Packings and Coverings of Groups

A Major Qualifying Project Report Submitted to The Faculty of Worcester Polytechnic Institute In partial fulfillment of the requirements for the Degree of Bachelor of Science

Written By

Kyle Dituro

Approved by:

Padraig Ó Catháin

May 6, 2021

Abstract

Let some finite group G be given. Then a *covering* of G is a collection of elements $C \subseteq G$ such that for every $g \in G$, there exists a representation of g as $\alpha\beta^{-1}$, where $\alpha, \beta \in C$. A *packing*, of G is – on the other hand – a collection of elements $D \subseteq G$ such that none of the differences $\alpha\beta^{-1}$ coincide (where $\alpha, \beta \in D$). Then the primary question associated with these objects involves minimizing the size of a covering, maximizing the size of a packing, and determining when these two definitions meet at a *planar difference set*. We seek to establish the background of this area of study, provide a comprehensive overview of the current work done regarding these objects, fill in gaps in the current literature, and give a brief introduction to the topics required to approach related problems.

Summary/Introductions

Let G be a finite group. In this thesis we consider the following substructures in G.

Definition 0.1. Let $X \subseteq G$. A subset $P \subseteq G$ is a *packing* of $X \subseteq G$ if, for each $x \in X$ there exists **at most one pair** $(g_1, g_2) \in P \times P$ such that

$$g_1 g_2^{-1} = x\,.$$

Definition 0.2. Let $X \subseteq G$. A subset $Q \subseteq G$ is a *covering* of $X \subseteq G$ if, for each $x \in X$ there exists **at least one pair** $(g_1, g_2) \in Q \times Q$ such that

$$g_1 g_2^{-1} = x\,.$$

When G is finite, we will typically take $X = G \setminus \{1_G\}$. The additional generality in our definition is motivated by work of various authors on finite intervals of $(\mathbb{Z}, +)$, which is the only infinite group we will seriously consider. There, it is useful to consider coverings and packing of finite intervals. One further definition is useful.

Definition 0.3. Suppose that G is a cyclic group of order $\binom{k}{2}+1$ and that $X = G\setminus\{1_G\}$. Then a subset D with the property that for each each $x \in X$ there exists **precisely one pair** $(g_1, g_2) \in P \times P$ such that

$$g_1 g_2^{-1} = x\,,$$

is called a *planar difference set*.

Packings and coverings are defined relative to any subset X of any abelian group G. The main questions concern upper bounds on the size of a packing and lower bounds on the size of a covering. In the case that $X = G \setminus \{1_G\}$, the optimal bounds will be proportional to $|G|^{1/2}$. The results of Chapters 1 and 2 establish upper and lower bounds for packings and coverings of intervals in the integers to prove this statement.

In Chapter 3, we consider the existence of planar difference sets. Our main result is a complete proof of a remarkable theorem of Singer relating planar difference sets to finite projective planes.

Finally, in Chapter 4 we report on results of Banakh and Gavrylkiv on bounds for coverings in finite cyclic groups. We also comment briefly on other classes of finite groups. In contrast to covering the problem of lower bounding the density of a packing in a non-abelian group appears to be substantially harder than bounding coverings.

Contents

1. Packings in the Integers

A packing in the $(\mathbb{Z}, +)$ is a collection of positive integers

$$\{a_1, a_2 \ldots\}$$

such that all differences between distinct elements $a_i - a_j$ (where $i \neq j$) are distinct.

Definition 1.1. A *Sidon set* in $\mathbb{Z}$ is a set

$$\{s_1, s_2, \ldots\}$$

of integers with the property that *sums* $s_i + s_j \neq s_k + s_\ell$ unless $\{i, j\} = \{k, \ell\}$.

Proposition 1.2. *A subset $P \subseteq \mathbb{Z}$ is a packing in $\mathbb{Z}$ if and only if it is a Sidon set.*

Proof. Suppose that P is a packing in $\mathbb{Z}$, and that

$$p_i + p_j = p_k + p_\ell \,. \tag{1}$$

Rearranging, we find that

$$p_i - p_k = p_j - p_\ell$$

From the packing property, $p_i = p_j$ and $p_k = p_\ell$. So the assumption in Equation (1) leads to $2p_i = 2p_k$ and p_i, p_j, p_k, p_ℓ are all equal. Hence the set $P + P$ consists of distinct sums, and a packing is necessarily a Sidon set.

In the other direction, suppose that S is Sidon, and that

$$s_i - s_j = s_k - s_\ell \,.$$

Then rearranging,

$$s_i + s_\ell = s_j + s_k \,,$$

and by the Sidon set property, $\{i, \ell\} = \{j, k\}$. If $s_i = s_j$ then the condition is vacuous. If $s_i = s_k$ then $s_j = s_\ell$ and the packing condition is satisfied. □

Sidon Sets were first introduced by Simon Sidon, motivated by problems arising in his work on Fourier series. These sets have since been studied extensively by combinatorialists from the Hungarian tradition.

Example 1.3. Consider the set

$$B = \{2^n \mid n \in \mathbb{N}\}.$$

This set is a packing. To see this, notice that for any $i \in \mathbb{N}$, $2^i + 2^{i-1} < 2^{i+1}$. Suppose now that

$$2^i - 2^j = 2^k - 2^\ell \,,$$

where 2^k is the largest power of 2 occuring. Then

$$2^i + 2^\ell - 2^k < 2^i + 2^\ell < 2^k \, .$$

But we have claimed equality, hence a contradiction. So this a packing in the integers.

Example 1.4. It is possible to construct a packing *greedily*. Beginning with 1, we repeatedly add the smallest integer to our set which does not result in two equal differences. This sequence begins as follows:

$$1, 2, 4, 8, 13, 21, 31, 45, 66, \ldots \, .$$

It was introduced by Mian and Chowla. Stöhr has shown that the k^{th} term in the sequences is at most k^3, but the precise asymptotics are not understood. For further details, see the survey of Bryant, [8].

The examples above demonstrate that infinite packings exist in the integers. It is natural to ask what is the densest possible packing in $\mathbb{Z}$? This turns out to be a rather subtle question. We will consider a slightly restricted problem:

Question 1.5. What is the densest subset of the interval $[1, \ldots, n]$ which is a packing in $\mathbb{Z}$?

Clearly, such a set must be finite, and call the maximum number of terms in such a set Pack(n) for a given n. Determining upper and lower bounds on Pack(n) for any given $n \in \mathbb{N}$ is the main problem associated with packings in the integers. We give these bounds in this Chapter.

Perhaps one of the most natural first ideas to this end would be to establish a counting bound, based on counting the number of possible differences of two elements.

Theorem 1.6. *Suppose that* $P = \{a_1, \ldots, a_t\}$ *is a packing of* $\mathbb{Z}$ *with*

$$0 < a_1 < a_2 < \ldots < a_t \leq n \, .$$

Then $t \leq \sqrt{2n}$.

Proof. Since P is a packing, the differences of pairs of elements are all distinct. Now let

$$A - A = \{a_i - a_j | i, j = 1, 2, \ldots, t, \, i \neq j\}$$

be the set of differences of pairs of distinct members of A. Then $|A - A| = t(t-1)$ and precisely half of the elements in $A - A$ are positive. Since these differences are distinct, we must have $\binom{t}{2} \leq n$.

Then simple algebraic manipulation gives:

$$\frac{t(t+1)}{2} \leq n$$
$$t(t+1) \leq 2n.$$

Since $t \geq 0$;

$$t^2 \leq 2n$$
$$t \leq \sqrt{2n},$$

which is what we sought to demonstrate. □

We will be interested in various measures of density for Sidon sets. We have shown that

$$\frac{\text{Pack}(n)}{\sqrt{n}} \leq \sqrt{2}\,,$$

for all $n \in \mathbb{N}$. Our next goal is to establish a lower bound on $\lim \text{supPack}(n)$. This will require some arithmetic with prime numbers. Using results on the density of prime numbers we can strengthen a lower bound on $\lim \text{supPack}(n)$ to a uniform lower bound.

To produce a lower bound, we need to explicitly construct an infinite family of Sidon sets in the intervals $[1, \ldots, n]$. The next construction is due to Erdős and Turán, [4].

Theorem 1.7. *Let p be a prime number. Then*

$$\mathit{Pack}(2p^2) \geq p - 1\,.$$

Proof. For each $k \in [1, \ldots, p-1]$, let $\varrho(k) = k^2 \bmod p$ (interpreted as an integer) and let

$$a_k = 2pk + \varrho(k) \text{ for } k = 1, 2, \ldots, p-1.$$

Now, since $k < p$, and since $\varrho(k) < p$,

$$\begin{aligned} a_k &= 2pk + \varrho(k) \\ &\leq 2p(p-1) + (p-1) \\ &< 2p^2. \end{aligned}$$

So $P = \{a_1, \ldots, a_{p-1}\} \subseteq [1, \ldots, 2p^2]$. We will show that this set is a packing. Suppose that

$$a_i - a_j = a_k - a_\ell\,.$$

Applying the definition of the a_i and rearranging, we get

$$2p(i + \ell - j - k) = \varrho(j) + \varrho(k) - \varrho(i) - \varrho(\ell)\,. \tag{2}$$

But $1 \leq \varrho(x) \leq p-1$ for all $x \in \{1, \ldots, p-1\}$ so that the right hand side is bounded in magnitude as follows

$$-2p < \varrho(j) + \varrho(k) - \varrho(i) - \varrho(\ell) < 2p\,.$$

But the expression on the left hand side of Equation (2) is divisible by $2p$. We conclude that both sides of this equation evaluate to 0.

So $i - j = k - \ell$ and $i^2 - j^2 = k^2 - \ell^2$. Factoring the quadratic equation gives $i + j = k + \ell$. We conclude that $i = k$ and $j = \ell$ and so differences of elements of P are distinct. We have constructed an explicit packing of $[0, \ldots, 2p^2]$ of size $p-1$ and the result follows. □

For any $\varepsilon > 0$ there exist infinitely many primes for which

$$\frac{\text{Pack}(2p^2)}{\sqrt{2p^2}} = \frac{p-1}{\sqrt{2p^2}} \geq \frac{1}{\sqrt{2}} - \varepsilon\,.$$

So the lim sup of the sequence $n^{-1/2}\text{Pack}(n)$ is at least $2^{-1/2}$. Using results on the density of the primes in the natural numbers, we can extend Theorem 1.7 to all natural numbers. Equivalently, we can show that the lower bound on the lim sup is in fact a lower bound on all sufficiently large terms in the sequence.

