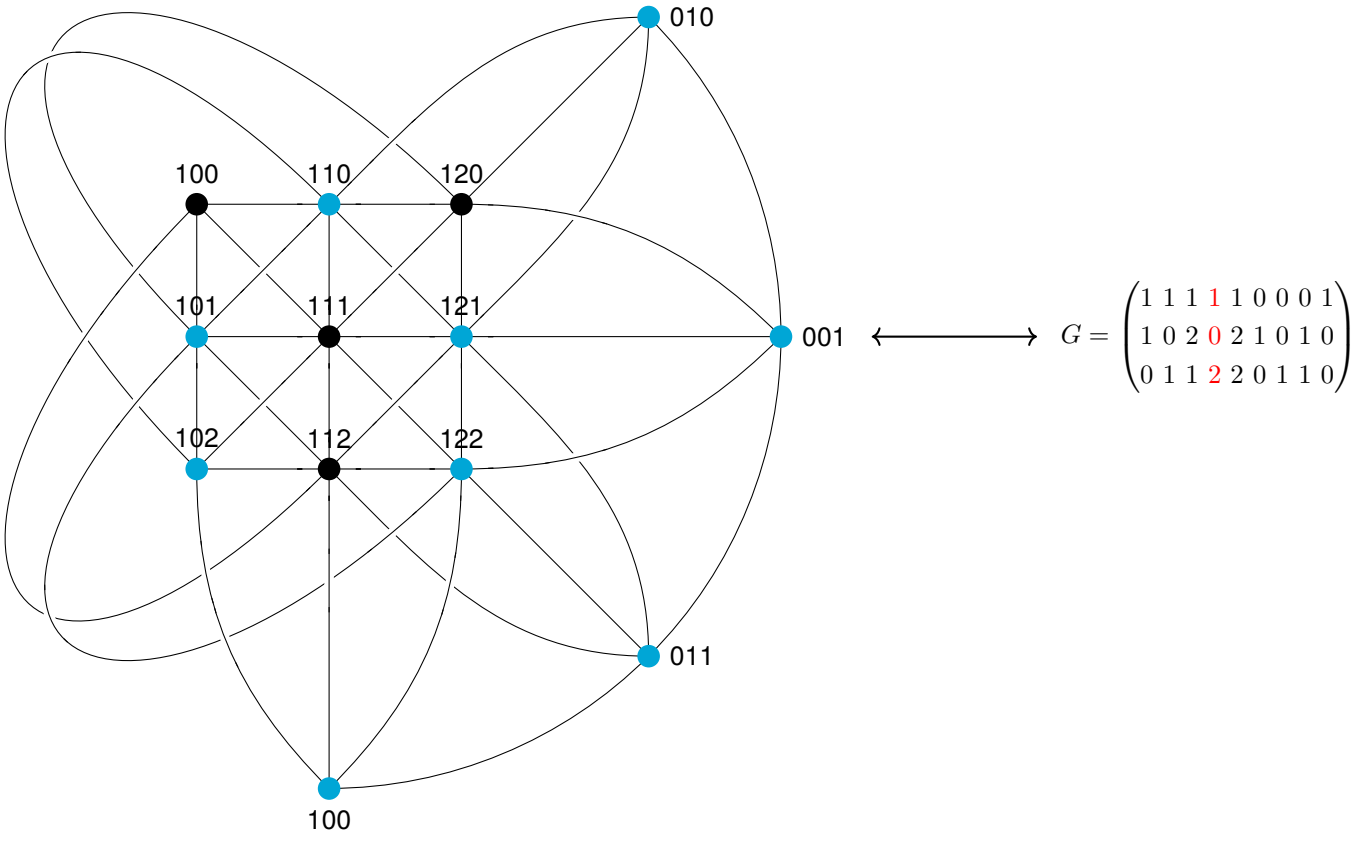
Bounds on Trifferent Codes

Linear trifferent codes, blocking sets and r-bounded trifferent codes

N.N. (Naivedya) Amarnani

Department of Applied Mathematics

Delft University of Technology



TU Delft

Bounds on Trifferent Codes

Linear trifferent codes, blocking sets and r-bounded trifferent codes

by

Naivedya Amarnani

to obtain the degree of Master of Science
at the Delft University of Technology,
to be defended publicly on Wednesday June 24, 2026 at 10:00 AM.

Student number:	6223125	
Institution:	Delft University of Technology	
Faculty:	Electric Engineering, Mathematics, and Computer Science	
Project duration:	December 1, 2025 – June 24, 2026	
Thesis committee:	Prof. Dr. D.C. Gijswijt,	TU Delft, Chair
	Dr. A. Bishnoi,	TU Delft, Daily Supervisor
	Dr. R. Versendaal,	TU Delft

An electronic version of this thesis is available at `http://repository.tudelft.nl/`.

TU Delft

Abstract

A trifferent code of length n is a subset of $\{0,1,2\}^n$ such that for any three distinct elements in it, there is a coordinate in which they all differ pairwise. The quantity $T(n)$ denotes the largest size of such a code of length n. A motivation to study this problem comes from an application in information theory, where $T(n)$ is related to the zero-error capacity of the (3/2)-channel, defined by Elias in 1988 [Eli88]. This problem has seen renewed interest due to recently established connections between linear trifferent codes, strong blocking sets in projective geometry and minimal codes in coding theory.

In this thesis, we examine the most recent breakthrough in the upper bound of $T(n)$ by Bhandari and Khetan [BK25], coming from r-bounded trifferent codes, which are trifferent codes with each codeword having exactly r many 2s. The quantity $T_b(n,r)$ denotes the largest size of r-bounded trifferent codes of length n.

