Moore - Greig Designs I

Jarred T. Collins and Norman J. Finizio
Department of Mathematics
University of Rhode Island
Kingston, RI 02881
finizio@uriacc.uri.edu

Abstract

This is the first in a series of three papers in which we investigate a special class of designs that we designate as "Moore - Greig Designs". The sobriquet is associated with the fact that ideas gleaned from two constructions, one due to E. H. Moore (1896) and the other due to M. Greig (2003), are combined to produce designs that have remarkable properties and features. A Moore - Greig Design is an RBIBD that contains, simultaneously, nested RBIBDs, nested GWhDs, many GWhD$_a$s, frames, nested frames, GWhFrames, nested GWhFrames, GWh$_a$Frames, RRDFs and *nested* RRDFs. All of these designs are Z-cyclic. To be more precise, let p be a prime and let $\{s_i\}_{i=1}^{m}$ be a monotone increasing sequence of positive integers such that $s_i|s_{i+1}$ for all i, $1 \leq i \leq m-1$. Let n be a positive integer such that $s_m \leq n$ and $s_m|n$. A Moore - Greig Design is a Z-cyclic $(p^n, p^{s_m}, p^{s_m}-1)$-RBIBD that contains (1) a Z-cyclic $(p^n, p^{s_i}, p^{s_i}-1)$-RBIBD for each i, $1 \leq i \leq m-1$, (2) a Z-cyclic (p^{s_i}, p^{s_m}) GWhD(p^n) for each i, $1 \leq i \leq m-1$, (3) for each i, $1 \leq i \leq m-1$, a Z-cyclic (p^{s_i}, p^{s_m}) GWhD$_a(p^n)$, for each $a = \alpha/(p^{s_i}-1)$, $\alpha = 1, 2, \ldots, p^{s_i}-2$, (4) a Z-cyclic $\{p^{s_m}\}$ - frame of type $(p^{s_m}-1)^q$, $q = (p^n-1)/(p^{s_m}-1)$, (5) a Z-cyclic (p^{s_i}, p^{s_m}) GWhFrame of type $(p^{s_m}-1)^q$, for each i, $1 \leq i \leq m-1$, (6) a Z-cyclic $(p^n-1, p^{s_i}-1, p^{s_i}, 1)$-RRDF for each i, $1 \leq i \leq m$. Other than a single published example there is no literature pertaining to GWhD$_a$s. Therefore the infinite classes of GWhD$_a$s constructed from the Moore-Greig Designs are the first general results related to this type of design. It is also believed that many of the other designs contained within the infinite classes of Moore - Greig designs are new. In this paper, Part I, we provide detailed descriptions of both the Moore construction and the Greig construction. In the case of the Moore construction we supply proofs since such proofs are lacking in Moore's paper. Also included in this paper is a description of Moore-Greig Designs corresponding to $m = 2$ and a discussion is given of the presence of the GWhFrames, nested designs and the RRDFs. Our methods are such that the constructions are straightforward if one has the (associated) Galois Field.

JCMCC **56** (2006), pp. 123-137

In Part II we investigate the Moore - Greig Designs in their complete generality, that is to say, for arbitrary m and focus on the infinite classes of GWhD$_a$s that are obtainable from them. Also in Part II we provide an extensive listing of primitive polynomials. In Part III we investigate the RRDFs, "nested" RRDFs and the frames that can be constructed from the general Moore - Greig Designs of Part II.

keywords: Moore - Greig Designs, Generalized Whist Tournaments, Z-Cyclic Designs, Resolvable BIBDs, Z-Cyclic Frames, Z-Cyclic Resolvable Relative Difference Families, Nested RBIBDs, nested frames.

1 Introduction

Throughout this paper there will be considerable reference to the fact that certain designs are Z-cyclic. If a (v, k, λ)-BIBD is resolvable then to say it is Z-cyclic means that the elements are in $Z_{v-1} \cup \{\infty\}$ and that the resolution classes can be arranged in an order, say $R_1, R_2, \ldots$, such that R_{i+1} can be obtained from R_i by adding $+1$ (mod $v-1$) to every element in R_i with the rule $\infty + 1 = \infty$. If the BIBD is nearly resolvable then to say it is Z-cyclic means that the elements are in Z_v and the near resolution classes can be cyclically generated as in the resolvable case except that here the arithmetic is (mod v). A nice feature of Z-cyclic (N)RBIBDs is that one need only provide an initial resolution class, say R_1, and the remaining resolution classes are obtained by development of R_1 in the cyclic manner described. Let p be a prime and let n, s be positive integers such that $s|n$. In his classic paper "Tactical Memoranda I - III", E. H. Moore [17] presents a scheme that produces a collection of p^{n-s} base blocks, each of size p^s, whose elements are in $Z_{p^n-1} \cup \{\infty\}$. Moore remarks that the development of these blocks via the elements of Z_{p^n-1} leads to a (Z-cyclic) $(p^n, p^s, p^s - 1)$-RBIBD. Moore also remarks that this RBIBD possesses the feature that its first $q = (p^n - 1)/(p^s - 1)$ resolution classes form a Z-cyclic $(p^n, p^s, 1)$-RBIBD. Moore offers this scheme as an example, albeit abstract, of certain tactical configurations discussed in his paper (see (g) on page 274 in [17]). Moore's paper contains very few proofs. In particular he gives no proof of the above remarks. In the development of a proof it became clear that Moore's scheme not only leads to the claimed RBIBDs but also to other types of designs that are useful tools in the construction of additional designs. Thus it was discovered that, using Moore's scheme, one can build Z-cyclic resolvable relative difference families (RRDFs) and frames (these