To illustrate how the distribution of primes influences our result we will demonstrate it with three different results (one condition dependent on the Riemann hypothesis). The Prime Number Theorem was established independently by Hadamard and by de la Vallée Pousin in the 1890s. It shows that number of primes in the interval $[1, \ldots, n]$ is proportional to $\frac{n}{\log(n)}$. Hence *on average* there exists a prime in an interval of the form $[n, n + \log(n)]$. Our proof will require bounds on the shortest interval around $\sqrt{n}$ which contains a prime. We will use the following.

(1) Bertrand's Postulate was established by Chebyshev in the 1850s. It asserts that there exists a prime in the interval $[n, 2n]$.
(2) Baker, Harman and Pintz show that there exists a prime in the interval $[n, n + n^{21/40}]$.
(3) Assuming the Riemann hypothesis, Cramer showed that there exists a prime in the interval $[n, n + n^{1/2}\log(n)]$. Cramer also conjectured that there exists a prime in $[n, n + \log^2 n]$ for all sufficiently large n.

We apply these results to extend Theorem 1.7.

Corollary 1.8. *Assuming Bertrand's Postulate, Pack*$(n) \geq \frac{1}{2\sqrt{2}}\sqrt{n}$ *for all integers* n. *For any stronger hypothesis on the distribution of primes, Pack*$(n) \geq \frac{1}{\sqrt{2}}\sqrt{n}$.

Proof. First observe that a packing in $[0, \ldots, n]$ is a packing in $[0, \ldots, n+k]$ for any integer k. We will use results on the distribution of primes to show that there exists a

packing as in Theorem 1.7 which occupies a large portion of $[0, \ldots, n]$ for any n. To do this we minimise $n - 2p^2$ subject to the restriction that this quantity is positive.

(1) Assuming only Bertrand's postulate, we have a prime p in the interval $[\frac{\sqrt{n}}{2\sqrt{2}}, \frac{\sqrt{n}}{\sqrt{2}}]$. So $\frac{n}{4} \leq 2p^2 \leq n$. We fill at least one quarter of the interval $[0, \ldots, n]$ with a packing of near optimal density. In this case, we get $\text{Pack}(n) \geq p \geq \sqrt{n/8}$.

(2) Next, assume the result of Baker, Harman and Pintz. Now we can find a prime in the interval $\frac{\sqrt{n}}{\sqrt{2}} - \frac{n^{21/80}}{\sqrt{2}}, \frac{\sqrt{n}}{\sqrt{2}}$. Now we find that there is a prime $p \geq \frac{\sqrt{n}}{\sqrt{2}} - O(n^{21/80})$. So there exists a constant C such that $n - 2p^2 < Cn^{21/40}$ for all sufficiently large n. Now, the packing constructed fills a proportion of the interval which tends to 1 as $n \to \infty$. In particular, for any $\varepsilon > 0$ the density of this packing exceeds $\frac{1}{\sqrt{2}} - \varepsilon$ for all sufficiently large n.

(3) The stronger conjectures involving the Riemann hypothesis allow more rapid convergence (and hence smaller N for any particular fixed ε in the language of the previous bound. □

At this point, we have established upper and lower bounds on the density of a packing in the interval $[0, n]$ for any integer n. These are contained in the next result.

Theorem 1.9. *For any integer $n \in \mathbb{N}$ the following bounds hold for the maximal density of a packing of the integers contained in the interval $[0, n]$.*

$$2^{-1/2} \leq \frac{Pack(n)}{\sqrt{n}} \leq 2^{1/2}$$

Theorem 1.7 does **not** construct an infinite packing of the integers, rather an entirely new sequence is constructed from scratch each time a new prime satisfies the inequality $2p^2 \leq n$. It is possible to ask about the density of an infinite packing in the following sense: if P is a packing in $\mathbb{Z}$ consisting of positive integers, what is the density of $P \cap [0, n]$?

Perhaps surprisingly, such infinite packings must be less dense than the finite packings. Erdos showed that an infinite packing satisfies

$$\lim_{n \to \infty} n^{-1/2} |P \cap \{1, \ldots, n\}| = 0 \,.$$

In fact, a slightly stronger result is possible:

$$\lim_{n \to \infty} \log^{1/2}(n) n^{-1/2} |P \cap \{1, \ldots, n\}| < 1$$

though it is not known whether this limit is non-zero. The densest known infinite packing was obtained by Rusza. It has density $n^{\sqrt{2}-1} \sim n^{0.41}$. For details, see [9].

2. Coverings in the Integers

We now approach what is – in some sense – a dual problem to the construction of packings. The problem of coverings is to construct *sparse* subsets of the integers which represent every integer as a difference of two elements in *at least* one way.

More precisely, for some number interval $I = \{0, 1, \ldots, n\}$, a **covering** of I is a collection $Q \subseteq I$ such that for each $x \in I \setminus \{0\}$, there exist (not necessarily unique) $a, b \in Q$ such that

$$x = a - b.$$

Note that, if it existed, a subset of the integers with the property that $x = a - b$ had a unique solution for every x would be a perfect solution both to Sidon's problem and the construction of coverings.

For a number interval $\{0, 1, \ldots n\}$, we denote the smallest possible covering of said interval $\mathrm{Cov}(n)$.

We start with some simple realizations.

Theorem 2.1. *For any $n \in \mathbb{N}$, let k be the smallest integer such that $\binom{k}{2} \geq n$. Then*

$$Cov(n) \geq k \geq \sqrt{2n}$$

Proof. This is a simple counting bound. Simply notice that in order to cover all n elements in the interval, we must take at least n differences, each of which must be taken with 2 distinct elements, where the first is greater than the second. Then in order to take n such differences, we must have at least k elements in our covering.

Since $n \leq \frac{k(k-1)}{2} \leq \frac{k^2}{2}$ we find $k \geq \sqrt{2n}$. □

Example 2.2. Consider the number interval $I = \{0, 1, 2, \ldots, 6\}$. The set $\{0, 1, 4, 6\}$ is a covering of I. This can be easily verified by noticing that

$$\begin{array}{c|c|c} 1 = 1 - 0 & 2 = 6 - 4 & 3 = 4 - 1 \\ 4 = 4 - 0 & 5 = 6 - 1 & 6 = 6 - 0. \end{array}$$

Also notice that our covering has size 4, and

$$\binom{4}{2} = 6.$$

Therefore, by Theorem 2.1, this covering is optimal, and $\mathrm{Cov}(6) = 4$.

Now, notice that we have only used the differences which are positive. When we consider the negative sums as well, we receive the following result:

Theorem 2.3. *If the set Q is a covering of the interval $I = \{0, 1, 2, \ldots n\}$, then it is also a covering of the interval $I' = \{-n, \ldots, n\}$.*

Proof. If Q is a covering of I, then for each element $x \in I$, there exists a pair $a, b \in Q$ (where $a > b$) such that

$$x = a - b$$

Then, when we consider the difference

$$y := b - a,$$

we will see that y is the unique integer such that

$$y + x = b - a + a - b = 0.$$

Then, as a consequence of this, we see that obviously $y = -x$, and so we cover the entirety of I' . □

Example 2.4. Consider again the number interval I from Example 2.2. We have already seen that the set $\{0, 1, 4, 6\}$ is a covering of I. Now see that

$$\begin{array}{c|c|c} -1 = 0 - 1 & -2 = 4 - 6 & -3 = 1 - 4 \\ -4 = 0 - 4 & -5 = 1 - 6 & -6 = 0 - 6. \end{array}$$

And thus our same covering of $I = \{0, 1, 2, \ldots 6\}$ gives us a covering also of $\{-6, -5, -4, \ldots, 4, 5, 6\}$.

Example 2.5. We will now consider an example which will prove important later. This example is attributed to Erdős by Rédei and Rényi in [6].

Let some $n \in \mathbb{N}$ be given. then the set

$$\left\{1, 2, \ldots, n, 2n, 3n, \ldots, n^2\right\}$$

is a covering for the interval $\{0, 1, 2, \ldots n^2 - 1\}$. This covering contains $2n$ elements, which should be compared with the bound of Theorem 2.1, which gives a bound of $\sqrt{2}n$.

2.1. **The Results of Rédei and Rényi.** Important early results on coverings of intervals in $\mathbb{Z}$ were obtained by Rédei and Rényi, [6]. Since their results were published in Russian and do not appear to have been translated into English, we describe their results in complete detail.

Their main result is that the sequence of densities of packings in finite intervals converges to a limit. To achieve this result, the following definition is required.

Definition 2.6. A sequence c_n of real numbers is *almost monotonically decreasing* if for all $n \in \mathbb{N}$ and for all real $\varepsilon > 0$, the inequality

$$c_i \leq c_n + \varepsilon \tag{3}$$

holds for all but a finite number of indices i. Equivalently, for every such (n, ε) pair, there exists some $N \in \mathbb{N}$ depending only on n and ε such that (3) holds whenever $i \geq N$.

Then the next Lemma is attributed to Szele.

Lemma 2.7 (Szele's Lemma)**.** *If c_n is almost monotonically decreasing which is bounded below, then $\lim_{n\to\infty} c_n$ exists, and*

$$\lim_{n\to\infty} c_n = \inf_{n\in\mathbb{N}} c_n.$$

Proof. Define $l = \inf_{n\in\mathbb{N}} c_n$. Then for any $\varepsilon_1 > 0$, there exists some $N_1 \in \mathbb{N}$ such that $c_n \leq l + \varepsilon_1$ when $n > N_1$ by the definition of the infimum. Therefore, when $n > N_1$

$$c_n \leq l + \varepsilon_1. \tag{4}$$

Then, by Definition 2.6, for any $\varepsilon_2 > 0$, there exists some $N_2 \in \mathbb{N}$ such that

$$c_m \leq c_n + \varepsilon_2 \tag{5}$$

whenever $n \geq N_2$. Now let some $\varepsilon > 0$ be given. Due to the arbitrarily of the epsilons in equations (4) and (5), we may decompose $\varepsilon = \varepsilon_1 + \varepsilon_2$, and take $N = \max\{N_1, N_2\}$, and have that for all $n \geq N$,

$$|c_m - l| \leq \varepsilon,$$

and thus the limit converges to the infimum. □

Now we move to the main result proven by Rédei and Rényi, which is their main contribution to the study of coverings.

