Spring 2024

Finding Maximal Cap Sizes for Quad Card Decks Using Share Strings

Oliver William Pawelek
Bard College

Finding Maximal Cap Sizes for *Quad* Card Decks Using Share Strings

A Senior Project submitted to
The Division of Science, Mathematics, and Computing
of
Bard College

by
Oliver Pawelek

Annandale-on-Hudson, New York
May, 2024

Abstract

This project introduces the concept of share strings and how they can be used to figure out maximal cap sizes for different decks of the card game *EvenQuads*. We prove that all caps must map to a share string with respect to a basis and that if no share strings exist for cap size k in a given dimension d, then the maximal cap size of that dimension $M(d)$ must be less than k. We prove the maximal cap sizes up to dimension 7 and show that there are at most 8 possible share strings for 19-caps of dimension 8.

Contents

Dedication

I dedicate this project to my parents and extended family as well as my late grandfather who, as he often proclaimed, was himself a mathematical genius.

Acknowledgments

I want to thank my advisor Stefan for working with me throughout the year on this project and helping me develop my math into a sound, usable language. I would like to thank Lauren who gave me the opportunity to pursue a wonderful research experience through the BSRI program as well as Minshi, Oliver, and Shay for being such a lovely group of friends to work with over the summer. Thank you to all of my teachers and professors, math and beyond, for opening me up to different ways of thinking and problem solving throughout my collegiate career. I want to thank all of my friends throughout the years who've made Bard my home away from home. Finally, I would like to thank my family for absolutely everything, you are my light.

1
Introduction

The game *EvenQuads*, or *Quads*, is a card game invented by Jeffery Perreira and Lauren Rose in 2013 that mimics the popularized card game *SET*. In *Quads*, some number of cards are laid out and players race to find a **quad**, or a set of four cards that adhere to the quad conditions that can be found in Chapter 2.1. There is, however, a possibility that a quad may not be present in the layout which would qualify the layout to be a **cap**. This possibility raises the following question: How many cards are required to ensure that a quad is present in a given layout? The question that better pertains to the math we will be exploring is what is the **maximal cap size**, or the largest possible cap, of $\mathbb{Z}_2^d$ when viewed as an affine space for given dimensions d? This was one of the driving questions in the original article "How Many Cards Should You Lay Out in a Game of *EvenQuads*: A Detailed Study of Caps in AG$(n, 2)$" ([3]) which comprised the results of the 2021-22 Bard Summer Research Initiative (BSRI) mathematics research groups. The paper proves the maximal cap sizes up to the standard *Quads* deck-size, or the dimension 6 deck, whose results can be found in Table 1.0.1, along with other interesting properties about caps and *Quad* cards.

During the summer of 2023, I worked with professor Lauren Rose through BSRI and helped expand the *Quads* research of the previous two mathematics groups. I was given an opportunity to experience the process of discovering new math in an attempt to solve large scale problems

Dimension	Maximal Cap Size
0	1
1	2
2	3
3	4
4	6
5	7
6	9

Table 1.0.1: (Results from [3]), Maximal Capsizes for dimensions 0-6

that had never fully been solved before. As opposed to the more rigid structure of a class, I had the ability to play freely with the material and come up with my own ways of solving problems using math. With this freedom, I noticed patterns in the structure of caps that led me to conceive what I now call **share strings** which are defined in section 3.1. I saw that these strings could provide information about the existence of caps of given sizes in different dimensions, enough so that they can be used to prove maximal cap sizes. For this project, I decided to continue answering the max-cap question for dimensions 7 and 8 using share strings and reprove dimensions 0-6 which were initially proved in [3].

Chapter 2 provides a more in depth description of *Quads* and its relation to *SET* along with a brief reiteration of how *Quad* cards are isomorphic to $\mathbb{Z}_2^d$ and the affine geometry $\mathrm{AG}(d, 2)$. A more detailed description can be found in [3] but I include all definitions and theorems needed to construct share strings. The majority of the math defined and proved in this chapter is derived from [3]. All definitions and theorems beyond this chapter are of my own discovery through research unless otherwise indicated.

Chapter 3 fully defines share strings along with other important terminology including **sharing**, **sumsets**, and **sum decompositions** which are used abundantly throughout the project. It also includes general theorems about share strings and their properties such as the frequently used Theorems 3.3.1 and 3.3.3 as well as the most important theorem, the **Share String Theorem**. Proofs for the max-cap sizes of dimensions 0-5 using share strings are also included in this chapter.

Sum Decomposition	Possible Share Strings
$(5^8, 7^2), (5^9, 9^1)$	(0,0,0,0,0,0,9,0,0,0,0)
$(5^7, 7^3)$	(0,0,0,0,0,0,7,2,0,0,0)
	(0,0,0,0,0,0,8,0,1,0,0)
$(5^6, 7^4)$	(0,0,0,0,0,0,5,4,0,0,0)
	(0,0,0,0,0,0,6,2,1,0,0)
	(0,0,0,0,0,0,7,0,2,0,0)
	(0,0,0,0,0,0,7,1,0,1,0)

Table 1.0.2: Remaining possible share strings for 19-caps of dimension 8

Chapters 4 and 5 attempt to prove the maximal cap sizes for dimensions 6, 7, and 8 using share strings. Other important theorems such as the Pair-Share Theorem are proved in chapter 4. I prove in full that the maximal cap size for dimension 7 is 12 and that the 7 share strings in Table 1.0.2 are the only 7 possible share strings for 19-caps of dimension 8 out of the potential 9^{11}, or 31381059609, initial possibilities.

Chapter 6 concludes the project and begins to formulate a description of **share string equivalencies** along with other potential future work with share strings.

2
Quads

2.1 Introduction to *Quads* and *SET*

In order to better understand *Quads*, it may be easier to look at *SET* as an analogue first. Much research has been done on *Set* which has been compiled and mainstreamed into the book *The Joy of SET* ([4]). Like *Quads*, *Set* involves players laying out some number of cards and racing to find a set of 3 cards that adhere to the required properties of a **set**. Each *SET* card contains some number of uniquely colored shapes filled with a unique texture. We call these properties the **attributes** of the cards.

There are 3 states for each attribute: 3 shapes (ovals, diamonds, or squiggles), 3 colors (red, green, or purple), 3 textures (filled, hollow, or hatched), and 3 numbers (1, 2, or 3 shapes on each card). For 3 cards to be a set, each attribute must be either alike on all 3 cards or different on all three cards. The 3 asterisked cards in Figure 2.1 form a set because their colors are all the same and the number and shape are all different.

What distinguishes *Quads* from *SET* is that there are 4 different states for each attribute and a quad is composed of 4 cards instead of 3. Similar to *SET*, each attribute in a quad may be different or alike across the 4 cards, but unlike in *SET,* having 2 different pairs of like attributes is also acceptable. For example, a quad could contain two cards that are red and two that are

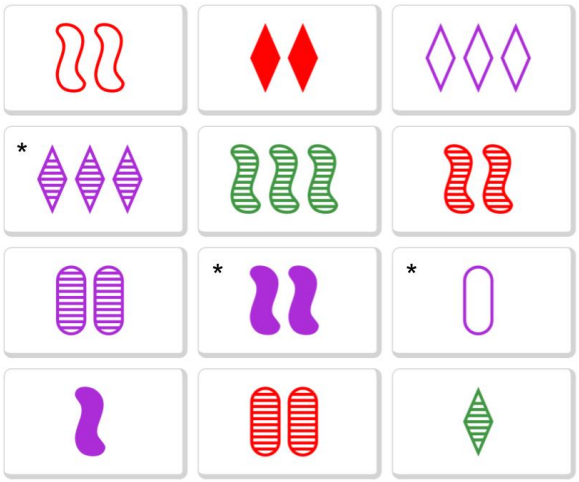


Figure 2.1.1: A layout of *SET* cards found at https://blog.untrod.com/2021/06/set-solver-in-python.html

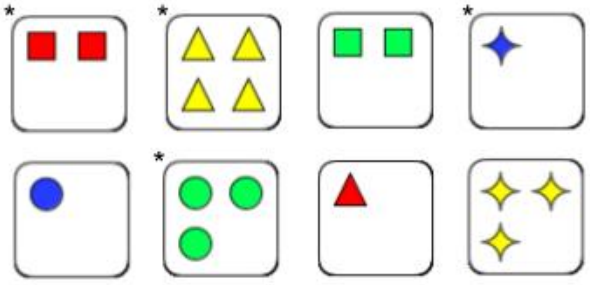


Figure 2.1.2: A layout of *Quad* cards

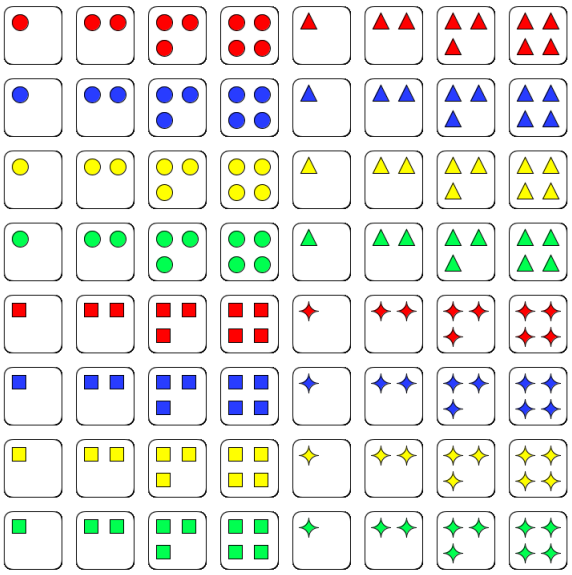


Figure 2.1.3: The standard $\mathbb{Z}_2^6$ *Quads* deck

blue. In Figure 2.1 the 4 asterisked cards form a quad because they have a different number, a different color, and a different shape. The official quad conditions from [3] are as follows:

Quad Conditions: A set of 4 cards forms a quad if for each attribute one of the following holds:

1. The states are the same on each card.
2. The states are different on each card.
3. Two different states occur, each on two cards.

Given that there are 4 possibilities for the 3 attributes of each card, there are $4^3 = 64$ unique quad cards in the *Quads* standard deck with 3 attributes as shown in Figure 2.1.3.

2.2 *Quads* and Binary

The heart of bridging *Quads* and mathematics lies in the fact that we can map *Quad* cards to elements of $\mathbb{Z}_2^d$. Before we look at individual cards, we can look at each attribute and how it can be mapped to an element of $\mathbb{Z}_2 \times \mathbb{Z}_2$ which is the set of binary strings of length 2: $\{00, 01, 10, 11\}$.

Attribute	00	01	10	11
Number	1	2	3	4
Color	Red	Blue	Yellow	Green
Shape	Circle	Square	Triangle	Twinkle

(Number, Color, Shape)$\in \mathbb{Z}_2^6$

Table 2.2.1: Mapping of *Quad* card attributes to elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$

We could, for example, have red cards correspond to (00), blue to (01), yellow to (10), and green to (11). Table 2.2.1 displays the arbitrary mapping of the attributes of the standard *Quads* deck to elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$ that we will use in the remainder of the project.

For example, the card with 2 green triangles would correspond to the element $(01, 11, 10) \in (\mathbb{Z}_2 \times \mathbb{Z}_2)^3$. Each element of the standard *Quads* deck must then correspond to an element of $(\mathbb{Z}_2 \times \mathbb{Z}_2)^3$. Even further, we can use the group isomorphism $(\mathbb{Z}_2 \times \mathbb{Z}_2)^3 \cong \mathbb{Z}_2^6$ to conclude that each card corresponds to an element of $\mathbb{Z}_2^6$.

What are some of the uses of mapping *Quad* cards to $\mathbb{Z}_2^6$? The first and most crucial property of any 4 cards that form a quad is that their corresponding vectors in $\mathbb{Z}_2^6$ will sum to the zero vector.

Theorem 2.2.1. *([3], Theorem 2.1). Let $a, b, c, d \in \mathbb{Z}_2^6$ be distinct. Then $\{a, b, c, d\}$ is a quad if and only if $a + b + c + d = \vec{0}$.*

Proof. Let $x, y, z, w \in \mathbb{Z}_2 \times \mathbb{Z}_2$.

Suppose the elements are all the same. Then using the property that elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$ are their own additive inverses, we get that $x+y+z+w = x+x+x+x = x+(-x)+x+(-x) = (00)$.

Suppose the elements are all different. Then since there are only 4 distinct elements in $\mathbb{Z}_2 \times \mathbb{Z}_2$, one will be equal to (00), one will be (01), one will be (10), and one will be (11). Thus $x + y + z + w = (00) + (01) + (10) + (11) = (0 + 0 + 1 + 1, 0 + 1 + 0 + 1) = (00)$.

Suppose the elements consist of two sets of repeated elements. Then there are two sets of equal elements, say $\{x, y\}$ and $\{z, w\}$. Thus $x + y + z + w = x + x + z + z = (00)$.

Therefore, by using the isomorphism $(\mathbb{Z}_2 \times \mathbb{Z}_2)^3 \cong \mathbb{Z}_2^6$, we can conclude that if each of the 3 attributes of a, b, c and d adhere to the properties of a quad, then $a + b + c + d = \vec{0}$.

The proof of the other direction is similar and will be omitted.

□

This theorem allows us to begin working with arbitrary vectors without having to use binary strings when referring to *Quad* cards. For the remainder of the project we will omit vector notation. We will refer to the zero vector as just 0 for simplicity and only use $\vec{0}$ if necessary.

We can look at an example to better visualize the relationship between *Quad* cards and their mappings to $\mathbb{Z}_2^6$:

Example 2.2.2. Observe the following elements of $\mathbb{Z}_2^6$:

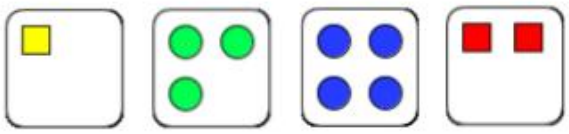
$$(0,0,1,0,0,1)$$

$$(1,0,1,1,0,0)$$

$$(1,1,0,1,0,1)$$

$$(0,1,0,0,0,0)$$

It is relatively easy to see that their sum will be 0, thus indicating that they form a quad. We can take our mapping to determine the cards represented by the vectors (ordered respectively):



The numbers and colors are all different and the shapes are half and half— in other words, we have a quad. voila!

Recall that $\mathbb{Z}_2^d$ is a vector space over the field $\mathbb{Z}_2$. This fact allows us to conclude the following proposition:

Proposition 2.2.3. *Let $p \in \mathbb{Z}_2^d$. The following are equivalent:*

1. $p = p$.

2. $p + p = 0$.

3. $p - p = 0$

we can remold this fact to make it more directly applicable to many of the theorems and proofs to come.

Theorem 2.2.4 (The Even Odd Theorem)**.** *Let* $p \in \mathbb{Z}_2^d$.

1. *p added an odd number of times is p.*

2. *p added an even number of times is* 0.

Proof. Let $k \in \mathbb{Z}$. Observe that $\sum_{i=1}^{2k+1} p = (p+p)+\cdots+(p+p)+p$ where there are k groupings of $(p+p)$. Using Proposition 2.2.3 we get that $(p+p) = 0$ so $(p+p)+\cdots+(p+p)+p = 0+\cdots+0+p = p$. Using the same logic we can deduce that $\sum_{i=1}^{2k} p = (p+p)+\cdots+(p+p) = 0+\cdots+0 = 0$. so p added an odd number of times is p and p added an even number of times is 0. □

We are very lucky for this very simple fact since this entire project would not be possible without it.

Seeing that we can map elements of $\mathbb{Z}_2^6$ to quad cards isomorphically, what happens if we map using elements of $\mathbb{Z}_2^5$ or $\mathbb{Z}_2^d$ for some natural number d? In the $\mathbb{Z}_2^5$ case, we end up reducing one of the attributes to just two options instead of 4. For example, we could reduce the number of possible shapes to just circles and squares which would correspond to the elements of $\mathbb{Z}_2$ (circles could be 0 and squares would be 1) instead of $\mathbb{Z}_2 \times \mathbb{Z}_2$. Then each quad card would correspond to a binary string of length 5 where the first two entries determine the number, the second two determine the color, and the last one determines the shape. Relative to the 3 attributes found in the standard $\mathbb{Z}_2^6$ deck, the deck corresponding to $\mathbb{Z}_2^5$ would have 2 full attributes and one half attribute. In theory, any combination of attributes such that the number of half attributes and half of the number of full attributes that adds to the size of the dimension would suffice.

Seeing that we can define quads mathematically, we can also define a quadless set of cards which we have been referring to as caps.

Definition 2.2.5. Let $C \subseteq \mathbb{Z}_2^d$.

1. The set C is a **cap** if C does not contain a quad, i.e., for any distinct $a, b, c, d \in C$, $a + b + c + d \neq 0$. A cap with k elements is called a k**-cap** ([3], Definition 3.1).

2. A cap C is **complete** if $C \cup \{c\}$ contains a quad for all $c \in \mathbb{Z}_2^d - C$

3. Suppose there exists a cap $C \subseteq \mathbb{Z}_2^d$ for a given d. Then C is **maximal** if there exists no caps with cardinality $|C + 1|$ in $\mathbb{Z}_2^d$.

4. We denote the maximal cap size of $\mathbb{Z}_2^d$ as $M(d)$.

△

A complete cap is a quadless set of cards that, when another card is added to the set, will necessarily contain a quad. It is complete, or full, in the sense that there are no cards left to add that allow the set to remain a cap. Maximal caps are the largest possible complete caps of a given dimension, meaning there exist no caps of a greater cardinality. It has been proved in [3] that in the $\mathbb{Z}_2^6$ deck, the maximal cap size is 9, meaning any set of 10 or more cards will necessarily contain a quad. We distinguish maximal caps from complete caps because there exist complete caps that are not maximal, where, for example, there exists 8-caps in $\mathbb{Z}_2^6$ that are complete but not maximal since larger 9-caps are attainable. Below is an example of a complete 8-cap of dimension 6:

$$\begin{array}{{}cccc{}} \{(000000), & (100000), & (010000), & (001000), \\ (000100), & (000010), & (000001), & (111111)\} \end{array}$$

Any other element of $\mathbb{Z}_2^6$ will form a quad with the elements of the above cap, thus making it complete. We can state a few facts about complete and maximal caps.

Proposition 2.2.6. *([3], Proposition 3.2). Let $S \subseteq \mathbb{Z}_2^d$.*

1. *If S has fewer than 4 elements then it is a cap.*

2. *maximal caps are complete.*

3. If all k-caps in dimension d are complete then they are maximal.

Proof. These properties descend directly from Definition 2.2.5 □

Since four cards are required to form a quad, any set of less than four *Quad* cards cannot be a quad. However, for any three cards, there is a unique fourth card that forms a quad with the original three which is proved in Corollary 2.2 in [3]. Given that there are then 61 remaining cards to choose from in the $\mathbb{Z}_2^6$ deck, there is a $\frac{1}{61}$ or a 1.64% chance of choosing the necessary card to form a quad. The entire deck has an obvious 100% probability of containing a quad since it quite literally contains all of the quads, but it is easy to see that we shouldn't need to lay out the entire deck to ensure that a quad is present. We could continue calculating probabilities in this manner, but calculations become extremely messy and difficult to work with so we will need to develop some more math to find the answers to our driving question. The size of maximal caps have been proven mathematically for dimensions 1 through 6 using the techniques developed in [3]. In theory we could pack up and go home at this point, but we still want to know how many cards we must lay out if we add attributes to play with, for example adding a background color to the cards, or perhaps different textures to the shapes like in *SET*. In the next chapter, we will begin to define and develop new math and techniques that form a continuation of [3] that we can use to prove the maximal cap sizes of dimensions 7 and 8. We must first, however, relate *Quad* cards to yet another field of math.