designs are defined in Section 2). If one has appropriate input designs then the resolvable relative difference families can be used to produce Z-cyclic GWhFrames (defined in Section 2). A guarantee that appropriate input designs exist follows from a result due to M. Greig. This result, originally circulated as a private communication, is described as Greig's Log Table Method by I. Anderson [3], and appears, with proof, in [1]. The original goal of the present study was to obtain some new results related to GWhFrames. However, we found that applying a structure analogous to that employed in Greig's Log Table Method to Moore's designs enabled us to obtain designs that possess remarkable features. Because of the manner in which we came upon these designs we chose to refer to them as "Moore - Greig Designs". Each Moore - Greig Design is simultaneously many distinct designs and contains many additional designs such as frames, resolvable relative difference families, generalized whist tournament designs, GWhDs, and generalized whist tournament designs with parameter a, GWhD$_a$s. Both of these latter designs are defined below.There is virtually no literature pertaining to GWhD$_a$s except for their definition and a single example contained in [1]. Thus the infinite families of GWhD$_a$s that can be constructed from our methods are the first such. Obviously the validity of our results rely heavily on the validity of both Moore's construction and Greig's construction. Because of this reliance we provide detailed descriptions of these methods and give complete proofs of Moore's claims. Section 3 is devoted to Moore's construction and Section 4 is devoted to Greig's construction. In Section 5 a brief comparison of the two methods is given. In Section 2 we provide definitions and background materials that are useful for our investigations. In Section 8 resolvable relative difference families are discussed and it is shown how one can obtain such designs from Moore's construction. In Section 6 we generalize Greig's approach and apply this generalization to Moore's construction thereby obtaining the Moore - Greig Designs. This is done only for the case of two parameters, i.e., $m = 2$, where m is the upper index of the sequence $\{s_i\}_{i=1}^{m}$ that is mentioned in the abstract. A brief discussion of the nested designs obtainable from the materials of this study is contained in Section 10. In Part II, Moore-Greig Designs are constructed in their complete generality and infinite families of GWhD$_a$s are built from these designs. In Part III, RRDFs, frames, GWhFrames, GWh$_a$Frames and "nested" RRDFs are constructed from the general results of Part II. It is believed that many of our results represent new infinite families of the respective designs. For any specific case, if one wishes to make any of the constructions discussed here then one would begin with the construction of the appropriate Galois Field. For this purpose one needs, in general, to know an appropriate primitive polynomial. Thus in Part II we provide, as an appendix, a listing of some primitive polynomials. This listing is considerably more extensive than those found in [9, 13, 15].

2 Some Preliminary Materials

Let p be a prime and n be a positive integer. Both Moore's Construction and Greig's Construction begin with the Galois Field GF(p^n). There is extensive literature pertaining to the theory of Galois Fields and the following two theorems are among the most basic. We quote them here simply for the fact that they substantiate some of the approaches we employ. The proofs of these theorems can be found in [8].

Theorem 2.1 *Any two finite fields having the same order are isomorphic.*

Theorem 2.2 *Given a finite field F of order p^n then F has a subfield of order p^s if and only if s divides n.*

If one wishes to construct GF(p^n) for specific p and n then one needs to know a primitive polynomial, $\Sigma_{i=0}^{n} a_i\theta^i$, where θ is a primitive element for GF(p^n). If $x \in$ GF(p^n), $x \neq 0$ then its multiplicative representation is θ^i and the exponent i is called the index of x. The additive representation for x is the polynomial form $c_{n-1}\theta^{n-1} + c_{n-2}\theta^{n-2} + \ldots + c_1\theta + c_0$, where the coefficients c_i are elements in Z_p and are calculated via manipulation of the primitive polynomial. It is convenient to abbreviate this latter representation by an n-string consisting of the coefficients only, i.e. $c_{n-1}c_{n-2}\cdots c_1c_0$. Another standard theorem of algebra that we will have occasion to use is the following.

Theorem 2.3 *If G is a finite Abelian group of order g then G has at least one subgroup of order h for each h that divides g.*

Example 2.1 The Galois Field of order 3^2, having primitive polynomial $\theta^2 + \theta + 2$, consists of the following 9 elements: 0, θ^i, $i = 0, 1, \ldots, 7$. The respective (abbreviated) additive representations are 00, 01, 10, 21, 22, 02, 20, 12, 11. Note that GF(3^2) has four additive subgroups of order 3, namely $< 00, 01, 02 >$, $< 00, 10, 20 >$, $< 00, 21, 12 >$, and $< 00, 22, 11 >$. Only the first of these is closed under multiplication and is therefore a subfield of order 3. This subfield is isomorphic to GF(3) $= Z_3$ via the map $0h \rightarrow h$.

We now list the definitions of three combinatorial structures that are of interest to us, namely generalized whist tournament designs, resolvable relative difference families and frames.

