Constructive Representation Theoretic Methods and non-Abelian Difference Sets

Robert A. Liebler*
Colorado State University
Fort Collins, Colorado 80523, USA

The historical development of a mathematical subject has often begun with the commutative case and then built on this case to unravel the non-commutative. Although the role of non-Abelian groups in algebraic combinatorics and finite geometry goes back at least to Dickson [9], genuinely non-Abelian difference sets have only appeared in the last few years [17],[21].

We celebrate Abelian difference sets because they exhibit an intimate interplay between combinatorics, finite geometry and number theory. The power of this combination is rightly recognized as a high point of algebraic combinatorics today.

Doesn't it seem odd that such a beautiful interplay exists only in a commutative context? Isn't it a worthy goal to broaden this unique synergy? More specifically, isn't it natural to find methods for algebraic combinatorics that move beyond linear algebra and systematically exploit integrality or even "setness". (I use this term to mean: More than a solution to an algebraic equation is sought, because an additional Diophantine-like condition is required that the solution must arise from a set.)

As a way of emphasizing this change in emphasis I use the term **constructive combinatorial representation theory** to mean those results that are helpful in finding new structures with specified algebraic properties (like designs, or distance regular graphs) and distinguish this subject from the companion **nonexistence theory** in which invariants are used to establish new parameter conditions on such objects.

*Support from an NSF grant is gratefully acknowledged.

I suspect that constructive combinatorial representation theory has wide application outside of algebraic combinatorics. More to the point, I argue that the study of non-Abelian difference sets is an excellent arena in which to build constructive machinery. I also aim to give a few hints as to how to adapt standard algebraic machinery to this task and to encourage you to join me in this adventure. But I warn you that if you aren't careful you might see that the tools of the non-commutative theory shed insight into wholly commutative constructs.

After a little algebraic history, we show how the movement from a design with a regular automorphism group to a subset of a group ring generalizes to the use of matrices over group rings. This is a fundamental tool in the study of incidence structures admitting a group of automorphisms. The methods of contraction, group representations and coding theory are all exploitation of homomorphic images of such matrix rings. We indicate the small adjustments required to use these basic methods for non-Abelian groups. We also mention a few situations where both Abelian and non-Abelian methods complement each other.

The third section presents the basic goals of a constructive theory and the few known examples of genuinely non-Abelian difference sets. The recipe used in building genuinely non-Abelian difference sets is also given as a way of framing some of the new machinery I have used to look for non-solvable difference sets.

In section 4 we review some of the most basic facts about the supporting representation theory. The emphasis is on reconciling the combinatorial imperative to remain integral with the standard practice of working over a splitting field. There follows a brief section containing examples from a current project: The study of difference sets in groups involving the alternating group A_5. This culminates in an explicit 3-coloring of a triangulation of the icosahedron with some remarkable autocorrelation properties. We end with a list of problems and conjectures.

Thanks to J. Iiams and K. W. Smith for many helpful suggestions.

1 History, Left and Right

It is widely acknowledged that Frobenius originated group representation theory more that 100 years ago [11]. I would like to take this opportunity to point that, because of its number theoretic origins, his work is more combinatorial than more modern methods. In particular, the methods of Frobenius are constructive.

Let us consider the **Frobenius** group $Frob_{7\cdot 3} =$

$$G = \langle a, b | a^7 = b^3 = 1 \quad ab = ba^2 \rangle = \left\{ a^i b^j | 0 \leq i \leq 6, 0 \leq j \leq 2 \right\}.$$

Order its elements: $a^i b^j \prec a^k b^l$ if $j \leq l$ and in case of equality $i < k$. Then introduce 21 variables $x_g, g \in G$ and establish the convention

$$x_{gh} := x_k \text{ where } k = gh, \; g, h, k \in G.$$

Next use $\mathbf{x}$ to denote the (column) vector with coordinates x_g, $g \in G$ and define two matrix valued functions $\lambda(\mathbf{x}), \rho(\mathbf{x})$. The h-th column of $\lambda(\mathbf{x})$ (respectively $\rho(\mathbf{x})$) having the monomial $x_{gh^{-1}}$ (respectively $x_{g^{-1}h}$) in g-th position.

One can show the functional identity $\Theta(G) := det(\lambda(\mathbf{x})) = det(\rho(\mathbf{x}))$. This function is the **group determinant**.

In the late 19th century Dedekind's study of algebraic number rings $\mathcal{O}$ had led him to the fact that the prime factors of the discriminant $\Delta(\mathcal{O})$ are precisely the primes that ramify in $\mathcal{O}$. He further realized that if $\mathcal{O}$ has a normal $\mathbb{Z}$-basis then the factorization of $\Delta(\mathcal{O})$ is determined by the Galois group $G = Aut_{\mathbb{Z}}(\mathcal{O})$.

In 1886 he found an effective way of identifying the primes that ramify in $\mathcal{O}$, when $Aut_{\mathbb{Z}}(\mathcal{O})$ is Abelian, by factoring $\Theta(Aut_{\mathbb{Z}}(\mathcal{O}))$. Ten years later he suggested that Frobenius consider the non-Abelian case. In less than a year, Frobenius published his answer.

Let ω, (ζ) be primitive complex 3-rd (7-th) roots of unity and "bar" denote complex conjugation. Frobenius' answer for our group G is:

$$\Theta(G) = (\Sigma_{g \in G} x_g) \; A \; \overline{A} \; B^3 \; \overline{B}^3$$

$$\text{where } A = \sum_{i,j} \omega^j x_{a^i b^j}, \quad B = det(M) \text{ and}$$

$$M = \begin{pmatrix} \Sigma\zeta^i x_{a^i} & \Sigma\zeta^i x_{a^i b} & \Sigma\zeta^i x_{a^i b^2} \\ \Sigma\zeta^{2i} x_{a^i b^2} & \Sigma\zeta^{2i} x_{a^i} & \Sigma\zeta^{2i} x_{a^i b} \\ \Sigma\zeta^{4i} x_{a^i b} & \Sigma\zeta^{4i} x_{a^i b^2} & \Sigma\zeta^{4i} x_{a^i} \end{pmatrix}.$$

Frobenius found this a little mysterious and in less than a year [10, p 82-103] he showed how to find a matrix P so that $P\lambda(\mathbf{x})P^{-1}$ is a block diagonal matrix whose diagonal entries are:

$$\Sigma x_g, A, \overline{A}, M, M, M, \overline{M}, \overline{M}, \overline{M}.$$

By putting the $\Theta(G)$ factorization in a natural context he introduced the concept of a (matrix) **representation**.

In modern language it is a group homomorphism ϕ from G to invertible (matrices) linear functions on a vector space V. Finding a representation of G amounts to finding a ring R $(= End(V))$ with (a homomorphic image of) G as a group of multiplicative units.

Today the **degree** of ϕ is the dimension of V and the **character** of ϕ is the composition of ϕ followed by the trace function. Their original meanings were associated with factors of $\Theta(G)$ namely its total degree and penultimate coefficient.