2.3 *Quads* and Affine Geometry

We can gain further insight into how *Quad* cards act by exploring the relationship between $\mathbb{Z}_2^d$ and affine geometry. As opposed to Euclidean geometry, affine geometry excludes angles and distance from the structure of points and planes in space. This takes privilege away from the zero vector and allows us to view all elements of $\mathbb{Z}_2^d$ the same. Caps were originally defined in the affine geometry $\mathrm{AG}(d, n)$ as collections of points in general position [3]. While we will not be working directly with the axioms of finite geometry, we can use its properties to strengthen the structure of *Quad* cards represented in $\mathbb{Z}_2^d$.

Definition 2.3.1. ([3], Definition 4.1). Let V be a finite dimensional vector space over a field K, and let $S = \{x_1, \ldots, x_n\} \subseteq V$.

1. An **affine combination** of S is a linear combination

$$\alpha_1 x_1 + \cdots + \alpha_n x_n,$$

where $\alpha_1, \ldots, \alpha_n \in K$ satisfy $\alpha_1 + \cdots + \alpha_n = 1$.

2. An **affine dependence** of S is a linear combination

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = 0,$$

where $\alpha_1 + \cdots + \alpha_n = 0$ and $\alpha_1, \ldots, \alpha_n$ are not all zero.

3. The **affine span** of a subset $S \subseteq V$ is the set $\text{aff}(S)$ of all affine combinations of finitely many elements of S.

4. S is **affinely dependent** if some element of S is in the affine span of the other elements. Otherwise S is **affinely independent**.

5. An **r-dimensional affine subspace** F of V, called an **r-flat**, is defined to be the affine span of $r+1$ affinely independent elements of V, or equivalently, the translate $L + v$ of an **r-dimensional linear subspace** L of V.

6. An **affine basis** for an r-flat $F \subseteq V$ is a set of affinely independent elements of V whose affine span is F. Equivalently, if $F = L + v$, then an affine basis for F is given by $\{x + v | x \in B \cup 0\}$, where B is a linear basis for L.

7. An **affine transformation** between vector spaces V and W over K is a function $A : V \to W$ for the form $A(x) = M(x) + y$ for all $x \in V$, where $M : V \to W$ is a linear transformation and $y \in W$ is a fixed vector.

8. An affine transformation A is an **affine isomorphism**, or **affine equivalence**, if A is invertible. In this case, we say that V and W are **affinely equivalent**, denoted $V \cong W$.

9. subsets $S, T \subseteq V$ are **affinely equivalent** if $A(S) = T$ for some affine isomorphism $A : V \to W$.

△

Throughout the rest of the project, we will use certain simplifications for some terms to make the reading easier. When referring to affine bases, we will drop the affine label and simply refer to them as **bases**. We will refer to an affine span as just a **span**. We will refer to elements of $\mathbb{Z}_2^d$ as **points**. Affinely independent points will be referred to as **independent points** or **basis points** if they are apart of a basis. Similarly, affinely dependent points will be referred to as **dependent points** if such distinction is necessary. The following propositions are standard and follow from Definition 2.3.1.

Proposition 2.3.2. *(*[3]*, Remark 4.2). The following results are standard and follow from Definition 2.3.1.*

1. *Any basis for a d-flat contains $d+1$ points, and every point of a flat can be written uniquely as an affine combination of basis points.*

2. *Two affinely independent sets of the same size are affinely equivalent.*

3. *When F is a field with q elements, a d-flat will contain q^d elements.*

Because we are looking at $\mathbb{Z}_2^d$, our field $\mathbb{Z}_2$ will contain 2 elements and for each dimension d we get that our deck will contain 2^d points. Any basis that spans dimension d or a d-flat will contain $d + 1$ points and the rest of the $2^d - (d + 1)$ points in the dimension will be affine combinations of the basis points.

Lemma 2.3.3. *(*[3]*, Lemma 4.3). Let $C = \{x_1, \ldots, x_n\} \subseteq \mathbb{Z}_2^d$.*

1. *An Affine combination of C is a sum of an odd number of points in C.*

2. *C is affinely dependent if and only if a sum of an even number of points in C equals 0.*

Proof. (1). Since the coefficients of an affine combination line in $\{0, 1\}$, the sum of the coefficients equals 1 if and only if the number of points is odd per Theorem 2.2.4.

(2). A dependence means that some $x_i \in C$ is an affine combination of other points in C, hence the sum of an odd number of them. Without loss of generality, assume $x_1 = x_2 + \cdots + x_{2t}$. Using the fact that $x_1 = -x_1$ we get that $x_1 + x_2 + \cdots + x_{2t} = 0$. □

Definition 2.3.4. ([3], Definition 5.9). Let $C \subseteq \mathbb{Z}_2^d$ be a cap.

1. The **dimension** of C, denoted $\dim(C)$, is the dimension of $\text{aff}(C)$, the smallest flat containing C.

2. We denote by $M(r)$ the **maximal cap size** in an r-flat in $\mathbb{Z}_2^d$.

3. If C is r-dimensional and complete, we say that C is a **complete cap in dimension** r, and that C **completes** the r-flat $\text{aff}(C)$.

△

When we refer to a cap or a set $C \subseteq \mathbb{Z}_2^d$, if $\dim(C) = d$ we will say that C is a cap *of* dimension d as opposed to a cap *in* dimension d. We will encounter 11-caps of dimension 7 and of dimension 8, but while the caps of dimensions 7 are technically affinely equivalent to caps *in* dimension 8, they do not span the entirety of $\mathbb{Z}_2^8$ and are thus not caps *of* dimension 8.

We can conclude that for any k-cap that spans dimension d, there will be an affine basis $B \subseteq C$ which will contain $d + 1$ affinely independent points in C. The points in $C - B$ will be affine combinations of the points in B, where each is a sum of some odd n points in B. We will prove that $5 \leq n \leq d + 1$ in Property 2.2.6. We will use these facts as a jumping off point for defining share strings in the next chapter.

3
Share Strings

3.1 Defining Share Strings

In this section, we will define all of the terms needed in order to define share string and prove several propositions that will aid us in using them.

Proposition 3.1.1. *Let $C \subseteq \mathbb{Z}_2^d$ be a k-cap of dimension d. Let $B \subseteq C$ be a basis of C. Then*

1. $|B| = d + 1$.
2. *Points in $C - B$ may be written as odd sums of between 5 and $d + 1$ points in B.*
3. $|C - B| = k - d - 1$.

Proof. (1) Because C is a cap *of* dimension d (as opposed to a cap *in* dimension d), it follows that C spans a d-flat. Because B is an affine basis for C, Property 2.3.2 tells us that B contains $d + 1$ elements.

(2) Because the points in C are in the span of the points in B, the points in $C - B$ are affine combinations of the points in B. From Lemma 2.3.3 we know that points in $C - B$ are sums of odd numbers of points in B. Such sums cannot contain more than $d+1$ basis points since there are only $d+1$ points in the basis. There cannot be points in $C - B$ equal to a single (sum of 1) point in B since Property 2.2.3 tells us the two points would be equal, indicating that a point in B is equal to a point in $C - B$ which is not possible. Let $s \in C - B$. Suppose for the sake of

contradiction that s is a sum of 3 points $a, b, c \in B$ where $s = a + b + c$. Then from Property 2.2.3 we get that $s + (a + b + c) = a + b + c + (a + b + c) = (a + a) + (b + b) + (c + c) = 0$. Then s, a, b, and c form a quad which contradicts the fact that C is a cap. Thus points in $C - B$ may not be written as sums of 3 points in B. Thus points in $C - B$ may be written as odd sums of between 5 and $d + 1$ points in B.

(3) Because $B \subseteq C$ it follows that $B \cap C = B$. Thus $|C - B| = |C| - |C \cap B| = |C| - |B| = k - (d + 1) = k - d - 1$. □

In order to better understand how these new definitions and properties will allow us to craft share strings, we will use a rolling example to visualize the definitions and properties to come.

Example 3.1.2. Let $C \subseteq \mathbb{Z}_2^7$ be an 11-cap of dimension 7. Then there exists a basis $B \subseteq C$ with 8 points $b_1, \ldots, b_8 \in B$. There are $11 - 7 - 1 = 3$ points $s_1, s_2, s_3 \in C - D$ that are dependent upon the basis and thus may be written as odd sums of between 5 and 8 basis points. Thus our two sum sizes may be either 5 or 7. Below is an arbitrary depiction of what the sums may look like:

$$s_1 = b_1 + b_2 + b_4 + b_5 + b_7$$

$$s_2 = b_1 + b_3 + b_4 + b_5 + b_6 + b_7 + b_8$$

$$s_3 = b_2 + b_3 + b_4 + b_7 + b_8$$

The fact that points are there own additive inverses is very important to many of the properties and theorems that will come later in the project. We will take a look at how this fact and Property 2.2.3 affects the structure of sums of points. Take s_1 from our example:

$$s_1 = b_1 + b_2 + b_4 + b_5 + b_7$$

Using Property 2.2.3 we can see that

$$s_1 + (s_1) = b_1 + b_2 + b_4 + b_5 + b_7 + (s_1)$$

$$\implies 0 = b_1 + b_2 + b_4 + b_5 + b_7 + s_1.$$

We will refer to any set of i points that sum to 0 as an i**-point dependency**. To take it further, any arrangement of the points in a sum will produce equivalent results:

$$s_1 + b_1 = b_2 + b_4 + b_5 + b_7$$

$$s_1 + b_1 + b_2 = b_4 + b_5 + b_7$$

$$s_1 + b_1 + b_2 + b_4 = b_5 + b_7$$

$$b_5 + b_1 + b_4 = b_7 + s_1 + b_2$$

$$\vdots$$

Throughout the rest of the project, we will omit plus and minus signs from our sums of points since it is the only binary operation we use. If $a, b, c \in \mathbb{Z}_2^d$ and $a + b = c$ we will say $ab = c$ to make the visualization of sums easier. We will also often denote numbered basis points b_i and b_j as just i and j for the same reason (although this we will indicate every time). We will also write sums with each basis point in a visual column. For example, we will write the sums

$$s_1 = b_1 + b_4 + b_5 + b_6 + b_8$$

$$s_2 = b_1 + b_2 + b_3 + b_4 + b_6 + b_8 + b_9$$

$$s_3 = b_2 + b_5 + b_7 + b_8 + b_9$$

as

s_1	=	1			4	5	6		8	
s_2	=	1	2	3	4		6		8	9
s_3	=		2			5		7	8	9

This will make it easier to visualize **sumsets** and how many of each basis point is shared by the sumsets of a cap.

Definition 3.1.3. Let $C \subseteq \mathbb{Z}_2^d$ be a k-cap of dimension d. Let B be a basis of C. Let $b \in B$ and let $s \in C - B$. Let $r = k - d - 1$.

1. Let $S = \{b_1, \ldots, b_n\}$ be the set of basis points that sum to s. We define S to be the the **sumset** of s. When working with multiple points in $C - B$, we will denote the sumset of a dependent point $s_i \in C - B$ as S_i.

2. We denote the set of sumsets of $C - B$ as $\mathbb{S}_B^C$.

3. Let $\mathbb{S}_b \subseteq \mathbb{S}_B^C$ be be the set of sumsets that contain b.

4. Any sumsets that contain b are said to **share** b.

5. $|\mathbb{S}_b|$ is the **share value** of b. We say that b is a $|\mathbb{S}_b|$**-share**.

△

The sumset of a point in $C - B$ is the set of basis points in its sum. We are ultimately referring to points in the same sumsets as being *shared* by those sumsets to more exclusively define the property. Since each basis point will be shared by some number of sumsets, we define that number to be the basis point's *share value*. If a basis point is shared by 4 sumsets, we will call that point a 4-share.

Proposition 3.1.4. *Let $C \subseteq \mathbb{Z}_2^d$ be a k-cap of dimension d. Let B be a basis of C. Let $b \in B$. Let $s_i \in C - B$ where $i \in \{1, \ldots, k - d - 1\}$.*

1. *$S_i \subseteq B$.*

2. *$|S_i|$ is odd and $5 \leq |S_i| \leq d + 1$.*

3. *$s_i = \sum_{p \in S_i} p$.*

4. *$|\mathbb{S}_B^C| = k - d - 1$*

5. *$0 \leq |\mathbb{S}_b| \leq k - d - 1$.*

Proof. (1), (2), (3). These properties follow directly from definition 3.1.3.

(4) There exists a unique sumset for each point in $C - B$ so $|\mathbb{S}_B^C| = |C - B| = k - d - 1$.

(5) Given there are $k - d - 1$ sums in $\mathbb{S}_B^C$ it follows that each point can be shared by anywhere between 0 and $k - d - 1$ sums. □

Example 3.1.5. (Continuation of Example 3.1.2) The sumsets for our points s_1, s_2, s_3 are

$$S_1 = \{b_1, b_2, b_4, b_5, b_7\}$$

$$S_2 = \{b_1, b_3, b_4, b_5, b_6, b_7, b_8\}$$

$$S_3 = \{b_2, b_3, b_4, b_7, b_8\}$$

and we can easily see that each sumset is a subset of the B. The set of sumsets of $C - B$ is $\mathbb{S}_B^C = \{S_1, S_2, S_3\}$. We can see that b_5 is shared by S_1 and S_2 so $\mathbb{S}_{b_5} = \{S_1, S_2\}$ and b_5 is a 2-share. The rest of the share values of the in-points will be between 0 and 3 since there are 3 sums in $\mathbb{S}_B^C$.

Definition 3.1.6. Let $C \subseteq \mathbb{Z}_2^d$ be a k-cap of dimension d. Let B be a basis of C. Let $b \in B$. Let $s_1 \in C - B$. Let $i \in \{1, \ldots, k - d - 1\}$.

1. We denote $X_i \subseteq B$ to be the set of i-shares in B.
2. $|X_i|$ is the ***i*-count** of $C - B$. The we denote $|X_i|$ as x_i.
3. The **share string** of a cap is the finite sequence $(x_0, x_1, \ldots, x_{k-d-1})$. We denote the share string of cap C with respect to B as ψ_B^C.

△

To put plainly, the share string of a cap C with basis B with r sumsets is a string $(x_0, \ldots, x_r)$ where each entry x_i is the number of basis points that are shared by i of the sumsets in $\mathbb{S}_B^C$. We are defining X_i to be the set of the x_i basis points that are shared i times which we may periodically refer to as the **count set**.

Example 3.1.7. (Continuation of Example 3.1.2) We can filter each basis point into their respective "count sets":

$$X_0 = \emptyset$$

$$X_1 = \{b_6\}$$

$$X_2 = \{b_1, b_2, b_3, b_5, b_8\}$$

$$X_3 = \{b_4, b_7\}.$$

Taking the cardinalities of these sets gets us our i-counts to which we can determine our share string:

$$x_0 = |X_0| = 0, \qquad x_1 = |X_1| = 1, \qquad x_2 = |X_2| = 5, \qquad x_3 = |X_3| = 2,$$

$$\psi_B^C = (x_0, x_1, x_2, x_3) = (0, 1, 5, 2).$$

Thus the share string for our cap C with respect to basis B is $(0, 1, 5, 2)$. We prove later that $(0, 1, 5, 2)$ is a possible share string for 11-caps of dimension 7.

We have now fully defined share strings, but how exactly will they help us in determining the maximal cap sizes in different dimensions?

Theorem 3.1.8 (The Share String Theorem)**.** *If there exists a share string for k-caps of dimension d but none for $(k+1)$-caps of dimension d then $M(d) = k$.*

Proof. Suppose there exist share strings for k-caps of dimension d but not for $(k+1)$-caps of dimension d. Then there exists a k-cap $C \subseteq \mathbb{Z}_2^d$ of dimension d with basis B with a share string ψ_B^C. Because there are no share strings for $(k+1)$-caps of dimension d it follows that there are no $(k+1)$-caps of dimension d. According to Definition 2.3.4 we can conclude that C is maximal so $M(d) = k$. □

We now have a definitive way of determining the maximal cap sizes for given dimensions. If we can prove that there exist no share strings for a cap size in a given dimension, we know that the next smallest cap size must be maximal (assuming there exist caps of that size in said dimension). The question now is how we go about proving whether or not any given share string can map to a cap or not. While showing that a cap that can map to a given share string is necessary for proving that said share string is viable for caps, we are really only going to care about proving that certain share strings cannot possibly map to caps. A lot of our proofs will distinguish "possible" and"impossible" share strings, where impossible strings cannot have any caps mapped to them and possible ones are not proved to be impossible (even if they are impossible). Methods on how to determine whether or not a string maps to an existing cap can be found in Appendix A.1.

3.2 Sum Decompositions

Before getting into the theorems that shave off string possibilities, we first have to grasp what the nature of the possibilities will look like for different cap sizes in relation to the dimension spanned by the cap. In our rolling example, we somewhat arbitrarily chose two 5-sums and one 7-sum. For every n dependent points in a cap, share strings may exist for every possible combination of possible sum-sizes such that there are n total. For example, in dimension 8, there will be 9 basis points which will allow for sumsets to have 5, 7, or 9 points. 11-caps of dimension 8 with two sums, for example, will have 6 options for sum sizes: 5 and 5, 7 and 7, 9 and 9, 5 and 7, 7 and 9, and 5 and 9. We will need to distinguish the options for different sum sizes when determining the options for possible share strings of caps in given dimensions.

Definition 3.2.1. Let $C \subseteq \mathbb{Z}_2^d$ be a k-cap of dimension d where $d \geq 4$. Let B be a basis for C. Let $r = k - d - 1$ and let z be the greatest odd integer less than or equal to $d + 1$.

1. Let S be the sumset of a point $s \in C - B$ where $|S| = i$. We refer to both S and s as **i-sums**.

2. The **sum decomposition** of $C - B$, denoted $\mathbb{D}_B^C$, is defined as

$$\mathbb{D}_B^C = (5^{n_1}, 7^{n_2}, \ldots, z^{n_{\frac{z-3}{2}}})$$

   where n_i is the number of $(3 + 2i)$-sums in $\mathbb{S}_B^C$.

3. The **decomposition value** of $\mathbb{D}_B^C$ denoted $|\mathbb{D}_B^C|$ is defined as

$$|\mathbb{D}_B^C| = \sum_{i=1}^{\frac{z-3}{2}} (2i + 3)n_i$$

   if $\mathbb{S}_B^C \neq \emptyset$ and $|\mathbb{D}_B^C| = 0$ if $\mathbb{S}_B^C = \emptyset$.

△

Before anything else, we will want to relate the decomposition value to the set of sumsets as it will be necessary for proving Theorem 3.3.3.

