Spreads and Resolutions of Ree Unitals

Jeremy Dover*
Department of Mathematics
Moravian College, Bethlehem, PA 18018

1 Introduction

In [6], Lüneburg constructed a family of unitals ($2-(q^3+1, q+1, 1)$ designs) associated with the Ree groups of type G_2. His construction is as follows: the Ree group $R(q), q = 3^{2s-1}, s \in \mathbf{N}$ has a representation as a 2-transitive permutation group on q^3+1 symbols. These conditions on q and $R(q)$ hold throughout the paper. The stabilizer of any two symbols is cyclic of order $q-1$, and therefore admits only one proper involution. It can be shown that this involution fixes exactly $q+1$ points. Now, our points are the q^3+1 symbols on which $R(q)$ acts, and our blocks are defined to be the sets of $q+1$ points fixed by involutions described above. That this forms a unital follows directly from 2-transitivity. Brouwer [3] analyzed the Ree unital of order 3 quite thoroughly, discussing issues such as its embeddability in a projective plane of order 9, spreads and resolutions, and some aspects of its code.

For higher order Ree unitals, there are several known results. The family of Ree unitals is known to be disjoint from that of the Hermitian unitals, as the Ree unitals admit O'Nan configurations. (An O'Nan configuration is a set of four blocks such that each pair of blocks meet in a point, but no three blocks share a point.) Further, it is known that no Ree unital can be embedded in any projective plane. As designs, some small arcs have been constructed in the Ree unitals (see Assmus and Key [1]), and a good deal is known about the codes associated with them (see Assmus and Key [2] and Hiss [5]).

In this paper, we wish to generalize some of the results obtained by Brouwer concerning spreads and resolutions of the Ree unitals. In particular, we show that these designs are resolvable in at least q^3+1 ways.

We begin by recalling some of the classical results about the Ree groups. We then give a method for constructing spreads of these unitals. After

*This research has been partially supported by NSA Grant MDA904-94-H-2033.

analyzing some of the properties of these spreads, including automorphism groups and orbit structure, we give a construction for resolutions.

2 Some Useful Facts

In this section, we wish to recall some basic facts about the Ree groups. We present them as a series of lemmas; proofs can be obtained from Lüneburg [6]. Our first two results deal with 2-subgroups and involutions in $R(q)$.

Lemma 2.1 *The Sylow 2-subgroups of $R(q)$ are elementary Abelian of order 8. In particular, $R(q)$ has no elements of order 4.*

Lemma 2.2 *Every involution of $R(q)$ has exactly $q+1$ fixed points, and there is a one-to-one correspondence between the involutions of $R(q)$ and the blocks of the associated unital. Further, all involutions of $R(q)$ are conjugate.*

In light of this result, we can define the following terminology. If B is a block of the unital, then σ_B will denote the unique involution of $R(q)$ whose fixed set is B. Similarly, if τ is an involution in $R(q)$, we will denote the block fixed pointwise by τ B_τ.

Our next lemma deals with the interplay of the involutions and the blocks with which they are associated.

Lemma 2.3 *Let σ_B and σ_C be involutions in $R(q)$, associated with blocks B and C respectively. Then, the following conditions are equivalent:*

1. *σ_B and σ_C commute.*
2. *σ_B leaves C invariant.*
3. *σ_C leaves B invariant.*

Corollary 2.4 *Let σ_B be an involution in $R(q)$. Then, the subgroup of $R(q)$ which leaves block B invariant is exactly the centralizer of σ_B in $R(q)$.*

We end with a lemma which describes how the stabilizer of a block acts.

