On 3-cube-free constructions in $\mathbb{Z}_{2^n}$

by Ethan Washock

December 15, 2022

A Masters Thesis submitted to the faculty of Worcester Polytechnic Institute

in partial fulfillment of the requirements for the Degree in Master of Science in

Applied Mathematics

Advisor

Professor Adam Zsolt Wagner

Thesis Advisor

____

Head of the Mathematical Sciences Department

____

Abstract

Classical theorems in extremal combinatorics due to Sperner, Erdős, Kleitman, and Samotij state that families minimizing the amount of chains in a Boolean lattice are restricted to a "layered" construction. These theorems translate from the Boolean lattice to the integers modulo 2^n when k-chains are replaced with projective cubes of dimension 2^{k-1} in the case of k being a power of two. This case was proven by Long and Wagner in 2018. Conjectured constructions of largest k-cube-free for any k are also conjectured in their paper, which also have a specific layered construction. However, these bounds on the size of a k-cube-free set aren't proven. In this thesis, I will investigate the structure of 3-cube-free subsets of the integers modulo 2^n and derive strategies for bounding the "fullness" of layers in a 3-cube-free construction that could possibly be extended to deal with any k-cube-free set.

Acknowledgements

Firstly, I'd like to thank the Mathematics graduate student body at WPI for welcoming me to seminars, events, and even just casual gatherings to play board games. Thank you for fostering an environment of growth for graduate students when it comes to presenting and writing. I would like to specifically thank Guillermo Nuñez Ponasso, who's a current PhD student at WPI working in the area of combinatorics who has had insightful conversations with me on this thesis matter. I'd also like to mention the Mathematical Sciences undergraduate students who I've been thankful to have as friends since my years as an undergraduate: Tony, Scar, Maggie, Ryan, Jakob, Char, and Forrest. Moreover, I'd like to thank Frederick "Forrest" Miller for his knowledge of linear programming and help in discussing the use of Gurobi.

Second, I'd like to thank Professor Wagner for giving me the opportunity to work on this problem and giving me advice throughout my work. I appreciate his input and suggestions of strategies to use and not to use throughout this thesis, along with his advice on life as a new graduate student in Mathematics.

Lastly, I'd like to thank my parents, Karrie and Brian, for their constant support throughout this work. Our conversations in periods outside of working on this thesis have kept my spirits high and I'm thankful to have them throughout the tough times I've had while working.

Contents

List of Figures

List of Tables

1 Introduction

The notion of a cube can be extended to any ring using the notion of a Hilbert cube. A set is a *Hilbert cube* (also called a *cube*), $H \subset \mathbb{N}$, if there exists a set $S = \{x_0, \ldots, x_d\} \subset \mathbb{N}$ (however, x_0 could be zero) such that $H = \{x_0 + \sum_{i \subset S} x_i \,:\, I \subset [d]\}$, where $[d] = \{1, \ldots, d\}$ and d is called the *dimension* of the cube. An early result of Ramsay theorem due to Hilbert states that if n is sufficiently large, then any coloring of $[n]$ with a fixed number of r colors must contain a monochromatic Hilbert cube of dimension d [9]. This smallest such value of n is denoted by $h(d, r)$ and is bounded above by

$$h(d, r) \leq (2r)^{2^{d-1}} \tag{1}$$

A connection has been made between sets without Hilbert cubes in the Boolean lattice $\mathbb{Z}_2^n$ and classical results in extremal combinatorics. Recall that for distinct sets $A, B \subset [n]$ form a 2-*chain* if $A \subset B$ or $B \subset A$. A collection of k distinct subsets of $[n]$ form a k-chain if any pair of subsets form a 2-chain. Sperner proved the following about families without 2-chains:

Theorem 1.1. *(Sperner [15], 1928) If a family $\mathcal{F} \subset \mathbb{Z}_{2^n}$ does not contain a 2-chain, then $|\mathcal{F}|$ is no larger than the size of the largest layer.*

Erdős extended this result to deal with families without chains of any length.

Theorem 1.2. *(Erdős [7], 1945) For all integers n, k such that $n \geq k \geq 2$, $\mathcal{F}$ being k-chain-free implies that $|\mathcal{F}|$ is no larger than the sum of the $k - 1$ largest layers.*

These results for the Boolean lattice have analogues in the cyclic group $\mathbb{Z}_{2^n}$ that incorporate the non-existence of projective cubes. These projective cubes have structure similar to Hilbert cubes, with the cube generated by a set S having the projective cube $\{\sum_{j \in I} j \,:\, \varnothing \neq I \subset S\}$. Specifically, Long and Wagner proved that for all integers n, k such that $n \geq k \geq 2$, $\mathcal{F}$ having no projective 2^{k-1}-cube implies that $|\mathcal{F}|$ is no larger than the union of its k largest layers [12]. There are conjectured l-cube-free subsets of $\mathbb{Z}_{2^n}$ for any integers l that aren't powers of 2, but there aren't any proofs that there exist no sets of larger size containing no l-cubes. This even includes the case of finding the largest subset of $\mathbb{Z}_{2^n}$ with no 3-cube. The hypothesized largest size of 3-cube-free set in $\mathbb{Z}_{2^n}$ has size $\frac{5}{8} \cdot 2^n$ and is comprised of all odd numbers and all numbers congruent to 4 modulo 8.

Several problems in extremal combinatorics can be implemented as *integer linear programs* [19]. The use of LP solvers quickly allow one to find a large pool of near-optimal solutions subject to a system of constraints, and will allow us to come up with conjectures on the structure of 3-cube-free sets. We present one way to implement this problem as such a program that can be solved exactly for the cases up to $n = 7$ through the state-of-the-art LP solver, Gurobi [8]. This implementation is coded in Python and is listed in the section "Code implementations" [17].

The goal of this thesis is to (i) investigate the structure of 3-cube free subsets of the integers modulo 2^n, (ii) formulate ways to most efficiently search for cube-free sets, and (iii) derive strategies for bounding the "fullness" of layers in a 3-cube-free construction that could possibly be extended to deal with any k-cube-free set.

The format of this thesis is as follows: Chapter 2 defines the problem which the thesis aims to tackle along with terminology used by Wagner and Long in their original paper which I will use throughout this thesis. Chapter 3 will elaborate on specific conditions which 3-cube-free sets must have, specifically involving inequalities on the sizes of the layers. Chapter 4 will discuss other methods which have been attempted to solve this problem, and will argue whether these techniques are applicable to this problem. Chapter 5 introduces the linear programming model and boolean satisfiabilty model for the 3-cube-free set problem which can be used to verify conjectures about 3-cube-free sets, along with a discussion of a possible way to eliminate isomorphic sets from the search space by introducing "orderly generation". Chapter 6 concludes with open conjectures which would lead directly to the proof of a $\frac{5}{8} \cdot 2^n$ upper bound and further questions that follow from my results.

2 Establishing the problem

In this section, we will define what a projective cube is, introduce a partition of $\mathbb{Z}_{2^n}$ which has special additive properties, and use those properties of layers to prove verify that Long and Wagner's proposed 3-cube-free construction is indeed 3-cube-free.

We begin by defining a projective cube as follows:

Definition. Let R be a ring and let $S \subset R$ be a multiset. The *projective cube* generated by S, denoted $\mathcal{C}(S)$, is the set

$$\mathcal{C}(S) := \left\{ \sum_{x \in J} x : \varnothing \neq J \subset S \right\} \tag{2}$$

If $S \subset R$ is finite with $|S| = k$, the projective cube $\mathcal{C}(S)$ is referred to as a *k-cube.*

In this thesis, we are interested in projective 3-cubes. Therefore, as shorthand, we state that the cube generated by elements x, y, z is $\mathcal{C}(x, y, z)$. The open question that we wish to tackle in this paper is "Given any $n \in \mathbb{N}$, what is the largest subset of $\mathbb{Z}_{2^n}$ that is 3-cube free? What is the most efficient way to verify the largest such subset for any given $n \in \mathbb{N}$?"

Oftentimes in our constructions of cube-free subsets of $\mathbb{Z}_{2^n}$, given a fixed $n \in \mathbb{N}$, the following subsets of $\mathbb{Z}_{2^n}$ arise quite often for whole numbers j such that $1 \leq j \leq n$:

$$L_j := \{x \in \mathbb{Z}_{2^n} \, : \, x \equiv 2^{j-1} \mod 2^j\} \tag{3}$$

These are all pairwise disjoint subsets of $\mathbb{Z}^*_{2^n}$ that partition the non-zero elements of the ring. One can verify that for any whole number n, $\mathbb{Z}^*_{2^n} = \cup_{k=1}^{n} L_k$. Another equivalent way of viewing these layers is as $L_j := \{x \in \mathbb{Z}^*_{2^n} \, : \, j = \max\{\, k \in \mathbb{N} \, : \, 2^{k-1} \,|\, x \,\}\}$. This view is useful in seeing that for any $n \in \mathbb{N}$ and distinct $k, l \in \mathbb{N}$ such that $1 \leq k, l \leq n$, $x + y \in L_{\min(k,l)}$ for all $x \in L_k$ and $y \in L_l$. This partition of the layers gives us an ordering of the layers in $\mathbb{Z}_{2^n}$, which will now be called the "layer ordering". For any $n \in \mathbb{N}$ and $x, y \in \mathbb{Z}_{2^n}$, we say that $x \preceq y$ if x belongs to a lower layer than y or the same layer as y, taking $L_{n+1} = \{0\}$.

The layer in which the sum of two elements lies in can be deduced when given the layers in which the two elements are in. Special rules for addition of elements in layers are listed below.

Theorem 2.1. *Let $n \in \mathbb{N}$ and let $x, y \in \mathbb{Z}_{2^n}$. Given that $x \in L_a$ and $y \in L_b$, then (i) $x + y \in L_{\min(a,b)}$ if $a \neq b$, (ii) $x + y \in L_c$ for some $c > b$ if $a = b$ (under the condition that $L_{n+1} = \{0\}$), (iii) $2x \in L_{a+1}$ (if $x \neq 0$), and (iv) $x/2 \in L_{a-1}$ (if $x \notin L_1$).*

16	L_5
8 24	L_4
4 12 20 28	L_3
2 6 10 14 18 22 26 30	L_2
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31	L_1

Figure 1: The sets $L_1, L_2, \ldots, L_n$ partition $\mathbb{Z}_{2^n}^*$. Shown is an example of this partition for $n = 5$. Any element can be moved from L_k to L_{k+1} by multiplying the element by 2, with any element of L_{k+1} being moved to L_k by dividing the element by 2.

