Hermitian unitals are code words

Aart Blokhuis, Andries Brouwer, Henny Wilbrink
Eindhoven University of Technology
a.blokhuis@tue.nl, aeb@cwi.nl, ha.wilbrink@telfort.nl

7 March 1990

Abstract

We show that a unital in $\mathrm{PG}(2, q^2)$ is Hermitian if and only if it is in the code generated by the lines of $\mathrm{PG}(2, q^2)$. This implies the truth of a conjecture made by Assmus and Key.

1 Introduction

In this paper, a *unital* in a projective plane of order m^2 will be a subset of size $m^3 + 1$ of the point set with the property that each line meets it in either $m + 1$ or 1 point(s). In the Desarguesian plane the set of isotropic points of a nondegenerate Hermitian form is the classical example of a unital. Such a unital is called a *Hermitian* unital. In [1] it is shown that a particular class of unitals in the Desarguesian plane $\mathrm{PG}(2, q^2)$ (the so-called Buekenhout-Metz unitals) always intersect a Hermitian unital in 1 mod p points (where p is prime and $q = p^e$), and the authors mention a conjecture by Assmus and Key that every unital has this property w.r.t. the Hermitian unital. Since the (characteristic vector of the) complement of any unital on m^3+1 points in any plane of order m^2 is in the orthogonal complement of the $\mathbb{F}_p$-code spanned by the (characteristic vectors of the) lines of the plane if $p \mid m$, it clearly suffices to show that the Hermitian unital is in the code of the Desarguesian plane to prove the conjecture.

Theorem. *Let $q = p^e$ with p prime and $e \in \mathbb{N}$. A unital in $\mathrm{PG}(2, q^2)$ is Hermitian if and only if it is in the $\mathbb{F}_p$-code spanned by the lines of $\mathrm{PG}(2, q^2)$.*

The proof of this theorem will be given in Section 3. In the preparatory Section 2 we recall some basic facts about Abelian difference sets in planes of square order (cf. [5] and also [2] for the cyclic case), and prove a new result (Lemma 2) that will be helpful in the proof of the theorem.

2 Abelian difference sets in planes of square order

Consider an abelian group G (written multiplicatively) of order n^2+n+1 with a planar difference set D chosen in such a way that D is fixed by every multiplier. If $n = m^2$, then $\mu = m^3$ is a multiplier of order 2. We shall assume that μ is a multiplier of order 2 and show that $n = m^2$ and $\mu = m^3$. We shall then describe the geometrical implications of μ. Define subgroups A and B of G by

$$A = \{x \in G \mid x^\mu = x^{-l}\}, \quad B = \{x \in G \mid x^\mu = x\},$$

and define homomorphisms $\alpha : G \to A$ and $\beta : G \to B$ by

$$g^{\alpha} := (gg^{-\mu})^{\frac{1}{2}}, \quad g^{\beta} := (gg^{\mu})^{\frac{1}{2}} \quad (g \in G).$$

Notice that $A \cap B = 1$ and that $g = g^{\alpha}g^{\beta}$ for every $g \in G$, i.e., G is the direct product of A and B, $G = A \times B$.

Since μ is a collineation of order two, it is either an elation (with $n+1$ fixed points), a homology (with $n+2$ fixed points), or a Baer involution (with $n + \sqrt{n} + 1$ fixed points). Since the number of fixed points $|B|$ divides $|G|$ it follows that μ is a Baer involution and that n is a perfect square, say $n = m^2$. It follows that $|A| = m^2 - m + 1$, $|B| = m^2 + m + 1$ and B is a Baer subplane. To show that $\mu = m^3$, observe that the orders of A and B are coprime so G has unique subgroups of order $m^2 - m + 1$ and $m^2 + m + 1$. Since m^3 is also an involutory multiplier, m^3 and μ have identical actions on A and B so $\mu = m^3$. Notice that $D \cap B$ is a difference set in B (D is fixed by μ and is therefore a Baer line).

Lemma 1 *For all d_1, $d_2 \in D$ we have $d_1^{\beta} = d_2^{\beta} \Leftrightarrow d_1 = d_2$ or $d_1 = d_2^{\mu}$.*

Proof. If $d_1^{\beta} = d_2^{\beta}$, then $d_1 d_2^{-1} = d_2^{\mu}(d_1^{\mu})^{-1}$, so since D is a planar difference set, $d_1 = d_2$ or $d_1 = d_2^{\mu}$. The converse is obvious. □

This lemma can be used to show that A is an arc (i.e., no three points of A are collinear): If $d_1 g$, $d_2 g \in Dg \cap A$, then $(d_1 g)^{\beta} = 1 = (d_2 g)^{\beta}$ so $d_1 = d_2$, or $d_1 = d_2^{\mu}$. (The same proof as in [2] can be used to show that A is in fact a maximal arc if $m > 2$.)