Lemma 2.5 *Let B be a block of the Ree unital of order q, and σ_B its associated involution. Then $C(\sigma_B)$ induces a group action G^* on B which is isomorphic to $PSL(2,q)$. The kernel of this action homomorphism is the subgroup generated by σ_B, and $C(\sigma_B)$ is isomorphic to the direct product $\langle\sigma_B\rangle \times PSL(2,q)$.*

3 Spreads

In a general design, a *spread* is a partition of the points into pairwise disjoint blocks. A necessary condition for this to occur is that the block size divide the number of points of the design. In the case of unitals, the block size is $q+1$, while the number of points is q^3+1. So in a unital, a spread is a set of q^2-q+1 pairwise disjoint blocks.

In his analysis of the Ree unital of order 3, Brouwer [3] found that it admitted 45 spreads. Using the software package MAGMA [4], we found that the 45 spreads broke up into two orbits: one of size 9, and the other of size 36.

As above, a spread of the Ree unital of order 3 is a set of seven pairwise disjoint blocks. It turns out that the two types of spreads can be distinguished by their automorphism groups. Spreads in the orbit of size 36 admit an automorphism group which cyclically permutes the blocks in the spread while the spreads in the orbit of size 9 do not.

In this section, we seek to generalize this second type of spread to Ree unitals of all orders. The other type of spread does not seem to generalize, at least not as a spread admitting a cyclic automorphism group.

Let $R(q)$, with $q = 3^{2s-1}$, $s \in \mathbf{N}$ be a Ree group, and let $U(q)$ be the unital associated with $R(q)$. Pick any block B of $U(q)$, and let σ_B be its associated involution. Pick any point P not in B. Then, since two distinct points determine a unique block, the block containing P and P^{σ_B} must be left invariant by σ_B. We wish to focus on the blocks left invariant by σ_B.

Lemma 3.1 *Let B be a block of $U(q)$, and let σ_B be its associated involution. Let C be a block which is left invariant by σ_B. Then, $B \cap C = \emptyset$.*

Proof: By way of contradiction, suppose $B \cap C \neq \emptyset$. Then, since two points determine a unique block, there exists a unique point x such that $x \in B \cap C$. Consider the action of σ_B on the block C. Since B is the fixed set of σ_B, the only fixed point of σ_B on C is x. Further, since σ_B is an involution which leaves C invariant, the remaining q points of C must be split up into orbits of size 2 under σ_B. But q is odd, which leads us to the desired contradiction. □

So, any block other than B left invariant by σ_B is necessarily disjoint from B. We now wish to show that any two blocks left invariant by σ_B are disjoint.

Lemma 3.2 *Let B be a block of $U(q)$, and let σ_B be its associated involution. Let C and D be two distinct blocks left invariant by σ_B. Then, $C \cap D = \emptyset$.*

Proof: By Lemma 3.1, the result is true if one of our blocks is B. So, assume neither C nor D is the block B. Again using Lemma 3.1, we know that $C \cap B = D \cap B = \emptyset$.

By way of contradiction, suppose $C \cap D \neq \emptyset$. Then, there exists a unique point x such that $x \in C \cap D$. Now, since C and D are both left invariant by σ_B, their intersection must also be left invariant. In particular, this implies x is fixed by σ_B. But, since $x \in C$, x cannot be an element of B. This is the desired contradiction, since the points fixed by σ_B are exactly those points in B. Therefore, C and D must be disjoint. □

With these two lemmas, we can now prove the existence of a spread in all Ree unitals.

Theorem 3.3 *The Ree unital of order q admits a spread.*

Proof: Let B be any block of the unital, and let σ_B be its associated involution. Let $\mathcal{S}$ be the set of all blocks left invariant by σ_B. By Lemmas 3.1 and 3.2, $\mathcal{S}$ is a set of pairwise disjoint blocks. To show that they form a spread, we need to show that these blocks cover the unital. Equivalently, we need to show that $|\mathcal{S}| = q^2 - q + 1$.