Proof. Fix $n \in \mathbb{N}$ and let $x, y \in \mathbb{Z}_{2^n}$ be arbitrary. Let $a, b \in \mathbb{N}$ such that $x \in L_a$ and $y \in L_b$. (i) Without loss of generality, take $a < b$. Taking $y = 2^b k + 2^{b-1}$ for some $k \in \mathbb{N}$, $y = 2^a(2^{b-a}k + 2^{b-a-1}) \equiv 0 \mod 2^a$. Therefore, $x + y \equiv 2^{a-1} \mod 2^a$, so $x + y \in L_a$. (ii) If $a = b$, then $x = 2^a k_1 + 2^{a-1}$ and $y = 2^a k_2 + 2^{a-1}$ for some $k_1, k_2 \in \mathbb{N}$. Therefore, $x + y = 2^a(k_1 + k_2) + 2^a \equiv 0 \mod 2^a$. It follows that $x + y$ cannot be in a lower layer than L_a, so $x + y \in L_c$ for some $c > a$. (iii) Taking $x = 2^a k + 2^{a-1}$ for some $k \in \mathbb{N}$, $2x = 2^{a+1}k + 2^a \equiv 2^a \mod 2^{a+1}$, so $2x \in L_{a+1}$. (iv) A similar process can be done by computing $x/2$ to show the fourth part of the theorem. □

Remark 2.1. *Using these facts, the set of cubes in $L_1 \cup L_2$ can be calculated. Given $\mathcal{C}(x, y, z) \subset L_1 \cup L_2$, $x, y, z \in L_1 \cup L_2$. Without loss of generality, we can let $x \prec y \prec z$ in the layer ordering. We cannot have two of the generators be in L_2, or else their sum would be in a layer above L_2. We also cannot have $x, y \in L_1$ and $z \in L_2$, since either $x + y \notin L_1 \cup L_2$ or $x + y + z = (x + y) + z$ is in a layer above L_2. Taking $x, y, z \in L_1$, $x + y = y_2$ for some $y_2 \in L_2$ so we can rewrite $y = y_2 - x$. Similarly, since $x + z \in L_2$, $z = z_2 - x$ for some $z_2 \in L_2$. We check that $x + z = y_2 + z + 2 - 2x = (y_2 + z_2) - 2x \in L_2$ and $x + y + z \in L_1$, so the cubes in $L_1 \cup L_2$ have the form*

$$\mathcal{C}(x, y_2 - x, z_2 - x) = \{x, y_2 - x, z_2 - x, y_2, z_2, y_2 + z_2 - 2x, y_2 + z_2 - x\}, x \in L_1, y_2, z_2 \in L_2 \quad (4)$$

The conjectured best construction for a 3-cube free subset of $\mathbb{Z}_{2^n}$ was formulated by Long and Wagner to be $L_1 \cup L_3$ [12]. The proof that $L_1 \cup L_3$ is cube-free can be done succinctly using the previous axioms.

Theorem 2.2. *$L_1 \cup L_3$ is 3-cube-free in $\mathbb{Z}_{2^n}$ for all $n \in \mathbb{N}$.*

Proof. Fix an arbitrary $n \in \mathbb{N}$. If $L_1 \cup L_3$ were to have a cube $\mathcal{C}(x, y, z) \subset L_1 \cup L_3$, its generators would need to be in $L_1 \cup L_3$. Without loss of generality, let $x \preceq y \preceq z$ in the layer ordering. We cannot have

y be in L_3, since that would imply that $z \in L_3$ and $y + z \succ z$ ($y + z$ belongs to a higher layer than L_3), showing that $\mathcal{C}(x, y, z) \not\subset L_1 \cup L_3$. We also cannot have z be in L_3 with $x, y \in L_1$. Since $x + y \succ x$ and the cube is a subset of $L_1 \cup L_3$, $x + y \in L_3$, but that would mean that $x + y + z = (x + y) + z \succ z$, showing that the cube is once again not in $L_1 \cup L_3$. If all the generators are in L_1 and the cube is in $L_1 \cup L_3$, then $x + y \in L_3$ and $y + z \in L_3$. Therefore, $z - y = (y + z) - 2y \in L_2$. However, this implies that $x + z = (x + y) + (z - y) \in L_2$, which means this cube isn't in $L_1 \cup L_3$. Since we have exhausted all possible choices for generators of a cube in $L_1 \cup L_3$, there are no cubes in $L_1 \cup L_3$. □

3 Conditions on 3-cube free subsets

In this section, I will begin deriving fundamental conditions on the structure of a 3-cube-free set. Moreover, I will establish inequalities on the "fullness" of each layer in a 3-cube-free set.

3.1 Triple-free subsets of $\mathbb{Z}_{2^n}$

Some fundamental conditions can be derived for all 3-cube free subsets based off of the following observations:

- $\mathcal{C}(0, 0, 0) = \{0\}$, so no 3-cube free subset of $\mathbb{Z}_{2^n}$ can contain 0 for all values of $n \in \mathbb{N}$.
- Let $a \in \mathbb{Z}_{2^n}$ for some $n \in \mathbb{N}$. Define the *triple generated by* a to be the set $\{a, 2a, 3a\}$. Since $\{a, 2a, 3a\} = \mathcal{C}(a, a, a)$, no triples can be in a 3-cube free subset.

We work to expand these conditions in the coming section. A naïve yet informative approach to this problem to start is to find the largest triple-free subset of $\mathbb{Z}_{2^n}$ for any $n \in \mathbb{N}$. Only having to check for triples would make computer searches more efficient and proofs more convenient, but this approach can only get us so far.

Remark 3.1. *A set being free of triples is almost never enough of a sufficient condition to satisfy a set being free of* 3*-cubes. For instance, in* $\mathbb{Z}_{32}$*, the set* $L_1 \cup L_3 \cup L_5$ *has no triples (all elements in the set don't have its double in the set) yet it contains the* 3*-cube* $\mathcal{C}(3, 4, 9)$.

From this point onward, we will use the word "cube-free" to mean 3-cube-free, with any other dimension cube being specified beforehand if the dimension is not three. Looking at only triples gives us a powerful theorem that we can use to investigate the size of a cube-free set when partitioned by layers.

Theorem 3.1. *Let* $n \in \mathbb{N}$*. For any cube-free (or even just triple-free) set* $S \subset \mathbb{Z}_{2^n}$ *and any* $k \in \mathbb{N}$ *such that* $k \leq n - 1$,

$$|S \cap L_k| + |S \cap L_{k+1}| \leq 2^{n-k} \tag{5}$$

Proof. Fix $n \in \mathbb{N}$ and let $S \subset \mathbb{Z}_{2^n}$. Hoping to reach a contradiction, assume that S is cube-free. For an arbitrary $k \in \mathbb{N}$ such that $k \leq n-1$, consider the following covering of $L_k \cup L_{k+1}$:

$$\{\mathcal{T}_x : x \in L_k\} \tag{6}$$

where $\mathcal{T}_x$ is the triple generated by x, $\{x, 2x, 3x\}$. For any $y \in L_k$ and $z \in L_{k+1}$,

$$\sum_{x \in L_k} |\{y\} \cap \mathcal{T}_x| = 2 \tag{7}$$

$$\sum_{x \in L_k} |\{z\} \cap \mathcal{T}_x| = 2 \tag{8}$$

since $z \in \mathcal{T}_{z/2}$ and $z \in \mathcal{T}_{z/2+2^{n-1}}$, while $y \in \mathcal{T}_y$ and $y \in \mathcal{T}_{3^{-1}y}$. Assuming $|L_k \cap S| + |L_{k+1} \cap S| > 2^{n-k}$,

$$2\,|L_k \cap S| + 2\,|L_{k+1} \cap S| = \sum_{x \in S} \sum_{y \in L_k} |\{x\} \cap \mathcal{T}_y| > 2 \cdot 2^{n-k} \tag{9}$$

However, there are 2^{n-k} subsets with 3 elements each in our covering. Therefore, by Pigeonhole Principle, $\mathcal{T}_x \subset S$ for some $x \in L_k$, so S is not triple-free and thus not cube-free. □

This theorem demonstrates how to most effectively look at the structure of a cube-free set: by bounding the sums of the sizes of layers when intersected by the set. Hopefully, viewing our problem as an optimization problem in n variables (n layers) as opposed to 2^n variables. Looking at an entire cube-free set and looking to find subsets to cover it often results in cumbersome calculations that don't reveal the required structure of these cube-free sets. These individual layer inequalities demonstrate the exact relationship between layers in a cube-free set.

Theorem 3.1 is enough to verify the size of the largest possible triple-free subset of $\mathbb{Z}_{2^n}$ for any $n \in \mathbb{N}$.

Corollary 3.1. *Let $n \in \mathbb{N}$. The largest size of a triple-free subset of $\mathbb{Z}_{2^n}$ has size $\sum_{1 \leq k \leq (n+1)/2} 2^{n-2k+1}$, with one such set of largest size being*

$$\bigcup_{1 \leq k \leq (n+1)/2} L_{2k-1} \tag{10}$$

Proof. To prove the first statement, fix $n \in \mathbb{N}$ and let $S \subset \mathbb{Z}_{2^n}$ be cube-free. If n is even,

$$\begin{aligned} |S| = \sum_{k=1}^{n} |S \cap L_k| &= \sum_{k=1}^{n/2} \left(|L_{2k-1} \cap S| + |L_{2k} \cap S|\right) \\ &\leq \sum_{k=1}^{n/2} 2^{n-2k+1} = \frac{2}{3}\left(2^n - 1\right) \end{aligned} \tag{11}$$

If n is odd,

$$\begin{aligned} |S| = \sum_{k=1}^{n} |S \cap L_k| &= \sum_{k=1}^{(n-1)/2} \left(|L_{2k-1} \cap S| + |L_{2k} \cap S|\right) + |L_n \cap S| \\ &\leq 1 + \sum_{k=1}^{(n-1)/2} 2^{n-2k+1} = \frac{1}{3}\left(2^{n+1} - 1\right) \end{aligned} \tag{12}$$

The set $R = \bigcup_{1 \leq k \leq (n+1)/2} L_{2k-1}$ is free of triples since for all elements $x \in R$, $2x \notin R$. $\square$

A way to view this construction is given a value of n, list all binary digits less than 2^n that end with an even amount of zeros. Since doubling an element that ends with an even amount of zeros in binary would make the element end in an odd amount of zeros, all elements don't contain their double.

