper, we prove that $\mathcal{U}$ is a classical unital if and only if there are two points in $\mathcal{U}$ such that the stabilizer of these two points in G has order q^2-1.

Keywords Unitals · Hermitian curves · Reed–Muller codes

1 Introduction

Unitals in Desarguesian projective planes, as one of the most important research areas in projective and combinatorial geometry, were a subject of many investigations. Group theoretical characterizations of classical unitals were obtained by several authors. One of the first is due to Hoffer who proves that a unital $\mathcal{U}$ in $\mathrm{PG}(2,q^2)$ is classical if and only if the group of projectivities stabilizing $\mathcal{U}$ contains $\mathrm{PSU}(3,q^2)$ [9]. In relation to the purpose of this paper, we may mention here also the papers of Abatangelo [1] and Ebert and Wantz [8]. In [1], Abatangelo proves that a Buekenhout–Metz unital $\mathcal{U}$ in $\mathrm{PG}(2,q^2)$, q odd, is classical if and only if there is a cyclic collineation group of order q^2-1, stabilizing $\mathcal{U}$ and fixing two distinct points of $\mathcal{U}$. In [8], the authors prove that a unital $\mathcal{U}$ in $\mathrm{PG}(2,q^2)$ is classical if and only if the group of projectivities stabilizing $\mathcal{U}$ contains a semidirect product $S \rtimes R$ where S has order q^3 and R has order q^2-1. For other group theoretic characterizations of classical unitals, see, e.g., [6, 7].

An important question is how much information concerning the group G of projectivities stabilizing a unital is needed to prove that the unital is classical. At the conference Combinatorics 2010, the authors made the following conjecture:

G. Donati · N. Durante (✉)
Università di Napoli "Federico II", Via Cintia, 80126 Naples, Italy
e-mail: ndurante@unina.it

Conjecture *If there is a linear collineation group of order q^2-1 stabilizing a unital $\mathcal{U}$ and fixing two distinct points of $\mathcal{U}$, then $\mathcal{U}$ is classical.*

In this paper, we prove that this conjecture holds true. The same result has been obtained by Giuzzi and Korchmáros. Their proof was completed only recently (July 2011) after one of us communicated a slight flaw in their arguments, see http://arxiv.org/abs/1009.6109.

2 Preliminary results

Let $\mathrm{PG}(2,q^2)$, $q=p^h$, p a prime number, be the projective plane over the Galois field $\mathrm{GF}(q^2)$. Throughout the paper, we will put $\mathrm{GF}(q)^*=\mathrm{GF}(q)\setminus\{0\}$. A *unital* in $\mathrm{PG}(2,q^2)$ is a set $\mathcal{U}$ of q^3+1 points meeting every line of $\mathrm{PG}(2,q^2)$ in either 1 or $q+1$ points. Lines meeting a unital $\mathcal{U}$ in 1 or $q+1$ points are respectively called *tangent* and *secant* lines to $\mathcal{U}$. Through each point of $\mathcal{U}$ there pass q^2 secant lines and one tangent line. Through each point P not on $\mathcal{U}$ there pass q^2-q secant lines and $q+1$ tangent lines, the tangent points are called the *feet* of P.

An example is the *non-degenerate Hermitian curve* or *classical* unital, that is, the set of the absolute points of a non-degenerate unitary polarity of $\mathrm{PG}(2,q^2)$. For more information on unitals in projective planes, see [3].

A *central* collineation of $\mathrm{PG}(2,q^2)$ is a collineation α fixing every point of a line ℓ (the *axis* of α) and fixing every line through a point C (the *center* of α). If $C\in\ell$, then α is an *elation*; otherwise α is a *homology*. It is well known that given a line ℓ and three distinct collinear points C,P,P' of $\mathrm{PG}(2,q^2)$, with $P,P'\notin\ell$, there is a unique central collineation with axis ℓ and center C mapping P onto P'. Note that a non-identity homology f of $\mathrm{PG}(2,q^2)$ stabilizing a unital $\mathcal{U}$ has as center a point V not on $\mathcal{U}$ and as axis a secant line ℓ to $\mathcal{U}$. Indeed, suppose, by way of contradiction, that V is on $\mathcal{U}$. Let P be a point of $\ell\cap\mathcal{U}$. The line VP is a secant line to $\mathcal{U}$, hence for any point Q on $(\mathcal{U}\cap VP)\setminus\{V,P\}$ we have that $|\langle f\rangle|=|Orb_{\langle f\rangle}(Q)||Stab_{\langle f\rangle}(Q)|$. Since $Stab_{\langle f\rangle}(Q)$ is the trivial subgroup, it follows that $|\langle f\rangle|$ divides $q-1$. Let m be a secant line to $\mathcal{U}$ through V such that $\ell\cap m\notin\mathcal{U}$. For any point R on $m\cap\mathcal{U}$ different from V, we have that $|\langle f\rangle|=|Orb_{\langle f\rangle}(R)|$, therefore $|\langle f\rangle|$ divides q. As q and $q-1$ are relatively prime, $|\langle f\rangle|=1$ and f is the identity, a contradiction. Suppose now that ℓ is a tangent line to $\mathcal{U}$. The line ℓ contains at most one of the feet of V, so there exists one of the feet of V, say T, not on ℓ. Since VT is the tangent line to $\mathcal{U}$ at T, it follows that $f(T)=T$, so f is the identity, a contradiction.