Lemma 3.2.2. *Let $C \subseteq \mathbb{Z}_2^d$ be a k-cap of dimension d with basis B. Let $r = k - d - 1$ and suppose $\{S_1, \ldots, S_r\} = \mathbb{S}_B^C$. Then*

$$|\mathbb{D}_B^C| = \sum_{i=1}^{r} |S_i|$$

Proof. Observe that the decomposition value is $5n_1 + 7n_2 + \cdots + zn_{\frac{z-3}{2}}$ where n_i is the number of $(2i+3)$-sums in $\mathbb{S}$. Knowing that each g-sum contains g points, the sum of the cardinalities of each g-sum will be g times the number of g-sums which is exactly $(2i+3) \cdot n_i$ where $2i+3 = g$. Thus the sum of the cardinalities of all r sums of $\mathbb{S}_B^C$ is equal to $\sum_{i=1}^{\frac{z-3}{2}} (2i+3)n_i = |\mathbb{D}_B^C|$. Thus

$$|\mathbb{D}_B^C| = \sum_{i=1}^{r} |S_i|$$

□

The following theorem provides us with the possible sum decompositions for a cap of a given size and dimension.

Theorem 3.2.3 (The Decomposition Theorem)**.** *Let $C \subseteq \mathbb{Z}_2^d$ be a k-cap of dimension d with basis B. Then the possibilities for the sum decomposition $\mathbb{D}_B^C = (5^{n_1}, 7^{n_2}, \ldots, z^{n_{\frac{z-3}{2}}})$ where z is the greatest odd integer less than or equal to $d+1$ are the non-negative integer solutions to the equation*

$$n_1 + \cdots + n_{\frac{z-3}{2}} = k - d - 1.$$

Proof. This follows directly from the fact that there are $k - d - 1$ sumsets in $\mathbb{S}_B^C$ and any combination of sum-sizes are possible in theory. Knowing there can be anywhere from 0 to $k-d-1$ sumsets of any size (of which there are $\frac{z-3}{2}$ sizes) such that the total number of sumsets is equal to $k - d - 1$, it follows that the possibilities for the sum decompositions of $C - B$ are the non-negative integer solutions to the equation

$$n_1 + \cdots + n_{\frac{z-3}{2}} = k - d - 1.$$

□

What this theorem tells us is there there will be several cases for sum decompositions when looking at caps. Given that we have $k - d - 1$ sums that we are dividing into $\frac{z-3}{2}$ sum sizes,

we can use the familiar box and ball problem that asks how many ways there are to arrange x balls into y boxes. In total, there will be $\binom{k-d-2-\frac{z-3}{2}}{k-d-1}$ cases for sum decompositions when searching for the share strings of k-caps of dimension d (where z is the greatest odd number less than or equal to d+1). If we know that there are q sum sizes and r sumsets, then the number of possible sum decompositions is $\binom{r+q-1}{r}$. Luckily, there are generally many cases that cannot exist because of restrictions on larger sums.

Example 3.2.4. Let $C \subseteq \mathbb{Z}_2^8$ be a 15-cap of dimension 8 with basis B. Then there will be $\binom{k-d-2-\frac{z-3}{2}}{k-d-1} = \binom{15-8-2-\frac{9-3}{2}}{15-8-1} = \binom{8}{6} = 28$ possible sum decompositions. We can also come to this conclusion from the fact that $|B| = d+1 = 9$ so $\mathbb{S}_B^C$ can contain 5,7, and 9-sums. Since there are $|\mathbb{S}_B^C| = 15-8-1 = 6$ sumsets and 3 sum sizes it follows that there will be $\binom{6+3-1}{6} = 28$ possible sum decompositions. We can list the possible options required from The Decomposition Theorem to verify:

$$(5^6), (7^6), (9^6)$$

$$(5^5, 7^1), (5^5, 9^1), (5^1, 7^5), (7^5, 9^1), (5^1, 9^5), (7^1, 9^5),$$

$$(5^4, 7^2), (5^4, 9^2), (5^2, 7^4), (7^4, 9^2), (5^2, 9^4), (7^2, 9^4)$$

$$(5^4, 7^1, 9^1), (5^1, 7^4, 9^1), (5^1, 7^1, 9^4)$$

$$(5^3, 7^2, 9^1), (5^3, 7^1, 9^2), (5^2, 7^3, 9^1), (5^1, 7^3, 9^2), (5^2, 7^1, 9^3), (5^1, 7^2, 9^3),$$

$$(5^3, 7^3), (5^3, 9^3), (7^3, 9^3)$$

$$(5^2, 7^2, 9^2)$$

Luckily, we will prove in Chapter 5 that there can be at most one 9-sum, at most four 7-sums, and no pairings of a 9 and 7-sum in dimension 8. Thus our list will diminish to

$$(5^6), (5^5, 7^1), (5^5, 9^1), (5^4, 7^2), (5^3, 7^3), (5^2, 7^4)$$

which is a much more manageable list of decompositions to explore.

Definition 3.2.5. Let $k, d \in \mathbb{N}$ and suppose $k \geq d+1$.

1. We denote the set of share strings for k-caps of dimension d as γ_k^d.

2. Suppose $d \geq 4$. We denote the set of share strings for k-caps of dimension d with string decomposition $\mathbb{D}$ as $\gamma_k^d(\mathbb{D})$.

3. We denote the set of possible i-counts that arise in γ_k^d as $X_k^d(i)$.

△

For every dimension and cap size, there will be a finite set of possible share strings that we denote as γ_k^d. We can further divide our sets by the different sum decompositions of the strings which we denote as $\gamma_k^d(\mathbb{D})$. Once we determine the possible share strings for a cap size in a given dimension, we can also determine what the possible x_i values are. Table 4.4.2 provides a list of the sets of possible i-counts for caps of dimension 7.

Lemma 3.2.6. *Let $k, d \in \mathbb{N}$ and suppose $k \geq d+1$. Let $i \in \{0, \ldots, k-d-1\}$.*

1. *$X_k^d(i) \subseteq \{0, \ldots, d+1\}$.*

2. *If $\gamma_k^d = \emptyset$ and $\gamma_{k-1}^d \neq \emptyset$ then $M(d) = k-1$.*

Proof. (1). Given that there are $d+1$ basis points of which anywhere between 0 and $d+1$ can be shared by i sumsets in $\mathbb{S}_B^C$, it follows that $X_k^d(i) \subseteq \{0, \ldots, d+1\}$.

(2). If a k-cap of dimension d exists then there will exist a share string in γ_k^d. Thus if γ_k^d is empty then there exist no k-cap of dimension d. Then there cannot exist caps of dimension d of greater size than $k-1$ since there are no k sized subcaps that can possibly exist. If $\gamma_{k-1}^d \neq \emptyset$ then there exists a share string for a $(k-1)$-cap of dimension d, and since there exist no $(k+n)$-caps of dimension d where $n \in \mathbb{N} \cup \{0\}$ it follows that k-caps of dimension d are maximal. □

The second fact from lemma 3.2.6 is another way of interpreting the Share String Theorem that we will use when proving the maximal cap sizes for dimensions.

3.3 Two Important Theorems for Using Share Strings

We now understand how to determine the share string of a cap given a basis and a set of dependence relations (or sums). The main goal, however, is to determine the maximal cap sizes for different dimensions which we will prove by determining the impossibility of share strings for caps in said dimension. We know that given a cap size k and a dimension d, there will be $k-d$ entries in the share strings and each entry can be anywhere from 0 to $d+1$. Thus we have $(d+1)^{k-d}$ possibilities which with high dimensions and cap sizes is a lot to look at.

Could the string $(9,2,6,12,0,1)$ map to an existing 19-cap of dimension 13? None of the entries are less than 0 or greater than $d+1 = 13+1 = 14$ so we can't rule it out from that property. However, seeing that we have only 14 basis points to work with and that $x_3 = 12$, all but two of the basis points must be 3 shares and yet the string tells us that there are several 0, 1, 2, and 5-shares in the basis. Thus it is not possible for $(9,2,6,14,0,1)$ to map to a cap of dimension 13. We will prove in general that the sum of the entries of a share string must be equal to the number of basis points.

Theorem 3.3.1. *Let $C \subseteq \mathbb{Z}_2^d$ be a k-cap of dimension d with basis B. Let $r = k-d-1$. Then*

$$\sum_{i=0}^{r} x_i = d+1.$$

Proof. We will first prove that the X_i's are a disjoint partition of B by proving $\bigcup_{i=0}^{r} X_i = B$ and then proving that all X_i's are disjoint.

Suppose for the sake of contradiction that $B - \bigcup_{i=0}^{r} X_i \neq \emptyset$. Then there exists a point $b \in B$ such that $b \notin \bigcup_{i=0}^{r} X_i$. Then $|\mathbb{S}_b| \notin \{0,\ldots,r\}$ which is a contradiction since there exists a share value in $\{0,\ldots,r\}$ for every point in B from Definition 3.1.6. Thus $B - \bigcup_{i=0}^{r} X_i = \emptyset$.

Suppose for the sake of contradiction that $\bigcup_{i=0}^{r} X_i - B \neq \emptyset$. Then there exists point b and some $n \in \{0,\ldots,r\}$ such that $b \in X_n$ and $b \notin B$ which is a contradiction since $X_n \subseteq B$ which we know from Proposition 3.1.4. Thus $\bigcup_{i=0}^{r} X_i - B = \emptyset$. Thus

$$B = \bigcup_{i=0}^{r} X_i.$$

Let $m, n \in \{0, \cdots, r\}$ where $m \neq n$. Suppose for the sake of contradiction that $X_m \cap X_n \neq \emptyset$. Then there exists a point b such that $b \in X_m$ and $b \in X_n$. Then $m = |\mathbb{S}_p| = n \neq m$ which is a contradiction so $X_m \cap X_n = \emptyset$.

Thus, we can conclude that the set of X_i's are a disjoint partition of B. Thus

$$d + 1 = |B| = \left| \bigcup_{i=0}^{r} X_i \right| = \sum_{i=0}^{r} |X_i| = \sum_{i=0}^{r} x_i.$$

□

Now we know that the entries of a share string have to add up to one greater than the dimension. This gives us enough information to find the share strings for caps of dimensions 0-3.

Theorem 3.3.2. *Let $d \in \{0, 1, 2, 3\}$. Then $M(d) = d + 1$.*

Proof. Let $C \subseteq \mathbb{Z}_2^d$ be a k-cap of dimension d with basis B. Then $|B| = d + 1 \leq 4$. Because there are not enough basis points to form a sum, it can only be the case that $k - d - 1 = 0$ so $k = d + 1$.

Using Theorem 3.3.1 we get that $x_0 = d + 1 = k$ so $\psi_B^C = (d + 1)$. Suppose $M(d) > d + 1$. Then there exists a $(d + 2)$-cap $C \subseteq \mathbb{Z}_2^d$ indicating that there will be $(d + 2) - d - 1 = 1$ sum which we determined cannot be the case. Thus $M(d) = d + 1$. □

We can archive sets of possible share strings given a cap size and dimension. In this case, the possible cap size and maximal cap size are both 1 plus the dimension:

d	γ_{d+1}^d	$M(d)$
0	$\{(1)\}$	1
1	$\{(2)\}$	2
2	$\{(3)\}$	3
3	$\{(4)\}$	4

Our archive will become more fruitful once we begin to work in dimensions that actually allow for sums to be produced. Our full archive up until 15-caps of dimension 8 can be found in Appendix A.2

Could the string $(0, 3, 6, 2, 1)$ with the sum decomposition $(5^2, 9^1, 11^1)$ map to an existing 16 cap of dimension 11? We can see that the sum of the entries is equal to 12 which is one greater than the dimension so the string cannot be ruled out by Theorem 3.3.1. The decomposition value, equal to $5+5+9+11 = 30$, indicates that the basis points will be shared across the sums 30 times. Looking at the string, we can decipher that 3 basis points will be shared by one sum, 6 will be shared by two (totalling 12 shares), 2 will be shared by three (totaling 6 shares) and 1 will be shared by four, totalling 3+12+6+4=25 shares across the sums which is contradictory to the 30 we require given our sum decomposition. We will prove that the decomposition value must be equal to the sum of each i-count multiplied by i.

Theorem 3.3.3. *Let $C \subseteq \mathbb{Z}_2^d$ be a k-cap of dimension d with basis B. Let $r = k - d - 1$. Then*

$$|\mathbb{D}_B^C| = \sum_{i=1}^{r} i \cdot x_i.$$

Proof. Let $\mathbb{S} = \mathbb{S}_B^C$ and let $\mathbb{D} = \mathbb{D}_B^C$. Let $S_1, \ldots, S_r$ be the sumsets of $\mathbb{S}$. Let $p \in B$ and let $S \in \mathbb{S}_B^C$.

Observe that if $p \in S$ then $|\{p\} \cap S| = 1$ and if $p \notin S$ then $|\{p\} \cap S| = 0$. Thus we can count the number of points in S using the equation $|S| = \sum_{b \in B} |\{b\} \cap S|$. Thus we can sum the cardinalities of each sum with the following equation:

$$\sum_{i=1}^{r} |S_i| = \sum_{i=1}^{r} \sum_{b \in B} |\{b\} \cap S_i| = \sum_{b \in B} \sum_{i=1}^{r} |\{b\} \cap S_i|.$$

because p is shared by $|\mathbb{S}_p|$ sumsets of the r sumsets, we can deduce that $\sum_{i=1}^{r} |\{p\} \cap S_i| = |\mathbb{S}_p|$. Thus

$$\sum_{i=1}^{r} |S_i| = \sum_{b \in B} |\mathbb{S}_b|.$$

From Lemma 3.2.2 we know that $\mathbb{D} = \sum_{i=1}^{r} |S_i| = \sum_{b \in B} |\mathbb{S}_b|$. Using the fact that the X_i's form a disjoint partition of B which was proved in Theorem 3.3.1, we can conclude that

$$\mathbb{D} = \sum_{b \in B} |\mathbb{S}_b| = \sum_{i=0}^{r} \sum_{b \in X_i} |\mathbb{S}_b| = \sum_{i=0}^{r} \sum_{j=1}^{x_i} i = \sum_{i=1}^{r} i \cdot x_i.$$

□

Theorems 3.3.1 and 3.3.3 give us enough information about the requirements for share strings for us to begin looking at the next set of dimensions with relative ease. We will first want to prove a simple fact about r-counts.

Theorem 3.3.4. *Let $C \subseteq \mathbb{Z}_2^d$ be a k-cap of dimension d with basis B. Let $r = k - d - 1$. Then $x_r \leq \min\{|S_1|, \ldots, |S_r|\}$.*

Proof. The value of x_r is the number of basis points that are shared by all the sumsets in $\mathbb{S}_B^C$. Thus x_r must be less than or equal to the size of the smallest sumset or else there would be more points shared by said sumset than it's cardinality which is not possible. Thus $x_r \leq \min\{|S_1, \ldots, S_r|\}$. □

This theorem is relatively intuitive and only gives only a little bit more information regarding the r-count. However, it can come in handy when whittling down the options for possible share strings of caps whose sizes are small relative to their dimensions.

Theorem 3.3.5. $M(4) = 6$.

Proof. Let $C \subseteq \mathbb{Z}_2^4$ be a k-cap of dimension 4 with basis $B = \{b_1, \ldots, b_5\}$ and share string $\psi_B^C = (x_0, \ldots, x_{k-5})$. Let $\mathbb{S} = \mathbb{S}_B^C$ and let $\mathbb{D} = \mathbb{D}_B^C$. Then $k \geq |B| = 5$ and all sumsets are 5-sums and $\mathbb{D} = (5^{k-5})$.

Suppose $k = 5$. Then from Theorem 3.3.1 we get that $x_0 = 5$ so $\psi_B^C = (5)$. Thus $\gamma_5^4 = \{(5)\}$.

Suppose $k = 6$. Then $|\mathbb{S}| = 6 - 4 - 1 = 1$ so there is one 5-sum $S \in \mathbb{S}$. From Theorem 3.3.3 we get that $x_1 = |\mathbb{D}_B^C| = |S| = 5$. Theorem 3.3.1 tells us that $x_0 + x_1 = 5$ so $x_0 = 0$. Thus $\psi_B^C = (0, 5)$ and $\gamma_6^4 = \{(0, 5)\}$.

Suppose $k = 7$. Then $|\mathbb{S}| = 7 - 4 - 1 = 2$ so there are two 5-sums $S_1, S_2 \in \mathbb{S}$. From Theorem 3.3.3 we get that $x_1 + 2x_2 = |\mathbb{D}_B^C| = |S_1| + |S_2| = 10$ and from Theorem 3.3.1 we get that $x_0 + x_1 + x_2 = 5$. By rearranging our equations, we can see that

$$5 - x_0 - x_2 = x_1 = 10 - 2x_2.$$

Theorem 3.3.4 tells us that $x_2 \leq 5$ and so by using the fact that $x_0 \geq 0$, we get that

$$5 \geq x_2 = x_0 + 5 \geq 5$$

so $x_2 = 5$ and $x_0 = x_1 = 0$. This indicates that both sumsets share all 5 basis points $b_1, \ldots, b_5 \in B$. Thus $s_1 = b_1 + \cdots + b_5 = s_2$ which contradicts the fact that the points in $C - B$ are distinct so there are no share strings for 7-caps of dimension 4. Thus the Share String Theorem allows us to conclude that $M(4) = 6$. □

We can add the following sets to our archive:

$$\gamma_5^4 = \{(5)\} \qquad \gamma_6^4 = \{(0,5)\}$$

3.4 Dimension 5 and Some More Important Theorems

In the max-cap proof of dimension 4, we showed that if two 5-sums shared 5 basis points, then the respective dependent points would be equal which we are assuming not to be the case when looking for possible caps. We can generalize this fact about any two like-sized sums as well as any two sums that have a size difference of 2.

Theorem 3.4.1. *Let $i, j \geq 5$ be odd integers where $j = i + 2$.*

1. *Any two i-sums can share at most $i - 2$ points in a cap.*

2. *An i and a j sum can share at most $i - 1$ points in a cap.*

Proof. (1). Suppose there exist a cap $C \subseteq \mathbb{Z}_2^d$ of dimension d with basis B with two i-sums $S_1, S_2 \in \mathbb{S}_B^C$ that share more than $i-2$ points. We start with the fact that an i-sum can share no more than i points. Suppose for the sake of contradiction that S_1 and S_2 share exactly i points. Then there exists i points $b_1, \ldots, b_i \in S_1 \cap S_2$ where $s_1 = b_1 + \cdots + b_i = s_2$ Which contradicts the fact that the points in $C - B$ are distinct. Thus no two i-sums can share more than $i - 1$ points. Suppose S_1 and S_2 share $i - 1$ points. Then there exists $i - 1$ points $b_1, \ldots, b_{i-1} \in S_1 \cap S_2$ and a point $p \in S_1 - S_2$ and a point $q \in S_2 - S_1$ where $s_1 = p + b_1 + \cdots + b_{i-1}$ and $s_2 = q + b_1 + \cdots + b_{i-1}$. Thus

$$s_1 + p = b_1 + \cdots + b_{i-1} = s_2 + q$$

so the points in $\{s_1, s_2, p, q\} \subseteq C$ form a quad which is a contradiction since we defined C to be a cap. Thus any two i-sums can share at most $i - 2$ points.

