2017

A New Almost Difference Set Construction

David Clayton

University of Richmond

A New Almost Difference Set Construction

David Clayton

Honors Thesis[*]

Department of Mathematics & Computer Science

University of Richmond

[*] Under the direction of Dr. James A. Davis

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

James A Davis

(Dr. James Davis, thesis advisor)

Della Dumbaugh

(Dr. Della Dumbaugh, departmental reader)

V Nall

(Dr. Van Nall, honors coordinator)

Abstract

This paper considers the appearance of almost difference sets in non-abelian groups. While numerous construction methods for these structures are known in abelian groups, little is known about ADSs in the case where the group elements do not commute. This paper presents a construction method for combining abelian difference sets into nonabelian almost difference sets, while also showing that at least one known almost difference set construction can be generalized to the nonabelian case.

Contents

1 Introduction

Coding theory is a branch of mathematics that focuses on communicating efficiently across noisy channels. [8] Unlike cryptography, which studies methods to protect messages from observation by untrusted outside observers, work in coding theory involves accidental errors that may take place during transmission of digital messages. Codes can easily be made highly redundant to reduce the possibility of error, such as by having the transmitter repeat each bit 101 times and having the receiver assume whichever value in $\{0, 1\}$ appears more than 50 times is the correct bit that was originally intended. However, this is clearly not a very efficient way of encoding messages. In order to have useful error-correcting codes, there must be a balance between the redundancy of the message and the number of bits used to encode it.

Coding theory employs a variety of combinatorial structures in order to construct codes with these desirable properties. These properties may vary widely from one application to another, but certain structures have proven interesting enough both theoretically and in applications to merit decades of study by mathematicians. Currently, 3G and 4G mobile communications and satellite communications often rely on turbo codes for near-optimal efficiency of communication on a noisy channel. [1] These are close to the Shannon upper bound [1] for passing information efficiently through a noisy channel, using a combination of parity bits and a technique called convolution, which applies boolean functions to subsets of the input bits, to introduce large amounts of redundancy to the code while still allowing for efficient decoding. The Reed-Solomon code, used in digital storage devices such as CDs and DVDs, converts binary messages to polynomials in a finite field and evaluates the polynomial at several points in the field. [8] As long as the number of points at which the polynomial is evaluated is greater than the degree of the polynomial, redundancy has been introduced into the message and errors that may occur in transmission can be detected and corrected by checking the message received against the valid outputs of the polynomial function. [13]

[1] This is the maximum information transfer rate which allows for the existence of codes that make the probability of error arbitrarily small.

1.1 Difference Sets

One structure of particular interest in coding theory for its algebraic properties is the difference set. These structures were first identified in 1939 by Bose in his attempts to construct symmetric block designs [2]. However, specific examples of these structures were known somewhat earlier, as exemplified by the Paley DSs [12] which appear later in the paper.

Definition 1.1. A (v, k, λ) *difference set* (DS) is a subset D of size k taken from an order-v group such that the multiset $\{d_1 d_2^{-1} | d_1, d_2 \in D\}$ contains each nonidentity group element precisely λ times. [2]

An equivalent way of stating this difference property is to say that $|D \cap Dg| = \lambda$ for each nonidentity group element g. (Here, Dg represents $\{dg | d \in D\}$.)

Example 1.1. *The set $D = \{1, 2, 4\}$ is a $(7, 3, 1)$ DS in $(\mathbb{Z}_7, +)$. This DS has a deep connection to the Fano plane. The translations of D give the lines in the plane; other DSs give rise to similar finite geometries or symmetric designs.*

Informally, difference sets are a sort of opposite structure to a subgroup. While the differences of a subgroup are contained entirely within the original subgroup, a DS has differences spread as broadly and evenly as possible across the entire group.

DS applications arise in coding theory, among other applications. While Reed and Solomon originally envisioned their codes as polynomials in a finite field, an alternative construction takes a basic error-correcting code called the Reed-Muller code containing linear binary functions and appends carefully-chosen *bent functions* as different from linear functions as possible. These bent functions turn out to have a one-to-one correspondence with difference sets in groups of the form $\mathbb{Z}_2^n$.

Another application of (primarily cyclic) DSs stems from their optimal *autocorrelation* values. The intuitive idea of autocorrelation is a measure of how much overlap a set has with a translation of the same set. Formally, we first define a binary sequence s to be a finite sequence

[2] While this definition uses multiplication as the binary operation, we will use addition for some examples.

whose entries are elements of $\{0,1\}$. The autocorrelation of s when shifted by w bits is then $C_s(w) = \sum_{t \in \mathbb{Z}_n} (-1)^{s(t+w)-s(t)}$. In radar systems, this allows the receiver to determine exactly when the signal has bounced back off of an object by distinguishing the original signal from a time-shifted version of it. [11]

A set is said to have k-level autocorrelation if the autocorrelation function takes on k distinct values over all possible inputs. Low values of k are considered desirable in radar and similar applications. All DSs have $k = 2$ because the autocorrelation is equal to $2\lambda - v$ for all nonzero values of w. (The shifted sequence differs from the original sequence in all but λ places, so the sum consists of λ terms equal to 1 and $v - \lambda$ terms equal to -1.) This is as low a value of k as possible, indicating that DSs are optimal for this purpose. For maximum efficiency, it is often desirable to have the size of the difference set or almost difference set be close to half the size of the cyclic group in use. [11]

Many different construction methods for DSs are known, exploiting the algebraic or combinatorial properties of various structures. Some simple examples and properties of DSs follow immediately from the definition. For example, the empty set and any singleton set are clearly $\lambda = 0$ DSs, while the full group G as well as $G \setminus \{g\}$ for any group element g are DSs with $\lambda = v$ and $\lambda = v - 2$ respectively. These are trivial cases of the difference set construction and are generally ignored.

Slightly less trivial is the fact that the complement of any DS is also a DS. The usual proof of this makes use of the group ring $\mathbb{Z}[G]$. This structure, defined as the polynomials with integer coefficients whose variables are the group elements, allows for an easy treatment of multisets of group elements and shows up in the proofs of several DS properties and construction methods. Within the group ring, we abuse notation slightly by using D to refer not just to the difference set itself but also to the ring element $\sum_{d \in D} d$. Furthermore, define $D^{(-1)} = \sum_{d \in D} d^{-1}$. We can now write the difference property of a DS as an equation in the group ring: $DD^{(-1)} = k1_G + \lambda(G - 1_G)$. For the complement of a difference set we have

$$(G-D)(G-D)^{(-1)} = GG^{(-1)} - GD^{(-1)} - DG^{(-1)} + DD^{(-1)} = (v-2k)G + k1_G + \lambda(G - 1_G)$$

$$= (v-k)1_G + (v-2k+\lambda)(G-1_G)$$

So more specifically, the complement of a (v,k,λ) DS is a $(v, v-k, v-2k+\lambda)$ DS. It is also easy to show that both automorphisms and translations of DSs remain DSs of the same parameters. Translations do not change the differences between elements: for any h, $g_1g_2^{-1} = (g_1h)(g_2h)^{-1}$. Additionally, the structure-preserving property of automorphisms ensure that $\phi(g_1g_2^{-1}) = \phi(g_1)\phi(g_2)^{-1}$ and so $\phi(D)\phi(D^{(-1)}) = \phi(DD^{(-1)}) = \phi((k-\lambda)1_G + \lambda G) = (k-\lambda)1_G + \lambda G$. This means that applying any combination of translations and automorphisms to a DS results in another DS; for cyclic groups in particular, this corresponds to adding or multiplying a constant value to each element of the DS.

Besides these very basic results, dozens of more sophisticated construction methods have been demonstrated as the theory of DSs has developed. However, the most general questions in the field remain unresolved: Given an arbitrary group, can we determine whether it has a DS? If it does, how might it be constructed?