Definition 2.1 *Let e, k, t, v be positive integers such that $v \equiv 0, 1 \pmod{k}$ and $k = et$. Let a be a positive rational number. A (t, k) generalized whist tournament design on v players, having parameter a, is a $(v, k, a(k-1))$-(N)RBIBD that satisfies the conditions indicated below. Each block of the BIBD is considered to be a game in which e teams of t players each compete*

simultaneously. Players on the same team are called partners and players in the same game but not on the same team are called opponents. For each pair of players, say $\{x, y\}$, x is to be a partner of y exactly $a(t-1)$ times and x is to be an opponent of y exactly $a(k-t)$ times. Such a design is denoted by (t, k) $GWhD_a(v)$. When $v \equiv 1 \pmod{k}$ consistency with the definition of a NRBIBD requires that a be an integer. When $v \equiv 0 \pmod{k}$, practical reasons require that each of $a(v-1)$, $a(k-1)$, $a(t-1)$ and $a(k-t)$ be an integer. When $a = 1$, all reference to the parameter a is suppressed.

This definition of generalized whist tournament designs appears in [1] but, to date, all of the literature pertaining to these designs deals only with the case $a = 1$. Of course if one can construct a (t, k) GWhD(v) then a (t, k) GWhD$_a(v)$ with a equal to a positive integer, say u, can be obtained by taking u copies of (t, k) GWhD(v). Thus the interesting situation is associated with fractional values for a. Clearly, if a is to be a fraction, the only permissable fractional values are those for which the denominator of a divides $\gcd(t-1, k-t)$. The conventional notation for a game in a generalized whist tournament design is to group teammates together and separate teams by semi-colons. Thus, for example, for $t = 2$ and $k = 6$ each game is written in the format $(a, b; c, d; e, f)$.

Definition 2.2 *Let G be an additive group of order v and let H denote a subgroup of G of order h. For a fixed positive integer k, a collection of k-subsets of G, $\mathcal{B} = \{B_1, B_2, \ldots, B_u\}$, is called a difference family over G relative to H if the list of differences of $\mathcal{B}$ covers every element in $G \setminus H$ exactly once and covers no element in H. Each subset B_i is called a base block of the difference family and k is called the block size. A difference family over G relative to H is said to be resolvable if the union of the base blocks constitutes a complete system of representatives for the nontrivial right (or left) cosets of H in G. A difference family over G relative to H that is also resolvable is typically denoted by $(G, H, k, 1)$-RRDF. It is also common notation to write $(v, h, k, 1)$-RRDF.*

Definition 2.3 *A frame is a group divisible design, $GDD_\lambda(X, \mathcal{G}, \mathcal{B})$ such that (1) the size of each block is the same, say k, (2) the block set can be partitioned into a family $\mathcal{F}$ of partial resolution classes and (3) each $F_i \in \mathcal{F}$ can be associated with a group $G_j \in \mathcal{G}$ so that F_i contains every point in $X \setminus G_j$ exactly once.*

The text by Furino et al. [12] is an excellent source of information pertaining to frames. If the blocks of a frame are of size k and if u_1 of the groups are of size g_1, u_2 of the groups are of size g_2, etc., u_m of the groups are of size g_m, then one refers to the frame as a $\{k\}$-frame of (group) type $g_1^{u_1} g_2^{u_2} \cdots g_m^{u_m}$. If the blocks of a frame possess any special properties then

it is common to have the notation for the frame reflect these properties. In particular a (t,k) GWh$_a$Frame is one for which the blocks can be partitioned into sub-blocks so that every pair of elements from distinct groups appear together in the same sub-block exactly $a(t-1)$ times and in the same block exactly $a(k-1)$ times. If $a=1$ then the notation is simply GWhFrame.

3 Moore's Scheme

Let p be a prime and let n,s be positive integers such that $s|n$. Let θ denote a primitive element in GF(p^n). Since GF(p^n) contains (up to isomorphism) precisely one subfield of order p^s, let H denote this subfield. Moore's scheme is as follows. Let H^+ denote the additive subgroup in H and denote by $\mathcal{B}$ the collection of p^{n-s} sets of size p^s consisting of H^+ and its $p^{n-s}-1$ additive cosets. Let $\mathcal{B}^*$ denote the collection of sets obtained from the sets of $\mathcal{B}$ by replacing each non-zero element by its index (relative to θ) and by replacing 0 by ∞. Moore's claim is that the sets in $\mathcal{B}^*$ are the base blocks of an initial resolution class of a (Z-cyclic) (p^n,p^s,p^s-1)-RBIBD and that the first $(p^n-1)/(p^s-1)$ resolution classes form a (Z-cyclic) $(p^n,p^s,1)$-RBIBD. We proceed now to prove these claims. It is important, for our purposes, that one knows the structure of H. Of course H contains 0 and an element, say z, that is of order p^s-1. There exists a unique positive integer j such that $z=\theta^j$ and therefore $(\theta^j)^{p^s-1}=1$. Consequently $j(p^s-1)$ must be a multiple of p^n-1 and, in turn, j must be a multiple of $q=(p^n-1)/(p^s-1)$. Of course, if $j=cq$ then c must be relatively prime to (p^s-1). There are then $\phi(p^s-1)$ choices for c, where ϕ is the Euler ϕ function. For convenience we choose $c=1$, since any other (appropriate) choice leads to the same subfield via Theorem 2.1. We conclude, then, that $H=\{0\}\cup\{\theta^{mq}: m=0,1,\ldots,p^s-2\}$. Let $a\in$GF(p^n) be such that $a\notin H$. Denote the coset $a+H^+$ by $C(a)$. Since $a\notin H$ there exist unique positive integers m and j such that $a=\theta^{mq+j}$, with $0\le m\le p^s-2$ and $0<j<q$. For each $g=1,2,\ldots,p^s-2$ set $b_g=\theta^{gq}a$. Of course, we can set $b_0=a$. Clearly $b_g\notin H$ for all g. Denote the coset b_g+H^+ by $C(b_g)$. In what follows all elements are considered to be represented in their additive format. For brevity and convenience we sometimes use the multiplicative symbolism to denote an additive element. Also, for convenience, we use division symbols and subtraction symbols to denote, respectively, multiplication by multiplicative inverse and addition by additive inverse.