Notice that the linear factors of $\Theta(G)$ are associated with the characters of the Abelian group $\overline{G} := G/\langle a\rangle$. And for each such character, the associated linear factor of $\Theta(G)$ equals the dot product of $\mathbf{x}$ with the vector of character values. The linear factors are just the value of **general element** $\mathbf{x} \in \mathbb{C}G$ at the various characters of $\overline{G}$.

Today we avoid typographic nightmares like the matrix M and deal directly only with group elements, letting the distributive law take care of the rest. Thus, the matrix M is $\phi(\mathbf{x})$ where ϕ is defined by:

$$\phi(a) = \begin{pmatrix} \zeta & & \\ & \zeta^2 & \\ & & \zeta^4 \end{pmatrix} \text{ and } \phi(b) = \begin{pmatrix} & 1 & \\ & & 1 \\ 1 & & \end{pmatrix}. \tag{1}$$

The representations defined by λ and ρ are of particular importance to our purpose here. Observe that the matrix $\lambda(s)$ (obtained from $\lambda(\mathbf{x})$ by setting $x_s = 1$ and $x_t = 0$ for all $t \neq s,\ s, t \in G$) has zeros in all positions except in positions $(sh, h),\ h \in G$ where it has 1s. Similarily $\rho(s)$ has zeros in all positions except in positions $(hs^{-1}, h),\ h \in G$ where it has 1s.

It is natural to identify the $h \in G$ with the specialization of $\mathbf{x}$ at the characteristic function of h (the h-th column of an identity matrix). Then

$$\lambda(s)h = sh \text{ and } \rho(s)h = hs^{-1}.$$

For this reason, λ, (ρ) is now called the **left (right) regular representation** of G These representations are SO important to us because the associative law $(g(xh) = (gx)h)$ in G implies that

$$\lambda(g)\rho(h) = \rho(h)\lambda(g), \quad g, h \in G.$$

This simple fact leads quickly to the crucial

Theorem 1.1 $Hom_{\lambda(\mathbb{Z}G)}(\mathbb{Z}G) = \rho(\mathbb{Z}G)$.

Of course, we stand on the shoulders of other giants as well and there are many other important contributions that deserve to be recognized. But there is neither time nor space to relive history here, so I will be content to mention but two other results of particular interest from our perspective.

Brauer's [2] study of just how big the coefficient field K needs to be before the structure of the group ring KG stabilizes is really important. He proved Maschke's conjecture of almost 50 years:

Theorem 1.2 *Suppose G is finite of exponent m. Let ζ_m be a primitive complex m-th root of unity. Then $\mathbb{Q}[\zeta_{exp(G)}]$ is a splitting field for G.*

I want also to mention the work of Maranda[18] because I suspect it may just be what those interested in difference sets need. Maranda starts with the group ring RG for G finite and R an integral domain. Maranda then considers $\overline{R}G$ where $\overline{R}$ is the residue class ring of R modulo the m-th of a prime ideal. The result is that for sufficiently large m, the two rings have the same structure.

This is one of the very few classical results involving representation theory and Galois rings of which I am aware.

2 Homomorphism Methods.

The most useful method of constructive design theory is the exploitation of homomorphic images. This method has as its basis an embedding of an incidence structure admitting a group G into a matrix ring over the group ring of G. We show here how this works for non-Abelian groups. In this section we also give a few examples of situations where the same object can be studied with both commutative and non-commutative machinery.

2.1 Incidence Relations and Matrices over Group Rings.

Suppose first that G acts regularly on Ω and $\mathcal{D} \subset \Omega \times \Omega$ is a G-invariant incidence relation with incidence matrix $A(\mathcal{D})$. This means that

$$(x, y) \in \mathcal{D} \text{ if and only if } (g(x), g(x)) \in \mathcal{D} \text{ for all } x, y \in \Omega, g \in G$$

since $\lambda(g)^T = \lambda(g)^{-1}$, this is equivalent to

$$\lambda(g)A(\mathcal{D}) = A(\mathcal{D})\lambda(g) \text{ for all } g \in G.$$

Because G acts regularly, we may pick $\omega \in \Omega$ and label Ω by G using $g\omega \mapsto g$.

In case $\mathcal{D}$ is a design, it is standard to shift attention to the associated difference set $\Delta \subseteq G$. But this shift works in general because Theorem 1.1 implies that $A(\mathcal{D}) = \rho(x)$ for some $x \in \mathbb{Z}G$. The fact that $A(\mathcal{D})$ is a $(0, 1)$-matrix implies that there is a subset $D \subseteq G$ such that

$$A(\mathcal{D}) = \rho(x) \text{ for } x = \sum_{g \in D} \rho(g).$$

In fact $D = \{h \in G \,|(h, 1) \in \mathcal{D}\} \subseteq G$.

Example 2.1 *($PG(2, 4)$ in $PG(2, 2)$)*
The subset $D = \{a, a^2, a^4, b, b^2\} \subseteq G = Frob_{7\cdot3}$ is a difference set and the associated design $\mathcal{D}$, having incidence matrix $A(\mathcal{D}) = \sum_{g\in D} \rho(g)$, is the (unique) projective plane of order 4, that is $PG(2, 4)$. Since $G \leq PGL(3, 2)$, G is also an automorphism group of the Fano plane acting regularly on the **flags** *(incident point-line pairs).*

Thus the **non-Abelian** *difference set D leads to an amusing new way to view $PG(2, 4)$, namely from within the Fano Plane. Indeed we implicitly have exhibited a set of five flags of $PG(2, 2)$ whose development under G forms a set of 21 "lines" of (the) projective plane of order 4.*

We (sadly) pose the following exercise: Show that it is impossible to find a set of five flags of $PG(2, 2)$ such that their development under the **full automorphism group** *of $PG(2, 2)$ forms a set of 21 "lines" of (the) projective plane of order 4.*

More generally, let Ω be any set upon which G acts and suppose $\omega_1 \ldots \omega_s$ are G-orbit representatives. Let $\mathcal{R}(\Omega)$ denote the ring generated by the set $Inv(G, \Omega)$ of all G-invariant relations on Ω.

Theorem 2.2 *Define the function* $\mu : \mathcal{R}(\Omega) \longrightarrow Mat_{ss}(\mathbb{Z}G)$ *by*

$$\mu(\Delta)_{i,j} = \frac{|G|}{|\Omega_j|} \sum_{(h\omega_i, \omega_j) \in \Delta} h,$$

for $\Delta \in Inv(G, \Omega)$. *Then* μ *is an injective ring homomorphism.*

Proof: As above, the map μ is the composition of two maps with the intermediate object being $Mat_{ss}(\rho(\mathbb{Z}G))$ and it all reduces to Theorem 1.1.