1.2 Almost Difference Sets

Precise answers to the DS existence and construction questions remain unknown. Several infinite DS families have been found and the existence of DSs in some groups is known to be impossible, as described in Chapter 2. However, no fully general method is known to prove the (non)existence of DSs in an arbitrary group. Furthermore, the nonexistence results that are known, together with brute force computer searches in small groups, indicate that most groups do not contain DSs. In these groups we would like to find those algebraic structures with properties as close as possible to those of a DS, a consideration which leads to the study of almost difference sets (ADSs). [7]

Definition 1.2. A (v,k,λ,t) *almost difference set* (ADS) is a subset A of size k taken from an order-v group such that the multiset $\{d_1d_2^{-1} | d_1, d_2 \in D\}$ contains t of the nonidentity group elements λ times and all other nonidentity group elements $\lambda+1$ times. We define S to be the set of group elements appearing precisely t times.

Because t can range from 0 to $v-1$, this gives us a great deal more flexibility in constructing ADSs. If t is in fact equal to either 0 or $v-1$, then the resulting structure is an ordinary DS.

Example 1.2. *The set $D = \{0, 2, 3, 8, 9, 11\}$ is a $(13, 6, 2, 6)$ ADS in $(\mathbb{Z}_{13}, +)$. In this case $S = \{1, 3, 4, 9, 10, 12\}$ are the elements generated twice by the differences of D.*

The notion of an ADS is a recent one. A similar structure known as a divisible difference set (DDS) has the property that the difference multiset $\{d_1 d_2^{-1} | d_1, d_2 \in D\}$ contains the nonidentity elements of some subgroup H exactly λ_1 times and all other nonidentity elements λ_2 times, for some λ_1 and λ_2. Davis [3] originally defined an ADS as a DDS where $|\lambda_1 - \lambda_2| = 1$, while around the same time Ding [4] defined an ADS in a way similar to the current definition, but with the added requirement that $t = \frac{v-1}{2}$. These two early definitions were broadened into the current definition by Ding, Helleseth, and Martinsen. [6]

In terms of autocorrelation, ADSs have 3-level autocorrelation if they are not full DSs. This is because translation by the identity produces a correlation value of v (since each digit of the sequence aligns with itself) while all other translations produce either $2\lambda - v$ or $2(\lambda + 1) - v$ (the argument is similar to that for a DS). This means that, when DSs are not known to exist, ADSs provide optimal autocorrelation for applications.

Another application of these structures is in secret-sharing schemes. These schemes allow several parties to create a shared secret, which can only be decrypted and revealed if a sufficient number of involved parties collaborates by using their private keys. ADSs give rise to linear codes which can be used to encode messages in precisely this way; in this case decryption is simply solving a system of linear equations in a finite field, which can be done if enough people combine information. [5]

As with ordinary DSs, taking any combination of complements, automorphisms, and translations of an ADS preserves the ADS property. And as with difference sets, we can express the difference property through an equation in the group ring:

$$DD^{(-1)} = (k - \lambda - 1)1_G + (\lambda + 1)G - S$$

Additionally, we can define concepts like multipliers and developments as we would for DSs.

As might be expected, problems of existence and construction for ADSs in arbitrary groups are even less well-understood than for DSs. The significantly weaker difference property required, along with the relatively recent development of the ADS concept, means that the theory of ADSs is still poorly understood.

2 Survey of Previous Results

Most of the research in DSs and ADSs has focused on abelian groups. Because all such groups are isomorphic to direct products of cyclic groups, these have a great deal of structure which can be exploited when constructing or proving the nonexistence of ADSs. Special even among these abelian groups are those which are actually the additive groups of a finite field. These have so much additional structure imposed on them that a great many construction methods are known, although even in these cases the full theory of ADSs is not entirely understood.

2.1 Important Construction Methods

Some of the earliest constructions of DSs and ADSs were given by Paley.

Theorem 2.1. *Let $q \equiv 3 \mod 4$ be a prime power. Then the set $D = \{f^2 | f \in GF(q) \setminus \{0\}\}$ is a $(q, \frac{q-1}{2}, \frac{q-3}{4})$ DS.*

Theorem 2.2. *Let $q \equiv 1 \mod 4$ be a prime power. Then the set $D = \{f^2 | f \in GF(q) \setminus \{0\}\}$ is a $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{2})$ ADS, where all nonsquares appear $\frac{q-5}{4}$ times in the differences and all nonzero squares appear $\frac{q-1}{4}$ times.*

Proof: [9] First, note that for any square $g_1 \in GF(q)$, there is a one-to-one correspondence between pairs $f_1 - f_2$ that produce a difference of g_1 and pairs that produce any other square g_2 given by the automorphism $a(x) = g_2 g_1^{-1} x$. Given that f_1 and f_2 are squares, $a(f_1)$ and $a(f_2)$ are products of squares and will therefore be squares themselves. This correspondence shows that all squares must appear equally many times in the differences generated by D. We can therefore without loss of generality consider the case of $g_1 = 1$ to determine how many times each square is generated.

Let S be the set of solutions to $x^2 - y^2 = 1$ in the finite field. We can implement the change of coordinates given by $(u, v) = (x + y, x - y)$ to simplify this equation. The transformation matrix $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ has determinant -2, which is nonzero because q is in either case an odd prime power, and so the change is invertible. So $x^2 - y^2 = 1$ has the same number of solutions as $uv = 1$. Clearly there is one such solution for each nonzero element of the field, so $|S| = q - 1$.

However, simply counting the solutions to $x^2 - y^2 = 1$ leads to overcounting the number of pairs (x^2, y^2) with a difference of 1. Replacing x by $-x$, replacing y by $-y$, or replacing both at once yields the same pair (x^2, y^2), so we overcount by a factor of 4 except when x or y is 0. The case of $y = 0$ yields $x = \pm 1$, while the case of $x = 0$ gives $y^2 = -1$. This latter possibility can only occur when -1 is a square, i.e. when $p \equiv 1 \mod 4$. Each of these leads to an overcount by a factor of only 2 for that particular case. So if $q \equiv 3 \mod 4$, 1 appears as a difference of squares $\frac{(q-1)+2}{4} = \frac{q+1}{4}$ times and if $q \equiv 1 \mod 4$ it appears $\frac{(q-1)+4}{4} = \frac{q+3}{4}$ times. Note that exactly one of each of these is the pair $(1, 0)$, which is excluded because D only includes nonzero squares, so 1 appears as a difference of elements in D $\frac{q-3}{4}$ and $\frac{q-1}{4}$ times, respectively.

Because there are precisely $\frac{(q-1)(q-3)}{4}$ possible differences, we can then verify the number of times the nonsquares appear as well. □

The appearance of Paley DSs in an infinitely large family of abelian groups allows the construction method described in the paper to make use of them to construct arbitrarily large ADSs.

Finite fields provide an especially elegant construction method for both DSs and ADSs through the method of cyclotomy. For a prime power r, an integer $N > 1$ dividing $r - 1$, and a primitive element α of $GF(r)$ (i.e. a generator of the multiplicative group), we define the cyclotomic classes $C_i^{(N,r)} = \alpha^i \langle \alpha^N \rangle$ for $i = 0, 1, \ldots, N - 1$. These classes give us a variety of construction methods for both DSs and ADSs. Typical examples include the two following theorems.

Theorem 2.3. *Let t be an odd integer such that $q = 4t^2 + 1$ is a prime power. Then $C_0^{(4,q)}$ is a $(q, \frac{q-1}{4}, \frac{q-5}{16})$ DS in $GF(q)$. [10]*

Theorem 2.4. *Let y be an odd integer such that $q = 25 + 4y^2$ or $q = 9 + 4y^2$ is a prime power. Then $C_0^{(4,q)}$ is a $(q, \frac{r-1}{4}, \frac{q-13}{16}, \frac{q-1}{2})$ ADS in $GF(q)$. [7]*

For example, since $37 = 4(3)^2 + 1$ is a prime power and 2 is a primitive element of $GF(37)$, we can construct the $(37, 9, 2)$ DS given by $D = 2^0\langle 2^4\rangle = \{1, 7, 9, 10, 12, 16, 26, 33, 34\}$.

In fact, the Paley constructions themselves turn out to be cyclotomic in nature. The squares of a finite field are simply $C_0^{(2,r)}$ and therefore both of the above Paley constructions are simply a special type of cyclotomic construction. However, neither these nor other cyclotomic constructions provide immediate insight on the construction of ADSs in nonabelian difference sets. Cyclotomy relies on the multiplicative properties of a finite field, and nonabelian groups necessarily do not permit a field structure.

