Europ. J. Combinatorics (1989) **10**, 297–308

Arcs and Ovals in the Hermitian and Ree Unitals

E. F. Assmus, Jr and J. D. Key

The hermitian unitals $\mathcal{U}(q)$ and the Ree unitals $\mathcal{RU}(q)$ are examined for the existence of ovals and arcs. It is shown that $\mathcal{U}(q)$ does not have ovals for $q > 2$ and that $\mathcal{RU}(q)$, like $\mathcal{U}(q)$, is embedded in a much larger design with block intersections of cardinality ≤ 2. Arcs of size $3q + 1$ are constructed for the Ree unitals $\mathcal{RU}(q)$; they are ovals only in the case $q = 3$. In this case, $\mathcal{U}(3)$ and $\mathcal{RU}(3)$ are embedded in the same design and its automorphism group, the symplectic group $Sp(6, 2)$, contains the automorphism groups of both the unitals; the coding-theoretic aspects are elucidated.

1. Introduction

For a 2-design $\mathcal{D}$, an arc, or s-arc, is a set $\mathcal{S}$ of s points of $\mathcal{D}$ which is such that no block of $\mathcal{D}$ meets $\mathcal{S}$ more than twice. The parameters of $\mathcal{D}$ determine an upper bound on the cardinality s of the arc, and when this bound is attained the arc is called an oval (see [1] or [2]). The existence of ovals in an even-order design can give useful information on the binary code generated by an incidence matrix of the design and, in certain cases, may determine the minimum weight of the code and its dual.

With the above connection in mind, we examine here the question of the existence of ovals in the hermitian and Ree unitals. For the hermitian unital $\mathcal{U}(q)$ with q odd, the non-existence of ovals has been proved by Andriamanalimanana [1]. Here we show that when q is even, only $\mathcal{U}(2)$ has ovals. For the Ree unital, $\mathcal{RU}(q)$, where $q = 3^{2n+1}$, the smallest, with $q = 3$, was previously shown to have ovals by determining the weight enumerator of the dual binary code (see Brouwer [3]). We show here how the ovals can be defined through the structure of the smallest Ree group, $R(3)$, and how this construction generalizes to the existence of $(3q + 1)$-arcs in $\mathcal{RU}(q)$ for all $q = 3^{2n+1}$. We were, however, unable to settle the general question of the existence of ovals in the Ree unitals for $q > 3$. For $q = 27$, computation showed that our $(3q + 1)$-arcs in $\mathcal{RU}(q)$ were complete, and thus not contained in ovals.

In the course of the construction of the $(3q + 1)$-arcs for $\mathcal{RU}(q)$, we obtain, as a byproduct, $(q + 1)$-arcs that form the blocks of a 2-design defined on the points of $\mathcal{RU}(q)$. This is analogous to a construction of Hölz [11], who showed that for the hermitian unital $\mathcal{U}(q)$, for q odd, a 2-$(q^3 + 1, q + 1, q + 1)$ design of arcs can be found, its union with the unital yielding a $2 - (q^3 + 1, q + 1, q + 2)$ design with the property that distinct blocks meet in at most two points. We show that designs with the same parameters and the same properties can be constructed for the Ree unitals.

These designs further highlight the special case $q = 3$: here the 2-$(28, 4, 5)$ designs from the hermitian and Ree unitals are isomorphic, and can be taken to be identical by taking for the blocks all the 4-sets in an orbit of the symplectic group $Sp(6, 2)$ acting on subsets of size 4 of a set of points of size 28. There is a unique orbit of size 315 in this action, and the unitary group $P\Gamma U(3, 3)$ and Ree group $R(3)$ $(= P\Gamma L(2, 8))$, acting inside $Sp(6, 2)$, each split this orbit into two orbits, one of size 63 and one of size 252. These orbits correspond to the blocks of the unital and the blocks of the design with $\lambda = 4$, respectively. The binary code for the design with $\lambda = 5$ is the same as the code for the hermitian unital, and its dual has the property of having only words of weight 0, 12, 16 and 28. We note here that Brouwer [3] discusses this code, and that Dillon [6] has pointed out an error in this discussion.

0195-6698/89/040297 + 12 $02.00/0

The arrangement of the paper is as follows: some basic notation and background material are given in Section 2; Section 3 deals with ovals in the hermitian unitals (Theorem A) and there, with the permission of the author, we reproduce the proof in [1] of the non-existence of ovals for odd-order unitals. In Section 4 we show how the $(3q+1)$-arcs are constructed in the Ree unitals (Theorem B) and how the $(q+1)$-arcs arise (Proposition 4.13): this section is rather long and somewhat complicated by our desire to give the proofs in terms both of the group-theoretical description of the Ree groups and unitals, and in terms of the geometric description of Tits [24]. In Section 5 we show how the related designs are defined (Theorem C) and in Section 6 we discuss the interesting case of $q=3$.

2. Preliminaries

We use standard notation: for geometries and designs as in [5] or [12]; for permutation groups as in [27]; and for coding theory as in [17].

For a 2-design $\mathcal{D}$ with parameters (v, k, λ), if r is the number of blocks through a point, then $r-\lambda$ is the order of the design. For $r-\lambda$ even and $\lambda \mid r$, the size of an oval is $(r+\lambda)/\lambda$; for $r-\lambda$ odd or $r-\lambda$ even and $\lambda \mid (r-1)$, the size of an oval is $(r+\lambda-1)/\lambda$ (see [1] or [2]).

An incidence matrix A for $\mathcal{D}$ is a $b \times v$ matrix of zeros and ones, such that $a_{i,j}=1$ if the ith block is incident with the jth point, and $a_{i,j}=0$ otherwise. Then for a non-trivial 2-design, A has rank v over the rational field, but A might possibly have smaller rank over a finite field $GF(p)$ when $p \mid (r-\lambda)$ (see [2] or [22]). We refer to the rank of A over $GF(p)$ as the p-rank of $\mathcal{D}$, and write $rk_p(\mathcal{D})$. This is also the dimension of C, the vector space spanned by the rows of A over $GF(p)$, so that C is a $(v, rk_p(\mathcal{D}))$ linear code. We write $C^{\perp}$ for the orthogonal to C with respect to the standard inner product. It is shown in [1] and [2] that if $\mathcal{D}$ is of even order, then the minimum weight of $C^{\perp}$ is at least $(r+\lambda)/\lambda$, with equality if $\mathcal{D}$ has ovals.

A unital or unitary design is a 2-design with parameters $2\text{-}(q^3+1, q+1, 1)$. It was shown by Kantor [15] that the only unitary designs with doubly-transitive automorphism groups are $\mathcal{U}(q)$, the design of absolute points and non-absolute lines of a unitary polarity of the projective plane $PG(2, q^2)$, where q is any prime power, and $\mathcal{R}\mathcal{U}(q)$, the Ree unitals defined by Lüneburg [16] from the Ree groups $R(q)$ for $q=3^{2n+1}$. Unitals have $r=q^2$ and order $(r-\lambda)=(q^2-1)=(q+1)(q-1)$. Mortimer [18] showed that for $\mathcal{D}=\mathcal{U}(q)$ or $\mathcal{R}\mathcal{U}(q)$, $rk_p(\mathcal{D})<q^3$ only for $p \mid (q+1)$.