(2). Suppose there exist a cap $C \subseteq \mathbb{Z}_2^d$ of dimension d with basis B with an i-sum $S_i \in \mathbb{S}_B^C$ and a j-sum $S_j \in \mathbb{S}_B^C$ that share more than $i-1$ points. We start with the fact that an i-sum can share at most i points. Suppose S_i and S_j share exactly i points. Then there exists i points $b_1, \ldots, b_i \in S_i \cap S_j$ and two points $p, q \in S_j - S_i$ where $s_i = b_1 + \cdots + b_i$ and $s_j = b_1 + \cdots + b_i + p + q$ so

$$s_i = b_1 + \cdots + b_{i-1} = s_j + p + q$$

so the points in $\{s_i, s_j, p, q\} \subseteq C$ form a quad which is a contradiction since we defined C to be a cap. Thus an i-sum and a j-sum can share at most $i-1$ points. □

Theorem 3.4.2 (The Dimension 5 Theorem)**.** *M(5)=7.*

Proof. Let $C \subseteq \mathbb{Z}_2^5$ be a k-cap of dimension 5 with basis B. Let $\mathbb{S} = \mathbb{S}_B^C$ and let $\mathbb{D} = \mathbb{D}_B^C$. Then $k \geq |B| = 6$ and all sums are 5-sums and $\mathbb{D} = (5^{k-6})$.

Suppose $k = 6$. Then from Theorem 3.3.1 we get that $x_0 = 6$. Thus $\psi_B^C = (6)$ and $\gamma_6^5 = \{(6)\}$.

Suppose $k = 7$. Then $|\mathbb{S}| = 7 - 5 - 1 = 1$ so there exists one sum $S \in \mathbb{S}$ and $\mathbb{D} = (5^1)$. From Theorem 3.3.3 we get that $x_1 = |\mathbb{D}| = |S| = 5$. Then $x_0 = 1$ so $\psi_B^C = (1, 5)$ and $\gamma_7^5 = \{(1, 5)\}$.

Suppose $k = 8$. Then $|\mathbb{S}| = 8 - 4 - 1 = 2$ so there are two 5-sums $S_1, S_2 \in \mathbb{S}$ and $\mathbb{D} = (5^2)$. From Theorem 3.3.3 we get that $x_1 + 2x_2 = |\mathbb{D}| = |S_1| + |S_2| = 10$ and from Theorem 3.3.1 we get that $x_0 + x_1 + x_2 = 6$. By rearranging our equations we can see that

$$10 - 2x_2 = x_1 = 6 - x_0 - x_2.$$

Theorem 3.4.1 tells us that $x_2 \leq 3$ (since no two 5-sums can share more than 3 points) and using the fact that $x_0 \geq 0$ we get that

$$3 \geq x_2 = x_0 + 4 \geq 4$$

which is a contradiction so C cannot be a cap. Thus $\gamma_8^5 = \emptyset$ and the Share String Theorem tells us that $M(5) = 7$. □

We can add the following sets to our archive.

$$\gamma_6^5 = \{(6)\} \qquad \gamma_7^5 = \{(1,5)\}$$

$$X_6^5(0) = \{6\} \qquad X_7^5(0) = \{1\} \qquad X_7^5(1) = \{5\}$$

In some of the proofs to come, we will be given information by the share string of a cap about the properties of subsets of the cap. While relatively intuitive, we will want to prove that a subset of a cap must also be a cap.

Definition 3.4.3. Let $C \subseteq \mathbb{Z}_2^d$ be a k-cap of dimension d. Let $C' \subseteq C$. We define C' to be a **subcap** of C. △

Theorem 3.4.4. *Let $C \subseteq \mathbb{Z}_2^d$ be a k-cap of dimension d with basis B. Let C' be a subcap of C.*

1. *If C is a cap then C' is a cap.*
2. *If C' is not a cap then C is not a cap.*

Proof. (1). Suppose for the sake of contradiction that C' is not a cap. Then there exists a quad $\{a, b, c, d\} \in C' \subseteq C$ so there exists a quad in C which contradicts the fact that C is a cap. Thus any subcap must be a cap. (2) is proved by the contrapositive of this proof. □

In many of the theorems to come, we will prove or disprove things about share strings that will involve looking at subcaps.

Theorem 3.4.5. *Let $k, d \in \mathbb{N}$ where $k \geq d + 1 \geq 5$. Let $n \in \mathbb{N}$. If $n < k - M(d-1) - 1$ then $X_k^d(n) \subseteq \{0\}$.*

Proof. We will prove this theorem using the contrapositive. Suppose that $X_k^d(n) \not\subseteq \{0\}$. Because $X_k^d(n) \subseteq \{0, \ldots, d+1\}$ there exists some non zero integer between 1 and $d+1$ in $X_k^d(n)$. Thus there exists a k-cap $C \subseteq \mathbb{Z}_2^d$ of dimension d with a basis B with share string ψ_B^C such that $0 < x_n < d + 1$. Because $x_n > 0$ it follows that there exists a point $b \in B$ such that $|\mathbb{S}_b| = n$. Thus there exists $k - d - 1 - n$ sumsets in $\mathbb{S}_B^C$ that do not share b. Let $A \subseteq C - B$ be the set of dependent points that do not contain b in their sums. Then A is in the affine span of

$B - \{b\}$. Let $C' = A \cup (B - \{b\})$. Because $A \subseteq C$ and $B - \{b\} \subseteq C$ it follows that $C' \subseteq C$ so Theorem 3.4.4 tells us that C' is a cap and $B - \{b\}$ is a basis for C'. Then C' spans a $(|B - \{b\}| - 1) = ((d+1) - 1 - 1) = (d-1)$-flat. Therefore C' is affinely equivalent to a cap that spans dimension $d-1$. Using the fact that A and $B - \{b\}$ are disjoint, we can conclude that $|C'| = |A \cup B - \{d\}| = |A| + |B - \{b\}| = (k - d - 1 - n) + (d + 1 - 1) = k - n - 1$. It follows that C' is affinely equivalent to a $(k-n-1)$-cap of dimension $d-1$. Thus $k - n - 1 \leq M(d-1)$ so $n \geq k - M(d-1) - 1$. By contrapositive, if $n < k - M(d-1) - 1$ then $X_k^d(n) \subseteq \{0\}$. □

Example 3.4.6. Suppose $C \subseteq \mathbb{Z}_2^7$ is a 12-cap of dimension 7 with basis $B = \{b_1, \ldots, b_8\}$ (we will refer to b_i as i) where

s_1	=	1	2	3	4	5			
s_2	=	1	2	3			6	7	
s_3	=	1		3		5	6	7	
s_4	=	1	2		4		6		8

We can see that the share string for this cap is $\psi_B^C = (0, 1, 3, 3, 1)$. Since $x_1 = 1 < 2 = 12 - 9 - 1$ where 12 is the cap size and 9 is the maximal cap size of the previous dimension it should follow that C is not a cap from Theorem 3.4.5.

We can visualize Theorem 3.4.5 using our sums to better understand what it is saying. Knowing that S_4 is the only sumset that shares b_8, we can take a subset of C, namely $C - \{b_8, s_4\}$, that can be spanned by $B - \{b\}$ since none of the other three dependence relations depend on b_8. Because B' uses only 7 points to span the other 3, we can deduce that it spans a 6-flat, meaning C' is affinely equivalent to a 10-cap of dimension 6. However, we've proved that $M(6) = 9$ so a set of 10 points in dimension 6 cannot possibly be a cap so C' is not a cap. Theorem 3.4.4 then allows us to conclude that C cannot possibly be a cap.

The fact proved in Theorem 3.4.5 is very useful when it comes to reducing the cases for share string possibilities when looking at higher cap sizes relative to the dimension. Knowing that entry places less that $k - M(d-1) - 1$ must be zero (or not exist), there can be at most $M(d-1) - d$ share string entries that will be non-zero which heavily limits the number of possible string cases.

The next theorem we will prove will be the first we have that will be able to invalidate share strings using the possible share strings of previous cap sizes of the same dimension. Given that we will have more facts of this nature, it will be useful to actually find all of the share strings for the different cap sizes of each dimension for disproving later cases.

Theorem 3.4.7. *Let $C \subseteq \mathbb{Z}_2^d$ be a k-cap of dimension d with basis B with share string $(x_0, \ldots, x_r)$.*

1. $x_r \leq \max(X_{k-1}^d(r-1))$.

2. *If* $x_r = \max(X_{k-1}^d(r-1))$ *then* $x_{r-1} = 0$.

Proof. (1). Let $n = \max(X_{k-1}^d(r-1))$. Then n is the maximum number of basis points in a $(k-1)$-cap of the same dimension that can be shared by all $r-1$ sumsets of said cap. Suppose for the sake of contradiction that $x_r > n$. Then there are more than n basis points shared by all r sumsets of $C - B$. Let $s \in C - B$ and let $C' = C - \{s\}$. Then C' is a $(k-1)$-cap of dimension d with basis B where all $r-1$ sumsets of $C' - B$ share more than n points which is a contradiction since n is the greatest number of points that can be shared by all sumsets of $(k-1)$-caps of dimension d. Thus it must be the case that $x_r \leq \max(X_{k-1}^d(r-1))$.

(2). Let $n = \max(X_{k-1}^d(r-1))$. Suppose for the sake of contradiction that $x_r = n$ and $x_{r-1} > 0$. Then there exists n basis points shared by all sumsets of $C - B$ and at least one basis point b that is shared by all but one sumset $S \in \mathbb{S}_B^C$. Let $C' = C - \{s\}$. Then C' is a $(k-1)$-cap of dimension d with basis B and all of the sumsets of $C' - B$ share b. Because there are n point in B shared by all sums of $C - B$ (which does not include b) it must be the case that those same points are also shared by all of the sumsets of $C' - B$. Thus there are at least $n+1$ basis points shared by all sums of $C' - B$ which is a contradiction since $(k-1)$-cap of dimension d can share at most $\max(X_{k-1}^d(r-1)) = n$ points. Thus it cannot be the case that $x_r = n$ and $x_{r-1} > 0$ so it must be the case that $x_{r-1} = 0$ if $x_r = \max(X_{k-1}^d(r-1))$. □

As we have seen throughout our max-cap proofs for each dimension, the number of share strings to check increases as well as the number of possible share strings that prove to be valid.

This makes sense, as the possibilities for different kinds of caps will increase as the dimension increases and more possible sum arrangements arise. This leads us to begin asking things like for how many dimensions will we be able to use share strings to prove the max-cap size with the theorems we have? We will see to what extent our theorems get us through dimensions 6 through 8 in the next chapter.

4
Dimensions 6 and 7

4.1 Dimension 6 and the "Sum All" Theorem

Before proving the Dimension 6 Theorem, we must prove a theorem that eliminates caps depending on the size of the point dependency that results when all the points in the sumsets are added. We know that there can be no 2 or 4 point dependencies in our caps since they'd indicate that either two points are equal or a quad is present. We will show that it is sometimes possible to tell if either of these dependencies will show up in a cap using its share string.

Theorem 4.1.1. *Let $(x_0, \ldots, x_r)$ be the share string of set $C \subseteq \mathbb{Z}_2^d$ with respect to basis B.*

1. *If $r + \sum_{i \text{ odd}} x_i = 4$ then C is not a cap.*

2. *If $r + \sum_{i \text{ odd}} x_i = 2$ then C is not a cap.*

Proof. From the hypothesis we know that there are r dependent points that make up the set $C - B$. The sum of these dependent points will be equal to the sum of the basis points shared by the respective sumsets of each dependent point as per Proposition 3.1.4. From The Even Odd Theorem we know that the basis points shared by an odd number of sums will be added an odd number of times and thus result in themselves while those shared by an even number of sums will be added an even number of times and thus get cancelled out. Thus the sum of the r affinely dependent points in $C - B$ will equal the sum of the basis points that are shared an odd

number of times. There are $\sum_{i \text{ odd}} x_i$ basis points shared an odd number of times so the size of the resulting point dependency will be $r + \sum_{i \text{ odd}} x_i$. If there are 4 points in the dependency then a quad exists in C and if there are 2 points in the dependency then the two points in C are equal. Both of these cases are not possible if C is a cap. Thus if $r + \sum_{i \text{ odd}} x_i$ is equal to 4 or 2 then C is not a cap. □

Example 4.1.2. Suppose $C \subseteq \mathbb{Z}_2^7$ is an 11-cap of dimension 7 with basis $B = \{b_1, \ldots, b_8\}$ and share string $\psi_B^C = (0, 1, 7, 0)$. Then there are 3 dependent point $s_1, s_2, s_3 \in C - B$. The string tells us that there are 7 basis points shared by two sumsets and 1 basis point shared by one of the sumsets. The sums may look something like the following arrangement (where we are denoting b_i as i):

$$\begin{array}{lllllllll} s_1 & = & 1 & 2 & 3 & 4 & 5 & & \\ s_2 & = & 1 & 2 & 3 & & & 6 & 7 \\ s_3 & = & & & & 4 & 5 & 6 & 7 & 8 \end{array}$$

By adding the points in $C - B$ we get $s_1 + s_2 + s_3 = b_8$ which indicates that s_1, s_2, s_3, and b_8 form a quad so C cannot be a cap. Because b_8 was the only basis point shared by an odd number of sumsets, it is the only point that is not cancelled out in the sum of the basis points. We can also see that $r + \sum_{i \text{ odd}} x_i = 3 + 1 = 4$ which verifies that our equation gives us the size of the point dependency when we add the points in $C - B$. Thus when we "sum all" of the dependent points of a supposed cap and are left with a 2 or 4 point dependency, we can conclude that the share string of the cap will be impossible and thus the sum of the number of dependent points and the odd-shares cannot be 2 or 4.

Theorem 4.1.3 (The Dimension 6 Theorem)**.** *$M(6) = 9$.*

Proof. Let $C \subseteq \mathbb{Z}_2^6$ be a k-cap of dimension d with basis B. Let $\mathbb{S} = \mathbb{S}_B^C$ and let $\mathbb{D} = \mathbb{D}_B^C$. Then $k \geq |B| = 7$ and sums in $\mathbb{S}$ are either 5-sums or 7-sums.

suppose $k = 7$. Then from Theorem 3.3.1 we get that $x_0 = 7$. Thus $\psi_B^C = (7)$ and $\gamma_7^6 = \{(7)\}$.

Suppose $k = 8$. Then $\mathbb{S} = 8 - 6 - 1 = 1$ so there exists one sum $S \in \mathbb{S}$. The Decomposition Theorem tells us that the possible sum decompositions are (5^1) and (7^1). Case 1: Suppose $\mathbb{D} = (5^1)$. Then from Theorems 3.3.1 and 3.3.3 we get that $x_0 + x_1 = 7$ and $x_1 = |\mathbb{D}| = |S| = 5$

k	γ_k^6
7	(7)
8	$(2,5),(0,7)$
9	$(0,4,3)$

Figure 4.1.1: Share Strings of Dimension 6

so $x_0 = 2$. Thus $\psi_B^C = (2,5)$ and $\gamma_8^6(5^1) = \{(2,5)\}$. Case 2: Suppose $\mathbb{D} = (7^1)$. Then from Theorems 3.3.1 and 3.3.3 we get that $x_0 + x_1 = 7$ and $x_1 = |\mathbb{D}| = |S| = 7$ so $x_0 = 0$. Thus $\psi_B^C = (0,7)$ and $\gamma_8^6(7^1) = \{(0,7)\}$.

Suppose $k = 9$. Then $\mathbb{S} = 9-6-1 = 2$ so there exist two sum $S_1, S_2 \in \mathbb{S}$. Theorem 3.3.1 tells us that $x_0 + x_1 + x_2 = 7$. From Theorem 3.4.5 we can conclude that $x_0 = 0$ since all x_i's where $i < k - M(d-1) - 1 = 9 - 7 - 1 = 2$ must be equal to 0 so $x_1 + x_2 = 7$. The Decomposition Theorem tells us that our options for sum decompositions are $(5^2), (5^1, 7^1)$, and (7^2). Case 1: Suppose $\mathbb{D} = (5^2)$. Then from Theorem 3.3.3 we get that $x_1 + 2x_2 = |\mathbb{D}| = 10$ so $x_1 = 4$ and $x_2 = 3$ and thus $\psi_B^C = (0,4,3)$ and $\gamma_9^6(5^2) = \{(0,3,4)\}$. Case 2: Suppose $\mathbb{D} = (5^1, 7^1)$. Then Theorem 3.3.3 tells us $x_1 + x_2 = |\mathbb{D}| = 12$ so $x_1 = 2$ and $x_2 = 5$. Thus the 5-sum and the 7-sum share 5 points which is not possible from Theorem 3.4.1 so $\gamma_9^6(5^1, 7^1) = \emptyset$. Case 3; Suppose $\mathbb{D}_B^C = (7^2)$. We can easily see that both 7 sums must share the seven basis points in B. This is a contradiction since Theorem 3.4.1 tells us any two 7-sums can share at most 5 points. Thus $\gamma_9^6(7^2) = \emptyset$.

Suppose $k = 10$. Then $\mathbb{S} = 10 - 6 - 1 = 3$ so there exist three sums $S_1, S_2, S_3 \in \mathbb{S}$. From the $k = 9$ case we saw that no 9-caps with 7-sums exist so the only possible sum decomposition is (5^3) and $\{S_1, S_2, S_3\}$ must all be 5-sums. Then from Theorems 3.3.1 and 3.3.3 we get that $x_0 + x_1 + x_2 + x_3 = 7$ and $x_1 + 2x_2 + 3x_3 = |\mathbb{D}| = 15$. From Theorem 3.4.5 we can conclude that $x_0 = x_1 = 0$ since all x_i's where $i < k - M(d-1) - 1 = 10 - 7 - 1 = 2$ must be equal to 0. Thus $x_2 + x_3 = 7$ and $2x_2 + 3x_3 = 15$ so $\psi_B^C = (0,0,6,1)$. Theorem 4.1.1 tells us that ψ_B^C cannot be a possible share string since $k - d - 1 + \sum_{i \text{ odd}} x_i = 10 - 6 - 1 + 1 = 4$ indicating any set of points that can map to ψ_B^C will necessarily contain a quad. Thus $\gamma_{10}^6 = \emptyset$ so The Share String Theorem tells us that $M(6) = 9$. □

While not the focus of this project, we can determine that $(0, 7)$ will map to a complete 8-cap of dimension 6. Let $C \subseteq \mathbb{Z}_2^6$ be an 8-cap of dimension 6 with basis B and share string $(0, 7)$. Then $\mathbb{D}_B^C = (7^1)$ meaning the single point $s \in C - B$ is a 7-sum. Because there are no sum decompositions with 7-sums for 9-caps, it follows that there is no point $p \in \mathbb{Z}_2^6 - C$ such that $C \cup \{p\}$ is a cap since it would require that both s and p be 5-sums which is not the case due to s being a 7-sum. Thus 8-caps that map to (0,7) are complete.

4.2 8, 9, and 10-Caps of Dimension 7

Due to the increase in share string possibilities, we will break up the $M(7)$ theorem into separate proofs. We will first prove a general theorem that tells us what all the share strings with non-zero x_0's will be in a dimension as it pertains to the previous dimension.