One construction method for ADSs similar to the one discussed in this paper uses DSs to construct ADSs in a larger product group.

Theorem 2.5. *Let A and B be $(k, \frac{k+1}{2}, \frac{k+1}{4})$ or $(k, \frac{k-1}{2}, \frac{k-3}{4})$ DSs in a group G, and let B^c be the complement of B in G. Then $D = (\{0, 2\} \times A) \cup (\{1\} \times B) \cup (\{3\} \times B^c)$ is a $(4k, 2k+1, k+1, k-1)$ or $(4k, 2k-1, k-2, k-1)$ ADS in $\mathbb{Z}_4 \times G$. [14]*

Progress has also been made in finding construction methods for *planar* ADSs, where $\lambda = 0$. These planar ADSs have the unique property that differences of their elements are all distinct, which is not shared by other ADSs and which makes for unique construction methods such as the following.

Theorem 2.6. *Let $q > 2$ be a prime power and α be a generator of $GF(q)^*$. Then $D_q = \{0 \leq i \leq q^2 - 2 | \mathrm{Tr}(\alpha^i) = 1\}$ is a $(q^2 - 1, q, 0, q - 2)$ ADS in $\mathbb{Z}_{q^2-1}$. [7]*

While several other methods similar to the ones above are known, deeper connections between

ADS construction methods have yet to be understood. While paths have been found leading to distinct ADS families, the full region of ADSs has yet to be mapped.

2.2 Requirements and Nonexistence Proofs

The most obvious constraint on the existence of DSs is that there are exactly $v-1$ nonidentity group elements and $k(k-1)$ differences that can be formed from the DS, and that therefore $k(k-1) = \lambda(v-1)$ for all DSs. This immediately precludes many groups from having difference sets of any sort. For example, no group of order $v = 12$ can have a nontrivial DS because $v-1$ does not divide $k(k-1)$ for any $1 < k < 11$.

This approach is less effective with almost difference sets, however. The analogous criterion is $k(k-1) = (\lambda+1)(v-1) - t$, and because t can be any value between 0 and $v-1$ there is always a way to satisfy this equation for a given triple (v, k, λ).

More helpful constraints can be derived by looking at the quotient of the group by various normal subgroups. While the paper referenced deals with cyclic groups exclusively, the same technique applies to normal subgroups of arbitrary groups. Given $N \lhd G$ with $|G| = a|N|$, we can represent the cosets of N as $g_0N = N$, g_1N, …, $g_{a-1}N$ for some group elements g_i. Suppose a (v, k, λ, t) ADS A exists in this group. We can then define constants $b_g = |A \cap gN|$ and $c_g = |S \cap gN|$, where S is the set of group elements appearing only λ times in the multiset of differences. From this and the definition of an ADS we can construct a system of equations involving the b_g and c_g. Specifically, manipulation of values in the group ring tells us that

$$\sum_{g \in G/N} c_g = t$$

$$\sum_{g \in G/N} b_g = k$$

$$\sum_{g \in G/N} b_g^2 = k + (a-1)(\lambda+1) - c_{1_G}$$

$$\sum_{g \in G/N} b_g b_{gh^{-1}} = a(\lambda+1) - c_h \quad (h \in (G/N) \setminus N)$$

The first two follow immediately from the definitions of an ADS. Next, note that $DD^{(-1)} = (k-\lambda-1)1_G + (\lambda+1)G - S$ gives rise to $DD^{(-1)} = (k-\lambda-1)1_G + (\lambda+1)aN - \sum_{g \in G/N} c_g g$ in the quotient of G by the normal subgroup. The coefficient of 1_G in this polynomial is then $k + (a-1)(\lambda+1) - c_{1_G}$, while the coefficient of each other h is $a(\lambda+1) - c_h$. We also have, again after forming the quotient group, that $D = \sum_{g \in G/N} b_g g$ and $D^{(-1)} = \sum_{g \in G/N} b_g g^{-1}$. But the coefficient of 1_G when these two polynomials are multiplied is simply b_g^2. This gives the third equality. The coefficients of other $h \in G/N$ are given by $\sum_{g \in G/N} b_g b_{gh^{-1}}$, which establishes the fourth equality as well.

If this system can be shown to have no solutions, then no ADS with the given parameters can exist in the group.

Example 2.1. *There is no* $(68, 12, 1, 2)$ *ADS in* $\mathbb{Z}_{68}$*. This is shown by taking the quotient with respect to* $\langle 34 \rangle$ *and observing that the system of equations given by*

$$c_0 + c_1 = 2$$

$$b_0 + b_1 = 12$$

$$b_0^2 + b_1^2 = 78 - c_0$$

$$2b_0 b_1 = 68 - c_1$$

has no solutions in the natural numbers. Clearly we cannot have $c_1 = 1$ *because the fourth equality shows* $68 - c_1$ *must be even. Then* c_2 *is either 0 or 2. But neither 76 nor 78 is the sum of two squares, so this system has no solutions. Therefore no ADS with these parameters exists in the group.*

This example shows that even when the value of t is chosen to fulfill the $k(k-1) = (\lambda+1)(v-1) - t$ criterion, it is still possible for no such ADSs to exist. Furthermore, an identical system of equations is generated by the abelian group $\mathbb{Z}_{34} \times \mathbb{Z}_2$ as well as the dihedral group D_{68} and one group of the form $\mathbb{Z}_{17} \rtimes \mathbb{Z}_4$, so an ADS with these parameters is immediately ruled out in each of these groups as well. While this test demonstrates nonexistence for several seemingly possible sizes of ADS, it is still imperfect. For example, a computer search reveals that no $(17, 6, 1, 2)$ ADS exists in $\mathbb{Z}_{17}$. This could not be ruled out by the quotient criterion because $\mathbb{Z}_{17}$ is a simple group.

This technique can also be used in the other direction, to help construct an ADS that is suspected to exist. For example, suppose we wish to find a $(16, 8, 3, 4)$ ADS in the modular group $\mathbb{Z}_8 \rtimes \mathbb{Z}_2$ given by $\langle a, x | a^8 = x^2 = e, ax = xa^5 \rangle$. We can form the quotient of the group by $\mathbb{Z}_2$ and find the system of equations

$$c_0 + c_1 = 4$$

$$b_0 + b_1 = 6$$

$$b_0^2 + b_1^2 = 36 - c_0$$

$$2b_0b_1 = 32 - c_1$$

The integer solution pairs to this are $(3, 5)$, $(4, 4)$, and $(5, 3)$. This tells us that if an $(16, 8, 3, 4)$ ADS exists, between 3 and 5 elements must be in the normal subgroup $\langle a \rangle$, immediately eliminating the 1698 combinations where more than 5 or fewer than 3 elements are in the normal subgroup. The search space can be further reduced by examining smaller quotient groups.

Other requirements can be derived from character theory. This area of mathematics uses *characters*, defined as homomorphisms $\chi : (G, \circ) \to (\mathbb{C} \setminus \{0\}, \times)$, to study the properties of groups. The *principal character* is the unique homomorphism χ_0 such that $\chi_0(g) = 1$ for all g. We can extend the action of a character on a group to the group ring in the natural way ($\chi(\sum a_i g_i) = \sum a_i \chi(g_i)$), and from there we find the following remarkable result.