Example 2.3 *(*$Frob_{7\cdot 3}$ *on* $\binom{7}{3}$*)*
Let $\Omega = \binom{X}{3}$ *be the* $3-$*sets of the 7-set* $\{0 \ldots 6\}$ *under the action of the group* $G = Frob_{7\cdot 3}$ *given by* $a \mapsto (0123456)$, $b \mapsto (124)(365)$. *Note that* G *has three orbits on* Ω *and take as orbit representatives* $\omega_1 = \{1, 2, 4\}$, $\omega_2 = \{0, 1, 2\}$, $\omega_1 = \{3, 5, 6\}$. *Consider the relation*

$$\Delta := \{(x, y) \in \Omega \times \Omega \ : |x \cap y| = 2\} \in \mathcal{R}(\Omega).$$

Set $M_{i,j} := \{h \in G : |h\omega_i \cap \omega_j| = 2\}$ *and identify a subset of* G *with its sum in the group ring* $\mathbb{Z}G$. *Then* $\mu(\Delta) = M \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}^{-1}$ *where* $M =$

$$\begin{pmatrix} 0 & (1+a^5+a^6)(1+b+b^2) & (a+a^2+a^4)(1+b+b^2) \\ (1+b+b^2)(1+a+a^2) & a+a^6+b+b^2+ab+a^5b^2 & (1+b+b^2)(a^3+a^4+a^5) \\ (a^3+a^5+a^6)(1+b+b^2) & (a^2+a^3+a^4)(1+b+b^2) & 0 \end{pmatrix}.$$

Note $M_{1,1} = M_{3,3} = 0$ *since* Ω_1 *and* Ω_3 *are the lines of two* G*-invariant Fano planes. Note also that* Δ *being a symmetric relation implies that* $M^T = M^-$ *where* $^-$ *is the extension to* Mat_{33} *of the* $\mathbb{Z}G-$*anti-autormorphism* $g \mapsto g^{-1}$.

In fact Δ *is the distance regular* **Johnson** *graph* $J(7, 3)$ *and* $\mu(\Delta)$ *has minimal polynomial* $(x-12)(x-5)x(x+3)$

The exchange of the original incidence matrix for such a larger matrix may seem foolish. Indeed I acknowledge it is not directly constructive. However, it provides a uniform way of viewing a wide variety of situations and captures, for example, finite dimensional Hecke algebras and difference sets in the same conceptual framework. In addition, this is a uniform inductive context and so the passage to subgroups or homomorphic images is simple and clean.

2.2 Contraction: Group Homomorphisms.

If $\phi : G \to H$ is a group homomorphism, then one may replace the entries of $\mu(\Delta)$ with their images under $\phi : \mathbb{Z}G \to \mathbb{Z}H$ to obtain the contraction of $\mu(\Delta)$ with respect to ϕ. This is the basis of a very important difference set method introduced by Bruck [3] and used by everyone else since. It works well because a subset of G maps to an element of $\mathbb{Z}H$ with non-negative coefficients and so "setness" in G can be recognized in $\mathbb{Z}H$.

Example 2.4 *Return to Example 2.3 and consider the group homomorphism $\phi : G \to G/\langle a \rangle$ extended to $Mat_{33}(\mathbb{Z}G)$. Then*

$$\phi(\mu(\Delta)) = \begin{pmatrix} 0 & 3(1+b+b^2) & (1+b+b^2) \\ (1+b+b^2) & 2(1+b+b^2) & (1+b+b^2) \\ (1+b+b^2) & 3(1+b+b^2) & 0 \end{pmatrix}$$

which has minimal polynomial $(x-12)x$.

In a way, many of the methods we introduce are an attempt to articulate circumstances where some of the power of contraction can be employed in the more general representation theoretic context.

2.3 Representations: Group Ring Homomorphisms.

Suppose ϕ is a representation of G. Then any property of the G-invariant incidence structure Δ that can be expressed in terms of arithmetic of its incidence matrix is reflected as matrix equations in the homomorphic ring $Mat(\phi(\ G))$. The most familiar instances of this are obtained from the trivial representation, in which case intersection matrices and results like Block's Lemma, arise.

In the study of Abelian difference sets, the use of characters is the use of nontrivial representations. The fact that $\mathbb{Z}G$ maps to a Dedekind domain contained in the cyclotomic integers $\mathbb{Z}[\zeta_{exp(G)}]$ is heavily expoited. More generally, the use of nontrivial $G-$linear representations leads to **generalized intersection matrices** eg.[14]. I am unsure of who first used them in a combinatorial setting.

Example 2.5 *Return to Example 2.3 and consider the representation ϕ appearing in Equation(1) extended to $Mat_{33}(\mathbb{Z}G)$. Let*

$\alpha = \zeta+\zeta^2+\zeta^4$, $\beta = 1+\zeta+\zeta^2$, $\gamma = \zeta^3\beta$ and let ${}^{(2)}$ denote $\mathbb{Z}[\zeta]$-automorphism taking ζ to ζ^2. Then $\phi(\mu(\Delta))diag(3,3,3,1,1,1,3,3,3)$ is:

$$\begin{pmatrix}
0 & 0 & 0 & \overline{\beta} & \overline{\beta} & \overline{\beta} & \alpha & \alpha & \alpha \\
0 & 0 & 0 & \overline{\beta}^{(2)} & \overline{\beta}^{(2)} & \overline{\beta}^{(2)} & \alpha & \alpha & \alpha \\
0 & 0 & 0 & \overline{\beta}^{(4)} & \overline{\beta}^{(4)} & \overline{\beta}^{(4)} & \alpha & \alpha & \alpha \\
\beta & \beta^{(2)} & \beta^{(4)} & \zeta+\zeta^6 & 1+\zeta & 1+\zeta^5 & \gamma & \gamma^{(2)} & \gamma^{(4)} \\
\beta & \beta^{(2)} & \beta^{(4)} & 1+\zeta^3 & \zeta^2+\zeta^5 & 1+\zeta^2 & \gamma & \gamma^{(2)} & \gamma^{(4)} \\
\beta & \beta^{(2)} & \beta^{(4)} & 1+\zeta^4 & 1+\zeta^6 & \zeta^4+\zeta^3 & \gamma & \gamma^{(2)} & \gamma^{(4)} \\
\overline{\alpha} & \overline{\alpha} & \overline{\alpha} & \overline{\gamma} & \overline{\gamma} & \overline{\gamma} & 0 & 0 & 0 \\
\overline{\alpha} & \overline{\alpha} & \overline{\alpha} & \overline{\gamma}^{(2)} & \overline{\gamma}^{(2)} & \overline{\gamma}^{(2)} & 0 & 0 & 0 \\
\overline{\alpha} & \overline{\alpha} & \overline{\alpha} & \overline{\gamma}^{(4)} & \overline{\gamma}^{(4)} & \overline{\gamma}^{(4)} & 0 & 0 & 0
\end{pmatrix}$$

$\phi(\mu(\Delta))$ has eigenvalues 5 to multiplicity 1, -3 to multiplicity 2 and 0 to multiplicity 6.

The use of all irreducible representations in this way is called the transformation from the combinatorial domain to the spectral domain. A fundamental problem is the recognition of incomplete data from one domain in the other.

Even when transformation to the spectral domain leads to difficult matrix computations, it is sometimes possible to play two very different incidence structures admitting the same group off against each other. For example, Vincent [23] uses this strategy with Hermitian unitals and generalized quadrangles admitting special groups of order q^3 to settle a conjecture about the modular rank of the Hermitian unital [1, p 300] for q odd.

2.4 Coding Theory: Coefficient Ring Homomorphisms.

A fundamentally different kind of homomorphism method is to replace the $\mathbb{Z}$ in $\mathbb{Z}G$ with a different ring R. Representation theorists generally work over a splitting field for G. By Brauer's Theorem 1.2 it is sufficient to work with R a cyclotomic number ring and a determined combinatorist can recover both integrality and setness from R. The homomorphic images of R are well understood because R is a Dedekind domain. By the Chinese remainder theorem we need only consider homomorphisms with kernel a primary ideal.