We generalize previous results by Bhandari and Khetan to give the upper bound $T_b(n,r) \leq c \times n^{r-2/5}$ for all $r \geq 3$. We also build upon ideas given by Bishnoi and Kovács and prove the lower bound $T_b(n,r) \geq n^{\lceil r/2 \rceil - o(1)}$ for all $r \geq 3$ using special existing hypergraph constructions. In order to improve the lower bound for the quantity $T_b(n,2)$, we use a SAT solver to compute small-sized 2-bounded trifferent codes. With the help of these computations, we come up with two new constructions for 2-bounded trifferent codes which improve the prevailing (trivially obtained) lower bound of $T_b(n,2) \geq 2n-2$ to $T_b(n,2) \geq 2n$ (from Construction 1, in joint work with Jozefien D'haeseleer) and an even better bound of $T_b(n,2) \geq (20/9)n - O(1)$ (from Construction 2).

Acknowledgement

This thesis would not have been possible without the constant guidance and support of many individuals. It is because of them that my time as a Master's student at TU Delft has been both personally and academically so enriching.

I am very thankful to my supervisor, Professor Anurag Bishnoi, for his unwavering support and willingness to offer help, even arranging meetings at short notices to accommodate my questions. I appreciate him taking out time from his holidays to meet with me online and allay many of my concerns regarding the thesis. I am thankful to both him as well as Professor Dion Gijswijt for providing me with invaluable constructive feedback on my writing to ensure my thesis is both rigorous and accessible. I would also like to thank Professor Rik Versendaal for agreeing to be part of my thesis committee.

As this thesis marks the conclusion of my time as a student at TU Delft, I consider myself extremely fortunate to fondly look back at the friendships and memories I made during this period. I am very grateful to my friends for making this journey so fulfilling and also to my family, for their continued support and words of encouragement.

Naivedya Amarnani
Delft, June 2026

Notation

Symbol/Notation	Description
Σ	Finite alphabet $\{0, 1, \ldots, q-1\}$
$\mathbb{F}_q$	Finite field of q elements for a prime power q
$T(n)$	Largest size of a trifferent code of block length n
$T_L(n)$	Largest size of a linear trifferent code of block length n
$T_b(n, r)$	Largest size of an r-bounded trifferent code of block length n
PG$(k-1, q)$	The projective space of dimension $k-1$ derived from the finite vector space $\mathbb{F}_q^k$
$b_q(k, s)$	The smallest size of an (affine) s-blocking set in $\mathbb{F}_q^k$
$b_q^*(k, t)$	The smallest size of a strong t-blocking set in PG$(k-1, q)$
$\begin{bmatrix} k \\ s \end{bmatrix}_q$	*Gaussian/q-binomial coefficient*: $\begin{bmatrix} k \\ s \end{bmatrix}_q = \frac{(q^k-1)(q^{k-1}-1)\cdots(q^{k-s+1}-1)}{(q^s-1)(q^{s-1}-1)\cdots(q-1)}$
$q/(q-1)$ channel	An information channel with the same input and output alphabet Σ, which is guaranteed to output a symbol other than the input symbol
cap(q)	*q-capacity*: cap$(q) = \limsup_{n\to\infty} \frac{1}{n} \log_2 \frac{T(q,n)}{q-1}$, where $T(q, n)$ denotes the maximum size of a $(q-1)$-list-decoding code of block length n for the $q/(q-1)$ channel.
$O(n)$	*Big-O notation*: $f(x) = O(g(x)) \implies \lvert f(x)\rvert \leq c \cdot \lvert g(x)\rvert$ for all $x \geq N$, and some $c, N > 0$
$o(n)$	*Little-o notation*: $f(x) = o(g(x)) \implies \lim_{x\to\infty} \frac{f(x)}{g(x)} \to 0$
$\mathbf{0}$	Zero element of relevant group, field or vector space
$\oplus$	*Direct sum*: For two linear subspaces S, T of a vector space V, $S \oplus T := \{s + t \in V \mid s \in S, t \in T\}$
$\langle S \rangle$	*Linear span*: For a subset S of a vector space V over field $\mathbb{F}$, $\langle S\rangle := \sum_{s_i \in S} \alpha_i s_i$ for all $(\alpha_1, \ldots, \alpha_{\lvert S\rvert}) \in \mathbb{F}^{\lvert S\rvert}$
$\alpha(G)$	*Independence number*: The largest size of an independent set in graph G
K_n	The complete graph on n vertices
$K_{s,t}$	The complete bipartite graph with parts of size s and t
ex(n, H)	*Extremal number*: The maximum number of edges in a graph on n vertices which does not contain the graph H as a subgraph
$z(u, v; s, t)$	*Zarankiewicz number*: The maximum number of edges in a bipartite graph with parts of size u, v which does not contain a copy of $K_{s,t}$
$f_r(n, v, e)$	The maximum number of edges in an r-uniform hypergraph which does not contain any set of e hyperedges spanned by v vertices
$\mathbb{P}, \mathbb{E}, \mathbb{I}$	Probability, Expectation, Indicator/Characteristic function
$r_3(N)$	The maximum size of a subset of $\{1, 2, \ldots, N\}$ which does not contain three distinct elements in an arithmetic progression
$r_3(\mathbb{F})$	The maximum size of a subset of a field $\mathbb{F}$ which does not contain three distinct elements in an arithmetic progression
$[n, k]_q/[n, k, d]_q$ code	A linear code over alphabet $\mathbb{F}_q$ with length n and dimension k (and if known, minimum Hamming distance d).
$A \cup B$	*Disjoint union*: The union of two sets A and B when $A \cap B = \emptyset$.

Contents

1

Introduction

Consider a simple question - When are two binary strings said to be different? The answer is precisely when they differ in at least one coordinate. For example, the strings (also called codewords) 1001 and 0000 are different because they differ in the first and fourth coordinates. Since these are binary strings, it is equivalent to say that two strings differ if there exists at least one coordinate in which one of them is 0 and the other is 1.