3. The Hermitian Unitals $\mathcal{U}(q)$

The hermitian unital $\mathcal{U}(q)$ is the design of absolute points and non-absolute lines of a unitary polarity of the projective plane $PG(2, q^2)$, where q is any prime power (see [12] or [19] for further background). The order of the design $\mathcal{U}(q)$ is q^2-1, so for q odd the oval size is q^2+1, and for q even the oval size is q^2. Notice that in the ambient projective plane the oval size is q^2+1 for q odd, and q^2+2 for q even.

Andriamanalimanana [1] examined the question of the existence of ovals for even-order hermitian unitals, i.e. $\mathcal{U}(q)$ for q odd. For $q=3$ he obtained the weight enumerators for the codes C and $C^{\perp}$ over $GF(2)$ and showed that there are no words of weight 10 in $C^{\perp}$. This shows that there are no ovals in $\mathcal{U}(3)$. We give here his general proof of the non-existence of ovals in $\mathcal{U}(q)$ for $q>3$ and q odd.

The following classical result is used in the proof:

Lemma 3.1 ([23]). *For $n \geq 2$ let $f(x_1, \ldots, x_n)$ and $g(x_1, \ldots, x_n)$ be polynomials*

over $GF(q)$ of degrees k and m having no common factor. Then the number of common roots in $GF(q)^n$ is at most $q^{n-2}km\min\{k, m\}$.

PROPOSITION 3.1 ([1; *Prop.* 2.6, *p.* 37]). *If q is odd, $\mathcal{U}(q)$ has no ovals.*

PROOF. Firstly, for $q=3$, the weight enumerator of $C^{\perp}$ proves the result, as discussed above, but the result follows also from the observation that the existence of an oval would imply the simultaneous solutions in ten distinct points of $PG(2, 9)$ of a quartic and a quadratic, which is not possible (see [3]).

Let $q \geq 5$. The oval size for q odd is q^2+1, so an oval $\mathcal{S}$ in $\mathcal{U}(q)$ is also an oval for $PG(2, q^2)$. Hence, by Segre's theorem (see [5; §1.4, p. 49]), $\mathcal{S}$ is a conic and, taking homogeneous co-ordinates, the points of $\mathcal{S}$ satisfy an irreducible equation of degree 2. These points are also absolute points of a unitary polarity, and hence satisfy an equation of degree $q+1$. Using Lemma 3.1, the number of common solutions is at most $4q^2(q+1)$. Thus the number of points of $\mathcal{U}(q)$ on the conic is at most $(4q^2(q+1)-1)/(q^2-1)$. For $q \geq 5$ this number is less than q^2+1. Hence ovals do not exist in $\mathcal{U}(q)$ for q odd. □

Segre's result does not hold for even q and we must replace it by a geometric argument that turns on the completion of q^2-arcs in $PG(2, q^2)$.

PROPOSITION 3.2. *If q is even, $\mathcal{U}(q)$ has ovals only when $q=2$.*

PROOF. For q even, q^2-1 is odd, so the oval size is q^2. For $q=2$, $\mathcal{U}(2)$ is a 2-(9, 3, 1) design and is thus the unique design with these parameters, $AG(2, 3)$. In this affine plane quadrangles exist and are ovals for the design.

Now take $q \geq 4$, and suppose that $\mathcal{U}(q)$ has an oval S, i.e. a q^2-arc. Then $\mathcal{S}$ is a q^2-arc in $PG(2, q^2)$ and hence is contained in an oval, $\mathcal{A}$, of $PG(2, q^2)$, [10; §8.7.2, p. 197]. Thus $\mathcal{A} = \mathcal{S} \cup \{P, Q\}$, where P and Q are points of $PG(2, q^2)$ that are not in $\mathcal{U}(q)$, and hence are non-absolute points with respect to the unitary polarity, σ.

Since $\mathcal{A}$ is a (q^2+2)-arc in $PG(2, q^2)$ it can have no tangents. For $R \in \mathcal{S}$, R^{σ} is an absolute line, and contains R and no other absolute point. As it must meet $\mathcal{A}$ again, it can only meet it at P or Q. Thus $P \in R^{\sigma}$ or $Q \in R^{\sigma}$, so that $R \in P^{\sigma}$ or $R \in Q^{\sigma}$. Now P^{σ} and Q^{σ} are non-absolute lines since P and Q are non-absolute points, and hence they are blocks of the unital. Every point R of $\mathcal{S}$ is on one of P^{σ} or Q^{σ}, and thus if there are more than four points on $\mathcal{S}$, we must have at least three of them together on a block, contradicting the assumption that $\mathcal{S}$ is an oval. Thus $\mathcal{U}(q)$ has no ovals for $q \geq 4$. □

Propositions 3.1 and 3.2 yield, in summary, the following result:

THEOREM *A*. *The hermitian unital consisting of the absolute points and non-absolute lines of a unitary polarity of $PG(2, q^2)$ has no ovals for $q > 2$.*

REMARKS. (1) Theorem A states that, given any unitary polarity and any set of (q^2+1) absolute points of $PG(2, q^2)$ when q is odd, or q^2 absolute points when q is even, then at least three of the points of the set are collinear.

(2) Proposition 3.2 also follows from results of Fisher, Hirschfeld and Thas [9].

4. The Ree Unitals $\mathcal{RU}(q)$, $q = 3^{2n+1}$, $n \geq 0$

The Ree unitals $\mathcal{RU}(q)$ were defined by Lüneburg [16] via the Ree groups $R(q)$ from the basic properties of these groups as given in Ree [20] or Tits [24]. We give here the geometric construction of the groups $R(q)$ as given in Tits [24], and use this, and the basic properties of these groups as derived by Ward [25] or Ree [21], to construct the Ree unital $\mathcal{RU}(q)$, and to obtain the properties we require for the construction of the arcs.

Firstly, we present the construction of Tits [24]. Let $F = GF(q)$, where $q = 3^{2n+1}$, $n \geq 0$, and let $s = 3^{n+1}$. Then $s^2 = 3q$. Let G denote the Ree group $R(q)$, simple for $n > 0$, and isomorphic to $P\Gamma L(2, 8)$ for $n = 0$. Then G is represented as a doubly transitive permutation group of degree $q^3 + 1$. The point set on which G acts will be denoted by π, where $\pi = \{\infty\} \cup F^3$, ∞ is a symbol, and F^3 denotes the cartesian product of three copies of F, i.e. $F \times F \times F$. We write $N = G_\infty$, the stabilizer of the point ∞, and construct N as follows: N is a semi-direct product of groups P and $F^\times$, where P is a 3-group defined below via a binary operation '+' on the set F^3, and $F^\times$ is the multiplicative group of F, cyclic of order $q - 1$. Thus

$$N = \{(x, y, z; k) \mid x, y, z \in F, k \in F^\times\}$$

with multiplication given by

$$(x, y, z; k)(x', y', z'; k') = (x + kx', y + k^{s+1}y' + x^s kx', z + k^{s+2}z' - xk^{s+1}y' + ykx' - x^{s+1}kx'; kk').$$

In particular, the binary operation '+' in P is given by

$$(x, y, z) + (x', y', z') = (x + x', y + y' + x^s x', z + z' - xy' + yx' - x^{s+1}x')$$

and the action of $F^\times$ on P by

$$k(x, y, z) = (kx, k^{s+1}y, k^{s+2}z).$$

Then N simply acts on the points of π via this action keeping ∞ fixed: for $x, y, z, a, b, c \in F$, $k \in F^\times$, $(x, y, z; k)(a, b, c) = (x, y, z) + (ka, k^{s+1}b, k^{s+2}c)$, where we write the action on the left to be consistent with the notation in [24].