Let ϕ be such a homomorphism as extended to first RG then matrices over RG.

Now the matrix $\phi(\mu(\Delta))$ takes values in a Galois ring and its study is a part of **coding theory**. It seems a natural setting to study difference sets for which the associated design has prime power order. Somewhat surprisingly, the supporting group representation theory has yet to be developed by group theorists and is my reason for mentioning Maranda's work.

Needless to say, the three basic homomorphism types can be used in combination and sometimes it is expedient, as in Vincent's work on Hermitian unitals, to work with a proper subgroup of the full group of automorphisms of the incidence relation under study.

There are some ways that non-commutative representations arise naturally in the study commutative structures. Suppose, for example, that R is a finite commutative ring. Then the group

$$AGL(1, R) = \{f : R \to R \mid f(x) = ax + b,\ a \in R^\star,\ b \in R\}$$

has some value in the study of R. The representation theory of $AGL(1, R)$ presents the structure of R in a useful way and provides substantial machinery for its study. This is how Mena and I [16] first studied Galois rings.

Cushman[6] is using this approach to study Cyclotomic association schemes and conjectures of Dillon's concerning cyclic difference sets.

3 Home Cooking.

The goals of a constructive theory are the following: Find ways of checking many cases at once **case collapsing**. Find theorems that reduce the necessary checking **load lightening**.

Contraction is the most important case collapsing tool. Both group homomorphic images and ring homomorphic images of the integral group ring have also been used to collapse cases. Powerful load lightening theorems like multiplier theorems exploit integrality and setness.

The study of difference sets in non solvable groups requires new machinery. We will introduce **modular intertwining** and **culling of bogus solutions** as new case collapsing tools and recognize large **Schur index** to be a load lightening property.

Theorem 3.1 *A k-subset D of a group G is a difference set of order n if and only if there is an integer λ such that satisfies the difference set equation*

$$DD^{-} = \lambda G + n \in \mathbb{Z}G, \qquad \text{(DSE in } \mathbb{Z}G\text{)}$$

where $^{-}$ denotes the $\mathbb{Z}G$ anti-isomorphism that takes each group element to its inverse. If K is a field, this is equivalent to

$$\phi(D)\phi(D^{-}) = nI, \qquad \text{(DSE under } \phi\text{)}$$

for each nontrivial projective indecomposable K-representation ϕ.

Of course, a set $D \subseteq G$ can be checked to be a difference set by counting the number of solutions to the equation $g = xy^{-1}, x, y \in D$ for each element $g \in G$. A fundamental theorem [4, 54.16] asserts that the multiplicities e_i and the degrees d_i of the projective indecomposable representations ϕ_i of G satisfy $|G| = \Sigma d_i e_i$. It follows that the switch to the spectral domain and representations is not by itself load lightening.

3.1 The Known Genuinely non-Abelian Difference Sets.

The Singer difference sets are associated with the point-hyperplane design $\mathcal{D}$ of a finite projective space $PG(n-1, q)$ and this design has automorphism group $P\Gamma L(n, q)$. Using the method of section (2.1) and $\mathcal{D}$, one can construct a difference set in any subgroup $G < P\Gamma L(n, q)$ that acts regularly on the points of $\mathcal{D}$. There are a number of non-Abelian such groups G when q is not prime. For a long time this was the only way known to construct non-Abelian difference sets. Later it was realized that certain Abelian difference set construction techniques didn't seem to "care" if the group was Abelian or not so long as a list of conditions were met.

At some point J. Dillon attributed the following conjecture to T. Storer.

The Storer conjecture: (Dillon)
There are no genuinely non-Abelian difference sets.

There is a second more important point that needs some clarification. **What is meant by genuinely non-Abelian?** I offer a hierarchy:

1. (Smith) The design does not admit a regular Abelian automorphism group.

2. The group has properties known to be incompatible with difference sets in an Abelian group.

3. (Dillon (Smith)) There are no Abelian difference sets with the same parameters.

4. The group is far from Abelian,for example, non-solvable.

To date the only successes in building difference sets that meet any of these criteria have been for the Hadamard/Menon parameter family: $(4n, 2n-n^{1/2}, n-n^{1/2})$. Not surprisingly, these constructions involve explicit groups and a lot of work with their representations:

The difference set in the modular group of order 64 (n=16) constructed by Smith [17] and the 2-group family it was generalized to by Davis and Smith [8] meets criterion 2 because the groups involved have exponent larger than the bound $2(log_2(exp(G)) - 2) < log_2(|G|)$ implied by work of Turyn [22] for Abelian groups. Later Davis and Iiams [7] gave a second family of difference sets in groups G where $|G| = 2^{4d+4}$, $exp(G) = 2^{3d+2}$ and so the Turyn bound for Abelian groups is violated more strongly.

The only non-Abelian difference set in print that meets criterion 3 is due to Smith [21] and has $G \leq AGL(1, GF(5^2))$ with parameters $(100, 45, 20)$. The accompanying computational work, as well as several other examples in different groups, is unpublished work of Shorter[20]. There are no Abelian difference sets with these parameters by a celebrated theorem of McFarland [19].

Each of these constructions breaks new mathematical ground and requires as substantial computation. Each has many unique features. We are content to only broadly describe the process that is used in these papers.

3.2 The Basic Recipe.

The basic steps that have been used to find genuinely non-Abelian difference sets in a given group G:

Identify sufficiently many $\mathbb{Z}G$ representations. This means that we must find explicit matrix representations $\phi \in \Omega$ of G so that $\delta \in \mathbb{Z}G$ is a solution to (DSE in $\mathbb{Z}G$) whenever it is a solution to (DSE under ϕ) for all $\phi \in \Omega$. It is highly desirable that these representations be unitary and that the matrix coefficients fall in as small a ring R as possible. These goals are sometimes in conflict and bad basis choices at this stage can make the subsequent steps intractable.

The optimal situation is that the representations be low degree and low rank permutation representations.

Reduce to finitely many solutions under each $\phi \in \Omega$. Take $\phi \in \Omega$. This step begins by classifying all solutions to the difference set equation under in the ring of matrices $\mathcal{M}$ over the coefficient ring R containing $\phi(\mathbb{Z}G)$. There may be infinitely many units in R, so one may have to find ways to invoke setness to complete this step.

One can often avoid exotic rings R by increasing the dimension of ϕ but this has the cost that $\mathcal{M}/\phi(\mathbb{Z}G)$ may grow large too.

Find elements of $\mathbb{Z}G$ mapping to each $\phi \in \Omega$. This important step produces what I call aliases $\{a_\phi | \ \phi \in \Omega\}$. In addition to revealing **bogus** solutions that are not in the $\phi(\mathbb{Z}G)$ it also returns the focus of attention to the $\mathbb{Z}G$ and the bases used in the earlier sufficient representations are no longer important.

Invert to global solution and get lucky. Each alias a_ϕ actually represents several potential solutions to (DSE under ϕ) under some normalization. For example, one typically only carries forward but one representative a_ϕ from $Ga_\phi G := \{ua_\phi v \ : \ u, v \in G\}$.