Analogously, three ternary strings (i.e. strings consisting of 0s, 1s and 2s) are said to be 'trifferent' if there exists at least one coordinate in which one of them is 0, one is 1 and the other one is 2. As an example, the three strings 01012, 20222 and 10200 are 'trifferent' because they contain all three symbols - 0,1,2 - in the first (and also fourth) coordinate. A collection of strings such that any three of them are trifferent, is called a 'trifferent code'.

The main question that arises next, which is also the one this thesis aims to shed more light on, is how large can a trifferent code of a fixed length[1] be.

While this puzzle is interesting by itself, there is also mathematical motivation to study this problem. The notion of 'trifferent codes' is linked to a more general notion of *q-perfect hash codes* (for $q = 3$, they are basically trifferent codes). Such codes appear in the study of families of perfect hash functions, a fundamental problem in computer science, as well as in information theory, to study the zero-error capacity of some discrete channels with list decoding. This information theoretic connection (further elaborated in Chapter 2) also gives some bounds on the sizes of such codes. Interestingly, there has been significant improvement on these bounds for the case $q > 4$, while the case $q = 3$ has seen relatively less progress. This further makes it interesting to look at trifferent codes and attempt to improve the existing bounds.

Definition 1.1. Let $\Sigma = \{0, 1, \ldots, q-1\}$ be a finite alphabet and $n, q \geq 2$ be positive integers. A code $\mathcal{C} \subseteq \Sigma^n$ is a *q-perfect hash code* of block length n if for any q distinct codewords $x_1, x_2, \ldots, x_q \in \mathcal{C}$, there exists a coordinate $i \in [n]$ for which the set of symbols $\{x_j(i) \mid 1 \leq j \leq q\} = \Sigma$, where $x(i)$ denotes the i^{th} coordinate[2] of the codeword x. When $q = 3$, a q-perfect hash code is known as a *trifferent code*.

Example 1.1. The following famous code, known as the tetra-code in coding theory, is a trifferent code of block length 4 and size 9. As a check, consider the codewords $2220, 0121, 1022$ - they are trifferent in the second coordinate as highlighted below.

0	0	0	0
1	1	1	0
2	2	2	0
0	1	2	1
1	2	0	1
2	0	1	1
0	2	1	2
1	0	2	2
2	1	0	2

[1] Here, length refers to the number of symbols in each string within the code.

[2] In the thesis, we always use the notation $x(i)$ to denote the i^{th} coordinate of a vector or codeword x.

Let $T(n)$ denote the maximum size of a trifferent code with block length n. The following recursive relation is quite immediate.

Proposition 1.1. *For $n \geq 2$, we have*

$$T(n) \leq \left\lfloor \frac{3}{2} \cdot T(n-1) \right\rfloor \tag{1.1}$$

Proof. Suppose $\mathcal{C}$ is a trifferent code of block length n and size $T(n)$. Let $a \in \{0, 1, 2\}$ be a symbol which occurs the least in the first coordinate of the codewords in $\mathcal{C}$. Then consider the subcode $\mathcal{C}' \subseteq \mathcal{C}$ which has all the codewords of $\mathcal{C}$ with the first coordinate any symbol other than a. By a simple application of the pigeonhole principle, we must have $\mathcal{C}' \geq (2/3)|\mathcal{C}|$. Let $\mathcal{C}''$ be the code of length $n-1$ obtained from $\mathcal{C}'$ by removing the first coordinate of each codeword in $\mathcal{C}'$. Clearly $|\mathcal{C}''| = |\mathcal{C}'| \geq (2/3) \cdot |\mathcal{C}|$. Note that any three codewords in $\mathcal{C}''$ were trifferent in the original code $\mathcal{C}$ in a coordinate other than the first since none of them had the symbol a appearing there and so, they continue to be trifferent in $\mathcal{C}''$. Hence $\mathcal{C}''$ is a trifferent code of length $n-1$, which must mean that $\mathcal{C}'' \leq T(n-1)$. Combining the two inequalities gives $T(n) \leq (3/2) \cdot T(n-1)$. Since $T(n)$ is an integer, the inequality can be made tighter by the floor function. □

Let us see what the value of $T(n)$ is for some small n. We first have $T(2) \geq 4$, achieved by the trifferent code $\{00, 11, 20, 12\}$. By noting that $T(1) = 3$ trivially, (1.1) also gives $T(2) \leq 4$ and hence $T(2) = 4$.

Similarly, the trifferent codes $\{012, 021, 102, 120, 201, 210\}$ and the tetra-code in Example 1.1 prove that $T(3) \geq 6$ and $T(4) \geq 9$ respectively. Again, repeated use of (1.1) gives the upper bounds $T(3) \leq 6$ and $T(4) \leq 9$ and hence these are also the exact values of $T(n)$ for $n = 3, 4$. The values $T(5) = 10$ and $T(6) = 13$ were only established in 2022 [DFGP22] while the values $T(7) = 16$, $T(8) = 20$ and $T(9) = 27$ were established by Kurz in 2024 [Kur24]. These are the only known exact values for $T(n)$ so far.

Determining and estimating the asymptotic growth of $T(n)$ is known as the *trifference problem*. In a seminal work, Elias showed that $T(n) \leq 2 \times (3/2)^n$ via purely information-theoretic arguments [Eli88]. A recursive use of the 'pruning argument' of Proposition 1.1 also gives the same bound, elaborated later in chapter 2. In the same year, Körner and Marton [KM88] gave the lower bound $T(n) \geq (9/5)^{n/4}$. Subsequent improvements made to the upper bound in [DFGP22] and [Kur24] were able to improve the constant 2 upto 0.6937 for $n \geq 10$ by using the newly established values of $T(n)$ for $n \leq 9$ and equation (1.1) recursively. It was only in 2025 that Bhandari and Khetan [BK25] gave the first polynomial improvement to this bound, showing that $T(n) \leq c \times n^{-2/5} \times (3/2)^n$.

