Can. J. Math., Vol. XLII, No. 6, 1990, pp. 1067–1083

A FAMILY OF UNITALS IN THE HUGHES PLANE

BARBU C. KESTENBAND

We construct a family of unitals in the Hughes plane. We prove that they are not isomorphic with the classical unitals, and in so doing we exhibit a configuration that exists in the latter, but not in the former. This new configurational property of the classical unitals might serve in the future again as an isomorphism test.

A particular instance of our construction has appeared in [11]. But it only concerns itself with the case where the matrix involved is the identity, whereas the present article treats the general case of symmetric matrices over a suitable field. Furthermore, [11] does not answer the isomorphism question. It states that (the English translation is ours) "It remains to be seen whether the unitary designs constructed in this note are isomorphic or not with known designs".

We shall use the notation of [9]:

F: $GF(q)$, q odd.

Φ: $GF(q^2)$, q odd.

t: a primitive root of Φ.

Φ_S, Φ_N: the sets of squares, nonsquares, respectively, in Φ.

Ψ: the regular nearfield of order q^2, with the same elements as Φ, in which addition is the same as in Φ, while multiplication, denoted by $\cdot$, is defined as follows:

$$\rho \cdot \sigma = \begin{cases} \rho\sigma & \text{if } \sigma \in \Phi_S \\ \rho^q \sigma & \text{if } \sigma \in \Phi_N \end{cases}$$

Since $\rho^q = \rho$ for all $\rho \in F$, we have $\rho \cdot \sigma = \rho\sigma$ for all $\rho \in F$ and $\sigma \in \Psi$.

Π: the Desarguesian projective plane over Φ.

Ω: the Hughes projective plane over Ψ.

We adopt the view that the points of Π and Ω are the same. The points of Ω will be denoted by $\begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$, $\begin{pmatrix} x \\ 1 \\ 0 \end{pmatrix}$ or $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, as the case may be. The points of Π will sometimes be denoted by $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$, where z is not necessarily an element of F.

Received July 10, 1990.

Subject classification: Primary 51E20, Secondary 05B30.

The lines of Ω are sets of points satisfying one of the following equations [9]:

$$y - sz = k \cdot (x - rz), \quad r, s \in F, \quad k \in \Psi - F;$$

$$y = mx + \lambda z, \quad m \in F, \quad \lambda \in \Psi;$$

$$x + \mu z = 0, \quad \mu \in \Psi; \quad \text{finally, } z = 0.$$

We use $\cdot$ only when multiplication in Ψ is not necessarily the same as in Φ. Thus we do not use $\cdot$ when z is involved, because we have established that $z \in F$ in all cases. Notice that the lines of the last three types contain the same points in Ω as in Π.

A $2-(v, k, 1)$ design is a set of v points, with distinguished subsets called blocks, such that each block has k points and any two distinct points appear in a unique block [5, p. 246]. We will occasionally use "block" and "line" interchangeably.

A $2-(s^3+1, s+1, 1)$ design is called a unital [5, p. 246]. The original unitals were obtained as the sets of absolute points and non-absolute lines of certain polarities of Π. Specifically, let $H = (h_{ij})$ be a Hermitian matrix over Φ, i.e. one for which $h_{ij}^q = h_{ji}$ for all i, j. A unital comprises the points $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ which satisfy the equation:

$$(1) \qquad h_{11}x^{q+1} + h_{22}y^{q+1} + h_{33}z^{q+1} + h_{12}xy^q + h_{21}x^q y + h_{13}xz^q + h_{31}x^q z + h_{23}yz^q + h_{32}y^q z = 0$$

If $\mathbf{u} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ is a point of Π (viewed as a column vector), let $\mathbf{u}^{(q)} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}^{(q)} = \begin{pmatrix} x^q \\ y^q \\ z^q \end{pmatrix}$. Then equation (1) can be written:

$$(2) \qquad \mathbf{u}^T H \mathbf{u}^{(q)} = 0$$

In time, as new families of unitals were found (see [1], [2], [4], [6], [8]), the original unitals began to be called "classical unitals". As the unitals constructed in this paper – in Ω – consist of the same points as the classical ones (but not of the same blocks), we deem it fitting to christen them "classical Hughes unitals".

If H is a symmetric matrix with entries from F, it is Hermitian over Φ. Then the classical unital it defines contains together with a point $\mathbf{u}$, the point $\mathbf{u}^{(q)}$. To see this, note that (2) is equivalent to:

$$\mathbf{u}^{(q)^T} H^T \mathbf{u} = 0$$

But $H^T = H$ by assumption, and also $[\mathbf{u}^{(q)}]^{(q)} = \mathbf{u}$ for any point $\mathbf{u}$, so that the last equation can be rewritten as:

$$\mathbf{u}^{(q)^T} H [\mathbf{u}^{(q)}]^{(q)} = 0$$

Comparing this with (2) proves the claim.

We need to introduce new notation:

L_{krs}: the line $y - sz = k(x - rz)$ in Π.

$\tilde{L}_{krs}$: the line $y - sz = k \cdot (x - rz)$ in Ω.

L^q_{krs}: the line $y - sz = k^q(x - rz)$ in Π.

$\tilde{L}^q_{krs}$: the line $y - sz = k^q \cdot (x - rz)$ in Ω.

P^q: the image of the point P under the involutory automorphism of Φ.

We have the following straightforward implications:

$$P \in L_{krs} \Leftrightarrow P^q \in L^q_{krs} \quad \text{and} \quad P \in \tilde{L}_{krs} \Leftrightarrow P^q \in \tilde{L}^q_{krs}.$$

THEOREM 1. *Let H be a symmetric matrix over F, and U, the classical unital it defines in Π. Then the lines $\tilde{L}_{krs}$ and L_{krs} have the same number of points in common with U.*

Proof. Observe first that if a point $P \in L_{krs}$, then either $P \in \tilde{L}_{krs}$ or $P \in \tilde{L}^q_{krs}$.

Let L_{krs} intersect U at the $u + v$ distinct points $P_1, \ldots, P_u$, $Q_1, \ldots, Q_v$, where $P_1, \ldots, P_u \in \tilde{L}_{krs}$ and $Q_1, \ldots, Q_v \in \tilde{L}^q_{krs}$.