Theorem 2.7. *Let χ be a non-principal character of a finite group G. Then $\chi(G) = 0$.*

Proof: Let G be a finite group with identity element e. The finite size of the group tells us that for all group elements g there is a positive integer a with $g^a = e$. In terms of characters, there is some a such that $\chi(g)^a = 1$. This tells us that each group element is mapped to a root of unity. The multiplicative group generated by any finite set of roots of unity is cyclic, so there is some $\chi(g)$ such that $\chi(G) = \sum_i \chi(g^i)$. But the sum over the powers of a root of unity is always 0, so $\chi(G) = 0$. □

Given the group ring expression of the ADS property given in chapter 1, we can apply a nonprincipal character to each side to find that $\chi(DD^{(-1)}) = (k - \lambda - 1) - \chi(S)$ and therefore (because χ is a homomorphism) $|\chi(DD^{(-1)})|^2 = (k - \lambda - 1) - \chi(S)$. This in turn allows the development of ADS criteria such as the following. [15]

Theorem 2.8. *In a cyclic group $\mathbb{Z}_v$ of even order, a (v, k, λ, t) ADS can only exist if*

- *t is even and there is at least one square in the set $\{k - \lambda - (t + 1 - 4l) | 0 \leq l \leq \frac{t}{2}\}$;*
- *t is odd, v is a multiple of 4, and there is at least one square in the set $\{k - \lambda - (t + 1 - 4l) | 0 \leq l \leq \frac{t-1}{2}\}$; or*
- *t is odd, v is not a multiple of 4, and there is at least one square in the set $\{k - \lambda - (t - 1 - 4l) | 0 \leq l \leq \frac{t-1}{2}\}$.*

While these proofs help to rule out the existence of ADSs in a few particular cases, very little work has been done with nonabelian groups in general. Even many results which can be generalized to arbitrary groups, such as the quotient method above, are often stated in terms of abelian or even cyclic groups specifically. This is partially because of the mathematical difficulties of nonabelian groups and partially because of the relative lack of applications for the noncommutative case. However, the nonabelian case is still interesting from a mathematical perspective, given the greater variety of groups under consideration. In the next chapter we will look at a variety of ways of dealing with ADSs and similar structures using computer algebra systems such as GAP, revealing many interesting types of ADS only found in nonabelian groups.

3 Methods of Working with ADSs

3.1 GAP

Using the abstract-algebra-focused programming language GAP (‘Groups, Algorithms, Programming’), it was possible to search ADSs in small groups in an automated manner, iterating through every possible subset of the group and checking whether it formed an ADS.

This brute force search was able to easily find all ADSs of each possible size in all groups with size $v \leq 23$. Furthermore, a greedy algorithm was able to check whether at least one ADS of each size existed in groups as large as $v = 28$. The table in the appendix lists the number of ADSs of size k in each group, up to automorphism and translation. Groups are sorted first in order of size, and second by their GAP ID number. Only ADSs with $k \leq \frac{v}{2}$ are listed, since each ADS larger than that is simply the complement of an ADS with $k < \frac{v}{2}$. For the later entries, * is used to indicate that at least one ADS of that size exists, but the total number is unknown. In these cases finding all equivalence classes of ADSs of the given size proved computationally prohibitive, but it was possible to iterate through combinations of group elements until an ADS was found.

In general, at least one ADS exists for almost every combination of v and k, given the right choice of group. But clearly some types of group tend to have more ADSs than others. On one end it is easy to show that $\mathbb{Z}_2^n$ cannot have any ADSs that are not DSs. This is because $ab^{-1} = ba^{-1}$ for all elements of such a group, and for any set D the differences generated by the elements of D must cover each group element an even number of times. This means that while DSs can exist as long as λ is even, it is impossible for one group element to appear λ times while another appears $\lambda + 1$ times.

Other groups, like the dihedral D_n, also have few ADSs. This is not especially surprising, since in $\langle a, x | a^{\frac{n}{2}} = x^2 = e, ax = xa^{-1} \rangle$ about half of all pairs (g_1, g_2) satisfy the property $g_1 g_2^{-1} = g_2 g_1^{-1}$, and again these ensure even multiplicities that make ADSs unlikely unless all of the elements align in precisely the right way. Conversely, the cyclic groups almost always have at least as many ADSs of each size as each other group of the same order. It is less clear why this should be the case, but it does indicate the rich variety of cyclic ADSs compared to ADSs in many other groups.

3.2 The Greedy Algorithm

One of the most obvious ways of attempting to construct an ADS is to add elements into a set one at a time in such a way that each new addition to the set preserves the ADS property. When it is impossible to add another element to the set in this way, the program may either terminate and return the ADS it has found or backtrack in the hopes of finding a larger ADS using different initial elements.

Unfortunately, this method scales extremely poorly. While better than brute force, it still requires enough computation time that the groups evaluated only grew in size from $v = 23$ to $v = 28$ when switching from brute force to greedy methods. The odds of producing a large ADS using the greedy algorithm without backtracking are vanishingly small, since the number of possible difference collisions grows as $O(n^4)$ with the size of the ADS being created.

Interestingly, it is only in the finite case that the greedy algorithm proves infeasible. Exploiting transfinite induction allows us to 'greedily' construct infinitely large ADSs in a variety of infinite abelian groups.

3.3 ADS Properties

As an interesting non-example of a general ADS construction, suppose we notice that in the group $\mathbb{Z}_3 \rtimes \mathbb{Z}_8$ given by the presentation $\langle a, x | a^3 = x^8 = e, ax = xa^{-1} \rangle$ there exist $(24, 12, 5, 6)$ ADSs. One example of such an ADS is

$$A = \{a, a^2, x, a^2x, a^2x^2, x^3, a^2x^3, x^4, ax^4, x^5, a^2x^5, x^6\},$$

whose differences generate the elements of $\{a, a^2, ax^2, a^2x^2, ax^6, a^2x^6\}$ 5 times and all other group elements 6 times. A reasonable conjecture, especially in light of the ADS construction method outlined in chapter 4, is that A is part of a general ADS family of the form

$$A = (H - D_1) \cup D_2x \cup (H - (D_1 \cup \{h\}))x^2 \cup D_2x^3 \cup (D_1 \cup \{h\})x^4 \cup D_2x^5 \cup D_1x^6$$

where D_1, D_2, and $D_1 \cup \{1_H\}$ are DSs in $H = \mathbb{Z}_3$ with parameters $(4\lambda+3, 2\lambda+1, \lambda)$, $(4\lambda+3, 2\lambda+2, \lambda+1)$, and $(4\lambda+3, 2\lambda+2, \lambda+1)$ respectively. However, we can easily show that these structures do not in general form ADSs, since the portion of $AA^{(-1)}$ contained in the coset Hx^2 of the normal subgroup H is

$$(H - D_1)(D_1x^6)^{(-1)} + (H - D_1 - h)x^2(H - D_1)^{(-1)} + D_2x^3(D_2x)^{(-1)}$$

$$+(D_1 + h)x^4((H - D_1 - h)x^2)^{(-1)} + D_2x^5(D_2x^3)^{(-1)} + D_1x^6((D_1 + h)x^4)^{(-1)}$$

$$= x^2 \left(HD_1^{-1} + HH - HD_1^{(-1)} - D_1H - hH + D_2D_2^{(-1)} \right.$$

$$\left. + D_1H + hH - 1_H + D_2D_2^{(-1)} \right)$$

$$= ((4\lambda+3)H - 1_H + 2((2\lambda+2)1_H + (\lambda+1)(H - 1_H)))x^2$$

$$= ((8\lambda+6)1_H + (6\lambda+5)(H - 1_H))x^2$$

Clearly as λ increases the values $(8\lambda + 6)$ and $(6\lambda + 5)$ will separate from each other, preventing any other structures formed this way from being an ADS. While it is still possible this ADS is part of a larger family, any such family cannot have a structure like the one described here.

For an example of a construction that can be shown to work using the group ring and the combinatorial properties of an ADS, see Chapter 4.

3.4 Infinite ADSs

The one case where we can use a greedy algorithm to construct ADSs is when the sets involved are infinite. In this case we can use transfinite induction to demonstrate that the construction must produce an ADS, which can even be infinitely large in groups with the correct properties.

Theorem 3.1. *Let G be a well-ordered abelian group and let $S = \{g^2 | g \in G\}$ be infinite. Then there exists a $(|G|, |S|, 0, t)$ ADS in G for some possibly infinite t.*

This follows from transfinite induction. Begin by defining $A_0 = \varnothing$. For each ordinal α with cardinality below $|S|$, we construct $A_{\alpha+1} = A_\alpha \cup \{a_\alpha\}$ where $a_\alpha \notin A_\alpha$ is chosen so that $A_{\alpha+1}$ has no repeated differences (i.e. is a planar ADS). Furthermore, for each limit ordinal β we define $A_\beta = \bigcup_{\alpha<\beta} A_\alpha$. In particular we claim that if γ is the least ordinal of cardinality $|S|$, A_γ is a $(|G|, |S|, 0, t)$ ADS. Because A_0 is trivially an ADS and A_β will always be an ADS if each A_α with $\alpha < \beta$ is an ADS, we need only prove that for any $\alpha < \gamma$ we can always choose an a_α that will keep $A_{\alpha+1}$ an ADS.