Theorem 4.2.1. *Let $k, d \in \mathbb{N}$. Suppose $k \geq d + 1 \geq 5$. Let $r = k - d - 1$. Let $n, x_1, \ldots, x_r \in \{0, \ldots, d + 1\}$. Suppose $n > 0$. Then $(n, x_1, \ldots, x_r) \in \gamma_k^d$ if and only if $(0, x_1, \ldots, x_r) \in \gamma_{k-n}^{d-n}$.*

Proof. $\implies$ Suppose $(n, x_1, \ldots, x_r) \in \gamma_k^d$. Then there exists a k-cap $C \subseteq \mathbb{Z}_2^d$ of dimension d with basis B such that $\psi_B^C = (n, x_1, \ldots, x_r)$. Then there exists a set P of n points in B that are not shared by any sumsets in $\mathbb{S}_B^C$. Because none of the points in $C - B$ are dependent upon the points in P, it follows that $B - P$ is a basis for $C - B$. Thus $C - P$ is a $|C - P| = |C| - |P| - |P - C| = (k - n)$-cap spanned by $|B - P| = |B| - |P| - |P - B| = d + 1 - n$ points, meaning $C - P$ spans a $(d - n)$-flat. Therefore $C - P$ is affinely equivalent to a $k - n$ cap that spans dimension $d - n$. Let $\{X_0', \ldots, X_r\}$ be the count sets of $C - P$ with respect to B. Because the the sumsets of of $C - B$ are spanned by $B - P$ it follows that $X_i' = X_i$ for $1 \leq i \leq r$. We can conclude that $X_0' = \emptyset$ since we subtracted all of the basis points that were not shared by any sums when creating $C - P$. $C - P$ must be a cap since it is a subset of C. Thus there exists a $(k - n)$-cap of dimension $d - n$ with share string $(0, x_1, \ldots, x_r)$, meaning $(0, x_1, \ldots, x_r) \in \gamma_{k-n}^{d-n}$.

$\impliedby$ Suppose $(0, x_1, \ldots, x_r) \in \gamma_{k-n}^{d-n}$. Then there exists a $(k - n)$-cap $C \subseteq \mathbb{Z}_2^{d-n}$ of dimension $d - n$ with basis B such that $\psi_B^C = (0, x_1, \ldots, x_r)$. It follows that there must be a $(k - n)$-cap $C' \subseteq \mathbb{Z}_2^d$ with basis B' that spans a $(d - n)$-flat in dimension d such that $\psi_{C'}^{B'} = (0, x_1, \ldots, x_r)$.

Thus there are n points $P = \{p_1, \ldots, p_n\} \subseteq \mathbb{Z}_2^d$ that are affinely independent of each other and the points in C' meaning $C' \cup P$ is a $|C' \cup P| = |C'| + |P| - |C' \cap P| = (k - n + n) = k$-cap that spans dimension $(d - n) + n = d$. The points in P are thus not shared by any of the sumsets of the points in $C' - B'$ so $\mathbb{S}_{B' \cup P}^{C' \cup P} = \mathbb{S}_B^C$. Let $X_0', \ldots, X_r'$ be the share sets of $C' - (B' \cup P)$. Suppose for the sake of contradiction that $X_i' \neq X_i$ for some $1 \leq i \leq k - d - 1$. Then there exists a point $b \in B \cup P$ that are shared by i sumsets in $\mathbb{S}_{B' \cup P}^{C' \cup P}$ by not in $\mathbb{S}_B^C$, or vice versa, which is a contradiction since we showed that $\mathbb{S}_{B' \cup P}^{C' \cup P} = \mathbb{S}_B^C$. Thus $X_i' = X_i$ for $1 \leq i \leq k - d - 1$. Observe that $X_0' = X_0 \cup P$ since X_0 are the points in B' that are not shared by any sumsets of $\mathbb{S}_{B' \cup P}^{C' \cup P}$ and P are the points we added to C' that were independent of any points in C' and thus are not shared by any sumsets of $\mathbb{S}_{B' \cup P}^{C' \cup P}$. Thus $x_0' = |X_0 \cup P| = |X_0| + |P| - |X_0 \cap P| = 0 + n + 0 = n$. Thus there exists a k-cap of dimension d with the share string $(n, x_1, \ldots, x_r)$ so $(n, x_1, \ldots, x_r) \in \gamma_k^d$.

Therefore $(n, x_1, \ldots, x_r) \in \gamma_k^d$ if and only if $(0, x_1, \ldots, x_r) \in \gamma_{k-n}^{d-n}$. □

This theorem is useful because when all of the possible share strings of a dimension are known, then all of the share strings with $x_0 \neq 0$ in the next dimension are also known. This fact, like many of the others we have proved, reduces the amount of cases that need to be checked by allowing us to set $x_0 = 0$ for the remainder of our calculations.

Lemma 4.2.2. $(8), (1, 7), (3, 5),$ *and* $(1, 4, 3)$ *are all the share strings for caps of dimension 7 such that* $x_0 \neq 0$.

Proof. Let $C \subseteq \mathbb{Z}_2^7$ be a k-cap of dimension d with basis B. Suppose $x_0 > 0$. Then from Theorem 4.2.1 and referring to Figure 4.1.1 we get that ψ_B^C could be equal to $(8), (1, 7), (3, 5)$, or $(1, 4, 3)$ and no other share strings with $x_0 \neq 0$ exist. □

Now when searching for share strings, we do not have to worry about the case in which $x_0 = 0$ which effectively eliminates an entire variable from cases and thus allowing for less cases to be checked. We will also want to know in advance if we can exclude any sum decompositions from our search to limit the number of cases we have to check.

Lemma 4.2.3. *A set of sumsets of a cap of dimension 7 cannot contain more than one 7-sum.*

Proof. Let $C \subseteq \mathbb{Z}_2^7$ be a k-cap of dimension d with basis $B = \{b_1, \ldots, b_8\}$. Suppose there are two 7-sums $S_1, S_2 \in \mathbb{S}_B^C$. Then S_1 and S_2 each share all but one point in B. Without loss of generality suppose $b_1 \notin S_1$ and $b_2 \notin S_2$. Then six points, namely $b_3, \ldots, b_8$ are shared by S_1 and S_2 which is a contradiction since Theorem 3.4.1 tells us that any two 7-sums can share at most 5 points. The same logic can be used to show that a similar contradiction will arise both sumsets exclude the same basis point. Thus a set of sumsets of a cap of dimension 7 cannot contain more than one 7-sum. □

With this fact, we can see that the sum decomposition of a cap of dimension 7 will contain at most one 7-sum, so there will be at most 2 possibilities for sum decompositions when working in dimension 7. More explicitly, with a sum decomposition for a k-cap of dimension 7 where $\mathbb{D} = (5^{n_1}, 7^{n_2})$, it will either be the case that $n_1 = k - d - 2$ and $n_2 = 1$, or $n_1 = k - d - 1$ and $n_2 = 0$.

Theorem 4.2.4. $\gamma_8^7 = \{(8)\}$ *and* $\gamma_9^7 = \{(3,5),(1,7)\}$.

Proof. Let $C \subseteq \mathbb{Z}_2^7$ be an 8-cap of dimension 7 with basis B. From Theorem 3.3.1 we get that $x_0 = 8$ so there are no share strings other than (8) for 8-caps of dimension 7.

Let $C \subseteq \mathbb{Z}_2^7$ be a 9-cap of dimension 7 with basis B such that $x_0 = 0$. Then $|\mathbb{S}_B^C| = 9-7-1 = 1$ so there exists one sum $S \in \mathbb{S}_B^C$ and it is either the case that $\mathbb{D}_B^C$ is equal to (5^1) or (7^1). Thus $|\mathbb{D}_B^C| = 5$ or $|\mathbb{D}_B^C| = 7$. From Theorem 3.3.1 and 3.3.3 we get that $x_0 + x_1 = 8$ and that $x_1 = |\mathbb{D}_B^C|$. Because there is no solution for x_1 when $x_0 = 0$ we can conclude that there are no strings other than $(3,5)$ and $(1,7)$ for 9-caps of dimension 7. □

Theorem 4.2.5. $\gamma_{10}^7 = \{(1,4,3),(0,6,2),(0,4,4)\}$

Proof. Let $C \subseteq \mathbb{Z}_2^7$ be an 10-cap of dimension 7 with basis B such that $x_0 = 0$. Let $\mathbb{S} = \mathbb{S}_B^C$ and let $\mathbb{D} = \mathbb{D}_B^C$. Then $|\mathbb{S}| = 10 - 7 - 1 = 2$ meaning there are 2 sums $S_1, S_2 \in \mathbb{S}$. The possible sum decompositions are $(5^2), (5^1, 7^1)$, and (7^2) from The Decomposition Theorem. From Lemma 4.2.3 we know there can be at most one 7-sum in $\mathbb{S}$ so it cannot be the case that $\mathbb{D} = (7^2)$.

From Theorem 3.3.1 and 3.3.3 we get that $x_1 + x_2 = 8$ and $x_1 + 2x_2 = |\mathbb{D}|$. For $\mathbb{D} = (5^2)$ we get that $\psi_B^C = (0, 6, 2)$ and for $\mathbb{D} = (5^1, 7^1)$ we get that $\psi_B^C = (0, 4, 4)$. Thus $\gamma_{10}^7 = \{(1, 4, 3), (0, 6, 2), (0, 4, 4)\}$. □

We now get to a point where we are repeating the same algorithm over and over again to find possible share strings while only changing a few simple parameters. We can use a computer program to calculate the possibilities for caps in the manner we have been doing without having to spend all of our time doing algebra. We use variations of the Processing code in Figure 4.2.1 to compute the possible share strings given a dimension, cap size, and sum decomposition with the constraints of Theorems 3.3.1, 3.3.3, 3.4.5 4.1.1, and 4.3.1. Later variations will also include Theorem 4.3.3.

4.3 11-Caps and the Pair-Share Theorem

In the proof for 11-caps, we will run into a case for a share string that we can rule out not by Theorem 4.1.1 but by a slightly different property that uses the same logic which we will prove next.

Theorem 4.3.1. *Let $C \subseteq \mathbb{Z}_2^7$ be a k-cap of dimension 7 with basis B. Then it cannot be the case that*

$$k + \sum_{i \ odd} x_i = 18.$$

Proof. Suppose for the sake of contradiction that $k + \sum_{i \text{ odd}} x_i = 18$. Because $|C - B| = |C| - |B| = k - 8$ we can conclude that $|C - B| + \sum_{i \text{ odd}} x_i = 10$ which indicates that the number of points in $C - B$ added to the number of basis points with odd share-values is 10. The Even Odd Theorem tells us that the sum of the points in $C - B$ will be equal to the sum of the basis points with odd share values. This of course indicates there is a 10 point dependency in C that includes the dependent points and the basis points with odd share values. From Theorem 3.4.4 we know that these 10 points form a 10-cap which we will call C'. Because $M(6) = 9$ it cannot be the case that C' span a dimension lower than 7 so it must span dimension 7. Thus there exists

```
int d = 7;    //dimension
int k = 11;   //cap size
int n1 = 2;   //number of 5-caps
int n2 = 1;   //number of 7-caps
int dv;       //decomposition value

dv = 5*n1 + 7*n2;
r = k - d - 1;

for(int x0=0; x0<=d+1; x0++){         //r+1 for loops should be used
  for(int x1=0; x1<=d+1; x1++){       //unless Theorem 3.4.5 is taken
    for(int x2=0; x2<=d+1; x2++){     //into consideraiton
      for(int x3=0; x3<=d+1; x3++){
        for(int x4=0; x4<=d+1; x4++){
          for(int x5=0; x5<=d+1; x5++){                //Theorem
           if((x0 + x1 + x2 + x3 + x4 + x5 == d+1  )   //3.3.1
           && (x1 + 2*x2 + 3*x3 + 4*x4 + 5*x5 == dv)   //3.3.3
           && (k-d-1 + x1 + x3 + x5 != 4           )   //4.1.1
           && (k-d-1 + x1 + x3 + x5 != 2           )   //4.1.1
           && (k-d-1 + x1 + x3 + x5 != 10          )   //4.3.1 (d = 7 only)
           && (x0 == 0)                            ){  //3.4.5

        println(x0, x1, x2, x3, x4, x5);

}}}}}}}
```

Figure 4.2.1: The share string finder: a Processing code that computes the possible share strings of a given cap size, dimension, and sum decomposition. This specific code computes the possible share strings for 11 caps of dimension 7 with the sum decomposition $(5^2, 7^1)$.

a basis B' for C' with 8 points meaning there exists $10 - 8 = 2$ sumsets $S_1, S_2 \in \mathbb{S}_{B'}^{C'}$. Knowing that there can be at most one 7-sum in the set of sumsets of a cap of dimension 7, we know that at least one of S_1 and S_2 is a 5-sum, say S_1. Then there exists 5 basis points $b_1, \ldots, b_5 \in B'$ such that $s_1 = b_1 + \cdots + b_5$. Observe that there exists 3 other basis points $\{b_6, b_7, b_8\}$. We know that the points in C' sum to 0 so $s_2 + b_6 + b_7 + b_8 = s_2 + b_6 + b_7 + b_8 + (s_1 + b_1 + \cdots + b_5) = 0$. Thus s_2, b_6, b_7, and b_8 form a quad meaning C' is not a cap and thus C is not a cap which contradicts our hypothesis. Thus it cannot be the case that $k + \sum_{i \text{ odd}} x_i = 18$. □

Theorem 4.3.2. $\gamma_{11}^7 = \{(0, 2, 5, 1), (0, 3, 3, 2), (0, 1, 5, 2)\}$.

Proof. Let $C \subseteq \mathbb{Z}_2^7$ be an 11-cap of dimension 7 with basis B. Let $\mathbb{S} = \mathbb{S}_B^C$ and let $\mathbb{D} = \mathbb{D}_B^C$. Then $\mathbb{S} = 11 - 7 - 1 = 3$ meaning there are 3 sums in $\mathbb{S}$. Thus the options for sum decompositions are $(5^3), (5^2, 7^1), (5^1, 7^2)$, and (7^3). The latter two decompositions cannot exist from Theorem 4.2.3.

Case 1: Suppose $\mathbb{D} = (5^3)$. Then $|\mathbb{D}| = 15$. Using our share string finder, we get that the options for possible share strings are $(0, 3, 3, 2)$ and $(0, 2, 5, 1)$, and $(0, 4, 1, 3)$. Observe that $18 = 11 + 4 + 3 = k + \sum_{i \text{ odd}} x_i$ so Theorem 4.3.1 tells us that $(0, 4, 1, 3)$ is not a possible share string for C.

Case 2: Suppose $\mathbb{D} = (5^2, 7^1)$. Then $|\mathbb{D}| = 17$. Using our share string finder, we get that the options for possible share strings are $(0, 2, 3, 3)$ and $(0, 1, 5, 2)$. We will disprove the possibility of $(0, 2, 3, 3)$ in example 4.3.4 using the Pair-Share Theorem. □

The next theorem will look at how the sum decomposition and the share string of a cap must adhere to a certain property. When any basis point is shared by two or more sumsets, we can calculate the number of *pairs* of sumsets that share the point. For example if a basis point b is a 4-share, then there are 4 sums that share b and $\binom{4}{2} = 6$ pairs of sumsets that share b. If the 4 sums are $S_1, \ldots, S_4$, then

$$b \in S_1 \cap S_2, \qquad b \in S_1 \cap S_3, \qquad b \in S_1 \cap S_4$$

$$b \in S_2 \cap S_3, \qquad b \in S_2 \cap S_4, \qquad b \in S_3 \cap S_4.$$

When looking at any pair of sums, we can use the facts from Theorem 3.4.1 to deduce how many possible "pair-shares" a sum decomposition can allow. For example, if a decomposition has two 5-sums and two 7-sums, then the two 5 sums can share at most 3 points, the two 7 sums can share at most 5 points, and the pairs of one 5 and one 7-sum can share at most 4 points between them of which there are $n_1 \times n_2 = 2 \times 2 = 4$ pairs. Thus, the sum decomposition allows for $3 + 5 + 4(4) = 24$ of these pair-shares to accumulate between the sumsets.

While a sum decomposition tells us the maximum possible number of pair-shares of a cap, a share string contains the information to tell us exactly how many pair-shares will arise in the cap. For each x_i, there are $\binom{i}{2}$ pairs of sums that will share each i-share and thus there will be exactly

$$\sum_{i=2}^{r} x_i \binom{i}{2}$$

pair-shares between the r sumsets. Knowing how many pair-shares are allowed by the sum decomposition, we know that such number must be greater or equal to the value of the above equation. Say the share string of our cap with sum-decomposition $(5^2, 7^2)$ is $(0, 2, 1, 2, 3)$. Seeing that $\sum_{i=1}^{4} x_i = 8$ we can conclude that $(0, 2, 1, 2, 3)$ is a potential 12-cap of dimension 7. We can't immediately discard the string simply by looking at the x_4 value since sets of 5 and 7-sums are allowed to share up to 3 points collectively. However, we can see that there will exist

$$\sum_{i=2}^{4} x_i \binom{i}{2} = x_2 \binom{2}{2} + x_3 \binom{3}{2} + x_4 \binom{4}{2} = 1(1) + 2(3) + 3(6) = 25$$

pair-shares which is greater than the greatest possible number allowed by the sum decomposition (24) which tells us the string cannot exist. We will now prove this fact for any sum decomposition for a cap of given size of a given dimension.

Theorem 4.3.3 (The Pair-Share Theorem)**.** *Let $C \subseteq \mathbb{Z}_2^d$ be a k-cap of dimension d where $\mathbb{D}_B^C = (5^{n_1}, 7^{n_2}, \ldots, z^{n_{\frac{z-3}{2}}})$ where z is the greatest odd integer less than or equal to $d+1$. Then ψ_B^C is only a possible share string if*

$$\sum_{i=1}^{\frac{z-3}{2}}(2i+1)\binom{n_i}{2}+\sum_{i=1}^{\frac{z-5}{2}}(2i+2)n_in_{i+1}+\sum_{i=1}^{\frac{z-7}{2}}\left(\sum_{j=i+2}^{\frac{z-3}{2}}(2i+3)n_in_j\right)\geq\sum_{i=2}^{r}x_i\binom{i}{2}.$$

Proof. We can count the number of possible pair-shares allowable by a sum-decomposition by counting the number of shares allowed by pairs of sums that are the same size, sums of size difference 2, and sums of size difference 4 and greater.

From Theorem 3.4.1 we know that any two g-sums can share at most $g-2$ points. Thus each pair of the n_i total $(2i+3)$-sums in $\mathbb{S}_B^C$ can share at most $2i+1$ points with each other. There are $\binom{n_i}{2}$ pairs of $(2i+3)$-sums. Therefore there are a maximum of $(2i+1)\binom{n_i}{2}$ shares between pairs of like size sums. Thus there are a maximum of

$$\sum_{i=1}^{\frac{z-3}{2}}(2i+1)\binom{n_i}{2}$$

possible shares between pairs of like-size sums in $\mathbb{S}_B^C$.