This theorem is also enough to show that if we wish to beat the conjectured largest 3-cube free subset of $\mathbb{Z}_{2^n}$, we need to include elements from at least three layers.

Theorem 3.2. *Let $n \in \mathbb{N}$ ($n \geq 5$) and let S be a subset of $\mathbb{Z}^*_{2^n}$ such that $|S| > \frac{5}{8} \cdot 2^n$. If S is 3-cube free, $|S \cap L_k| \neq 0$ for some $k \geq 5$.*

Proof. Fix $n \in \mathbb{N}$ and let S be a subset of $\mathbb{Z}^*_{2^n}$. Assume that S is 3-cube free. Therefore, it does not contain any triples. Thus, by Theorem 3.1, $\sum_{j=1}^{4} |S \cap L_j| \leq \frac{5}{8} \cdot 2^n$. Since $|S| = \sum_{j=1}^{n} |S \cap L_j| > \frac{5}{8} \cdot 2^n$, $|S \cap L_j| > 0$ for some $j \geq 5$ and $L_j \cap S \neq \varnothing$ for that value of j. $\square$

Remark 3.2. *Note that for $n = 1, 2, 3, 4$, the size of the largest triple-free set is exactly $\frac{5}{8} \cdot 2^n$. Therefore, the largest cube-free subset of $\mathbb{Z}_{2^n}$ for $n = 1, 2, 3, 4$ has size $\frac{5}{8} \cdot 2^n$.*

Remark 3.3. *Taking the size of the largest possible triple-free subsets of $\mathbb{Z}_{2^n}$ as a function of n gives a function asymptotically approaching $\frac{2}{3} \cdot 2^n$.*

Lastly, we can use this sum of adjacent layers inequality to bound how many elements can be in the first three layers of a cube-free set.

Theorem 3.3. *Let $n \in \mathbb{N}$ ($n \geq 3$) and let $S \subset \mathbb{Z}_{2^n}$ be cube-free with $|S| > \frac{5}{8} \cdot 2^n$. Then,*

$$\frac{13}{24} \cdot 2^n < |S \cap L_1| + |S \cap L_2| + |S \cap L_3| \leq \frac{5}{8} \cdot 2^n \tag{13}$$

Proof. Fix $n \in \mathbb{N}$ and let $S \subset \mathbb{Z}_{2^n}$ be 3-cube free. The upper bound can easily be verified since $|S \cap L_1| + |S \cap L_2| \leq \frac{1}{2} \cdot 2^n$ and $|S \cap L_3| \leq \frac{1}{8} \cdot 2^n$. The lower bound can be computed by splitting n into two cases based on its parity. If n is odd,

$$\begin{aligned} |S \cap L_1| + |S \cap L_2| + |S \cap L_3| &= |S| - \sum_{k=2}^{(n-1)/2} (|S \cap L_{2k}| + |S \cap L_{2k+1}|) \\ &> \frac{5}{8} \cdot 2^n - \sum_{k=2}^{(n-1)/2} 2^{n-2k} \\ &= \frac{5}{8} \cdot 2^n - \frac{1}{12} \cdot 2^n + \frac{2}{3} > \frac{13}{24} \cdot 2^n \end{aligned} \tag{14}$$

On the other hand, if n is even,

$$\begin{aligned} |S \cap L_1| + |S \cap L_2| + |S \cap L_3| &= |S| - |S \cap L_n| - \sum_{k=2}^{\frac{n}{2}-1} (|L_{2k} \cap S| + |L_{2k+1} \cap S|) \\ &> \frac{5}{8} \cdot 2^n - 1 - \frac{1}{12} \cdot 2^n + \frac{4}{3} \\ &> \frac{13}{24} \cdot 2^n \end{aligned} \tag{15}$$

□

3.2 Expanding our approach for any cube

Previously, we restricted a set from having only $\{x, 2x, 3x\}$ for any $x \in \mathbb{Z}_{2^n}$. This restriction lowers our bound on the size of a cube-free set to about $\frac{2}{3}|\mathbb{Z}_{2^n}|$. However, the size of this set is still quite a distance away from $\frac{5}{8} \cdot 2^n$. We must look at other types of cubes to get closer to the desired optimal construction.

The first new type of cube we will consider is one that goes through 3 layers. Initially, trying to use the same Pigeonhole Principle argument that I used before gave weaker results than the triple-free restrictions formulated in Section 3.1. However, this bound can be strengthened by fixing an upper-layer element in a cube-free set, which we must have if the size is larger than $\frac{5}{8} \cdot 2^n$ by Theorem 3.2.

Theorem 3.4. *Let $n \in \mathbb{N}$ and let $S \subset \mathbb{Z}_{2^n}$ be 3-cube free. Let $l \in \mathbb{N}$ such that $L_l \cap S \neq \varnothing$. Then, for all j, k such that $j < k < l$,*

$$4 \cdot \frac{|S \cap L_j|}{2^{n-j}} + 2 \cdot \frac{|S \cap L_k|}{2^{n-k}} \leq 5 \tag{16}$$

Proof. Fix $n \in \mathbb{N}$ and let $S \subset \mathbb{Z}_{2^n}$ be cubefree. Suppose there exists $l \in \mathbb{N}$ such that $L_l \cap S \neq \varnothing$ and let $j, k \in \mathbb{N}$ be distinct such that $j < k < l$. Using an element $z \in L_l$, this proof is by a careful choice of covering subsets of $L_j \cup L_k \cup \{z\}$. Fixing an element $z \in L_l \cap S$, consider the set of subsets

$$\mathcal{A} = \{\{x_j, x_k, z, x_j + x_k, x_j + z, x_k + z, x_j + x_k + z\} \,:\, x_j \in L_j, x_k \in L_k\} \tag{17}$$

One can verify for each element of the subsets that each element of L_j appears $4 \cdot 2^{n-k}$ times, each element of L_k appears $2 \cdot 2^{n-j}$ times, and z is included in each subset. If none of the subsets are full, by Pigeonhole Principle,

$$4 \cdot 2^{n-k}|S \cap L_j| + 2 \cdot 2^{n-j}|S \cap L_k| \leq 5 \cdot 2^{2n-k-j} \tag{18}$$

However, each of the subsets in $\mathcal{A}$ are precisely $\mathcal{C}(x_j, x_k, z)$. Thus, since S is cube-free, none of the subsets can be full. Our desired results follows by dividing both sides of (18) by 2^{2n-k-j}. □

This new inequality gives us another condition on cube-free sets if the size of the set is larger than $\frac{5}{8} \cdot 2^n$. The conjectured largest cube-free set has no elements in L_2, so it is worth asking if a set larger than $\frac{5}{8} \cdot 2^n$ must contain an element in L_2. The answer to this question is *yes.*

Corollary 3.2. *Let $n \in \mathbb{N}$ ($n \geq 5$) and let $S \subset \mathbb{Z}_{2^n}$ be cube-free. Then, $|S| > \frac{5}{8} \cdot 2^n$ implies that $S \cap L_2 \neq \varnothing$.*

Proof. Fix an arbitrary $n \in \mathbb{N}$ and let $S \subset \mathbb{Z}_{2^n}$ be cube-free. We will proceed by proving its contrapositive. Assume $S \cap L_2 = \varnothing$ and denote $\mu = \max\{k \in \mathbb{N} \,:\, S \cap L_k \neq \varnothing\}$ (the value of the largest non-empty layer). Considering $\mu \leq 5$ (by Theorem 3.2), it follows from the results of Theorems 3.1 and 3.4 along with the fact that $|S \cap L_1| \leq \frac{1}{2} \cdot 2^n$ that

$$
\begin{aligned}
|S| = \sum_{k=1}^{\mu} |S \cap L_k| &= |S \cap L_1| + \sum_{k=3}^{\mu-2} |S \cap L_k| + |S \cap L_{\mu-1}| + |S \cap L_\mu| \\
&\leq |S \cap L_1| + \sum_{k=3}^{\mu-2} \left(\frac{5}{2} \cdot 2^{n-k} - \frac{4}{2^k} |S \cap L_1| \right) + 2^{n-\mu+1} \\
&= |S \cap L_1| + \left(\frac{5}{2} \cdot 2^n - 4 |S \cap L_1| \right) \left(\frac{1}{4} - \frac{4}{2^\mu} \right) + 2 \cdot 2^{n-\mu} \\
&= \frac{5}{8} \cdot 2^n + \frac{8}{2^\mu} \cdot (2 |S \cap L_1| - 2^n) \leq \frac{5}{8} \cdot 2^n
\end{aligned} \tag{19}
$$

□

Now, we know more about the layer distribution of a hypothetical cube-free set of size larger than $\frac{5}{8} \cdot 2^n$: at least one element must be in L_2 and at least one element must be in L_5 or above. This is tied together in our next theorem regarding the structure of a cube-free set beating the $\frac{5}{8} \cdot 2^n$ bound.