Let R be a commutative ring with identity and consider the group ring $R[G]$. We shall use the following notational conventions. We shall identify a subset $X = \{x_1, x_2, \ldots, x_s\} \subseteq G$ with the element $X = x_1 + x_2 + \cdots + x_s$ in $R[G]$. Also, for a homomorphism γ of G, we define the R-homomorphism $[\gamma]$ of $R[G]$ by

$$\left(\sum_{g \in G} \xi_g g \right)^{[\gamma]} := \sum_{g \in G} \xi_g g^{\gamma}.$$

Using these conventions our next lemma can be formulated as follows.

Lemma 2 *$D^{[\beta]} + (D \cap B)^{[\frac{1}{2}]2} = 2B$ in $\mathbb{Z}[G]$.*

Proof. Notice that on the left hand side of this identity all terms certainly belong to B and are of the form $(d_1 d_2)^{\frac{1}{2}}$ with d_1 and d_2 in D. There are $(m^2 + 1) + (m + 1)^2 = 2(m^2 + m + 1)$ terms on the left hand side. Since $(d_1 d_2)^{\frac{1}{2}} = (d_3 d_4)^{\frac{1}{2}}$ implies that $\{d_1, d_2\} = \{d_3, d_4\}$ and since the terms with $d_1 = d_2$ appear twice, once in $D^{[\beta]}$ and once in $(D \cap B)^{[\frac{1}{2}]2}$, the identity follows. □

It is well known (and easy to check) that the correspondence

$$g \leftrightarrow Dg^{-1}, \quad g \in G$$

defines a polarity. The set of absolute points is $D^{[\frac{1}{2}]}$. (Thus, $(D \cap B)^{[\frac{1}{2}]}$ is an oval in B if n is odd and a line of B if n is even.) It is equally easy to check that the correspondence

$$g \leftrightarrow Dg^{-\mu}, \quad g \in G$$

also defines a polarity. Clearly, g is absolute w.r.t. this polarity if and only if $g^{2\beta} \in D$. Since $A = \ker(\beta)$ the following result is now clear.

Lemma 3 *The polarity $g \leftrightarrow Dg^{-\mu}$ has m^3+1 absolute points namely the points of $U = A(D \cap B)^{[\frac{1}{2}]}$.*

It is well known that U is a unital (see e.g. [3, p. 246] or [5]). To end this section, we shall now discuss how all of this applies to the Hermitian unital. The standard method to see the cyclic difference set for $\mathrm{PG}(2, q^2)$ is to start with $\mathbb{F}_{q^6}$ as the underlying 3-dimensional vector space over $\mathbb{F}_{q^2}$ and to identify the points of $\mathrm{PG}(2, q^2)$ with the elements of

$$G = \mathbb{F}_{q^6}^*/\mathbb{F}_{q^2}^* \ ,$$

a cyclic group of order q^4+q^2+1. Let $x \to \langle x \rangle$ be the homomorphism $\mathbb{F}_{q^6}^* \to G$ and let $\mathrm{Tr} : \mathbb{F}_{q^6} \to \mathbb{F}_{q^2}$, be the usual trace function. Now

$$D = \{\langle x \rangle \mid x \in \mathbb{F}_{q^6},\ \mathrm{Tr}(x) = 0\}$$

is a line of the plane and therefore serves as a difference set in G.

Notice that D is invariant under the multiplier $\langle x \rangle \mapsto \langle x^p \rangle$. Since U is the set of $g \in G$ such that $g^{\mu+1} = g^{q^3+1} \in D$, it follows that

$$U = \{\langle x \rangle \mid x \in \mathbb{F}_{q^6}^*,\ \mathrm{Tr}(x^{q^3+1}) = 0\}.$$

Hence, U is just the set of isotropic points of the nondegenerate Hermitian form $H(x, y)$ on $\mathbb{F}_{q^6}$ defined by

$$H(x, y) = \mathrm{Tr}(xy^{q^3}) \ ,$$

i.e., U is a Hermitian unital.