From Theorem 3.4.1 we know that any g and $g+2$-sums can share at most $g-1$ points. Thus each pair of the n_i total $(2i+3)$-sums and n_{i+1} total $(2i+5)$-sums in $\mathbb{S}_B^C$ can share no more than $g-1$ points. In total, there are n_in_{i+1} pairs of sums that contain a unique pairing of a $(2i+3)$-sum and a $(2i+5)$-sum. Therefore there are a maximum of $(2i+2)n_in_{i+1}$ shares between such pairs. Therefore there are a maximum of

$$\sum_{i=1}^{\frac{z-5}{2}}(2i+2)n_in_{i+1}$$

possible shares between pairs of sumsets with a size difference of 2 in $\mathbb{S}_B^C$.

Given that there are no universal sharing restrictions between sums with a size difference of 4 or greater, we can conclude that such sums can only share as many points as the size of the smallest sum. Thus each pair of the n_i total $(2i+3)$-sumsets and the $n_{i+1+\frac{k}{2}}$ total $(2i+5+k)$-sumsets in $\mathbb{S}$ can share a maximum of $2i+3$ points. There are $n_in_{i+1+\frac{k}{2}}$ pairs of such sets, and thus the culmination of such pairs can have at most $in_in_{i+1+\frac{k}{2}}$ shares. In order to add together the maximum number of possible shares by such pairs of sums, we will, for each sum size $2i+3$ of $\mathbb{S}$ such that there is a sum of size 4 or greater, add the maximum number of shares by such

pairs of sums for all sums of size of 4 or greater. Since $\frac{z-3}{2}$ is the greatest sum size, only sums up to size $\frac{z-7}{2}$ will be able to share points with sums of size 4 or greater. Thus there are a maximum of

$$\sum_{i=1}^{\frac{z-7}{2}}\left(\sum_{j=i+2}^{\frac{z-3}{2}}(2i+3)n_in_j\right)$$

possible shares between pairs of sumsets with a size difference of 4 or greater in $\mathbb{S}_B^C$.

Collectively, there are at most

$$\sum_{i=1}^{\frac{z-3}{2}}(2i+1)\binom{n_i}{2}+\sum_{i=1}^{\frac{z-5}{2}}(2i+2)n_in_{i+1}+\sum_{i=1}^{\frac{z-7}{2}}\left(\sum_{j=i+2}^{\frac{z-3}{2}}(2i+3)n_in_j\right)$$

possible pair shares between pairs of sumsets in $\mathbb{S}_B^C$ given by the requirements of $\mathbb{D}_B^C$. Thus, this value must then be greater than the exact number of pair-shares which we can figure out using ψ_B^C. For each point $b \in X_i$, b is shared by i sums. Between such sums there are $\binom{i}{2}$ total pairs of sums that share p. Given that there are x_i basis points in X_i, we can conclude that there are $x_i\binom{i}{2}$ total pair-shares involving x_i-shares. Thus there are exactly

$$\sum_{i=2}^{r}x_i\binom{i}{2}$$

total pair-shares of $\mathbb{S}_B^C$. Thus for ψ_B^C to be a possible share string it must be the case that

$$\sum_{i=1}^{\frac{z-3}{2}}(2i+1)\binom{n_i}{2}+\sum_{i=1}^{\frac{z-5}{2}}(2i+2)n_in_{i+1}+\sum_{i=1}^{\frac{z-7}{2}}\left(\sum_{j=i+2}^{\frac{z-3}{2}}(2i+3)n_in_j\right)\geq\sum_{i=2}^{r}x_i\binom{i}{2}.$$

□

Example 4.3.4. Take the share string $(0,2,3,3)$ which maps to an 11-cap of dimension 7. Our decomposition value is $\sum_{i=1}^{3} i\cdot x_i = 1(2)+2(3)+3(3) = 17$ which is equal to $5n_i+7n_2$ which indicates that our sum decomposition must be $(5^2,7)$. The two 5-sums can share at most 3 points with each other and can each share at most 4 points with the 7-sum per Theorem 3.4.1. Thus there are at most 11 shares possible within the sum decomposition. Knowing 7 is the greatest sum-size in $\mathbb{D}_B^C$ We can use the formula to verify:

$$\sum_{i=1}^{2}(2i+1)\binom{n_i}{2}+\sum_{i=1}^{1}(2i+2)n_in_{i+1}+\sum_{i=1}^{0}\left(\sum_{j=i+2}^{2}(2i+3)n_in_j\right)$$

$$= (2 \cdot 1 + 1)\binom{2}{2} + (2 \cdot 2 + 1)\binom{1}{2} + (2 \cdot 1 + 2)2 \cdot 1 = 11.$$

Looking at our string, we can see that there are two 1-shares which aren't shared by any pairs of sums. The three 2-shares are each shared by exactly 1 pair of sums, and the three 3-shares are shared by exactly $\binom{3}{2} = 3$ pairs of sums. Thus the string requires that there are 3(1)+3(3)=15 shares between pairs of sums which is greater than the maximum number of shares possible given the sum decomposition of the cap. We can use the formula to verify:

$$\sum_{i=2}^{r} x_i \binom{i}{2} = \sum_{i=2}^{3} x_i \binom{i}{2} = x_2\binom{2}{2} + x_3\binom{3}{2} = 3(1) + 3(3) = 15 > 11.$$

Therefore, the string $(0, 2, 3, 3)$ is not a possible for 11-caps of dimension 7.

We can try to construct a cap C with basis B where $\psi_B^C = (0, 2, 3, 3)$ to better visualize why it is impossible. Since $x_3 = 3$ we know there exists 3 basis points $b_1, b_2, b_3 \in B$ shared by all sumsets $s_1, s_2, s_3 \in \mathbb{S}_B^C$. By denoting b_i as i, we can start off by writing

$$\begin{array}{lcccc} s_1 & = & 1 & 2 & 3 \\ s_2 & = & 1 & 2 & 3 \\ s_3 & = & 1 & 2 & 3 \end{array}$$

Without loss of generality, we can assume S_1 will be the 7-sum. Then we know that S_2 and S_3 cannot share any more points with each other since 5-sums can share at most 3 points. Since $x_2 = 3$ there exists 3 basis points $b_4, b_5, b_6 \in B$ shared by 2 sums in $\mathbb{S}_B^C$. We know that they each must be shared by S_1 and one of $\{S_2, S_3\}$ since S_2 and S_3 cannot share any more points together. Thus two of the 2-shares would have to be shared by one of the 5-sums, say S_2, which would look like the following:

$$\begin{array}{lcccccccc} s_1 & = & 1 & 2 & 3 & 4 & 5 & 6 \\ s_2 & = & 1 & 2 & 3 & 4 & 5 & \\ s_3 & = & 1 & 2 & 3 & & & 6 \end{array}$$

Thus one of the 5-sums (S_2) and the 7-sum (S_1) will inevitably be forced to share 5 points which is not possible from Theorem 3.4.1 so there cannot exist a cap with the share string $(0, 2, 3, 3)$.

4.4 12-Caps and the Dimension 7 Theorem

Theorem 4.4.1. $\gamma_{12}^7 = \{(0, 0, 5, 2, 1), (0, 0, 4, 4, 0), (0, 0, 3, 4, 1)\}$.

Proof. Let $C \subseteq \mathbb{Z}_2^7$ be a 12-cap of dimension 7 with basis B. Let $\mathbb{S} = \mathbb{S}_B^C$ and let $\mathbb{D} = \mathbb{D}_B^C$. Then $|\mathbb{S}| = 12 - 7 - 1 = 4$ meaning there are 4 sums in $\mathbb{S}$. Using Theorem 4.2.3 we can conclude that $\mathbb{D} = (5^4)$ or $\mathbb{D} = (5^3, 7^1)$.

Case 1: suppose $\mathbb{D} = (5^4)$. Using our share string finder, we get that the options for valid share strings are $(0, 0, 5, 2, 1)$ and $(0, 0, 4, 4, 0)$.

Case 2: suppose $\mathbb{D} = (5^3, 7^1)$. Using our share string finder, we get that the options for possible share strings are $(0, 0, 3, 4, 1)$ and $(0, 0, 4, 2, 2)$. The latter string is not possible from Theorem 3.4.7 since $x_4 = 2 = \max(X_{11}^7(3))$ and $x_3 \neq 0$. Thus $\gamma_{12}^7 = \{(0, 0, 5, 2, 1), (0, 0, 4, 4, 0), (0, 0, 3, 4, 1)\}$. □

In theory, the equation in Theorem 4.3.3 can be implemented into the code in Figure 4.2.1 that we are using to calculate strings. My amateur computer science abilities at the moment are unfortunately not practiced enough to code the entire equation with the program I am using. However, it is manageable to hand calculate the pair-share values for each string decomposition and compare it to the value given by the share string within the code. It just takes a little more time depending how complicated the decompositions are (which will not be very complicated even in dimension 8). Thus, our share string finder code will include Theorem 4.3.3 throughout the rest of the project.

Theorem 4.4.2 (The Dimension 7 Theorem)**.** $M(7) = 12$.

Proof. Suppose there exists a 13-cap $C \subseteq \mathbb{Z}_2^7$ of dimension 7 with basis B. Let $\mathbb{S} = \mathbb{S}_B^C$ and let $\mathbb{D} = \mathbb{D}_B^C$. Then $|\mathbb{S}| = 13 - 7 - 1 = 5$ meaning there are 5 sums in $\mathbb{S}$. Using Lemma 4.2.3 we can conclude that $\mathbb{D} = (5^5)$ or $\mathbb{D} = (5^4, 7^1)$.

Case 1: suppose $\mathbb{D} = (5^5)$. Using our share string finder, we get that the only possible share string is $(0, 0, 0, 7, 1, 0)$.

Case 2: suppose $\mathbb{D} = (5^4, 7^1)$. Using our share string finder, we get that there are no possible share strings with sum decomposition $(5^4, 7^1)$.

Thus it must be the case that $\psi_B^C = (0,0,0,7,1,0)$. Then $\mathbb{D}_B^C = (5^5)$ so there exist five 5-sums $S_1, \ldots, S_5 \in \mathbb{S}$ with respective sum points $s_1, \ldots, s_5 \in C - B$. There exists one 4-share $p \in X_3$ shared by all but one sum, say S_1, in $\mathbb{S}$. We can then conclude that the rest of the points in B are 3-shares. Since S_1 is a 5-sum, there exists 5 points $a, b, c, d, e \in X_3$ such that $S_1 = \{a, b, c, d, e\}$. Our sums as we have constructed them up to this point will look like the following:

$$\begin{array}{lllllllll} s_1 & = & & & & a & b & c & d & e \\ s_2 & = & p & & & & & & & \\ s_3 & = & p & & & & & & & \\ s_4 & = & p & & & & & & & \\ s_5 & = & p & & & & & & & \end{array}$$

Then there remain two basis points $f, g \in X_3$ that are each shared by three of the four sums in $\mathbb{S} - \{S_1\}$. Thus there exists one sum in $\mathbb{S} - \{S_1\}$, say S_4, that does not share f and one sum in $\mathbb{S} - \{S_1\}$, say S_5, that does not share g. Thus there are at least two sums, namely S_2 and S_3 that both share p, f and g. Since no two 5-sums can share more than 3 points from 3.4.1 it follows that the remaining points shared by S_2 and S_3 are not shared by both S_2 and S_3. Thus there are 4 points in $\{a, b, c, d, e\}$, such that two of them, lets say a and b, are shared by S_2 and two of them, lets say c and d, are shared by S_3. Our sums as we have constructed them up to this point will look like the following:

$$\begin{array}{lllllllll} s_1 & = & & & & a & b & c & d & e \\ s_2 & = & p & f & g & a & b & & & \\ s_3 & = & p & f & g & & & c & d & \\ s_4 & = & p & & & & & & & \\ s_5 & = & p & & & & & & & \end{array}$$

We can see that $s_1 + s_2 + s_3 = e$ which indicates s_1, s_2, s_3, and e form a quad. In other words, the dependent point who's sumset does not share the 4-share (s_1) and the two dependent points who's sumsets share both of the other two points excluded by S_1 (s_2, s_3) will form a quad with the point shared by s_1 but not s_2 or s_3 (e). Thus C cannot be a cap so $(0,0,0,7,1,0)$ is not a possible share string. Thus $\gamma_{13}^7 = \emptyset$ so $M(7) = 12$. □

We have now proved that the maximal cap size of dimension 7 is 12. Hooray! Table 4.4.1 contains all of the possible share strings for caps of dimension 7 and Table 4.4.2 provides the sets of possible i-counts. There ended up being only one share string that our general theorems

k	γ_k^7
8	(8)
9	$(3,5),(1,7)$
10	$(0,6,2),(0,4,4),(1,4,3)$
11	$(0,2,5,1),(0,3,3,2),(0,1,5,2)$
12	$(0,0,5,2,1),(0,0,4,4,0),(0,0,3,4,1)$

Table 4.4.1: Share strings of dimension 7

cap size	i-count sets
8	$X_8^7(0)=\{8\}$
9	$X_9^7(0)=\{1,3\}$ $X_9^7(1)=\{5,7\}$
10	$X_{10}^7(0)=\{0,1\}$ $X_{10}^7(1)=\{4,6\}$ $X_{10}^7(2)=\{2,3,4\}$
11	$X_{11}^7(0)=\{0\}$ $X_{11}^7(1)=\{1,2,3\}$ $X_{11}^7(2)=\{3,5\}$ $X_{11}^7(3)=\{1,2\}$
12	$X_{12}^7(0)=\{0\}$ $X_{12}^7(1)=\{0\}$ $X_{12}^7(2)=\{3,4,5\}$ $X_{12}^7(3)=\{2,4\}$ $X_{12}^7(4)=\{0,1\}$

Table 4.4.2: The sets of possible i-counts for share strings of dimension 7

up to this point could not eliminate. However, the "brute force" method we used to disprove the possibility of (0,0,0,7,1) is sufficient when there aren't too many cases.

5
Dimension 8

5.1 General Theorems and Results of Dimension 8

We saw in the previous chapters that finding the possible share strings of the different cap sizes in a dimension could help us eliminate strings in later cap sizes. What would happen if we were to skip the lower cap sizes and go straight to the size we think is lowest size that is greater than the max-cap? Knowing there exists 18-caps of dimension 8 and that there has yet to be an example of a 19-cap found, we will first attempt to prove that $M(8) = 18$ by showing that there exist no possible share strings for 19-caps of dimension 8 without using an archive of known share strings of previous cap sizes. Before jumping straight into our attempt, we will want to prove some other things to make the search easier.

With $k - d - 1 = 19 - 8 - 1 = 10$ sumsets and 3 sum-sizes (3, 5, and z=9 being the highest) in 19-caps of dimension 8, there are, in theory, a total of

$$\binom{k-d-2+\frac{z-3}{2}}{k-d-1} = \binom{19-8-2+\frac{9-3}{2}}{19-8-1} = \binom{12}{10} = 66$$

possible sum decompositions to choose from according to Theorem 3.2.3. This is a lot of cases that would take a very long time to go through. The following three lemmas will help us narrow down the possibilities for our sum decompositions.

Lemma 5.1.1. *There cannot exist sum decomposition of dimension 8 with both a 7-sum and a 9-sum.*

Proof. Suppose for the sake of contradiction that there exists a k-cap $C \subseteq \mathbb{Z}_2^8$ of dimension 8 with basis B such that $\mathbb{S}_B^C$ has at least one 7-sum S_1 and at least one 9-sum S_2. We know that the 9-sum will share all 9 basis points in B and will thus share all of the points shared by the 7-sum meaning S_1 and S_2 share 7 points collectively. Theorem 3.4.1 tells us that a 7-sum and a 9-sum can share at most 6 points which is a contradiction since we deduced they share 7. Thus there cannot exist sum decomposition of dimension 8 with both a 7-sum and a 9-sum. □

Lemma 5.1.2. *There can exist at most one 9-sum in a sum decomposition of dimension 8.*

Proof. This lemma can easily be proved using the same logic used to prove Lemma 5.1.1. □

Lemma 5.1.3. *There can exist at most four 7-sums in a sum decomposition of dimension 8.*

Proof. Suppose for the sake of contradiction that there exists a k-cap $C \subseteq \mathbb{Z}_2^8$ of dimension 8 with basis B that has more than four 7-sums in $\mathbb{S}_B^C$. Then There exists at least five 7-sums $S_1, \ldots, S_5 \in \mathbb{S}_B^C$. Let $C' = B \cup \{s_1, \ldots, s_5\}$ and let $(x_0, \ldots, x_5) = \psi_B^{C'}$. Then $\mathbb{D}_B^{C'} = (7^5)$. Observe that

$$\sum_{i=1}^{\frac{7-3}{2}} (2i+1)\binom{n_i}{2} + \sum_{i=1}^{\frac{7-5}{2}} (2i+2)n_i n_{i+1} + \sum_{i=1}^{\frac{7-7}{2}} \left(\sum_{j=i+2}^{\frac{7-3}{2}} (2i+3)n_i n_j \right)$$

$$= \sum_{i=1}^{2} (2i+1)\binom{n_i}{2} + \sum_{i=1}^{1} (2i+2)n_i n_{i+1} + \sum_{i=1}^{0} \left(\sum_{j=i+2}^{2} (2i+3)n_i n_j \right)$$

$$= 5\binom{5}{2} + 0 + 0 = 50.$$

From Theorem 4.3.3 we know that

$$\sum_{i=2}^{4} x_i \binom{i}{2} \leq 50.$$

```
int d = 8;    //dimension
int k = 19;   //cap size
int r;        //number of sums
int n1 = 6;   //number of 5-sums
int n1 = 4;   //number of 7-sums
int dv;       //decomposition value
int ps;       //pair-shares allowed by sum decomposition

dv = 5*n1 + 7*n2;
r = k - d - 1;
ps = 171;     //hand calculated using equaiton in Theorem 4.3.3

for(int x6=0; x6<=d+1; x6++){        //Theorem 3.4.5 tells us that
  for(int x7=0; x7<=d+1; x7++){      //only x6 through x10 will be
    for(int x8=0; x8<=d+1; x8++){    //non-zero
      for(int x9=0; x9<=d+1; x9++){
        for(int x10=0; x10<=d+1; x10++){                      //Theorem
        if(   (x6 + x7 + x8 + x9 + x10 == d+1  )              //3.3.1
           && (6*x6 + 7*x7 + 8*x8 + 9*x9 + 10*x10 == dv)      //3.3.3
           && (15*x6 + 21*x7 + 28*x8 + 36*x9 + 45*x10 <= ps){ //4.3.3

        println("0 0 0 0 0 0", x6, x7, x8, x9, x10);

}}}}}}}
```

Figure 5.1.1: Share String Finder code for possible 19-caps of dimension 8 with sum decomposition $(5^6, 7^4)$

By implementing this equation into our share string finder code, we can conclude that there are no possible share strings for C'. Thus no more than four 7-sums can exist in the set of sumsets of a cap of dimension 8. □

Thus, in dimension 8, there exists no sum decompositions with more than one 9-sum, with more than four 7-sums, or with both a 7-sum and a 9-sum.