In this thesis, we examine recent bounds on the size of largest trifferent codes in an attempt to improve upon them. We also look at r-bounded trifferent codes and provide both, some new constructions leading to improved lower bounds, and some better upper bounds on their largest sizes.

The thesis is structured as followed. In chapter 2, we provide a small background on relevant information theory concepts and explain how it relates to the theory of trifferent codes. From this relation, we also explain how Elias' theorem [Eli88] in information theory provides the first significant bound on the largest size of a trifferent code.

In chapter 3, we discuss recent improvements in the upper bounds of $T(n)$ given by Bhandari and Khetan [BK25]. We also generalize their theorem bounding the largest size of 2 and 3-bounded trifferent codes to r-bounded trifferent codes and thus show that the new bound they obtained for $T(n)$ is the best that can be obtained by a direct generalization of their proof for larger r. We also formally prove some lower bounds for the quantity $T_b(n, r)$ based on ideas given by Bishnoi and Kovács.

In chapter 4, we introduce the notion of linear trifferent codes and prove their equivalence with strong blocking sets in projective geometry and also with minimal codes. We also provide some background for both these combinatorial objects to provide a more complete picture of this equivalence.

In chapter 5, we discuss the computational approach which we took to attempt improving the lower bound of the largest size of 2-bounded trifferent codes. In lieu of these new computational results that we obtain and also in joint work with Jozefien D'haeseleer, we are able to provide two new constructions of 2-bounded trifferent codes in chapter 6, both of which improve the current lower bound for $T_b(n, 2)$. These computations and new constructions constitute our main contribution in the thesis. We wrap up the report by stating the main conclusions of the thesis and outlining the scope of further research in chapter 7.

2

Link to Information Theory

We first give a brief introduction of the relevant concepts in information theory.

The $q/(q-1)$ channel is a communication channel where the input and output alphabet is the same list of q characters, $\mathcal{X} = \{0, 1, \ldots, q-1\}$; and when an input symbol i is passed through the channel, the output symbol can be anything except i itself.

For the $q/(q-1)$ channel, it is not possible to determine the input message without error if the code has at least two codewords. In fact, no matter how large the block length of the message is, for every set of up to $(q-1)$ input codewords, one can (adversarially) construct an output word that is compatible with all of them (since at each coordinate, the $(q-1)$ input codewords may only cover at most $(q-1)$ symbols out of the q-sized alphabet).

Example 2.1. Consider the $4/3$ channel. If the symbol 2 was sent via this channel, the possible list of outcome symbols is $\{0, 1, 3\}$. Now if the input message has $4-1=3$ codewords, each of length 4, say $0122, 2130$ and 3113, then the output word 1201 is compatible with all the three input messages.

However, it is possible to design codes where on receiving an output word from the $q/(q-1)$ channel, one can narrow down the input message to a set of size at most $(q-1)$ - in this case, we say that we can *list-decode* with lists of size $q-1$. Such codes are called $(q-1)$-list-decoding codes for the $q/(q-1)$ channel. It is well-known that a q-perfect hash code $\mathcal{C}$ of block length n is equivalent to a $(q-1)$-list-decoding code for the $q/(q-1)$ channel with length n (refer the introduction of [BR21]). We prove this equivalence for $q = 3$ later in the chapter.

Definition 2.1. A code $\mathcal{C} \subseteq \{0, 1, \ldots, q-1\}^n$ is an 'ℓ-list-decoding code' for the $q/(q-1)$ channel, if for every output word $\tau \in \mathcal{X}^n$, $|\{\sigma \in \mathcal{C} : \text{the input word } \sigma \text{ is compatible with } \tau\}| \leq \ell$. The zero-error list-of-ℓ-rate of $\mathcal{C}$, is given by $\frac{1}{n}\log_2(|\mathcal{C}|/\ell)$ and the list-of-ℓ-capacity of the $q/(q-1)$ channel, denoted by $\mathsf{cap}(q, \ell)$ is the least upper bound on the attainable zero-error list-of-ℓ-rate across all ℓ-list-decoding codes.

Since we are specifically interested in the list-of-$(q-1)$-capacity of the $q/(q-1)$ channel, we use the standard notation $\mathsf{cap}(q)$ (also called q-*capacity*) to denote $\mathsf{cap}(q, q-1)$, which can then be defined as

$$\mathsf{cap}(q) = \limsup_{n\to\infty} \frac{1}{n} \log_2 \frac{T(q,n)}{q-1} \tag{2.1}$$

where $T(q,n)$ denotes the maximum size of a $(q-1)$-list-decoding code of block length n for the $q/(q-1)$ channel.

There has been significant research and improvements made in studying the quantity $\mathsf{cap}(q)$ in the case $q > 3$. We provide a small summary of the results here and refer the reader to the paper of Bhandari and Radhakrishnan [BR21] for a more thorough overview of this topic. In a seminal work, Fredman and Komlós [FK84] established $\mathsf{cap}(q) \leq \exp(-O(q))$. Guruswami and Riazanov [GR22] then demonstrated that the Fredman-Komlós upper bound is not tight for $q \geq 4$ and were able to provide explicit improvements for $q = 5, 6$. For $q = 4$, Dalai et.al. [DGR19] improved the upper bound to $\mathsf{cap}(4) \leq 6/19 \approx 0.3158$, while Körner and Marton [KM88] established a lower bound of $\mathsf{cap}(4) \geq (1/3)\log(32/29) \approx 0.0473$. Further, Xing and Yuan [XY23] were able to extend Körner and Marton's concatenation technique, and as a result, proved improved lower bounds of $\mathsf{cap}(q)$ for $q = 4, 8$, all odd integers greater than 3 and less than 25, and also sufficiently large q not congruent to 2 $(\mathrm{mod}\ 4)$.