Theorem 3.5. *Let S be a 3-cube free subset of $\mathbb{Z}_{2^n}$. If $|S| > \frac{5}{8} \cdot 2^n$, $|S \cap L_1| + |S \cap L_3| \leq \frac{1}{2} \cdot 2^n$.*

Proof. Fix $n \in \mathbb{N}$ and let $S \subset \mathbb{Z}_{2^n}^*$ be 3-cube free with $|S| > \frac{5}{8} \cdot 2^n$. This proof is by a careful choice of elements in a covering of $L_1 \cup L_3$. Since $|S| > \frac{5}{8} \cdot 2^n$, we can choose an element $z \in S \cap (L_5 \cup L_6 \cup \cdots \cup L_n)$ (Corollary 3.2) and a $y_2 \in S \cap L_2$ (Corollary 3.2). This proof will be done in the cases of $y_2 \equiv 2 \mod 8$ and $y_2 \equiv 6 \mod 8$: the former case will be proven below with similar logic following for the latter case. Assuming that $y_2 \equiv 2 \mod 8$, consider the covering of $L_1 \cup \{y_2\} \cup L_3 \cup \{z\}$ as follows:

$$
\mathcal{A} = \left\{ \mathcal{C} \left(\frac{1}{2} y_2 + 2 - 4l, \frac{1}{2} y_2 - 2 + 4l, z - \frac{1}{2} y_2 - 2 + 4l \right) \ : \ l \in 1, 2, \ldots, 2^{n-2} \right\} \tag{20}
$$

By expanding out each of the subsets in $\mathcal{A}$, each subset contains y_2 and z, and each element in L_3 appears in exactly two subsets. Since $y_2 \equiv 2 \mod 8$, $y_2/2 \equiv 1 \mod 4$, so all elements that are $3 \mod 4$ appear in exactly 3 subsets while all elements that are $1 \mod 4$ appear in exactly 1 subset. Considering S is cube-free, none of these subsets can be full. Therefore, Pigeonhole Principle tells us that S must satisfy

$$
|S \cap (8\mathbb{Z} + 2)| + 3|S \cap (8\mathbb{Z} + 6)| + 2|S \cap L_3| \leq 2^n \tag{21}
$$

Next, note that if $S \cap L_3 = \varnothing$, $|S \cap (8\mathbb{Z} + 6)| + 3|S \cap (8\mathbb{Z} + 2)| + 2|S \cap L_3| \leq 2^n$. Otherwise, fix an arbitrary $z_3 \in L_3$ and consider the covering of $L_1 \cup \{y_2\} \cup L_3$ by

$$
\mathcal{B} = \left\{ \mathcal{C} \left(\frac{y_2}{2} - 4l, \frac{y_2}{2} + 4l, z_3 - \frac{y_2}{2} + 4l \right) : l = 1, 2, \ldots, 2^{n-2} \right\} \tag{22}
$$

By expanding out each of the subsets in $\mathcal{B}$, each subset contains y_2 and z_3, and each element in L_3 (except z_3) appears in exactly two subsets. Since $y_2 \equiv 2 \mod 8$, $y_2/2 \equiv 1 \mod 4$, so all elements that are $1 \mod 4$ appear in exactly 3 subsets while all elements that are $3 \mod 4$ appear in exactly 1 subset. Considering S is cube-free, none of these subsets can be full. Therefore, Pigeonhole Principle tells us that S must satisfy

$$|S \cap (8\mathbb{Z}+2)| + 3|S \cap (8\mathbb{Z}+6)| + 2|S \cap L_3| \leq 2^n \tag{23}$$

Adding equations (21) and (23) and dividing the expression by 4 gives $|S \cap L_1| + |S \cap L_3| \leq \frac{1}{2} \cdot 2^n$. $\square$

The final inequality that we shall form can be created by connecting cubes in one ring to cubes in another. For instance, consider the sets $\{1, 3, 8, 4, 9, 11, 12\}$ in $\mathbb{Z}_{16}$ and $\{2, 6, 16, 8, 18, 22, 24\}$ in $\mathbb{Z}_{32}$. Both of these sets are cubes in their respective rings, but the second cube is a multiple of the previous cube. Moreover, the first cube is in $L_1 \cup L_3 \cup L_4$ of $\mathbb{Z}_{16}$ while the second cube is in $L_2 \cup L_4 \cup L_5$. If we can think of all cubes in one set to be cubes in another set scaled by a power of two, the bound on the size of one cube-free set is connected to the bound on the size of a cube-free set in another ring. This idea can be formalized in the following theorem.

Theorem 3.6. *Let $n \in \mathbb{N}$ and $N \in \mathbb{N}$ such that $|S| \leq N$ for all cube-free subsets of $\mathbb{Z}_{2^n}$. Then, for all $k \in \mathbb{N}$ and all cube-free subsets $S \subset \mathbb{Z}_{2^{n+k}}$,*

$$\sum_{j=1}^{n} |S \cap L_{k+j}| \leq N \tag{24}$$

Proof. Fix $n \in \mathbb{N}$ and let $k \in \mathbb{N}$. We proceed by proving the contrapositive. Suppose that for an $N \in \mathbb{N}$, there exists a cube-free subset $S \subset \mathbb{Z}_{2^{n+k}}$ such that $\sum_{j=1}^{n} |S \cap L_{k+j}| > N$. Consider the mapping φ defined by

$$\begin{aligned} \varphi : \mathbb{Z}_{2^n} &\longrightarrow \{0\} \cup \bigcup_{j=1}^{n} L_{k+j}^{(k+n)} \\ \varphi(x) &= 2^k x \mod 2^{n+k} \end{aligned} \tag{25}$$

(the superscripts on the layers are to clarify that they are the layers of $\mathbb{Z}_{2^{n+k}}$). φ is a bijection and moreover holds the property that for all $x, y \in \mathbb{Z}_{2^n}$, $\varphi(x+y) = \varphi(x) + \varphi(y)$ and $\varphi(xy) = \varphi(x)\varphi(y)$ (a ring isomorphism). φ being a ring isomorphism implies that φ^{-1} is a ring isomorphism as well. Defining $\tilde{S} = S \cap \left(\bigcup_{j=1}^{n} L_{k+j}\right)$, we propose that $\varphi^{-1}(\tilde{S})$ is cube-free in $\mathbb{Z}_{2^n}$. Letting $a, b, c \in \mathbb{Z}_{2^n}$ be arbitrary, $\mathcal{C}(\varphi(a), \varphi(b), \varphi(c)) \not\subset \tilde{S}$ since $\tilde{S} \subset S$, which is cube-free. However, this implies that

Assumptions	**Inequality**	**Description**
$1 \leq j \leq n-1$	$\lvert S \cap L_j\rvert + \lvert S \cap L_{j+1}\rvert \leq 2^{n-j}$	No triples
$1 \leq j < k < l \leq n$, $S \cap L_l \neq \varnothing$	$\lvert S \cap L_j\rvert + 2^{k-j-1}\lvert S \cap L_k\rvert \leq \frac{5}{4} \cdot 2^{n-j}$	–
The largest cube-free subset of $\mathbb{Z}_{2^{n-k}}$ has size N	$\sum_{j=1}^{n-k} \lvert S \cap L_{k+j}\rvert \leq N$	–

Table 1: Useful layer "fullness" inequalities for any cube-free set $S \subset \mathbb{Z}_{2^n}$.

$\varphi^{-1}(\mathcal{C}(\varphi(a), \varphi(b), \varphi(c)) = \mathcal{C}(a,b,c) \not\subset \varphi^{-1}(\tilde{S})$. a, b, c are arbitrary elements of $\mathbb{Z}_{2^n}$, so $\varphi^{-1}(\tilde{S})$ is cube-free in $\mathbb{Z}_{2^n}$. It follows from the fact that φ is a bijection that $|\varphi^{-1}(\tilde{S})| = |\tilde{S}| > N$, so our proof by contrapositive is complete.

□

The result from Theorem 3.6 allows us to "inductively" construct assumptions about the size of cube-free subsets of sets for larger values of n. For instance, if we know that the largest cube-free subset of $\mathbb{Z}_{2^n}$ has size $\frac{5}{8} \cdot 2^n$, then any cube-free subset $S \subset \mathbb{Z}_{2^{n+1}}$ with size larger than $\frac{5}{8} \cdot 2^{n+1}$ must satisfy the condition

$$|S \cap L_1| = |S| - \sum_{j=2}^{n+1} |S \cap L_j| > \frac{5}{4} \cdot 2^n - \frac{5}{8} \cdot 2^n = \frac{5}{16} \cdot 2^{n+1} = \frac{5}{8}|L_1| \tag{26}$$

with the layers corresponding to the set $\mathbb{Z}_{2^{n+1}}$.

4 A graph theory and counting approach

In this section, I discuss a possible approach using graph theory, specifically graph theory, that could be useful in proving layer size inequalities.

The previous sections have shown that we can construct an extensive amount of cubes with four elements from one layer, two elements from one higher layer, and one element from an even higher layer. Consider the cube $\{x, y, z, x+y, x+z, y+z, x+y+z\}$ for $x, y, z \in \mathbb{Z}_{2^n}^*$ where $x \prec y \prec z$. If S is cube-free and $\{x, z, x+y, x+z, x+y+z\} \subset S$, this means that either y or $y+z$ cannot be included in S. We can connect this idea to a concept in graph theory using the following term:

Definition. Let $G = (V, E)$ be a graph. A subset of the vertex set $S \subset V(G)$ is an **independent set** if $v \not\sim w$ for all distinct $v, w \in S$. A set $S' \subset V(G)$ is **maximally independent** if there is no independent set in G with cardinality larger than S'.

Remark 4.1. *For a fixed number of vertices, the size of a maximal independent set decreases as the amount of edges in a graph increases. A loopless graph on n vertices always has an independent set of size 1 (whose size can't always be increased, take K_n) and has an independent set of size n if and only if G is the empty graph on n vertices (there are no edges at all).*

Since the size of an independent set decreases as the amount of edges in a graph increases, we expect there to be a bound on the size of an independent set as a function of edges. This can be done as follows using a counting argument:

Theorem 4.1. *Let G be a graph with n vertices and $e(G)$ edges. The size of an independent set in G is bounded by $\frac{1}{2}\left(1+\sqrt{1-8e(G)-4n+4n^2}\right)$.*

Proof. Fix G to be an arbitrary graph on n vertices. Supposing there exists an independent set I, we can consider the amount of edges incident to I and I^{c}. The edges in G can only be incident to

- one vertex in I and one vertex in I^{c} **OR**
- two vertices in I^{c}

Therefore, the size of the edge set is at most $|I|(n-|I|)+\binom{n-|I|}{2}$. Expanding out this expression and multiplying by -2 gives

$$0 \geq |I|^2 - |I| - \left(n^2 - n - 2e(G)\right) \tag{27}$$

However, we can use the quadratic formula to factor the right side to get

$$\left(|I| - \frac{1}{2}\left(1+\sqrt{1+4n^2-4n-8e(G)}\right)\right)\left(|I| - \frac{1}{2}\left(1-\sqrt{1+4n^2-4n-8e(G)}\right)\right) \leq 0 \tag{28}$$

This forces one factor to be positive and one to be negative. It follows that since the second term must be positive, $|I| \leq \frac{1}{2}\left(1+\sqrt{1+4n^2-4n-8e(G)}\right)$. □

The use of this theorem is that it could be used to rule out elements in a cube-free set. For instance, consider the cube $\mathcal{C}(1,2,16) = \{1,2,16,3,17,18,19\}$ in $\mathbb{Z}_{32}$. If we are given that for a cube-free set S, $\{1,2,3,17,16\} \subset S$, either $2 \notin S$ or $18 \notin S$. Therefore, we could view $\{2,18\}$ as an edge in a graph with vertex set L_2. This corresponds to an independent set of the graph on vertex set L_2 with edge set $\{\{2,18\}\}$. The bound on the independent set can be calculated using the amount of edges. Counting the amount of edges in this graph to use in Theorem 4.1 could be computed using the following counting technique.