Theorem 3.1 *If $g\neq f$ then $C(b_g)\cap C(b_f)=\emptyset$.*

Proof: Assume the contrary. Hence there exist elements $h_1, h_2 \in H^+$ such that $\theta^{gq}a + h_1 = \theta^{fq}a + h_2$. That is to say, $a(\theta^{gq} - \theta^{fq}) = h_2 - h_1$. Since H is closed under multiplication and addition, this latter statement indicates that $a \in H$, a contradiction. ∎

Thus the additive cosets of H^+, neglecting H^+ itself, can be partitioned into $y = (p^{n-s} - 1)/(p^s - 1)$ cells $C(a_1)$, $C(a_2)$, ..., $C(a_y)$ with $C(a_i) = \{C(a_i), C(\theta^q a_i), \ldots, C(\theta^{(p^s-2)q} a_i)\}$. Let $a \in \{a_1, a_2, \ldots, a_y\}$. Denote by $C^*(a)$ the set of indices of the elements in $C(a)$ and by $\mathcal{C}^*(a)$ the collection $\{C^*(a), \ldots, C^*(\theta^{(p^s-2)q}a)\}$. Certainly if $C^*(a) = \{i_1, i_2, \ldots, i_{p^s}\}$ then $C^*(\theta^{gq}a) = \{i_1 + gq, i_2 + gq, \ldots, i_{p^s} + gq\}$. It follows then that the set of differences arising from the elements in $C^*(a)$ is identical to the set of differences arising from the elements in the set $C^*(\theta^{gq}a)$ for each of $g = 1, 2, \ldots, p^s - 2$. Thus if d is a difference arising from the elements in $C^*(a)$ then, in the totality of differences, d occurs at least $p^s - 1$ times. It suffices to show that any such d occurs as a difference exactly $p^s - 1$ times.

Theorem 3.2 *Let $a \in \{a_1, a_2, \ldots, a_y\}$. No difference arising from the elements in the set $C^*(a)$ is a multiple of q.*

Proof: Suppose otherwise. Then there exist $h_1, h_2, h_3 \in H^+$ such that $h_1 \neq h_2$, $h_3 \neq 0, 1$ and $(a + h_1)/(a + h_2) = h_3$. It follows that $a(1 - h_3) = h_3h_2 - h_1$. Since H is a subfield and $h_3 \neq 1$, we conclude that $a \in H$, a contradiction. ∎

Theorem 3.3 *Let $a \in \{a_1, a_2, \ldots, a_y\}$. All differences arising from the elements in $C^*(a)$ are distinct.*

Proof: If the theorem is false, there exist $h_1, h_2, h_3, h_4 \in H^+$ such that $h_1 \neq h_2$, $h_3 \neq h_4$, $h_1 \neq h_3$, and $h_2 \neq h_4$ such that $(a + h_1)/(a + h_2) = (a + h_3)/(a + h_4)$. It follows that $a(h_1 + h_4 - h_2 - h_3) = h_2h_3 - h_1h_4$. Once again we arrive at the contradiction that $a \in H$, unless both $(h_1 + h_4 - h_2 - h_3) = 0$ and $(h_2h_3 - h_1h_4) = 0$. Now if these latter two equations were to hold then equating the two solutions for h_1 leads to the contradiction that $h_3 = h_4$. ∎

Theorem 3.4 *All differences arising from the elements in the sets $C^*(a_1), C^*(a_2), \ldots, C^*(a_y)$ are distinct.*

Proof: Assume the contrary. Let $a, b \in \{a_1, \ldots a_y\}$, $a \neq b$. There exist $h_1, h_2, h_3, h_4 \in H^+$ such that $h_1 \neq h_2$, $h_3 \neq h_4$ for which $(a + h_1)/(a + h_2) = (b + h_3)/(b + h_4)$. It follows that $a = bh_5 + h_6$ where $h_5 = (h_2 - h_1)/(h_4 - h_3)$ and $h_6 = (h_2h_3 - h_1h_4)/(h_4 - h_3)$. Since $h_5 \neq 0$ we have $h_5 = \theta^{gq}$ for some $g = 0, 1, \ldots, p^s - 2$. This allows us to conclude that $a \in C(\theta^{gq}b)$ which contradicts the manner in which the a_i were chosen. ∎

Each set $C^*(a_i)$ produces $p^s(p^s-1)$ differences. Therefore the totality of differences arising from the sets $C^*(a_1),\ldots,C^*(a_y)$ is $yp^s(p^s-1)=p^n-p^s$. The number of elements in $\mathrm{GF}(p^n)\setminus H$ is also p^n-p^s. Thus we have established the following theorem.