Lemma 2.8. *For any $n \in \mathbb{N}$, there exist values $m \in \mathbb{N}$ and q a prime power such that*

$$Cov(n) \leq Cov(m)(q+1).$$

Proof. Let m be a natural number, and q a prime-power, the values of which we will determine precisely later. Singer's construction tells us that there is a set D of size $q+1$ over the interval $[1, 2, \ldots, q^2+q+1]$ such that for any α on the interval, either the equation $\alpha = d_i - d_j$, or $\alpha = m + d_i - d_j$ is solvable with elements of D. Then, let B be a covering of the interval $[1, \ldots, m]$ such that $|B| = \mathrm{Cov}(m)$.

Then, the set of integers

$$P := \left\{ d_i + (q^2+q+1)b_j \mid i = 1, \ldots q+1,\ j = 1, \ldots, \mathrm{Cov}(m) \right\}$$

are all distinct and lie in the interval $[1, \ldots, m(q^2+q+1)]$. Then the set of differences $P - P$ has elements that are of the form

$$(d_i - d_j) + (q^2+q+1)(b_k - b_l).$$

By the observation by Erdős (at Example 2.5), we see that this set P covers the entire interval up to $m(q^2+q+1)$.

Now it is a trivial realization that

$$\mathrm{Cov}\left(m(q^2+q+1)\right) \leq (q+1)\mathrm{Cov}(m).$$

Let $\varepsilon > 0$ be fixed, and now let q be a prime-power such that

$$\sqrt{\frac{n}{m}} \leq q \leq (1+\theta)\sqrt{\frac{n}{m}} \quad (0 \leq \theta \leq \vartheta), \tag{6}$$

which is guaranteed to exist by the prime number theorem when n is large enough. Now, observe that $n \leq m(q^2+q+1)$, so

$$\mathrm{Cov}(n) \leq \mathrm{Cov}(m)(q+1).$$

□

Theorem 2.9. *The sequence*

$$\frac{Cov(n)}{\sqrt{n}} \quad (n \in \mathbb{N})$$

is almost monotonically decreasing.

Proof. Observe first that if Q is a covering of $[1, \ldots, n+k]$ then Q is *a fortiori* a covering of $[1, \ldots, n]$. We will choose values of m and q such that $n < m(q^2+q+1)$ in order to apply Lemma 2.9.

Let $\varepsilon > 0$ be given. We will choose $m \in [1, \ldots, \lfloor n^{1/3} \rfloor]$ momentarily. Let q be a prime power satisfying $(1-\delta)\sqrt{n/m} \leq q \leq \sqrt{n/m}$. By the results of Baker, Harman and Pintz quoted in Chapter 1, for any fixed constant c, there exists a prime in the interval $[t, (1+c)t]$. So δ may be chosen arbitrarily small. In fact, we choose the pair (δ, m) to satisfy the conditions

$$\delta\frac{\mathrm{Cov}(m)}{\sqrt{m}} \leq \frac{\varepsilon}{2}, \quad \frac{\mathrm{Cov}(m)}{\sqrt{n}} \leq \frac{\varepsilon}{2}$$

noting that this is always possible for sufficiently large n depending only on ε. This completes the parametrisation.

Substituting for the upper bound of (6) and dividing by $\sqrt{n}$, we get that

$$\frac{\mathrm{Cov}(n)}{\sqrt{n}} \leq (1+\delta)\frac{\mathrm{Cov}(m)}{\sqrt{m}} + \frac{\mathrm{Cov}(m)}{\sqrt{n}}.$$

By the choice of m and δ, we get

$$\frac{\mathrm{Cov}(n)}{\sqrt{n}} < \frac{\mathrm{Cov}(m)}{\sqrt{m}} + \varepsilon.$$

So for any choice of m and ε there exists a constant C such that $\frac{\mathrm{Cov}(n)}{\sqrt{n}} < \frac{\mathrm{Cov}(m)}{\sqrt{m}} + \varepsilon$ holds for all $n \geq C$, and the sequence is almost monotonically decreasing, as claimed. □

Corollary 2.10. *The sequence* $\frac{Cov(n)}{\sqrt{n}}$ *converges, and*

$$\lim_{n\to\infty} \frac{Cov(n)}{\sqrt{n}} = \inf_{n\in\mathbb{N}} \frac{Cov(n)}{\sqrt{n}}.$$

Proof. Follows directly from Theorem 2.9, along with Szele's lemma, Lemma 2.7. □

2.2. **Numerical Bounds on the covering ratio.** By Corollary 2.10, Rédei and Rényi established that the covering ratiov $\frac{\mathrm{Cov}(n)}{\sqrt{n}}$ converges to a definite limit as $n \to \infty$. An explicit upper bound for this limit can be computed by finding values of n for which $\frac{\mathrm{Cov}(n)}{\sqrt{n}}$ is small.

- In Example 2.2, we have shown that $\mathrm{Cov}(6) = 4$. Therefore, Corollary 2.10 tells us that
$$\lim_{n\to\infty} \frac{\mathrm{Cov}(n)}{\sqrt{n}} \leq \frac{\mathrm{Cov}(6)}{\sqrt{6}} = \frac{4}{\sqrt{6}} \sim 1.632993\,.$$
- It was shown by Golay that $\mathrm{Cov}(6166) \leq 128^2$. From this we obtain the bound
$$\lim_{n\to\infty} \frac{\mathrm{Cov}(n)}{\sqrt{n}} \leq \frac{\mathrm{Cov}(6166)}{\sqrt{6166}} = \frac{128}{\sqrt{6166}} \sim 1.630077\,.$$
To our knowledge this remains the best known upper bound.

Then, in order to get their lower bound, Rédei and Rényi begin with a covering $Q = \{b_1, b_2, \ldots b_k\}$ of the interval $[0, 1, 2, \ldots n]$. Now consider the function

$$|f(x)| = \sum_{r=1}^{k}\sum_{s=1}^{k} e^{i(b_r - b_s)x} \geq 0.$$

Then in the exponent of e, each of $\pm 1, \pm 2, \ldots, \pm n$ appears at least once in the sum, and 0 occurs at least k times. Then, the number of terms in the sum will be $k^2 - k - 2n$. Now, we set up for some algebra. Since $|f(x)| \geq 0$, we know that

$$\left(k + 2\sum_{r=1}^{n} \cos rx\right) + \left(k^2 - k - 2n\right) \geq 0. \tag{7}$$

Now we introduce the "Dirichlet kernel", $D_n(x)$:

$$D_n(x) = 1 + 2\sum_{r=1}^{n} \cos rx = \frac{\sin\frac{2n+1}{2}x}{\sin\frac{x}{2}}. \tag{8}$$

Then, by rearranging term in equation (7) and substituting in with (8), we get that

$$2n + 1 - D_n(x) \leq k^2.$$

Now Rédei and Rényi find a minimum at $x = \frac{3\pi}{2n+1}$, and thus we evaluate:

$$D_n(x) = -\frac{1}{\sin\frac{x}{2}} < -\frac{x}{2} = -\frac{2}{3\pi}(2n+1)$$
$$(2n+1)\left(1 + \frac{2}{3\pi}\right) < k^2.$$

Then, if the covering Q is optimal for the given interval bounded by n, we get

$$\sqrt{\left(1 + \frac{2}{3\pi}\right)\left(2 + \frac{1}{n}\right)} < \frac{\mathrm{Cov}(n)}{\sqrt{n}}$$

Numerically, this bound evaluates to approximately 1.557. Via a more careful analysis, Leech improved upon the lower bound, by computing explicitly $\max_{0<\phi<\pi} \frac{2\sin(\phi)}{\phi+\pi}$. As a result, he obtains a slightly larger lower bound of approximately 1.56. To summarise, the tightest known bounds on the covering ratio of an interval are as follows.

Theorem 2.11. *For any natural number n, we get the lower and upper bounds:*

$$1.56 \sim \sqrt{2 + \max_{0<\phi<\pi} \frac{2\sin(\phi)}{\phi+\pi}} \leq \lim_{n\to\infty} \frac{Cov(n)}{\sqrt{n}} \leq \frac{Cov(6166)}{\sqrt{6166}} \sim 1.63$$

3. Singer Difference Sets

A special case of a famous theorem of Singer gives a construction for perfect packings and coverings in certain cyclic groups. While this result is often cited in the literature, it is not easy to find a full and detailed proof: we provide this proof in this Chapter.

Definition 3.1. A *planar difference set* in a finite group G is a subset D with the property that $d_i - d_j = g$ has a unique solution for every $g \in G$. If $|G| = v$ and $|D| = k$, we say that D is a $(v, k, 1)$-difference set. It is both a perfect covering and a perfect packing of G.

Clearly the existence of a planar difference set in a group G of order v requires that $v - 1 = k(k-1)$ where $k = |D|$. In fact, Singer's theorem shows that such sets exist whenever $k - 1$ is a prime power. The *prime power conjecture*, a famous open problem in combinatorics, asserts that planar difference sets exist only in this case. The following example gives the smallest non-trivial Singer difference set with $k = 2 + 1$ and $v = 3 \cdot 2 + 1$, associated with the prime 2.

Example 3.2. Let C_7 be the cyclic group of order 7, written additively. The smallest example of a Singer difference set is $D_7 = \{0, 1, 3\} \subseteq \mathbb{Z}_7$, because

$$\begin{aligned} 1 - 0 &= 1 \\ 3 - 1 &= 2 \\ 3 - 0 &= 3 \\ 0 - 3 &= 4 \\ 1 - 3 &= 5 \\ 0 - 1 &= 6 \end{aligned}$$

Notice that D_7 is a *perfect* covering and a *perfect* packing of $C_7 \setminus \{0\}$.

To establish Singer's theorem we require ideas and results from field theory, group theory, finite geometry and linear algebra. We will develop each of these areas in turn, but it may aid the reader to have a road map of the proof to refer to.

(1) Associated to a difference set is a combinatorial object called a 2-design. Corresponding to Singer's difference sets are a class of designs called *finite projective planes*. We begin by giving a direct construction of these planes and establishing properties necessary for the proof.
(2) A 2-design yields a difference set if and only if the automorphism group has a subgroup acting regularly on points and on blocks.

(3) To establish Singer's theorem, we prove that the so-called Singer cycles in the automorphism group of a Desarguesian projective plane satisfy all the requirements of a difference set.

Before constructing some projective planes we review properties of finite fields.

3.1. **Finite Fields.** We establish some basic properties of finite fields in this section. This material is well known, and can be found (for example) in Isaacs' book, [5].

Recall that a field E is an *extension* of F if and only if $F \subseteq E$. The field axioms yield immediately that E is a vector-space over F. The dimension of E as an F-vector-space is the *degree* of E over F, and is denoted $|E/F|$. We will often use standard linear algebra terminology in our discussion.

