

University of Richmond

UR Scholarship Repository

Honors Theses

Student Research

4-28-2005

Relative difference sets in 2-groups : a group cohomological viewpoint

Brian Wyman
University of Richmond

Follow this and additional works at: <https://scholarship.richmond.edu/honors-theses>



Part of the [Computer Sciences Commons](#), and the [Mathematics Commons](#)

Recommended Citation

Wyman, Brian, "Relative difference sets in 2-groups : a group cohomological viewpoint" (2005). *Honors Theses*. 472.

<https://scholarship.richmond.edu/honors-theses/472>

This Thesis is brought to you for free and open access by the Student Research at UR Scholarship Repository. It has been accepted for inclusion in Honors Theses by an authorized administrator of UR Scholarship Repository. For more information, please contact scholarshiprepository@richmond.edu.

UNIVERSITY OF RICHMOND LIBRARIES



3 3082 00937 3951

Math
Wym

*Relative difference sets in 2-groups:
A group cohomological viewpoint*

By

Brian Wyman

Honors Thesis

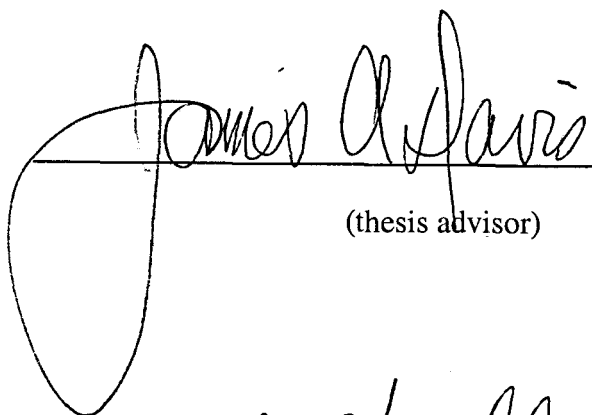
In

*Department of Mathematics and Computer Science
University of Richmond
Richmond, VA*

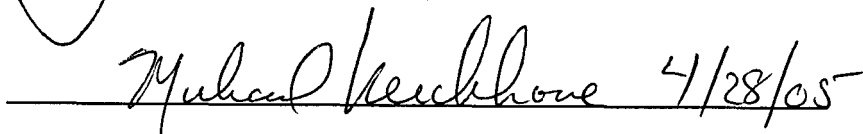
April 28, 2005

Advisor: Dr. James A. Davis

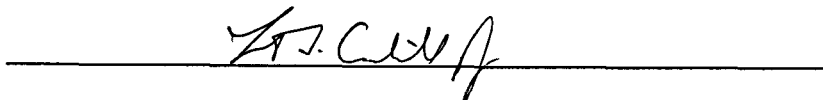
The signatures below, by the thesis advisor, a departmental reader, and the honors coordinator for mathematics, certify that this thesis, prepared by Brian Wyman, has been approved, as to style and content.

 James A. Davis 4/28/05

(thesis advisor)

 Michael Keckhove 4/28/05

(reader)

 F.S. Culp

(honors coordinator)

Relative difference sets in 2-groups: a group cohomological viewpoint

Brian Wyman
Advisor: Dr. James Davis
University of Richmond
brian.wyman@richmond.edu

April 28, 2005

Abstract

Relative difference sets (RDS) have been studied at great lengths in Abelian groups. RDSs in 2-groups have connections to constructions of divisible designs, which in turn are in correspondence with binary codes with good error correcting properties. In particular, a recent paper of Galati exhibited a $(4, 4, 4, 1)$ -RDS in a non-Abelian group relative to a normal but not central subgroup, the first known example of such an RDS. We study RDS with this anomaly as our motivation. In our investigations, we found that there is a correspondence between the existence of relative difference sets and the existence of short exact sequences of groups. We appeal to group cohomology to study these short exact sequences and to gain insight into the existence of these RDS.

1 Introduction

In a finite multiplicative group G of order $g = mn$, we call a k -element subset D a (m, n, k, λ) -relative difference set in G relative to a normal subgroup N of order n if the multiset of formal differences $DD^{-1} = \{d_1 d_2^{-1} : d_1, d_2 \in D\}$ contains each nonidentity element of $G \setminus N$ exactly λ times and intersects with N only in the identity. N is often referred to as the forbidden subgroup, as it is avoided by $DD^{-1} \setminus \{1\}$.

Example 1.1. In the group \mathbb{Z}_8 , the set $D = \{0, 1, 3\}$ is a $(4, 2, 3, 1)$ -RDS relative to the normal subgroup $\{0, 4\}$. The verification of this is a straightforward computation of differences. Note, however, that we would write this group additively and compute $DD^{-1} = \{d_1 - d_2 : d_1, d_2 \in D\}$.

Example 1.2. G is always itself a $(|G|, 1, |G|, |G|)$ -RDS relative to the trivial subgroup.

Relative difference sets are of interest to us because of their connections to geometry and coding theory. In particular, RDSs can be used to construct divisible designs and, in certain cases, projective planes. These combinatorial (and algebraic and geometric) constructs have deep ties to coding theory - they give rise to constructions of codes. Often, these codes have a large minimum distance (enabling them to correct large numbers of errors) because of the connection to geometry. Additionally, the associated geometry often is used to design efficient decoding algorithms. Thus, RDSs have an indirect practical application.

We consider the $\lambda = 1$ case for several reasons. First, it is in a sense the limiting case. That is, the existence of a (m, n, k, λ) -RDS in G relative to N guarantees the existence of a $(m, 1, k, \lambda n)$ -RDS in G/N . In general, if there is a $U \leq N \trianglelefteq G$ such that $U \trianglelefteq G$, then we can construct a $(m, \frac{n}{u}, k, u\lambda)$ -RDS in the factor group G/U . So, in some cases, we can construct RDS with larger λ from those with smaller λ . In addition, as λ gets larger, there is more known about these RDS, and there is relatively little known about RDS with $\lambda < \sqrt{m}$. The $\lambda = 1$ case is also associated to projective planes, which gives us a nice geometry connection. In these ways, it is natural for us to stick to the $\lambda = 1$ case.

This paper traces our year-long study of RDS. We began the year looking at Dembowski and Piper's theorem classifying projective planes with quasiregular collineation groups. We saw that one of the cases corresponded to a quasiregular collineation group with an associated $(2^\alpha, 2^\alpha, 2^\alpha, 1)$ -RDS. We then moved on to generalize this geometric idea in a more algebraic setting, semifields. While studying semifields and their connections to RDS, we also began reading a paper of Horadam and Perera. We were able to connect ideas from the two studies, noting that the cohomology approach of Horadam and Perera was in fact a generalization of the semifield case. After studying the methods and theorems of Horadam and Perera, we looked at an example of an RDS, due to Flannery, in a nonabelian group relative to a normal but not central subgroup. Horadam and Perera had only treated the case of central forbidden subgroups. This brought us to the end of our year, when we started to delve more deeply into the cohomology, studying the group extension problem for cyclic extensions.

2 The Beginning: Projective Planes, Collineation Groups, and Semifields

This section consists of two major parts. First we consider projective planes and collineation groups. We'll see that quasiregular collineation groups of projective planes correspond to RDS. Next we introduce semifields and their use in constructing projective planes. We can use the properties of a semifield to prove existence of an RDS in a group constructed on the set S^2 , where S is a semifield.

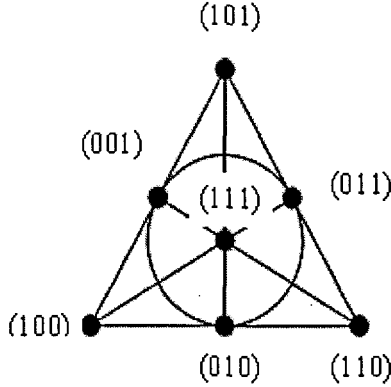


Figure 1: The Fano Plane can be constructed from \mathbb{Z}_2^3

2.1 Projective planes and quasiregular collineation groups

We begin with some basic definitions and examples.

Definition. A *projective plane* consists of a set of points, a set of lines, and an incidence relation determining when a point and line are incident, which satisfy:

1. there is exactly one line incident with each pair of points,
2. each pair of lines intersects in exactly one point, and
3. there exist four points, no three of which are collinear (avoids trivial case).

We will be dealing with finite projective planes. That is, our lines have a finite number of points. Therefore, it may be helpful to note that “points” and “lines” are not “points” and “lines” in the usual sense. Rather, points are any structure we so choose, and lines can be described as lists of the points that they contain.