Given an $n \in \mathbb{N}$ and a set $S \subset \mathbb{Z}_{2^n}$, introduce a characteristic vector associated with S. The characteristic vector $\vec{x} \in \{0,1\}^{2^n}$ associated with S is defined to be

$$x_i = \begin{cases} 1, & i \in S \\ 0, & i \notin S \end{cases} \tag{29}$$

We can count occurrences of sum sets using the characteristic vector and summations, with the arithmetic in the variable index being done modulo 2^n. The cardinality of S can be found by computing $\sum_{j=0}^{2^n-1} x_j$, but the amount of occurrences for other sum-sets can be calculated in a similar way. For instance, suppose that $|S \cap L_1| + 2|S \cap L_2| > \frac{1}{2} \cdot 2^n$. Then, either $|S \cap (4\mathbb{Z}+1)| + |S \cap L_2| > \frac{1}{4} \cdot 2^n$ or $|S \cap (4\mathbb{Z}+3)| + |S \cap L_2| > \frac{1}{4} \cdot 2^n$. In the latter case, we can create a lower bound on $|\{a, b \in S \;:\; a+b \in S\}|$ by computing

$$\begin{aligned}
&\sum_{a \in L_1} \sum_{b \in L_2} x_a x_b x_{b+a} \\
&= \sum_{a \in L_1} x_a \sum_{b \in L_2} x_b x_{b+a} \\
&= \sum_{a \in 4\mathbb{Z}+1} x_a \sum_{b \in L_2} x_b x_{b+a} + \sum_{a \in 4\mathbb{Z}+3} x_a \sum_{b \in L_2} x_b x_{b+a} \\
&\geq \sum_{a \in 4\mathbb{Z}+1} x_a \sum_{b \in L_2} x_b x_{b+a} \geq \sum_{a \in 4\mathbb{Z}+1} x_a \left(|S \cap (4\mathbb{Z}+3)| + |S \cap L_2| - \frac{1}{4} \cdot 2^n \right) \\
&= |S \cap (4\mathbb{Z}+1)| \left(|S \cap (4\mathbb{Z}+3)| + |S \cap L_2| - \frac{1}{4} \cdot 2^n \right)
\end{aligned} \tag{30}$$

Bounding the total $\sum_{b \in L_2} x_b x_{b+a}$ in line three can be done by fixing an arbitrary $\tilde{a} \in 4\mathbb{Z}+1$. This sum is analogous to the minimum number of sets that are full in the collection $\{\{b, b+\tilde{a}\} \;:\; b \in L_2\}$. Each element in L_2 and $4\mathbb{Z}+3$ appears once in the covering sets, so $|S \cap (4\mathbb{Z}+3)| + |S \cap L_2| > \frac{1}{4} \cdot 2^n$ implies that there are at least $|S \cap (4\mathbb{Z}+3)| + |S \cap L_2| - \frac{1}{4} \cdot 2^n$ full subsets. This process can be refined to give better bounds for whatever sum-set is desired. The problem with the strategy listed above can be seen in an attempt to use this in practice.

We can split the sets in (4) into L_1 and L_2 elements. When given a set $S \in \mathbb{Z}_{2^n}$ that's cube-free and $|S \cap L_1| > \frac{1}{4} \cdot 2^n$, we can count how many subsets have all its L_1 elements in S and how many have all its L_2 elements in S. To count how many subsets have all its L_2 elements in S, we can use the polynomial counting technique to get exactly

$$
\begin{aligned}
&\sum_{a\in L_1}\sum_{b\in L_2}\sum_{c\in L_2} x_b x_c x_{b+c-2a} \\
=&\sum_{b\in L_2} x_b \sum_{c\in L_2} x_c \sum_{a\in L_1} x_{b+c-2a} \\
=& 2\,|S\cap L_2| \sum_{b\in L_2} x_b \sum_{c\in L_2} x_c = 2\,|S\cap L_3|^3
\end{aligned}
\tag{31}
$$

To count how many subsets have all its L_1 elements in S, we can use the polynomial counting technique to get

$$
\begin{aligned}
&\sum_{a\in L_1}\sum_{b\in L_2}\sum_{c\in L_2} x_a x_{b-a} x_{c-a} x_{b+c-a} \\
=&\sum_{a\in L_1} x_a \sum_{b\in L_2} x_{b-a} \sum_{c\in L_2} x_{c-a} x_{b+c-a}
\end{aligned}
\tag{32}
$$

Similar to the previous example, the summation $\sum_{c\in L_2} x_{c-a}x_{b+c-a}$ is analogous to the scenario of given fixed, arbitrary $a \in L_1$ and $b \in L_2$ and finding the minimum number of full subsets in $\{\{c-a, b+c-a\} : c \in L_2\}$. There are $\frac{1}{4}\cdot 2^n$ subsets in this collection, with each element in $4\mathbb{Z}+1$ appearing in one subset and each element in $4\mathbb{Z}+3$ appearing in one subset. Therefore, minimum number of full subsets is $|S\cap L_1| - \frac{1}{4}\cdot 2^n$. Using this lower bound, we get the amount of subsets that have all their L_1 elements in S is at least

$$
\begin{aligned}
&\geq \left(|S\cap L_1| - \frac{1}{4}\cdot 2^n\right) \sum_{a\in L_1} x_a \sum_{b\in L_2} x_{b-a} \\
&= \left(|S\cap L_1| - \frac{1}{4}\cdot 2^n\right) \left(\sum_{a\in 4\mathbb{Z}+1} x_a \sum_{b\in L_2} x_{b-a} + \sum_{a\in 4\mathbb{Z}+3} x_a \sum_{b\in L_2} x_{b-a}\right) \\
&= 2|S\cap(4\mathbb{Z}+1)||S\cap(4\mathbb{Z}+3)| \left(|S\cap L_1| - \frac{1}{4}\cdot 2^n\right)
\end{aligned}
\tag{33}
$$

If the amount of subsets that have all of their L_1 elements in S and the amount of subsets that have all of their L_2 elements in S total to more than the total amount of subsets, one of the subsets in the collection must be full (which yields a cube). Therefore, a cube-free set S such that $|S\cap L_1| > \frac{1}{4}\cdot 2^n$ must satisfy

$$
2|S\cap L_1|^3 + 2|S\cap(4\mathbb{Z}+1)||S\cap(4\mathbb{Z}+3)| \left(|S\cap L_1| - \frac{1}{4}\cdot 2^n\right) \leq \frac{1}{32}\cdot 2^{3n} \tag{34}
$$

Unfortunately, the problem with this result is a cubic equation which involves both the values 1 mod 4 and 3 mod 4, which is quite nasty to handle. This approach could be refined to give simpler, tighter results, but this approach as shown doesn't seem to get as nice results as I would've hoped to get.

5 Approaches to finding cube-free subsets

In this section, I layout a linear programming model along with a SAT solver model to use in finding cube-free subsets. Additionally, I discuss what isomorph-free generation aims to do and how I tried to apply it to the cube-free set problem.

Combinatorial problems such as the set covering problem [3] and graph matching problems [6] have formulations as linear programs. This fact, along with the increasing speed of LP solvers such as Gurobi, makes one consider whether our "largest cube-free set" problem can be posed as a linear program. Our problem can be posed as an linear program as follows:

Approach 1. Given $n \in \mathbb{N}$ and the ring $\mathbb{Z}_{2^n}$, denote $N = 2^n$. Defining the variables $x_0, x_1, \ldots, x_{N-1}$, an integer linear program can be constructed with the objective

$$\text{maximize} \sum_{j=0}^{N-1} x_j \tag{35}$$

subject to the constraints

$$x_0 = 0 \tag{36}$$

$$x_j \in \{0,1\} \, (\forall\, j = 1, \ldots, N-1) \tag{37}$$

$$x_j + x_k + x_l + x_{j+k} + x_{j+l} + x_{k+l} + x_{j+k+l} \leq 6 \; (\forall\, j,k,l = 1, \ldots, N-1, j \leq k \leq l) \tag{38}$$

with the arithmetic in the subscript for equation 38 done modulo N. A 3-cube free subset(s) of largest size in $\mathbb{Z}_{2^n}$ can be recovered by taking $\vec{x} \in \texttt{argmax}(x_1 + \ldots + x_{N+1})$ and constructing the set $\{j \in \mathbb{Z}_N \,:\, x_j = 1\}$.

It may seem problematic to apply linear programming techniques to this problem, considering the listed variables are binary variables and classic linear programming techniques (including Dantzig's simplex algorithm [18]) give an optimal result only over the real numbers. However, Gurobi can relax the integer constraints to be real numbers and apply techniques such as the "Branch and Bound" technique [11] and cutting planes [5] to prune unfeasible integer solutions and find an optimal integral solution.

The result of this approach is an output showing the most non-zero elements in a 3-cube free subset of $\mathbb{Z}_{2^n}$, with the `argmax` of the algorithm displaying the membership of the largest 3-cube-free subsets S, with $x_j = 1$ if $j \in S$ and $x_j = 0$ otherwise. This is exactly why we force $x_0 = 0$, since 0 is never in any cube-free subset of $\mathbb{Z}_{2^n}$. The code used to implement this algorithm in Python using Gurobi is listed in the section "Code implementations". Gurobi takes this model (along with other constraints you may give it, such as the minimum size of a specific layer) and gives results in $n = 6$ in just over a minute.

Our goal of finding a cube-free subset of $\mathbb{Z}_{2^n}$ beating $\frac{5}{8} \cdot 2^n$ can also be done by solving the associated Boolean satisfiability problem as stated below:

Approach 2. Given $n \in \mathbb{N}$ with $N = 2^n$ and Boolean variables $\{x_j\}_{j=0}^{N-1}$, generate a configuration of variables that satisfy the clauses

$$\neg x_0 \tag{39}$$

$$\neg(x_a \wedge x_b \wedge x_c \wedge x_{a+b} \wedge x_{a+c} \wedge x_{b+c} \wedge x_{a+c} \wedge x_{a+b+c}),\ (\forall a, b, c = 1, \ldots, N-1, a \leq b \leq c) \tag{40}$$

where the operations in the subscript are done modulo N. Once a configuration of Booleans that satisfy the aforementioned conditions is generated (denote that set $\{\tilde{x}_j\}_{j=0}^{N-1}$), the set $\{j \in \mathbb{Z}_{2^n} : \tilde{x}_j = \texttt{TRUE}\}$ is 3-cube-free. The largest subsets constructed from this method are the largest 3-cube-free subsets of $\mathbb{Z}_{2^n}$.