Then $Q^q_i \in \tilde{L}_{krs}$, $i = 1, \ldots, v$, and thus $\tilde{L}_{krs}$ includes $P_1, \ldots, P_u$, $Q^q_1, \ldots, Q^q_v$.

These points are distinct, for if $P_i = Q^q_j$ for some i, j, then $P_i \in L_{krs} \cap L^q_{krs}$,

so $P_i = \begin{pmatrix} r \\ s \\ 1 \end{pmatrix}$, but then $Q_j = \begin{pmatrix} r \\ s \\ 1 \end{pmatrix}^{(q)} = \begin{pmatrix} r \\ s \\ 1 \end{pmatrix} = P_i$, a contradiction.

Furthermore, the above points are all in U, so we see that $|\tilde{L}_{krs} \cap U| \geqq u + v$.

To show that equality holds, assume, contrariwise, that $\tilde{L}_{krs}$ contains another point R of U.

This extra point cannot be $\begin{pmatrix} r \\ s \\ 1 \end{pmatrix}$: if $\begin{pmatrix} r \\ s \\ 1 \end{pmatrix}$ is on U, then, since it is on L_{krs} as well, it must be one of the points $P_1, \ldots, P_u$, $Q^q_1, \ldots, Q^q_v$, whereas R is not supposed to be on this list.

Since $\tilde{L}_{krs} \subset L_{krs} \cup L^q_{krs}$, we have either $R \in L_{krs} \cap U$ or $R \in L^q_{krs} \cap U$, but not both.

In the first situation, as R is distinct from $P_1, \ldots, P_u$, it has to be one of the Q_j's. But this is not possible, either, because the Q_j's are on $\tilde{L}^q_{krs}$, while R is on

$\tilde{L}_{krs}$, and these two lines meet at $\begin{pmatrix} r \\ s \\ 1 \end{pmatrix} \neq R$.

The case $R \in L^q_{krs} \cap U$ is disposed of in like manner, by taking into account the fact that L^q_{krs} meets U at $P^q_1, \ldots, P^q_u$, $Q^q_1, \ldots, Q^q_v$. Q.E.D.

As the lines $\tilde{L}_{krs}$ are the only lines of Ω that are different from those of Π, what Theorem 1 shows is that the lines of Ω intersect U at $q+1$ points or at one point. Hence

COROLLARY 1. *Let U be a classical unital defined by a symmetric matrix over F. Then the points of U, together with the lines of Ω that are not tangent to U, as blocks, form a unital.*

As already agreed upon, we shall henceforth refer to the unitals of Corollary 1 as the "classical Hughes unitals".

We now tackle the non-isomorphism problem. In order to show that the two families are distinct, we will describe a configuration which always exists in the classical unital, but only sometimes in the new unital. Specifically:

We will say that a unital has property κ if it meets the following requirement:

For any point P and any block $B_1 = \{Q_0, \ldots, Q_q\}$ not on P, consider the blocks $C_0, \ldots, C_q$, containing the pairs $\{P, Q_0\}, \ldots, \{P, Q_q\}$. Then:

(i) There are $q-1$ blocks $B_2, \ldots, B_q$, mutually disjoint and also disjoint from B_1, such that each B_i intersects each C_j, $i = 1, \ldots, q$, $j = 0, \ldots, q$.

(ii) No other block intersects more than two of the C_j's.

We now prove that the classical unitals do, and the classical Hughes unitals do not, have property κ.

THEOREM 2. *Classical unitals have property κ.*

Proof. Since any two classical unitals are equivalent, in the sense that there is a collineation of Π that maps one onto the other, ([5], p. 62), it suffices to prove the theorem for the unital U:

$$y^{q+1} + xz^q + x^q z + yz^q + y^q z = 0, \quad \text{where } H = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Let Γ be the subgroup of $PGL(V)$ that fixes U (also known as the unitary group). It is known that Γ is 2-transitive on the points of U ([5], p. 62). Hence, if a point $P \in U$ and a block $B_1 = \{Q_0, \ldots, Q_q\}$ are given, there is an element of Γ that maps P, Q_0, onto $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, respectively. Thus we will assume without loss of generality, that $P = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \in B_1$.

Note further that $\begin{pmatrix} a \\ b \\ 1 \end{pmatrix} \in U$ for some $a, b \in \Phi$, and $\omega + \omega^q = 0$, implies that

https://doi.org/10.4153/CJM-1990-057-1 Published online by Cambridge University Press

$\begin{pmatrix} a+\omega \\ b \\ 1 \end{pmatrix} \in U$ as well. Hence the points on any block through P are, besides P, of the form $\begin{pmatrix} a+\omega \\ b \\ 1 \end{pmatrix}$, where a, b are fixed, while ω ranges through the solution set of the equation $x + x^q = 0$.

On the other hand, the collinearity of $\begin{pmatrix} a_0 \\ b_0 \\ 1 \end{pmatrix}, \ldots, \begin{pmatrix} a_q \\ b_q \\ 1 \end{pmatrix}$ entails that of $\begin{pmatrix} a_0+\rho \\ b_0 \\ 1 \end{pmatrix}, \ldots, \begin{pmatrix} a_q+\rho \\ b_q \\ 1 \end{pmatrix}$ for any ρ.

We have thus established that the map $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} a \\ b \\ 1 \end{pmatrix} \longrightarrow \begin{pmatrix} q+\omega \\ b \\ 1 \end{pmatrix}$, with $\omega + \omega^q = 0$, is a central automorphism of U, in the sense of [3], p. 82, with $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ as center. These automorphisms form a group isomorphic with the additive group of F, because $\omega + \omega^q = 0$ implies $c\omega + (c\omega)^q = 0$ for any $c \in F$.

Now, B_1 being given, the blocks $B_2, \ldots, B_q$ are obtained by the action of this group on B_1.

It remains to be shown that no other block of U intersects more than two of the C_j's.