From now on, we identify, unambiguously, a projectivity of $\mathrm{PG}(2,q^2)$ with its matrix representation with respect to a frame of the plane. Then a group of projectivities of the plane will be identified with a group of 3×3 matrices.

The group of projectivities preserving a classical unital $\mathcal{U}$ in $\mathrm{PG}(2,q^2)$ is called the *projective unitary group* and is denoted by $\mathrm{PGU}(3,q^2)$. The group $\mathrm{PGU}(3,q^2)$ is 2-transitive on the points of $\mathcal{U}$ and the 2-point stabilizer is isomorphic to the multiplicative group of $\mathrm{GF}(q^2)$.

Let A, B, and C be three non-collinear points of $\mathrm{PG}(2,q^2)$, and let $\mathcal{T}$ be the set of all non-degenerate Hermitian curves containing both A and B with CA and CB

as tangent lines at A and B, respectively. Without loss of generality, we may suppose $A=(1,0,0)$, $B=(0,1,0)$, and $C=(0,0,1)$. Under such assumptions, every Hermitian curve of $\mathcal{T}$ has equation

$$\alpha x_1 x_2^q + \alpha^q x_1^q x_2 + x_3^{q+1} = 0,$$

where α is an element of $\mathrm{GF}(q^2)^*$. The linear collineation group preserving a Hermitian curve of $\mathcal{T}$ has as stabilizer of both A and B the cyclic group

$$E_{AB} = \left\{ \begin{pmatrix} \xi^{(q+1)k} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \xi^k \end{pmatrix} : k = 1, \dots, q^2-1 \right\}, \tag{1}$$

where ξ is a primitive element of $\mathrm{GF}(q^2)$.

We now recall some definitions and results on codes that will be useful in what follows; for more details, see [2, 4]. Let $\mathrm{F} = \mathrm{GF}(q), q = p^h$, and let C be a *linear code* (i.e., a subspace of a vector space over F with reference to a particular basis $\mathcal{B}$) over F and let $C' \subset C$ be a set of vectors of C all of whose coordinates w.r.t. $\mathcal{B}$ are in a subfield F' of F. Then C' is a *subfield subcode* of C over F'.

Let now $V = \mathrm{F}^m$ and consider the vector space F^V over F of all functions from V to F with basis $\{v^\omega, \omega \in V\}$, where v^ω denotes the characteristic vector of the subset $\{\omega\}$ of V.

Each polynomial $p(x_1,\dots,x_m)$ in m variables over F generates a function from F^m into F. Observe that different polynomials can generate the same function and that any polynomial $p(x_1,\dots,x_m)$ can be reduced modulo $x_i^q - x_i$ for every $i = 1,\dots,m$ to a new polynomial $p'(x_1,\dots,x_m)$ such that p and p' generate the same function and $\deg_i p' \le q-1$, for $i=1,\dots,m$, where $\deg_i p'$ denotes the degree of p' w.r.t. x_i. A polynomial $p(x_1,\dots,x_m)$ is called a *reduced* polynomial if $\deg_i p \le q-1$ for $i=1,\dots,m$. There is a one-to-one correspondence between reduced polynomials and the mappings from F^m to F. Let $\mathcal{R}(m,q)$ be the set of all reduced polynomials in m variables over F. The subset of $\mathcal{R}(m,q)$ consisting of all polynomials with degree at most r is denoted by $\mathcal{R}_r(m,q)$ and it is a subspace of $\mathcal{R}(m,q)$. A basis for $\mathcal{R}_r(m,q)$ is the set of monomials of the form:

$$x_1^{i_1} \cdots x_m^{i_m} \quad \text{where } \sum_{k=1}^m i_k \le r.$$

If the elements of F^m are ordered $\underline{\alpha}_1,\dots,\underline{\alpha}_{q^m}$, the *value table* of a polynomial $p \in \mathcal{R}(m,q)$ is defined to be the q^m-tuple $(p(\underline{\alpha}_1),\dots,p(\underline{\alpha}_{q^m}))$. The set of value tables for all polynomials of $\mathcal{R}(m,q)$ is a vector space of dimension q^m over F. The *rth order generalized Reed–Muller* code of length q^m is the set of value tables of polynomials in $\mathcal{R}_r(m,q)$ and it is denoted by $\mathrm{GRM}_r(m,q)$. Obviously, $\mathrm{GRM}_r(m,q)$ is a subspace of $\mathrm{GRM}_{m(q-1)}(m,q)$ which is the space of all value tables. The *rth order punctured generalized Reed–Muller* code, $0 \le r < m(q-1)$, is the code $\mathrm{GRM}_r(m,q)^*$ obtained from $\mathrm{GRM}_r(m,q)$ by *puncturing* at $\underline{0} \in V$, that is, by removing the position corresponding to $\underline{0}$ for every $f \in \mathrm{GRM}_r(m,q)$. Let now b be a divisor of $q-1$ and let again $0 \le r < m(q-1)$. Denote by $\underline{e} = (1, 0, \dots, 0)^t$ the transpose of the first vector of the standard basis of F^m and by S the companion matrix of order $m \times m$ of a Singer cycle of $\mathrm{PG}(m-1, q)$. The *non-primitive generalized Reed–Muller* code $\mathrm{GRM}_r^b(m, q)^*$ of order r is the code of length $\frac{q^m-1}{b} = n$ given by the set of vectors

$$\big\{\big(p\big(\underline{e}^t\big), p\big((S\underline{e})^t\big), \dots, p\big(\big(S^{n-1}\underline{e}\big)^t\big)\big) : p(x_1, \dots, x_m) \in \mathcal{R}_r^b(m, q)\big\},$$

where

$$\mathcal{R}_r^b(m, q) = \left\langle x_1^{i_1} \cdots x_m^{i_m} \in \mathcal{R}_r(m, q) : \sum_{k=1}^{m} i_k \equiv 0 \pmod{b} \right\rangle.$$

Let $\mathcal{C}_p(m-1, q)$ be the code of points and hyperplanes of $\mathrm{PG}(m-1, q)$, that is, the subspace of the characteristic vectors of the hyperplanes of $\mathrm{PG}(m-1, q)$. We will need in what follows this result on codes (see Theorem 5.7.1 in [2]).

Proposition 2.1 *Let $q = p^h$ and let $F = \mathrm{GF}(q)$. The subfield subcode over $\mathrm{GF}(p)$ of $\mathrm{GRM}_{q-1}^{q-1}(m, q)^*$, denoted by $\mathcal{P}(1, m)$, is the code $\mathcal{C}_p(m-1, q)$.*

3 Characterization

Throughout the paper, A and B are two distinct points of a unital $\mathcal{U}$ in $\mathrm{PG}(2, q^2)$ and we will denote by G the group of projectivities stabilizing $\mathcal{U}$, by C the common point to the tangent lines to $\mathcal{U}$ at A and at B, by G_{AB} the stabilizer of both A and B in G, by H_{AB} the group of homologies of G with center C and axis AB, and by L_{AB} the group of projectivities induced on the line AB by G_{AB}. From now on, we will assume, without loss of generality, that $A = (1, 0, 0)$, $B = (0, 1, 0)$, and $C = (0, 0, 1)$.

Lemma 3.1 *If $\mathcal{U}$ is a unital in $\mathrm{PG}(2, q^2)$, then G_{AB} is a cyclic group of order dividing $q^2 - 1$.*

Proof It is clear that the factor group $\frac{G_{AB}}{H_{AB}}$ is isomorphic to L_{AB}. If P is any point of $\mathcal{U}$ on the line AB different from A and from B, then $|L_{AB}| = |Orb_{L_{AB}}(P)|\,|Stab_{L_{AB}}(P)|$. Since $Stab_{L_{AB}}(P)$ is the trivial subgroup, it follows that the orbits under L_{AB} of points on $\mathcal{U} \cap AB$ different from A and from B have the same size, namely $|L_{AB}|$. Therefore, $\frac{|G_{AB}|}{|H_{AB}|}$ divides $q-1$. Moreover, let ℓ be a secant line to $\mathcal{U}$ through C such that $\ell \cap AB \notin \mathcal{U}$. If Q is any point of $\mathcal{U} \cap \ell$, then $|H_{AB}| = |Orb_{H_{AB}}(Q)||Stab_{H_{AB}}(Q)|$. Since $Stab_{H_{AB}}(Q)$ is the trivial subgroup, it follows that the orbits under H_{AB} of points on $\mathcal{U} \cap \ell$ have the same size, namely $|H_{AB}|$. Thus $|H_{AB}|$ divides $q+1$. Hence $|G_{AB}|$ divides $q^2 - 1$.