Theorem 5.1.4.

$$\gamma_{19}^{8} \subseteq \{(0,0,0,0,0,0,0,9,0,0,0,0),\ (0,0,0,0,0,0,0,7,2,0,0,0),$$

$$(0,0,0,0,0,0,0,8,0,1,0,0),\ (0,0,0,0,0,0,0,5,4,0,0,0),$$

$$(0,0,0,0,0,0,0,6,2,1,0,0),\ (0,0,0,0,0,0,0,7,0,2,0,0),$$

$$(0,0,0,0,0,0,7,1,0,1,0),\ (0,0,0,0,0,0,8,0,0,0,1).$$

Proof. Suppose $C \subseteq \mathbb{Z}_2^8$ is a 19-cap of dimension 8 with Basis B. Let $\mathbb{S} = \mathbb{S}_B^C$ and let $\mathbb{D} = \mathbb{D}_B^C$. Then $\mathbb{S} = 19 - 8 - 1 = 10$ so there are 10 sums in $\mathbb{S}$. Using Lemmas 5.1.1, 5.1.2, and 5.1.3 and the Decomposition Theorem, we can conclude that our possibilities for sum decompositions are $(5^{10}), (5^9, 9^1), (5^9, 7^1), (5^8, 7^2), (5^7, 7^3)$, and $(5^6, 7^4)$.

From Theorems 3.3.1 and 3.3.3 we get that $x_0 + \cdots + x_{10} = 9$ and $x_1 + \cdots + 10x_{10} = |\mathbb{D}_B^C|$. Since $6 = 19 - 12 - 1 = 19 - M(7) - 1$ it follows from Theorem 3.4.5 that $x_0 = \cdots = x_5 = 0$ so $x_6 + \cdots + x_{10} = 9$ and $6x_6 + \cdots + 10x_{10} = |\mathbb{D}|$. By rearranging our equations we can see that

$$6x_6 + \cdots + 10x_{10} - 6(x_6 + \cdots + x_{10}) = |\mathbb{D}| - 6(9)$$

$$\implies x_7 + 2x_8 + 3x_9 + 4x_{10} = |\mathbb{D}| - 54.$$

Because all i-counts are non-negative it follows that $0 \leq x_7 + 2x_8 + 3x_9 + 4x_{10} = |\mathbb{D}| - 54$ so $|\mathbb{D}| \geq 54$. Thus it cannot be the case that $\mathbb{D} = (5^{10})$ or $\mathbb{D} = (5^9, 7^1)$. Using the code in Figure 5.1, we can conclude that the possible share strings for $C - B$ are

$(5^8, 7^2), (5^9, 9^1)$
(0,0,0,0,0,0,9,0,0,0,0)

$(5^7, 7^3)$
(0,0,0,0,0,0,7,2,0,0,0)
(0,0,0,0,0,0,8,0,1,0,0)

$(5^6, 7^4)$
(0,0,0,0,0,0,5,4,0,0,0)
(0,0,0,0,0,0,6,2,1,0,0)
(0,0,0,0,0,0,7,0,2,0,0)
(0,0,0,0,0,0,7,1,0,1,0)
(0,0,0,0,0,0,8,0,0,0,1)

□

From here, none of our theorems rule out any of the strings (at least those not pertaining to the share strings from previous cap sizes). However, given that there are only 8 possibilities (technically 9 because one of them is possible under two different sum decompositions), we can attempt to disprove each string individually.

Lemma 5.1.5. $(0,0,0,0,0,0,8,0,0,0,1) \notin \gamma_{19}^8$.

Proof. Suppose there exists a 19-cap $C \subseteq \mathbb{Z}_2^8$ of dimension 8 with basis B with share string $\psi_B^C = (0,0,0,0,0,0,8,0,0,0,1)$. Let $\mathbb{S} = \mathbb{S}_B^C$ and let $\mathbb{D} = \mathbb{D}_B^C$. Then $\mathbb{D} = ((5^6, 7^4))$ so there exists four 7-sums $S_1, S_2, S_3, S_4 \in \mathbb{S}$ and six 5-sums $S_5, S_6, S_7, S_8, S_9, S_{10} \in \mathbb{S}$. There exists a 10-share $t \in X_{10}$ and eight 6-shares $a, \ldots, h \in X_6$. Then each 7-sum will share t and 6 other points in $B - \{t\}$. Given $|B - \{t\}| = 8$ it follows that each 7 sum will exclude exactly 2 points from $B - \{t\}$.

We will show in the next two paragraphs that each point in $B - \{t\}$ is excluded by exactly one 7-sum. We will use our share string archive to aid our proof unlike in the proof of Theorem 5.1.4.

Without loss of generality, suppose for the sake of contradiction that a point $a \in B - \{t\}$ is excluded by two 7-sums in $\mathbb{S}$, say S_1 and S_2. Given that each 7-sum excludes two basis points, S_1 and S_2 will each exclude one other point, say b and c respectively, from $B - \{a, t\}$. Thus a, b, and c are excluded by one or both of S_1 and S_2. Because S_1 and S_2 do not exclude any more basis points, it follows that $d, e, f, g, h, t \in S_1 \cap S_2$ which is a contradiction since Theorem 3.4.1 tells us that any two 7-sums can share at most 5 basis points. Thus each point in $B - \{t\}$ must be excluded from one or zero 7-sums.

Without loss of generality suppose a point $a \in B - \{t\}$ is excluded from none of the 7-sums in $\mathbb{S}$. Then both a and t are shared by the four 7-sums. Let $C' = B \cup \{s_1, s_2, s_3, s_4\}$. Then, drawing from our table in Appendix A.2, we can conclude that $\psi_B^{C'} \in \gamma_{13}^8(7^4) = \{(0,0,0,8,1)\}$ so $\psi_B^{C'} = (0,0,0,8,1)$. Thus all 4 sums must share exactly one point collectively which is a contradiction since they share two points, a and t. Thus each point in $B - \{t\}$ is excluded by exactly one 7-sum. Thus the 2 points excluded by each 7-sum are shared by the other three.

Without loss of generality assume $S_1 = B - \{a, b\}$, $S_2 = B - \{c, d\}$, $S_3 = B - \{e, f\}$, and $S_4 = B - \{g, h\}$. Our sums as we have constructed them up to this point will look like the following:

$$
\begin{array}{lcccccccccc}
s_1 & = & t & a & b & c & d & e & f & & \\
s_2 & = & t & a & b & c & d & & & g & h \\
s_3 & = & t & a & b & & & e & f & g & h \\
s_4 & = & t & & & c & d & e & f & g & h \\
s_5 & = & t & & & & & & & & \\
 & \vdots & & & & & & & & & \\
s_{10} & = & t & & & & & & & &
\end{array}
$$

Observe that a 5-sum in $\mathbb{S}$ cannot share all 5 of its points with any single 7-sum in $\mathbb{S}$ due to 3.4.1. Thus each 5-sum must share at least one point excluded by each of the four 7-sums. Because all sums share t and each 5-sum has 4 remaining points to share, it must be the case that, for each 5-sum, the 4 remaining points shared are excluded by exactly one 7-sum. In other words, each 5-sum will share t, one of a and b, one of c and d, one of e and f, and one of g and h.

We will now show that there must exist a pair of 5-sums in $\mathbb{S}$ that share exactly 3 points. Suppose for the sake of contradiction that any two 5-sums share at most 2 points. because each point in $B - \{t\}$ is a 6-share and is shared by exactly three of the 7-sums, it follows that each point in $B-\{t\}$ will be shared by exactly three of the 5-sums. Without loss of generality suppose a is shared by S_5, S_6, and S_7. Then S_5, S_6, and S_7 share 2 points, namely t and a, and thus no two of them can share any more points in common. Because each of the 3 sums must share 3 more points each that are not shared by the other two, it follows that there must be 9 other points in $B - \{t, a\}$ shared by the sums which is impossible since $|B - \{t, a\}| = 7$. Thus there must be at least one pair of 5-sums, say S_5 and S_6, that share 3 points. Knowing they share t, we know they must share two points in $B - \{t\}$ that are not excluded by the same 7-sum, say a and c. Our sums as we have constructed them up to this point will look like the following:

$$
\begin{array}{lcccccccccc}
s_1 & = & t & a & b & c & d & e & f & & \\
s_2 & = & t & a & b & c & d & & & g & h \\
s_3 & = & t & a & b & & & e & f & g & h \\
s_4 & = & t & & & c & d & e & f & g & h \\
s_5 & = & t & a & & c & & & & & \\
s_6 & = & t & a & & c & & & & &
\end{array}
$$

The remaining portion of the proof will show that the remaining points shared by s_5 and s_6 will force them to form a quad with the two 7-sums that both share a and c, namely s_1 and s_2.

We deduced above that no two points shared by a 5-sum in $\mathbb{S}$ may be excluded from a single 7-sum (it could not be the case, for example, that both a and b are shared by S_5 and S_6 since both a and b are excluded by S_4). This indicates that S_5 and S_6 share points together that are excluded by the remaining two 7-sums, namely S_3 and S_4. Thus S_5 must share one point excluded from S_3 and one point excluded from S_4, say e and g, and S_6 must share the other point excluded from S_5 and the other point excluded from S_6, namely f and h. Our sums as we have constructed them up to this point will look like the following:

$$\begin{array}{lllllllllll}
s_1 & = & t & a & b & c & d & e & f & & \\
s_2 & = & t & a & b & c & d & & & g & h \\
s_3 & = & t & a & b & & & e & f & g & h \\
s_4 & = & t & & & c & d & e & f & g & h \\
s_5 & = & t & a & & c & & e & & g & \\
s_6 & = & t & a & & c & & & f & & h
\end{array}$$

Thus $s_1 s_2 s_5 s_6 = 0$ which indicates that s_1, s_2, s_3, and s_4 form a quad. In other words, the two 5-sums that share 3 points in common, the two points 6-shares (a and c) and the 10-share (t), will necessarily form a quad with the the two 7-sums (s_1 and s_2) that both share the two 6-shares shared by the two 5-sums (a and c). Thus C cannot be a cap so $(0,0,0,0,0,0,8,0,0,0,1) \notin \gamma_{19}^8$. □

So far, this is the only complete proof that we have of the impossibility of any of the remaining share strings. We do, however, have proofs of a similar fashion as Lemma 5.1.5 in progress as well as proofs that could potentially utilize our archive of existing share strings up to 18-caps (which we have yet to find all of).

6
Conclusion and Future Work

6.1 Share String Equivalencies

One of the crucial aspects of mapping caps to share strings is the fact that the strings are dependent on an arbitrary basis for the cap. Can a single cap map to multiple share strings through different bases? We can look at an example to see that there are indeed caps that can map to different share strings by changing bases.

Example 6.1.1. Let $C \subseteq \mathbb{Z}_2^7$ be a 10-cap of dimension 7 with the share string $\psi_B^C = (0, 6, 2)$ for some basis B. Then there exists two 5-sums $S_1, S_2 \in \mathbb{S}_B^C$. There exists two points $a, b \in B$ that are shared by both sums and 3 points $c, d, e \in S_1 - S_2$ and 3 points $f, g, h \in S_2 - S_1$. Our sums will look like the following:

$$\begin{array}{cccccccc} s_1 & = & a & b & c & d & e & \\ s_2 & = & a & b & & & f & g & h \end{array}$$

By adding these sums we get

$$s_1 \quad s_2 \quad = \quad c \quad d \quad e \quad f \quad g \quad h$$

We can rearrange the s_1 sum to show that $a = s_1bcde$ and we can rearrange the addition of the sums to show that $f = s_1s_2cdegh$. Let $B' = \{s_1, s_2, b, c, d, e, g, h\}$. Then $C - B' = \{a, f\}$. Because both a and f are dependent upon the points in B' and $|B'| = 8 = d+1$, we can conclude

that B' must be a basis for C. Then $\mathbb{S}_B^C = \{A, F\} = \{\{s_1, b, c, d, e\}, \{s_1, s_2, c, d, e, g, h\}\}$ so $\psi_{B'}^C = (0, 4, 4)$. Thus there exists bases for C that map C to both $(0, 6, 2)$ and $(0, 4, 4)$.

One thing to note about the process of creating a new basis for a cap using the sums of the dependent points is that when we added the two sums, we gained more information about the point dependencies of the cap. We know that caps will have a basis as well as dependent points that form point dependencies with the basis points (which are our sums), but there will often exist many more point dependencies that can be found by adding different combinations of the point dependencies we already have.

Conjecture 6.1.2. *Let $C \subseteq \mathbb{Z}_2^d$ be a k-cap of dimension d with basis B where $k > d + 1$. Let $r = k - d - 1$.*

1. *There are $2^r - 1$ point dependencies that define the cap that can be found by taking all possible sums of the points in $C - B$.*

2. *Each point in C will be shared by 2^{r-1} of the point dependencies.*

Proof. (1). We know there exist r point dependencies such that the points in $C - B$ for some basis B are each shared once. Then there are $\binom{r}{2}$ ways to add any two of the dependencies, $\binom{r}{3}$ ways to add three and so forth until we add all r dependencies. Observe that each point dependency will have some unique pairing of points in $C - B$ that cannot be duplicated in any other dependencies so we can conclude that no two point dependencies will contain the same points. There cannot be any additional dependencies since that would mean there are additional points that are dependent upon the points in our initial basis which cannot be the case. Thus there will be exactly

$$\sum_{i=1}^{r} \binom{r}{i} = 2^r - 1$$

point dependencies that define a cap.

(2). Proof to come. □

Given that we need r sumsets to achieve a share string, there will be $\binom{2^r-1}{r}$ possible arrangements of r sums using the $2^r - 1$ dependencies (including our initial arrangement). It is not the

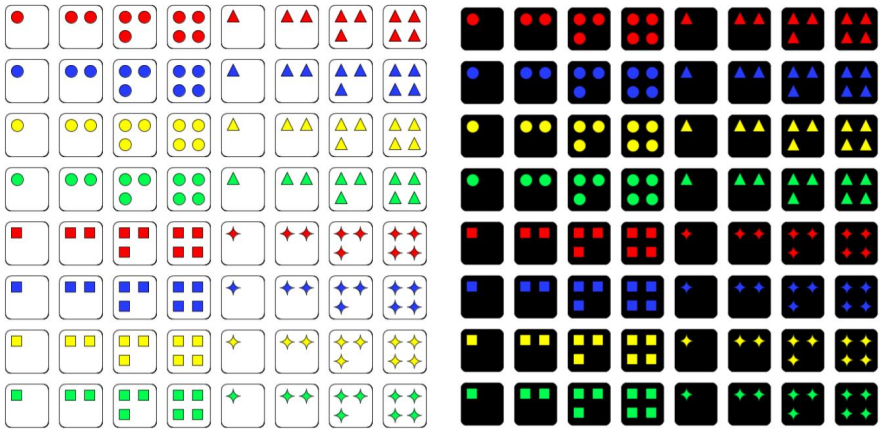


Figure 6.2.1: *Quads* Deck of dimension 7

case that all of these arrangements will be able to map to a cap, however we have found through trial and error that more than one arrangement will often work. This raises some questions: How many different arrangements of point dependencies can sufficiently map to share strings? Can two different bases map the same cap to the same share string? If a cap with share string ψ can map to another share string ψ', will all caps that map to ψ be able to map to ψ' and vice versa? If the answer to the last question is both yes and provable, then one can disprove the possibility of several share strings that can map to each other by only disproving one. If we can prove that the remaining strings for 19-caps of dimension 8 can all be mapped to by the same cap through a change of basis then we can conclude that none of them are possible since we've proved one of them is impossible. A potential term for share strings that can map to the same cap through a change of bases could be **equivalent share strings** that are connected through **share string equivalencies**. We are, of course, open to other terminologies too.

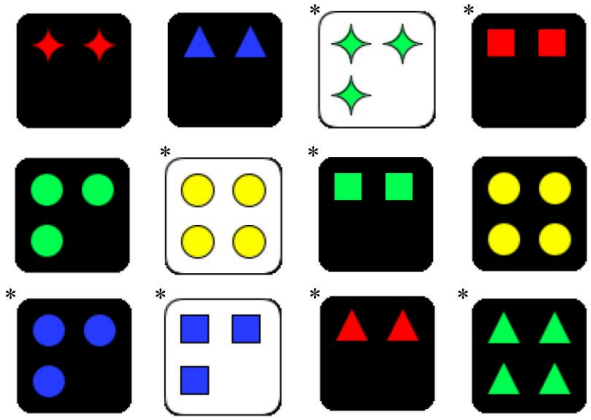
6.2 One Big Example

While we've seen a lot of examples throughout this project, it may be useful to see an example of a cap that relates a set of *Quad* cards directly to a share string. Figure 6.2.1 shows a *Quads* deck of dimension 7 where the additional half attribute is the option for a light or a dark background. The following table shows how we will map the additional half attribute to $\mathbb{Z}_2$.

Attribute	0	1
Background Color	White	Black

We will order our background state at the end of the the attributes found in Table 2.2.1 where (Number, Color, Shape, Background)$\subseteq \mathbb{Z}_2^7$ will be the mappings to our dimension 7 *Quads* deck. A card will have a white background if the last term is 0 and a black background if the last term is 1.

Example 6.2.1. Suppose we are playing *Quads* with the dimension 7 deck and lay out the following 12 cards:



We can use our mapping found in Table 2.2.1 and the one above to determine the points of our cards which we will display respective to our layout and call C:

$$\begin{aligned} C = \{&(0100111), \quad (0101101), \quad (1011110), \quad (0100011), \\ &(1011001), \quad (1110000), \quad (0111011), \quad (1110001), \\ &(1001001), \quad (1001010), \quad (0100101), \quad (1111101)\} \end{aligned}$$

After a bit of searching, we find a basis B for our set (which we have asterisked in out layout) and can then also determine $C - B$:

$$\begin{aligned} B = \{&a = (1011110), \quad b = (0100011), \quad c = (1110000), \quad d = (0111011), \\ &e = (1001001), \quad f = (1001010), \quad g = (0100101), \quad h = (1111101)\} \\ C - B = \{&s_1 = (0101101), \quad s_2 = (1110001), \quad s_3 = (1011001), \quad s_4 = (0100111)\} \end{aligned}$$

We can then figure out the the sums for our points in $C - B$:

$$\begin{array}{cccc}
 & & & (0100101) \\
 & & & (1111101) \\
(1110000) & (1011110) & (1110000) & (1011110) \\
(1001010) & (1001010) & (0111011) & (0100011) \\
(1111101) & (0100011) & (1001010) & (1110000) \\
(0100011) & (0111011) & (0100101) & (0111011) \\
+(1001001) & (1111101) & (1111101) & (1001001) \\
\hline
(0101101) & (1110001) & (1011001) & (0100111)
\end{array}$$

$$\Longrightarrow$$

$$\begin{array}{lcccccccc}
s_1 = & & b & c & & e & f & & h \\
s_2 = & a & b & & d & & f & & h \\
s_3 = & & & c & d & & f & g & h \\
s_4 = & a & b & c & d & e & & g & h
\end{array}$$

We can see that our sum decomposition is $\mathbb{D}_B^C = (5^3, 7^1)$ which we know is a valid possibility for 12-caps of dimension 7. We can put each basis point into its respective count set:

$$X_0 = \emptyset$$

$$X_1 = \emptyset$$

$$X_2 = \{a, e, g\}$$

$$X_3 = \{b, c, d, f\}$$

$$X_4 = \{h\}$$

Thus the share string for our cap is $\psi_B^C = (0, 0, 3, 4, 1)$ which is a possible share string for dimension 7. One thing to observe is that we have not proved that a set of points is necessarily a cap just because it maps to a possible share string. For example, if our sums looked like the following,

$$\begin{array}{lcccccccc}
s_1 = & a & b & c & d & e & f & g & \\
s_2 = & a & b & c & d & e & & & \\
s_3 = & a & b & & d & & f & & h \\
s_4 = & a & & c & & e & & g & h
\end{array}$$

we could deduce that $\{s_1, s_2, f, g\}$ forms a quad despite the fact that this the share string for these sums would be $(0, 0, 3, 4, 1)$ which we know is possible. However, for our cap C, we can

look at all the point dependencies taken from sums of the dependent points that Conjecture 6.1.2 tells us will give us all the defining dependencies of the cap. We will refer to s_i as i.

$$\begin{array}{cccc} 1 = bcefh & 2 = abdfh & 3 = cdfgh & 4 = abcdegh \\ 12 = acde & 13 = bdeg & 14 = adfg & 23 = abcg \\ 24 = cefg & 34 = abef & 123 = aeg & 234 = deh \\ 341 = ach & 412 = bgh & 1234 = bcdf & \end{array}$$

We can see that there are only 6 and 8 point dependencies so there are no quads or equal points and thus our layout is a cap.