However, the progress for the case $q = 3$ has been somewhat slower in comparison. In 1988, Elias [Eli88] proved that[1]

$$\mathsf{log}(q/(q-1)^{q/(q-1)}) \leq \mathsf{cap}(q) \leq \mathsf{log}(q/(q-1)).$$

This implies

$$0.08 \approx \mathsf{log}_2\left(3/2\sqrt{2}\right) \leq \mathsf{cap}(3) \leq \mathsf{log}_2(3/2) \approx 0.58$$

Körner and Marton [KM88] managed to improved the lower bound by code concatenation to

$$0.212 \approx (1/4)\,\mathsf{log}_2(9/5) \leq \mathsf{cap}(3).$$

Both these results gave the first bounds on the quantity $T(n)$ because of the following observation.

Proposition 2.1. *A code $\mathcal{C}$ is trifferent if and only if it is a 2-list decoding code for the $3/2$ channel.*

Proof. Suppose $\mathcal{C}$ is trifferent. Let $\tau \in \{0,1,2\}^n$ be an output word of the $3/2$ channel. Let $S_\tau = \{\sigma \in \mathcal{C} :$ the input word σ is compatible with $\tau\} \subseteq \mathcal{C}$. Note that compatibility for this channel means that each $\sigma \in S_\tau$ must differ from τ in all coordinates. Suppose $|S_\tau| > 2$. Let $x, y, z \in S_\tau$. Then, by definition of compatibility, $\{x_i, y_i, z_i\} \subseteq \{0,1,2\} \setminus \{\tau_i\}$ for each coordinate i, which contradicts the trifference condition for the codewords x, y, z. This implies that $|S_\tau| \leq 2$ and hence, $\mathcal{C}$ is a 2-list decoding code for the $3/2$ channel.

Now suppose $\mathcal{C}$ is a 2-list decoding code for the $3/2$ channel and there exist $x, y, z \in \mathcal{C}$ such that for all $i \in [n]$, $\{x_i, y_i, z_i\} \subsetneq \{0,1,2\}$. Then, the output word $\tau \in \{0,1,2\}^n$ with $\tau_i \in \{0,1,2\} \setminus \{x_i, y_i, z_i\}$, is compatible with all three input words x, y and z, which contradicts $\mathcal{C}$ being a 2-list decoding code. Hence, $\mathcal{C}$ must be trifferent. □

For the $3/2$ channel (i.e. when $q = 3$), Elias' result states that $\mathsf{cap}(3) \leq \mathsf{log}_2(3/2)$. In other words, if $\mathcal{C}$ is a 2-list decoding code for the $3/2$ channel, we have

$$\begin{aligned} & \frac{1}{n}\,\mathsf{log}_2(|\mathcal{C}|/2) \leq \mathsf{log}_2(3/2) \\ \implies \quad & |\mathcal{C}| \leq 2 \times (3/2)^n. \end{aligned}$$

Then Proposition 2.1 implies that for any trifferent code $\mathcal{C}$, we have $|\mathcal{C}| \leq 2 \times (3/2)^n$. In other words,

$$T(n) \leq 2 \times (3/2)^n.$$

2.1. Pruning Argument

We now provide a simpler proof of Elias' upper bound using the pigeonhole principle. This proof technique has also been referred to as the pruning argument in literature and is identical to the argument used in proving (1.1).

Proposition 2.2. *The largest size of a trifferent code of block length n, $T(n)$, is bounded above by:*

$$T(n) \leq 2 \times (3/2)^n.$$

Proof. Let $\mathcal{C} \subseteq \{0,1,2\}^n$ be a trifferent code of block length n and size m. Suppose $z \in \{0,1,2\}$ is one of the symbols which occurs the least in the first coordinate of all codewords in $\mathcal{C}$. Let $\mathcal{C}^{(1)} \subseteq \mathcal{C}$ be the subset of codewords **not** having z in the first coordinate. By the pigeonhole principle (PHP), $|\mathcal{C}^{(1)}| \geq \frac{2}{3}m$. Further, since none of the codewords in $\mathcal{C}^{(1)} \subseteq \mathcal{C}$ have z in their first coordinate, they continue to be trifferent with each other, making $\mathcal{C}^{(1)} \subseteq \mathcal{C}$ a trifferent code as well. This process can done iteratively by removing codewords with least occurring element in the i^{th} coordinate in $\mathcal{C}^{(i-1)}$ to obtain the trifferent code $\mathcal{C}^{(i)}$, till we reach $\mathcal{C}^{(n)}$, which must also be a trifferent code. However, $\mathcal{C}^{(n)}$ contains codewords which have one element absent in each of the coordinates and hence no three codewords in it can exhibit the trifference condition. This implies $\left|\mathcal{C}^{(n)}\right| \leq 2$. Moreover, the iterative bounds on the sizes of $\mathcal{C}^{(i)}$ result in $\left|\mathcal{C}^{(n)}\right| \geq \left(\frac{2}{3}\right)^n m$. Combining the two bounds results in $m \leq 2 \times \left(\frac{3}{2}\right)^n$, which proves the proposition. □

[1] We are stating Elias' result in the specific case when the channel is the $q/(q-1)$ channel. The original result works for any finite discrete memory-less channel.

3

Recent Bounds on Trifferent Codes

In this chapter, we look at the recent improvements in the bounds for both trifferent and 'r-bounded' trifferent codes, as shown by Bhandari and Khetan [BK25].

Before doing so, we first state and prove a well-known result from graph theory, which will be used later in proving other results.