The *characteristic* of a field F is the least positive integer n such that $n \cdot 1 = 0$, or 0 if there is no such n. If the characteristic is positive, then it is prime, since if $n = ab$ then

$$\underbrace{a + a + \cdots + a}_{b} = 0,$$

which implies that $a(1 + 1 + \cdots + 1) = 0$, so $b < n$ satisfies the definition of the characteristic. But the characteristic is the length of the minimal sum of 1's which vanishes, to n cannot be composite.

If the characteristic n is positive then the multiples of 1 form a subfield isomorphic to $\mathbb{Z}_n$. If $n = 0$ then $\mathbb{Z}$ is a subring of F, and completing this to a field shows that $\mathbb{Q} \subseteq F$. In fact, these are the *prime fields*, the unique fields having no proper subfields.

It will be convenient to consider a field F of positive characteristic as a vector space over its prime field. Since we are interested in finite fields, the degree of this extension will be finite. It is clear that the size of a finite field is a prime power, since it is a vector space of finite degree over a prime field.

We recall the construction of extension fields.

Lemma 3.3. *Suppose that $g(x)$ is an irreducible polynomial of degree n over $\mathbb{F}_p$. Then $E = \mathbb{F}_p[x]/(g(x))$ is an extension field of degree n of $\mathbb{F}_p$.*

Proof. In a finite ring, every element is either a zero-divisor or a unit. To see this, consider the function $m_x(y) = xy$ which multiplies each element of E by x. If this map is *surjective* then there exists y' such that $xy' = 1$ and x is a unit in E. Otherwise, by the Pigeonhole Principle, there exist distinct elements y and y' such that $xy = xy'$. But then $x(y - y') = 0$ and x is a zero-divisor.

Recall that the elements of E are in bijection with polynomials of degree $\leq n - 1$ in $\mathbb{F}[x]$. A non-trivial zero divisor corresponds to a factorisation $a(x)b(x) = c(x)g(x)$ where $c(x)$ has degree $\leq n$. By irreducibility of $g(x)$, it must divide $a(x)$ or $b(x)$, so at least one of these terms is zero. Hence E lacks proper zero-divisors. By above argument all non-zero elements are invertible, and E is a field. □

Example 3.4. We construct a finite field of order 27. It suffices to find an irreducible polynomial of degree 3 over $\mathbb{F}_3$. Since a polynomial of degree 3 is irreducible if and only if it has no root in the field, this is easily done. For example, x^3+x^2+2 is irreducible.

Then the elements of the factor ring

$$\mathbb{F}_3[x]/\langle x^3+x^2+2\rangle = \left\{ax^2+bx+c+\langle x^3+x^2+2\rangle | a,b,c\in\mathbb{F}_3\right\}$$

are in bijection with polynomials of degree ≤ 2 over $\mathbb{F}_3$. Multiplication is accomplished in the quotient by equating x^3 with $2x^2+1$. For example,

$$\left(x^2+1\right)\left(2x^2+x+1\right) = 2x^4+x^3+x+1\,.$$

Upon long division by x^3+x^2+2, it can be verified by the reader that the remainder term is x^2. So in the quotient field,

$$\left(x^2+1\right)\left(2x^2+x+1\right) = x^2\,.$$

It is well known that the multiplicative group of a finite field is cyclic. The element $y=x^2+1$ satisfies the identities

$$y^2 = x\,,\quad y^{13}=2$$

and so is a generator for the multiplicative group. In fact, $y^3=2x^2+x+1$ and $y^4=x$ so that the displayed equation above is equivalent to $yy^3=y^4$. Of course the additive structure of the field is obscure from this perspective.

We conclude this section by proving that the finite field of order q is unique up to isomorphism.

Lemma 3.5. *Let L be a field of prime characteristic p and let $q=p^n$ for some n. Then L contains a subfield of order q if and only if the polynomial x^q-x splits in $L[x]$. In this case, $E=\{\alpha\in L|\alpha^q=\alpha\}$ is the unique subfield of L with order q.*

Proof. Since L is of characteristic p and $q=p^n$, we see that

$$\forall\alpha,\beta\in E,\ (\alpha-\beta)^q=\alpha^q-\beta^q.$$

Then $\{\alpha\in L|\alpha^q=\alpha\}$ is an additive subgroup of L, which, in accordance with the theorem statement, we will call E. Since $\alpha/\beta=\alpha^q/\beta^q$ for $\beta\neq 0$, and thus E must be a subfield..

Now let $f(x):=x^q-x$, and see that E is the roots of f in L. Thus $|E|\leq\deg(f)=q$. Thus $|E|=q$ only if f splits over L.

Now we must finish by showing that $K\subseteq L$ (where $|K|=q$) implies that f splits over L, and $K=E$.

Now suppose that $\alpha \in K$. Then, suppose $\alpha \neq 0$ (since the zero case is trivial). Then $\alpha^{q-1} = 1$, since α is in the multiplicative group of K, which has been established to have order $q-1$. Therefore, $\alpha \in E$. □

Theorem 3.6. *Let $q = p^n$ for some prime p. Then there exists a field of order q, and every such field is isomorphic to a splitting field for $f(x) = x^q - q$ over $F = \mathbb{Z}/p\mathbb{Z}$. In particular, all fields of order q are isomorphic.*

Proof. Let L be a splitting field for f over F, and there is a subfield of L of order q. Now it suffices to show uniqueness.

Let E_0 be a field of order q. Then let F_0 be the prime subfield of E_0. Notice that $F_0 \cong F$ since E_0 has characteristic p. Then f splits over E_0, and E_0 contains a splitting field L_0 for f over F_0. Then, since splitting fields are unique, we get that $L_0 \cong L$. Therefore, $E_0 = L_0 \cong L$. □

Thus we have shown the existence and uniqueness of what are commonly called the *Galois fields*, and will use either $\mathrm{GF}(q)$ or $\mathbb{F}_q$ to denote the unique Galois field of order q (where q is a prime power).

3.2. **Projective Planes.** Next we introduce combinatorial and geometric structures which capture the relations between straight lines in 3-dimensional space. We give the construction in some generality, so begin with the definition of an incidence structure.

Definition 3.7. An *incidence structure* on a finite set of 'points' V is a set of 'blocks' $B \subseteq \mathcal{P}(V)$, where $\mathcal{P}$ is the power set of V. We denote an incidence structure by (V, B).

Projective planes are a well-studied class of incidence structures. In this context, the elements of V are normally called (projective) points and the elements of B are (projective) lines.

Definition 3.8. A *projective plane* $\Pi = (V, B)$ is an incidence structure satisfying the following axioms.

(1) every pair of points (in V) are belong to a unique line (blocks in B);
(2) every pair of lines intersects in a unique point;
(3) there exist four points, no three belonging to any line

Example 3.9. Perhaps one of the most famous examples of projective geometries is $\mathrm{PG}(2,2)$, often called the *Fano plane*. Let $V = \{p_0, p_1, \ldots p_6\}$ then let $B = \{b_1, b_2, \ldots, b_7\}$, where

$$\begin{array}{lll} b_1 = \{p_0, p_1, p_3\}, & b_2 = \{p_1, p_2, p_4\}, & b_3 = \{p_2, p_3, p_5\}, \\ b_4 = \{p_3, p_4, p_6\}, & b_5 = \{p_0, p_4, p_5\}, & b_6 = \{p_1, p_5, p_6\}, \ . \\ b_7 = \{p_0, p_2, p_6\}. & & \end{array}$$

To verify that the axioms of a projective plane are satisfied, one must check that any pair of points (e.g. p_2, p_5) are contained in a unique block (in this case b_3 and that every pair of blocks (e.g. b_1, b_6) intersect in a unique point (in this case p_1).

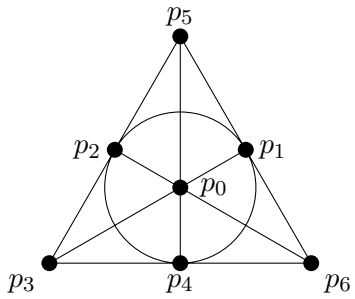

Fig. 1. The Fano Plane

Example 3.10. Suppose that V is a 2-dimensional vectorspace over a field k (finite or infinite). We adjoin to V an 'extended line at infinity': as a set this consists of points $\{x_a \mid a \in k\} \cup \{x_\infty\}$. We then define an incidence structure which has as points the vectors of V together with the points at infinity.

Observe that (affine) lines of V intersect in a unique point *unless* they are parallel, and that parallel lines have the same slope (as in high school geometry determined uniquely by any two points on the line, and taking a value in $k \cup \{\infty\}$). We define a block to be a line of V extended by the point at infinity labelled by the slope of that line. The points at infinity also form a line.

The axioms of a projective plane may be verified with a little effort. This construction is really motivated by the observation of medieval artists that parallel lines converge to a 'vanishing point' on the horizon.

Example 3.11 (The Moulton Plane)**.** Let the incidence structure $\mathcal{M} = (P, B)$ with $P = \mathbb{R}^2$ and $B = (\mathbb{R} \cup \{\infty\}) \times \mathbb{R}$, where ∞ is a point at infinity. Now define block membership such that, for $p = (x, y) \in P$, $l_{m,b} \in B$, $p \in l$ if and only if:

- $x = b$ when $m = \infty$,
- $y = \frac{1}{2}mx + b$ when $m \leq 0$, $x \leq 0$,
- and $y = mx + b$ if $m \geq 0$ or $x \geq 0$.

This example, so named for Robert Moulton who discovered it in [7]. In fact, it cannot be constructed from a vector space over a field, and we will later see that the Theorem of Desargues does not hold in this plane.

The next result gives the best known construction for projective planes, which is also the most useful in applications. It is essentially equivalent to Example 3.10 but has the advantage of making the automorphism group apparent. The following result holds more generally for division algebras over a field, but we will not need that level of generality in this thesis.

Theorem 3.12. *Let k be a field, and $\mathcal{V}$ a three-dimensional vector space over k. Let V be the set of 1-dimensional subspaces of $\mathcal{V}$ and B the set of 2-dimensional subspaces. Then (V, B) is a projective plane.*

Proof. We verify the axioms of the projective plane.

Lemma 3.13. *Any two distinct elements of $\mathcal{P}$ lie on a unique element of $\mathcal{L}$.*

Since a projective point is a one-dimensional subspace and a projective line is a two-dimensional subspace, the assertion is equivalent to the statement that two linearly independent vectors space a unique two dimensional space.

Lemma 3.14. *Any two elements of $\mathcal{L}$ meet at a unique element of $\mathcal{P}$.*

A projective line is a two dimensional subspace in three dimensional space: it is defined by a single linear equation. The intersection of two distinct projective lines is then described by the set of solutions of a pair of independent linear equations in three unknowns, which is a one dimensional subspace.