The only way $A_{\alpha+1}$ can fail to be an ADS is if some group element g appears multiple times in the differences. Given that A_α is a planar ADS, this is only possible if all but one of the differences producing g includes a_α. There are three cases to consider.

First, it is possible that $a_\alpha b^{-1} = cd^{-1}$ for some $b, c, d \in A_\alpha$. This can only occur when $a = bcd^{-1}$. Second, a collision can occur if $a_\alpha b^{-1} = a_\alpha c^{-1}$ for distinct $b, c \in A_\alpha$. But this is clearly impossible by group properties. Third, we may have $a_\alpha b^{-1} = c a_\alpha^{-1}$ for $b, c \in A_\alpha$. This is equivalent to saying $a_\alpha^2 = bc$.

There are $|A_\alpha^2|$ ways to choose a pair $b, c \in A_\alpha$, and so only $|A_\alpha^2| < |S|$ possible squares that can be produced by a product of the form bc. So there are at least $|S|$ elements of S not produced in this manner, and (by the definition of S) at least $|S|$ group elements which do not square to an element of the form bc for $b, c \in A_\alpha$.

Within these $\geq |S|$ group elements, there can be at most $|A_\alpha|$ which are already in A_α and at most

$|A_\alpha^3|$ which are of the form bcd^{-1} for some $b, c, d \in A_\alpha$. But again both of these are smaller than $|S|$, so there are at least $|S|$ group elements not of this form. Any of these elements may be chosen as a_α, since it cannot cause any of the three cases of repeated differences and so $A_{\alpha+1}$ is guaranteed to be a planar ADS.

By transfinite induction, $A = A_\gamma$ is a $(|G|, |S|, 0, t)$ ADS for some t.

Theorem 3.2. *Let G be an infinite well-ordered abelian group where all nonidentity elements have order greater than 2. Then there exists a $(|G|, |G|, 1)$ DS in G.*

Note that because each nonidentity element has order above 2, $S = \{g^2 | g \in G\}$ has the same cardinality as G. Furthermore, we can assume WLOG that the order type of G is γ, the least ordinal of cardinality $|G|$. Any such well-order will also provide a well-order for S with order type no greater than γ.

This theorem also follows from transfinite induction. In this case we start with $D_0 = \{1_G\}$ and construct $D_{\alpha+1} = D_\alpha \cup \{g_\alpha, d_\alpha g_\alpha\}$ and $D_\beta = \bigcup_{\alpha<\beta} A_\alpha$ for nonzero limit ordinals β. Here d_α is the first group element not generated by the differences of A_α and g_α is an arbitrary group element not in A_α, whose inclusion ensures that $(d_\alpha g_\alpha)g_\alpha^{-1} = d_\alpha$ is generated by the differences of $A_{\alpha+1}$. Because we iterate over γ, each group element must be produced by some difference of elements in D_γ. Again D_0 has no repeated differences and D_β can have no repeated differences given that the D_α do not, so we need only prove that a pair of g_α and $d_\alpha g_\alpha$ can always be chosen in a way that $A_{\alpha+1}$ has no repeated differences either.

There are significantly more ways for $\{g_\alpha, d_\alpha g_\alpha\}$ to cause repeated differences than for $\{a_\alpha\}$ in the previous theorem:

- $g_\alpha a^{-1} = bc^{-1}$
- $(d_\alpha g_\alpha)a^{-1} = bc^{-1}$
- $(d_\alpha g_\alpha)g_\alpha^{-1} = ab^{-1}$

- $ag_\alpha^{-1} = g_\alpha b^{-1}$
- $(d_\alpha g_\alpha)g_\alpha^{-1} = g_\alpha a^{-1}$
- $a(d_\alpha g_\alpha)^{-1} = g_\alpha b^{-1}$
- $g_\alpha(d_\alpha g_\alpha)^{-1} = g_\alpha a^{-1}$
- $a(d_\alpha g_\alpha)^{-1} = (d_\alpha g_\alpha)b^{-1}$
- $g_\alpha(d_\alpha g_\alpha)^{-1} = (d_\alpha g_\alpha)a^{-1}$
- $g_\alpha(d_\alpha g_\alpha)^{-1} = (d_\alpha g_\alpha)g_\alpha^{-1}$

It is nonetheless unsurprising that each of these is either impossible or precludes only $|A_\alpha^n| < |G|$ group elements for some finite n, so there will always be $|G|$ group elements remaining to choose as g_α. For example, the second of these possibilities simplifies to $g_\alpha = abc^{-1}d_\alpha^{-1}$, which precludes only $|A_\alpha^3|$ group elements, while the last simplifies to $d_\alpha^2 = e$, which is impossible because we required all nonidentity elements to have order above 2. Furthermore the fact that $1_G \in D_0$ means that d_α is a nonidentity element and so the elements of the pair $\{g_\alpha, d_\alpha g_\alpha\}$ are in fact distinct. So, again by transfinite induction, $D = D_\gamma$ is a $(|G|, |G|, 1)$ DS in G.

Example 3.1. *Assuming the axiom of choice holds, there exists a set R of real numbers which intersects any nonidentity translation $R + a$ at exactly one point.*

Example 3.2. *Assuming the axiom of choice holds, there exists a set S of positive real numbers such that all positive real numbers, except 1, can be written as a ratio of elements of S in a unique way.*

It is likely that these may be extended to produce families of ADSs and DSs for larger values of λ in certain well-ordered infinite abelian groups. However, the general theory of infinite DSs and ADSs is beyond the scope of this paper, and the possibility of structures like a $\left(2^{\aleph_0}, 2^{\aleph_0}, \aleph_0\right)$ DS in $\mathbb{R}$ must remain conjectural.

4 New Results and Future Directions

4.1 A New Construction

We now introduce a family of ADSs in nonabelian groups, building off of known DSs in groups one-quarter the size. Because infinite DS families of these sizes are known, this new construction method can produce arbitrarily large ADSs in nonabelian groups formed by semidirect products.

Theorem 4.1. *Let D_1 and D_2 be $\left(v, \frac{v-1}{2}, \frac{v-3}{4}\right)$ DSs in some group H such that $D_1 \cup \{1_H\}$ is a $\left(v, \frac{v+1}{2}, \frac{v+1}{4}\right)$ DS. Then $A = D_1 \cup D_2 x \cup (D_1 \cup \{1_H\})x^2 \cup (H \setminus D_2)x^3$ is a $(4v, 2v, v-1, v)$ ADS in the group $G = H \rtimes \mathbb{Z}_4$ where $hx = xh^{-1}$.*

Note that because translations preserve difference properties, if there is any $h \in H \setminus D_1$ such that $D_1 \cup \{h\}$ is a DS, we can simply translate D_1 by h^{-1} to get a DS $D_1 h^{-1} \cup \{1_H\}$ which fulfills the requirement of the theorem.