The elements of G_{AB} have the following form

$$\begin{pmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & b \end{pmatrix},$$

where a and b are non-zero elements of $\mathrm{GF}(q^2)$. The map

$$\Phi : \begin{pmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & b \end{pmatrix} \in G_{AB} \mapsto b \in \mathrm{GF}(q^2)^*$$

is a homomorphism between G_{AB} and the multiplicative group of $\mathrm{GF}(q^2)$. Let

$$f = \begin{pmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

be an element of the kernel of Φ. Since f is a homology with axis the tangent line CB and center A, it follows that f is the identity (see Sect. 2). The groups G_{AB} and $\Phi(G_{AB})$ are thus isomorphic. As $\Phi(G_{AB})$ is a subgroup of the multiplicative group of $\mathrm{GF}(q^2)$, we have that G_{AB} is a cyclic group. □

Proposition 3.2 *Let $\mathcal{U}$ be a unital in* $\mathrm{PG}(2, q^2)$ *such that G_{AB} has order $q^2 - 1$. The subgroup H_{AB} has order $q + 1$.*

Proof The group L_{AB}, isomorphic to the factor group $\frac{G_{AB}}{H_{AB}}$, has order a divisor of $q-1$ (see proof of Lemma 3.1). Since $|G_{AB}| = q^2 - 1$, we have that $q + 1$ divides $|H_{AB}|$. Moreover, $|H_{AB}|$ divides $q + 1$ (see proof of Lemma 3.1), hence $|H_{AB}| = q + 1$. □

Proposition 3.3 *Let $\mathcal{U}$ be a unital in* $\mathrm{PG}(2, q^2)$ *such that G_{AB} has order $q^2 - 1$. If P is a point of* $\mathrm{PG}(2, q^2)$ *not on the edges of the triangle ABC, then the orbit of P under the action of H_{AB} is a Baer subline of the line CP.*

Proof Every homology of G with center C and axis AB has the following form $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & b \end{pmatrix}$, where b is a non-zero element of $\mathrm{GF}(q^2)$. The map

$$\Phi' : \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & b \end{pmatrix} \in H_{AB} \mapsto b \in \mathrm{GF}\big(q^2\big)^*$$

is a monomorphism between H_{AB} and the multiplicative group of $\mathrm{GF}(q^2)$, so $\Phi'(H_{AB})$ is a multiplicative subgroup of $\mathrm{GF}(q^2)$ of order $q + 1$. It follows that

$$H_{AB} = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & b \end{pmatrix} : b^{q+1} = 1 \right\}.$$

Under our hypothesis, we may assume that $P = (1, 1, 1)$. The orbit of P under the action of H_{AB} is the set $\mathcal{O}_P = \{(1, 1, b) : b^{q+1} = 1\} = \{(x_1, x_2, x_3) : x_1 = x_2$ and $x_2^{q+1} - x_3^{q+1} = 0\}$. Therefore, $\mathcal{O}_P$ is a Baer subline of the line CP. □

Proposition 3.4 *Let $\mathcal{U}$ be a unital in* PG$(2,q^2)$ *such that G_{AB} has order q^2-1. Then $\mathcal{U}$ intersects the line AB in a Baer subline whose points are the feet of C.*

Proof The map

$$\Psi : \begin{pmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & b \end{pmatrix} \in G_{AB} \mapsto a \in \mathrm{GF}\big(q^2\big)^*$$

is a homomorphism between G_{AB} and the multiplicative group of GF(q^2). The kernel of Ψ is H_{AB}, hence $\Psi(G_{AB})$ is isomorphic to the factor group $\frac{G_{AB}}{H_{AB}}$. As $|H_{AB}| = q+1$ (see Proposition 3.3), $\Psi(G_{AB})$ is a subgroup of order $q-1$ of the multiplicative group of GF(q^2), thus $\Psi(G_{AB}) = \mathrm{GF}(q)^*$. Moreover, since G_{AB} is a cyclic group and $\Phi(G_{AB}) = \mathrm{GF}(q^2)^*$, it follows that

$$G_{AB} = \left\{ \begin{pmatrix} \rho^k & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \xi^k \end{pmatrix} : k = 1, \ldots, q^2-1 \right\},$$

where ξ is a primitive element of GF(q^2) and ρ is a primitive element of GF(q). Let P be a point of $\mathcal{U} \cap AB$ different from A and from B. We may assume that $P = (1,1,0)$. The orbit of P under the action of G_{AB} is the set $\mathcal{O}_P = \{(\rho^k,1,0) : k = 1,\ldots,q^2-1\}$. Hence

$$\mathcal{O}_P \cup \{A,B\} = \big\{(x_1,x_2,0)\ :\ \beta x_1 x_2^q + \beta^q x_1^q x_2 = 0\big\},$$

where β is an element of GF(q^2) such that $\beta^{q-1} = -1$. The set $\mathcal{U} \cap AB$ is thus a Baer subline of AB. Let ℓ be a secant line to $\mathcal{U}$ through C and let Q be a point of $\ell \cap \mathcal{U}$ not on the line AB. Since $\mathcal{U} \cap \ell$ is the orbit of the point Q under H_{AB} and since $|H_{AB}| = q+1$, it follows that no point of $\mathcal{U} \cap \ell$ is on AB. Hence the points of $AB \cap \mathcal{U}$ are the feet of C. □