Lemma 3.15. *There exist four points, no three collinear.*

Consider the projective points spanned by $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$ and by $(1, 1, 1)$. An easy exercise shows that any three are linearly independent and so are not contained in a projective line. □

Example 3.16. It is convenient to write $[x : y : z]$ for the one-dimensional subspace spanned by the vector (x, y, z). Then $[x : y : z] = [\lambda x : \lambda y : \lambda z]$ for any non-zero vector λ and without loss of generality we may assume that the leading term is 1. The projective points $[1 : x : y]$ for $x, y \in k$ form a 2-dimensional vector space (the axioms may be verified directly). The points of the form $[0 : 1 : x]$ and $[0 : 0 : 1]$ form the $|k| + 1$ points at infinite of Example 3.10.

In the remainder of this section, we provide some counting results in the special case that the projective plane is defined over a field of prime order.

Proposition 3.17. *If Π is a projective plane defined over a field of order q then the following hold.*

(1) $|\mathcal{P}| = |\mathcal{L}| = q^2 + q + 1$
(2) *Each $\ell \in \mathcal{L}$ contains $q + 1$ projective points.*

(3) *Each $p \in \mathcal{P}$ is contained in $q+1$ projective lines.*

Proof. Let $V = \mathbb{F}_q^3$ be a vector space. Now consider the collections

$$\mathcal{P} = \{\mathrm{Sp}(\mathbf{v}) \mid \mathbf{v} \in V\}$$
$$\mathcal{L} = \{\mathrm{Sp}(\mathbf{v_1}, \mathbf{v_2}) \mid \mathbf{v} \in V\}.$$

The elements of $\mathcal{P}$ are *projective points* and the elements of $\mathcal{L}$ are *projective lines*. We begin by computing the number of projective points and lines.

Lemma 3.18. $|\mathcal{P}| = |\mathcal{L}| = q^2 + q + 1$

There are $q^3 - 1$ nonzero vectors in V, and any given vector will span the same one-dimensional subspace as $q-1$ other vectors. Then there are $\frac{q^3-1}{q-1} = q^2 + q + 1$ distinct subspaces, and so $|\mathcal{P}| = q^2 + q + 1$.

Similarly, there are $q^3 - 1$ nonzero vectors from which we can construct a two-dimensional vector subspace of V. There are $\frac{(q^3-1)(q^3-q)}{2}$ ways of choosing two linearly independent vectors to span a subspace. Now we see that $\frac{(q^2-1)(q^2-q)}{2}$ bases will construct the same vector space. So we get

$$\begin{aligned}
|\mathcal{L}| &= \frac{(q^3-1)(q^3-q)}{(q^2-1)(q^2-q)} \\
&= \frac{q(q^2-1)(q^3-1)}{q(q^2-1)(q-1)} \\
&= \frac{q^3-1}{q-1} \\
&= q^2 + q + 1 \\
&= |\mathcal{P}|.
\end{aligned}$$

□

Lemma 3.19. *Every projective line has $q+1$ points on it.*

Proof. Let some line $\ell \in \mathcal{L}$ be given. Then, by the theorems just proven, ℓ must intersect $q^2 + q$ other lines. Therefore, the number of points n on the line ℓ must divide $q^2 + q$. Thus, either $n = q$ or $n = q + 1$. Notice that if $n = q$, then each point p must lie on $q + 2$ lines, and if $n = q + 1$, then each point must lie on $q + 1$ lines.

We now make a quick aside to think about projective points. Let some point $p \in \mathcal{P}$ be given. Then, since every pair of points intersects on a unique line, p must be joined to $q^2 - q$ other points by lines, and we find ourselves in a similar situation to before. Realize again that the number of lines must divide the number of points, so there are either q or $q + 1$ lines that meet at every point. However, we just demonstrated that a projective point either meets at $q + 1$ or $q + 2$ lines.

It is now clear that in order to reconcile these two constraints, $n = q + 1$. □

3.3. **Incidence Matrices, their automorphisms and Block's Lemma.** In this Section, we only consider *Balanced Incomplete Block Designs*, which are defined as follows.

Definition 3.20. Let V be a set with v elements and B a collection of k-subsets of V. The pair (V, B) is a *t-design* if

(1) each $b \in B$ has size k
(2) each t-set of V is contained in λ blocks of B.

We say that (V, B) is a t-(v, k, λ) design.

Designs were initially investigated for applications in statistics, but have found use in multiple other areas including signal processing.

Proposition 3.21. *A finite projective plane of order q is a 2-$(q^2 + q + 1, q + 1, 1)$ design.*

Proof. Let V be the collection of projective points in the plane Π, and for each projective line ℓ, define B_ℓ to be the set of points incident with ℓ. Set $\mathcal{B} = \{B_\ell \mid \ell \in \Pi\}$.

By Lemma 3.18, $|V| = |\mathcal{B}| = q^2 + q + 1$. By Lemma 3.19, all blocks in $\mathcal{B}$ have size $q + 1$. Finally, every pair of elements from V is contained in a unique set B_ℓ by the axioms for a projective plane. □

Proposition 3.22. *If M is the incidence matrix of a symmetric design with parameters (v, k, λ) such that $k > \lambda$ then M is invertible.*

Proof. By the definition of a symmetric design, M is a square matrix which satisfies $MM^\top = (k - \lambda)I + \lambda J$ where J is the all-ones matrix. Observe that the eigenvalues of J are v with multiplicity 1 and 0 with multiplicity $v - 1$. Since $(k - \lambda)I$ is a scalar matrix, we observe that an eigenvalue of $(k-\lambda)I + \lambda J$ is just $(k-\lambda) + \mu$ where μ is an eigenvalue of λJ. We conclude that the eigenvalues of $(k - \lambda)I + \lambda J$ are $(v - 1)\lambda + k$ with multiplicity 1 and $(k - \lambda)$ with multiplicity $v - 1$. In particular, the eigenvalues of $MM^\top$ are all non-zero, so this matrix has full rank. But the rank of $MM^\top$ cannot exceed the rank of M and the proof follows. □

Definition 3.23. When thinking about these incidence structures (V, B), since every b in B is a subset of V, the natural thing to do is to create the *incidence matrix* whose column vectors represent blocks, and whose rows represent elements of V. Explicitly, we define

$$M = [x_{p,b}]_{\substack{p \in V \\ b \in B}} \qquad x_{p,b} = \begin{cases} 1 & p \in b \\ 0 & \text{otherwise} \end{cases}.$$

Theorem 3.24 (Fisher's Inequality, cf. [3])**.** *In any design the number of blocks in a design is at least the number of points.*

Proof. Let M be the incidence matrix of a 2-design (V, B). The (i, j) entry of $MM^\top$ counts the number of blocks containing v_i and v_j, which is r if $i = j$ and λ otherwise, by Definition 3.20. Hence $MM^\top = (r - \lambda)I + \lambda J$. This matrix has full rank, v. Hence M has rank v, which forces $b \geq v$. □

Definition 3.25. An *automorphism* of (V, B) is a permutation σ of V such that $b^\sigma \in B$ for all $b \in B$. The set of all automorphisms of D is denoted $\mathrm{Aut}(D)$.

Note. An automorphism $\sigma : V \to V$ naturally acts pointwise on the blocks of the design (V, B). In other words, for any given $b \in B$, $b^\sigma = \{\sigma(v) \mid v \in b\}$.

Recall the Fano plane of Example 3.9, which can be represented as incidence structure as follows:

$$V = \mathbb{Z}/7\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6\}$$

with the blocks

$$\begin{array}{lll} b_1 = \{0, 1, 3\}, & b_2 = \{1, 2, 4\}, & b_3 = \{2, 3, 5\}, \\ b_4 = \{3, 4, 6\}, & b_5 = \{0, 4, 5\}, & b_6 = \{1, 5, 6\}, \\ b_7 = \{0, 2, 6\}. & & \end{array} .$$

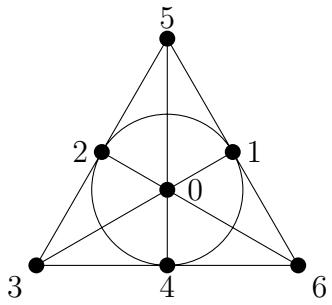

Fig. 2. The Fano Plane, labeled as suggested by the above incidence structure.

We define a permutation on the set V by $v^\sigma = v + 1 \pmod 7$ for all $v \in V$. It is easily verified that $b_i^\sigma = b_{i+1 \pmod 7}$ for all $b_i \in \mathcal{B}$. Hence σ is an automorphism of the Fano plane.

In the context of incidence matrices of designs, an automorphism is a pair of permutation matrices (P, Q) such that $PM = MQ$. Notice that either one of P and Q is completely determined by the other. Using some concepts from representation theory, we can prove a useful result. (The reader unfamiliar with representation theory may skip the next proof.)

Proposition 3.26 (Block, cf. [3])**.** *On a symmetric design, the number of orbits on points equals the number of orbits on blocks, for any subgroup of Aut*(D)*.*

Proof. Suppose that (P, Q) is an automorphism of a design with incidence matrix M. By Proposition 3.22, the incidence matrix of a symmetric design is invertible. Then

$$PMQ^\top = M\,,$$

which implies that

$$P = MQM^{-1}\,.$$

In particular, P and Q are conjugate matrices, and so have the same trace. Since the trace of a permutation matrix is just the number of fixed points of the corresponding permutation, we see that projection onto P and Q determine conjugate representations of the automorphism group. By the Cauchy-Frobenius Lemma, the number of orbits on points and blocks are equal. □

If G is a group of permutations acting regularly on the points of D then G also acts regularly on the blocks of D. This has rather interesting consequences for D, as illustrated in the next section.

3.4. **Difference Sets.** Generalising planar difference sets, we have the next definition and examples.

Definition 3.27. A subset X of finite group G is a *difference set* if, for each nontrivial element $g \in G$ there exist a fixed number λ of ordered pairs $x, y \in X$ such that $xy^{-1} = g$.

Example 3.28. In the cyclic group of integers mod 7 Z_7, the set $D = \{0, 1, 3\}$ is a difference set. Notice that, in this difference set, every element g of Z_7 has exactly $\lambda = 1$ representation as a difference of two elements:

$$\begin{array}{ll} 0 = 0 - 0 & 1 = 1 - 0 \\ 2 = 3 - 1 & 3 = 3 - 0 \\ 4 = 0 - 3 & 5 = 1 - 3 \\ 6 = 0 - 1 & \end{array}$$

Example 3.29. For a slightly less trivial example, consider the additive group G of the vector space $V = \mathbb{F}_2^4$. then the set

$$D = \{(0,0,0,0), (1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1), (1,1,1,1)\}$$

is a difference set for G. For a brief exercise, find the value of the parameter λ.