Assume that U has three collinear points $\begin{pmatrix} a_i+x \\ b_i \\ 1 \end{pmatrix}, \begin{pmatrix} a_j+y \\ b_j \\ 1 \end{pmatrix}, \begin{pmatrix} a_k+z \\ b_k \\ 1 \end{pmatrix}$ with x, y, z all different, and also b_i, b_j, b_k all different, where $\begin{pmatrix} a_i \\ b_i \\ 1 \end{pmatrix}, \begin{pmatrix} a_j \\ b_j \\ 1 \end{pmatrix}, \begin{pmatrix} a_k \\ b_k \\ 1 \end{pmatrix} \in B_1$. We will prove that this assumption leads to a contradiction.

The collinearity of the three points in B_1 is equivalent to $\dfrac{a_j - a_i}{b_j - b_i} = \dfrac{a_k - a_i}{b_k - b_i}$.

If the first triple is also collinear, we get $\dfrac{a_j - a_i + y - x}{b_j - b_i} = \dfrac{a_k - a_i + z - x}{b_k - b_i}$, which reduces to $\dfrac{y-x}{b_j - b_i} = \dfrac{z-x}{b_k - b_i}$.

As x, y, z are all different, the last equation can be rewritten as $\dfrac{y-x}{z-x} = \dfrac{b_j - b_i}{b_k - b_i}$.

Since $\begin{pmatrix} a_i \\ b_i \\ 1 \end{pmatrix}, \begin{pmatrix} a_i + x \\ b_i \\ 1 \end{pmatrix} \in U$, we obtain the equations:

$$b_i^{q+1} + a_i + a_i^q + b_i + b_i^q = 0 \tag{3}$$

and $b_i^{q+1} + a_i + x + a_i^q + x^q + b_i + b_i^q = 0$, whence $x + x^q = 0$.

Similarly, $y + y^q = z + z^q = 0$.

As a consequence, we have $y - x = -(y-x)^q$ and $z - x = -(z-x)^q$. Thus:

$$\frac{y-x}{z-x} = \left(\frac{y-x}{z-x}\right)^q, \text{ in other words } \frac{y-x}{z-x} \in F.$$

Denote $\dfrac{y-x}{z-x} = s \neq 0, 1$. We have $s = s^q$. Then:

$$b_j - b_i = s(b_k - b_i) \tag{4}$$

and also $a_j - a_i = s(a_k - a_i)$.

Equation (4) gives successively:

$$b_j = b_i + s(b_k - b_i), \quad b_j^q = b_i^q + s(b_k^q - b_i^q),$$
$$b_j^{q+1} = b_i^{q+1} + s(b_i^q b_k + b_i b_k^q - 2b_i^{q+1}) + s^2(b_k - b_i)^{q+1}.$$

Upon substituting these three equations into (3) (with i replaced by j), and then using (3) repeatedly, one obtains $(s^2 - s)(b_k - b_i)^{q+1} = 0$.

This final equation gives $b_k = b_i$, the contradiction that completes the proof. Q.E.D.

We turn now to proving that the classical Hughes unitals do not enjoy property κ. A few preparatory results are needed.

Throughout the remainder of the paper, U will stand for the unital in Theorem 2, regarded as a point-set, both in Π and Ω. Also, we will denote $t^{(q+1)/2}$ by w, t being a primitive root of Φ.

It is an easy check that the solutions of the equation $x + x^q = 0$ are $x = aw$, where a ranges through F.

LEMMA 1. *The line $y = \alpha x$, $\alpha \neq 0$, meets U at points whose first coordinates x are of the form:*

$$x = \left(\frac{1}{\alpha} + \frac{1}{\alpha^{q+1}}\right)[t^{i(q-1)} - 1], \quad i = 0, \ldots, q.$$

Proof. In the equation of U (see Theorem 2), let $z = 1$, and substitute $y = \alpha x$ to obtain:

$$\alpha^{q+1}x^{q+1} + (\alpha^q + 1)x^q + (\alpha + 1)x = 0 \tag{5}$$

https://doi.org/10.4153/CJM-1990-057-1 Published online by Cambridge University Press

We have the readily verified identity:

$$\left(\alpha x + 1 + \frac{1}{\alpha^q}\right)^{q+1} = \alpha^{q+1}x^{q+1} + (\alpha^q + 1)x^q + (\alpha + 1)x + \left(1 + \frac{1}{\alpha^q}\right)^{q+1}$$

Thus (5) is equivalent to:

$$\left(\alpha x + 1 + \frac{1}{\alpha^q}\right)^{q+1} = \left(1 + \frac{1}{\alpha^q}\right)^{q+1},$$

whence:

$$\alpha x + 1 + \frac{1}{\alpha^q} = \left(1 + \frac{1}{\alpha^q}\right) t^{i(q-1)}, \quad i = 0, \ldots, q.$$

Now solve for x. Q.E.D.

LEMMA 2. *For $i = 1, \ldots, q$, denote $t^{i(q-1)} - 1 = t^{r_i}$. Then:*
If $q \equiv 1 \bmod 4$, i and r_i have opposite parities.
If $q \equiv 3 \bmod 4$, i and r_i have the same parity.

Proof. Since $-1 = t^{(q^2-1)/2}$, the equation in the statement of the lemma can be written as:

(6) $$t^{r_i} = t^{i(q-1)} + t^{(q^2-1)/2}$$

As $(-1)^q = -1$, raising both sides of (6) to the qth power gives:

(7) $$t^{qri} = t^{qi(q-1)} + t^{(q^2-1)/2}$$

We have the identity (check!):

$$t^{qi(q-1)} + t^{(q^2-1)/2} = t^{(q^2-1)/2 - i(q-1)}[t^{i(q-1)} + t^{(q^2-1)/2}].$$

Therefore, using (6) and (7), we obtain:

$$t^{qr_i} = t^{(q-1)(q+1/2-i)} t^{r_i}$$

Hence $t^{(q-1)r_i} = t^{(q-1)(q+1/2-i)}$, so that: $(q-1)r_i \equiv (q-1)\left(\frac{q+1}{2} - i\right) \bmod q^2 - 1$, i.e. $r_i + i \equiv \frac{q+1}{2} \bmod q + 1$.