Example 2.1. Take the points of our construct to be the one-dimensional subspaces of the vectorspace $V = \mathbb{Z}_2^3$. They are then $\langle(001)\rangle$, $\langle(010)\rangle$, $\langle(100)\rangle$, $\langle(011)\rangle$, $\langle(101)\rangle$, $\langle(110)\rangle$, $\langle(111)\rangle$. Lines are then the two-dimensional subspaces of V . That is, $L_1 = \{\langle(010)\rangle, \langle(100)\rangle\}$, $L_2 = \{\langle(011)\rangle, \langle(100)\rangle\}$, $L_3 = \{\langle(101)\rangle, \langle(100)\rangle\}$, $L_4 = \{\langle(011)\rangle, \langle(001)\rangle\}$, $L_5 = \{\langle(111)\rangle, \langle(101)\rangle\}$, $L_6 = \{\langle(011)\rangle, \langle(101)\rangle\}$, and $L_7 = \{\langle(111)\rangle, \langle(001)\rangle\}$. Figure 1 illustrates this configuration.

Notice that this design does, in fact, satisfy the conditions for it to be a projective plane. We can now talk about its collineation group.

Definition. A *collineation* is a permutation of the points of a projective plane sending lines to lines. A *collineation group* is a collection of collineations that forms a group under composition. The group is called *regular* if the group is sharply transitive on the points; that is, if given 2 points P and Q of the plane, there exists a unique collineation in the group that sends P to Q .

More generally, we can talk about automorphism groups of designs as groups of permutations of the points of the design that send blocks to blocks, with regularity of the group defined as the existence of a unique automorphism sending any point P to any other point Q . Regular automorphism groups of symmetric designs contain RDS relative to the trivial subgroup. These are not of particular interest to us, but the proof is simple and illustrates the general principle. For this, we need one more definition.

Definition. The *development* of an RDS is the set of translates of the RDS. That is, if $D \subseteq G$ is an RDS, then (written multiplicatively) $\{Dg = \{dg : d \in D\} : g \in G\}$ is the development of D .

Notice that each element of the development produces the same multiset of differences, and thus is an RDS in itself. This is trivial, as

$$(d_1g)(d_2g)^{-1} = (d_1g)(g^{-1}d_2^{-1}) = d_1d_2^{-1}.$$

This brings us to our first theorem.

Theorem 2.1. *The existence of a symmetric (g, k, λ) design with a regular automorphism group G is equivalent to the existence of a relative $(g = |G|, 1, k, \lambda)$ difference set in G relative to the identity subgroup.*

Proof. Given a group G with such a difference set D , the development of the RDS is the line set of the symmetric design, and the points are the group elements (in a symmetric design, any pair of points determines λ lines - a projective plane is a symmetric design with $\lambda = 1$). We claim that given any two group elements (points) g and h , there exist exactly λ blocks containing g and h . They are as follows. Consider the RDS. There are λ pairs of points with difference gh^{-1} . Choose one such pair $(a, b) \subseteq D$ so that $ab^{-1} = gh^{-1}$. Note that in any such pair, we can determine b uniquely by fixing a . Then the translate (line) $D(a^{-1}g)$ contains both

1. $a(a^{-1}g) = g$ and
2. $b(a^{-1}g) = (ba^{-1})g = (ab^{-1})^{-1}g = (gh^{-1})^{-1}g = (hg^{-1})g = h$.

Since $a^{-1}g$ is unique to our choice of a , our λ pairs of points sharing a difference give rise to λ different translates (now viewed as lines) of D containing both g and h . Thus we have a symmetric design. It is also clear that G acts regularly on this design by the group operation.

On the other hand, if we start with the symmetric design and regular automorphism group, then choose a point x in the design. Associate the point gx (remember the group acts on the design) with the group element g . Now we claim that any line of the design is a difference set in G . There are λ distinct lines containing any pair of points. Because the mapping is regular, we can treat each line as a translate of any other line. Choose two group elements g and h . Since λ lines contain both g and h , and since each line of the design is a different translate of a given line, we see that there are λ pairs of points

on each line whose difference is gh^{-1} as follows. Take the lines \mathcal{L}_i ($1 \leq i \leq \lambda$) containing g and h . Then for any line \mathcal{M} we can write $\mathcal{M} = \mathcal{L}_i a_i$ for distinct $a_i \in G$. The (distinct) elements $ga_i \in \mathcal{M}$ each have a corresponding $ha_i \in \mathcal{M}$ such that $ga_i(ha_i)^{-1} = gh^{-1} \in \mathcal{M}\mathcal{M}^{-1}$. Since each element of $G \setminus \{1\}$ appears λ times in $\mathcal{M}\mathcal{M}^{-1}$, we see that each line of the design is itself a (trivially relative) difference set. \square

Having an understanding of regular collineation groups, we can now move onto the so-called *quasiregular* collineation group acting on a projective plane.

Definition. A group Γ acts quasiregularly on a projective plane if for each $\gamma \in \Gamma$, p a point in the plane, and L a line in the plane:

1. $p\gamma = p$ implies that $x\gamma = x$ for all $x \in p\Gamma$, and
2. $L\gamma = L$ implies that $X\gamma = X$ for all $X \in L\Gamma$.

Therefore a quasiregular collineation group fixes either all or none of the points (resp. lines) in a given orbit.

For the simplest example of such a group, we look to the smallest example of a projective plane: the Fano plane. The following argument is described in [1]. In Figure 1, we indexed the points and lines as the one- and two-dimensional subspaces of the three-dimensional vectorspace over \mathbb{Z}_2 . Based on the classification of Dembowski and Piper, we select one point as “the point at infinity”. Similarly, we will choose one line (which must contain the point at infinity) to be “the line at infinity”. We will denote these by ∞ and L_∞ respectively, and we will let $\langle(001)\rangle = \infty$ and $L_7 = L_\infty$. The classification says that we should be looking for collineations that fix the special point at infinity and the line at infinity (though not necessarily the additional points on that line), and that the collineation should have 3 point orbits. Since there are 4 points in the projective plane that are not on L_∞ , there should be 4 elements of our group. That is, we are looking for 4 collineations. Because the mappings are collineations (taking lines to lines) and because we must fix the line and point at infinity, it turns out that the image of any point off of L_∞ , say $\langle(100)\rangle$, determines the entire mapping as follows:

1. $\langle(100)\rangle \mapsto \langle(100)\rangle$. This is the identity mapping, where each point and line maps to itself. We denote this mapping I .
2. $\langle(100)\rangle \mapsto \langle(101)\rangle$. We see that $\langle(101)\rangle \mapsto \langle(100)\rangle$, since ∞ must be fixed and lines must map to lines. Then since we want the collineation to be quasiregular, it can't fix anything in this point orbit (since there's already something that's not fixed). Hence $\langle(010)\rangle$ and $\langle(011)\rangle$ map to each other. All the points on L_∞ are fixed, and this is our entire map. We call it ϕ_1 .
3. $\langle(100)\rangle \mapsto \langle(011)\rangle$. By fixing ∞ , we see that $\langle(101)\rangle \mapsto \langle(010)\rangle$. To get 3 point orbits, we must send $\langle(010)\rangle \mapsto \langle(100)\rangle$ and $\langle(011)\rangle \mapsto \langle(101)\rangle$. This swaps the two non- ∞ points on L_∞ , and we call this map ϕ_2 .

4. $\langle\langle 100 \rangle\rangle \mapsto \langle\langle 010 \rangle\rangle$. This map takes $\langle\langle 100 \rangle\rangle \mapsto \langle\langle 010 \rangle\rangle \mapsto \langle\langle 101 \rangle\rangle \mapsto \langle\langle 011 \rangle\rangle \mapsto \langle\langle 100 \rangle\rangle$. As above, this map swaps the two non- ∞ points on L_∞ . We call this ϕ_3 .