If ξ is a primitive element of GF(q^2), then every primitive element of GF(q) is given by $\xi^{\lambda(q+1)}$, where λ is a suitable positive integer such that λ and $q-1$ are relatively prime and $\lambda < q-1$. If g_λ is the projectivity of PG$(2,q^2)$ with matrix representation

$$\begin{pmatrix} \xi^{\lambda(q+1)} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \xi \end{pmatrix},$$

then, from the proof of the previous proposition, there exists an integer λ such that

$$G_{AB} = \langle g_\lambda \rangle = \{g_\lambda^k : k = 1,\ldots,q^2-1\}. \tag{2}$$

Proposition 3.5 *Let $\mathcal{U}$ be a unital in* PG$(2,q^2)$ *such that G_{AB} has order q^2-1. If P is a point not on the edges of the triangle ABC, then the orbit $\mathcal{O}_P$ of P under the action of G_{AB} is contained in the Baer subpencil of lines with vertex C containing the lines CA, CB and CP. Moreover, $\mathcal{O}_P$ meets every line through A, different from AB and AC, in a unique point.*

Proof Without loss of generality, we may assume that $P = (1, 1, 1)$. From (2), we have that $\mathcal{O}_P = \{(\xi^{\lambda(q+1)k}, 1, \xi^k) : k = 1, \ldots, q^2 - 1\}$. The Baer subpencil of lines $\mathcal{P}$ with vertex C containing CA, CB and CP is the rank 2 Hermitian curve of $\mathrm{PG}(2, q^2)$ with equation $\beta x_1 x_2^q + \beta^q x_1^q x_2 = 0$, where β is an element of $\mathrm{GF}(q^2)$ such that $\beta^{q-1} = -1$. Since $\mathcal{O}_P$ is contained in $\mathcal{P}$, the assertion follows. Moreover, let ℓ be a line through A different from AB and AC. The line ℓ is represented by the equation $x_2 = \rho x_3$, with $\rho \neq 0$. It follows that $\mathcal{O}_P \cap \ell = \{((\rho^{-1})^{\lambda(q+1)}, 1, \rho^{-1})\}$. □

Proposition 3.6 *Let $\mathcal{U}$ be a unital in* $\mathrm{PG}(2, q^2)$ *such that G_{AB} has order $q^2 - 1$. If P is a point on the line AB not on $\mathcal{U}$ then the feet of P form a Baer subline contained in a line through C.*

Proof Let ℓ_1 be a tangent line to $\mathcal{U}$ through P and let $P_1 = \ell_1 \cap \mathcal{U}$. From Proposition 3.3, the orbit of P_1 under the action of H_{AB} is a Baer subline contained in a line through C. Since the points of this orbit coincide with the feet of P, the assertion follows. □

For any non-zero element α of $\mathrm{GF}(q^2)$, consider the set $\mathcal{H}_{\alpha,\lambda}$ of the $\mathrm{GF}(q^2)$-rational points of the algebraic curve with equation

$$x_3^{\lambda(q+1)} + \alpha x_1 x_2^{\lambda(q+1)-1} + \alpha^q x_1^q x_2^{\lambda(q+1)-q} = 0,$$

where λ and $q - 1$ are relatively prime and $0 < \lambda < q - 1$.

Proposition 3.7 *The group $\langle g_\lambda \rangle$ stabilizes every set of the family $\{\mathcal{H}_{\alpha,\lambda} : \alpha \in$* $\mathrm{GF}(q^2)^*\}$.

Proof Let $P = (y_1, y_2, y_3)$ be a point of $\mathcal{H}_{\alpha,\lambda}$. The element g_λ^k of $\langle g_\lambda \rangle$ maps P onto the point $P' = (\xi^{\lambda(q+1)k} y_1, y_2, \xi^k y_3)$ that also satisfies the equation of $\mathcal{H}_{\alpha,\lambda}$. □

Proposition 3.8 *The group H of all homologies of* $\mathrm{PG}(2, q^2)$ *with center A and axis BC has a sharply transitive action on the set* $\{\mathcal{H}_{\alpha,\lambda} : \alpha \in \mathrm{GF}(q^2)^*\}$ *for any fixed λ.*

Proof Let α_1 and α_2 be any two elements of $\mathrm{GF}(q^2)^*$. The homology $(x_1, x_2, x_3) \mapsto (\alpha_1 x_1, \alpha_2 x_2, \alpha_2 x_3)$ belongs to H and maps the set $\mathcal{H}_{\alpha_1,\lambda}$ onto the set $\mathcal{H}_{\alpha_2,\lambda}$. Since there are $q^2 - 1$ homologies in H and $q^2 - 1$ sets $\mathcal{H}_{\alpha,\lambda}$ (with λ fixed), the assertion follows. □

Proposition 3.9 *Every secant line to a set $\mathcal{H}_{\alpha,\lambda}$ through A meets $\mathcal{H}_{\alpha,\lambda}$ in a Baer subline.*