Thus $r_i + i$ is an odd multiple of $\frac{q+1}{2}$ and the conclusion follows. Q.E.D.

LEMMA 3. *The lines $y = \alpha x$ and $y = \alpha \cdot x$, $\alpha \neq 0$, intersect U at $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ and q more points. Denote the first coordinate of the latter by x.*

https://doi.org/10.4153/CJM-1990-057-1 Published online by Cambridge University Press

If $q \equiv 1 \bmod 4$ and $\frac{1}{\alpha}+\frac{1}{\alpha^{q+1}} \in \Phi_S$, or $q \equiv 3 \bmod 4$ and $\frac{1}{\alpha}+\frac{1}{\alpha^{q+1}} \in \Phi_N$, $\frac{q+1}{2}$ of these points have $x \in \Phi_s$, while the remaining $\frac{q-1}{2}$ points have $x \in \Phi_N$.

Furthermore, the above paragraph remains valid if Φ_N and Φ_S are interchanged.

Proof. It is an immediate consequence of Lemmas 1 and 2 that the present one holds for the line $y = \alpha x$ in Π.

If $\alpha \in F$, the two lines in question are one and the same. So assume $\alpha \notin F$. Let the points of U on $y = \alpha x$ be:

$$\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} \sigma_1 \\ \alpha\sigma_1 \\ 1 \end{pmatrix}, \dots, \begin{pmatrix} \sigma_u \\ \alpha\sigma_u \\ 1 \end{pmatrix}, \begin{pmatrix} \nu_1 \\ \alpha\nu_1 \\ 1 \end{pmatrix}, \dots, \begin{pmatrix} \nu_v \\ \alpha\nu_v \\ 1 \end{pmatrix},$$

where $\sigma_i \in \Phi_S$, $i = 1, \dots, u$, $\nu_j \in \Phi_N$, $j = 1, \dots, v$, $u, v = \frac{q \pm 1}{2}$ and $u+v = q$.

Then the line $y = \alpha \cdot x$ has the following points in common with U:

$$\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} \sigma_1 \\ \alpha\sigma_1 \\ 1 \end{pmatrix}, \dots, \begin{pmatrix} \sigma_u \\ \alpha\sigma_u \\ 1 \end{pmatrix}, \begin{pmatrix} \nu_1^q \\ \alpha^q\nu_1^q \\ 1 \end{pmatrix}, \dots, \begin{pmatrix} \nu_v^q \\ \alpha^q\nu_v^q \\ 1 \end{pmatrix}$$

The proof is finished, because the involutory automorphism of Φ leaves Φ_S and Φ_N invariant. Q.E.D.

LEMMA 4. *In Π, the lines $y = wx$ and $y = w^q x$ meet U at $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ and at exactly one more point for which $y \in F$.*

Proof. To find the points of intersection between $y = wx$ and U, one solves the equation:

$$y^{q+1} + \frac{y}{w} + \frac{y^q}{w^q} + y + y^q = 0 \tag{8}$$

Since we want $y \in GF(q)$, we impose $y = y^q$. Besides, we have $w^q = t^{(q^2+q)/2} = t^{(q^2-1)/2} t^{(q+1)/2} = -t^{(q+1)/2} = -w$. Thus (8) becomes:

$$y^2 + \frac{y}{w} - \frac{y}{w} + 2y = 0,$$

yielding $y = 0, -2$. Similarly for $y = w^q x$. Q.E.D.

COROLLARY 2. *In Ω, the line $y = w \cdot x$ meets U at $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ and at exactly one more point with $y \in F$.*

https://doi.org/10.4153/CJM-1990-057-1 Published online by Cambridge University Press

Proof. When $q \equiv 3 \bmod 4$, w is a square and then so is $-2/w$, hence $\begin{pmatrix} -2/w \\ -2 \\ 1 \end{pmatrix}$ is on $y = w \cdot x$.

Assume there were a third point in U with $y \in F$ for which $y = w \cdot x$. As y is a square, and w is, too, x must be a square as well. But then $y = wx$ for this point, so we have found a third point in U that lies on $y = wx$ and has $y \in F$, in violation of Lemma 4.

If $q \equiv 1 \bmod 4$, w is a nonsquare, and so is $-2/w^q$, hence $\begin{pmatrix} -2/w^q \\ -2 \\ 1 \end{pmatrix}$ is on $y = w \cdot x$. The rest is as in the previous paragraph. Q.E.D.

LEMMA 5. *Let $a \in F$, $a \neq 0$. Among the solutions of the equation $x + x^q = a$, there are: $\frac{q+1}{2}$ nonsquares and $\frac{q-1}{2}$ squares if $q \equiv 3$ mod 4. $\frac{q-1}{2}$ nonsquares and $\frac{q+1}{2}$ squares if $q \equiv 1$ mod 4.*

Proof. If u is a solution of $x + x^q = 1$, then au, where $a \in F$, is a solution of $x + x^q = a$, because $a = a^q$.

Since, on the other hand, $a \in F$ implies $a \in \Phi_S$, we see that the number of squares and nonsquares among the solutions of $x + x^q = a \neq 0$ is independent of a.

Further, we noted earlier than the solutions of $x + x^q = 0$ are $x = aw$, $a \in F$. Therefore they are all in Φ_S (if $w \in \Phi_S$) or all (except $x = 0$) in Φ_N (if $w \in \Phi_N$).

But $w = t^{(q+1)/2}$, so that $w \in \Phi_S$ for $q \equiv 3 \bmod 4$ and $w \in \Phi_N$ for $q \equiv 1 \bmod 4$.

Assume first $q \equiv 3 \bmod 4$. Then the solutions of $x + x^q = 0$ are all in Φ_S. Among the remaining $q^2 - q$ elements of Φ there are $\frac{q^2-1}{2}$ nonsquares and $\frac{(q-1)^2}{2}$ squares. But there are $q - 1$ equations of type $x + x^q = a \neq 0$. Thus each of these equations has $\frac{q+1}{2}$ roots in Φ_N and $\frac{q-1}{2}$ roots in Φ_S.

If $q \equiv 1 \bmod 4$, the nonzero solutions of $x + x^q = 0$ are in Φ_N. The rest is as in the preceding case. Q.E.D.