For each $|\Omega|$-tuple $\mathbf{a} = (a_\phi)_{\phi \in \Omega}$ of aliases, the inversion formula [15] produces the unique element $A \in \mathbb{Z}G$ such that $\phi(A) = \mathbf{a}_\phi$ for all $\phi \in \Omega$. One is left with trying all elements represented by a_ϕ, for all $\phi \in \Omega$. The challenge is to find ways to synchronize the left,right units for various ϕ so that A turns out to be a set.

In the known constructions, this synchronization is organized by a representation theoretic **sieve** based on normal series for the group G and contraction with respect to smaller and smaller normal subgroups. When the group is non-solvable **modular intertwining** seems to take up the slack.

4 Supporting Representation Theory.

To do constructive combinatorial representation theory we really have to work over the integers whenever possible. The current theory of integral representations is more theoretical and aimed more at interplay with structrual proerties of the group than directed toward combinatorial application. This section attempts to bridge some of the gap and to point to some standard sources.

A standard abstract algebra topic is the structure theory of modules of a principal ideal domain. When restricted to the integers and expressed in terms of matrices it is:

Theorem 4.1 *(Matrix normal forms:) Given $M \in Mat_{ab}(\mathbb{Z})$ there exist units $P, Q \in Mat(\mathbb{Z})$ and:*

1. *$Smith(M) := D := PMQ$ is zero off diagonal and has diagonal entries d_{ii} such that $d_{ii} | d_{i+1,i+1}$.*
2. *Each row of $Hermite(M) := PM$ has the same leading coefficient as $Smith(M)$.*

The geometric version of this theorem involves a $\mathbb{Z}$-**Lattice** Λ, a $\mathbb{Z}$-submodule of a free $\mathbb{Z}$-module. If Λ is the integral row space of the matrix M then the Smith normal form describes how to pick a basis $\mathcal{B}$ of $\mathbb{Z}^n$ (the matrix Q) and a basis L of Λ (the matrix P) so that L is linearly independent and spans Λ over $\mathbb{Z}$ and also if $x \in L$ then some $\mathbb{Q}$-multiple of x is in $\mathcal{B}$. The Hermite normal form describes what can be done if you can only work with the Λ basis L.

The integral group ring $\mathbb{Z}G$ is a $\mathbb{Z}$-lattice that is also a ring. A $\mathbb{Q}$-**algebra** $\mathcal{A}$ is a ring with center containing $\mathbb{Q}$ and of finite dimension as a $\mathbb{Q}$-vector space. A $\mathbb{Z}$-**order** in $\mathcal{A}$ is a subring of $\mathcal{A}$ that is a $\mathbb{Z}$-lattice (relative the inclusion $\mathbb{Z} \subset \mathbb{Q}$). Thus $\mathbb{Z}G$ is a $\mathbb{Z}$-order in $\mathbb{Q}G$.

The following theorem involves little more than the structure theory of modules of a principal ideal domain.

Theorem 4.2 *([4, 23.16]) Suppose M is a $\mathbb{Q}G$-module. Then there is a $\mathbb{Q}$-basis $\mathcal{B}$ of M with respect to which elements of $\mathbb{Z}G$ have matrices with integer entries.*

When one applies a coefficient ring homomorphism and reduces each matrix entry modulo an ideal π in the coefficient ring, one obtains an π-**modular** representation. The resulting modular representation depends on $\mathcal{B}$, but its composition factors do not.

Theorem 4.3 *(Brauer Nesbitt [4, 82.1]) Suppose the irreducible $\mathbb{Q}G$-module M is written over $\mathbb{Z}$ as above and then the matrix entries are reduced modulo p, for some prime $p \in \mathbb{Z}$. Then the composition factors of the resulting $GF(p)G$-module are uniquely determined by those of M. Moreover the resulting $GF(p)G$-module is irreducible whenever p does not divide $|G|$.*

The integral **decomposition matrix** of G has rows labeled by the irreducible $\mathbb{Q}G$-modules and columns labeled by irreducible $GF(p)G$-modules. The $\phi-$th row contains the multiplicities of the various irreducible $GF(p)G$-modules in the reduction of the ϕ modulo p.

Example 4.4 *(Decomposition Matrices)*
The 5*-modular integral decomposition matrix (bordered by degrees) of* S_5 *is:*

	1	3	5	5	3	1
1	1					
4	1	1				
5			1			
6		1			1	
5				1		
4					1	1
1						1

Complete explanation of this matrix appears in [13, sec 6.3]. We explain just the first two rows. The first row simply says that the trivial representation 1 *of* G *remains irreducible when reduced modulo* 5*. In the interest of happiness, we consider the natural permutation representation* η *of* S_5*. For* $g \in S_5$*,* $\eta(g)$ *is a* 5×5 *permutation matrix.*

The span of the all ones vector, $\mathbf{j}$ *and its orthogonal complement* $\mathbf{j}^{\perp}$ *are 1 and 4 dimensional* S_5*-invariant* $\mathbb{Q}$*-subspaces. Thus in characteristic* 0*,* η *decomposes into* 1 *and an irreducible* 4 *dimensional representation that we will call* 4*. However the integral representations* η *and 1+4 are not* $\mathbb{Z}$*-equivalent because the transition matrix from one* $\mathbb{Q}$*-basis to the other is not invertible over* $\mathbb{Z}$*.*

In fact, modulo 5*,* $\mathbf{j} \in \mathbf{j}^{\perp}$ *and so the* 5*-modular decomposition of* η *has a submodule series with factors of dimensions* $1/3/1$*. The* 3 *factor must be irreducible, so this a composition series, because* η *restricted to* S_4 *has the same structure in characteristic* 0 *as in characteristic* 5*, namely* $1+3+1$*. It follows that the reduction of* 4 *modulo 5 has irreducible composition factors of degrees* 1 *and* 3*, as indicated in the decomposition matrix.*

There is a more subtle point in Theorem 4.2 that leads to the idea of **bogus** solutions in combinatorial representation theory. Once $\mathcal{B}$ is chosen, we have a $\mathbb{Z}$-homomorphism $\psi_{\mathcal{B}}$ of $\mathbb{Z}G$ into the ring M of all integer matrices regarded as a $\mathbb{Z}$-module (corresponding to $\phi^* \otimes \phi$). The quotient module $M/im(\psi_{\mathcal{B}})$ is, apparently, not commonly studied, but it is nontrivial precisely when ϕ is decomposable.

The process of culling bogus solutions is nothing more than removing from consideration those candidates in M that are not in $im(\psi_{\mathcal{B}})$. This can be done in a number of ways some of which are more efficient than others. In the end they are all just another application of the matrix normal forms theorem, with $\Lambda = im(\psi_{\mathcal{B}})$.

4.1 Extending Coefficients.

A major focus of the foundations of representation theory is to extend the integral decomposition map to absolutely irreducible representations. By Brauer's Theorem, this requires that the coefficient ring must be changed to be at least $\mathbb{Z}[\zeta_m]$. Sadly, $\mathbb{Z}[\zeta_m]$ is to complicated and much more machinery (discrete valuation rings, completions, etc.) comes into play. It may be a worthwhile project to sort out just how much of this machinery is really necessary for the study of G-invariant relations.