Theorem 3.5 *The differences arising from the sets $C^*(a_1),\ldots,C^*(a_y)$ cover the set $Z_{p^n-1}\setminus(\{0\}\cup\{gq : g=1,2,\ldots,p^s-2\})$ exactly once.*

We can now conclude that the totality of differences that arise from the sets in $C^*(a_1),\ldots,C^*(a_y)$ cover the set $Z_{p^n-1}\setminus(\{0\}\cup\{gq : g=1,2,\ldots,p^s-2\})$ exactly p^s-1 times. To complete the verification of the construction of the Z-cyclic RBIBD we need to investigate the set of differences arising from the elements in $H^*=\{\infty,0,q,2q,\ldots,(p^s-2)q\}$. Since $-gq$ is the index of the multiplicative inverse of θ^{gq} it easily follows that the totality of the differences of elements in H^* matches that of Z_{p^s-1}. Thus each multiple of q occurs as a difference exactly p^s-1 times.

The net result of the above discussion is that Moore's scheme does indeed produce an initial resolution class of a Z-cylic (p^n,p^s,p^s-1)-RBIBD in the case that $s|n$. Let $a\in\{a_1,\ldots,a_y\}$. For $b\in Z_{p^n-1}$ let $b+C^*(a)$ denote the collection of sets obtained by adding b modulo (p^n-1) to every element in every set in $C^*(a)$. It easily follows from the structure of the sets in $C(a)$ that $gq+C^*(a)=C^*(a)$, for all $g=0,1,\ldots,p^s-2$. Similarly $gq+H^*=H^*$. Thus the RBIBD consists of p^s-1 copies of a $(p^n,p^s,1)$-RBIBD. If the order of the elements in the blocks is unimportant then these latter RBIBDs are identical.

Example 3.1 Consider $\mathrm{GF}(3^4)$ with primitive polynomial $\theta^4+\theta+2$. Let $s=2$ then $q=10$ and $H=\{0000,0001,1121,2210,2211,0002,2212,1120,1122\}$. A set of coset representatives is $\{0010,0100,1000,0021,2100,0111,2001,1020\}$ with respective indices $1,2,3,4,6,8,12,18$. Note that $y=1$ therefore there is one basic coset, say $C(0010)$, and the others are of the form $C(\theta^{10g}(0010))$. Here, the order of an element in a block is not important one can list only the indices of the basic set, namely $C^*(0010)=\{1,53,78,49,36,44,37,55,22\}$ Consequently the (Z-cyclic) $(3^4,3^2,3^2-1)$-RBIBD is given by $\{\infty,0,10,20,$
$30,40,50,60,70\}$, $C^*(0010)+10g$, $g=0,1,2,\ldots,7$. It is an easy observation that the first 10 resolution classes form a (Z-cyclic) $(3^4,3^2,1)$-RBIBD.

Example 3.2 Consider $\mathrm{GF}(2^6)$ with primitive polynomial $\theta^6+\theta^4+\theta^3+\theta+1$. Let $s=3$ then $q=9$ and $H=\{000000,000001,110101,010111,110100,100001,100011,010110\}$. A set of coset representatives is $\{000010,000100,001000,010000,011011,101001,001110,\}$ with respective indices $1,2,3,4,6,12,21$. Note that $y=1$, hence there is one basic coset, say $C(000010)$, and

the others are of the form $C(\theta^{9g}(000010))$. Thus it suffices to list only the indices of the basic set, namely $C^*(000010) = \{1, 56, 8, 40, 7, 5, 30, 51\}$. Consequently the ($Z$-cyclic) $(2^6, 2^3, 2^3-1)$-RBIBD is given by $\{\infty, 0, 9, 18, 27, 36, 45, 54\}$, $C^*(000010) + 9g$, $g = 0, 1, 2, \ldots, 6$. Again, it easily follows that the first 9 resolution classes form a (Z-cyclic) $(2^6, 2^3, 1)$-RBIBD.

4 Greig's Log Table Method

Although the log table method of M. Greig has been reported elsewhere [1, 3] we choose to describe it again here. Our approach is to emphasize the algebra of the method thereby making the generalized whist design applications a bit more transparent. We first introduce some notation and terminology. Let p be a prime and let w and r be positive integers such that $w \leq r$. Unless otherwise indicated the elements of our Galois fields are to be represented in the (abbreviated) additive form. Thus if $a \in \mathrm{GF}(p^r)$ then $a = c_{r-1}c_{r-2}\cdots c_1c_0$. Consider the set $G = \{a \in \mathrm{GF}(p^r) : c_{r-1} = \cdots = c_w = 0\}$. Clearly G is an additive subgroup of $\mathrm{GF}(p^r)$ and G has order equal to p^w. We call G the Greig subgroup of order p^w in $\mathrm{GF}(p^r)$ and denote it by $G(p; w, r)$. The Greig subgroup is a clever choice because it allows for an easy interpretation as to why the associated Z-cyclic $(p^r, p^w, p^w - 1)$-RBIBD contains an appropriate $(p^r, p^m, p^m - 1)$-RBIBD for any $m < w$. It is this latter feature that prompts us to investigate the Greig method in some detail.