Lemma 3.1. *Any graph can be made bipartite with parts of almost equal size by removing at most half of its edges.*

Proof. Let $G = (V, E)$ be a graph with $|V| = n$ and $|E| = m$. Suppose $S \subseteq V$ with $|S| = n/2$ (or $\lfloor n/2 \rfloor$ in case n is odd) chosen uniformly at random. Then the probability that an edge $xy \in E$ has both endpoints in either S or $V \setminus S$ can be calculated as -

$$\begin{aligned}
\mathbb{P}(x, y \in S \text{ or } x, y \in V \setminus S) &= \mathbb{P}(x, y \in S) + \mathbb{P}(x, y \in V \setminus S) \\
&= \frac{\binom{n-2}{n/2-2}}{\binom{n}{n/2}} + \frac{\binom{n-2}{n/2}}{\binom{n}{n/2}} \\
&= \frac{\frac{(n-2)!}{(n/2-2)!(n/2)!} + \frac{(n-2)!}{(n/2)!(n/2-2)!}}{\binom{n}{n/2}} \\
&= \frac{2 * \frac{(n-2)!}{(n/2)!(n/2-2)!}}{\frac{n!}{((n/2)!)^2}} \\
&= 2 * \frac{\frac{(n/2)!}{(n/2-2)!}}{\frac{n!}{(n-2)}!} \\
&= 2\frac{(n/2)(n/2-1)}{n(n-1)} \\
&= \frac{1}{2}\left(\frac{n-2}{n-1}\right) \\
&\leq \frac{1}{2}.
\end{aligned}$$

A similar but much more careful counting argument also results in the same inequality in case n is odd and $|S| = \lfloor n/2 \rfloor$. Thus, the probability that an edge is across S, i.e. has one endpoint in S and the other in $V \setminus S$, $\mathbb{P}(xy \text{ is across } S) \geq 1/2$.

With this, the expected number of edges across S can be calculated as:

$$\begin{aligned}
\mathbb{E}_{e \in E}[\mathbb{I}[e \text{ is across } S]] &= \sum_{e \in E} \mathbb{P}(e \text{ is across } S) \\
&\geq \sum_{e \in E} \frac{1}{2} \\
&\geq \frac{m}{2}.
\end{aligned}$$

This implies that there must exist $S \subseteq V$ such that at least $m/2$ edges go across S. In other words, removing all the other (at most $m/2$) edges makes G bipartite with partition consisting of S and $V \setminus S$, where S and $V \setminus S$ have almost equal sizes, since $|S| = \lfloor n/2 \rfloor$. □

To establish the upper bounds, Bhandari and Khetan [BK25] made use of the following theorem, which we refer to as the local-global density lemma.

Lemma 3.2 (Local-global density lemma)**.** *Let H be a vertex-transitive*[1] *hypergraph on vertex set V and S be any subset of V. Then, the independence ratio of H is at most the independence ratio of $H[S]$, the hypergraph induced by S, i.e.,*

$$\frac{\alpha(H)}{|V|} \leq \frac{\alpha(H[S])}{|S|}. \tag{3.1}$$

Proof. Let $I \subseteq Y$ be an independent set in H of size $\alpha(H)$, G be the automorphism group of H and S any subset of V. For any automorphism $g \in G$, $g(I) \cap S$ is also an independent set in S (by definition of an automorphism) and hence, $|g(I) \cap S| \leq \alpha(H[S])$.

Consider the set $\chi = \{(g, x) \mid g \in G, x \in g(I) \cap S\}$. Clearly, $|\chi| = \sum_{g \in G} |g(I) \cap S| \leq |G| \cdot \alpha(H[S])$. Counting by x, we also get $|\chi| = \sum_{x \in S} |\{g \in G \mid x \in g(I)\}| = \sum_{x \in S} \sum_{y \in I} |\{g \in G \mid x = g(y)\}|$.
Claim: For any $y, z \in V$, $|\{g \in G \mid z = g(y)\}| = |G|/|V|$.
Proof of claim: Consider the action of the group $G = Aut(H)$ on V. For any $x \in V$, the orbit-stabilizer theorem states that $|Orb(x)| = \frac{|G|}{|Stab(x)|}$, where $Orb(x) := \{g(x) \mid g \in G\}$ and $Stab(x) := \{g \in G \mid g(x) = x\}$. Since H is vertex-transitive, $Orb(x) = V$ for any vertex $x \in V$ and so, $|Stab(x)| = |G|/|V|$. Let $h \in G$ such that $h(y) = z$. Note that such an h exists because of vertex-transitivity of H.

Consider the map $\psi : Stab(y) \to \{g \in G : g(y) = z\}$ given by $g \mapsto hg$. Clearly, for any $g \in Stab(y)$, $\psi(g)(y) = hg(y) = h(g(y)) = h(y) = z$ and so $\psi(g) \in \{g \in G : g(y) = z\}$. It is also easy to see that ψ is a bijection with the inverse map being h^{-1}. This implies that $|\{g \in G : g(y) = z\}| = |Stab(y)| = |G|/|V|$.

From the claim, we get that

$$\begin{aligned}
|\chi| &= \sum_{x \in S} \sum_{y \in I} |\{g \in G \mid x = g(y)\}| \\
&= \sum_{x \in S} \sum_{y \in I} \frac{|G|}{|V|} \\
&= |S| \cdot |I| \cdot \frac{|G|}{|V|} \\
&= \alpha(H) \cdot \frac{|S||G|}{|V|}
\end{aligned}$$

Comparing the two counts of $|\chi|$ gives

$$\begin{aligned}
&\alpha(H) \cdot \frac{|S||G|}{|V|} \leq |G| \cdot \alpha(H[S]) \\
\implies &\frac{\alpha(H)}{|V|} \leq \frac{\alpha(H[S])}{|S|}.
\end{aligned}$$

□

Now consider the 3-uniform hypergraph H with vertex set $\mathbb{F}_3^n$ and three vectors forming a hyperedge if they violate the trifference condition, i.e. $(x, y, z) \in E(H)$ if for each coordinate $i \in [n]$, the set $\{x(i), y(i), z(i)\} \subsetneq \mathbb{F}_3$. It is easy to see that an independent set of size m in H corresponds to a trifferent code of size m and block length n. For any two vertices $x, y \in \mathbb{F}_3^n$ of this hypergraph, consider the function $\phi_{xy} : V(H) \to V(H)$ which maps $z \mapsto z + (y - x)$. By the properties of the field $\mathbb{F}_3$, ϕ_{xy} is clearly a bijection. Since any three codewords $a, b, c \in \{0, 1, 2\}^n$ are trifferent if and only if the codewords $a + z, b + z, c + z$ are trifferent for a fixed $z \in \{0, 1, 2\}$, ϕ_{xy} maps hyperedges and non-hyperedges to hyperedges and non-hyperedges respectively. This implies that ϕ_{xy} is an automorphism and clearly, $\phi_{xy}(x) = y$. Hence, this hypergraph is vertex-transitive. So we can apply Lemma 3.2 to this hypergraph, obtaining the following corollary.