To do this, we count the number of blocks left invariant by σ_B. As mentioned above, the block containing the points P and P^{σ_B} is left invariant by σ_B for every P not in B. Clearly, any block left invariant by σ_B will have this form. One can easily count that there are $\frac{q^3-q}{2}$ distinct pairs of points of the form $\{P, P^{\sigma_B}\}$, each of which determines a block left invariant by σ_B. By Lemma 3.1, any such block is disjoint from B. So, each block left invariant by σ_B, except B, contains $\frac{q+1}{2}$ such pairs. Therefore, exactly $q^2 - q$ blocks, other than B, are left invariant by σ_B. Together with B, this means $|\mathcal{S}| = q^2 - q + 1$, and the theorem is proven. □

We will call the spread obtained in this manner S_B. In this construction, the block B seems to play a special role, as it is the only block of the spread fixed pointwise by σ_B. It turns out that in the order 3 case, there is nothing special about the line with which you start. Indeed for a given spread S of this form, any block in S will generate the spread. This yields the 9 spreads of one orbit. However, this turns out to be misleading. We would like to show that if $q > 3$ and S_B is a spread generated by block B, there is no other block of the unital which will generate S_B in this manner. We begin with a technical lemma which deals with the elements of $R(q)$ which induce involutions on a block B.

Lemma 3.4 *Let B be a block of $U(q)$. If $\tau \in R(q)$ is an element which induces an involution on B, then τ is an involution in $R(q)$.*

Proof: Let τ be any element which induces an involution on B. Then, τ^2 fixes B pointwise, which means either $\tau^2 = 1$ or $\tau^2 = \sigma_B$, as these are the

only two elements of $R(q)$ fixing B pointwise (See Lüneburg [6]). If $\tau^2 = 1$, then τ is an involution. If $\tau^2 = \sigma_B$, then $\tau^4 = 1$, which forces τ to have order 4. This contradicts Lemma 2.1, so no such τ can exist. Therefore, τ must be an involution of $R(q)$, and we are finished. □

Theorem 3.5 *Let σ be an involution in $R(q), q > 3$ which fixes block B_σ pointwise. Then, there exists no involution $\tau \in R(q)$ which fixes the same set of blocks as σ.*

Proof: By way of contradiction, suppose τ is an involution which fixes the same set of blocks as σ. In particular, this means τ fixes B_σ, so by Lemma 2.3, σ and τ commute. Let $\{B_\sigma, B_{\mu_1}, \ldots, B_{\mu_{q^2-q}}\}$ be the blocks left invariant by both σ and τ, where the μ_i's are the involutions associated with these blocks. Again using Lemma 2.3, we have that μ_i commutes with σ, and also commutes with τ for all $i \in \{1, \ldots, q^2 - q\}$. Further, since no other block can be left invariant by σ, and therefore τ, these are the only involutions which commute with σ, and therefore τ. (It should be noted that one of the μ_i's is τ, as B_τ is left invariant by σ.)

Summarizing, we have that each of the involutions $\mu_1, \ldots \mu_{q^2-q}$ commutes with each of σ and τ. Further, the set of involutions commuting with σ is $\{\sigma, \mu_1, \ldots, \mu_{q^2-q}\}$. This set is also the set of involutions commuting with τ. So, we have $\{\sigma, \mu_1, \ldots, \mu_{q^2-q}\} \subseteq C(\sigma) \cap C(\tau)$.

Now by Lemma 2.5, $C(\sigma)$ induces an action G^* on B_σ which is isomorphic to $PSL(2, q)$. Let θ be the homomorphism from $C(\sigma)$ onto G^*. Since $q > 3$, $PSL(2, q)$ is simple, and therefore G^* is generated by its involutions. Using the homomorphism θ, we obtain that $C(\sigma)$ is generated by all of the elements of $R(q)$ which induce involutions on B_σ, together with the kernel of θ. By Lemma 3.4, the only elements of $R(q)$ which induce involutions on B_σ are involutions of $R(q)$ which fix B_σ, and the kernel of θ is $\langle\sigma\rangle$, again using Lemma 2.5. Therefore, $C(\sigma)$ is generated by the set $\{\sigma, \mu_1, \ldots, \mu_{q^2-q}\}$.