Now, we connect back to designs. Namely, we will show that every difference set of a group suggests a 2-design, and (perhaps more importantly for us) every 2-design with a regular group of automorphisms admits a difference set.

Theorem 3.30. *Let $X \subseteq G$ be a difference set in G. Then $\{Xg \mid g \in G\}$ is the set of blocks of a symmetric 2-design with point set G.*

Conversely, if (V, B) *is a symmetric* 2-(v, k, λ) *design admitting a regular group of automorphisms isomorphic to* G *on points, then there exists a difference set of size of* k *in* G*.*

Proof. Let $X \subset G$ be a λ difference set. Then every group element $g \in G$ can be represented as a difference $xy^{-1} = g$ in exactly λ ways. Now consider two distinct blocks $B_1 = Xg_1$ and $B_2 = Xg_2$. We consider the intersection $B_1 \cap B_2$. If $g \in B_1 \cap B_2$, then $\exists x_i, x_j \in X$ such that $x_i g_1 = x_j g_2$, and thus $x_i x_j^{-1} = g_2 g_1^{-1}$.

This reveals that every element in this intersection must be equal to $g_2 g_1^{-1}$, which, since X is a λ difference set, will occur exactly λ times. Therefore, for any pair of distinct blocks, their intersection has fixed size λ.

On the other hand, Suppose that we have a symmetric design (V, B) given as a symmetric 2-$v, k, \lambda)$ design with automorphism group G. Then label the points according to the regular group action (i.e. choose a point $p \in V$ and label it with the identity $e \in G$, and label v^g with G). Now, we have the design as a collection of group elements.

Then, by Block's lemma (Proposition 3.26), the group action is transitive on blocks. Then, since the action is transitive, and since $|\mathrm{Orb}(x)| = [G : \mathrm{Stab}(x)]$ for all $x \in G$, the stabilizer of a point must be $\{e\}$. Therefore, the action is regular, and a difference set can be constructed with every point contained in exactly λ blocks. □

3.5. **Aside: Desarguesian planes.** This subsection is not strictly necessary to our exposition but describes some connections between algebraic and geometric conditions on a projective plane, and explains the adjective Desarguesian.

The following theorem due to Desargues appears at first to be purely geometric, [1]:

Theorem 3.31 (Desargues)**.** *Let* l_1, l_2, l_3 *be distinct lines which meet in a point* P*. Let* Q, Q' *be points on* l_1*,* R, R' *be points on* l_2*, and* S, S' *be points on* l_3 *which are all distinct from* P*.*

We assume

$$\overline{QR} \mid\mid \overline{Q'R'} \quad \textit{and} \quad \overline{QS} \mid\mid \overline{Q'S'}.$$

Then

$$\overline{RS} \mid\mid \overline{R'S'}.$$

Simply put; if two pairs of sides of a triangle align (from a certain perspective), then the third side must also align.

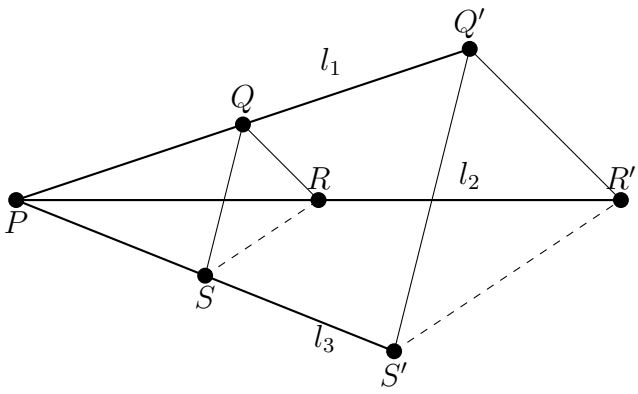

Fig. 3. A simple diagram illustrating Theorem 3.31.

Historically, this result is due to Desargues, who established it for the real and complex projective planes. His proof does **not** follow from the axioms of a project plane alone, however. He requires the structure of a field to co-ordinatise the points and lines in his plane. In fact, it turns out that Desargues theorem holds for a projective plane (whether finite or infinite) **if and only if** the plane is obtained from a three dimensional vector space over a division algebra (which need not be a field). Hence a seemingly geometric theorem requires an algebraic structure.

3.6. **Automorphisms of Projective planes.** We now prove the existence of a large group of automorphisms of a Desarguesian projective plane. (In contrast, non-Desarguesian planes need not have any symmetries at all.)

Definition 3.32. An *automorphism* of a field is a function $\sigma : E \to E$ which satisfies

$$(x+y)^\sigma = x^\sigma + y^\sigma, \quad (xy)^\sigma = x^\sigma y^\sigma \,.$$

If E is a field of characteristic p, then $\binom{p}{c} \equiv 0 \pmod{p}$ for all $1 \leq c \leq p-1$, so that

$$(x+y)^p = x^p + y^p$$

hence raising elements to the p^{th} power is a field automorphism. This is called the *Frobenius automorphism* of the field.

The automorphisms of a field E form a group, and the fixed points of an automorphism form a subfield. Note that the prime fields have no automorphisms (the Frobenius automorphism fixes all elements pointwise), so that the prime field is always fixed. An extension is *Galois* if the number of automorphisms is equal to the degree of the extension.

Definition 3.33. Let K be a field, and let K^n be a vector space. Then a *semilinear transformation* of K^n is a map $f : K^n \to K^n$ for which there exists a field automorphism $\tau : K \to K$ such that

$$f(c_1\mathbf{v_1} + c_2\mathbf{v_2}) = \tau(c_1)f(\mathbf{v_1}) + \tau(c_2)f(\mathbf{v_2}) \quad (c_1, c_2 \in K,\ \mathbf{v_1}, \mathbf{v_2} \in K^n).$$

If f bijective, we call f a *semilinear automorphism.*

Now call the family of all semilinear automorphisms $\Gamma\mathrm{L}_n(K)$. Then, $Z(K) \trianglelefteq \Gamma\mathrm{L}_n(K)$, and we call the quotient $\Gamma\mathrm{L}_n(K)/Z(K) := \mathrm{P}\Gamma\mathrm{L}_n(K)$.

We have not had occasion to use Projective Geometries of rank greater than 2 in this thesis, though they are defined similarly to projective planes: one takes the 1-dimensional subspaces of a n-dimensional vector space over the field $\mathbb{F}$ to obtain the projective space $\mathrm{PG}(n-1, \mathbb{F})$. Amazingly, in dimensions greater than 2, **all** projective spaces are Desarguesian, and so come from vector spaces over a field. Unfortunately, there are many constructions for non-Desarguesian projective planes, so we can state the following theorem only in the Desarguesian case.

Theorem 3.34 (Fundamental Theorem of Projective Geometry)**.** *Let q be a prime power, and let $n \in \mathbb{N}$ with $n \geq 2$. Then*

$$P\Gamma L_{n+1}(\mathbb{F}_q) \cong Aut(PG(n, q))$$

(Here, $PG(2, q)$ is Desarguesian by definition.)

Proof. A proof of this result is rather lengthy, and can be found in [1]. □

It will be sufficient for our purposes to know that all of $\mathrm{PGL}_2(q)$ acts by automorphisms on the Desarguesian projective plane of order q.

3.7. **Singer's Theorem.** We now have almost all the results required to prove Singer's Theorem. It remains only to embed the field $\mathbb{F}_{q^3}$ into the matrix algebra $M_3(q)$. This is the associative algebra analogue of Cayley's thoerem for finite groups.

Theorem 3.35. *Suppose that A is a d-dimensional associative algebra over K. Then A there exists an injective homomorphism from A to $M_d(K)$, the algebra of $k \times k$ matrices.*

Proof. Let $B = \{a_1, a_2, \ldots, a_d\}$ be a basis for A as a vector space. Right multiplication in A is k-linear by definition. So $R_a : a_i \mapsto a_i a$ is a linear transformation for any $a \in A$. Now, representing R_a as a $d \times d$ matrix with respect to the basis B gives an injective homomorphism from A into $\mathrm{M}_d(k)$ as required. □

Next, we require the fact that the multiplicative group of a finite field is cyclic.

Theorem 3.36. *The multiplicative group of a finite field is cyclic*

For a proof of this, see [1]

Proposition 3.37. *The group $GL_3(q)$ contains a cyclic subgroup of order q^3-1, called a **Singer cycle**.*

Proof. By Theorem 3.36, the multiplicative group of the field K of order q^3 is cyclic of order q^3-1. By the field axiom, multiplication by a non-zero element is bijective in the field, so in the embedding of K into the algebra of 3×3 matrices over q, all non-zero elements are invertible. Hence by Theorem 3.35, there exists a subgroup of order q^3-1 in the group $\mathrm{GL}_3(q)$. □

To conclude our proof of Singer's theorem, we just need to understand the induced action of a Singer cycle on the points and lines of the corresponding projective plane.

Theorem 3.38 (Singer)**.** *Let $\Pi(q)$ be the Desarguesian projective plane of order q. Then $Aut(\Pi(q)) \cong P\Gamma L_3(q)$ contains a cyclic subgroup of order q^2+q+1 acting regularly on the points of $\Pi(q)$.*

Equivalently, for any prime power q the cyclic group of order q^2+q+1 contains a planar difference set.

Proof. Let S be a generator of a Singer cycle, as in Proposition 3.37, and write s for the corresponding generator of the multiplicative group of $\mathbb{F}_{q^3}$. Consider the permutation action of S on the q^3 points of the underlying vector space. For non-negative integer t, a fixed point of S^t corresponds to a solution of the equation

$$s^t x = x$$

in the field. By the field axioms, either $x=0$ or $s^t=1$. Hence the only fixed point of S is the zero vector, and all other vectors are permuted transitively.

Since multiplication by an element of the base field fixes all lines through the origin, the Singer cycle contains scalar matrices, and the image in $\mathrm{PGL}_3(q)$ has size q^2+q+1. Since the action on vectors of V is transitive, the action on one-dimensional subspaces is transitive, and hence regular.

Now apply Lemma 3.26, to see that the action on projective lines must be transitive. The requirements of Theorem 3.30 are satisfied, and so the cyclic group of order q^2+q+1 contains a difference set.