Under composition, it is clear that ϕ_3 does not square to the identity. Hence this group must be isomorphic to \mathbb{Z}_4 . Indeed, the set $\{I, \phi_1\}$ in this group is a $(2, 2, 2, 1)$ -RDS relative to $\{I, \phi_1\}$, the normal subgroup generated by the element ϕ_1 of order 2. Looking, then, at \mathbb{Z}_4 , we see (as we expect) that the set $\{0, 1\}$ is a $(2, 2, 2, 1)$ -RDS relative to the normal subgroup $\{0, 2\}$. In fact, we can do this in general. If we take a point from the large point orbit, say $p = \langle\langle 100 \rangle\rangle$, and a line from the large line orbit, say L_2 , and we define the set $D = \{g \in G : p^g \in L_2\} = \{I, \phi_2\}$, we can see that D is a $(2, 2, 2, 1)$ -RDS relative to the normal subgroup $\langle\phi_1\rangle$. It's clear that this process works in this case, but it also works in general. Take a point from the large point orbit and a line from the large line orbit, and we can construct our RDS D as above [1].

Conversely, we can always construct a projective plane from a group G with a $(2^a, 2^a, 2^a, 1)$ -RDS. There are 2^{2^a} translates of the RDS, and 2^a cosets of the forbidden subgroup, which we treat as lines. Treating the group elements as points, we get a structure with 2^{2^a} points and $2^{2^a} + 2^a$ lines. Nonparallel lines intersect in one point. This is an affine plane of order 2^a . We can extend this by adding a point at infinity for each parallel class of lines (2^a of these come from translates of the RDS, and 1 of these comes from the set of cosets). We'd like any 2 of these points to determine a line as well, so we add a line at infinity containing all of the points at infinity. This new structure has $2^{2^a} + 2^a + 1$ lines on as many points. Nonparallel lines intersect in one point as follows. Each translate of the RDS contains at most 1 element from each coset of the forbidden subgroup, since differences of elements in the same coset are in the forbidden subgroup. Moreover, there are 2^a cosets of the forbidden subgroup and 2^a elements of each translate of the RDS, so each translate must contain exactly 1 element from each coset. In other words, RDS translates and cosets (viewed as lines) intersect in exactly one point. Cosets are parallel to each other, as they do not share elements. Distinct translates of an RDS intersect in at most one point as well. Take, for instance, an RDS $D = \{d_1, d_2, \dots, d_{2^a}\}$ and a translate Da . If $|D \cap Da| > 1$, then there exist $d_i, d_j \in D$ such that $d_i a = d_k$ and $d_j a = d_l$ for some $(k, l) \neq (i, j)$. But then $d_k d_l^{-1} = (d_i a)(d_j a)^{-1} = d_i d_j^{-1}$, which contradicts $\lambda = 1$.

Thus the constructed set is a projective plane. This plane has a quasiregular collineation group associated with it, defined by translation by G on the affine plane (points of which are indexed by elements of G).

We summarize these results with a theorem.

Theorem 2.2. *There exists a $(2^a, 2^a, 2^a, 1)$ -RDS in a group G of order 2^{2^a} if and only if G is a quasiregular collineation group with 3 point orbits of a projective plane of order 2^a .*

2.2 Semifields

In some cases, as above, the geometry can help us to construct an RDS. There is a more general method for constructing these projective planes which involves an algebraic construct known as a semifield.

Definition. A *semifield* is a set S along with two binary operations, $+$ and \cdot , such that

1. $(S, +)$ is an abelian group with identity 0.
2. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in S$.
3. There is a multiplicative identity 1.
4. There are no zero divisors. That is, if $a \cdot b = 0$, either $a = 0$ or $b = 0$.

Therefore a semifield is much like an integral domain, only semifields do not necessarily have associativity or commutativity of multiplication. We call a semifield *proper* if it is not itself a field. There are proper semifields of order 2^k for $k \geq 4$. A paper of Knuth [8] showed that semifields can be used to construct projective planes in much the same way as fields. That is, we view 1 dimensional subspaces of the 3 dimensional vectorspace (3 copies of the abelian group underlying the semifield) as points, and we view 2 dimensional subspaces as lines. Since semifields can construct projective planes, and since we know that certain quasiregular collineation groups of projective planes contain RDSs, we can relate semifields to certain RDSs as follows.

Let S be a finite semifield. We create the group G on the set S^2 under the following operation:

$$(a, b)(c, d) = (a + c, b + d + a \cdot c).$$

This group turns out to be isomorphic to the quasiregular collineation group of the projective plane, but we can show more directly (avoiding planes altogether) that this group has an RDS.

Theorem 2.3. *Let S be a semifield of order $|S| = 2^a$ for some a , where the underlying abelian group has exponent 2. Then in the group G on the set S^2 (under the above operation), $D = \{(g, 0) : g \in S\}$ is a $(|S|, |S|, |S|, 1)$ -RDS relative to the normal subgroup $N = \{(0, x) : x \in S\}$.*

Proof. We note first that the group identity is $(0, 0)$ and that $(a, b)^{-1} = (a, a^2 + b)$ for any $a, b \in S$. Take $(a, 0)$, $(b, 0)$, $(c, 0)$, and $(d, 0) \in D$ with $(a, 0) \neq (c, 0)$, and assume that $(a, 0)(b, 0)^{-1} = (c, 0)(d, 0)^{-1}$. Substituting for the inverses and performing the group operation yields $(a + b, b^2 + a \cdot b) = (c + d, d^2 + c \cdot d)$, giving us $a + b = c + d$ and $b^2 + a \cdot b = d^2 + c \cdot d$. Substituting the first into the second yields $(a + b) \cdot b = (a + b) \cdot d$, or

$$(a + b)(b - d) = 0.$$

Since, in our case, the group underlying the semifield is of exponent 2, and since semifields by definition have no zero divisors, either $a = b$ or $b = d$. Of course, if $a = b$ then $(a, 0)(b, 0)^{-1}$ is the identity. This accounts for $|S|$ copies of the identity in DD^{-1} . Otherwise, if $b = d$, then $a = c$ (since $a+b = c+d$ from above), whence no two pairs of distinct elements of D produce the same difference. Since there are $|S|^2 - |S|$ distinct ordered pairs of elements in D (and $|S|^2 - |S|$ elements in the set $S^2 \setminus N$), all that remains is to show that DD^{-1} avoids N and that N is normal. If $(0, x) = (a, 0)(b, 0)^{-1} = (a, 0)(b, b^2) = (a + b, b^2 + a \cdot b)$, then $a = b$, which we already noted yields the identity as the difference. Moreover, $(0, x) \in Z(G)$ for all $x \in S$, so $N \trianglelefteq G$, and thus G contains a $(|S|, |S|, |S|, 1)$ -RDS (namely D) relative to N . \square

To recap, we know how to construct RDS from projective planes - we find a quasiregular collineation group of the plane (there are usually several), and in it sits an RDS. Finding these groups, in general, is not easy. So, we appeal to the work of Knuth [8], who says that semifields can be used to construct projective planes, and these semifields provide a simple way to define the quasiregular collineation group. This construction, though, takes a bit of doing. If we are only concerned about finding the RDS, Theorem 2.3 allows us to do that.

So, we seem to have tied up the business of associating projective planes to RDS. But, we haven't yet considered the case of an RDS appearing in a group that is *not* coming from a semifield construction. We look for a generalization in the following sections.

3 Group cohomology

To decide if a certain group G has an RDS with certain parameters, we may simply compute all of the appropriately sized normal subgroups of G and perform an exhaustive search over the subsets of G (potential D 's). Of course, as the group size gets large, this becomes infeasible. In addition, it is difficult even to enumerate all of the groups of order 32 (there are 51), much less those of order 64 (there are 267) or 128 (there are 2328). This makes it essentially unfeasible to search for something as small as even $(16, 16, 16, 1)$ -RDS using this approach. This seems to be the wrong way to approach the problem.

We try another method. If G has an RDS, then the RDS must be relative to *something!* There must be a normal subgroup N and a quotient group $H \cong G/N$. So, another approach to this problem is to look at pairs (N, H) and look at properties of groups G that admit N as a normal subgroup with quotient H . As it turns out, this problem has a name (aptly, the *group extension problem*) and has been studied extensively.

3.1 Group extensions and factor sets

A *short exact sequence* of groups is a sequence as follows:

$$1 \rightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} H \rightarrow 1,$$

where ι and π are homomorphisms, ι is injective, π is surjective, and $image(\iota) = ker(\pi)$. Here we will say that G is an extension of N by H (books vary here - some refer to G as extending H by N). If the elements of H are $1, u, v, \dots, w$, then we will denote the cosets of N in G by $\bar{1}N, \bar{u}N, \bar{v}N, \dots, \bar{w}N$. Similarly, we will choose a set of coset representatives $\bar{1}, \bar{u}, \bar{v}, \dots, \bar{w}$ such that $\pi(\bar{u}) = u$ for each $u \in H$. We'll call our choice of coset representatives a *transversal*, given by the mapping $\tau : H \rightarrow G$, where $\tau(h) = \bar{h}$.