3 Proof of the theorem

We shall now prove that U is in the $\mathbb{F}$-code spanned by the lines for every field $\mathbb{F}$ in which $m^2+1 \neq 0 \neq |G|$ (clearly this implies the 'only if' part of the theorem). We shall work in the group algebra $\mathbb{F}[G]$ and show that U is in the ideal generated by D. For this we have to show that

$$\chi(D) = 0 \Rightarrow \chi(U) = 0$$

for every absolutely irreducible $\mathbb{F}$-character χ of G. So assume $\chi(D) = 0$. Since $\chi(U) = \chi(A)\chi((D \cap B)^{[\frac{1}{2}]})$ by Lemma 3, we may assume that $\chi(A) \neq 0$. Now $\chi(g) = \phi(g^\alpha)\psi(g^\beta)$, $g \in G$, where ϕ is a character of A and ψ is a character of B. Hence, $\phi(A) = \chi(A) \neq 0$ implies that $\phi = 1_A$ and so $\chi(g) = \psi(g^\beta)$ for all $g \in G$. In particular

$$\chi(D) = \psi(D^{[\beta]}) \ \text{ and } \ \chi((D \cap B)^{[\frac{1}{2}]}) = \psi((D \cap B)^{[\frac{1}{2}]}) \ .$$

Since $1_B(D^{[\beta]}) = m^2 + 1 \neq 0$, it follows that $\psi \neq 1_B$ and so, by Lemma 2,

$$\psi((D \cap B)^{[\frac{1}{2}]})^2 = \psi((D \cap B)^{[\frac{1}{2}]2}) = \psi(2B) - \psi(D^{[\beta]}) = 0 - 0 = 0,$$

completing the proof that U is in the code.

For the converse, assume that U is a unital in the Desarguesian projective plane $\mathrm{PG}(2,q^2)$, $q=p^e$, p prime, $e\in\mathbb{N}$, which is in the code spanned by the lines of the plane.

Proposition. *Let X be a subset of $\mathrm{PG}(2,q)$ which is in the $\mathbb{F}$-code of the plane and let P be a point not in X. Then the points Q for which the line PQ is tangent to X (i.e., $PQ\cap X=\{Q\}$) are all collinear.*

Proof. If $q=2$ this is easy to check so assume $q>2$. Let $Q_i,\ i=1,2,3$, be three distinct points of X for which PQ_i is a tangent line. Coordinatize the plane in such a way that $P=(1,0,0)$ and $Q_i=(x_i,y_i,1)$, $i=1,2,3$ (here we use $q>2$). Notice that $y_i\neq y_j$ if $i\neq j$ since P, Q_i, Q_j are not collinear. Thus, there exist nonzero $w_1,w_2,w_3\in\mathbb{F}_q$, such that

$$w_1+w_2+w_3=0, \qquad w_1y_1+w_2y_2+w_3y_3=0.$$

Give weight w_ix to a point $(x,y_i,1)$ on the horizontal line PQ_i, $x\in\mathbb{F}_q$, $i=1,2,3$, and weight zero to all other points. This defines a word in the dual code (over $\mathbb{F}_q$) of the plane (e.g., a line $X=aY+bZ$ has inner product $\sum_i w_i(ay_i+b)=0$, a line $Y=y_iZ$ has inner product $\sum_x w_ix=0$.) Since X is in the code, X has inner product zero with this word, i.e.,

$$w_1x_1+w_2x_2+w_3x_3=0$$

proving that Q_1, Q_2 and Q_3 are collinear. □

Thus, for the unital U and a point P not in U, the $q+1$ points Q_i for which PQ_i is a tangent line, are all on one line which we shall denote by $p^\perp$. For a point P in U we define $P^\perp$ to be the tangent at P. We want to show that this defines a (Hermitian) polarity. For this it suffices to show that $Q\in P^\perp$ implies that $P\in Q^\perp$ and the only difficult case is with P and Q not in U. Assume that P and Q are points not in U such that $Q\in P^\perp$. We can choose coordinates in such a way that $P=(1,0,0)$ and $P^\perp$ is the line $X=0$. Let $Q_i=(0,y_i,1)$, $i=1,2,\ldots,q+1$ be the points of U on $P^\perp$ and let $Q=(0,y_0,1)$. Then $Y=y_0Z$ is the equation of the line PQ. There exist nonzero w_i, $i=0,1,\ldots,q+1$ such that

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ y_0 & y_1 & \cdots & y_{q+1} \\ y_0^2 & y_1^2 & \cdots & y_{q+1}^2 \\ \vdots & \vdots & \ddots & \vdots \\ y_0^q & y_1^q & \cdots & y_{q+1}^q \end{pmatrix} \begin{pmatrix} w_0 \\ w_1 \\ \\ \vdots \\ w_{q+1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \\ \vdots \\ 0 \end{pmatrix}.$$