Define a p^{r-w} by p^w table as follows. Label the columns by the last w coefficients of the elements in $G(p; w, r)$ adopting the convention that the first column is labeled $00\cdots0$. Label the rows by the p^{r-w} possible structures for the first $r-w$ coefficients for an element in $\mathrm{GF}(p^r)$. Adopt the convention that the first row is labeled $00\cdots0$. The (i, j) entry in the table is the string of symbols obtained by adjoining the label of the j-th column to the end of the label of the i-th row. Clearly then the first row consists of the elements in $G(p; w, r)$ and the i-th row consists of the elements in the coset $a + G(p; w, r)$ where a is the element whose first $r - w$ coefficients are the label of the i-th row and whose last w coefficients are all 0. Denote this (coset) table as $CG(p; w, r)$. In $CG(p; w, r)$ replace 0 by ∞ and every other entry by its index. The resulting table, with the labeling of the columns as indicated below, is the so-called Greig Log Table. We will denote this table by the symbol $LG(p; w, r)$. If one treats each row of $LG(p; w, r)$ as the blocks of a design, it is proven in [1] that these blocks form the initial resolution class of a (Z-cyclic) $(p^r, p^w, p^w - 1)$-RBIBD. Suppose now that $m < w$. In $CG(p; w, r)$ rearrange the column labels into groupings of p^m columns in such a way that the labels in the first grouping are precisely the elements in the first row of $CG(p; m, w)$, the labels in the second grouping

are precisely the elements in the second row of $CG(p; m, w)$, etc. With this rearrangement it is clear that each row of $CG(p; w, r)$ is made of p^{w-m} sub-rows, each sub-row being a coset of $G(p; m, r)$. Thus the totality of sub-blocks in the corresponding (Z-cyclic) $(p^r, p^w, p^w - 1)$ are precisely the blocks of the initial resolution class of the (Z-cyclic) $(p^r, p^m, p^m - 1)$-RBIBD that would be obtained from $LG(p; m, r)$. It easily follows that Greig's Log Table Method produces a Z-cyclic (p^m, p^w) GWhD(p^r) for all positive integers $m < w \leq r$.

Example 4.1 Consider GF(2^4) with primitive polynomial $\theta^4+\theta+1$. There are three Greig subgroups, one of order 2 one of order 4 and one of order 8. Let us consider that we wish to construct the initial round of a Z-cyclic $(2^1, 2^3)$ GWhD(2^4)-RBIBD. The column labels for $CG(2; 3, 4)$ would be (in order) $000, 001, 010, 011, 100, 101, 110, 111$. Row 1 is labeled 0 and row 2 is labeled 1. The blocks of the corresponding GWhD are $(\infty, 0; 1, 4; 2, 8; 5, 10)$ and $(3, 14; 9, 7; 6, 13; 11, 12)$.

Example 4.2 Consider GF(3^2) as in Example 2.1. Our goal is to construct the initial round of a Z-cyclic $(3^1, 3^2)$ GWhD(3^2)-RBIBD. The column labels for $CG(3; 2, 2)$ would be (in order) $00, 01, 02, 10, 11, 12, 20, 21, 22$. Row 1 is labeled 0. There is only one block of the corresponding GWhD, namely, $(\infty, 0, 4; 1, 7, 6; 5, 2, 3)$.

5 Comparison of the two methods

Clearly both methods utilize a coset table of an additive subgroup in the Galois Field, GF(p^n). Moore demands that the additive subgroup be that of a subfield and Greig demands that the subgroup has a specific structure. Greig's approach, presumably motivated by generalized whist designs and/or nested RBIBDs, has considerable flexibility in that one only requires that $m < w \leq n$. One could allow $m = w$ but from the point of view of generalized whist designs this would mean that there is only one team competing in a game. This latter circumstance would lend itself to a more reasonable interpretation that each team consists of exactly one player. That is to say, $m = w$ is analogous to $m = 0$. Greig's structure is such that it is virtually self-evident that the resulting RBIBD possesses the generalized whist design requirements. Moore's approach is more restrictive since the demand is that $s|n$. The advantage, however, is that Moore's RBIBD contains several very useful designs such as RRDFs and frames. These latter designs are touched upon in Sections 8 and 9 and in greater detail in Part III of this three part series. In the next section we refine Moore's construction by incorporating Greig's approach.

6 Moore - Greig Designs

In this section we combine the ideas of Moore and Greig and obtain infinite classes of designs, the Moore - Greig Designs, that are quite fascinating. Here we restrict our attention to the sequence $\{s_i\}_{i=1}^{2}$ and leave the complete generality to Part II of this series. For convenience set $s_1 = u$ and $s_2 = s$. We require that u, s and n be positive integers such that $u < s \leq n$ and for which $u|s$ and $s|n$. Set $q' = (p^n - 1)/(p^u - 1)$, and $q = (p^n - 1)/(p^s - 1)$. Let $w = (p^s - 1)/(p^u - 1)$ and $r = (w - 1)/p^u = (p^{(s-u)} - 1)/(p^u - 1)$. Note that $w > 1$ and $q' = wq$. We induce an ordering in Moore's subfield of order p^s in such a way that the first p^u elements are the elements in Moore's subfield of order p^u and every grouping of p^u elements thereafter is a coset of the additive group associated with the subfield of order p^u. Given that this structure parallels Greig's scheme it is obvious from the results of Section 3 that the resulting $(p^n, p^s, p^s - 1)$-RBIBD will be such that its blocks can be broken into sub-blocks of size p^u and these sub-blocks will form an RBIBD having all of the features associated with the Moore construction. The $(p^n, p^s, p^s - 1)$-RBIBD formed as described above is called a *Moore - Greig Design* with parameters p, n, u, s and is denoted by MG$(p; n, s, u)$.