LEMMA 6. *Consider the unital U in Π and Ω. Of the $q+1$ blocks joining the point $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ with the $q+1$ points of the block $y = wx$ (in Π) or $y = w \cdot x$ (in Ω), two are $y = 0$ and $y = -2z$. The x-coordinates of the points in these two blocks satisfy $x + x^q = 0$.*

For all the points in the remaining $q - 1$ blocks, $x + x^q \neq 0$.

Proof. Let $z = 1$. We require $x + x^q = 0$ and $y = wx$ in the equation of U. This gives $y^{q+1} + y + y^q = 0$, in other words $w^{q+1}x^{q+1} + wx + w^q x^q = 0$.

But $w^q = -w$ and $x^q = -x$, which reduces the last equation to $wx(wx+2) = 0$, whence $y = wx = 0$ or -2.

The same conclusion must hold for $y = w \cdot x$. Q.E.D.

LEMMA 7. *Any two classical Hughes unitals are equivalent.*

Proof. Let U, U' be two classical Hughes unitals. We will exhibit a collineation θ of Ω with $U^\theta = U'$.

The points of U, U' form two classical unitals in Π, defined by the symmetric matrices H, H', respectively: $\mathbf{u}^T H \mathbf{u}^{(q)} = 0$, $\mathbf{u}^T H' \mathbf{u}^{(q)} = 0$.

Their intersections with the Desarguesian subplane Ω_0 of Ω are the two conics $\Delta : \mathbf{u}^T H \mathbf{u} = 0$, $\Delta' : \mathbf{u}^T H' \mathbf{u} = 0$.

Since any two conics in Ω_0 are equivalent ([5], p. 52), there exists a matrix A over F with $H = A^T\ H'A$. Thus A defines a collineation of Ω_0, which extends to a collineation θ of Ω [10]:

$$\mathbf{a}^\theta = A\mathbf{a} \text{ for any } \mathbf{a} \in \Omega$$

Let $\mathbf{a} \in U$, i.e. $\mathbf{a}^T H \mathbf{a}^{(q)} = 0$. Then:

$$(A\mathbf{a})^T H' (A\mathbf{a})^{(q)} = \mathbf{a}^T A^T H' A^{(q)} \mathbf{a}^{(q)} = \mathbf{a}^T A^T H' A \mathbf{a}^{(q)} = \mathbf{a}^T H \mathbf{a}^{(q)} = 0,$$

showing that $A\mathbf{a} \in U'$, hence $U^\theta = U'$. Q.E.D.

THEOREM 3. *The classical Hughes unitals do not have property* κ.

Proof. By Lemma 7, it suffices to consider the unital U in Ω.

We will choose the point P and the block B_1 to be $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ and $y = w \cdot x$. We will then obtain a block (as a matter of fact there are many) that intersects at least three, but not all, of the C_j's, in violation of property κ.

Let $q \equiv 3 \bmod 4$, in which case $w \in \Phi_S$.

In Fig. 1 we illustrate the situation in Π – where property κ holds – for

$P = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ (not shown) and $B_1 : y = wx$.

Here, $-2/w, \sigma_2, \ldots, \sigma_u \in \Phi_S$, $\nu_1, \ldots, \nu_v \in \Phi_N$.

In view of what follows, we need to make sure that $u \geqq 2$. By Lemma 3 (applied to Π), as long as $q \geqq 7$, we have $u \geqq \dfrac{q-1}{2} \geqq 3$.

For $q = 3$, we have $w = t^2$ and $t^8 = 1$, whence $\dfrac{1}{w} + \dfrac{1}{w^4} = t^6 + 1$ and it is an easy check that $t^6 + 1 \in \Phi_N$, so that by Lemma 3 again, $u = 2$ as needed.

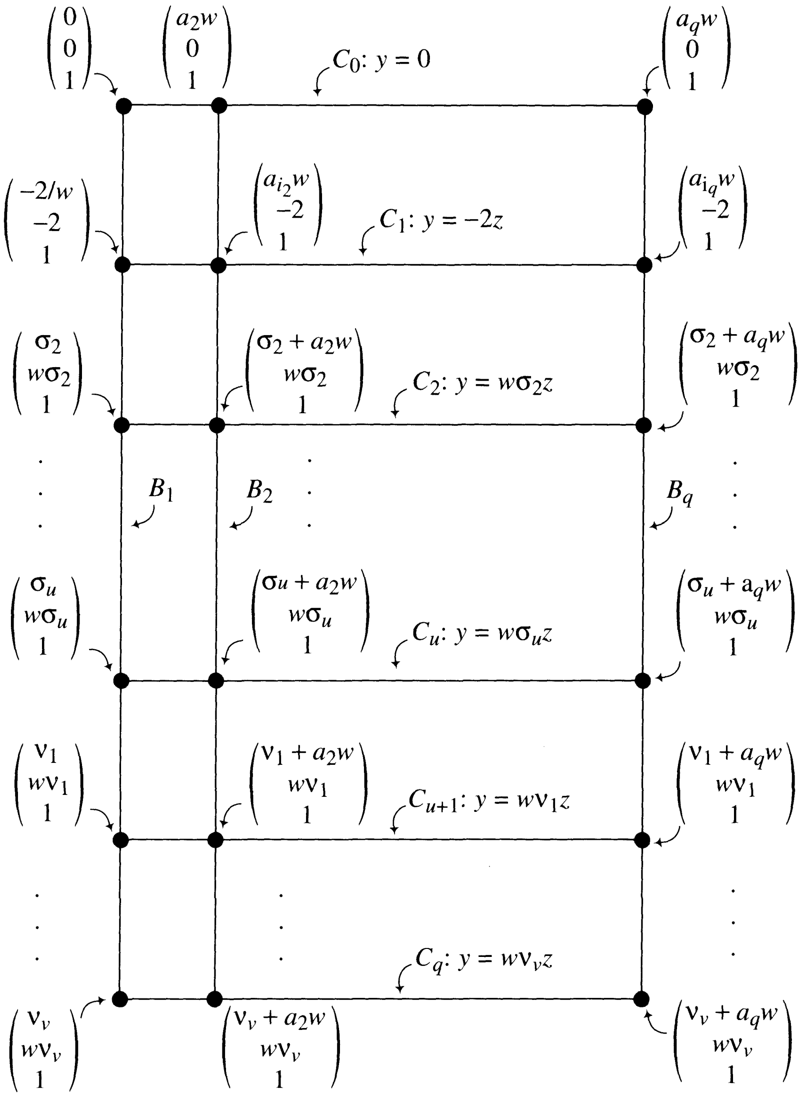

Fig. 1

The block $C_0 : y = 0$ contains points whose first coordinates satisfy $x+x^q = 0$, i.e. multiples of w by the elements of F.