Thus far we have a transitive action of N on F^3, with P acting regularly. The members of F^3 and the elements of P are identified and we may also identify the elements $(x, y, z; 1)$ of N with (x, y, z) of F^3 or P. In order to obtain G we need to move the point ∞, and for this a new element, ω, is adjoined. This element is defined to interchange ∞ and $(0, 0, 0)$ and to act on any other point $(a, b, c) \neq (0, 0, 0)$ of F^3 as follows:

$$\omega((a, b, c)) = \left(\frac{u(a, b, c)}{w(a, b, c)}, \frac{v(a, b, c)}{w(a, b, c)}, \frac{c}{w(a, b, c)}\right),$$

where the functions u, v, w are defined by

$$u(a, b, c) = (ab)^s - c^s + ab^2 + bc - a^{2s+3},$$

$$v(a, b, c) = a^2 b - ac + b^s - a^{s+3},$$

$$w(a, b, c) = ac^s - a(ab)^s + a^{s+3}b + (ab)^2 - b^{s+1} - c^2 + a^{2s+4}.$$

Then ω is an involution. On adjoining ω to N, we obtain $G = \langle N, \omega \rangle = R(q)$, and G has the property that every $g \in G$ is either in N, and hence uniquely given in the form $(x, y, z; k)$, or is uniquely of the form

$$(x, y, z; 1)\omega(x', y', z'; k).$$

Note that all the above is described in [24], but there are some small errors in that paper that have been corrected by Tits, and communicated in the survey article of Enguehard [8]. We have also changed the notation slightly in the definition of ω.

Ward [25] derives important properties of $R(q)$, some of which we will need here. We note these properties below as Propositions 4.1–4.5, giving them also in the co-ordinate form of the geometric construction defined above.

The following notation will be used throughout this section:

$G = R(q)$, the Ree group of order $(q^3+1)q^3(q-1)$;

$P \in \mathrm{Syl}_3(G)$, the set of Sylow 3-subgroups of G;

$Z = Z(P)$, the centre of P;

$N = N_G(P)$, the normalizer of P in G;

$T = \{t \mid t \text{ an involution in } N\}$.

PROPOSITION 4.1. *The group P is nilpotent of class* 3 *and* $|P| = q^3$. *The derived group of* P, $[P, P] = P'$, is elementary abelian. *If* $q > 3$. *Then* $|P'| = q^2$ *and* $P' > Z$, *which is also elementary abelian, of order* q. *In this case every element* g *of* $P \backslash P'$ *has order* 9, *and* $Z = \{g^3 \mid g \in P\}$. *Further,* $N = PW$, *where* $W \cong C_{q-1}$, *the cyclic group of order* $q-1$. *If* $q = 3$, $P' = Z \cong C_3$ *and* N' *is cyclic of order* 9.

In terms of co-ordinates, $P = \{(x, y, z; 1) \mid x, y, z \in F\} \equiv \{(x, y, z) \mid x, y, z \in F\}$ *under* '+'; $g \in P$ *has order* 9 *if* $g = (x, y, z)$ *where* $x \neq 0$; *for* $q > 3$, $P' = \{(0, y, z) \mid y, z \in F\}$; $Z = Z(P) = \{0, 0, z) \mid z \in F\}$; $N = \{(x, y, z; k) \mid x, y, z \in F, k \in F\}$.

PROPOSITION 4.2. *If* t *is an involution in* G, *then* $C_G(t) \cong PSL(2, q) \times \langle t \rangle$. *If* $t \in T$ *then* $C_P(t) \cap Z = 1$ *and for* $q > 3$, $C_P(t) = C_{P'}(t)$, $P' = \bigcup_{t \in T} C_P(t) \cup Z$.

In terms of co-ordinates, $T = \{(x, -x^{s+1}, z; -1) \mid x, z \in F\}$. *Setting* $t_{x,z} = (x, -x^{s+1}, z', -1)$, $C_P(t_{x,z}) = \{(0, b, -xb) \mid b \in F\} = C_P(t_{x,z'})$ *for any* $z' \in F$; $C_P(t_{x,z}) \cap Z = \{(0, 0, 0)\}$.

PROPOSITION 4.3. *The group* G *has only one conjugacy class of involutions, each involution fixing precisely* $(q+1)$ *points, and the Sylow* 2*-subgroups of* G *are elementary abelian of order* 8.

In terms of co-ordinates, $\mathrm{Fix}(t_{x,z}) = \{\infty\} \cup \{(-x, b, xb - z - x^{s+2}) \mid b \in F\}$.

With these properties of G we can now define the Ree unital, following Lüneburg [16]. For the points of the unital we take the set of all Sylow 3-subgroups of G, with G acting by conjugation. This is equivalent to the action on the set π as described above, where $N = G_\infty = N_G(P) \equiv G_P$, the stabilizer of $P \in \mathrm{Syl}_3(G)$ under G by conjugation. Thus ∞ takes the role of P in this description. For the blocks of the unital we take the involutions of G, where the points incident with a block t will be the set of $(q+1)$ fixed points of the involution or, equivalently, the set of $(q+1)$ Sylow 3-subgroups that t normalizes. Thus P is on t if $P^t = P$, i.e. $t \in N_G(P) = G_P$. By conjugation, G is doubly transitive on points and transitive on blocks, with a block stabilizer equal to the centralizer of the corresponding involution.

PROPOSITION 4.4. *Let* $g \in G$, $g \neq 1$, *and suppose* $|\mathrm{Fix}(g)| \geq 3$. *Then* g *is an involution and* $\mathrm{Fix}(g)$ *is the set of points of a block.*

In terms of co-ordinates, let $g \in G$ *fix* ∞ *and* $Q = (0, 0, 0)$. *Then* $g \in G_{\infty,Q} = N_Q = \{(0, 0, 0; k) \mid k \in F^\times\}$, *and* $\mathrm{Fix}((0, 0, 0; k)) = \{Q, \infty\}$ *if* $k \neq -1$, *and* $\mathrm{Fix}((0, 0, 0;$

$-1)) = \mathrm{Fix}(t_{0,0})$. *Write* $\mathrm{Fix}(t_{x,z}) = l_{x,z} = \{(-x, b, xb - z - x^{s+2}) \mid b \in F\} \cup \{\infty\}$ *for the block through* ∞ *and the point* $(-x, 0, -z - x^{s+2})$.

PROPOSITION 4.5 *The group P acts regularly on* $\pi\backslash\{P\}$.

NOTES. (1) It is, of course, usual to write the action of a group by conjugation on the right, whereas, to be consistent with the notation in [24], we have written the co-ordinate action on the left. We will use the action of G on the right when speaking of G acting by conjugation on the set of Sylow 3-subgroups as points and the set of involutions as blocks, and we will use the action on the left when using the co-ordinate form. This should not cause confusion, as the two notations will never be mixed.
(2) The Ree unital $\mathcal{RU}(q)$ is the 2-$(q^3 + 1, q + 1, 1)$ design of point set π and block set $\mathcal{B}$, where $|\pi| = q^3 + 1$, $|\mathcal{B}| = q^2(q^2 - q + 1)$, and r, the number of blocks per point, is q^2. The point set π will be taken to be the set $\mathrm{Syl}_3(G)$ when not using the co-ordinate notation, and $\{\infty\} \cup F^3$ when using co-ordinates. The block set $\mathcal{B}$ corresponds to the set of all involutions, each involution identified by its set of fixed points.
(3) By restricting the field to $GF(3)$, we see that the smallest Ree unital $\mathcal{RU}(3)$ is embedded in $\mathcal{RU}(q)$ for any $q > 3$, with each block of $\mathcal{RU}(3)$ a subset of some block of $\mathcal{RU}(q)$.