Similar to the LP model, $x_j = 1$ when j is in the set S and 0 otherwise. The model begins with $x_0 = \texttt{FALSE}$ since a cube-free set never has 0 while the second line states that no projective cube can contain all elements. One can establish a requirement of at least k true Boolean variables in an efficient manner by using Boolean counter variables [2] if they wish to bypass smaller cube-free sets. The goal is to define $s_{i,j}$ for $0 \leq i \leq N$ and $0 \leq j \leq k$ such that

$$s_{i,j} = \begin{cases} \texttt{TRUE}, \text{at least } j \text{ of } x_1, \ldots, x_i \text{ are } \texttt{TRUE} \\ \texttt{FALSE}, \text{otherwise} \end{cases} \tag{41}$$

This can be done by setting $s_{0,j}$ to be false for $1 \leq j \leq k$, $s_{i,0}$ to be true for $0 \leq i \leq N$ (both follow from our previous definition) and by adding the clauses

$$s_{i,j} \Leftrightarrow (s_{i-1,j} \vee (x_i \wedge s_{i-1,j-1})) \quad \text{for } 1 \leq i \leq N \text{ and } 1 \leq j \leq k \tag{42}$$

5.1 The automorphism group of cube-free sets

This section contains the use of terminology from group theory, specifically group actions on a set. The most important term used is the *orbit* of an element under a group element.

Definition. Let X be a set and let G be a group acting on X. The *orbit* of a subset $S \subset X$ under the group G, denoted $\mathrm{orb}_G(S)$, is the set $\mathrm{orb}_G(S) := \{gs : g \in G, s \in S\}$.

We use orbits to discuss the automorphisms of the cube-free subsets in $\mathbb{Z}_{2^n}$, denoted $\mathcal{C}_n$. The automorphisms of $\mathcal{C}_n$ are defined as follows:

Definition. Fix $n \in \mathbb{N}$. A function $\varphi : S_{2^n} \to S_{2^n}$ is an *automorphism of cube-free sets* if for all $S \subset \mathbb{Z}_{2^n}$, there exists a subset $S' \subset \mathbb{Z}_{2^n}$ such that $\varphi(\mathcal{C}(S)) = \mathcal{C}(\varphi(S'))$.

We begin with a set of transformations that preserve the quality of being cube-free.

Theorem 5.1. *Let $\phi_k^{(n)} : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ denote the scaling map $\phi_k^{(n)}(x) = kx$ for $n, k \in \mathbb{N}$. Then, for any n in $\mathbb{N}$ and $k \equiv 1 \mod 2$, (i) $\phi_k^{(n)}$ is a bijective function and (ii) for any cube-free subset of S, $\phi_k^{(n)}(S)$ is cube-free with $|S| = |\phi_k^{(n)}(S)|$.*

Proof. Fix $n \in \mathbb{N}$ and $k \equiv 1 \mod 2$. Since $\phi_k^{(n)}$ is a linear transformation, we can show that $\ker(\phi_k) = \{0\}$ (we omit the superscript in ϕ when the value of n is unambiguous). $\phi_k(0) = 0$, so $0 \in \ker(\phi_k)$. On the other hand, if $x \in \ker(\phi_k)$, $kx = 0$. Since k and 2^n are coprime, k^{-1} exists in $\mathbb{Z}_{2^n}$. Thus, $x = 0$, showing that $\ker(\phi_k) = \{0\}$. Since ϕ_k is a map between finite sets that is injective, ϕ_k is a bijection.

Fix $n \in \mathbb{N}$, $k \equiv 1 \mod 2$, and $S \subset \mathbb{Z}_{2^n}$ such that S is cube-free. Therefore, for all $a, b, c \in S$, $\mathcal{C}(a, b, c) \not\subset S$. Now, let $a, b, c \in \mathbb{Z}_{2^n}$ be arbitrary elements. Since ϕ is a bijection and therefore invertible, $\phi_k^{-1}(a), \phi_k^{-1}(b), \phi_k^{-1}(c) \in \mathbb{Z}_{2^n}$. It follows that $\mathcal{C}(\phi_k^{-1}(a), \phi_k^{-1}(b), \phi_k^{-1}(c)) \not\subset S$, so $\mathcal{C}(a, b, c) \not\subset \phi_k(S)$. Considering a, b, c are arbitrary elements of $\mathbb{Z}_{2^n}$, we have shown that $\phi_k(S)$ is cube-free. The last statement can be observed by noting that since ϕ_k is a bijection, $|S| = |\phi_k(S)|$. □

The motive of Theorem 5.1 is to show that there exist *automorphisms* of cube-free subsets of $\mathbb{Z}_{2^n}$. Given a fixed $n \in \mathbb{N}$, the automorphisms $\{\phi_k : k \text{ odd}, 1 \leq k \leq 2^n\}$ form an abelian group of size 2^{n-1}. Therefore, the orbit of each subset of $[\mathbb{Z}_{2^n}^*]$ has size at most 2^{n-1}. These automorphisms allow us to restrict values in cube-free subsets in certain cases by the following theorem.

Theorem 5.2. *Let $n \in \mathbb{N}$ and let $S \subset \mathbb{Z}_{2^n}^*$ be a 3-cube free set such that $|S| \geq 2^{n-1}$. Then, there exists $k \in \{1, \ldots, n-1\}$ such that $1 \in \phi_k(S)$.*

Proof. Let $S \subset \mathbb{Z}_{2^n}^*$ be cube-free and let $|S| \geq 2^{n-1}$. If $1 \in S$, we are done. So, assume $1 \notin S$. Since $|S| \geq 2^{n-1}$ and there are $2^{n-1} - 1$ elements not equal to 0 that are even, there exists $y \in S$ such that $y \equiv 1 \bmod 2$. Since $y \equiv 1 \bmod 2$, y^{-1} exists in $\mathbb{Z}_{2^n}$ and $y^{-1} \equiv 1 \bmod 2$. It follows that $\phi_{y^{-1}}(S)$ contains $\phi_{y^{-1}}(y) = 1$. □

This automorphism of 3-cube free subsets of a fixed cardinality allows us to more quickly construct 3-cube free subsets.

Corollary 5.1. *Let $k \geq 2^{n-1}$. If all subsets $S \subset \mathbb{Z}_{2^n}$ of size k with $1 \in S$ has a 3-cube, there are no 3-cube free subsets of $\mathbb{Z}_{2^n}$ with size k.*

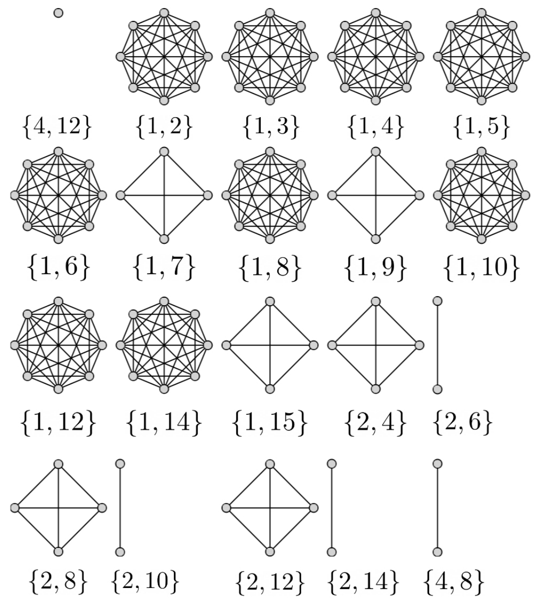

Figure 2: A graph with vertex set consisting of size-2 subsets of $\mathbb{Z}_{16}^*$ with vertices a and b being adjacent if $a = \phi_k(b)$ for some $k \equiv 1 \mod 2$. Listed below each connected component is a vertex from that component. Any two components that are connected are either both cube-free or not cube-free, so we only have to check one vertex from each component (Graphs generated by Maple 2021 [13]).

We have already established that for any cube-free subset S of $\mathbb{Z}_{2^n}$ (denote the set of cube-free subsets of $\mathbb{Z}_{2^n}$ by $\mathcal{C}_n$), $\phi_k(S)$ is cube-free as well for any odd k between 1 and 2^n. This begs the question–what is the smallest subset of $A \subset [\mathbb{Z}_{2^n}^*]$ such $\text{orb}_{\text{Aut}(\mathcal{C}_n)}(A) = [\mathbb{Z}_{2^n}^*]$? If two subsets belong to the same orbit in the automorphism group, they are both cube-free or both have a cube. Therefore, we only have to check one element from each orbit of the automorphism group. This strategy is called *orderly generation* [4]. The trick to this approach is to choose one element from each equivalence class under $\text{Aut}(\mathcal{C}_n)$ (this certainly does not give a *unique* set of smallest size).

Consider a smaller case when orderly generation shows its power. For $\mathbb{Z}_{16}^*$, consider the subsets of $\mathbb{Z}_{16}^*$ that have cardinality 2. Checking each of these individual sets by computer would require checking $\binom{15}{2} = 105$ subsets. However, we can divide these subsets into equivalence classes by our previously defined automorphisms. Visually, we can think of these equivalence classes as connected components in a graph with the vertex set being size-2 subsets of $\mathbb{Z}_{2^n}$ and an edge being between two vertices if they are equivalent under an automorphism. Since all elements in each equivalence class are either cube-free or not cube-free, we can check one element from each class. Given that there are 20 equivalence classes, we only have to check 20 subsets instead of 105. See Figure 2 for a visual representation of these equivalence classes and one element from each equivalence class.