But, $C(\tau)$ also contains all of these elements, and therefore $C(\sigma) \subseteq C(\tau)$. σ and τ are involutions of $R(q)$ and are conjugate by Lemma 2.2. Thus, $|C(\sigma)| = |C(\tau)|$, and this forces $C(\sigma) = C(\tau)$.

In particular, this means τ commutes with every element of $C(\sigma)$, and thus $\tau \in Z(C(\sigma))$. So, $Z(C(\sigma))$ has order at least 4, and contains $Ker(\theta)$. Therefore, the center of G^* is nontrivial. But, G^* is isomorphic to $PSL(2, q)$, which is simple. This is the desired contradiction. So, τ cannot have the same set of fixed blocks as σ. □

Corollary 3.6 *Let S_B be the spread generated as in Theorem 3.3 by block B, and S_C be the spread generated by block C, $C \neq B$. If $q > 3$, then $S_B \neq S_C$.*

This corollary implies that there is one spread of this form for each block of the unital, if $q > 3$. So, the Ree unital associated with $R(q), q > 3$ admits at least $q^2(q^2 - q + 1)$ distinct spreads. We can compute the subgroup of $R(q)$ which fixes the spread S_B as follows.

Theorem 3.7 *Let B be a block of $U(q)$, $q > 3$ and let σ_B be its associated involution. Then, the subgroup of $R(q)$ which leaves the spread S_B invariant is $C(\sigma_B)$.*

Proof: Let C be any block of the Ree unital, and let σ_C be its associated involution. If τ is any element of $R(q)$, then C^τ is a block with associated involution $\tau^{-1}\sigma_C\tau$.

Applying this to our situation, let $\tau \in R(q)$ be any group element which leaves our spread S_B invariant. Recall from Theorem 3.5 that every involution associated with a block of S_B lies in $C(\sigma_B)$. Since τ leaves S_B invariant, the conjugates $\tau^{-1}\mu\tau$ must lie in $C(\sigma_B)$ for all involutions μ in $C(\sigma_B)$. But, also from the proof of Theorem 3.5, we know $C(\sigma_B)$ is generated by its involutions. This implies that τ must normalize $C(\sigma_B)$. Clearly, any element of $N(C(\sigma_B))$ will leave our spread invariant, so we have that the subgroup of $R(q)$ leaving our spread invariant is $N(C(\sigma_B))$.

In the proof of Theorem 3.5, we showed that the only involution contained in the center of $C(\sigma_B)$ is σ_B. Let $\tau \in N(C(\sigma_B))$. Then, the center of $C(\sigma_B)$ is left invariant under conjugation by τ, so we have $\tau^{-1}\sigma_B\tau = \sigma_B$. This forces τ and σ_B to commute, which implies τ is actually in $C(\sigma_B)$. Therefore, $C(\sigma_B)$ is a self-normalizing subgroup, and we have that the subgroup of $R(q)$ leaving S_B invariant is $C(\sigma_B)$. □

Finally, we would like to compute the orbit structure of this stabilizer acting on our spread S_B. Recall that S_B consists of the blocks which are the fixed sets of involutions in $C(\sigma_B)$. From Lemma 2.5, we know that $C(\sigma_B)$ is isomorphic to the direct product $\langle\sigma_B\rangle \times PSL(2, q)$. In particular, this means that $C(\sigma_B)$ has a subgroup P isomorphic to $PSL(2, q)$. We wish to partition the involutions in $C(\sigma_B)$ into three parts:

1. $\mathcal{I}$, the set of involutions which lie in P,
2. $\mathcal{C}$, the set of involutions which are the product of σ_B with some involution in P, and
3. σ_B itself.