Since N is normal in G , the mapping $a \rightarrow \bar{u}^{-1}a\bar{u}$ is an automorphism of N (note that although $\bar{u} \in G$, $\bar{u}^{-1}N\bar{u} = N$). Moreover, since $u \in H$, this defines a group action of H on N , namely

$$a^u = \bar{u}^{-1}a\bar{u}. \tag{1}$$

Since, in general, it is not the case that $\bar{u}\bar{v} = \overline{uv}$, we define a mapping $\psi : H \times H \rightarrow N$ that satisfies the equation

$$\bar{u}\bar{v} = \overline{uv}\psi(u, v). \tag{2}$$

The set of elements that can be written as $\psi(u, v)$ for some $u, v \in H$ is called a *factor set*, since it, in effect, determines products of inverse images of elements of the factor group. Since applying the homomorphism π to equation (2) gives that $\pi(\psi(u, v)) = 1$, it is apparent that $\psi(u, v) \in N$. Moreover, if we adopt the convention that $\bar{1} = 1$ we see from Equation (2) that $\psi(u, 1) = 1 = \psi(1, v)$ for all $u, v \in H$. We'll call a factor set *normalized* if it satisfies this condition.

To define G , we need only the following:

1. The normal subgroup N .
2. The factor group H .
3. The automorphisms $a \mapsto a^u$ of N .
4. The factor set $\psi(u, v) \in N; u, v \in H$.

Hall then presents necessary and sufficient conditions for G to exist with normal subgroup N and factor group $H \cong G/N$.

Theorem 3.1. *There exists a group G with normal subgroup N and factor group H if and only if there exists $\psi : H \times H \rightarrow N$ such that for all $a \in N, u, v, w \in H$,*

1. $(a^u)^v = \psi(u, v)^{-1}(a^{uv})\psi(u, v)$, and
2. $\psi(uv, w)\psi(u, v)^w = \psi(u, vw)\psi(v, w)$.

Proof. (\Rightarrow) Assume such a G exists. Define ψ as above, so that $\bar{u}\bar{v} = \overline{uv}\psi(u, v)$ for all $u, v \in H$. Then taking $a \in N$, we see that

$$(a^u)^v = \psi(u, v)^{-1}(a^{uv})\psi(u, v),$$

by the definition of ψ . In addition, because associativity of G gives that $(\bar{u}\bar{v})\bar{w} = \bar{u}(\bar{v}\bar{w})$, we can discern the following equality. Using the left hand side, we get:

$$\begin{aligned}
(\bar{u}\bar{v})\bar{w} &= (\bar{u}\bar{v}\psi(u, v))\bar{w} \\
&= (\bar{u}\bar{v}(\bar{w}\bar{w}^{-1})\psi(u, v))\bar{w} \\
&= (\bar{u}\bar{v}\bar{w}(\bar{w}^{-1}\psi(u, v)\bar{w})) \\
&= (\bar{u}\bar{v}\bar{w})\psi(u, v)^w \\
&= \bar{u}\bar{v}\bar{w}\psi(uv, w)\psi(u, v)^w.
\end{aligned}$$

Using the right hand side, we get:

$$\begin{aligned}
\bar{u}(\bar{v}\bar{w}) &= \bar{u}(\bar{v}\bar{w}\psi(v, w)) \\
&= \bar{u}\bar{v}\bar{w}\psi(u, vw)\psi(v, w).
\end{aligned}$$

Equating the two, and cancelling the $\bar{u}\bar{v}\bar{w}$, we're left with

$$\psi(uv, w)\psi(u, v)^w = \psi(u, vw)\psi(v, w).$$

(\Leftarrow) On the other hand, assume we have automorphisms and a factor set satisfying the above. Consider the symbols $\{\bar{u}a : u \in H, a \in N\}$. We'll define a binary operation (product) on these symbols given by

$$\bar{u}a \cdot \bar{v}b = \bar{u}\bar{v}\psi(u, v)a^v b.$$

We'll call this system of symbols with a binary operation G . G is associative as follows:

$$\begin{aligned}
(\bar{u}a \cdot \bar{v}b) \cdot \bar{w}c &= (\bar{u}\bar{v}\psi(u, v)a^v b) \cdot \bar{w}c \\
&= \bar{u}\bar{v}\bar{w}\psi(uv, w)\psi(u, v)^w [(a^v)^w] b^w c \\
&= \bar{u}\bar{v}\bar{w}\psi(uv, w)\psi(u, v)^w [\psi(v, w)^{-1} (a^v w)\psi(v, w)] b^w c \\
&= \bar{u}\bar{v}\bar{w}[\psi(uv, w)\psi(u, v)^w \psi(v, w)^{-1}] (a^v w)\psi(v, w) b^w c \\
&= \bar{u}\bar{v}\bar{w}[\psi(u, vw)] (a^v w)\psi(v, w) b^w c \\
&= \bar{u}a \cdot \bar{v}\bar{w}\psi(v, w) b^w c \\
&= \bar{u}a \cdot (\bar{v}b \cdot \bar{w}c).
\end{aligned}$$

While it's not necessary to assume that $\psi(1, 1) = 1$, it does make our computations easier. We'll assume this, with the understanding that we may use the equality $1 = \bar{1}\psi(1, 1)^{-1}$ (from $\bar{1}\bar{1} = \bar{1}\psi(1, 1)$) instead, and that our result is in fact the same. If we take $u = v = 1$ in $(a^u)^v = \psi(u, v)^{-1} a^{uv} \psi(u, v)$, we get that $(a^1)^1 = a^1$. Since $a^1 = c$ is arbitrary, we have $c^1 = c$ for all $c \in N$. Using $u = v = 1$ appropriately in $\psi(uv, w)\psi(u, v)^w = \psi(u, vw)\psi(v, w)$ yields $1 = \psi(1, w)$, and if we instead use $v = w = 1$, we get that $\psi(u, 1) = 1$, and these hold for all $u, w \in H$. These equalities yield $\bar{1}\bar{1}$ to be a right and left identity, as $\bar{1}\bar{1} \cdot \bar{w}c = \bar{w}\psi(1, w)c = \bar{w}c$, and $\bar{u}a \cdot \bar{1}\bar{1} = \bar{u}\psi(u, 1)a = \bar{u}a$. Moreover, since $a \mapsto a^u$ is an automorphism of N , then there is an element $d \in N$ such that

$d^w = \psi(w^{-1}, w)^{-1}c^{-1}$ for any given $c \in N$ and $w \in H$. So for arbitrary $\bar{w}c$ in G , we have that $w^{-1}d \cdot \bar{w}c = \bar{1}\psi(w^{-1}, w)d^wc = \bar{1}1$, the identity. The system is clearly closed under the binary operation, and with associativity, identity, and left inverses, we have that G is a group.

The mapping $\phi : \bar{u}a \mapsto u$ is a homomorphism of G onto H , where the kernel consists of the elements $\bar{1}a$. Since $\bar{1}a \cdot \bar{1}b = \bar{1}\psi(1, 1)ab = \bar{1}ab$, the mapping $\bar{1}a \mapsto a$ is an isomorphism between the kernel of ϕ and N . Hence N is normal in G , with factor group H . \square

For reasons we will see shortly, we will be focusing on *central extensions*, those where $\psi(u, v) \in Z(G)$ for all $u, v \in H$. Note that this does not imply that $N \leq Z(G)$, only that the factor set (contained in N) is central. This reduces our two conditions from Theorem 3.1 to only the second. That is, $\psi(uv, w)\psi(u, v)^w = \psi(u, vw)\psi(v, w)$.

3.2 Cohomological foundations

As we stated above, we have H acting on N by conjugation. We can view this action as a left or right group action on N . If we instead let H act on both sides of $N \cap Z(G)$, an abelian group, we can view this group as a double H -module, a group that admits H as a group of operators on each side. The group action must be well-defined and obey distributive and associative laws. Hall [5] remarks that often in double sided modules, the group action on one side is often trivial. In our case, that would mean $h \cdot x = x$ for all $h \in H$ and x in the factor set, where here we denote the left group action by (\cdot) . So we will ignore the action of H on the left. This way we can use H as we have been, but we get to make use of some module theory.