We can cull duplicate subsets of $\mathbb{Z}_{2^n}$ (sets that are equivalent under the automorphism group) using the construction in $\mathbb{Z}_{2^n}$ defined by

$$\mathcal{B}_n^{(1)} := \bigcup_{j=1}^{n} \left\{ S \subset \bigcup_{k=j}^{n} L_k \;:\; 2^{j-1} \in S \right\} \tag{43}$$

We can argue that any subset of $\mathbb{Z}_{2^n}^*$ is isomorphic to some element of $\mathcal{B}_n^{(1)}$. Given any arbitrary subset $S \in \mathbb{Z}_{2^n}^*$, it must have a lowest non-empty layer, so we denote it $\alpha = \min\{m \in \mathbb{N} : S \cap L_m \neq \varnothing\}$. Taking an arbitrary element $x \in S \cap L_m$, since 2^{m-1} divides x and $\gcd(x, 2^n) = 2^{m-1}$, there exists an $a \in \{1, 3, \ldots, 2^n - 1\}$ such that $ax \equiv 2^{m-1} \mod 2^n$. Thus, $\phi_a(S)$ contains $ax = 2^{m-1}$, showing that S is isomorphic to a set in $\mathcal{B}_n^{(1)}$. Note that the collection of sets in the union of (43) are disjoint and

$$\begin{aligned} \left| \left\{ S \subset \bigcup_{k=j}^{n} L_k : 2^{j-1} \in S \right\} \right| &= 2^{\left(2^n - \sum_{k=1}^{j-1} 2^{n-k}\right) - 2} \\ &= 2^{2^{n-j+1} - 2} \end{aligned} \tag{44}$$

Therefore, the size of $|\mathcal{B}_n^{(1)}|$ is the sum of (44) from $j = 1$ to n. The benefit of defining the set listed in Equation 43 is that the search space is diminished by about half compared to the original search space of $[\mathbb{Z}_{2^n}^*] \setminus \{0\}$. Table 2 demonstrates this decrease in search space. A more limited set could be constructed from which any element of $[\mathbb{Z}_{2^n}^*] \setminus \{0\}$ is isomorphic to some element in that set, but this leads to one of the first problems that I thought of with this approach.

Theorem 5.3. *Let $n \in \mathbb{N}$. The number of equivalence classes of $[\mathbb{Z}_{2^n}^*]$ under the automorphism group $\{\phi_k : 1 \leq k \leq 2^n, k \equiv 1 \mod 2\}$ is at least $2|[\mathbb{Z}_{2^n}^*]|/2^n = 2^{2^n - n}$.*

Proof. Fix an arbitrary $n \in \mathbb{N}$. Letting $\Phi = \{\phi_k : 1 \leq k \leq 2^n, k \equiv 1 \mod 2\}$, we can form an equivalence relation on $[\mathbb{Z}_{2^n}^*]$ with $A \sim B$ if $A = \varphi(B)$ for some $\varphi \in \Phi$. These equivalence classes all have size of at most $\frac{1}{2} \cdot 2^n$, since there are $\frac{1}{2} \cdot 2^n$ choices of automorphisms. Therefore, the amount of equivalence classes is at least $|[\mathbb{Z}_{2^n}^*]|/2^{n-1} = 2^{2^n - n}$. □

There are two issues with the approach of using orderly generation for finding cube-free sets. The first problem is that narrowing the size of the set down to something lower than $|\mathcal{B}_n^{(1)}|$ is quite challenging. What is the most logical way to eliminate more and more "copies" of an element under the automorphism group? The sets $\{1, 5\}$ and $\{1, 13\}$ are both elements of $\mathcal{B}_4^{(1)}$ yet $\phi_{13}(\{1, 5\}) = \{1, 13\}$, so our set still contains isomorphic copies of the same set. Moreover, there may not be an explicit formula to generate all non-isomorphic elements of $[\mathbb{Z}_{2^n}^*]$. In that case, it may be more fruitful to investigate isomorph-free exhaustive generation algorithms [10] [14].

Even a unique element could be chosen from each equivalence class for any $n \in \mathbb{N}$, it seems like these sets would be hard to implement into Gurobi in a way that would make solving more efficient. Gurobi sees these extra conditions on sets that are non-isomorphic as more constraints on the system, which would

n	$\lvert[\mathbb{Z}_{2^n}^*]\rvert$ (a)	$\left\lvert\mathcal{B}_n^{(1)}\right\rvert$ (b)	$\lceil 2^{2^n-n}\rceil$ (c)	(b)/(a)	(c)/(a)
4	32768	16453	4096	0.5021	0.1250
5	2.15×10^9	1.07×10^9	1.34×10^8	0.5000	0.0625
6	9.22×10^{18}	4.61×10^{18}	2.88×10^{17}	0.5000	0.0313
7	1.70×10^{38}	8.51×10^{37}	2.66×10^{36}	0.5000	0.0156

Table 2: The size of the total search space of non-empty subsets of $[\mathbb{Z}_{2^n}^*]$ in comparison to the size of the refined set $\mathcal{B}_n^{(1)}$ and the smallest theoretical bound on distinct (non-isomorphic) elements of $[\mathbb{Z}_{2^n}^*]$, calculated for for a few values of n.

probably end up slowing down Gurobi anyway. Finally, even if this set of canonical elements could be coded into Gurobi efficiently, the reduction on the amount of sets being searched over is at most $1/2^{n-1}$ times fewer than an exhaustive search over all subsets. This improvement in efficiency may be helpful when n gets large enough, but the amount of subsets being searched over is already incredibly large, so solutions still may not get generated in a timely manner despite our optimization strategy.

6 Further work

In the end, our inequalities show that the triple-free construction $\bigcup_{1\le j\le n/2} L_{2j-1}$ is not cube-free. It would seem that these inequalities would get us closer and closer to an upper bound of $\frac{5}{8}\cdot 2^n$ for a cube-free set. However, these inequalities end up moving the distribution of elements in each layer in such a way that no layer is completely full (except perhaps the higher layers). There is still hope that the goal of treating this problem as a n-variable optimization problem instead of a 2^n-variable optimization problem is a viable strategy, however.

There is one conjecture which would lead to proving that $\frac{5}{8}\cdot 2^n$ is the largest possible size of 3-cube-free subset of $\mathbb{Z}_{2^n}$.

Conjecture 6.1. Let $n \in \mathbb{N}$ be arbitrary and let S be 3-cube-free. If $|S \cap L_1| > \frac{5}{8}|L_1| = \frac{5}{16}\cdot 2^n$, then $|S \cap L_1| + 2|S \cap L_2| \le \frac{1}{2}\cdot 2^n$.

This conjecture shows that if the size of $S \cap L_1$ is large enough, the addition of elements in L_2 to S drastically decreases the amount of elements in L_1. Note that this conjecture isn't necessarily true if $|S \cap L_1| \le \frac{5}{16}\cdot 2^n$.

Remark 6.1. *We propose that the set $K = (4\mathbb{Z}+1) \cup L_2$ is cube-free for any $n \in \mathbb{N}$ $(n \ge 2)$. A cube must interpolate at least two layers, so a cube in K would have to be in $L_1 \cup L_2$. Any cube in $L_1 \cup L_2$ must be of the form $\{x, y_2 - x, z_2 - x, y_2, z_2, y_2 + z_2 - 2x, y_2 + z_2 - x\}$ with $x \in L_1$, and $y_2, z_2 \in L_2$ by (4).*

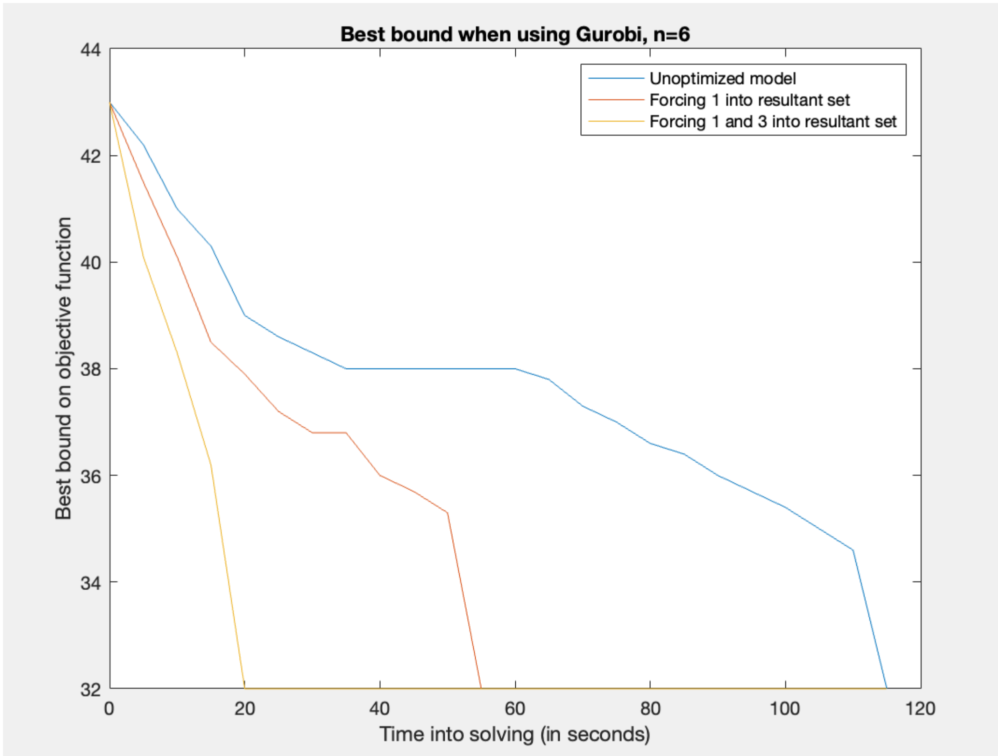

Figure 3: The best bound for the objective function in Conjecture 6.1 over time ($n = 6$), given by Gurobi. Computation time is reduced by about 80% by forcing 1 and 3 into the optimal set as opposed to the unoptimized model which doesn't force 1 nor 3 into the optimal set.

If K had a cube, one of the generators would need to be $1 \mod 4$, but then $y_2 + z_2 - x \equiv 3 \mod 4$ for all $y_2, z_2 \in L_2$, showing that $\mathcal{C}(x, y_2 - x, z_2 - x) \not\subset K$ for any $x \in K \cap L_1$ and $y_2, z_2 \in L_2$. It follows that K is cube-free, showing that Conjecture 6.1 is not true when $|S \cap L_1| \leq \frac{5}{16} \cdot 2^n$.

Checking this conjecture for values past $n = 6$ can be done in a quicker manner using the automorphism group of cube-free sets. If $S \cap L_1$ must be non-empty, it exists some element $a \in L_1$. However, S would then be isomorphic to $\phi_{a^{-1}}(S)$, which contains 1. Therefore, we can force any subset in the search space to have 1 by enforcing `x[1] == 1` in the Python model. Moreover, if $|S \cap L_1| > \frac{1}{2} \cdot |L_1|$, then $\{a, 3a\}$ is a subset of S for some $a \in L_1$. It follows that S is isomorphic to $\phi_{a^{-1}}(S)$, which contains 1 and 3. Therefore, we can force any subset in the search space to have 1 and 3 by enforcing `x[1] == 1` and `x[3] == 1` in the Python model. Using these tricks makes the computation time much quicker—see Figure 3 to see how drastic this improvement in solve times is for $n = 6$ in Conjecture 6.1.