The same holds for the block $C_1 : y = -2z$, because in this case $y^{q+1} + yz^q + y^q z = (-2z)^{q+1} - 2z^{q+1} + (-2z)^q z = 4z^{q+1} - 2z^{q+1} - 2z^{q+1} = 0$ and thus the

https://doi.org/10.4153/CJM-1990-057-1 Published online by Cambridge University Press

equation of U boils down to $x + x^q = 0$ (because $z = 1$).

Thus, in Fig. 1, $a_2, \ldots, a_q$ are the nonzero elements of F. Then, $a_{i_2}, \ldots, a_{i_q}$ are also distinct elements of F, one of which is zero, and related to the former (straightforward verification) as follows:

$$a_{i_k} = -\frac{2}{w^2} + a_k, \quad k = 2, \ldots, q \tag{9}$$

The blocks B_i are subsets of the lines:

$$y + a_i w^2 z = wx, \quad i = 2, \ldots, q \tag{10}$$

Fig. 2 shows what takes place in Ω. Here, $B_1 : y = w \cdot x$.

The blocks $C_0, \ldots, C_u$ are the same as in Fig. 1, while $C'_{u+1}, \ldots, C'_q$ are the images of $C_{u+1}, \ldots, C_q$, respectively, under the involutory automorphism of Φ.

Consider the blocks C_u and C'_{u+1}. By Lemma 6, the x-coordinates of the points in these blocks satisfy $x + x^q = a \neq 0$ (a could be different for the two blocks). Thus, by Lemma 5, on both blocks, the first coordinate is a nonsquare $\frac{q+1}{2}$ times.

Since $\frac{q+1}{2} + \frac{q+1}{2} > q$, there must be an "overlap", in the sense that there exists a nonzero element $a_l \in F$ for which $\sigma_u + a_l w$ and $\nu_1^q - a_l w$ are both nonsquares.

Consider the block $y + a_l w^2 z = w \cdot x$. It is a simple check that it contains the three points $\begin{pmatrix} a_l w \\ 0 \\ 1 \end{pmatrix}$, $\begin{pmatrix} a_{i_l} w \\ -2 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} \nu_1^q - a_l w \\ w^q \nu_1^q \\ 1 \end{pmatrix}$.

The block in question, however, does not meet C_u: if it does, the point of intersection either has $x \in \Phi_S$ and therefore satisfies the equation $y + a_l w^2 z = wx$ (but there is no such point, because on C_u the only point that satisfies this last equation is $\begin{pmatrix} \sigma_u + a_l w \\ w\sigma_u \\ 1 \end{pmatrix}$ and we already know that $\sigma_u + a_l w \notin \Phi_S$), or it has $x \in \Phi_N$ and hence must satisfy the equation:

$$y + a_l w^2 z = w^q x \tag{11}$$

But this cannot be the case, either, because this last line (in Π) meets C_0 and C_1, at $\begin{pmatrix} -a_l w \\ 0 \\ 1 \end{pmatrix}$, $\begin{pmatrix} -a_{i_l} w \\ -2 \\ 1 \end{pmatrix}$, respectively, and if it intersected C_u as well, it would be (by property κ, which *does* hold in Π) one of the blocks $B_2, \ldots, B_q$, which it is not, because its equation —(11)— does not agree with (10).