Definition. For a double H -module N , we define $C^n(N, H)$ to be the additive group of functions $f : H^n \rightarrow N$ such that $f(x_1, x_2, \dots, x_n) = 0$ if x_i is the identity element of H for any i . We will call such functions *n-dimensional cochains*.

There is an operator δ , called the *coboundary operator* that maps C^n homomorphically into C^{n+1} . For each $f \in C^n$, we have:

$$\begin{aligned} (\delta f)(x_0, x_1, x_2, \dots, x_n) &= x_0 \cdot f(x_1, \dots, x_n) \\ &+ (-1)^{n-1} f(x_0, \dots, x_{n-1}) \cdot x_n \\ &+ \sum_{t=1}^n (-1)^t f(x_0, x_1, \dots, x_{t-1}x_t, x_{t+1}, \dots, x_n). \end{aligned}$$

Hall [5] proves the following theorem, to which we will appeal soon:

Theorem 3.2. *If $f \in C^n$, then $\delta^2 f = 0$.*

Definition. If $f \in C^n$ and $\delta f = 0$, then f is an *n-dimensional cocycle*. Moreover, if there exists a g in C^{n-1} such that $\delta g = f$ (that is, if f is in the range of the coboundary operator), then we say that f is a *coboundary*.

Note here that every coboundary is indeed a cocycle by Theorem 3.2 above. The cocycles comprise the kernel of the coboundary operator (recall that δ is a homomorphism) from C^n into C^{n+1} . Hence the cocycles are a normal subgroup of the cochains, and we write this set as $Z^n(N, H)$. Moreover, the coboundaries, $B^n(N, H)$ are normal in the cocycles, and their quotient group, $Z^n(N, H)/B^n(N, H)$ is called the n^{th} cohomology group of the double H -module N , and it is denoted $H^n(N, H)$. Lastly, we'll call two cochains *cohomologous* if their difference is a coboundary.

So what does this all mean to us? Let's go back and consider normalized factor sets. They satisfy $\psi(u, 1) = 1 = \psi(1, v)$. It seems that $\psi : H \times H \rightarrow N$ satisfies the conditions of being a 2-dimensional cochain. Now, the 2-dimensional coboundary operator looks like:

$$(\delta f)(x_0, x_1, x_2) = x_0 \cdot f(x_1, x_2) - f(x_0, x_1) \cdot x_2 - f(x_0 x_1, x_2) + f(x_0, x_1 x_2).$$

x_0, x_1 , and x_2 are in H , so let's call them u, v , and w respectively. Now noting that we are ignoring left group actions, the coboundary equation becomes:

$$(\delta f)(u, v, w) = f(v, w) - f(u, v) \cdot w - f(uv, w) + f(u, vw).$$

Cocycles are 0 under the coboundary operator, so they satisfy the equation:

$$0 = f(v, w) - f(u, v) \cdot w - f(uv, w) + f(u, vw).$$

We can rearrange to get:

$$f(uv, w) + f(u, v) \cdot w = f(v, w) + f(u, vw).$$

Looking back, we notice that this is the same as condition 2 in Theorem 3.1. The ψ we've been using to define the factor set has many of the same properties as a 2-dimensional cocycle. This section is best tied up with two theorems. The first of which is due to Hall [5].

Theorem 3.3. *The groups that are extensions of an abelian group N by a group H form a group of their own. It is isomorphic to $H^2(N, H)$ where*

1. H operates trivially on the left of N .
2. H induces automorphisms of N on the right.
3. Factor sets are the cocycles of $Z^2(N, H)$.
4. Equivalent factor sets differ by coboundaries in $B^2(N, H)$.

The second of which is found in Dummit and Foote:

Theorem 3.4. *A function $f : H \times H \rightarrow N$ is a normalized factor set for some extension G of N by H if and only if f is a normalized cocycle in $Z^2(N, H)$.*

We summarize the above theorems as follows. First, factor sets and cocycles are the same things. So, once we've picked automorphisms, all we need to do is find some cocycles to generate group extensions. Second, cocycles that differ by coboundaries produce isomorphic groups. That is, the groups that we get as extensions depend on the cocycles modulo the coboundaries. Interestingly, the first theorem says that the groups that we can get as extensions actually form a group themselves, where the group operation stems from pointwise multiplication of the cocycles generating the groups.

4 Tying cohomology to RDS: the Horadam approach

As we saw in section 3, cocycles determine group extensions. In [6], Horadam describes what she refers to as *central relative difference sets* by using cocyclic generalized Hadamard matrices. That is, she generates a matrix representing the cocycle, and she then uses properties of the matrix to discern properties of the extension. In particular, she can tell if the extension has a relative difference set.

For a finite group H , a finite abelian group N , and a cocycle $\psi : H \times H \rightarrow N$, the cocyclic matrix M_ψ is the $|H| \times |H|$ matrix (with rows and columns indexed by elements of H) such that $M_{i,j} = \psi(i, j)$. Horadam's paper only treats the case of *central extensions*; that is, $N \leq Z(G)$, where G is an extension of N by H (again, books vary on this - some refer to an extension where the factor set is central as a central extension). This means that we may omit the group action in the cocycle equation $\psi(uv, w)\psi(u, v)^w = \psi(u, vw)\psi(v, w)$ to leave us with:

$$\psi(uv, w)\psi(u, v) = \psi(u, vw)\psi(v, w).$$

Again, we will only consider normalized cocycles, those where $\psi(u, 1) = \psi(1, v) = 1$ for all $u, v \in H$. In the following example, we consider the simplest possible case: extension of an abelian group by a cyclic group.

Example 4.1. Suppose H is cyclic (that is, $\cong \mathbb{Z}_m$ for some m) and that $n \in N$. If we write $H = \langle a : a^m = 1 \rangle = \{1, a, a^2, \dots, a^{m-1}\}$, then we can define

$$\psi(a^i, a^j) = \begin{cases} 1 & \text{if } i + j < m; \\ n & \text{if } i + j \geq m. \end{cases}$$

Let $u = a^i, v = a^j$, and $w = a^k$. Then $\psi(uv, w)\psi(u, v) = n^{\lfloor \frac{(i+j)(\text{mod } m)+k}{m} \rfloor + \lfloor \frac{i+j}{m} \rfloor}$, and $\psi(u, vw)\psi(v, w) = n^{\lfloor \frac{(i+(j+k)(\text{mod } m))+k}{m} \rfloor + \lfloor \frac{j+k}{m} \rfloor}$. These quantities are equal (and thus the cocycle equation holds) if and only if $\lfloor \frac{(i+j)(\text{mod } m)+k}{m} \rfloor + \lfloor \frac{i+j}{m} \rfloor = \lfloor \frac{(i+(j+k)(\text{mod } m))+k}{m} \rfloor + \lfloor \frac{j+k}{m} \rfloor$. We have two possibilities. Either $i + j \geq m$ or $i + j < m$. Consider only the left hand side of the equation. If $i + j \geq m$, which makes $\lfloor \frac{i+j}{m} \rfloor = 1$, then $\lfloor \frac{(i+j)(\text{mod } m)+k}{m} \rfloor = \lfloor \frac{i+j+k}{m} \rfloor - 1$, since $i + j$

$(\text{mod } m) = i + j - m$. This makes the left hand side $\lfloor \frac{i+j+k}{m} \rfloor$. A similar argument shows that the right hand side equals the same quantity. On the other hand, if $i + j < m$, then $(i + j) \pmod{m} = i + j$ and $\lfloor \frac{i+j}{m} \rfloor = 0$, so the left hand side is still $\lfloor \frac{i+j+k}{m} \rfloor$. We equate the right hand side in the same manner. In either case, the function ψ is a cocycle, with cocyclic matrix

$$M_\psi = \begin{bmatrix} 1 & 1 & \dots & 1 & 1 \\ 1 & 1 & \dots & 1 & n \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & 1 & \dots & n & n \\ 1 & n & \dots & n & n \end{bmatrix}. \quad \square$$

When we are extending a group N by a group H , we consider the group $G_\psi = \{(n, h) : n \in N, h \in H\}$. We define multiplication on this group to be

$$(m, g)(n, h) = (mn\psi(g, h), gh).$$

Notice that independent of our choices of N and H , G_ψ will always have the property that $N \trianglelefteq G_\psi$ and that $G_\psi/N \cong H$.