Approaching the proof of Conjecture 6.1 could be done by looking at equation (4) for the exhaustive list of cubes in $L_1 \cup L_2$. One view of this collection of sets in $L_1 \cup L_2$ is a bipartite hypergraph with vertex classes L_1 and L_2, and theory regarding hypergraphs could be used [1]. Another approach would be to view this problem using more advanced machinery from additive combinatorics such as Fourier analysis [16], but this may be overkill for this sort of conjecture. This conjecture would lead to the desired result of Wagner and Long for the 3-cube:

Theorem 6.1. *Let $n \in \mathbb{N}$ and let $S \subset \mathbb{Z}_{2^n}$ be 3-cube-free. If Conjecture 6.1 is true, then $|S| \leq \frac{5}{8} \cdot 2^n$.*

Proof. This proof is done by strong induction on the value of n. Computer search (using Gurobi) has shown that the largest 3-cube-free subset of $\mathbb{Z}_{2^n}$ has size $\frac{5}{8} \cdot 2^n$ for all $n \leq 7$. Assume that for some $n \in \mathbb{N}$, the largest cube-free subset of $\mathbb{Z}_{2^k}$ has size $\frac{5}{8} \cdot 2^k$ for all $k \leq n$. Letting $S \subset \mathbb{Z}_{2^{k+1}}$ be cube-free, suppose that $|S| > \frac{5}{8} \cdot 2^{k+1}$. By Theorem 3.6, $|S \cap L_1| > |S| - \sum_{j=2}^{k+1} \frac{5}{8} \cdot 2^{k+1} - \frac{5}{8} \cdot 2^k = \frac{5}{16} \cdot 2^{k+1}$, so Conjecture 6.1 would hold. Similarly, $|S \cap L_1| + |S \cap L_2| = |S| - \sum_{j=3}^{k+1} |S \cap L_j| > \frac{5}{8} \cdot 2^{k+1} - \frac{5}{8} \cdot 2^{k-1} = \frac{15}{32} \cdot 2^{k+1}$. However, $|S \cap L_1| + 2|S \cap L_2| \leq \frac{1}{2} \cdot 2^{k+1}$ if Conjecture 6.1 is true, which would force $|S \cap L_2| \leq \frac{1}{32} \cdot 2^{k+1}$. On the other hand, $|S \cap L_1| + |S \cap L_2| + |S \cap L_3| = |S| - \sum_{j=4}^{k+1} |S \cap L_j| > \frac{5}{8} \cdot 2^{k+1} - \frac{5}{8} \cdot 2^{k-2} = \frac{35}{64} \cdot 2^{k+1}$. Thus, by Theorem 3.5, $|S \cap L_2| > \frac{35}{64} \cdot 2^{k+1} - |S \cap L_1| - |S \cap L_3| \geq \frac{3}{64} \cdot 2^{k+1}$. This contradicts our requirement that $|S \cap L_2| \leq \frac{1}{32} \cdot 2^{k+1}$. Thus, $|S| \leq \frac{5}{8} \cdot 2^{k+1}$, so by induction, $\frac{5}{8} \cdot 2^n$ is the size of the largest possible 3-cube-free set in $\mathbb{Z}_{2^n}$ for all $n \in \mathbb{N}$. □

Using this strong induction technique along with the subtraction of upper bounds on the higher layers gives the best possible bounds on the size of the bottom three layers. Specifically, getting $|S \cap L_1| + |S \cap L_2| + |S \cap L_3| > \frac{35}{64} \cdot 2^n$ is better than the $\frac{13}{24} \cdot 2^n$ bound achieved in Theorem 3.3.

The next logical step would be to discover the largest 5-cube free subsets of $\mathbb{Z}_{2^n}$ for any $n \in \mathbb{N}$. We can approach this problem in a similar way we did for 3-cube free subsets by starting with the largest subset free of $\{x, 2x, 3x, 4x, 5x\}$ for all $x \in \mathbb{Z}_{2^n}$. The best construction is listed below.

Theorem 6.2. *Let $n \in \mathbb{N}$. The largest subset of $\mathbb{Z}_{2^n}$ that does not contain $\{x, 2x, 3x, 4x, 5x\}$ for all $x \in \mathbb{Z}_{2^n}$ has size $\frac{6}{7} \cdot 2^n$ and one such without $\{x, 2x, 3x, 4x, 5x\}$ for all $x \in \mathbb{Z}_{2^n}$*

$$C = \bigcup_{\substack{j \leq n \\ 3 \nmid j}} L_j \tag{45}$$

Proof. Let $n \in \mathbb{N}$ be arbitrary and let $S \subset \mathbb{Z}_{2^n}$ such that $\{x, 2x, 3x, 4x, 5x\} \cap S = \varnothing$ for all $x \in \mathbb{Z}_{2^n}$. For any $j \in \mathbb{N}$, consider the covering of $L_j \cup L_{j+1} \cup L_{j+2}$ by

$$\{\mathcal{C}(x, x, x, x, 3x) \,:\, x \in L_j\} \tag{46}$$

These sets are exactly $\{x, 2x, 3x, 4x, 5x, 6x, 7x\}$. Each element of L_j, L_{j+1}, and L_{j+2} appears exactly 4 times. Thus, in order for none of these subsets to be full by Pigeonhole Principle,

$$4|S \cap L_j| + 4|S \cap L_{j+1}| + 4|S \cap L_{j+2}| \leq 6 \cdot 2^{n-j} \tag{47}$$

In the case of n being a multiple of 3, the size of $|S|$ is bounded by

$$\begin{aligned}\sum_{j=1}^{n}|S\cap L_j| &\leq \sum_{k=1}^{n/3}|S\cap L_{3k-2}|+|S\cap L_{3k-1}|+|S\cap L_{3k}| \\ &= \sum_{k=1}^{n/3}\frac{3}{2}\cdot 2^{n-3k+2} \\ &= 6\cdot\sum_{k=1}^{n/3}2^{n-3k} = \frac{6}{7}\left(2^n-1\right)\end{aligned} \tag{48}$$

This process can be done for $n \equiv 1 \mod 3$ and $n \equiv 2 \mod 3$ to show that $|S| \leq \frac{6}{7}\cdot 2^n$.

For any $x \in C$, $x \in L_j$ for some $j \not\equiv 0 \mod 3$. Thus, either $2x$ or $4x$ is in L_k for some $k \equiv 0 \mod 3$. It follows that C doesn't contain $\{x, 2x, 3x, 4x, 5x\}$ for any $x \in \mathbb{Z}_{2^n}$. □

The derived inequalities for 3-cube-free sets may become a bit unwieldy as the dimension of the cube increases, so unless there is a simpler layer inequality that works easily for all dimensions, these layer inequalities may not be helpful when looking for the bound on the largest k-cube-free set.

A Code implementations

A.1 Approach 1 code

```
from gurobipy import *

m = Model(”cube−freeSubset”)

Set power of 2 for characteristic of ring.
n = 7
N = 2**n

Set variables.
x = m.addVars(N, name=”x”, vtype=GRB.BINARY)
m.update()
m.setObjective(quicksum(x), GRB.MAXIMIZE)
m.update()

Add constraints.
m.addConstr(x[0]==0)
for j in range(N):
    for k in range(j,N):
        for l in range(k,N):
            m.addConstr(x[j] + x[k] + x[l] + x[(j+k) % N] + x[(j+l) % N] +
            x[(k+l) % N] + x[(j+k+l) % N] <= 6)
    m.update()
m.optimize()
obj = m.getObjective()
print(obj.getValue())

Create largest cube−free subset.
S = []
for i in range(N):
    if x[i].x > 0.5:
        S.append(i)

Print largest cube−free subset.
print(S)
```

References

[1] Alain Bretto. *Hypergraph theory an introduction.* Springer International Publishing, 2013.

[2] Curtis Bright, Jürgen Gerhard, Ilias Kotsireas, and Vijay Ganesh. Effective problem solving using sat solvers. *Communications in Computer and Information Science*, page 205–219, 2020.

[3] Alberto Caprara, Matteo Fischetti, and Paolo Toth. A heuristic method for the set covering problem. *Operations Research*, 47(5):730–743, 1999.

[4] Charles J. Colbourn and Ronald C. Read. Orderly algorithms for graph generation. *International Journal of Computer Mathematics*, 7(3):167–172, 1979.

[5] Gérard Cornuéjols. Valid inequalities for mixed integer linear programs. *Mathematical Programming*, 112(1):3–44, 2007.

[6] Jack Edmonds and Ellis L. Johnson. Matching: A well-solved class of integer linear programs. *Combinatorial Optimization — Eureka, You Shrink!*, page 27–30, 2003.

[7] P. Erdös. On a lemma of littlewood and offord. *Bulletin of the American Mathematical Society*, 51(12):898–902, 1945.

[8] Gurobi Optimization, LLC. Gurobi optimizer reference manual, 2018.

[9] David Hilbert. Über die irreducibilität ganzer rationaler functionen mit ganzzahligen coefficienten. *Journal für die reine und angewandte Mathematik*, 1892(110):104–129, 1892.

[10] Petteri Kaski and Patric Östergård. *Classification algorithms for codes and designs.* Springer, 2006.

[11] A. H. Land and A. G. Doig. page 497–520. London School of Economics and Political Science, 1960.

[12] Jason Long and Adam Zsolt Wagner. The largest projective cube-free subsets of $\mathbb{Z}_{2^n}$, 2018.

[13] Maplesoft, a division of Waterloo Maple Inc.. Maple.

[14] Brendan D McKay. Isomorph-free exhaustive generation. *Journal of Algorithms*, 26(2):306–324, 1998.

[15] Emanuel Sperner. Ein satz über untermengen einer endlichen menge. *Mathematische Zeitschrift*, 27(1):544–548, 1928.

[16] Terence Tao and Van Vu. *Additive combinatorics.* Cambridge University Press, 2012.

[17] Guido Van Rossum and Fred L. Drake. *Python 3 Reference Manual.* CreateSpace, Scotts Valley, CA, 2009.

[18] Robert J. Vanderbei. *Linear programming—foundations and extensions*, volume 285 of *International Series in Operations Research & Management Science*. Springer, Cham, [2020] ©2020. Fifth edition [of 1433802].

[19] Vijay V. Vazirani. *Approximation algorithms*. Springer, 2001.