We show now how the $(3q + 1)$-arcs are constructed, leading to ovals in the case $q = 3$. Where appropriate we illustrate the construction in terms of co-ordinates, taking P to be ∞, and using the notation as developed in this section. We will write (x, y, z), or $(x, y, z; 1)$ whenever convenient for the points of $\pi\backslash\{\infty\}$, corresponding to the elements of P. The construction will follow from Propositions 4.6–4.18 below.

We continue to use the notation already defined, with the following addition needed to define the arcs for each $P \in \pi$:

$$\Lambda(P) = \{\zeta \mid \zeta \text{ an orbit of } Z \text{ on } \pi\backslash\{P\}\}.$$

In co-ordinates, $\zeta = \{(x, y, z) \mid z \in F\} = \zeta(x, y)$, and we can index the q^2 members of $\Lambda(P)$ in this way, for $x, y \in F$. Thus $\Lambda(P) = \{\zeta(x, y) \mid x, y \in F\}$, $|\Lambda(P)| = q^2$, and $|\zeta(x, y)| = q$.

PROPOSITION 4.6. *For distinct* $P_1, P_2 \in \zeta \in \Lambda(P)$, P, P_1, P_2 *are not together on a block.*

PROOF. Suppose the block $t \in T$ contains P, P_1, P_2. Then as an involution of G, t fixes P, P_1 and P_2. Let $g \in Z$ be such that $P_1^g = P_2$. Then t^g fixes P, $P_1^g = P_2$, and hence $t^g = t$, since there is only one block through any two points. Thus $g \in C_P(t)$, contradicting (4.2).

In terms of co-ordinates, any two points of $\zeta = \zeta(x, y)$ have the form (x, y, z_1) and (x, y, z_2). By (4.4), the blocks $\ell_{x,z}$ through ∞ are indexed by the first and last co-ordinate, and hence cannot pass through two distinct points of the above form. □

PROPOSITION 4.7. *Let* ℓ *be a block not containing the point P. Then there is a unique involution in T that fixes* ℓ *(and has no fixed points on* ℓ*).*

PROOF. Let $t \in T$ be any involution in N. Then t has $(q + 1)$ fixed points, one of which is P, and $\frac{1}{2}q(q^2 - 1)$ transpositions. Each transposition corresponds to a block fixed by t, and such a block must consist entirely of transpositions occurring in t, since if an involution fixes a block, it fixes all or no points of that block. Each block fixed in

this way consists of $\frac{1}{2}(q+1)$ transpositions in t, and so t fixes $\frac{1}{2}(q^3-q)/\frac{1}{2}(q+1) = q(q-1)$ blocks in this way. These are the only blocks it fixes, apart from the block through P, all of whose points are fixed.

The number of blocks of the unital is $q^2(q^2-q+1)$, so that the number not through P is $q^3(q-1)$. We show now that no two involutions in T can fix the same block not through P. For let $g \in N_\ell$. Then g fixes the set of $q+1$ points of ℓ. If g fixed a point Q of ℓ, then $g \in N_Q \cong C_{q-1}$, and g fixes also the remaining $q-1$ points of the block through P and Q. Clearly, g cannot fix another point of ℓ, for no non-trivial element of G fixes a triangle pointwise. But $|g| \mid (q-1)$, and g acts semi-regularly on $\ell\backslash\{Q\}$, so that $|g| \mid q$. This is impossible, so g cannot fix any point Q of ℓ. Thus g acts semi-regularly on ℓ, and $|g| \mid (q+1)$. Also $|g| \mid |N| = q^3(q-1)$, and hence $|g| = 1$ or 2. Thus $|N_\ell| = 1$ or 2. If $|N_\ell| = 1$ for some ℓ, then $|\ell^N| = q^3(q-1) = |N|$, and hence all blocks not through P are in the orbit of ℓ under N. Thus no block is fixed by any non-trivial element of N_ℓ, which contradicts the conclusion that every involution fixes some blocks. Thus $|N_\ell| = 2$, ℓ is fixed by a unique involution, and the q^2 involutions in T fix $q^3(q-1)$ blocks not through P, i.e. every block not through P is fixed by a unique involution in T.

Further, since $|\ell^N| = \frac{1}{2}q^3(q-1)$, N partitions the blocks not through P into two orbits of equal length. Similarly, G_ℓ has two orbits of equal length on points not on ℓ. □

PROPOSITION 4.8. *If $z \in Z$, and $t \in T$, then $z^t = z^{-1}$ and zt, $tz \in T$.*

PROOF. Z is characteristic in P, hence normal in N, so that $t \in T$ induces an automorphism of Z, by conjugation. Since $z^t \neq z$ for any $z \neq 1$ in Z, by (4.2), t is a fixed-point-free automorphism of Z, and hence by Zassenhaus (see [13]), $z^t = z^{-1}$. Thus $(zt)^2 = (tz)^2 = 1$. □

PROPOSITION 4.9. *Let $Q \in \zeta \in \Lambda(P)$. If $\theta(\zeta) = \bigcup_{t\in T} \zeta^t$ and $Q^T = \{Q^t \mid t \in T\}$, then $\theta(\zeta) = Q^T$ and $|\theta(\zeta)| = q^2$.*

PROOF. Clearly, $Q^T \subseteq \theta(\zeta)$. Let $R \in \theta(\zeta)$. Then $R \in \zeta^t$ for some $t \in T$, so that $R = Q^{zt}$ for some $z \in Z$. By (4.8), $zt \in T$, so $R \in Q^T$, and $Q^T = \theta(\zeta)$.

To show that $|Q^T| = q^2$: suppose $Q^{t_1} = Q^{t_2} = Q_1$ for distinct t_1, $t_2 \in T$. Then the transposition (Q, Q_1) occurs in both t_1 and t_2, and hence the block through Q and Q_1 is fixed by two distinct involutions in N, in contradiction to (4.7). Thus $|Q^T| = q^2 = |\theta(\zeta)|$.

In co-ordinates, if $\zeta = \zeta(0,0) = \{(0,0,z) \mid z \in F\}$, and $Q = (0,0,0) \in \zeta$, then $\theta(\zeta) = \bigcup_{x\in F} \zeta(x, -x^{s+1})$, where $\zeta(x, -x^{s+1}) = t_{x,z}(\zeta)$. □

PROPOSITION 4.10. *If $R \in \theta(\zeta)$ and $Q \in \zeta$, then P, R, Q are not together on a block.*

PROOF. If $R \in \zeta$ then we have the proof from (4.6). So let $R = Q^t$, $t \in T$. If P, Q, R are on a block, there is an involution t_1 fixing P, Q, R, so that t_1^t fixes P and $Q^t = R$, whence $t_1^t = t_1$ and $t \in C_N(t_1)$, which contradicts t_1 being the only involution in $C_N(t_1)$. □

PROPOSITION 4.11. *Let $\zeta \in \Lambda(P)$, $\theta = \theta(\zeta)$ and $K = N_\theta$. Then for any $Q \in \zeta$, if $q > 3$, $K = ZN_Q$, and if $q = 3$, $K = N'N_Q$.*

PROOF. First we show that $K \geqslant N_Q$ for any $Q \in \zeta$. Thus let $g \in N_Q$ and let $t \in T$. Then $(Q^t)^g = Q^{gtg} = Q^{tg}$, and $t^g \in T$, so that g fixes $Q^T = \theta$. This holds for any $Q \in \zeta$.