Theorem 3.8 *In the Ree unital of order q, with $q > 3$, let B be a block with associated involution σ_B. Then, the involutions of $C(\sigma_B)$ fall into three orbits under the inner automorphism group of $C(\sigma_B)$: $\mathcal{I}$, $\mathcal{C}$, and σ_B, using the notation above.*

Proof: First, we note that σ_B is certainly in its own orbit, since for all $\tau \in C(\sigma_B)$, we have $\tau^{-1}\sigma_B\tau = \sigma_B$. Further, we note that P is a subgroup of index 2 in $C(\sigma_B)$, and is thus normal. Therefore, the inner automorphism group of $C(\sigma_B)$ certainly leaves the sets $\mathcal{I}$ and $\mathcal{C}$ invariant.

It remains to show that our inner automorphism group is transitive on these two sets $\mathcal{I}$ and $\mathcal{C}$. However, all involutions in $PSL(2,q)$ are conjugate. In particular, this implies that $Inn(C(\sigma_B))$ is transitive on the involutions in $\mathcal{I}$, and so $\mathcal{I}$ is an orbit under $Inn(C(\sigma_B))$.

Finally, let $\sigma_B\mu_1$ and $\sigma_B\mu_2$ be two involutions in $\mathcal{C}$. Then, there exists $\tau \in C(\sigma_B)$ such that $\mu_2 = \tau^{-1}\mu_1\tau$. We can quickly compute that $\tau^{-1}\sigma_B\mu_1\tau = \sigma_B\tau^{-1}\mu_1\tau = \sigma_B\mu_2$. Therefore, $\sigma_B\mu_1$ and $\sigma_B\mu_2$ are conjugate. Since μ_1 and μ_2 were arbitrary elements of $\mathcal{C}$, we have that $\mathcal{C}$ is an orbit under $Inn(C(\sigma_B))$. □

Corollary 3.9 *The automorphism group of the spread S_B has three orbits on the S_B:*

1. *The blocks which are fixed sets of elements of $\mathcal{I}$,*
2. *The blocks which are fixed sets of elements of $\mathcal{C}$, and*
3. *B.*

Proof: Let C and D be two blocks of S_B, with associated involutions σ_C and σ_D. Then, there exists an automorphism of S_B which maps C onto D if an only if there exists an element $\tau \in C(\sigma_B)$ such that $\sigma_D = \tau^{-1}\sigma_C\tau$. The result then follows from Theorem 3.8. □

4 Resolutions

We now move on to the issue of resolvability. We can construct a large number of spreads by using the procedure in Theorem 3.3. We now would like to see if we can put some of them together to get a resolution.

Again, Brouwer [3] has fully analyzed the $U(3)$ case. He found that this unital is resolvable in 10 ways. Nine of these resolutions use the cyclic spreads which we have not generalized, but the other resolution uses only spreads of the type we have. It is this idea that we will use.

Theorem 4.1 *Let P be a point of the Ree unital of order q. For each of the q^2 blocks $\{B_1, \ldots, B_{q^2}\}$ containing P, construct the spread S_{B_i} as in Theorem 3.3. These q^2 spreads form a resolution of the Ree unital.*

Proof: We abbreviate S_{B_i} to S_i. To show that the spreads $\{S_1, \ldots S_{q^2}\}$ form a resolution, it suffices to show that no two of these spreads have a

block in common. Clearly, no two of these spreads share a block through P, by their construction. By way of contradiction, suppose that there is a block C which is contained in two of these spreads, say S_i and S_j. Let τ be the involution of $R(q)$ which fixes C pointwise, and let B_i be the block in S_i which contains P, and define B_j analogously. Since C is in S_i, by the definition of S_i, C is fixed by the involution σ_{B_i} associated with B_i. Therefore, by Lemma 2.3, τ must leave the block B_i invariant. Similarly, τ must leave B_j invariant. So, B_i and B_j are two blocks left invariant by τ. But by Lemma 3.2 we must have $B_i \cap B_j = \emptyset$. This is a contradiction since both of these blocks contain the point P. Therefore, the spreads $\{S_1, \ldots, S_{q^2}\}$ are pairwise disjoint, and form a resolution. □

As mentioned above, there is only one resolution of this type when $q = 3$. However if $q > 3$, one can easily obtain distinct resolutions.