Because $\mathbb{Z}$ is the fundamental group ring coefficient ring when studying combinatorial designs, combinatorists wishing to use the current representation theory must work in these more exotic rings only temporarily and ultimately return to $\mathbb{Z}$. There are essentially three ways that the coefficient ring is changed: moving toward a field of fractions (localization), moving to an algebraic extension and moving to a homomorphic image. We are mostly concerned about the first two because each of these has the cost to the combinatorist that extraneous solutions may be introduced and that setness information is lost. On the other hand the benefit to the representation theorist is that complete reducibility may be obtained.

Perhaps the best way to deal with this dilemma is to try to keep sufficient track of the movement so that one can "pull it all back" to $\mathbb{Z}$.

Example 4.5 *(Changing Fields)*
1. Let $H = \langle h : h^3 = 1\rangle$ and consider $\rho : \mathbb{Z}H \to Mat_{22}(\mathbb{Z})$ given by $\rho(h) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. Then ρ is irreducible but it becomes reducible if coefficients

are extended to $\mathbb{Z}[\zeta_3]$ $(\rho \otimes_{\mathbb{Z}} [\zeta_3])$.*(This means there is no integral matrix* P *but there is a* $\mathbb{Z}[\zeta_3]$ *matrix* P*, namely* $\begin{pmatrix} -\zeta_3 & -1 \\ 1 & 0 \end{pmatrix}$*, such that* $P^{-1}\rho(h)P$ *is properly block triangular.)*

Observe that $\rho(h)$ *is not diagonalizable until coefficients have been extended to include both* ζ_3 *and* 3. *Then* ρ *is completely reducible and its irreducible constituents are Galois conjugates. (Here this means that,* $\rho(h)$ *is diagonalizable and that its eigenvectors are conjugate under some* $\mathbb{Q}(\zeta_3)$*-automorphism.)*

2. Let G *be the group generated by the two matrices*

$$a := \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \; b := \frac{1}{2}\begin{pmatrix} -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 \\ 1 & 1 & 1 & -1 \end{pmatrix}.$$

Then $G = 2A_4$ *is the* **binary tetrahedral** *group. The matrix representation* (ρ) *of* G *afforded by these matrices is irreducible over* $\mathbb{Q}$*. When coefficients are extended to* $\mathbb{Q}(\zeta_4)$ *it is completely reducible. (This means there is a* $\mathbb{Q}(\zeta_4)$*-matrix* P *such that* $P^{-1}gP$ *is block diagonal for each* $g \in G$ *and that the representation afforded by each block is irreducible)*

However in contrast with the preceding example, there is **only one irreducible constituent** ϕ *having multiplicity 2. (This means that* P *may be chosen so that* ϕ *appears in both diagonal blocks of* $P^{-1}gP$*.) The matrix*

$$P = \begin{pmatrix} 1 & 1 & 1 & -1 \\ -\zeta_4 & \zeta_4 & -\zeta_4 & -\zeta_4 \\ -1 & 1 & 1 & 1 \\ -\zeta_4 & -\zeta_4 & \zeta_4 & -\zeta_4 \end{pmatrix}$$

leads to

$$\phi(a) = \frac{1+\zeta_4}{2}\begin{pmatrix} -1 & \zeta_4 \\ 1 & \zeta_4 \end{pmatrix}, \; \phi(b) = \begin{pmatrix} \zeta_4 & 0 \\ 0 & -\zeta_4 \end{pmatrix}.$$

Theorem 4.2 allows one to avoid localization as long as the coefficient ring is a principal ideal domain. Example 4.5.1 shows that the field hypothesis in the following theorem is necessary.

Theorem 4.6 *[12, 9.21] Suppose* F *is a field and* M *is an irreducible* FG*-module,* E *a splitting field (***arbitrary characteristic***). Then*

1. *$M^E(:= M \otimes_F E)$ is completely reducible.*

2. *The irreducible constituents of M^E are Galois conjugate and occur to equal multiplicity $m(M)$ (independent of E).*

3. *Let C be one of these constituents and let L be the fixed field of the E automorphisms leaving C invariant. Then The LG-module M^L has all constituents to multiplicity 1.*

The **Schur index** of M is $m(M)$. If M has non-trivial Schur index then the commuting algebra has coefficients in a non-trivial division ring $\mathbb{H}$. Example 4.5.2 has Schur index 2. It turns out that the presence of $\mathbb{H}$ makes it is much easier to solve the difference set equation under ϕ for representations ϕ with nontrivial Schur index.

A theorem of Wedderburn implies that the Schur index is always 1 in finite characteristic. In general, calculation of Schur indices is non-trivial and every natural number occurs as the Schur index of some representation of some finite group.

4.2 The Anti-isomorphism $^-$.

There is another obstruction to the use of integral representations as a way of keeping track of setness. The DSE under ϕ involves $\phi(D^-)$ which may or may not be $\overline{\phi(D)}^T$ because it is not automatic that ϕ be unitary. The fundamental theorem is due to Schur.

Theorem 4.7 *[4, p 49] If the coefficient ring contains $\mathbb{Q}$ then any representation of a finite group is equivalent to a unitary representation.*

Sadly this theorem is tight. There is a 3-dimensional representation ρ of alternating group A_5 that is realized as the symmetry group of a regular icosahedron. The representation ρ is orthogonal and therefore unitary, but Example 4.9 shows that Theorems 4.2 and 4.7 cannot be simultaneously satisfied.

On the other hand, for any integral representation $\rho : \mathbb{Z}G \to Mat_{n,n}(\mathbb{Z})$, there is a natural G-invariant symmetric bilinear form on $\mathbb{Z}^n$ defined by the matrix $M_\phi := \sum_{g \in G} \rho(g)^T \rho(g)$ and the Hasse-Minkowski theory of integral quadratic forms can be applied.

We may also consider the matrix valued function $Q : \mathbb{Z}G \to Mat_{n,n}(\mathbb{Z})$ defined by $Q(x) = \rho(x^-)\rho(x)$ and recognize that each of its entries defines a quadratic form $Q_{i,j}$ on the free $\mathbb{Z}$-module $\mathbb{Z}G$. When the representation ρ has nontrivial Schur index, Q must factor through the commuting division ring. This is **load lightening**. In particular, the $2A_4$-irreducible constituent ϕ appearing in Example 4.5.2 satisfies $\phi(x)\phi(x^-) = norm(x)$ where norm is a positive definite quadratic form in four variables each being $\mathbb{Z}$-linear in the x coefficients because G is a group of units in a quaternionic division order $\mathcal{O}$, whose existence is indicated by the nontrivial Schur index.