Next we show that $Z \leq K$. Let $z \in Z$, $t \in T$. Then $(\zeta^t)^z = \zeta^{tz} = \zeta^{z^{-1}t} = \zeta^t$, by (4.8). Thus $Z \leq K$.

Now $Z \lhd N$, so $Z \lhd K$ and $Z \cap N_Q = 1$ implies that $|ZN_Q| = q(q-1)$ and $ZN_Q \leq K$. Let $M = ZN_Q$. Then $M_Q = N_Q$ (for $Q \in \zeta$) has order $q-1$, so the orbit of M containing Q in ζ has size q. If for some $P_1 \notin \zeta$ we have $M_{P_1} \neq 1$ then there is an element $g \in M_{P_1}$ with $g \notin Z$, so that $g \in N_{Q_1}$ for some $Q_1 \in \zeta$. Thus g fixes a triangle (by (4.10)) which is impossible. Thus $M_{P_1} = 1$ for all $P_1 \in \theta \backslash \zeta$, and M has one short orbit ζ, of length q, and one long orbit $\bigcup_{\zeta' \neq \zeta} \zeta'$ of length $q(q-1)$.

Suppose that $K \neq M$. Then K cannot fix ζ since the stabilizer of any point of ζ is as large as it can be inside N. Thus K is transitive on the q^2 point of θ, and $|K| = q^2(q-1)$. Hence $K \supseteq T$, Z and N_R for all $R \in \theta$. Let $L = \langle T, Z \rangle \leq K$. Then $L \lhd N$ and L is transitive on θ. So $q^2 \mid |L|$. Let $L^* = L \cap P$. Then $L^* \lhd P$ and $q^2 \mid |L^*|$. Now $L^* \cap C_P(t) = 1$ for all $t \in T$: for any $t \in T$ fixes θ, and hence will fix some Z-orbit ζ_1 inside θ. It will thus also fix a point Q_1 of ζ_1. Now, if $g \in L^* \cap C_P(t)$, then $t^g = t$, so g fixes the block corresponding to t, i.e. P, Q_1, Q_1^g will be together on a block. But (4.10) is now contradicted, since K is transitive on θ, so what was true for the orbit ζ is now true for any of the other orbits ζ^t. Thus $L^* C_P(t) \leq P$ and $|L^* C_P(t)| = q^3$, so $L^* C_P(t) = P$. Then $P/L^* \cong C_P(t)$ is abelian, so $L^* \geq P'$. For $q > 3$, $L^* = P'$ and for $q = 3$, $L^* > P'$. Thus for $q > 3$ we have a contradiction, since $C_P(t) = C_{P'}(t) > 1$. Hence for $q > 3$, $K = M = N_\theta = ZN_Q$.

For $q = 3$, $K = N'N_Q$ is of order 18 ($|\theta| = 9$ in this case), and K is transitive on θ.

In terms of co-ordinates, taking $\zeta = \zeta(0, 0) = \{(0, 0, z) \mid z \in F\}$; $\theta(\zeta) = \theta = \{(x, -x^{s+1}, z) \mid z \in F\}$; for $q > 3$, $N_\theta = \{(0, 0, z; k) \mid z \in F, k \in F^\times\}$; for $q = 3$, $N_\theta = \{(x, -x, z; k) \mid x, z \in F, k \in F^\times\}$, *i.e.* $|N_\theta| = 18$. □

PROPOSITION 4.12. *Let $\zeta \in \Lambda(P)$ and $\theta = \theta(\zeta)$. Then every block through P meets θ exactly once.*

PROOF. Let $P_1, P_2 \in \theta$. We need to show that the block P_1P_2 does not contain P. If $P_1, P_2 \in \zeta'$, or if P_1 or $P_2 \in \zeta$ then (4.6) and (4.10) prove it. So suppose $P_1, P_2 \in \theta \backslash \zeta$ and hence that there is $g \in N_\theta$ such that $P_1^g = P_2$. If P, P_1, P_2 are on a block then let t be the involution corresponding to this block, i.e. fixing P, P_1 and P_2. Then $t^g = t$, so that $g \in C_N(t)$. Now if $|g| = 3r$, then $g^r \in Z$ and $Z \cap C_N(t) = 1$, so $g^r = 1$. So $3 \nmid |g|$, and $g \notin Z$, so that $g \in N_R$ for some $R \in \zeta$ (since $N_\theta = Z \cup \bigcup_{R \in \zeta} (N_R \backslash \{1\})$). Thus g fixes P, R, the block PR and the block t. It cannot fix any point other than P on the block t, and neither can any of its non-identity powers, since the blocks PR and t are distinct (by (4.10)), and no non-identity element of G can fix a triangle pointwise. Hence $|g| \mid q$, which contradicts the above.

In terms of co-ordinates, $\theta = \{(x, -x^{s+1}, z) \mid x, z \in F\}$. The blocks through ∞ have the form $\ell_{a,c} = \{(-a, b, ab - c - a^{s+2}) \mid b \in F\} \cup \{\infty\}$, by (4.4). If $x = -a$ then $b = -x^{s+1}$ holds for only one value of b, so the block cannot intersect θ more than once. □

PROPOSITION 4.13. *Let ℓ be a block through the point Q, where $Q \in \zeta \in \Lambda(P)$. Then if $\theta = \theta(\zeta)$, ℓ meets $\theta \cup \{P\}$ exactly once again, and $\zeta \cup \{P\}$ is a $(q+1)$-arc.*

PROOF. If P is on ℓ then ℓ cannot meet θ again, by (4.12). Suppose $P \notin \ell$. By (4.7 there is a unique involution $t \in T$ that fixes ℓ, and fixes no point of ℓ. Thus every block through Q meets $\theta \cup \{P\}$ again. Now there are q^2 blocks through Q and each must meet $\theta \cup \{P\}$ again. Since $\theta \cup \{P\} \backslash \{Q\}$ has precisely q^2 points, every block meets $\theta \cup \{P\}$ exactly once again. Thus $\zeta \cup \{P\}$ is a $(q+1)$-arc. □

PROPOSITION 4.14. *The product of any two involutions in T is in P.*

PROOF. $N = PW$, where $P \lhd N$, $P \cap W = 1$ and $W \cong C_{q-1}$. Let t be the unique involution of W, and let $h \in T$. Then $h = gw$, where $g \in P$, $w \in W$, and $h^2 = gwgw = gg^{w^{-1}}w^2 = 1$, i.e. $w^2 = 1$, so that $w = t$. Thus every involution of N can be written in the form gt, where $g \in P$ and $gg^t = 1$, i.e. $g^{-1} = g^t$. Now let $t_1, t_2 \in T$. Then $t_1 = g_1 t$, $t_2 = g_2 t$, $t_1 t_2 = g_1 t g_2 t = g_1 g_2^{-1} \in P$, as required. □