Example 6.1 Consider GF(3^4) as in Example 3.1 and take $u = 1$, $s = 2$. Note that $q' = 40$, $q = 10$, $w = 4$ and $r = 1$. In accordance with the Moore - Greig ordering H^+ is presented as $H^+ = \{0000, 0001, 0002, 1121, 1122, 1120, 2212, 2210, 2211\}$. The set of coset representatives is as in Example 3.1. In contrast to Example 3.1 the order in which elements occur in each block is important thus we present the entire initial resolution class of the MG$(3; 4, 2, 1)$ design here. We use semi-colons to emphasize the sub-blocks. Using symmetric differences [4] it is easy to show that these blocks form a $(81, 9, 8)$-RBIBD and that the sub-blocks form a $(81, 3, 2)$-RBIBD. That is to say, MG$(3; 4, 2, 1)$ is a $(3, 9)$ GWhD(81).

$(\infty, 0, 40; 10, 70, 60; 50, 20, 30)$ $(1, 53, 44; 78, 22, 55; 37, 49, 36)$
$(11, 32, 46; 63, 65, 47; 54, 8, 59)$ $(21, 75, 69; 42, 57, 64; 56, 73, 18)$
$(31, 67, 28; 5, 74, 66; 79, 52, 3)$ $(41, 4, 13; 77, 76, 9; 38, 15, 62)$
$(51, 6, 72; 14, 19, 48; 23, 7, 25)$ $(61, 29, 35; 16, 58, 33; 2, 24, 17)$
$(71, 68, 27; 39, 43, 12; 45, 26, 34)$.

7 GWhDs having parameter a

A major feature of Moore - Greig Designs, from our perspective, is that one can obtain infinite classes of GWhD$_a$s with $a \neq 1$. As mentioned earlier there is at present only one published example of these designs and that appears in [1]. In Part II of this study [10] we will develop Moore - Greig Designs in a general fashion thereby providing infinite classes of GWhD$_a$s.

We content ourselves here to point out that if one takes the first 40 rounds of the MG$(3;4,2,1)$ given in Example 6.1 one obtains a $(3,9)$ GWhD$_a(81)$ with $a = 1/2$.

8 Z-cyclic RRDFs

Relative difference families have been known and used for quite some time [9]. Referring to relative difference families as resolvable is a fairly new concept. The terminology begins with Buratti [5] and such difference families appear in [7] where they are refered to as 1-rotational difference families. Most of the literature concerning resolvable relative difference families is due to Buratti. Resolvable relative difference families can be found in the work of Hanani [16] and that of Greig [14] (although neither of them used this terminology) . As with any type of design, resolvable relative difference families have an intrinsic interest in their own right. On the other hand, RRDFs are powerful tools with which to build other designs as, for example, they can be used to construct frames (see Section 9 and also the materials in [11]). The fact that resolvable relative difference families can be used to construct frames was previously known [14]. It is not clear as to whether it is well known that combining resolvable relative difference families with other designs can produce frames that possess special properties [2, 6].

Clearly Theorem 3.5 establishes that $C^*(a_1), C^*(a_2), \ldots, C^*(a_y)$ are base blocks for a Z-cyclic $(p^n - 1, p^s - 1, p^s, 1)$-relative difference family (RRDF). Since $s|n$ it follows that $p^n - 1 = (p^s - 1)(p^{s(\mu-1)} + p^{s(\mu-2)} + \ldots + p^s + 1)$, where $\mu = n/s$. Our structure of the cells $C(a_1)$, $C(a_2)$, $\ldots$, $C(a_y)$ allows for easy discernment that this difference family is also resolvable with respect to the cosets $B_g = \{0, q, 2q, \ldots, (p^s - 2)q\} + g$, $g = 1, 2, \ldots, (q-1)$. That is to say, if $j \in C^*(a_i) \cup B_g$ then the remaining elements in B_g will be found, one each, in the sets $C^*(\theta^q a_i), C^*(\theta^{2q} a_i), \ldots C^*(\theta^{(p^s-2)q})$.

Example 8.1 The materials in Example 3.2 yield a Z-cyclic $(7 \cdot 9, 7, 8, 1)$-RRDF. This RRDF has but one base block, namely, $(1, 5, 7, 8, 30, 40, 51, 56)$.

Example 8.2 The materials in Example 6.1 enable us to give a Z-cyclic $(8 \cdot 10, 8, 9, 1)$-RRDF. This RRDF has but one base block, namely, $(1, 53, 44, 78, 22, 55, 37, 49, 36)$.

Example 8.3 In a manner that will be made precise in [11] one can also obtain a Z-cyclic $(2 \cdot 40, 2, 3, 1)$-RRDF from the materials in Example 6.1. This RRDF has 13 base blocks.