Proof Let r be a secant line to a set $\mathcal{H}_{\alpha,\lambda}$ through A. From Proposition 3.8, it is enough to show that $\mathcal{H}_{1,\lambda}$ intersects the line r in a Baer subline. Suppose that $r = AB$. The set $\mathcal{H}_{1,\lambda} \cap r$ is $\{A, B\} \cup \{(x, 1, 0) : x^{q-1} = -1\}$ which is a Baer subline. Suppose now that r has equation $x_2 = x_3$. The set of common points of $\mathcal{H}_{1,\lambda}$ and r is $\{A\} \cup \{(x, 1, 1) : 1 + x + x^q = 0\}$, which is a Baer subline. Since $\langle g_\lambda \rangle$ stabilizes $\mathcal{H}_{1,\lambda}$ and has a sharply transitive action on the lines through A different from AB and AC (being AC a tangent line to $\mathcal{H}_{1,\lambda}$), it follows that any line through A, different from AB and AC meets $\mathcal{H}_{1,\lambda}$ in a Baer subline. □

Proposition 3.10 *Every set $\mathcal{H}_{\alpha,\lambda}$ has q^3+1 points.*

Proof From Proposition 3.9, every secant line to $\mathcal{H}_{\alpha,\lambda}$ through A meets $\mathcal{H}_{\alpha,\lambda}$ in q points distinct from A. Since AC is the unique tangent line to $\mathcal{H}_{\alpha,\lambda}$ at A, it follows that $|\mathcal{H}_{\alpha,\lambda}| = q^3+1$. □

Let s be the line of $PG(2,q^2)$ with equation $x_2 = x_3$ and let $B' = s \cap BC = (0,1,1)$.

Proposition 3.11 *Every Baer subline of s containing A and not containing B' is contained in a unique set of the family $\{\mathcal{H}_{\alpha,\lambda} : \alpha \in \mathrm{GF}(q^2)^*\}$ for any fixed λ.*

Proof Let s_0 be a Baer subline of s containing A and not containing B'. There exists an element $\theta \in \mathrm{GF}(q^2)^*$ such that s_0 has equations $x_2^{q+1} + \theta x_1 x_2^q + \theta^q x_1^q x_2 = 0$ and $x_2 = x_3$. The set $\mathcal{H}_{\theta,\lambda}$ is the unique set of the family $\{\mathcal{H}_{\alpha,\lambda} : \alpha \in \mathrm{GF}(q^2)^*\}$ meeting s in the Baer subline s_0. □

Proposition 3.12 *Every Baer subline containing both A and B is contained in $q-1$ sets of the family $\{\mathcal{H}_{\alpha,\lambda} : \alpha \in \mathrm{GF}(q^2)^*\}$ for any fixed λ.*

Proof Let ℓ_0 be a Baer subline of AB containing A and B. The subline ℓ_0 is represented by equations $\theta x_1 x_2^q + \theta^q x_1^q x_2 = 0$, $x_3 = 0$, for any θ in a coset Ω of $\mathrm{GF}(q)^*$ in the multiplicative group $\mathrm{GF}(q^2)^*$. Hence ℓ_0 is contained in exactly $q-1$ sets of $\{\mathcal{H}_{\alpha,\lambda} : \alpha \in \mathrm{GF}(q^2)^*$, namely $\mathcal{H}_{\theta,\lambda}$ with $\theta \in \Omega$. □

Proposition 3.13 *Every point P of* $\mathrm{PG}(2,q^2)$ *not on the edges of the triangle ABC is contained in q sets of the family $\{\mathcal{H}_{\alpha,\lambda} : \alpha \in \mathrm{GF}(q^2)^*\}$ for any fixed λ.*

Proof Let $P = (y_1, y_2, 1)$. The number of sets of the family $\{\mathcal{H}_{\alpha,\lambda} : \alpha \in \mathrm{GF}(q^2)^*\}$ containing P coincides with the number of solutions of the equation $1 + \alpha y_1 y_2^{\lambda(q+1)-1} + (\alpha y_1 y_2^{\lambda(q+1)-1})^q = 0$ in the unknown α. Since this number is q the assertion follows. □

Proposition 3.14 *If a set $\mathcal{H}_{\alpha,\lambda}$ is a unital in* $\mathrm{PG}(2,q^2)$, *then $\lambda = 1$.*

Proof Suppose that a set $\mathcal{H}_{\beta,\lambda}$ is a unital in $\mathrm{PG}(2,q^2)$. From Proposition 3.9 and from a famous result due to Casse, O'Keefe, Penttila [5] and Quinn, Casse [10], it follows that $\mathcal{H}_{\beta,\lambda}$ is a Buekenhout–Metz unital with respect to A. The linear collineation group preserving the unital $\mathcal{H}_{\beta,\lambda}$ has as stabilizer of both A and B exactly the group $\langle g_\lambda \rangle$ of size q^2-1. Hence $\mathcal{H}_{\beta,\lambda}$ is a classical unital (see [3]) with CA and CB as tangent line at A and at B, respectively, so $G_{AB} = E_{AB}$ (see (1) in Sect. 2). From this condition, it follows that $\lambda = 1$. □

From (2) there exists an integer λ such that $G_{AB} = \langle g_\lambda \rangle$. Let $\mathcal{P}$ be the set formed by the point C, by all the $q+1$ Baer sublines containing both A and B, and by the orbits under $G_{AB} = \langle g_\lambda \rangle$ of the points of $\mathrm{PG}(2,q^2)$ not on the edges of the triangle ABC. Let $\mathcal{L}$ be the set formed by the line AB, by the Baer subpencils of lines with vertex C and projecting a Baer subline containing both A and B, and by the q^2-1 sets $\mathcal{H}_{\alpha,\lambda}$ for $\alpha \in \mathrm{GF}(q^2)^*$. We show that $\mathcal{P}$ and $\mathcal{L}$ are respectively the set of points and the set of lines of a projective plane.