[1] A (hyper)graph is said to be *vertex-transitive* if for every pair of vertices in it, there exists an automorphism of the (hyper)graph mapping one vertex to the other.

Corollary 1. *Let $T(S)$ denote the size of the largest trifferent code contained in $S \subseteq \mathbb{F}_3^n$. Then, we have*

$$T(n) \leq \frac{T(S)}{|S|} \times 3^n.$$

It makes sense to now look at different possible subsets $S \subseteq \mathbb{F}_3^n$ for which we can either find the value of $T(S)$ or prove an upper bound for it, which can consequently improve the upper bound for $T(n)$ in lieu of Corollary 1.

Bhandari and Khetan [BK25] studied the following class of subsets and were able to derive better bounds for $T(n)$ from them.

$$S_r := \{x \in \mathbb{F}_3^n \mid x \text{ contains exactly } r \text{ 2's}\}.$$

Definition 3.1. An *r-bounded* trifferent code $\mathcal{C} \subseteq \mathbb{F}_3^n$ is a trifferent code in which each codeword has exactly r many 2s, i.e. $\mathcal{C} \subseteq S_r$.

$T(S_r)$ is often denoted in literature as $T_b(n, r)$ - the maximum size of an *r-bounded* trifferent code of block length n. The following recursive relation is immediate.

Proposition 3.3. *For $n \geq 2$, we have*

$$T_b(n, r) \geq T_b(n-1, r). \tag{3.2}$$

Proof. Let $\mathcal{C} \subseteq \mathbb{F}_3^{n-1}$ be an r-bounded trifferent code of size $T_b(n-1, r)$. We can obtain a new r-bounded trifferent code $\mathcal{C}' \subseteq \mathbb{F}_3^n$ from it by appending a 1 to each codeword of $\mathcal{C}$. Clearly, each codeword in $\mathcal{C}'$ also contains exactly r many 2s. Further, since $\mathcal{C}$ is trifferent, any three codewords in $\mathcal{C}'$ are trifferent in one of the first $n-1$ coordinates, and thus $\mathcal{C}'$ is also trifferent. So, we get

$$T_b(n, r) \geq |\mathcal{C}'| \geq |\mathcal{C}| = T_b(n-1, r).$$

□

Let us now see what the values of $T_b(n, 0)$ and $T_b(n, 1)$ are, and what bounds they can provide for $T(n)$ from Corollary 1.

First, consider the case $r = 0$. Recall that $S_0 = \{x \in \mathbb{F}_3^n \mid x \text{ does not contain any 2's}\}$. We clearly have $S_0 \cong \mathbb{F}_2^n$. So, $|S_0| = 2^n$ and $T_b(n, 0) = 2$ since no three elements of $\mathbb{F}_2^n$ can exhibit the trifference property. Applying the corollary for S_0 gives us

$$\begin{aligned} T(n) &\leq \frac{2}{2^n} \times 3^n \\ \implies T(n) &\leq 2 \times \left(\frac{3}{2}\right)^n. \end{aligned}$$

So, we again obtain Elias' classical bound.

Now, let us consider 1-bounded trifferent codes.

Proposition 3.4. *We have $T_b(n, 1) = 2n$.*

Proof. Consider the following set of n codewords -

$$\begin{matrix} 2 & 1 & \cdots & 1 \\ 0 & 2 & \cdots & 1 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 2 \end{matrix}$$

This code can also be described mathematically as

$$\bigcup_{i \in [n]} \{x_i \in S_1 : x_i(j) = 0 \text{ for } j < i, x_i(i) = 2, x_i(j) = 1 \text{ for } j > i\}.$$

2	1	$\cdots$	1
0	2	$\cdots$	1
$\vdots$		$\ddots$	$\vdots$
0	0	$\cdots$	2
2	0	$\cdots$	0
1	2	$\cdots$	0
$\vdots$		$\ddots$	$\vdots$
1	1	$\cdots$	2

Table 3.1: $2n$ codewords showing $T_b(n,1) \geq 2n$

Any three of these codewords x_i, x_j, x_k with $i < j < k$ exhibit trifference in the j^{th} coordinate by construction and hence $T_b(n,1) \geq n$ (we use this fact and this construction in later proofs). To see $T_b(n,1) \geq 2n$, consider n additional codewords formed by inverting 0s and 1s in these n codewords. The set of codewords can then be written as shown in Table 3.1.

From the same reasoning as before, any three codewords in this new set of n codewords are also trifferent. The only other case to check is when two codewords belong to one of these sets and the third in the other set.

Suppose x_1, x_2, x_3 are three of these codewords and i_1, i_2, i_3 are the coordinates where 2s are present respectively in them. Assume wlog that x_1 and x_2 are of the first type with $i_1 < i_2$ and x_3 is of the second type. The following cases need to be checked.

i. If $i_3 = i_1$(or i_2), then $x_1(i_2) \neq x_3(i_2)$ since they are of different types and both are not equal to $x_2(i_2) = 2$. Hence, they achieve trifference at the i_2 (or i_1) coordinate.

ii. If $i_3 \neq i_1$ and $i_3 \neq i_2$, then it is easy to check that the three codewords achieve trifference at one of the coordinates i_1 or i_2.