The elements of the difference set correspond to the points on a projective line. Any 2-dimensional subspace of V can be used for this purpose. In the literature, the elements of field trace 0 are often used, since they have a definition intrinsic to the field (so it is not necessary to choose a basis or write out explicit matrices). This completes the proof. □

As an illustration of Singer's construction, let σ be any invertible linear transformation $\sigma : \mathbb{F}_2^3 \to \mathbb{F}_2^3$. Obviously, σ induces a permutation on the pointset of the

Fano plane. Observe that $v_1, v_2, v_3 \in \mathbb{F}_2^3$ satisfy the condition $v_1 + v_2 + v_3 = 0$ if and only if they are collinear, because over $\mathbb{F}_2$ this is equivalent to $v_1 + v_2 = v_3$. Then $\sigma(v_1 + v_2 + v_3) = \sigma(0)$, so $\sigma(v_1) + \sigma(v_2) + \sigma(v_3) = 0$, so $\sigma(v_1)\sigma(v_2), \sigma(v_3)$ must be collinear. Hence M preserves the set of blocks, and so is an automorphism of the Fano plane. We have shown that $\mathrm{GL}_3(2)(= \mathrm{PGL}_3(2))$ acts on the Fano plane.

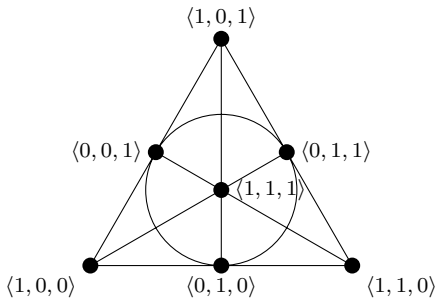

Fig. 4. The Fano Plane, labeled with blocks determined by 2-dimensional subspaces of $\mathbb{F}_2^3$. Notice that, for each line l, $\sum_{\mathbf{p}\in l} \mathbf{p} = 0$, verifying that these are, indeed, 2-dimensional subspaces.

Example 3.39. Let $q = 3$, and our goal is thus to construct the difference set for C_{13}. The polynomial $p(x) = x^3 + 2x + 1$ is irreducible over $\mathbb{F}_3$. Now consider $\mathbb{F}_{3^3}$ as a 3-dimensional vector space over $\mathbb{F}_3$. If ω is a primitive element of $\mathbb{F}_{3^3}$. Then

$\omega^0 = 1$	$\omega^9 = 2\omega^2 + 2\omega + 2$	$\omega^{18} = \omega + 1$
$\omega^1 = \omega$	$\omega^{10} = \omega^2 + 2\omega + 1$	$\omega^{19} = \omega^2 + \omega$
$\omega^2 = \omega^2$	$\omega^{11} = \omega + 2$	$\omega^{20} = 2\omega^2 + 2$
$\omega^3 = \omega^2 + 2$	$\omega^{12} = \omega^2 + 2\omega$	$\omega^{21} = 2\omega + 2\omega + 1$
$\omega^4 = \omega^2 + 2\omega - 1$	$\omega^{13} = 2$	$\omega^{22} = \omega^2 + \omega + 1$
$\omega^5 = 2\omega + 2$	$\omega^{14} = 2\omega$	$\omega^{23} = 2\omega^2 + \omega + 2$
$\omega^6 = 2\omega^2 + 2\omega$	$\omega^{15} = 2\omega^2$	$\omega^{24} = 2\omega + 1$
$\omega^7 = \omega^2 + 1$	$\omega^{16} = 2\omega^2 + 1$	$\omega^{25} = 2\omega + \omega$
$\omega^8 = \omega^2 + \omega + 2$	$\omega^{17} = 2\omega^2 + \omega + 1$	$\omega^{26} = 1$

Now we need a 2-dimensional subspace of $\mathbb{F}_{3^3}$. Arbitrarily, we will take the one spanned by $\{1, \omega\}$. This subspace will be

$$S = \{a\omega + b | a, b \in \mathbb{F}_3\}$$

Then S will contain the elements

$0\omega + 0 = 0$	$0\omega + 1 = \omega^0$	$0\omega + 2 = \omega^{13}$
$1\omega + 0 = \omega$	$1\omega + 1 = \omega^{18}$	$1\omega + 2 = \omega^{11}$
$2\omega + 0 = \omega^{14}$	$2\omega + 1 = \omega^{24}$	$2\omega + 2 = \omega^5$

So taking the nonzero elements, we get

$$S = \left\{0, \omega^0, \omega, \omega^5, \omega^{11}, \omega^{13}, \omega^{14}, \omega^{18}, \omega^{24}\right\}$$

Then, considering S in the context of C_{3^2+3+1}, we see that, when removing redundancy (and the zero vector),

$$S = \left\{\omega^0, \omega, \omega^5, \omega^{11}\right\}$$

Thus, our Singer difference set for C_{13} is $\{0, 1, 5, 11\}$.

Observe that

$$1-0=1,\ \ 0-11=2,\ \ 1-11=3,\ \ 5-1=4,\ \ 5-0=5,\ \ 11-5=6\,,$$

and the remaining non-zero elements are obtained by negating these equations.

We conclude with explicit bounds on the liminf and limsup of packings and coverings in a cyclic group.

Theorem 3.40. *As $n \to \infty$ the limit superior of the normalised density of a packing in the cyclic group C_n tends to 1;*

$$\limsup P(C_n)/\sqrt{n} = 1\,.$$

Dually, as $n \to \infty$ the limit inferior of the normalised density of a covering in the cyclic group C_n tends to 1;

$$\liminf C(C_n)/\sqrt{n} = 1\,.$$

Unfortunately, the packing and covering properties in C_n are unrelated to those in C_{n+1} so that the arguments of Redei and Renyi for intervals in $\mathbb{Z}$ do not translate to cyclic groups. Nevertheless, their methods were adapted by Banakh and Gavrylkiv to give upper bounds on the density of a covering of a cyclic group. This is the topic of the next chapter.

4. Coverings in Cyclic Groups

In this Chapter we describe recent work of Banakh and Gavrylkiv which gives the best known upper bounds on the covering numbers of cyclic groups.

Example 4.1. Let q be a prime power. Then, according to the Theorem 3.38 of Singer, $G = C_{q^2+q+1}$ has a has a covering of $G \setminus \{0\}$ which is of the optimal size $q+1$. Therefore, $\mathrm{Cov}[C_{q^2+q+1}] = q+1$.

Since

$$\lim_{q\to\infty} \frac{\mathrm{Cov}(C_{q^2+q+1})}{\sqrt{q^2+q+1}} = 1\,,$$

for prime powers q. We refer to this ratio as the *covering ratio* of a group. Banakh and Gavrylkiv give an estimate which holds for any cyclic group.

4.1. **Coverings of intervals and cyclic groups.** We relate coverings of intervals to those of cyclic groups. For some computations in Proposition 4.2 and Theorem 4.5 it will be convenient to represent cyclic groups as groups of complex numbers. In the remainder of this chapter, we fix the cyclic group of order n to be

$$C_n = \{\omega_n \in \mathbb{C} \mid \omega_n^n = 1\}\ .$$

Proposition 4.2. *For a natural number k and $\varepsilon \in \{0,1\}$ the following bounds hold:*

$$Cov(C_{2k+\varepsilon}) \le Cov(k) \quad \textit{and} \quad \frac{Cov(C_{2k+\varepsilon})}{\sqrt{2k+\varepsilon}} \le \frac{Cov(k)}{\sqrt{2k}}.$$

Proof. Define a homomorphism $\gamma : \mathbb{Z} \to C_n$ by

$$\gamma(t) = \omega_n^t$$

Let $D \subset \mathbb{Z}$ of cardinality $|D| = \mathrm{Cov}(k)$ such that D covers the interval $[1,k]$. Since $x - y = -(y-x)$ then D also covers the interval $[-k,-1]$, and trivially $x-x$ covers 0.

Since D is a cover of the integers in the interval $[-k,k]$, $\gamma(D)$ is a cover of the cyclic group $C_{2k+\varepsilon}$ for $\varepsilon \in \{0,1\}$.

For the second claim, we simply normalise appropriately.

$$\begin{aligned}\frac{\mathrm{Cov}[C_n]}{\sqrt{n}} = \frac{\mathrm{Cov}(C_n)}{\sqrt{n}} &\leq \frac{\mathrm{Cov}(k)}{\sqrt{k}}\frac{\sqrt{k}}{\sqrt{n}} \\ &\leq \frac{\mathrm{Cov}(k)}{\sqrt{k}}\sqrt{\frac{n/2}{n}} \\ &\leq \frac{\mathrm{Cov}(n)}{\sqrt{2n}}\end{aligned}$$

□

By the results of Chapter 2, the upper bound

$$\frac{\mathrm{Cov}(n)}{\sqrt{n}} \leq \frac{128}{\sqrt{6166}} \sim 1.63$$

holds. Proposition 4.2 allows us to improve this bound by a factor of $\sqrt{2}$, so we find that

$$\frac{\mathrm{Cov}(C_{2k+\varepsilon})}{\sqrt{2k+\varepsilon}} \leq \frac{128}{\sqrt{2 \cdot 6166}} \sim 1.15\,.$$

4.2. **A recursive construction.** In Banakh's recursive construction, we require the maximal gap between two elements of a difference basis of a cyclic group, as illustrated below.

Definition 4.3. For an integer n, let

$$\mu(n) = \max_{D} \max_{x,y \in D} |x - y|$$

where D ranges over all covers of C_n of minimal size, and distances are measured in the integers between preimages of x, y in the interval $[0, n-1]$.

Example 4.4. The Singer difference set in the cyclic group of order $73 = 8^2 + 8 + 1$ is as follows:

$$D = \{0, 1, 12, 20, 26, 30, 33, 35, 57\}$$

The maximal gap between two elements in the sequence is $57 - 35 = 22$. So $\mu(73) \geq 22$.

While Banakh gives a more complicated result, the bound resulting from the Pigeonhole Principle suffices for us.

Theorem 4.5. *For any natural number $n \geq 3$,*

$$\mu[C_n] \geq \left\lfloor \frac{n}{Cov[C_n]} \right\rfloor .$$

Proof. Fix a difference basis $D \subset C_m$ of size $|D| = \mathrm{Cov}[C_m]$. Since cyclic shifts of a difference basis are still difference bases, we may assume that D contains $0, 1$.