4.3 The Need for Happiness.

There is a more direct approach to the imperative of keeping track of setness. Define the **value set** $v(\rho) := \{(\rho(g))_{ij} \mid g \in G, \text{ for all } i, j\ \}$ for each matrix representation (ρ) and introduce formal variables x_λ for , $\lambda \in v(\rho)$. Define the **value enumerator** V_ρ to be the matrix having entries in $\mathbb{Z}[\ldots x_\lambda \ldots]$ given by

$$(V_\rho)_{ij} = \sum_{\lambda \in v(\rho)} |\{g \in G : \ \rho(g)_{ij} = \lambda\}| x_\lambda.$$

Note that the value set of a permutation representation π is $v(\pi) = \{0, 1\}$ If further, π is transitive of degree d then its value enumerator is given by $(V_\pi)_{ij} = ((1 - d^{-1})x_0 + d^{-1}x_1)|G|; 1 \leq i, j \leq d.$

Lemma 4.8 *Given the value enumerator of a representation ρ one can compute bounds on $(\rho(\Delta))_{i,j}$ for a subset $\Delta \subset G$ in that are linear in $|\Delta|$.*

Perhaps it is sufficient to find representations with really simple value enumerator. Unfortunately, I have no really effective idea how to achieve this rather vague objective. For this reason, I will call such a representation **happy**. Perhaps you will then accept that I cannot tell you what happiness is but only that I seem to be able to recognize it when I find it.. Happiness is highly basis dependent and therefore not spectral. **Perhaps, happiness is combinatorial.**

Example 4.9 *(Happiness)*
The group A_5 has absolutely irreducible representations of degrees $1, 4, 5, 3, 3$ in characteristic 0. Some of these representations are easily constructed from others as tensor products and Galois conjugates. Thus, one need only work

intensively with those of degrees $1, 4, 5, 3$. *The 1 is trivial and the* $4, 5$ *are best studied as constituents of permutation representations of degrees* $5, 6$. *We focus on the 3. The minimal degree monomial representation involving* 3 *has degree* 10. *and the image of* $\mathbb{Q}G$ *has dimension only 34, which is pretty small compared to* 10^2.

On the other hand the 3 *dimensional representation* ϕ *all by itself is realized by the group of of rotational symmetries of the regular icosahedron (dodecahedron). A matrix version* ρ *requires coefficients in* $\mathbb{Q}(\sqrt{5})$. *The ring of integers in this field is* $\mathbb{Z}[\sigma]$ *where* $\tau, \sigma = (1 \pm \sqrt{5})/2$ *are zeros of* $x^2 - x - 1$.

Define permutations having cycle decompositions $a := (12345), b := (254)$. *Then* $A_5 = \langle a, b \mid a^5 = b^3 = (ab)^2 = 1\rangle$. *The following matrices define an orthogonal version of* 3*:*

$$\phi(a) := \frac{1}{2}\begin{pmatrix} \sigma & -\tau & -1 \\ -\tau & 1 & \sigma \\ 1 & -\sigma & -\tau \end{pmatrix}, \ \phi(b) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

But $\phi(a)$ *is NOT integral. An equivalent integral representation is :*

$$\psi(a) := \begin{pmatrix} \sigma & \sigma & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}, \ \psi(b) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

But ψ *is not orthogonal. In fact, it is impossible to find a basis with respect to which this representation is both integral and orthogonal.*

The value sets and value enumerators of these representations are also independent of matrix position.

$$v(\phi) = \{0, \pm 1, \pm 1/2, \pm\sigma/2, \pm\tau/2\}, \qquad v(\psi) = \{0, \pm 1, \pm\sigma\},$$
$$(V_\phi)_{ij} = 8(v(\phi)) - 6(x_1 + x_{-1}); \qquad (V_\psi)_{ij} = 10v(\psi) + 10x_0.$$

It does seem that a key to happiness is to find a basis that your group prefers. Sometimes you can actually get the group to tell you this by studying the eigenspaces of its elements. For example, the first step in finding the bases in the above example was to realize that the normalizer of $\langle b\rangle$ could be monomial and to analyze the eigenspaces of its elements.

5 Icosahedral Difference Sets?

This section returns to the basic steps and describes how they play out in the search for difference sets with parameters (120,35,10) in groups with A_5 homomorphic images

The natural permutation representation π on 5 letters leads to four representative matrix solutions of the difference set equation under π. One of these is

$$M_5 = \begin{pmatrix} 10 & 8 & 6 & 4 & 7 \\ 8 & 7 & 6 & 10 & 4 \\ 6 & 6 & 11 & 6 & 6 \\ 7 & 4 & 6 & 8 & 10 \\ 4 & 10 & 6 & 7 & 8 \end{pmatrix}.$$

Similarly the permutation representation ρ on 6 letters leads to seven representative matrix solutions. For each of these, each representative represents any matrix obtained from it by arbitrary row and column permutations.

The orthogonal 3-dimensional representation ϕ leads to only six representative solutions, each of which represents any matrix obtained from it by left and/or right multiplication by group elements. One of these representatives together with a $\mathbb{Z}G$-alias is:

$$M_3 = \begin{pmatrix} -2 & 1 & 2\sqrt{5} \\ 4 & -2 & \sqrt{5} \\ \sqrt{5} & 2\sqrt{5} & 0 \end{pmatrix} \qquad \begin{array}{lll} -2(14)(23) & -4(12435) & +2(13452) \\ +2(24)(35) & -2(14325) & -4(12534) \\ +2(234) & -3(123) & -2(154). \end{array}$$

Perhaps some comment about the computation of integral aliases is appropriate. Suppose ϕ has degree d and is realized over R, and $m = [R : \mathbb{Z}]$. Regard $\phi(\mathbb{Z}G)$ as a lattice Λ in the md^2 dimensional vector space $\phi(\mathbb{Q}G)$. One must compute an integral basis $\mathcal{B}$ of Λ and express the matrix solutions from basic recipe step 2 in terms of $\mathcal{B}$.

Lemma 5.1 *One can compute an integral basis for Λ as follows: Form an $|G|$ by md^2 integer matrix M such that the g-th row consists of the entries $(\phi(g))_{\mathcal{B}}$ of $\phi(g)$ expressed in terms of a $\mathbb{Z}$-basis $\mathcal{B}$ of R. Augment M with an identity matrix to obtain $(M|I)$. Then every element of the integral row space of the resulting matrix M has the form $(\phi(\Sigma x_g g)_{\mathcal{B}}|\mathbf{x})$ where $\mathbf{x}$ has g-th coordinate x_g. The right hand portion of the d^2 rows that contain pivotal columns of the Hermite normal form (Integer analog of reduced row echelon form) of $(M|I)$ form an integral basis for $\phi(\ ZG)$.*

It turns out that the ρ survivor classes can be substantially reduced by culling bogus solutions not in the image of $\rho(\mathbb{Z}G)$.

The next step is to synchronize the different matrix solutions using modular intertwining.

Just as with S_5, the 5-modular decomposition of the natural permutation representation π of A_5 has a composition series $1/3/1$. Moreover, since $\sigma \equiv -2 \equiv \tau \ (mod\ 5)$, A_5 has a unique (absolutely) irreducible 5-modular representation ϕ of degree 3.