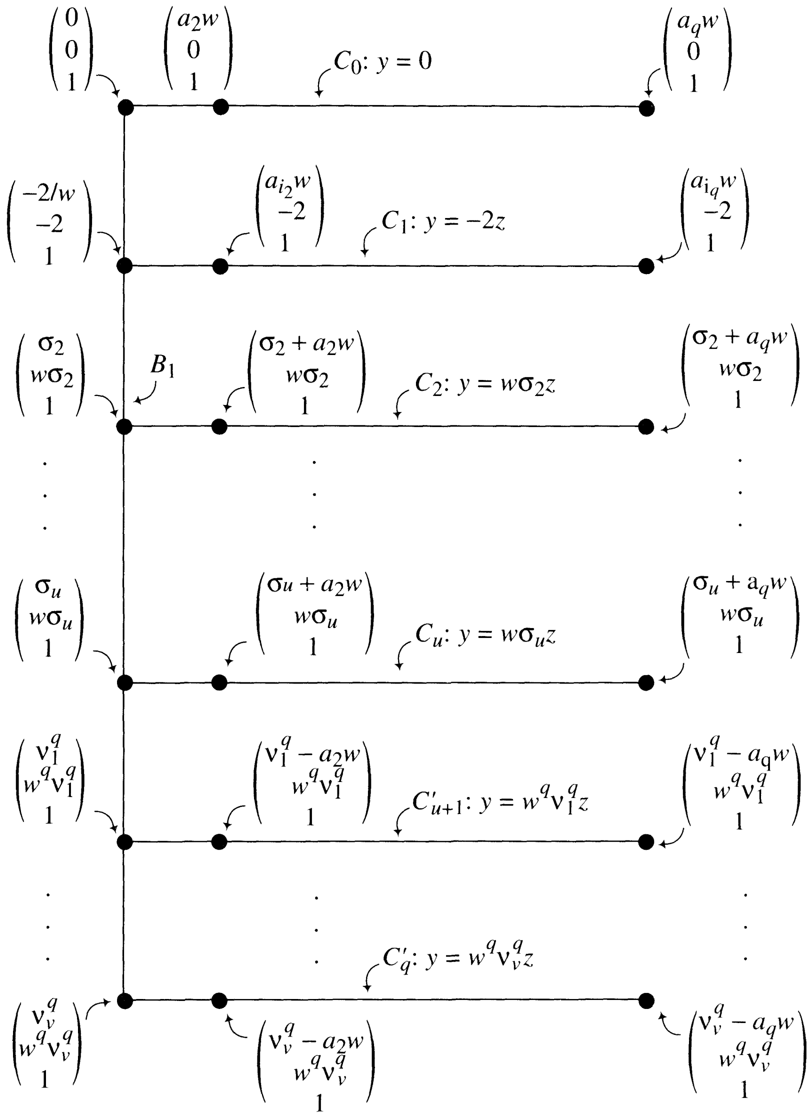

Fig. 2

We have thus shown that the block $y + a_l w^2 z = w \cdot x$ meets C_0, C_1, C'_{u+1}, but not C_u, in conflict with property κ.

If $q \equiv 1 \bmod 4$, the proof is fairly similar, but there are differences that need to be explained. In this case $w \in \Phi_N$.

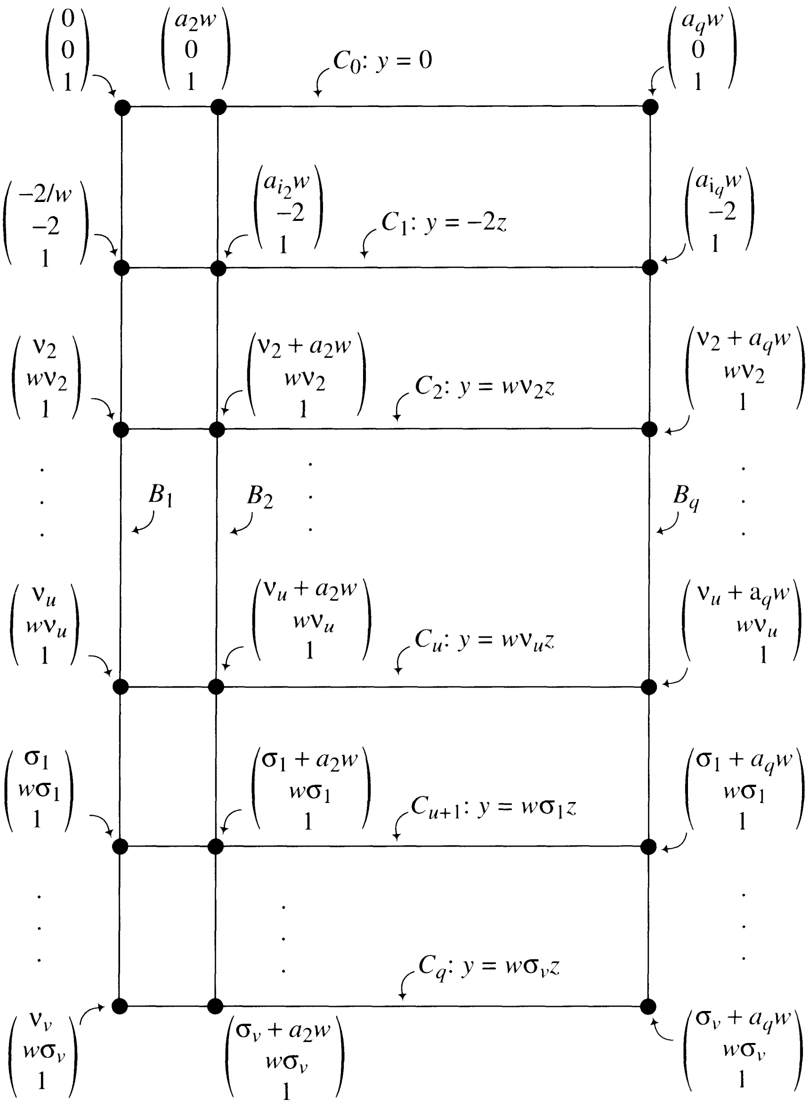

Fig. 3

Fig. 3 illustrates the situation in Π, for $P = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ and $B_1 : y = wx$.

We have $-2/w, \nu_2, \ldots, \nu_u \in \Phi_N$, and $\sigma_1, \ldots, \sigma_v \in \Phi_S$.

By Lemma 3 again, $u \geqq \dfrac{q-1}{2}$. But $q \geqq 5$, so $u \geqq 2$.

Furthermore, (9) and (10) hold in this case, too.

Fig. 4 shows what happens in Ω.

https://doi.org/10.4153/CJM-1990-057-1 Published online by Cambridge University Press