<u>Proof:</u> The group ring allows us to prove this result. The value of $AA^{(-1)}$ is equal to a sum of terms which can be split into four parts: those terms contained in the normal subgroup H and those contained in each of the three cosets Hx, Hx^2, and Hx^3. The terms of $AA^{(-1)}$ which land in H will be

$$D_1 D_1^{(-1)} + D_2 x (D_2 x)^{(-1)} + (D_1 + 1_H)x^2((D_1 + 1_H)x^2)^{(-1)} + (H - D)x^3((H - D)x^3)^{(-1)}$$

$$= D_1 D_1^{(-1)} + D_2 D_2^{(-1)} + (D_1 + 1_H)(D_1 + 1_H)^{(-1)} + (H - D)(H - D)^{(-1)}$$

Because each of these four terms is just $DD^{(-1)}$ for some difference set $D \subseteq H$, this reduces to

$$2v 1_H + (v-1)(H - 1_H)$$

The terms of $AA^{(-1)}$ in Hx are

$$D_2 x (D_1)^{(-1)} + (D_1 + 1_H)x^2 (D_2 x)^{(-1)} + (H - D_2)x^3((D_1 + 1_H)x^2)^{(-1)} + D_1((H - D)x^3)^{(-1)}$$

$$= (D_2D_1 + (D_1 + 1_H)D_2 + (H - D_2)(D_1 + 1_H) + D_1(H - D_2))x$$

$$= (HD_1 + H + D_1H)x$$

$$= vHx$$

This part of the proof exploits the fact that conjugation by x inverts the elements of H, showing that this particular choice of semidirect product is necessary for the construction to work. In Hx^2, the terms of $AA^{(-1)}$ are given by

$$D_1((D_1 + 1_H)x^2)^{(-1)} + D_2x((H - D_2)x^3)^{(-1)} + (D_1 + 1_H)x^2D_1^{(-1)} + (H - D_2)x^3(D_2x)^{(-1)}$$

$$= (D_1(D_1^{(-1)} + 1_H) + D_2(H - D_2^{(-1)}) + (D_1 + 1_H)D_1^{(-1)} + (H - D_2)D_2^{(-1)}))x^2$$

$$= (D_1D_1^{(-1)} + D_1 + D_2H - D_2D_2^{(-1)} + D_1D_1^{(-1)} + D_1^{(-1)} + HD_2^{(-1)} - D_2D_2^{(-1)})x^2$$

$$= (D_1 + D_1^{(-1)} + (v - 1)H)x^2$$

Note that because $D_1 \cup \{1_H\}$ is a DS, in the group ring we must have

$$(D_1 + 1_H)(D_1 + 1_H)^{(-1)} = \frac{v+1}{2}1_H + \frac{v+1}{4}(H - 1_H)$$

$$D_1D_1^{(-1)} + D_1 + D_1^{(-1)} + 1_H = \frac{v+1}{2}1_H + \frac{v+1}{4}(H - 1_H)$$

$$D_1 + D_1^{(-1)} = H - 1_H$$

So the above sum is in fact equal to

$$((H - 1_H) + (v - 1)H)x^2$$

$$= ((v - 1)1_H + v(H - 1_H))x^2$$

And the Hx^3 case proceeds identically to the Hx case. Therefore A is an ADS where x^2 and the nonidentity elements of the normal subgroup H appear $v - 1$ times in the differences and all other elements appear v times. □

An alternate proof avoids the group ring notation in favor of the size of intersections of A with its translations. Here we can split the possible intersections into four cases. If $g \in H$, then $|A \cap Ag| = |D_1 \cap D_1 h| + |D_2 x \cap D_2 x h| + |(D_1 \cup h)x^2 \cap (D_1 \cup h)x^2 h| + |(H \setminus D_2)x^3 \cap (H \setminus D_2)x^3 h| = v - 1$ because each of the four individual intersections is the intersection of a DS with its translation. Other cases are trickier, but follow the same general outline as the proof using the group ring. In general the two proof methods are very similar, and given a proof of an ADS construction in one method it is easy to extract a proof using the other.

4.2 Example ADSs

The simplest possible example of an ADS of this form is a $(12, 6, 2, 3)$ ADS in $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$. Using the presentation $\langle a, x | a^3 = x^4 = e, ax = xa^{-1} \rangle$, we note that $D_1 = \{a\}$ and $D_2 = \{a^2\}$ are trivial $(3, 1, 0)$ DSs in the normal subgroup $\mathbb{Z}_3$. These choices give us the ADS $A = \{a, a^2x, x^2, ax^2, x^3, a^2x^3\}$, which can easily be verified to produce the elements of $\{a, a^2, x^2\}$ twice and all other nonidentity group elements three times.

Note that the normal subgroup H is not required to be cyclic, or even abelian. For example, we can produce a $(108, 54, 26, 27)$ ADS starting from the order-27 group $H = \langle a, x | a^9 = x^3 = e, ax = xa^7 \rangle$. However, given that finding DSs in arbitrary groups may be quite difficult, it is most useful to consider choices of H where we already know how to construct DSs.

The Paley DS construction mentioned earlier provides a mechanism for finding DSs that can be used to build ADSs. If $q \equiv 3 \mod 4$ is a prime power, the squares in $GF(q)$ form a $\left(q, \frac{q-1}{2}, \frac{q-3}{4}\right)$ DS. Furthermore, because each element of the field is either a square or the additive inverse of a square, appending 0 to this DS forms another DS one element larger. So we can build a $(4q, 2q, q-1, q)$ ADS in $\mathbb{Z}_q \rtimes \mathbb{Z}_4$ for any such q.

For example, in $GF(7)$, the set of squares is $D = \{1, 2, 4\}$. If we choose $D_1 = D$ and $D_2 = D + 1$, then in $\mathbb{Z}_7 \rtimes \mathbb{Z}_4$ there is a $(28, 14, 6, 7)$ ADS

$$A = \{a, a^2, a^4, a^2x, a^3x, a^5x, x^2, ax^2, a^2x^2, a^4x^2, x^3, ax^3, a^4x^3, a^6x^3\}.$$

The existence of the Paley difference sets demonstrates that there are infinitely many ADSs generated by this new construction method, though the ADSs formed from the Paley construction are only a proper subset of all the ADSs which can be generated in groups of the form $H \rtimes \mathbb{Z}_4$.

4.3 Generalizing the Direct Product Method

Chapter 2 includes a similar product construction, forming a $(4k, 2k-1, k-2, k-1)$ or $(4k, 2k+1, k+1, k-1)$ ADS in $\mathbb{Z}_4 \times G$ using $D = (\{0, 2\} \times A) \cup (\{1\} \times B) \cup (\{3\} \times (G \setminus B))$ for DSs A and B. This is itself a generalization of previously known constructions in direct product groups, but we can generalize it still farther to apply it to the nonabelian case of the semidirect product where elements of $\mathbb{Z}_4$ act on the elements of G in such a way that $gx = xg^{-1}$.

Given that D_1 and D_2 are $(k, \frac{k+1}{2}, \frac{k+1}{4})$ or $(k, \frac{k-1}{2}, \frac{k-3}{4})$ DSs in a group H, we know from [14] that we can construct the $(4k, 2k+1, k+1, k-1)$ or $(4k, 2k-1, k-2, k-1)$ ADS

$$A = (D_1 \times \{0, 2\}) \cup (D_2 \times \{1\}) \cup ((H \setminus D_2) \times \{3\})$$

in $G = H \times \mathbb{Z}_4$. Using the group ring, we can both verify this construction and demonstrate that the same construction method works to construct an ADS B with the same parameters in $G' = H \rtimes \mathbb{Z}_4$.

Once again, the products $AA^{(-1)}$ and $BB^{(-1)}$ contain terms in each of the cosets of H. The terms in H itself are simply

$$D_1D_1^{(-1)} + D_2x(D_2x)^{(-1)} + D_1x^2(D_1x^2)^{(-1)} + (H - D_2)x^3((H - D_2)x^3)^{(-1)}$$

which as a sum of terms of the form $DD^{(-1)}$ for difference sets D yields either $(2k+1)1_H + k(H - 1_H)$

or $(2k-1)1_H + (k-2)(H-1_H)$ depending on the parameters of D_1 and D_2, regardless of whether the product is direct or semidirect. The terms of $AA^{(-1)}$ in Hx are then

$$D_2D_1^{(-1)}x + D_1D_2^{(-1)}x + (H-D_2)D_1^{(-1)}x + D_1(H-D_2)^{(-1)}x$$

$$= (HD_1^{(-1)} + D_1H)x$$

while the terms of $BB^{(-1)}$ in Hx are

$$D_2D_1x + D_1D_2x + (H-D_2)D_1x + D_1(H-D_2)x$$

$$= (HD_1 + D_1H)x$$

producing $(k+1)Hx$ or $(k-1)Hx$ in both cases by simple cancellation of terms. Furthermore, in Hx^2 the terms of both $AA^{(-1)}$ and $BB^{(-1)}$ are

$$D_1D_1^{(-1)}x^2 + (H-D_2)D_2^{(-1)}x^2 + D_1D_1^{(-1)}x^2 + D_2(H-D_2)^{(-1)}x^2$$

$$= (HD_2^{(-1)} + D_2H)x^2$$

because x^2 commutes with all elements of G even in the semidirect product. Again we are left with $(k+1)Hx^2$ or $(k-1)Hx^2$, showing that these elements are also generated $\lambda+1$ times. The Hx^3 case is the same as the Hx case, and so we have shown A and B are ADSs in $G \times \mathbb{Z}_4$ and $G \rtimes \mathbb{Z}_4$ respectively.