It follows that there is an **intertwining matrix** $A \neq 0$ such that

$$\pi(x)A \equiv A\phi(x) \ (mod\ 5, \mathbf{J}) \text{ for all } x \in \mathbb{Z}G.$$

In our case,

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & -1 \\ 0 & 0 & 0 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{pmatrix}.$$

By direct computation

$$M_5A = \begin{pmatrix} 2 & -1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 0 \\ -2 & 1 & 0 \\ -1 & -2 & 0 \end{pmatrix} \quad and \quad \begin{pmatrix} 2 & -1 & 0 \\ -1 & -2 & 0 \\ 0 & 0 & 0 \\ 1 & 2 & 0 \\ -2 & 1 & 0 \end{pmatrix} = AM_3.$$

Therefore the defining property of an intertwining matrix implies that the rows of M_5 must be permuted by the permutation (245) to obtain N_5 which is compatible with M_3. Because of the congruence modulo $\mathbf{J}$ any cyclic permutation of the rows of N_5 is also compatible with M_3. Moreover if the columns of M_5 are not permuted, then only these are compatible with M_3! This collapses the $(M_3, \sigma M_5 \tau)$ synchronization cases to 25 from $(5!)^2 = |\{(\sigma, \tau) : \sigma, \tau \in S_5\}|$.

To date no new difference set has found me in this search. I can only offer the element $s = s_1 - s_2 \in \mathbb{Z}A_5$ which satisfies the equation $ss^{-} = 25$.

$$\begin{aligned} s_1 &= (15324) + (13425) + (14352) + (12534) + (15243) + (13245) \\ &\quad +(142) + (243) + (152) + (134) + (354) + (123) \\ &\quad +(13)(24) + (14)(25) + (15)(24) \\ s_2 &= (13254) + (13452) + (12354) + (15342) \\ &\quad +(345) + (234) + (153) + (24)(35) + (13)(45) + (15)(34). \end{aligned}$$

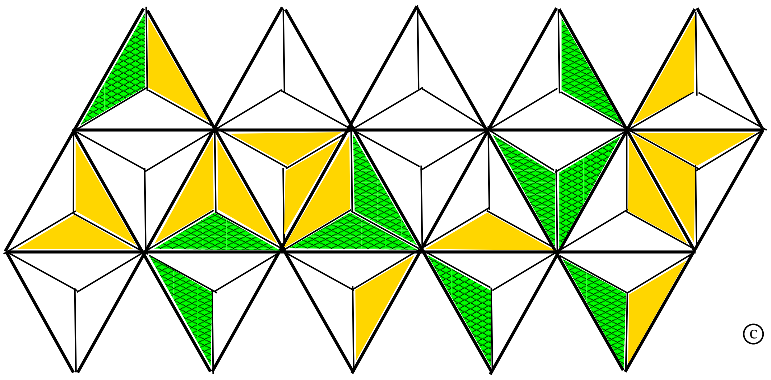

Figure 1: Icosahedral sequence with flat autocorrelation

A graphic illustration of this sequence is the coloring of the faces of an icosahedron in Figure 1. It has the property that if the colored positions are compared to those obtained by any rotation of the icosahedron then the number of regions having matching colors always equals the number of regions having mismatched colors (positions colored but once are ignored).

Problems

- Classify difference sets in groups of order p^3. (Xiang)
- Classify difference sets in groups of order $4p^2$. (Iiams)
- Classify difference sets in the finite subgroups of division algebras.
- Find more load lightening properties like the Schur index.
- Find non-Abelian building block analogs. (Smith)

Theorem 5.2 *Let D be a difference set of order $n = k - \lambda$ in G. Suppose $D \in Z(\mathbb{Z}G)$. Then D is a union of conjugacy classes $\mathcal{C}_1, \ldots \mathcal{C}_s$.*

Let $g_1, \ldots g_s$ be conjugacy class representatives and for each non-trivial character χ of G define

$$\lambda_i := \Sigma \chi_i(g_j)|\mathcal{C}_j| \in \mathbb{Z}[\zeta_{exp(G)}].$$

Then $\lambda_i/\chi_i(1)$ is an algebraic integer all of whose algebraic conjugates have modulus n.

Conjectures.

- If a difference set $D \in Z(\mathbb{Z}G)$ then G is Abelian.
- (Davis,Dillon) A 2-group has a difference set if all its Abelian (dihedral) homomorphic images satisfy Turyn's (Dillon's) Theorems.
- (Iiams) A 2-group G has a difference set only if

$$log_2(exp(G)/(G)) \leq 2/3.$$

- There exist nonsolvable difference sets.

References

[1] E. F. Assmus Jr. and J. D. Key, *Designs and Their Codes*,Cambridge Univ. Press, 1992

[2] R. Brauer, On the Representation of a Group of Order g in the Field of th g-th Roots of Unity. *Amer. J. Math.* **67** (1945); 243-250.

[3] R. C. Bruck, Difference Sets in a Finite Group. *Trans. Amer. Math. Soc.* **78** (1955), 464-481.

[4] C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras* J. Wiley, New York, 1966.

[5] C. W. Curtis and I. Reiner, *Methods of Representation Theory I,II* Wiley-Interscience, New York, 1981, 1987.

[6] A. Cushman, (private communication).

[7] J.A. Davis and J.E. Iiams, Hadamard Difference Sets in nonAbelian 2-groups with High Exponent, *J. Algebra* **199** (1998) 62–87.

[8] J.A. Davis and K.W. Smith, A Construction of Difference Sets in High Exponent 2-groups Using Representation Theory, *J. Algebraic Combin.* **3** (1994), 137–151.

[9] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory* Teubner, Leipzig, 1901 (reprint Dover, New York 1958).

[10] F. G. Frobenius, *Gesammelte Abhandlungen*, Springer Verlag, Berlin 1998, Band 3.

[11] T. Hawkins, New Light on Frobenius' Creation of the Theory of Group Characters, *Arch. History Exact Sci.*, **12**(1974), 217-243.

[12] I. M. Isaacs *Character Theory of Finite Groups*, Academic Press, New York, 1976

[13] G. James and A. Kerber, *The Representation Theory of the Symmetric Group*, Addison Wesley, London, (1981).

[14] R. A. Liebler, Relations Among the Projective Geometry Codes, in *Finite Geometries and Designs,* London Math. Soc. Lecture Notes Series **49** (1981), pp.221-225.

[15] R.A. Liebler, The Inversion Formula, *J. Combin. Math. and Combin. Computing* **13** (1993), 143-160.

[16] R.A. Liebler and R.A. Mena, Certain Distance-Regular Digraphs and Related Rings of Characteristic 4. *Journal of Comb. Theory,* Series A, **47** (1988), 111- 123.

[17] R. A. Liebler and K. W. Smith, On Difference Sets in Certain 2-groups, in *Coding Theory, Design Theory, Group Theory: Proceedings of the Marshall Hall Conference* ed. D Jungnickel, John Wiley & Sons, 1993.

[18] J. M. Maranda, On p-adic Integral Representations of Finite Groups, *Canad. J. Math.* **5** (1953), 344-355.

[19] R.L.McFarland, Difference Sets in Abelian Groups of Order $4p^2$, *Mitt. Math. Sem. Giessen* **192**(1989), pp. 1-70.

[20] T. Shorter, (Private communication).

[21] K. W. Smith, Non Abelian Hadamard Difference Sets. *Journal of Comb. Theory,* Series A, **70** (1995), 144- 156.

[22] R. Turyn, Character Sums and Difference Sets. *Pac. J. Math.* **15**, 319-346.

[23] M. Vincent, (private communication).