PROPOSITION 4.15. *For $\zeta \in \Lambda(P)$, let $T_\zeta = \{t \mid t \in T, \zeta^t = \zeta\}$. Let $t_1 \in T \backslash T_\zeta$, $\zeta_1 = \zeta^{t_1}$. Then ζ_1^t is independent of $t \in T_\zeta$, and setting $\zeta_2 = \zeta_1^t$, we have $\zeta_2 \subset \theta(\zeta)$ and $\zeta_2^{t_1} = \zeta_2$.*

PROOF. For $q = 3$, N_θ is transitive on θ, and there are only three Z-orbits in the set θ, so the conclusion follows immediately. Thus let $q > 3$. Then $N_\zeta = N_\theta$. For N acts transitively on $\Lambda(P)$, so $|N| = |\Lambda(P)|\,|N_\zeta| = q^2\,|N_\zeta| = q^3(q-1)$. Thus $|N_\zeta| = q(q-1) = |N_\theta|$, and we know that $N_\theta \leqslant N_\zeta$ for $q > 3$, by (4.11).

Now since $t_1 \notin T_\zeta$, $\zeta_1 \neq \zeta$. Let $t, t^* \in T_\zeta$; then $\zeta_1^t = \zeta_1^{t^*}$ iff $(tt^*)^{t_1} \in N_\zeta$. Now $tt^* \in N_\zeta$, and, by (4.14), $tt^* \in P$, thus $tt^* \in Z$. Since $Z \lhd N$, $(tt^*)^{t_1} \in Z$, and hence $(tt^*)^{t_1} \in N_\zeta$. Thus ζ_1^t is invariant for all $t \in T_\zeta$. Since $T_\zeta \subset N_\theta$, $\zeta_1^t = \zeta_2 \subset \theta(\zeta)$ for any $t \in T_\zeta$. Also, $\zeta_2^{t_1} = \zeta_1^{tt_1} = \zeta^{t_1 t t_1}$, and hence $\zeta_2^{t_1} = \zeta_2$ iff $(t_1 t)^2 t_1 \in N_\zeta$, i.e. $(t_1 t)^3 \in N_\zeta$, (since $t \in N_\zeta$). But $t_1 t \in P$ by (4.14), and, by (4.1), $(t_1 t)^3 \in Z < N_\zeta$. □

We are finally ready to define the $(3q+1)$-arcs: with notation as in (4.15), let

$$\mathscr{A} = \{P\} \cup \zeta \cup \zeta_1 \cup \zeta_2.$$

We have then the following three results:

PROPOSITION 4.16. *The stabilizer $N_{\mathscr{A}} = \langle Z, t, t_1 \rangle$ for any $t \in T_\zeta$, $|N_{\mathscr{A}}| = 6q$, and $N_{\mathscr{A}}$ is transitive on $\zeta \cup \zeta_1 \cup \zeta_2$.*

PROOF. Clearly, Z fixes $\mathscr{A}$, and since $t: \zeta_1 \to \zeta_2$ and $t_1: \zeta \to \zeta_1$, $N_{\mathscr{A}}$ is transitive on $\zeta \cup \zeta_1 \cup \zeta_2$. Since $|N_{\mathscr{A},Q}| = 2$, and this is as large as possible here, $|N_{\mathscr{A}}| = 6q$.

In co-ordinates, let $\zeta = \{(0, 0, z) \mid z \in F\}$, $\zeta_1 = \{(a, -a^{s+1}, c) \mid c \in F\}$, $T_\zeta = \{t_{0,z} = (0, 0, z; -1) \mid z \in F\}$; $t_{0,z}((a, -a^{s+1}, c)) = (-a, -a^{s+1}, *)$, so $t_{0,z}(\zeta(a, -a^{s+1})) = \zeta(-a, -a^{s+1}) = \zeta_2$; $\mathscr{A} = \{\infty\} \cup \zeta(0, 0) \cup \zeta(a, -a^{s+1}) \cup \zeta(-a, -a^{s+1})$ for any $a \in F^\times$; $N_{\mathscr{A}} = \{(ma, -(ma)^{s+1}, z; k) \mid m \in GF(3), z \in F, k = \pm 1\}$. □

PROPOSITION 4.17. *The set $\mathscr{A}$ is a $(3q+1)$-arc.*

PROOF. By (4.13), any block through $Q \in \zeta$ will meet $\mathscr{A}$ at most once again. Since $N_{\mathscr{A}}$ is transitive on $\mathscr{A} \backslash \{P\}$, this property will hold also for blocks through points of ζ_1 or ζ_2. Also, by (4.12), any block through P will meet $\mathscr{A}$ at most once again, and hence $\mathscr{A}$ is a $(3q+1)$-arc. □

PROPOSITION 4.18. *For the arc $\mathscr{A}$, $G_{\mathscr{A}} = N_{\mathscr{A}}$.*

PROOF. If $G_{\mathscr{A}} \neq N_{\mathscr{A}}$ then $G_{\mathscr{A}}$ moves P, and is transitive on $\mathscr{A}$. Thus $(3q+1) \mid |G|$, i.e. $(3q+1) \mid (q^3+1)(q-1) = q^4 - q^3 + q - 1$. Suppose a prime p divides $(3q+1)$. Then $3q \equiv -1 (\mathrm{mod}\, p)$. Obviously, $p \neq 3$, so $q^4 - q^3 + q - 1 \equiv 0 \pmod p \Leftrightarrow (3q)^4 - 3(3q)^3 + 3^3(3q) - 3^4 \equiv 0 \pmod p$. Thus $p = 2$ or 13.

For $p = 2$, $2 \mid (3q+1)$ and $2 \mid (q^3+1)(q-1)$. If 2 is the only prime dividing $(3q+1)$ then $3q + 1 \leqslant 2^3$, since we know that 2^3 is the highest power of 2 dividing $|G|$ (by (4.3)). This is clearly impossible.

For $p = 13$, we have $q = 3^{2n+1}$, so $3q = 3^{2m}$, where $m = n + 1$. Then $9 \equiv -4 \pmod{13} \Rightarrow 3q = 3^{2m} \equiv (-4)^m \pmod{13}$. Now $(-4)^2 \equiv 16 \equiv 3$, $(-4)^3 \equiv -12 \equiv 1(13)$, so $(-4)^m \not\equiv -1 \pmod{13}$ for any m, i.e. $13 \nmid (3q + 1)$. □

For $q = 3$, $3q + 1 = q^2 + 1$, so that $\mathscr{A}$ is an oval for $\mathscr{RU}(3)$. For $q > 3$ we have shown by computation that when $q = 3^3$, the $(3q + 1)$-arcs are complete arcs. i.e. cannot have extra points added while retaining the property of being an arc. Also, for $q = 3^3$ and $q = 3^5$, we have shown by computation that θ is not an arc. Thus we are not hopeful of obtaining ovals for $\mathscr{RU}(q)$ for $q > 3$ in this way, should they exist at all.