Proposition 3.15 *The incidence structure* $(\mathcal{P}, \mathcal{L})$, *where the incidence relation is set theoretic inclusion, is a projective plane of order* q.

Proof Observe that $|\mathcal{P}| = |\mathcal{L}| = q^2+q+1$. We claim that every line ℓ of $\mathcal{L}$ has $q+1$ points. This is clearly true for the line AB. If the line ℓ is a Baer subpencil projecting a Baer subline ℓ_0 containing both A and B, then it contains $q-1$ orbits under G_{AB} of points not on the edges of the triangle ABC, it contains ℓ_0 and the point C. If ℓ is a set $\mathcal{H}_{\alpha,\lambda}$, it contains q orbits of points not on the edges of the triangle ABC and a Baer subline containing both A and B.

We claim that every point P of $\mathcal{P}$ is incident with $q+1$ lines. This is clearly true for the point C. If P is a Baer subline containing both A and B, then it is contained in $q-1$ sets of the family $\{\mathcal{H}_{\alpha,\lambda} : \alpha \in \mathrm{GF}(q^2)^*\}$ (see Proposition 3.12), it is contained in the line AB and in the Baer subpencil with vertex C projecting P. If P is an orbit under G_{AB} of a point not on the edges of the triangle ABC, then it is contained in q sets of the family $\{\mathcal{H}_{\alpha,\lambda} : \alpha \in \mathrm{GF}(q^2)^*\}$ (see Proposition 3.13) and it is contained in a Baer subpencil of lines with vertex C projecting a Baer subline containing both A and B (see Proposition 3.5).

Finally, we prove that any two distinct points P_1 and P_2 of $\mathcal{P}$ are incident with exactly one line of $\mathcal{L}$. If P_1 and P_2 are Baer sublines containing both A and B, then AB is the unique line containing them. If $P_1 = C$ and P_2 is a Baer subline containing both A and B, then the Baer subpencil of lines with vertex C projecting P_2 is the unique line containing P_1 and P_2. If $P_1 = C$ and P_2 is an orbit under G_{AB} of a point not on the edges of the triangle ABC, then, from Proposition 3.5, there exists a unique element of $\mathcal{L}$ containing both P_1 and P_2. Suppose now that P_1 and P_2 are distinct orbits under G_{AB} of points not on the edges of the triangle ABC. From Proposition 3.5, each one of the orbits P_1 and P_2 meets the line s with equation $x_2 = x_3$ in a unique point, say Q_1 and Q_2, respectively.

Let s_0 be the Baer subline of s containing A, Q_1 and Q_2. If s_0 contains the point $s \cap BC$, then P_1 and P_2 are both contained in the Baer subpencil of lines with vertex C projecting s_0. Such a subpencil is the unique line containing P_1 and P_2. If s_0 does not contain the point $s \cap BC$, then, from Proposition 3.11, there exists a unique set of the family $\{\mathcal{H}_{\alpha,\lambda} : \alpha \in \mathrm{GF}(q^2)^*\}$ containing s_0. Such a set is the unique line containing P_1 and P_2. □

Proposition 3.16 *The characteristic vector* $v^{\mathcal{H}_{\alpha,\lambda}}$ *of the set* $\mathcal{H}_{\alpha,\lambda}$ *is in the linear code of* $\mathrm{PG}(2,q^2)$.

Proof It is sufficient to prove the result for $\mathcal{H}_{1,\lambda}$ (see Proposition 3.8). From Proposition 2.1, we need only to show that $v^{\mathcal{H}_{1,\lambda}} \in \mathcal{P}(1,3)$. Consider the polynomial

$$p(x_1,x_2,x_3) = 1 - \left(x_3^{\lambda(q+1)} + x_1 x_2^{\lambda(q+1)-1} + x_1^q x_2^{\lambda(q+1)-q}\right)^{q-1}.$$

