Hermitian unitals are code words

Aart Blokhuis, Andries Brouwer and Henny Wilbrink

Department of Mathematics, Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB Eindhoven, Netherlands

Received 7 March 1990

In memory of Egmont Köhler.

Abstract

Blokhuis, A., A. Brouwer and H. Wilbrink, Hermitian unitals are code words, Discrete Mathematics 97 (1991) 63-68.

We show that a unital PG(2, q^2) is Hermitian if and only if it is in the code generated by the lines of PG(2, q^3). 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 an Hermitian unital. In [1] it is shown that a particular class of unitals in the Desarguesian plane 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 PG(2, q^2) is Hermitian if and only if it is in the \( \mathbb{F}_p \)-code spanned by the lines of PG(2, q^3).

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 $\mu$ is a multiplier of order 2 and show that $n = m^2$ and $\mu = m^3$. We shall then describe the geometrical implications of $\mu$. Define subgroups $A$ and $B$ of $G$ by

$$A = \{ x \in G \mid x^2 = x^{-1} \}, \quad B = \{ x \in G \mid x^n = x \},$$

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

$$g^\alpha := (g^{-\mu})^3, \quad g^\beta := (g^\mu)^3 \quad (g \in G).$$

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 $\mu$ 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 $\mu$ 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 $\mu$ 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 $\mu$ and is therefore a Baer line).

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

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

This lemma can be used to show that $A$ is an arc (i.e., no three points of $A$ are collinear): If $d_1 g, d_2 g \in D g \cap A$, 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 $X = \{ x_1, x_2, \ldots, x_t \} \subseteq G$ with the element $X = x_1 + x_2 + \cdots + x_t$ in $R[G]$. Also, for a homomorphism $\gamma$ of $G$, we define the $R$-homomorphism $[\gamma]$ of $R[G]$ by

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

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

**Lemma 2.** $D^\beta + (D \cap B)^{\beta} = 2B$ 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 $D^{(1)}$ and once in $(D \cap B)^{(1)}$, 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 $D^{[1]}$. (Thus, $(D \cap B)^{(1)}$ 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

$$U = A(D \cap B)^{(1)}.$$
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 $m^2 + 1 \neq 0$ (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 $\chi$ of $G$. So assume $\chi(D) = 0$. Since $\chi(U) = \chi(A)\chi((D \cap B)^{[1]})$ by Lemma 3, we may assume that $\chi(A) \neq 0$. Now $\chi(g) = \phi(g^a)\psi(g^b)$, $g \in G$, where $\phi$ is a character of $A$ and $\psi$ is a character of $B$. Hence, $\chi(A) = \chi(A) \neq 0$ implies that $\phi = 1_A$ and so $\chi(g) = \psi(g^b)$ for all $g \in G$. In particular

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

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

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

completing the proof that $U$ is in the code.

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

**Proposition.** Let $X$ be a subset of $PG(2, q)$ which is in the $\mathbb{F}_p$-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

$$w_1 + w_2 + w_3 = 0, \quad w_1 y_1 + w_2 y_2 + w_3 y_3 = 0.$$

Give weight $w_i x$ 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 innerproduct $\Sigma_i w_i(a y_i + b) = 0$, a line $Y = y_iZ$ has innerproduct $\Sigma x w_i x = 0$.) Since $X$ is in the code, $X$ has innerproduct zero with this word, i.e.,

$$w_1 x_1 + w_2 x_2 + w_3 x_3 = 0,$$

proving that $Q_1, Q_2$ and $Q_3$ are collinear. \(\square\)
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

\[
\begin{pmatrix}
1 & 1 & \cdots & 1 \\
y_0 & y_1 & \cdots & y_{q+1} \\
y_0^2 & y_1^2 & \cdots & y_{q+1}^2 \\
\vdots & \vdots & \ddots & \vdots \\
y_0^q & y_1^q & \cdots & y_{q+1}^q
\end{pmatrix}
\begin{pmatrix}
w_0 \\
w_1 \\
w_2 \\
\vdots \\
w_{q+1}
\end{pmatrix}
= \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.
\]

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, \( 1 \leq k \leq q \). Give weight \( w_i x^k \) 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

\[
\sum_{j=1}^{q+1} w_j x_j^k = 0.
\]

Define the powersums \( \pi_k \), \( k \geq 1 \), by

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

The generating functions

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

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 \( n \leq q \), \( n \not\equiv 0 \pmod{p} \). Using induction it then follows that \( \pi_k = 0 \) for \( k \geq q + 1 \), \( k \not\equiv 1 \pmod{p} \). In particular it follows that \( \pi_{q+1} z = 0 \) if \( p \neq 3 \) and \( \pi_{q-4} z = 0 \) 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 \((Q, P; R_j, R_0)\):
\[
(Q, P; R_j, R_0) = (0, \infty; x_j, x_0) = \frac{(0-x_j)(\infty-x_0)}{(\infty-x_j)(0-x_0)} = \frac{x_i}{x_0}.
\]

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
\[
0 = \sum_{j=1}^{q+1} (R, Q; R_j, R_0) = \sum_{j=1}^{q+1} (x, 0; x_j, x_0) = \frac{x_0}{x-x_0} \left(\sum_{j=1}^{q+1} \frac{x}{x_j} - 1\right)
\]
\[
= \frac{-x_0}{x-x_0}.
\]

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**