To summarize, Propositions 4.1–4.18 give the following result:

THEOREM B. *Let $\mathscr{RU}(q)$ be the Ree unital, $G = R(q)$ the Ree group for $q = 3^{2n+1}$, $n \geq 0$. Let P be a Sylow 3-subgroup of G, N the normalizer of P in G, T the set of all involutions in N, Z the centre of P. Then for ζ any orbit of Z distinct from $\{P\}$, we have:*

(i) *$\zeta \cup \{P\}$ is a $(q + 1)$arc;*

(ii) *if $t, t_1 \in T$, $t \in N_\zeta$, $t_1 \notin N_\zeta$, then $\mathscr{A} = \{P\} \cup \zeta \cup \zeta^{t_1} \cup \zeta^{t_1 t}$ is a $(3q + 1)$-arc, and $|G_{\mathscr{A}}| = 6q$;*

(iii) *for $q = 3$, $\mathscr{A}$ is an oval for the design $\mathscr{RU}(3)$.*

5. Designs from Ree Unitals

For q odd, Hölz [11] constructed two classes, $\mathscr{U}_1(q)$ and $\mathscr{U}_2(q)$, of 2-designs from $\mathscr{U}(q)$ as follows. Let $\mathscr{U}(q)$ have point set π and block set $\mathscr{B}$; then $\mathscr{U}_1(q) = (\pi, \mathscr{B}_1)$ is a $2\text{-}(q^3 + 1, q + 1, q + 1)$ design with block set $\mathscr{B}_1$, where the blocks are $(q + 1)$-arcs in $\mathscr{U}(q)$ formed by taking the intersections of a certain class of Baer subplanes of $PG(2, q^2)$ with the point set π of $\mathscr{U}(q)$, and $\mathscr{U}_2(q) = (\pi, \mathscr{B} \cup \mathscr{B}_1)$ is the $2\text{-}(q^3 + 1, q + 1, q + 2)$ design formed by taking all the blocks of $\mathscr{U}(q)$ and $\mathscr{U}_1(q)$. Both $\mathscr{U}_1(q)$ and $\mathscr{U}_2(q)$ have the property that blocks meet in at most two points.

We obtain similar designs for the Ree unitals by using Z-orbits, together with $\{P\}$, for the $(q + 1)$-arcs.

THEOREM C. *Let $G = R(q)$ be the Ree group acting doubly transitively on the points of its unital $\mathscr{RU}(q) = (\pi, \mathscr{B})$. For each $P \in \pi$ (viewed as a Sylow 3-subgroup of G) let $\Lambda(P) = \{\zeta \mid \zeta$ an orbit of $Z(P)$ on $\pi \backslash \{P\}\}$ and set $\mathscr{B}_1 = \bigcup_{P \in \pi} \{\zeta \cup \{P\} \mid \zeta \in \Lambda(P)\}$. If $\mathscr{RU}_1(q) = (\pi, \mathscr{B}_1)$ and $\mathscr{RU}_2(q) = (\pi, \mathscr{B} \cup \mathscr{B}_1)$, then $\mathscr{RU}_1(q)$ is a $2\text{-}(q^3 + 1, q + 1, q + 1)$ design and $\mathscr{RU}_2(q)$ is a $2\text{-}(q^3 + 1, q + 1, q + 2)$ design with distinct blocks meeting in at most two points; G is an automorphism group of both designs.*

PROOF. Consider the structure $\mathscr{RU}_1(q)$: by the definition of $\mathscr{B}_1$, G is clearly transitive on blocks. Also,

$$|\mathscr{B}_1| = (q^3 + 1)q^2, \qquad \text{and} \qquad r = \frac{(q^3 + 1)q^2(q + 1)}{(q^3 + 1)} = q^2(q + 1).$$

Thus $\lambda = q + 1$. (The structure is clearly a 2-design since it has a 2-transitive group acting on it.) To show that blocks meet in at most two points, we show that the $\lambda = q + 1$ blocks through two given points do not meet again. By double transitivity, this will give the required result. We prove this using the co-ordinate form of the construction, with $P = \infty$ and $Q = (0, 0, 0)$, by forming the $(q + 1)$ blocks of $\mathscr{B}_1$ containing P and Q. Let $\zeta = \zeta(0, 0) = \{(0, 0, z) \mid z \in F\}$. Let $\mathscr{C} = \{\delta \mid \delta \in \mathscr{B}_1$ and $P, Q \in \delta\}$. Let $\delta_0 = \zeta \cup \{\infty\} \in \mathscr{C}$. Then $\omega(\delta_0) = \delta_1 = \{\infty\} \cup \{(0, 0, 0)\} \cup \{(z^{s-2}, 0, -z^{-1}) \mid z \in F^\times\}$, where ω is defined in Section 4. Thus $\delta_1 \in \mathscr{C}$.

Now $(1, 0, -1) \in \acute{o}_1$ so that $(0, 0, 0) \in (1, 0, -1)^{-1}(\acute{o}_1)$. From Section 4 we find $(1, 0, -1)^{-1} = (-1, 1, 1)$, so $\acute{o}_2 = (-1, 1, 1)(\acute{o}_1) = \{\infty\} \cup \{(-1, 1, 1)\} \cup \{(z^{s-2} - 1, -(z^{s-2}-1), 1 - z^{-1}) \mid z \in F^\times\}$. For $z = 1$ we obtain $(0, 0, 0) \in \acute{o}_2$, so $\acute{o}_2 \in \mathscr{C}$, and quite clearly $\acute{o}_2 \neq \acute{o}_0, \acute{o}_1$. For any $k \in F^\times$, let $k\acute{o}_2 = (0, 0, 0; k)(\acute{o}_2) = \{\infty\} \cup \{(-k, k^{s+1}, k^{s+2})\} \cup \{k(z^{s-2} - 1), -k^{s+1}(z^{s-2} - 1), k^{s+2}(1 - z^{-1}) \mid z \in F^\times\}$.

Then $k\acute{o}_2 \in \mathscr{C}$ for each $k \in F^\times$ (and for $k = 1$, $1\acute{o}_2 = \acute{o}_2$). We show that this is the full set $\mathscr{C}$, i.e. $\mathscr{C} = \{\acute{o}_0, \acute{o}_1\} \cup \{k\acute{o}_2 \mid k \in F^\times\}$ and that any two members of $\mathscr{C}$ meet only in ∞ and $(0, 0, 0)$. This is clear for $\acute{o}_0$ and $\acute{o}_1$, and $\acute{o}_0$ and $k\acute{o}_2$, since $z^{s-2} - 1 = 0$ only for $z = 1$: ths is because $s - 2$ is an automorphism, with $(z^{s-2})^{s+2} = z^{s^2-4} = z^{3q-4} = z^{-1}$, whence $z = 1$. For the same reason $\acute{o}_1$ and $k\acute{o}_2$ meet only in ∞ and $(0, 0, 0)$.

Suppose $k_1\acute{o}_2$ and $k_2\acute{o}_2$ have another point in common: then, since the ratio of the second co-ordinate to the first co-ordinate in $k\acute{o}_2$ is $-k^s$, we must have $-k_1^s = -k_2^s$, i.e. $k_1 = k_2$.