On the other hand, we can use a given group G to construct a short exact sequence and cocycle. Again, using our short exact sequence,

$$1 \rightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} H \rightarrow 1,$$

we choose a transversal function $\tau : H \rightarrow G$ such that $\pi(\tau(h)) = h$ for each $h \in H$. In other words, τ chooses a set of representatives of the cosets of N . The element $\tau(g)\tau(h)\tau(gh)^{-1}$ of G is in the image of ι . We know this because $\pi(\tau(g)\tau(h)\tau(gh)^{-1}) = 1$ (remember π is a homomorphism), and by the definition of a short exact sequence, the image of ι is the kernel of π . Since this element of G is in the image of ι , $\iota^{-1}(\tau(g)\tau(h)\tau(gh)^{-1})$ is defined. We define the cocycle $\psi_\tau(g, h) = \iota^{-1}(\tau(g)\tau(h)\tau(gh)^{-1})$.

Theorem 4.1. *If we use τ to construct G_{ψ_τ} , we create a group isomorphic to G via the isomorphism ϕ , where $\phi : (n, h) \mapsto \iota(n)\tau(h)$.*

Proof. We see that ϕ is a homomorphism, since $\phi((m, g)(n, h)) = \phi(mn\psi_\tau(g, h), gh) = (\iota(m)\iota(n)\tau(g)\tau(h)\tau(gh)^{-1})\tau(gh) = \iota(m)\iota(n)\tau(g)\tau(h)$, but since $\iota(N) \leq Z(G)$, this is equal to $\iota(m)\tau(g)\iota(n)\tau(h)$, which is $\phi(m, g)\phi(n, h)$. To show that ϕ is 1-1, if $\phi(m, g) = \phi(n, h)$, we'd have $\iota(m)\tau(g) = \iota(n)\tau(h)$. Applying π to both sides (and remembering that $\text{image}(\iota) = \ker(\pi)$ and that $\pi(\tau(x)) = x$ for all x), we are left with $g = h$. We cancel in G to get $\iota(m) = \iota(n)$, which means that $m = n$ by the injectivity of ι . Hence ϕ is injective. Moreover, given $g \in G$, we can see that ϕ is surjective since π chooses the coset of N in which g exists, and there is a unique element of N by which $\tau(\pi(g))$ can be multiplied to get g back. \square

We can finally compile our work into a result about difference sets. The following result allows us to write a difference set in a canonical form when the forbidden subgroup is abelian.

Theorem 4.2. *Let N be a finite abelian group of order w and H be a finite group of order v , such that $w|v$. There exists a relative $(v, w, v, \frac{v}{w})$ -difference set in a central extension G of N by H , relative to N , if and only if there exists a cocycle ψ such that $G \cong G_\psi$ and $\{(1, h) : h \in H\}$ is a relative $(v, w, v, \frac{v}{w})$ -difference set in G_ψ relative to $N \times \{1\}$.*

Proof. (\Leftarrow) This is obvious. Take the RDS to be the image of $\{(1, g)\}$ under the isomorphism.

(\Rightarrow) Since translates of an RDS are still RDSs, we may assume that our RDS, D in G contains the identity. Since D contains an element from each coset of N , define a transversal $\tau : H \rightarrow G$ so that the image of τ is D . Then let ψ_τ be the cocycle determined by τ (see above), whence $G \cong G_{\psi_\tau}$. Then, the isomorphic image D^* in G_{ψ_τ} is a $(v, w, v, \frac{v}{w})$ -difference set in G_{ψ_τ} , and thus D^* is also a complete transversal in G_{ψ_τ} . We can thus write $D^* = \{(a_h, h) : h \in H\}$. We define a coboundary $\partial\phi(g, h) = \phi(g)^{-1}\phi(h)^{-1}\phi(gh)$, where $\phi : H \rightarrow N$, $\phi(h) = a_h^{-1}$ for each $h \in H$. If we let $\psi = \psi_\tau \partial\phi$, then (since ψ and ψ_τ are cohomologous, there is an isomorphism $\Phi : G_{\psi_\tau} \rightarrow G_\psi$). We'll let $\Phi(a, h) = (a\phi(h), h)$, whence, remembering $D^* = \{(a_h, h) : h \in H\}$, we see that $\Phi(D^*) = \{(a_h(a_h)^{-1}, h) : h \in H\} = \{(1, h) : h \in H\}$. By the isomorphism, $\Phi(D^*)$ is then a $(v, w, v, \frac{v}{w})$ -RDS in G_ψ (and it is, in fact, relative to $N \times \{1\}$). \square

An important point to make here is that this is a generalization of the relative difference sets we found in the semifield construction! In that case, we found a $(v, v, v, 1)$ -difference set in a group G relative to $N = \{(0, x)\}$. The group structure on G was that $(a, b)(c, d) = (a + c, b + d + a \cdot c)$. Switching the components of everything (and thereby creating an isomorphic group), we have a group with operation $(a, b)(c, d) = (a + c + b \cdot d, b + d)$. Recall that we defined the operation in the group constructed by the cocycle method as $(m, g)(n, h) = (mn\psi(g, h), gh)$, and notice that the cocycle takes the place of semifield multiplication. We can now see the semifield construction phrases in the language of group extensions. Taking a semifield S as an additive (abelian) group under semifield addition, we can extend S by itself, using the semifield multiplication as the cocycle. We can see that semifield multiplication satisfies the cocycle equation if we note that it distributes over addition and that addition is commutative. For instance,

$$\begin{aligned}
 \psi(uv, w)\psi(u, v) &= (u + v) * w + u * v \\
 &= u * w + v * w + u * v \\
 &= u * v + u * w + v * w \\
 &= u * (v + w) + v * w \\
 &= \psi(u, vw)\psi(v, w).
 \end{aligned}$$

Horadam and Udaya have seen this and refer to cocycles of this type as *multiplicative cocycles*. The idea of using cocycles to try to find difference sets, then, has led us to find at least one example we already knew.

We had mentioned before that Horadam and Perera had used cocyclic generalized Hadamard matrices to get results about relative difference sets. We begin with this definition.

Definition. A $v \times v$ matrix M with entries in a finite (multiplicative) group W of order w is a *generalized Hadamard matrix* $GH(w, \frac{v}{w})$ over W if, for fixed i and k , $i \neq k$, the multiset of quotients $m_{ij}m_{kj}^{-1}$, $1 \leq j \leq v$ contains each element of W exactly $\frac{v}{w}$ times. This $GH(w, \frac{v}{w})$ is *normalized* if the entire first row and column have only W 's identity as their entries. The matrix is *G-cocyclic* if its entries are values in the range of some cocycle from $G \times G$ into W .

Example 4.2. The additive group of \mathbb{F}_4 , the finite field with 4 elements $(0, 1, \alpha, \alpha^2)$, is isomorphic to \mathbb{Z}_2^2 . We can construct a normalized \mathbb{Z}_2^2 -cocyclic $GH(4, 1)$ over \mathbb{Z}_2^2 from the finite field. Write \mathbb{Z}_2^2 as $\langle a, b : a^2 = b^2 = (ab)^2 = 1 \rangle$. Let $\psi : \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^2$ be multiplication in \mathbb{F}_4 . That is, use the isomorphism $\phi : \mathbb{Z}_2^2 \rightarrow (\mathbb{F}_4)_+$, $\phi : 1 \mapsto 0, a \mapsto 1, b \mapsto \alpha, ab \mapsto \alpha^2$, and let $\psi(g, h) = \phi^{-1}(\phi(g) * \phi(h))$, where $*$ denotes multiplication in \mathbb{F}_4 . That ψ is indeed a cocycle is more easily seen by looking at the cocycle equation in terms of elements of \mathbb{F}_4 , remembering that ψ is field multiplication, and the group operation is field addition. We see that

$$[(x + y) * z] + [x * y] = [x * (y + z)] + [y * z], \quad x, y, z \in \mathbb{F}_4.$$

Thus we verify that

$$[\psi(uv, w)] [\psi(u, v)] = [\psi(u, vw)] [\psi(v, w)] \quad u, v, w \in \mathbb{Z}_2^2.$$

We can then use ψ to generate

$$M_\psi = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & a & b & ab \\ 1 & b & ab & a \\ 1 & ab & a & b \end{bmatrix}.$$

M_ψ is an example of a normalized \mathbb{Z}_2^2 -cocyclic $GH(4, 1)$ over \mathbb{Z}_2^2 . We can see that it is normalized as its first row and column only contain the identity. Horadam [7] refers to cocycles that come from semifield or field multiplication as *multiplicative cocycles*. Since fields are themselves semifields, the group extension G_ψ has a $(4, 4, 4, 1)$ -RDS by Theorem 2.3.