This gives us another construction method for ADSs in nonabelian groups. For example, given that $D_1 = \{a, a^2, a^4\}$ and $D_2 = \{e, a, a^3\}$ are $(7,3,1)$ DSs in $\langle a | a^7 = e\rangle$, we know that

$$A = \{a, a^2, a^4, x, ax, a^3x, ax^2, a^2x^2, a^4x^2, a^2x^3, a^4x^3, a^5x^3, a^6x^3\}$$

is a $(28, 13, 5, 6)$ ADS in $\langle a, x | a^7 = x^4 = e, ax = xa^{-1}\rangle$.

This construction method does not rely on the particular algebraic properties of the group, as shown by the near-identical proofs in the cases of both the direct and semidirect products. On the other hand, the new semidirect product construction given in section 1 does not have an analogous construction in the direct product, and does exploit the fact that $gx = xg^{-1}$. Attempting to construct the same ADS in the direct product causes problems in the cosets Hx and Hx^3. Specifically, let

$$A = D_1 \times \{0\} \cup D_2 \times \{1\} \cup (D_1 \cup \{1_H\}) \times \{2\} \cup (H \setminus D_2) \times \{3\}$$

and check the terms of $AA^{(-1)}$ contained in $H \times \{1\}$:

$$(D_2 D_1^{(-1)} + (D_1 + 1_H)D_2^{(-1)} + (H - D_2)(D_1 + 1_H)^{(-1)} + D_1(H - D_2)^{(-1)}) \times \{1\}$$

$$= (D_2^{(-1)} + HD_1^{(-1)} + H - D_2 + D_1 H) \times \{1\}$$

$$= (vH + D_2^{(-1)} - D_2) \times \{1\}$$

And here the $D_2^{(-1)} - D_2$ need not cancel out nicely. Testing the method in groups like $\mathbb{Z}_{28} = \mathbb{Z}_7 \times \mathbb{Z}_4$ shows that this method in general does not produce an ADS.

The presence of an ADS construction in the semidirect product but not in the direct product suggests that semidirect products have the potential to generate ADSs which are not just obvious nonabelian analogues to the well-known abelian ADSs. The question immediately arises of which other semidirect products allow us to easily construct ADSs. We saw in chapter 3 that at least one attempt to generalize to $H \rtimes \mathbb{Z}_8$ fails. In fact none of the ADSs in $\mathbb{Z}_3 \rtimes \mathbb{Z}_8$ have a similar $S = \{g \in G : |A \cap Ag| = \lambda\}$, suggesting that there is no way to generalize to this larger product. Regardless, more research would likely produce some deeper understanding of when and why the product constructions exist.

4.4 Other Potential Construction Methods

As seen in chapter 3, an ADS that seems to be formed from a predictable pattern need not generalize into a true family of ADSs. Even if a family exists, the way it is generated may not be obvious. However, there are some especially nice ADSs which seem likely to come from some combinatorial construction rather than just occurring 'by chance'. Particularly interesting are those that seem likely to generalize. For example, while A_4 does have multiple nonequivalent $(12, 6, 2, 3)$ ADSs, A_4 has properties distinct from the other alternating groups and so it is not obvious that similar structures would appear in A_n for larger n.

- In the order-20 semidirect product group $\mathbb{Z}_5 \rtimes \mathbb{Z}_4$ given by $\langle a, x | a^5 = x^4 = e, ax = xa^{-1} \rangle$, there is a single (up to automorphism and translation) $(20, 10, 4, 5)$ ADS where each element of $\langle a \rangle x^2$ appears 4 times and all other group elements appear 5 times. One representative of this equivalence class is

  $$A = \{a, a^2, a^3, a^4, x, a^3x, a^4x, x^2, x^3, a^3x^3\}.$$

  Is this given by some analogous $H \rtimes \mathbb{Z}_4$ construction for $|H| \equiv 1 \mod 4$?

- Besides $\mathbb{Z}_{16}$, the only group to have a $(16, 8, 3, 4)$ ADS out of 14 order-16 groups is the modular group $\mathbb{Z}_8 \rtimes \mathbb{Z}_2$ given by $\langle a, x | a^8 = x^2 = e, ax = xa^5 \rangle$. One representative for the sole equivalence class is

  $$A = \{e, a, a^2, a^3, a^5, x, ax, a^4x\}$$

  Each element of $S = \{a^2, a^6, a^2x, a^6x\}$ is generated 3 times and each other nonidentity group element is generated 4 times. Is the existence of this ADS indicative of similar structures in larger 2-groups?

- The group $\mathbb{Z}_3 \times S_3 = \mathbb{Z}_3 \times D_3$ has an ADS of every size, despite the fact that the symmetric and dihedral groups typically have close to the fewest ADSs of any groups. Representatives of the two $(18, 9, 4, 13)$ ADSs in this group are

$$A_1 = \{(0, e), (0, a), (0, a^2), (0, x), (1, a), (1, a^2), (1, ax), (2, e), (2, ax)\}$$

$$A_2 = \{(0, a), (0, a^2), (0, ax), (0, a^2x), (1, e), (1, ax), (1, a^2x), (2, ax), (2, x)\}$$

In both cases, the elements of $\{(1, a), (1, a^2), (2, a), (2, a^2)\}$ appear 5 times while all other nonidentity elements appear 4 times. Note that another way of producing this group is the wreath product $\mathbb{Z}_3 \wr \mathbb{Z}_2$, and that $\mathbb{Z}_2 \wr \mathbb{Z}_2 = D_8$ also has an ADS equal to half the size of the group despite large ADSs being rare in dihedral groups. Is there some general wreath product construction of ADSs in $G \wr \mathbb{Z}_2$?

5 Addendum: ADSs in Small Groups

The following is a list of groups with size no greater than 28 along with the number of almost difference sets of various sizes.

	2	3	4	5	6	7	8	9
$\mathbb{Z}_4$	1							
$\mathbb{Z}_2 \times \mathbb{Z}_2$	0							
$\mathbb{Z}_5$	1							
S_3	1	0						
$\mathbb{Z}_6$	2	1						
$\mathbb{Z}_7$	1	1						
$\mathbb{Z}_8$	2	1	3					
$\mathbb{Z}_4 \times \mathbb{Z}_2$	1	0	1					
D_8	1	0	1					
Q_8	1	1	1					
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	0	0	0					
$\mathbb{Z}_9$	2	1	2					
$\mathbb{Z}_3 \times \mathbb{Z}_3$	1	1	1					
D_{10}	1	0	0	0				
$\mathbb{Z}_{10}$	2	1	2	2				
$\mathbb{Z}_{11}$	1	1	1	1				
$\mathbb{Z}_3 \rtimes \mathbb{Z}_4$	3	2	0	1	3			
$\mathbb{Z}_{12}$	4	3	1	3	3			
A_4	1	1	0	1	2			
D_{12}	2	0	0	1	0			
$\mathbb{Z}_6 \times \mathbb{Z}_2$	2	1	0	2	2			
$\mathbb{Z}_{13}$	1	2	1	3	4			
D_{14}	1	1	0	0	0	0		
$\mathbb{Z}_{14}$	2	3	1	6	5	0		
$\mathbb{Z}_{15}$	3	4	3	8	2	1		
$\mathbb{Z}_{16}$	3	4	2	5	0	1	4	
$\mathbb{Z}_4 \times \mathbb{Z}_4$	1	1	1	0	3	1	0	
$(\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2$	1	0	0	0	4	0	0	
$\mathbb{Z}_4 \rtimes \mathbb{Z}_4$	2	1	0	0	3	1	0	
$\mathbb{Z}_8 \times \mathbb{Z}_2$	3	2	0	1	2	0	0	
$\mathbb{Z}_8 \rtimes \mathbb{Z}_2$	3	2	1	1	2	0	1	
D_{16}	2	1	0	0	0	0	0	
SD_{16}	3	2	0	1	2	0	0	
Q_{16}	3	3	2	1	2	0	0	
$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	1	0	0	0	2	0	0	
$\mathbb{Z}_2 \times D_8$	1	0	0	0	2	0	0	
$\mathbb{Z}_2 \times Q_8$	1	1	1	0	2	0	0	
$(\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2$	2	1	0	0	2	0	0	
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	0	0	0	0	1	0	0	
$\mathbb{Z}_{17}$	1	2	2	3	0	4	8	
D_{18}	2	1	0	0	0	0	0	0
$\mathbb{Z}_{18}$	4	5	4	3	6	11	8	6