Then $p(x_1,x_2,x_3) = 1$ if and only if (x_1,x_2,x_3) is a point of $\mathcal{H}_{1,\lambda}$ and $p(x_1,x_2,x_3) = 0$ elsewhere. Moreover, $p(x_1,x_2,x_3)$ is given in terms of monomial functions in the non-primitive generalized Reed–Muller code $\mathrm{GRM}_{q^2-1}^{q^2-1}(3,q^2)$, since each monomial of $p(x_1,x_2,x_3)$ has degree exactly q^2-1 once reduced modulo $x_i^{q^2} - x_i$. Since $p(x_1,x_2,x_3) \in \{0,1\}$ for all (x_1,x_2,x_3), it follows that the value table of $p(x_1,x_2,x_3)$ has all entries in the subfield $\mathrm{GF}(p)$. Thus, from Proposition 2.1, the incidence vector $v^{\mathcal{H}_{1,\lambda}}$ of length $\frac{(q^2)^3-1}{q^2-1} = q^4+q^2+1$ is the subfield subcode $\mathcal{P}(1,3)$. □

Proposition 3.17 *Let $\mathcal{U}$ be a unital in* $\mathrm{PG}(2,q^2)$ *such that G_{AB} has order q^2-1. Then $|\mathcal{U} \cap \mathcal{H}_{\alpha,\lambda}| \geq 3$ for all $\alpha \in \mathrm{GF}(q^2)^*$ and for all possible λ.*

Proof From the previous proposition $v^{\mathcal{H}_{\alpha,\lambda}} = v^{m_1} + \cdots + v^{m_t}$ for some lines $m_1,\dots,m_t$ ($t \geq 3$ since $|\mathcal{H}_{\alpha,\lambda}| = q^3+1$). If $\cdot$ denotes the usual inner product, then $|\mathcal{U} \cap \mathcal{H}_{\alpha,\lambda}| = v^{\mathcal{U}} \cdot v^{\mathcal{H}_{\alpha,\lambda}} = v^{\mathcal{U}} \cdot (v^{m_1} + \cdots + v^{m_t}) = t \bmod p$.

Consider the line AB, this intersects $\mathcal{H}_{\alpha,\lambda}$ in a Baer subline, hence in $1 \bmod p$ points. Each line m_i intersects AB in again $1 \bmod p$ points (either 1 or q^2+1). As $v^{\mathcal{H}_{\alpha,\lambda}} = v^{m_1} + \cdots + v^{m_t}$, we have that $t = 1 \bmod p$. Since A, B are common points to $\mathcal{U}$ and $\mathcal{H}_{\alpha,\lambda}$ it follows $|\mathcal{U} \cap \mathcal{H}_{\alpha,\lambda}| \geq p+1 \geq 3$. □

Theorem 3.18 *If $\mathcal{U}$ is a unital in* $\mathrm{PG}(2,q^2)$ *such that G_{AB} has order q^2-1, then $\mathcal{U}$ is classical.*

Proof There exists an integer λ such that $G_{AB} = \langle g_\lambda \rangle$ (see (2)). From the previous proposition, the unital $\mathcal{U}$ has at least one point different from A and B with each set $\mathcal{H}_{\alpha,\lambda}$, and hence it has one orbit in common with each $\mathcal{H}_{\alpha,\lambda}$. This gives that $\mathcal{U}$ is a line of the projective plane $(\mathcal{P},\mathcal{L})$, since it is a subset of size $q+1$ of $\mathcal{P}$ meeting every line. Therefore, the set $\mathcal{U}$ coincides with a set $\mathcal{H}_{\gamma,\lambda}$ for some non-zero $\gamma \in \mathrm{GF}(q^2)$. From Proposition 3.14, we have that $\lambda = 1$ and $\mathcal{U}$ is the classical unital $\mathcal{H}_{\gamma,1}$. □

References

1. Abatangelo, L.M.: Una caratterizzazione gruppale delle curve hermitiane. Matematiche **39**, 101–110 (1984)
2. Assmus, E.F. Jr., Key, J.D.: Designs and Their Codes. Cambridge University Press, Cambridge (1992)
3. Barwick, S.G., Ebert, G.L.: Unitals in Projective Planes. Springer Monographs in Mathematics. Springer, New York (2008)
4. Bruen, A.A., Forcinito, M.A.: Cryptography, Information Theory and Error-Correction. Wiley-Interscience, New York (2006)
5. Casse, L.R.A., O'Keefe, C.M., Penttila, T.: Characterizations of Buekenhout–Metz unitals. Geom. Dedic. **59**, 29–42 (1996)
6. Cossidente, A., Ebert, G.L., Korchmáros, G.: A group theoretic characterization of classical unitals. Arch. Math. **74**, 1–5 (2000)

7. Cossidente, A., Ebert, G.L., Korchmáros, G.: Unitals in finite Desarguesian planes. J. Algebr. Comb. **14**, 119–125 (2001)
8. Ebert, G.L., Wantz, K.: A group theoretic characterization of Buekenhout–Metz unitals. J. Comb. Des. **4**, 143–152 (1996)
9. Hoffer, A.R.: On unitary collineation groups. J. Algebra **22**, 211–218 (1972)
10. Quinn, C.T., Casse, L.R.A.: Concerning a characterization of Buekenhout–Metz unitals. J. Geom. **52**, 159–167 (1995)