6.3 Conclusion

In conclusion, we proved using share strings that the maximal cap size in dimension 7 is 12 and reduced the number of possible share strings for 19-caps of dimension 8 to just the seven in Table 1.0.2. We also proved the maximal cap sizes for previous dimensions which verified the results of [3]. Seeing that we were able to prove the impossibility of one of the remaining strings in dimension 8, we are led to think that the others can be proven impossible through similar means. While not directly considered in this project, it could be possible to program a code that checks all of the possibilities for arrangements of sums that adhere to a given share string to see if any of them form caps or not. We also have yet to find all of the possible share strings for all 15 to 18-caps of dimension 8 which, as we saw in several of our theorems, could help us knock of even more of our remaining cases.

We've seen that the number of possible share strings increases at a relatively steep rate with four possibilities in dimension 6, twelve possibilities in dimension 7, and over one hundred twenty-five possibilities for just 9 through 14-caps of dimension 8. This tells us that calculating all of the possible share strings of a given dimension with certainty would be an incredibly lengthily process as we look at greater and greater dimensions. However, we gain insight into just how many different caps and different types of caps there are in greater dimensions which may be a factor in proving things about caps no matter what strategies we use. We also proved many general theorems that shaved off a majority of the possibilities we looked at and left us with a

still relatively small number of cases to check (1 case in dimension 7 and 9 cases in dimension 8).

Appendix A
Finding Existing Caps and Share String Archives

A.1 Finding Caps Using the Qap Visualizer

As we explained at the end of Section 3.1, we only really cared about proving that strings are impossible as opposed to proving there exist caps that can map to possible share strings. In this section, we will show methods of finding existing caps given a share string.

For any dimension, the set

$$\mathbf{B} = \{0, (100\ldots), (010\ldots0), (001\ldots0), \ldots, (0\ldots010), (0\ldots001)\}$$

is a basis that spans said dimension. With an arbitrary cap C with basis $B = \{b_1, \ldots, b_n\}$ and set $C - B = \{s_1, \ldots, s_r\}$, we can arbitrarily equate the elements of $\mathbf{B}$ to the points in B and determine $s_1, \ldots, s_r$ using our sums.

Take, for example, the share string $(0, 4, 3)$ which maps to a 9-cap $C = \{a, b, c, d, e, f, g, s_1, s_2\}$ of dimension 6. An arrangement of sums could look like the following:

$$\begin{array}{lllllll} s_1 & = & a & b & c & d & e \\ s_2 & = & a & b & c & & f \quad g \end{array}$$

where $\{d, e, f, g\} = X_1$ and $\{a, b, c\} = X_2$. We can take any mapping of the points in B to $\mathbf{B}$ such as the following:

$$a = (000000), b = (100000), \ldots, g = (000001)$$

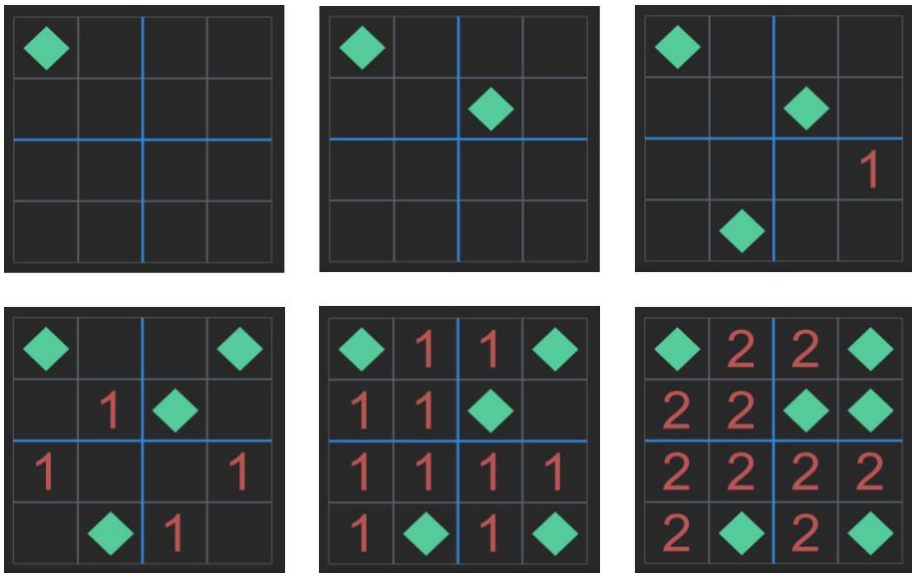


Figure A.1.1: Formation of a 6-cap of dimension 4 using the Qap Visualizer

It then follows that $s_1 = (111100)$ and $s_2 = (110011)$. Thus with basis $\mathbf{B}$, the cap $\{(000000), (100000), (010000), (001000), (000100), (000010), (000001), (111100), (110011)\}$ maps to the share string (0,3,3,2).

It is easy to see that all the points in our cap are distinct, but in order to verify that there are no quads we must, in theory, take every combination of 4 points and check whether or not there exists a quad. While there are likely ways to quicken this process, it still is not very time friendly.

The **Qap Visualizer** is a web-based app that represents $\mathbb{Z}_2^d$ using rectangular grids divided into squares that represent each element of $\mathbb{Z}_2^d$. The user may select boxes they would like include in their cap which will show green diamonds. With enough points selected, there will be points outside the cap that will necessarily form a quad with the points already in the cap which we call **exclude points**. Boxes with exclude points will show a red number that indicates the number of quads that will be formed if said point were to be added to the current cap. The user may continue adding to the cap until all the remaining points are no longer usable, indicating that the cap is complete.

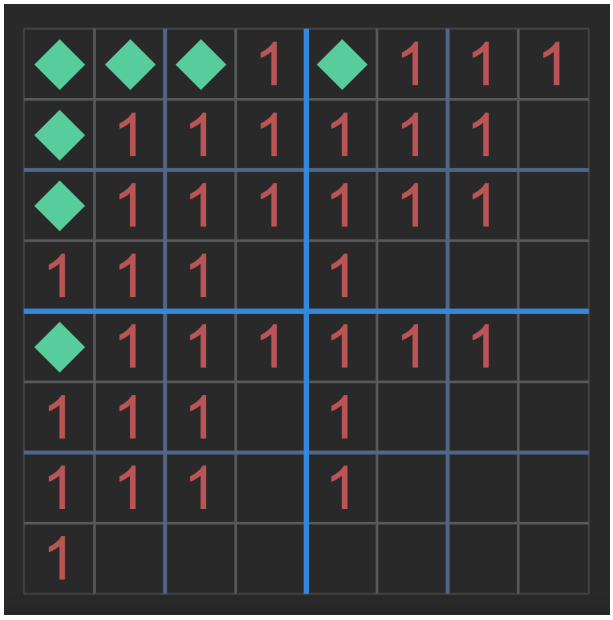


Figure A.1.2: A basis for dimension 6 in the Qap Visualizer

Figure A.1.1 shows an example of how the Qap Visualizer can be used to construct a 6-cap of dimension 4. The red 1's indicate that adding that point to the cap would form 1 quad with 3 of the points in the cap. All the 1s turn to 2s once the 6-cap is formed because each of the 10 exclude point forms a quad with two disjoint sets of 3 points in the cap of which there happen to be $\binom{6}{3} \div 2 = 10$ unique partitions (cool!).

Once one develops a familiarity with the Qap Visualizer, they can find caps without having to use vectors. Figure A.1.2 is a typical basis used for dimension 6 since determining the other points of the cap using basis sums is relatively easy compared to other bases we could choose. We can then choose some arbitrary mapping of our basis points in B as shown in Figure A.1.3. With practice, one can learn how to determine what boxes correspond to each set of odd sums of basis points. For now, We may use the aid of Figure A.1.4 to determine which boxes correspond to s_1 and s_2 which we see in Figure A.1.5.

With the help of the Qap Visualizer, we can easily find existing caps without having to work directly with elements of $\mathbb{Z}_2^d$.

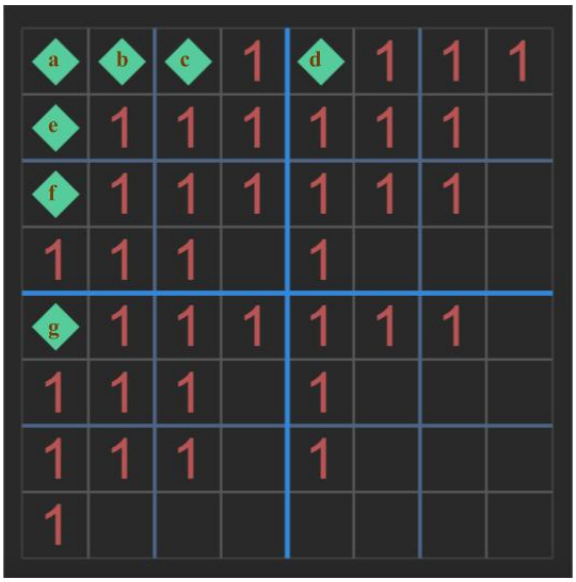


Figure A.1.3: The points in B mapped to the Qap Visualizer basis

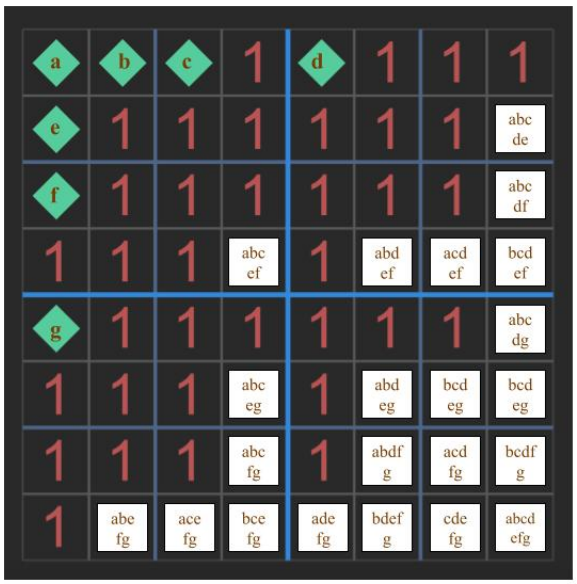


Figure A.1.4: The sumsets of the additional points that can be added to the cap

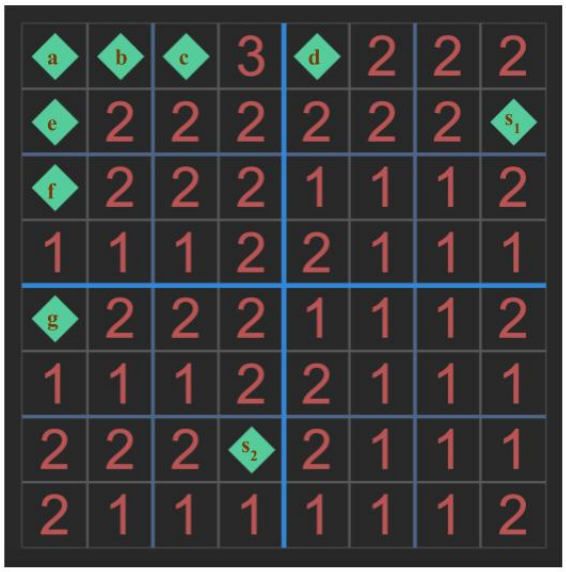


Figure A.1.5: Cap C represented by the Qap Visualizer

A.2 Archive of Possible Share Strings

A.2.1 Dimensions 0-7

All sum decompositions can be determined by each share string in Dimensions 0-7 so we will omit them.

d	$(d+1)$-caps
0	(1)
1	(2)
2	(3)
3	(4)

cap-size	$d = 4$
5	(5)
6	(0,5)

cap-size	$d = 5$
6	(6)
7	(1,5)

cap-size	$d = 6$
7	(7)
8	(2,5), (0,7)
9	(0,4,3)

cap-size	$d = 7$
8	(8)
9	(3,5), (1,7)
10	(1,4,3), (0,6,2), (0,4,4)
11	(0,2,5,1), (0,3,3,2), (0,1,5,2)
12	(0,0,5,2,1), (0,0,4,4,0), (0,0,3,4,1)

A.2.2 Dimension 8

9-caps	
no sums	(9)

10-caps	
(5^1)	(4,5)
(7^1)	(2,7)
(9^1)	(0,9)

11-caps	
(5^2)	(0,8,1), (1,6,2), (2,4,3)
$(5^1, 7^1)$	(0,6,3), (1,4,4)
(7^2)	(0,4,5)
$(5^1, 9^1)$	(0,4,5)

12-caps	
(5^3)	(0,3,6,0,), (0,4,4,1), (0,5,2,2), (0,6,0,3), (1,2,5,1), (1,3,3,2)
$(5^2, 7^1)$	(0,2,6,1), (0,3,4,2), (0,4,2,3), (1,1,5,2)
$(5^1, 7^2)$	(0,1,6,2), (0,2,4,3)
$(5^2, 9^1)$	(0,1,6,2), (0,2,4,3)
(7^3)	(0,0,6,3)

13-caps	
(5^4)	(0,0,7,2,0),(0,1,5,3,0),(0,1,6,1,1),(0,2,3,4,0),(0,2,4,2,1), (0,2,5,0,2),(0,3,1,5,0),(0,3,2,3,1),(0,3,3,1,2),(0,4,0,4,1), (1,0,4,4,0),(1,0,5,2,1)
$(5^3, 7^1)$	(0,0,5,4,0),(0,0,6,2,1),(0,1,3,5,0),(0,1,4,3,1),(0,1,5,1,2), (0,2,1,6,0),(0,2,2,4,1),(0,2,3,2,2),(0,2,4,0,3),(1,0,3,4,1),
$(5^2, 7^2)$	(0,0,3,6,0),(0,0,4,4,1),(0,0,5,2,2),(0,1,1,7,0),(0,1,3,3,2), (0,2,0,6,1)
$(5^3, 9^1)$	(0,0,3,6,0),(0,0,4,4,1),(0,0,5,2,2),(0,1,2,5,1),(0,1,3,3,2)
$(5^1, 7^3)$	(0,0,2,6,1),(0,0,3,4,2)
(7^4)	(0,0,0,8,1)

14-caps	
(5^5)	(0,0,2,7,0,0),(0,0,3,5,1,0),(0,0,4,3,2,0),(0,0,4,4,0,1),(0,0,5,1,3,0), (0,0,5,2,1,1),(0,0,6,0,2,1),(0,0,6,1,0,2),(0,1,0,8,0,0), (0,1,1,6,1,0), (0,1,2,4,2,0),(0,1,2,5,0,1),(0,1,3,2,3,0),(0,1,3,3,1,1) (0,1,4,0,4,0), (0,1,4,1,2,1)
$(5^4, 7^1)$	(0,0,0,9,0,0),(0,0,1,7,1,0),(0,0,2,5,2,0),(0,0,2,6,0,1),(0,0,3,3,3,0), (0,0,3,4,1,1),(0,0,4,1,4,0),(0,0,4,2,2,1),(0,0,4,3,0,2), **(0,0,5,0,3,1)*** (0,1,0,6,2,0),(0,1,0,7,0,1),(0,1,1,4,3,0),(0,1,1,5,1,1), (0,1,2,2,4,0) (0,1,2,3,2,1),(0,1,3,0,5,0)
$(5^4, 9^1)$	(0,0,0,7,2,0),(0,0,1,5,3,0),(0,0,1,6,1,1),(0,0,2,3,4,0), (0,0,2,4,2,1),(0,0,2,5,0,2),(0,0,3,1,5,0),(0,0,3,2,3,1), (0,1,0,4,4,0), (0,1,0,5,2,1)
$(5^3, 7^2)$	(0,0,0,7,2,0),(0,0,0,8,0,1),(0,0,1,5,3,0), (0,0,1,6,1,1),(0,0,2,3,4,0) (0,0,2,4,2,1),(0,0,2,5,0,2),(0,0,3,1,5,0),(0,0,3,2,3,1),(0,1,0,4,4,0), (0,1,0,5,2,1),(0,1,1,2,5,0)
$(5^2, 7^3)$	(0,0,0,5,4,0),(0,0,0,6,2,1),(0,0,0,7,0,2),(0,0,1,3,5,0), (0,0,1,4,3,1), (0,0,2,1,6,0)
$(5^1, 7^4)$	(0,0,0,3,6,0)
(7^5)	$\emptyset$

15-caps	
(5^6)	(0,0,0,6,3,0,0),(0,0,0,7,1,1,0),(0,0,0,8,0,0,1),(0,0,1,4,4,0,0),(0,0,1,5,2,1,0) (0,0,1,6,0,2,0),(0,0,1,6,1,0,1)
$(5^5, 7^1)$	to be figured out

19-caps	
$(5^8, 7^2), (5^9, 9^1)$	(0,0,0,0,0,0,9,0,0,0,0)
$(5^7, 7^3)$	(0,0,0,0,0,0,7,2,0,0,0), (0,0,0,0,0,0,8,0,1,0,0)
$(5^6, 7^4)$	(0,0,0,0,0,0,5,4,0,0,0), (0,0,0,0,0,0,6,2,1,0,0), (0,0,0,0,0,0,7,0,2,0,0) (0,0,0,0,0,0,7,1,0,1,0)

We note $(0, 0, 5, 0, 3, 1)$ because we think it is impossible however the proof is still in progress.

Bibliography

[1] Michèle Audin, *Geometry*, Springer-Verlag, Heidelburg Berlin, 2003.

[2] Ethan Bloch, *Proofs and Fundamentals*, Springer, New York, 2011.

[3] Julia Crager, Felicia Flores, Timothy E. Goldberg, Lauren L. Rose, Daniel Rose-Levine, Darrion Thornburgh, and Rapheal Walker, *How Many Cards Should You Lay Out in a Game of EvenQuads: A Detailed Study of Caps in* $AG(n, 2)$, La Matematica (5 April 2023).

[4] Liz McMahon, Gary Gordon, Hannah Gordon, and Rebecca Gordon, *The Joy of SET: The Many Mathematical Dimensions of a Seemingly Simple Card Game*, Princeton University Press, 2016.

[5] Eric W. Weisstein, *Binomial Coefficient*, *MathWorld*–A Wolfram Web Resource.