Let P and Q be two distinct points of $U(q)$, $q > 3$. Let R_P and R_Q be the resolutions of $U(q)$ obtained by using Theorem 4.1 with points P and Q respectively.

We wish to show that these resolutions have exactly one spread in common. Indeed, suppose there exists a spread $\mathcal{S}$ of $U(q)$ which is contained in both R_P and R_Q. Then, by the construction of R_P, there exists a block B containing P such that $\mathcal{S} = S_B$, i.e. $\mathcal{S}$ is the spread obtained from Theorem 3.3 by beginning with block B. Similarly, there exists a block C containing Q such that $\mathcal{S} = S_C$. In particular, this implies $S_B = S_C$. By Corollary 3.6, this forces $B = C$ since $q > 3$. In other words, a spread can be contained in the resolutions R_P and R_Q if and only if it is generated by the unique block containing P and Q. Therefore, R_P and R_Q have only one spread in common, and thus cannot be equal. Since there are $q^3 + 1$ points in $U(q)$, this leads to $q^3 + 1$ distinct resolutions of $U(q)$.

Consider the resolutions we have constructed in Theorem 4.1 as points and the spreads constructed in Theorem 3.3 as blocks, with incidence given by reverse containment. We claim that this structure is a unital of order q. By the above, we have $q^3 + 1$ points, and any two distinct points lie on a unique block.

Let $\mathcal{S}$ be any block of this design, i.e. $\mathcal{S}$ is a spread. By our construction, $\mathcal{S} = S_B$ for some block B of $U(q)$. This spread will be in a resolution R if and only if the block B contains the point which generates R as in Theorem 4.1. Since B contains $q + 1$ points, the spread $\mathcal{S}$ is contained in $q+1$ resolutions of this type. In other words, every block of our new design contains exactly $q + 1$ points.

One can quickly check that this new unital is in fact isomorphic to the unital with which we started. However, it does give a new model for this $U(q)$, which might be useful.

5 Conclusion

While we have constructed a large number of spreads and resolutions in the Ree unitals, one natural question is if these are the only such objects. Certainly the answer is no in the order 3 case, but the examples there do not seem to generalize to the general case. This question remains open.

Another interesting question regards the O'Nan configurations contained in $U(q)$. In the order 3 case, it turns out (see Brouwer [3]) that every O'Nan configuration can be extended uniquely to a five-fold O'Nan configuration, i.e. a set of five blocks which pairwise meet in a point, but no three of which are concurrent. It would be interesting to see if this result extends to all Ree unitals.

Finally, there are many interesting questions involving the codes of the Ree unitals which can be asked. Due to the two-transitivity of the groups involved, these codes can be used to generate new designs which admit the Ree groups as automorphisms.

References

[1] E.F. Assmus, Jr. and J.D. Key, Arcs and ovals in the Hermitian and Ree unitals, *Europ. J. Combinatorics* **10** (1989), 297–308.

[2] E.F. Assmus, Jr. and J.D. Key, *Designs and their Codes* Cambridge University Press, 1992.

[3] A.E. Brouwer, Some unitals on 28 points and their embeddings in projective planes of order 9, In *Geometries and Groups*, volume 893 of *Lecture Notes in Mathematics*, pages 183–188. Springer-Verlag, New York/Berlin, 1981.

[4] J. Cannon and C. Playoust, An Introduction to MAGMA, University of Sydney, Sydney, 1993.

[5] G. Hiss, On the incidence matrix of the Ree unital, *Des. Codes Cryptogr.*, to appear.

[6] H. Lüneburg, Some remarks concerning the Ree groups of type (G_2), *J. Algebra* **3** (1966), 256–259.