Thus blocks of $\mathscr{RU}_1(q)$ meet at most twice. For the same property in $\mathscr{RU}_2(q)$, we need only note that the blocks of $\mathscr{RU}_1(q)$ have been shown to be $(q + 1)$-arcs (see Proposition 4.13), and thus meet blocks of $\mathscr{RU}(q)$ at most twice. □

6. The Hermitian and Ree Unitals on 28 Points

The above considerations yield an interesting relationship between the two non-isomorphic 2–(28, 4, 1) designs, $\mathscr{U}(3)$ and $\mathscr{RU}(3)$. In fact, the extended designs given by Hölz for the hermitian unital, and in Section 5 for the Ree unital, are isomorphic with automorphism group the symplectic group $Sp(6, 2)$. This design is one of the elliptic quadric designs given by Theorem 3 in [7]. Here $Sp(6, 2)$, in its doubly-transitive action on 28 points, has exactly one orbit of length 315 in its induced action of the 4-subsets. With this orbit as the block set, we obtain the design with $d = m - 1$ and $m = 3$ of the class of designs found by Dillon and Wertheimer ([7] or [26]). From this orbit, the hermitian and Ree unitals (with $q = 3$) can be extracted group-theoretically.

The coding-theoretic aspects are interesting as well, and in describing them we correct an error made in the Note on p. 188 of [3]. Firstly, both $P\Gamma L(2, 8) = R(3)$ and $P\Gamma U(3, 3)$ are subgroups of $Sp(6, 2)$ and hence act on any code acted on by $Sp(6, 2)$, in particular on the binary code generated by the orbit of length 315 described above. Further, this code is the dual of the code mentioned in the Note of [3].

In more detail: let C be the binary code defined by $\mathscr{U}(3)$ in the usual way (see Section 2). Then C is a (28, 21) binary code, with minimum weight 4, and, in addition to the vectors given by the blocks of the unital, there are 252 further weight-4 vectors. These minimum-weight vectors give the design $\mathscr{D}$ of [7], with automorphism group $Sp(6, 2)$. This is also the design $\mathscr{U}_2(3)$ of Hölz, as described in Section 5.

The small Ree group $P\Gamma L(2, 8)$ also acts on $\mathscr{D}$, and the Ree unital $\mathscr{RU}(3)$ occurs as a subdesign of $\mathscr{D}$. If C_1 is the binary code of such a unital, then $C_1 < C$, and has dimension 19. Also $C = C_1 + C_1^\perp$, and $C^\perp = C_1 \cap C_1^\perp$, the latter code being the (28, 7) code with weight distribution $x^0 + 63(x^{12} + x^{16}) + x^{28}$ of the Note at the end of [3]. Since the all-one vector occurs in $C^\perp$, the 6-dimensional 2-modular representation of $Sp(6, 2)$ given by the quotient space will be the natural one for the symplectic group.

The question still remains, then, as to the uniqueness of a (28, 7) binary code with minimum weight 12, since the two given by the hermitian unital, $C^\perp$, and the Ree unital, $C_1 \cap C_1^\perp$, are isomorphic (in fact, identical, in the construction we have just described).

The embedding of $\mathscr{RU}(3)$ in the design $\mathscr{D}$ is the smallest case of a general embedding of certain Steiner systems with parameters 2–$(2^{m-1}(2^m - 1), 2^{m-1}, 1)$ in the

elliptic quadric designs described in [7] and acted on by $Sp(2m, 2)$. These designs are described in [4] or [14], for example, and for $m > 3$ have $1\frac{1}{2}$—but not 2-transitive automorphism groups. The Ree unital $\mathcal{RU}(3)$ may fit more naturally into this collection, as the smallest hermitian unital, $\mathcal{U}(2)$, fits naturally into the collection of affine planes.

ACKNOWLEDGEMENTS

We would like to thank A. R. Camina for drawing our attention to the designs dual to ovals of $PG(2, 2^m)$. We are also indebted to K. Mackenzie for her computations to obtain the weight enumerators for the codes of the extended designs. Finally, we would like to point out that the connection amongst these designs and their codes is known to Dillon and Wertheimer [6, 7].

Financial support from S.E.R.C., U.K. (E.F.A.) and the C.N.R., Italy (J.D.K.) is gratefully acknowledged.

REFERENCES

1. R. Andriamanalimanana, Ovals, unitals and codes, Ph.D. thesis, Lehigh University, 1979.
2. E. F. Assmus, Jr., The binary code arising from a 2-design with a nice collection of ovals, *IEEE, IT* **29** (1983), 367–369.
3. A. E. Brouwer, Some unitals on 28 points and their embeddings in projective planes of order 9, in *Geometries and Groups* (M. Aigner and D. Jungnickel, eds), Springer Lecture Notes No. 893, 1981, pp. 183–189.
4. F. Buekenhout, A. Delandtsheer and J. Doyen, Finite linear spaces with flag-transitive groups *J. Comb. Theory, Ser. A* **49** (1988), 268–293.
5. P. Dembowski, *Finite Geometries*, Springer, 1968.
6. J. F. Dillon, Private communication.
7. J. F. Dillon and M. A. Wertheimer, Graphs, codes, and designs in quadrics, *Congressus Numerantium* **55** (1986), 15–22.
8. M. Enguehard, Caractérisation des groupes de Ree, *Soc. Math. Fr. Astérisque* 142–143, (1986), 49–139.
9. J. C. Fisher, J. W. P. Hirschfeld and J. A. Thas, Complete arcs in planes of square order, *Ann. Discr. Math.* **30** (1986), 243–250.
10. J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford, 1979.
11. G. Hölz, Construction of designs which contain a unital, *Arch. Math.* **37** (1981), 179–183.
12. D. R. Hughes and F. C. Piper, *Design Theory*, Cambridge University Press, 1985.
13. Z. Janko and J. G. Thompson, On a class of finite simple groups of Ree, *J. Algebra* **4** (1966), 274–292.
14. W. M. Kantor, Plane geometries associated with certain 2-transitive groups, *J. Algebra* **37** (1975), 489–521.
15. W. M. Kantor, Homogeneous designs and geometric lattices, *J. Comb. Theory, Ser. A* **38** (1985), 66–74.
16. H. Lüneburg, Some remarks concerning the Ree groups of type (G_2), *J. Algebra* **3** (1966), 256–259.
17. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-correcting Codes*, North-Holland, 1983.
18. B. Mortimer, The modular permutation representations of the known doubly transitive groups, *Proc. Lond. Math. Soc.* (3) **41** (1980), 1–20.
19. M. E. O'Nan, Automorphisms of unitary block designs, *J. Algebra* **20** (1972), 495–511.
20. R. Ree, A family of simple groups associated with the simple Lie algebra of type (G_2), *Am. J. Math.* **83** (1961), 432–462.
21. R. Ree, Sur une famille de groupes de permutations doublement transitifs, *Can. J. Math.* **16** (1964), 797–820.
22. C. Salwach, Planes, biplanes and codes, *Am. Math. Monthly* **88** (1981), 106–125.
23. W. M. Schmidt, *Equations over Finite Fields*, Springer, 1976.
24. J. Tits, Les groupes simples de Suzuki et de Ree, *Séminaire Bourbaki 13* (1960/61), No. 210, 1–18.
25. H. N. Ward, On Ree's series of simple groups, *Trans. Am. Math. Soc.* **121** (1966), 62–89.
26. M. A. Wertheimer, Designs in quadrics, Ph.D. thesis, University of Pennsylvania, 1986.
27. H. Wielandt, *Finite Permutation Groups*, Academic Press, 1964.

Received 15 October 1987

E. F. ASSMUS, JR† AND J. D. KEY
Department of Mathematics, University of Birmingham, Birmingham B15 2TT, England

† Permanent address: Department of Mathematics, Lehigh University, Bethlehem, Pennsylvania 18015, U.S.A.