Define $k = \left\lfloor \frac{n}{\mathrm{Cov}[C_n]} \right\rfloor$, and let $I_c = [c, c+1, \ldots, c+k]$ be the image of an interval of length k in C_n. On average the interval I_c contains at most 1 element of D. But

for $-k+1 \leq c \leq 0$, the interval I_c contains both 0 and 1. From the definition of the expected value, there exists at least one interval I_c disjoint from D. □

Theorem 4.6. *For any non-negative integers n, m, we get the upper bound*

$$Cov[nm + \mu[C_m] - 1] \leq Cov[n] \cdot Cov[C_m]$$

Proof. Let a difference basis D of optimal size be given for the interval $[-n, n]$. Then, there exists a set $A \subset [0, m]$ of size $|A| = \mathrm{Cov}(C_m)$ such that $A - A + m\mathbb{Z} = \mathbb{Z}$, and $|A \cap [0, \mu[C_m])|$ is empty.

Find two numbers $\lambda, l \in D$ where $\lambda - l = n$. Then define the set

$$B := \{a + md \mid a \in A,\ d \in D\} \cup \{a + m(\lambda + 1) \mid a \in A \cap [0, \mu[C_m])\}$$

It is clear that the cardinality of this set is

$$|B| \leq |D| \cdot |A| + |A \cap [0, \mu[C_m])| \leq \mathrm{Cov}(n) \cdot \mathrm{Cov}(C_m).$$

Then the interval $J = \{(-mn - \mu(C_m)), \ldots, -2, -1, 0, 1, 2, \ldots (mn + \mu(C_m))\}$ is contained in the set of differences of elements of B. In order to see this, notice that the set of differences $B - B$ is symmetric, and so it suffices to demonstrate this fact for the positive elements of $B - B$. Let some $x \in J$ be given. Then we can write x as $x = my + z$, where $0 \leq y \leq n$ and $0 \leq z < m$. Then, by the definition of A, there exist values $a, b \in A$ such that $z = a - b + mj$ for some integer j. Then, since $|mj| = |a - b - z| \leq |a - b| + |z| < 2m$, $|j| \leq 1\mathrm{m}$ and therefore $|y + j| \leq n + 1$.

Then, it follows that

$$x - my + z = m(y + j) + a - b.$$

The case where $|y + j| \leq n$ follows directly, so assume that $|y + j| = n + 1$, Then

$$x = m(y + j) + 1 - n = m(n + 1) + a - b.$$

Then, since $x < mn + \mu[C_m]$, we can conclude that

$$a \leq m + a - b = x - mn < \mu[C_m],$$

and hence $a + m(\lambda + 1) \in B$. Then

$$\begin{aligned} x &= m(n + 1) + a - b \\ &= m(\lambda - l + 1) + a - b \\ &= a + m(\lambda + 1) - (b + ml) \in B - B. \end{aligned}$$

Then, since the choice of x was arbitrary, $J \subset B - B$, and the result is proven. □

Corollary 4.7. *Let n be a natural number, q a prime-power, and $k = n(q^2+q+1)+q+1$. For any natural number $l \leq 2k+1$ we get the upper bound*

$$\begin{aligned} Cov(C_l) &\leq Cov(k) \\ &\leq Cov(nm + \mu[C_m] - 1) \\ &\leq Cov(n) \cdot Cov(C_m) = Cov(n) \cdot (q+1) \end{aligned}$$

Proof. From the theorem of Singer, a cyclic group C_{q^2+q+1} (where q is a prime power) has difference size $\mathrm{Cov}(C_{q^2+q+1}) = q+1$. Then, by Theorem 4.5, $\mu[C_{q^2+q+1}] \geq q+2$.. Then, following directly from Theorem 4.6,

$$\begin{aligned} \mathrm{Cov}[C_l] &\leq \mathrm{Cov}[k] \\ &\leq \mathrm{Cov}[nm + \mu[C_{q^2+q+1}] - 1] \\ &\leq \mathrm{Cov}[n] \cdot \mathrm{Cov}[C_{q^2+q+1}] = \mathrm{Cov}[n] \cdot (q+1) \end{aligned}$$ □

4.2.1. *Numerical Bounds.* We now look at some of the numerical bounds given in [2].

First, we will establish some bounds for larger cyclic groups: namely, when $n \geq 11$.

A direct application of corollary 4.7 with $n = 6166$ yields the following result:

Lemma 4.8. *Let q be a prime power, and let a natural number $n \leq 12332q^2+12334q+12335$ be given. Then*

$$Cov[C_l] \leq 128(q+1).$$

Proof. Consider the cyclic group C_{q^2+q+1}. Then Singer guarantees us a covering of C_{q^2+q+1} of size $q+1$. Then, Theorem 4.5 tells us that $\mu[C_{q^2+q+1}] \geq q+2$. Then, Theorem 4.6 gives us the upper bound

$$\begin{aligned} \mathrm{Cov}(C_n) &\leq \mathrm{Cov}(6166m + \mu[C_m] + 1) \\ &\leq \mathrm{Cov}(6166) \cdot \mathrm{Cov}(C_m) = 128(q+1) \end{aligned}$$ □

And furthermore, for all $n \geq 926$ we achieve the upper bound

By taking $n \geq 926$ and factoring the quadratic in q in this corollary, we can see the following result.

Theorem 4.9. *Let r^+ denote the positive root of the quadratic $12332q^2+12334q+12335$, and let q be the largest prime-power less than r^+. Then for all $n \geq 926$, we achieve the upper bound*

$$Cov(C_n) \leq 128\left(1 + q \cdot r^+\right) = \frac{64}{\sqrt{3084}}\sqrt{n} + O\left(n^{21/80}\right).$$

Proof. First, notice that r^+ is well-defined only when $n \geq 926$, and

$$n = 12332 \cdot (r^+)^2 + 12334 \cdot r^+ + 12335 \leq 12332q^2 + 12334q + 12335$$

Then – according to Banakh and Gavrylkiv in [2] – Baker, Harman, and Pintz demonstrated that $q \leq r^+ + O\left((r^+)^{21/40}\right)$, so

$$\begin{aligned} \mathrm{Cov}(C_N) \leq 128(q+1) &= 128\left(r^+\right) + O\left(x^{21/40}\right) \\ &= \frac{128}{\sqrt{12332}}\sqrt{n} + O\left(n^2 1/80\right) \\ &= \frac{64}{\sqrt{3083}}\sqrt{n} + O\left(n^{21/80}\right) \end{aligned}$$ □

By taking substantially larger n (on the order of 10^{15}, we can improve the assumption of the distribution of primes, and achieve

$$\mathrm{Cov}(C_n) < \frac{2}{\sqrt{3}}\sqrt{n}.$$

with the exact same method.

Unfortunately, these results require n to be quite large. Thus, we simply state a result for substantially smaller n. This result is due in large to computational work done in [2] again by Banakh and Gavrylkiv.

Theorem 4.10. *If $n \geq 9$, then $Cov(C_n) \leq \frac{12}{\sqrt{73}}\sqrt{n}$. Furthermore, if $n \neq 292$, $Cov(C_n) \leq \frac{24}{\sqrt{293}}\sqrt{n}$.*

5. Conclusion

We have surveyed the literature on Packings and Coverings of Abelian groups, with particular emphasis on intervals of $\mathbb{Z}$ and finite cyclic groups. We established the following bounds on the density of a packing and a covering in these cases (for n sufficiently large).

	Number intervals	**Cyclic groups**
Packings	$0.707 \leq \frac{\text{Pack}(n)}{\sqrt{n}} \leq 1.414$	$.5 \leq \frac{\text{Pack}(C_n)}{\sqrt{n}} \leq 1$
Coverings	$1.56 \leq \frac{\text{Cov}(n)}{\sqrt{n}} \leq 1.63$	$1 \leq \frac{\text{Cov}(C_n)}{\sqrt{n}} \leq 1.40$

While these results are not optimal, they are not far from it.

We conclude this thesis with some observations about packings and coverings in more general finite groups. It would appear that the covering problem is rather easier than the packing problem, since the following easy result is available.

Proposition 5.1. *Suppose that G is a finite group of order nm with a subgroup H of order m. Then G has a covering of size $n+m$.*

Proof. Let T be a transversal of H in G. Then every element of G can be written in the form $t_i h_j$ for some $t_i \in T$ and some $h_j \in H$. Hence $H \cup T$ is a covering of G. □

Obviously the optimal case for this proposition occurs when $|H| \sim |G|^{1/2}$ in which case, $|T \cup H|$ is also proportional to $|G|^{1/2}$, and so is within a constant factor of optimality. Without the classification of finite simple groups, it is known that a group G must have a subgroup of order $\sim |G|^{1/3}$, from which a covering of size $|G|^{2/3}$ is obtained. Using the classification of finite simple groups, it can be shown that any finite group G has a subgroup of order $\sim |G|^{1/2}$. From this fact, Kozma and Lev obtain the much tighter bound of a covering of size $4/\sqrt{3}|G|^{1/2} \sim 2.309|G|^{1/2}$ for any finite group.

Still tighter results have been obtained for more restricted classes of groups. In particular, Banakh and Gavrylkiv have proved that a finite abelian p-group has covering number bounded above by $\sqrt{2}|G|^{1/2} \sim 1.41|G|^{1/2}$.

In contrast, results on packings in finite groups appear to be substantially more difficult. Particularly in non-abelian groups, it quickly becomes difficult to control products of elements drawn from distinct subgroups, so preventing collisions becomes troublesome. Babai and Sos have used the probabilistic method to show than any finite group contains a packing of size $c|G|^{1/3}$ for some universal constant c. For various classes of well-behaved groups (e.g. elementary abelian groups and direct products of certain cyclic groups) they obtain near optimal bounds on the size of a packing.

References

[1] E. Artin. Geometric Algebra. New York, Interscience Pulishers, 1957.

[2] T. Banakh and V. Gavrylkiv. Difference bases in cyclic groups, 2017.

[3] T. Beth, D. Jungnickel, and H. Lenz. Design Theory, volume 2 of Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2 edition, 1999.

[4] P. Erdös and P. Turán. On a problem of Sidon in additive number theory, and on some related problems. J. London Math. Soc., 16:212–215, 1941.

[5] M. Isaacs. Algebra: a graduate course. Graduate studies in Mathematics. American Mathematical Society, 2009.

[6] A. R. L. Rédei. On the representation of the numbers $1, 2, \ldots, n$ by means of differences. Mat. Sb. (N.S.), 24(66):385–389, 1949.

[7] F. R. Moulton. A simple non-desarguesian plane geometry. Transactions of the American Mathematical Society, 3(2):192–195, 1902.

[8] K. O'Bryant. A complete annotated bibliography of work related to sidon sequences. The Electronic Journal of Combinatorics, 2004.

[9] I. Z. Ruzsa. An infinite sidon sequence. Journal of Number Theory, 68(1):63–71, 1998.