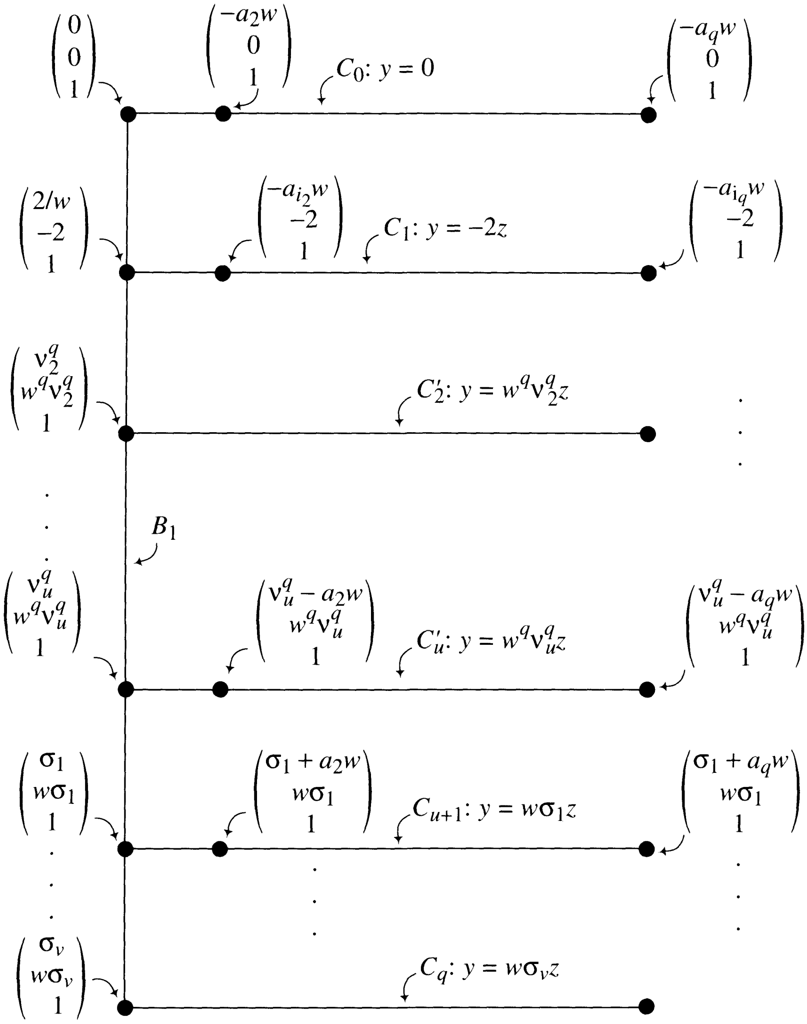

Fig. 4

Here, $B_1 : y = w \cdot x$.

Consider the blocks C'_u and C_{u+1}.

Using Lemma 5 as in the first case, we see that there must exist a nonzero element $a_l \in F$ for which $\nu_u^q - a_l w$ and $\sigma_1 + a_l w$ are both squares.

Consider, in Ω, the block $y + a_l w^2 z = w \cdot x$. It contains the points $\begin{pmatrix} -a_l w \\ 0 \\ 1 \end{pmatrix}$, $\begin{pmatrix} -a_{i_l} w \\ -2 \\ 1 \end{pmatrix}$, $\begin{pmatrix} \sigma_1 + a_l w \\ w\sigma_1 \\ 1 \end{pmatrix}$.

We will now show that this block fails to intersect the block C'_u: if it does, and the point of intersection has $x \in \Phi_N$, that point will satisfy the equation $y + a_l w^2 z = w^q x$. But the only point on C'_u satisfying this equation is $\begin{pmatrix} \nu_u^q - a_l w \\ w^q \nu_u^q \\ 1 \end{pmatrix}$ and we have seen that $\nu_u^q - a_l w \notin \Phi_N$.

If, on the other hand, the point of intersection has $x \in \Phi_S$, it has to satisfy $y + a_l w^2 z = wx$, i.e. $w^q \nu_u^q + a_l w^2 = wx$, whence:

$$x = -\nu_u^q + a_l w \tag{12}$$

But all the points on C'_u have $x = \nu_u^q - a_i w$ for some i. Upon combining this with (12), one gets $\nu_u^q = (a_l + a_i)w/2$, whence, because $w^q = -w$, one obtains:

$$\nu_u = -\nu_u^q \tag{13}$$

The point $\begin{pmatrix} \nu_u \\ w\nu_u \\ 1 \end{pmatrix}$ must satisfy the equation of U, so we also have:

$$w^{q+1}\nu_u^{q+1} + \nu_u + \nu_u^q + w\nu_u + w^q \nu_u^q = 0 \tag{14}$$

Using (13) and $w^q = -w$, equation (14) yields $\nu_u = -2/w$, which transforms (12) into $x = -\dfrac{2}{w} + a_l w$. Now, by (9), this in turn becomes $x = a_{i_l} w$, which corresponds to the block C_1 and this block has no points with $x \in \Phi_S$.

Hence our block intersects C_0, C_1, C_{u+1}, but not C'_u, so property κ does not hold and the proof is complete. Q.E.D.

In the interest of future research we wish to point out to another configurational property that seems to distinguish the classical unitals from their Hughes counterparts.

It is known ([7]) that the classical unitals do not admit the so-called Pasch (or, as it has been known lately, O'Nan) configuration, which is defined as a family of four blocks each of which intersects the other three at three distinct points, and it is a long-standing conjecture that the lack thereof characterizes them.

We have carried out the actual construction of the classical Hughes unital on 28 points, and it does contain some Pasch configurations, reinforcing one's belief in the above conjecture. There are, however, pairs of intersecting blocks that are not embeddable in said configuration and we have not been able to discern an encouraging regular pattern. For this reason we had to resort to property κ for the nonisomorphism proof.

https://doi.org/10.4153/CJM-1990-057-1 Published online by Cambridge University Press

References

1. A. E. Brouwer, *Some unitals on 28 points and their embeddings in projective planes of order 9*, Lecture Notes in Mathematics 893, p. 183–188.
2. F. Buekenhout, *Existence of unitals in finite translation planes of order q^2 with a kernel of order q*, Geometriae Dedicata *5* (1976), p. 189–194.
3. P. Dembowski, *Finite Geometries*, Springer-Verlag N.Y., Inc., 1968.
4. M. J. Ganley, *A class of unitary block designs*, Math. Zeitschrift 128, p. 34–42 (1972).
5. D. R. Hughes, F. C. Piper, *Projective Planes*, Springer-Verlag, 1973.
6. R. Metz, *On a class of unitals*, Geometriae Dedicata *8* (1979), p. 125–126.
7. M. E. O'Nan, *Automorphisms of unitary block designs*, Journal of Algebra *20* (1972), p. 495–511.
8. F. C. Piper, *Polarities of finite projective planes*, Atti del Convegno di Geometria Combinatoria e sue Applicazioni (univ. degli studi di Perugia, Perugia) 1970, p. 373–376, Ist. Mat. Univ. Perugia, Perugia 1971.
9. T. G. Room, *Polarities and ovals in the Hughes plane*, J. Austr. Math. Soc. *13* (1972), p. 196–204.
10. L. A. Rosati, *I gruppi di collineazioni dei piani di Hughes*, Boll. Un. Mat. Ital. *13* (1958), p. 505–513.
11. L. A. Rosati, *Disegni unitari nei piani di Hughes*, Geometriae Dedicata *27* (1988), p. 295–299.

New York Institute of Technology
Wheatley Rd., Old Westbury
N.Y. 11568, U.S.A.