(10, 70, 60)	(1, 53, 44)	(78, 22, 55)	(37, 49, 36)
(11, 32, 46)	(63, 65, 47)	(54, 8, 59)	(21, 75, 69)
(42, 57, 64)	(56, 73, 18)	(31, 67, 28)	(5, 74, 66)
(79, 52, 3)			

9 Z-Cyclic Frames

As described in Section 2 if the blocks of a frame possess any specific property then it is commonplace to emphasize that property when referencing the frame. The interest here focuses on GWhFrames. For a GWhFrame the partial resolution classes will be called rounds of the frame.

Definition 9.1 *Suppose $S = Z_v$, $v = h\gamma$ and Z_v has a subgroup H of order h. Suppose a GWhFrame of type h^γ has a special round R_1, called the initial round, whose elements form a partition of $S \setminus H$ and is such that it, together with all the other rounds, can be arranged in a cyclic order, say $R_1, R_2, \ldots$ so that R_{j+1} can be obtained by adding $+1$ modulo v to every element in R_j. A frame with these properties is said to be Z-cyclic.*

Clearly the set $H^* \setminus \{\infty\}$ associated with Moore's construction is a subgroup of order $p^s - 1$ in the ring Z_{p^n-1}. It is also clear that removal of the block H^* from the initial round of Moore's (p^n, p^s, p^s-1)-RBIBD yields the initial round of a Z-cyclic frame of type $(p^s-1)^q$. If one removes the first block from the initial round of the MG$(3; 4, 2, 1)$ design of Example 6.1 one obtains the initial round of a $(3, 9)$ GWhFrame of type 8^{10}. The extraction of GWhFrames from Moore - Greig Designs will be discussed in more detail in [10, 11].

10 Nested Designs

It follows from the materials of Sections 4 and 6 that the designs discussed have sub-designs built into them. That is to say, there are designs nested within the (super) design. As will be shown in [10, 11] this nesting can go quite deeply into the (super) design. It is not too difficult to see that the Moore - Greig Designs contain nested frames and GWhFrames. It is also a fact, but perhaps not quite so obvious, that the Moore - Greig Designs contain "nested" RRDFs (as, for example, the $(2 \cdot 40, 2, 3, 1)$-RRDF of Example 8.3). Here again we leave the discussion of these features to Parts II and III of this study.

Acknowledgement. The authors wish to express their appreciation to the referee who, in addition to providing editorial improvements, indicated that appropriate field extensions, analogous to those found in [13], combined with Greig's Method produce designs with the structure that we have associated with Moore's Construction. Such an approach provides an additional, perhaps stronger, connection between the Moore and Greig Constructions.

References

[1] R.J.R. Abel, N.J. Finizio, M. Greig and S.J. Lewis, Generalized whist tournament designs, Discrete Math., 268(2003), 1–19.

[2] R.J.R. Abel, N.J. Finizio, G. Ge and B.J. Travers, Some new Z-cyclic $(2,6)$ GWhD(v), preprint.

[3] I. Anderson, Some Cyclic and 1 - Rotational Designs, in J.W.P. Hirschfeld (ed.), *Surveys in Combinatorics 2001*, London Math. Soc. Lecture Notes, Series 288, Cambridge University Press (2001), 47 – 73.

[4] I. Anderson, *Combinatorial Designs and Tournaments*, Oxford University Press, Oxford, 1997.

[5] M. Buratti, On resolvable difference families, Des. Codes Cryptogr. **11** (1997), 11–23.

[6] M. Buratti, N.J. Finizio, M. Greig and B.J. Travers, Z-cyclic $(t,8)$ GWhD(v), $t = 2,4$, Utilitas Math. (to appear).

[7] M. Buratti and F. Zuanni, G - Invariantly resolvable Steiner 2 - designs which are 1 - rotational over G, J. Combin. Des. **7** (1999), 406–425.

[8] R.D. Carmichael, *Introduction to the Theory of Groups of Finite Order*, Dover Publications, New York, N.Y., 1956.

[9] C.J. Colbourn and J.H. Dinitz, (eds.) *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, FL., 1996.

[10] J.T. Collins and N.J. Finizio, Moore - Greig Designs II, Cong. Numer. **173** (2005), 17–32.

[11] J.T. Collins, S. Costa and N.J. Finizio, Moore - Greig Designs III, Cong. Numer. **175** (2005), 203–221.

[12] S. Furino, Y. Miao and J. Yin, *Frames and Resolvable Designs: Uses, Constructions, and Existence*, CRC Press, Boca Raton, FL, 1996.

[13] D.H. Green and I.S. Taylor, Irreducible polynomials over composite Galois Fields and their application in coding techniques, Proc. Inst. Elec. Engr. **121** (1974), 935–939.

[14] M. Greig, Some group divisible design constructions, J. Combin. Math. Combin. Comput. **27** (1998), 33–52.

[15] M. Greig, Some BIBD constructions, J. Combin. Math. Combin. Comput. **27** (1998), 33–52.

[16] H. Hanani, Balanced incomplete block designs and related designs. Discrete Math. **11** (1975), 255–369.

[17] E.H. Moore, Tactical Memoranda I – III, Amer. J. Math. **18** (1896), 264–303.