Definition. A cocycle $\psi : H \times H \rightarrow N$ is *orthogonal* if for each $h \neq 1 \in H$, there are $\frac{|H|}{|N|}$ solutions $x \in H$ to $\psi(h, x) = n$ for a given $n \in N$.

That is to say that an orthogonal cocycle gives rise to a cocyclic matrix where there is a uniform distribution of elements in each noninitial row. Of course, all normalized cocyclic generalized Hadamard matrices have this uniform distribution since the set of quotients of corresponding elements of any two rows must be uniformly distributed (this is the definition of a generalized Hadamard matrix), and the first row is all the identity (see Example 4.2). In

fact, the converse is true as well. That is, the cocyclic matrix of any normalized orthogonal cocycle is a normalized cocyclic generalized Hadamard matrix, which we prove as follows, using the group ring $\mathbb{Z}N$. In essence, we treat elements of N as the coordinate vectors of an $|N|$ -dimensional vectorspace over \mathbb{Z} .

Lemma 4.3. *Let $\psi : H \times H \rightarrow N$ be a cocycle. In $\mathbb{Z}N$, for each pair of elements $h, k \in H$,*

$$\sum_{g \in H} \psi(h, g)\psi(k, g)^{-1} = \psi(hk^{-1}, k)^{-1} \sum_{g \in H} \psi(hk^{-1}, g).$$

Proof. For computational ease, set $d = hk^{-1}$. Then

$$\begin{aligned} \sum_{g \in H} \psi(h, g)\psi(k, g)^{-1} &= \sum_{g \in H} \psi(dk, g)\psi(k, g)^{-1} \\ &= \sum_{g \in H} (\psi(d, k)^{-1}\psi(d, kg)\psi(k, g))\psi(k, g)^{-1} \\ &= \psi(d, k)^{-1} \sum_{g \in H} \psi(d, kg) \\ &= \psi(hk^{-1}, k)^{-1} \sum_{g \in H} \psi(hk^{-1}, g), \end{aligned}$$

with lines 2 and 4 of the above string of equalities coming from the cocycle equation and the fact that $g \mapsto kg$ is an automorphism of H . \square

We can now prove the theorem we mentioned before.

Theorem 4.4. *The normalized G -cocyclic matrix M_ψ over N is a generalized Hadamard matrix if and only if for every $g \neq 1 \in H$, $\sum_{h \in H} \psi(g, h) = \frac{v}{w}(\sum_{n \in N} n)$ in $\mathbb{Z}N$ (that is, ψ is an orthogonal cocycle).*

Proof. (\Rightarrow) This is obvious, as aforementioned, since the first row consists of only the identity.

(\Leftarrow) We appeal to Lemma 4.3. Choose two rows of M_ψ , say the h row and the k row. The left hand side of the equation in Lemma 4.3 counts the number of times each element of N occurs as a quotient between corresponding elements of these rows. Remember that if this distribution is uniform for all h and k , then the matrix is generalized Hadamard. The right hand side is equal to $\psi(hk^{-1}, k)^{-1}(\sum_{n \in N} n)$ in $\mathbb{Z}N$ since ψ is orthogonal. Noting that $n \mapsto \psi(hk^{-1}, k)^{-1}n$ is an automorphism of N , we see that the right hand side is equal to simply $\sum_{n \in N} n$, and our cocyclic matrix is generalized Hadamard. \square

We still haven't talked about why we're interested in normalized cocyclic generalized Hadamard matrices, but we have found that they are equivalent to normalized orthogonal cocycles. The main result of the Horadam and Perera paper makes a connection between these cocyclic generalized Hadamard matrices. Though I did not work through this proof in detail, I can give a sketch of its content.

Theorem 4.5. *Let H be a finite group of order v and N be a finite group of order w such that $w|v$. Then the following are equivalent:*

1. *There is an H -cocyclic $GH(w, \frac{v}{w})$ over N .*
2. *There is a relative $(v, w, v, \frac{v}{w})$ -difference set in a central extension of N by H , relative to N .*
3. *There is a divisible $(v, w, v, \frac{v}{w})$ -design, class regular with respect to N , with a central extension of N by H as a regular group of automorphisms.*

Proof. (2 \Leftrightarrow 3) This is a well-known result.

(1 \Rightarrow 3) Use the cocyclic matrix to define a cocycle and create a group extension G . The points of the design are the elements of G . The point classes are the cosets of N in G , and the blocks are the sets $\{(\psi(h_i, h_j)n_k, h_i)\}$ where j, k are fixed and i ranges, $h_i, h_j \in H$, and $n_k \in N$.

(2 \Rightarrow 1) Horadam uses an algebraic structure known as the twisted group ring to prove that if $\sum_{g \in H} \sum_{h \in H} (1, g)(1, h)^{-1} = v(1, 1) - \frac{v}{w} \sum_{a \in N} (a, 1) + \frac{v}{w} \sum_{a \in N} \sum_{h \in H} (a, h)$ in the ring $(\mathbb{Z}C)G_\psi$, then for all $g \neq 1 \in G$, $\sum_{h \in H} \psi(g, h)^{-1} = \sum_{a \in N} a$ in $\mathbb{Z}C$. What this statement is saying, essentially is that if we look at the multiset of differences from the set $\{(1, g) : g \in H\}$, we'll get v copies of the identity $[(1, 1)]$, and $\frac{v}{w}$ copies of every other element of the group G_ψ on the set $N \times H$ (this corresponds to the summation of (a, h)), except we subtract off the elements that look like $(a, 1)$, since they are in the forbidden subgroup (isomorphic to N). The computation in the twisted group ring then says that if this occurs (that is, if there is a relative difference set in G_ψ relative to $N \times \{1\}$, since we know that if there is one at all, then there is one that looks like $\{(1, h) : h \in H\}$), then the equation $\sum_{h \in H} \psi(g, h)^{-1} = \sum_{a \in N} a$ holds in $\mathbb{Z}C$, or in other words, the cocycle ψ is orthogonal. We've already seen that orthogonal cocycles produce generalized Hadamard matrices in Theorem 4.4. \square

This essentially completes our study of the Horadam and Perera paper. It is worth noting that most of the arguments in the paper are only good when the normal subgroup is central in the extension. The next thing I'd like to do is go back through many of these proofs to see where the cocycle equation (which is not in generality) was invoked. Hopefully these results can be changed slightly. For instance, I don't think that, in general, we care about generalized Hadamard matrices. On the other hand, I think orthogonal cocycles are essential, but I haven't proved it yet.

5 An anomolous $(4, 4, 4, 1)$ -relative difference set

Relative difference sets have been studied in great detail in abelian groups. In fact, several nonabelian examples of groups that admit relative difference sets are known, too, but they had all been examples of difference sets relative to central subgroups. This is what makes an example that appeared in a paper of

Galati (but due to Flannery) [4] so intriguing. There is no motivation for the following - only the example.

Example 5.1. In the group $G = \langle x, y : x^8 = y^2 = 1, yxy = x^5 \rangle$, $R = \{1, x^2, x^3, xy\}$ is a $(4, 4, 4, 1)$ relative difference set, relative to the normal but not central subgroup $N = \langle x^4, y \rangle$. We can verify this directly.

So seemingly out of nowhere comes a nonabelian example of a group with a RDS relative to a normal subgroup that is not in the center of the group. More surprisingly, perhaps, is that this example is in a small semi-direct product. We finally get to a research question! In which nonabelian groups might there be a $(2^n, 2^n, 2^n, 1)$ -RDS relative to a normal but not central subgroup? In an attempt to further explore this, we look at this example cohomologically.