	2	3	4	5	6	7	8	9	10	11	12	13	14
$\mathbb{Z}_3 \times S_3$	4	5	1	1	1	1	1	2					
$(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_2$	1	1	0	0	0	0	0	0					
$\mathbb{Z}_6 \times \mathbb{Z}_3$	2	2	1	1	0	2	2	0					
$\mathbb{Z}_{19}$	1	3	4	1	6	5	1	1					
$\mathbb{Z}_5 \rtimes \mathbb{Z}_4$	3	3	4	0	2	1	0	0	1				
$\mathbb{Z}_{20}$	4	6	8	0	18	5	0	2	5				
$\mathbb{Z}_5 \rtimes \mathbb{Z}_4$	2	2	0	0	0	1	0	0	2				
D_{20}	2	1	0	0	0	1	0	0	0				
$\mathbb{Z}_{10} \times \mathbb{Z}_2$	2	2	1	0	8	2	0	0	0				
$\mathbb{Z}_7 \rtimes \mathbb{Z}_3$	2	4	5	1	4	1	1	4	1				
$\mathbb{Z}_{21}$	3	7	11	1	15	1	3	17	21				
D_{22}	1	1	0	0	0	0	0	0	0	0			
$\mathbb{Z}_{22}$	2	5	8	0	18	0	9	16	9	4			
$\mathbb{Z}_{23}$	1	3	7	1	11	0	15	5	0	1			
$\mathbb{Z}_3 \rtimes \mathbb{Z}_8$	5	8	9	1	6	4	7	2	2	4	4		
$\mathbb{Z}_{24}$	6	13	23	2	18	7	28	2	6	4	16		
$SL(2,3)$	3	6	10	2	7	1	4	1	0	0	0		
$\mathbb{Z}_3 \rtimes Q_8$	5	7	8	1	1	1	5	0	0	0	0		
$\mathbb{Z}_4 \times S_3$	5	5	0	0	0	1	0	0	0	0	0		
D_{24}	4	3	0	0	0	0	0	0	0	0	0		
$\mathbb{Z}_2 \times (\mathbb{Z}_3 \rtimes \mathbb{Z}_4)$	4	4	3	0	0	1	2	0	0	0	0		
$(\mathbb{Z}_6 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2$	4	3	0	0	0	1	0	0	0	0	0		
$\mathbb{Z}_{12} \times \mathbb{Z}_2$	5	6	5	0	6	2	4	0	0	0	0		
$\mathbb{Z}_3 \times D_8$	5	6	2	0	3	3	0	0	6	0	0		
$\mathbb{Z}_3 \times Q_8$	4	6	7	1	4	1	4	0	0	2	0		
S_4	2	2	1	0	0	0	0	0	2	0	0		
$\mathbb{Z}_2 \times A_4$	2	2	0	0	1	0	0	0	0	0	0		
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times S_3$	2	1	0	0	0	0	0	0	0	0	0		
$\mathbb{Z}_6 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	2	1	0	0	1	0	0	0	0	0	0		
$\mathbb{Z}_{25}$	2	4	11	3	8	4	12	0	7	15	17		
$\mathbb{Z}_5 \times \mathbb{Z}_5$	1	1	2	1	1	2	1	0	1	1	2		
D_{26}	1	2	1	0	0	0	0	0	0	0	0	0	
$\mathbb{Z}_{26}$	2	7	17	3	6	14	6	0	*	*	*	*	
$\mathbb{Z}_{27}$	3	6	18	10	3	22	4	5	*	*	0	0	
$\mathbb{Z}_9 \times \mathbb{Z}_3$	3	5	7	5	1	7	0	0	*	*	0	0	
$(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_3$	2	3	3	2	0	1	0	0	*	*	0	0	
$\mathbb{Z}_9 \rtimes \mathbb{Z}_3$	3	7	9	2	0	6	0	0	*	*	0	*	
$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	1	1	1	1	0	0	0	0	0	*	0	*	
$\mathbb{Z}_7 \rtimes \mathbb{Z}_4$	3	5	8	3	0	0	0	3	0	0	0	*	*
$\mathbb{Z}_{28}$	4	10	26	10	1	42	0	18	*	0	0	*	*
D_{28}	2	3	1	0	0	0	0	0	0	0	0	*	0
$D_{14} \times \mathbb{Z}_2$	2	5	6	0	3	12	0	4	*	0	0	*	0

References

[1] C. Berrou, A. Glavieux, and P. Thitimajshima. Near shannon limit error-correcting coding and decoding. *Proceedings of IEEE Telecommunications Conference*, 1993.

[2] R. C. Bose. On the construction of balanced incomplete block designs. *Annals of Eugenics*, 9(4): 353-399, 12 1939. ISSN 2050-1439. doi: 10.1111/j.1469-1809.1939.tb02219.x. URL https://dx.doi.org/10.1111/j.1469-1809.1939.tb02219.x.

[3] J. Davis. Almost difference sets and reversible difference sets. *Archives of Mathematics*, 59:595-602, 1992.

[4] C. Ding. The differential cryptanalysis and design of the natural stream ciphers. *Proceedings of FSE 1993*, pages 101-115, 1994.

[5] C. Ding, D. Kohel, and S. Ling. Secret-sharing with a class of ternary codes. *Theoretical Computer Science*, (246):285-298, 2000.

[6] C. Ding, T. Helleseth, and H. Martinsen. New families of binary sequences with optimal three-level autocorrelation. *IEEE Transactions on Information Theory*, 47:428-433, 2001.

[7] C. Ding. *Codes from Difference Sets*. World Scientific, 2014.

[8] D. Hankerson et al. *Coding Theory and Cryptography: The Essentials*. CRC Press, 2000.

[9] K. Kedlaya, B. Poonen, and R. Vakil. *The William Lowell Putnam Mathematical Competition 1985-2000: Problems, Solutions, and Commentary*. The Mathematical Association of America, 2002.

[10] E. Lehmer. On residue difference sets. *Canadian Journal of Mathematics*, 5:425-432, 1953.

[11] K. Nowak. A survey on almost difference sets. *arXiv*, 2014.

[12] R. Paley. On orthogonal matrices. *Journal of Mathematical Physics MIT*, 12: 311-320, 1933.

[13] I. Reed and G. Solomon. Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300-304, 1960. doi: 10.1137/0108018.

[14] X. Tang and C. Ding. New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value. *IEEE Transactions on Information Theory*, 56(12):6398-6405, 2010.

[15] Y. Zhang, J. Lei, and S. Zhang. A new family of almost difference sets and some necessary conditions. *IEEE Transactions on Information Theory*, 52(5), 2006.

[16] J.A. Davis, J. Jedwab, A unifying construction for difference sets, *J. Combin. Theory Ser. A* **13** (1997), 80-1.

[17] J.F. Dillion, Variations on a scheme of McFarland for noncylic difference sets, *J. Combin. Theory Ser. A* **40** (1985), 9-21.

[18] J.F. Dillon, Personal correspondence.

[19] R. L. McFarland, A family of difference sets in non-cyclic groups, *J. Combin. Theory Ser. A* **15** (1973), 1-10.