The w_i can be taken nonzero since deleting a column from the above matrix yields a nonsingular $(q+1)\times(q+1)$ matrix (Vandermonde). Let k be an integer, $1\le k\le q$. Give weight w_ix^k to a point $(x,y_i,1)$, $x\in\mathbb{F}_{q^2}$, $i=0,1,2,\ldots,q+1$, and weight zero to all other points. Again this defines a word in the dual code as one easily verifies. Hence, if the $q+1$ points of the unital on the line $Y=y_0Z$ are given by $R_j=(x_j,y_0,1)$, $j=1,2,\ldots,q+1$, then it follows that

$$\sum_{j=1}^{q+1} w_0x_j^k=0\ .$$

Define the power sums π_k, $k \geq 1$, by

$$\pi_k = \sum_{j=1}^{q+1} x_j^k \ .$$

The generating functions

$$\pi(z) = \sum_{k=1}^{\infty} \pi_k z^k \ , \quad \text{and} \quad \sigma(z) = \prod_{j=1}^{q+1} (1 - x_j z) = \sum_{k=0}^{\infty} \sigma_j z^k$$

satisfy $\sigma(z)\pi(z) + z\sigma'(z) = 0$. From this one deduces the Newton identities

$$\sum_{m=0}^{n-1} \pi_{n-m}\sigma_m + n\sigma_n = 0 \ , \quad n \geq 1 \ .$$

Hence, since $\pi_k = 0$ for $k = 1, \ldots, q$, it follows that $\sigma_n = 0$ for $n \leq q$, $n \neq 0$ mod p. Using induction it then follows that $\pi_k = 0$ for $k \geq q+1$, $k \neq 1$ mod p. In particular it follows that $\pi_{q^2-2} = 0$ if $p \neq 3$ and $\pi_{q^2-4} = 0$ if $p = 3$, i.e., (using $x^{q^2-2} = x^{-1}$ and $x^{q^2-4} = x^{-3}$ if $x \in \mathbb{F}_{q^2}^*$) $\sum_{j=1}^{q+1} x_j^{-1} = 0$.

Let $R_0 = (x_0, y_0, 1)$ be any point on the line PQ, $R_0 \neq Q, P, R_j$, $j = 1, \ldots, q+1$ and compute the cross ratio $(Q, P; R_j, R_0)$:

$$(Q, P; R_j, R_0) = (0, \infty; x_j, x_0) = \frac{(0 - x_j)(\infty - x_0)}{(\infty - x_j)(0 - x_0)} = \frac{x_j}{x_0} \ .$$

Thus we have shown that $\sum_{j=1}^{q+1}(Q, P; R_j, R_0) = 0$. Hence, interchanging the rôles of P and Q and writing $R = (x, y_0, 1)$ for the point of intersection of $Q^\perp$ and PQ it follows that

$$\begin{aligned} 0 \ &= \ \sum_{j=1}^{q+1}(R, Q; R_j, R_0) \ = \ \sum_{j=1}^{q+1}(x, 0; x_j, x_0) \ = \\ &= \ \frac{x_0}{x - x_0}\left(\sum_{j=1}^{q+1} x/x_j - 1\right) \ = \ \frac{-x_0}{x - x_0} \ . \end{aligned}$$

We conclude that $x = \infty$, i.e., $P = R \in Q^\perp$.

Added in proof. Our theorem was conjectured by Assmus and Key in [6].

References

[1] R.D. Baker and G.L. Ebert, *Intersection of unitals in the Desarguesian plane*, preprint, appeared in Proceedings of the Twentieth Southeastern Conference on Combinatorics, Graph Theory, and Computing (Boca Raton, FL, 1989), vol. 70, 1990, pp. 87–94.

[2] J.C. Fisher, J.W.P. Hirschfeld and J.A. Thas, *Complete arcs in planes of square order*, Ann. Discrete Math. **30** (1986) 243–250.

[3] D.R. Hughes and F.C. Piper, *Projective Planes*, Springer, Berlin, 1973.

[4] C. Lefèvre-Percsy, *Characterization of Hermitian curves*, Arch. Math. **39** (1982) 476–480.

[5] M. Seib, *Unitäre Polaritäten endlicher projektiver Ebenen*, Arch. Math. **21** (1970) 103–112.

[6] E.F. Assmus Jr and J.D. Key, *Baer subplanes, ovals and unitals*, in: Coding Theory and Design Theory, part I: Coding Theory (Springer, Berlin, 1990) l–8.