Let $N = \langle a, b : a^2 = b^2 = (ab)^2 = 1 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and let $H = \langle x : x^4 = 1 \rangle$. We define a homomorphism $\epsilon : H \rightarrow \text{Aut}(N)$ so that $a^{\epsilon(x)} = a$ and $b^{\epsilon(x)} = ab$. As we'll see in the next section, since a is fixed by our automorphism, we can write a cocycle

$$[\psi_a(x^i, x^j)] = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & a \\ 1 & 1 & a & a \\ 1 & a & a & a \end{bmatrix}.$$

Additionally, we saw above that we could define a coboundary given any set mapping. We define that mapping as follows:

$$\phi : H \rightarrow N, \phi : 1 \mapsto 1, x \mapsto a, x^2 \mapsto a, x^3 \mapsto b.$$

Then our coboundary $\partial\phi : H \times H \rightarrow N$, given by $\partial\phi(x^i, x^j) = \phi(x^i)\phi(x^j)^{\epsilon(x^i)}\phi(x^{i+j})^{-1}$ has cocyclic matrix

$$[\psi_a(x^i, x^j)] = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & a & b & b \\ 1 & b & 1 & b \\ 1 & ab & b & 1 \end{bmatrix}.$$

Their pointwise product ψ is also a cocycle equivalent to ψ_a , since they are cohomologous. Its matrix is given by

$$[\psi(x^i, x^j)] = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & a & b & ab \\ 1 & b & a & ab \\ 1 & b & ab & a \end{bmatrix}.$$

The elements of the extension G look like elements of the set $N \times H$ with the group operation $(n_1, h_1)(n_2, h_2) = (n_1 n_2^{\epsilon(h_1)} \psi(h_1, h_2), h_1 h_2)$. The homomorphism generated by $(b, 1) \mapsto y$ and $(b, x) \mapsto z$ is an isomorphism onto $G = \langle z, y : z^8 = y^2 = 1, yzy = z^5 \rangle$, which is the group listed in Example 5.1.

It is worth noting here that ψ is an orthogonal cocycle (notice the uniform distribution of elements in each row), even though its cocyclic matrix is not

generalized Hadamard. In fact, I am so impressed by this that I leave this connection between orthogonal cocycles and RDS as a conjecture. Note that I haven't put much time into trying to resolve this conjecture, though in the case where N is central, this reduces to Theorem 4.5 by the equivalence of orthogonal cocycles and generalized Hadamard matrices in the N central case.

Conjecture 5.1. *There is a relative $(v, w, v, \frac{v}{w})$ -difference set in an extension of N by H , relative to N if and only if there is a (cocycle, automorphisms) pair such that there is an orthogonal cocycle from $H \times H \rightarrow N$.*

I took a particular interest in seeing if there were more RDS in cyclic extensions of elementary abelian groups (that is, where $N \cong \mathbb{Z}_2^n$ and $H \cong \mathbb{Z}_{2^m}$). Unfortunately, I ran out of time. I did, however, find a section of Hall's book that treated cyclic extensions in some detail, which I present in Section 6 as follows.

6 Cyclic extensions

Early on, we made a point that to define an extension of a group N by a group H , we needed only describe the automorphisms $a \mapsto a^u$ of N and the factor set $\psi(u, v) \in N$ for $u, v \in H$. We'll do just that as follows.

Suppose H is a cyclic group of order m , generated by an element x , so that the elements of H are $1, x, x^2, \dots, x^{m-1}$. Further suppose G is an extension of a group N by H , so that $G/N \cong H$. If we let \bar{x} be the coset representative of the coset of N that maps to x , then we can also let $\bar{x}^2, \bar{x}^3, \dots, \bar{x}^{m-1}$ be representatives of the cosets that map to x^2, x^3, \dots, x^{m-1} respectively. $\bar{x}^m = \alpha$ for some $\alpha \in N$, since $(\bar{x}N)^m = N$. So, applying the automorphism $a \mapsto a^x$ of N m times, we get:

$$a^{x^m} = \alpha^{-1}a\alpha. \tag{3}$$

(Remember that $a^x = \bar{x}^{-1}a\bar{x}$). Since $\alpha = \bar{x}^m$, we see that $\alpha^x = \bar{x}^{-1}\alpha\bar{x} = \bar{x}^m$, or simply:

$$\alpha^x = \alpha. \tag{4}$$

It can actually be shown that Equations (3) and (4) are also sufficient to have an extension of N by H .

Theorem 6.1. *Let N, H be finite groups, H cyclic of order m . Then an extension G of N by H exists if and only if there exists an automorphism $a \mapsto a^x$ of N and $\alpha \in N$ such that Equations (3) and (4) hold.*

Proof. (\Rightarrow) Clear from the previous discussion.

(\Leftarrow) The elements of H are $\{x^i : 0 \leq i \leq m-1\}$. Suppose then that we define automorphisms as follows:

$$a^{x^0} = a, \quad a^{x^i} = (a^{x^{i-1}})^x, \quad 1 \leq i \leq m-2.$$

We define our factor set

$$\psi(x^i, x^j) = \begin{cases} 1 & \text{if } i + j < m; \\ \alpha & \text{if } i + j \geq m. \end{cases}$$

Hall says that it's clear to see, then, that our choice of automorphisms and factor set satisfy the premises of Theorem 3.1, which would imply that an extension G exists, but I had to work a little to understand this. Let's first show that this satisfies $(a^u)^v = \psi(u, v)^{-1} a^{uv} \psi(u, v)$. Let $u = x^i$ and $v = x^j$. If $i + j < m$, then $\psi(u, v) = 1$, and our equation reads $(a^{x^i})^{x^j} = a^{x^i x^j} = a^{x^{i+j}}$. This equation clearly follows from the definition of our automorphism. On the other hand, if $i + j \geq m$, then $(a^{x^i})^{x^j} = (a^{x^{(i+j) \pmod{m}}})^{x^m} = \alpha^{-1} (a^{x^{(i+j) \pmod{m}}}) \alpha$, which is what we wanted to show. As for the other equation to satisfy, that is, $\psi(uv, w) \psi(u, v)^w = \psi(u, vw) \psi(v, w)$, we've already seen in Example 4.1 that the right hand side of the equation is equal to $\alpha^{\lfloor \frac{i+j+k}{m} \rfloor}$, where $u = x^i$, $v = x^j$, and $w = x^k$. The left hand side, then, is $\alpha^{\lfloor \frac{(i+j) \pmod{m} + k}{m} \rfloor} (\bar{x}^{-1})^k \alpha^{\lfloor \frac{i+j}{m} \rfloor} \bar{x}^k$, but since $\alpha = \bar{x}^m$, the above elements commute, and so the action of w is trivial, and we are reduced entirely to Example 4.1, and the left hand side and right hand side are equal. \square

Amazingly, this simple theorem decides the question of the existence of cyclic extensions. It does not, however, give much information about relative difference sets. We began looking at trying to extend elementary abelian groups by cyclic groups. The next step in this program, then, would be to attempt to classify the automorphisms of the elementary abelian groups (the N 's) that we are extending by H . In general, the number of automorphisms of \mathbb{Z}_2^n is $\prod_{k=0}^{n-1} (2^n - 2^k)$, which comes from counting the number of ways we can choose n linearly independent generators for \mathbb{Z}_2^n . This number is reduced by the condition that the automorphism has to have a fixed point.

7 Conclusion

I spent a lot of time this year doing expository work. In fact, most of what I did this year involved reading books and papers and working through examples. Only a small part of my time was spent on the cyclic extensions and trying to eliminate or create possible groups in which we may find a difference set. The first places to look are the groups of order 32 and 64 of small exponent (it seems that most of the 2-groups that have RDS have small exponent). While I haven't solved a problem, I have learned a lot, and the counting proof that the semifield gives rise to a difference set is one that I have not seen elsewhere. I plan to take this problem with me as I move on, and hopefully I will make more progress on it.

8 Acknowledgements

This paper is the author's undergraduate senior thesis, taken under the direction of Professor James Davis, and the author thanks him for his encouragement, for his assistance, and for many meaningful conversations. The author also thanks Professor Michael Kerckhove, whose comments have greatly improved the readability of this paper.

References

- [1] J. Davis, Relative difference sets in nonabelian 2-groups with $\lambda = 1$: A preliminary study, manuscript.
- [2] P. Dembowski, Finite Geometries, Springer, Berlin, 1997.
- [3] D. Dummit and R. Foote, Abstract Algebra, 2nd ed., Wiley, New York, 1999.
- [4] J. Galati, Application of Gaschtz' theorem to relative difference sets in non-abelian groups, J. Comb. Design., 11, No.5 (2003), 307-311.
- [5] M. Hall, Theory of Groups, 2nd ed., Chelsea, New York, 1976.
- [6] K. Horadam and A. Perera, Cocyclic generalised Hadamard matrices and central relative difference sets, Designs, Codes, and Cryptography, 15 (1998), 187-200.
- [7] K. Horadam and P. Udaya, A new construction of central relative $(p^a, p^a, p^a, 1)$ -difference sets, Designs, Codes, and Cryptography, 27 (2002), 281-295.
- [8] D. Knuth, Finite semifields and projective planes, Ph. D. thesis, 1963.