Since we have constructed a 1-bounded trifferent code of size $2n$, we must have $T_b(n,1) \geq 2n$.

Further, for any set of $2n+1$ codewords in S_1, there must exist three codewords which have 2 present at the same coordinate, by PHP. These codewords violate the trifference condition and hence $T_b(n,1) \leq 2n$. The two inequalities together show that $T_b(n,1) = 2n$. □

Interestingly, applying Corollary 1 to this value of $T_b(n,1) = 2n$ gives the bound $T(n) \leq 4 \times (3/2)^n$, which is worse than the classical bound, which was also obtained from the case $r = 0$.

3.1. Polynomial Improvement to the upper bound of $T(n)$

The polynomial improvements made to the upper bound of the quantity $T(n)$ by Bhandari and Khetan [BK25] were obtained by proving upper bounds for the quantities $T_b(n,2)$ and $T_b(n,3)$ and then applying Corollary 1.

We will first look at their proof for the case of 2-bounded trifferent codes and then generalize their proof for all $r > 2$.

Let us first state the following famous result of Kővári-Sós-Turán [KST54], called the KST theorem, on the extremal number[2] of complete bipartite graphs, which is used in the proof.

Theorem 3.5 (KST Theorem [KST54])**.** *For integers $t \geq s \geq 1$,*

$$\text{ex}(n, K_{s,t}) \leq \frac{1}{2}(t-1)^{1/s} n^{2-1/s} + \frac{1}{2}(s-1)n$$

In other words, $\text{ex}(n, K_{s,t}) = O(n^{2-1/s})$.

Theorem 3.6. *There exists a constant c such that $T_b(n,2) \leq c \times n^{5/3}$.*

[2]The extremal number of a graph H, denoted $\text{ex}(n,H)$ is the largest number of edges in a graph on n vertices which does not contain H as a subgraph (not necessarily induced).

Proof. Suppose $\mathcal{C} \subseteq \{0,1,2\}^n$ is a 2-bounded trifferent code. Let $G = (V, E)$ be a graph with vertex set $V = \{1, 2, \ldots, n\}$. Let $\{i, j\}$ be an edge in G if there exists $x \in \mathcal{C}$ such that $x(i) = x(j) = 2$. Note that due to trifference, at most 2 codewords can have the 2s at the same set of coordinates and thus, $|E| \geq \frac{1}{2}|\mathcal{C}|$.

Now we will show that G is $K_{3,65}$-free. Suppose not. Assume i_1, i_2, i_3 along with $j_1, j_2, \ldots, j_{65}$ form $K_{3,65}$ as a subgraph in G. Since each edge corresponds to at most 2 codewords, let one of these codewords be denoted as $x_{i_1 j_k}$.

For fixed k, consider the set of codewords $\mathcal{C}_k = \{x_{i_1 j_k}, x_{i_2 j_k}, x_{i_3 j_k}\}$. After rearranging coordinates, these codewords can be written as follows.

Codeword/Coordinate	i_1	i_2	i_3	$\cdots$	j_k
$x_{i_1 j_k}$	2	a	b	$\cdots$	2
$x_{i_2 j_k}$	c	2	d	$\cdots$	2
$x_{i_3 j_k}$	e	f	2	$\cdots$	2

where each of a, b, c, d, e, f are binary symbols. So, $(a, b, c, d, e, f) \in \{0,1\}^6$. Now such a 6-tuple exists for each $k \in \{1, 2, \ldots, 65\}$. This means there are 65 such binary 6-tuples, each corresponding to a given $k \in \{1, 2, \ldots, 65\}$. Since there only $2^6 = 64$ binary 6-tuples in total, by the pigeonhole principle (PHP), there must exist two values of $k \in \{1, 2 \ldots, 65\}$ for which the corresponding 6-tuples are exactly the same. Let these values of k be k' and k'' and let the common binary 6-tuple be $(\alpha, \beta, \gamma, \delta, \epsilon, \mu)$.

Then the following six codewords, $x_{i_1 j_{k'}}, x_{i_1 j_{k''}}, x_{i_2 j_{k'}}, x_{i_2 j_{k''}}, x_{i_3 j_{k'}}, x_{i_3 j_{k''}}$, after rearranging coordinates, can be written as -

Codeword/Coordinate	i_1	i_2	i_3	$\cdots$	$j_{k'}$	$j_{k''}$
$x_{i_1 j_{k'}}$	2	α	β	$\cdots$	2	$*$
$x_{i_1 j_{k''}}$	2	α	β	$\cdots$	$*$	2
$x_{i_2 j_{k'}}$	γ	2	δ	$\cdots$	2	$*$
$x_{i_2 j_{k''}}$	γ	2	δ	$\cdots$	$*$	2
$x_{i_3 j_{k'}}$	ϵ	μ	2	$\cdots$	2	$*$
$x_{i_3 j_{k''}}$	ϵ	μ	2	$\cdots$	$*$	2

where each of the $* \in \{0,1\}$. Out of these, consider the three codewords with a $*$ in the $j_{k''}$ coordinate. Again, by PHP, two of these codewords must have the same element in this coordinate. WLOG, suppose $x_{i_1 j_{k'}}$ and $x_{i_2 j_{k'}}$ have $\nu \in \{0,1\}$ in their $j_{k''}$ coordinate. Then the three codewords $x_{i_1 j_{k'}}$, $x_{i_1 j_{k''}}$ and $x_{i_2 j_{k'}}$ have the following structure:

Codeword	i_1	i_2	i_3	$\cdots$	$j_{k'}$	$j_{k''}$
$x_{i_1 j_{k'}}$	2	α	β	$\cdots$	2	ν
$x_{i_1 j_{k''}}$	2	α	β	$\cdots$	$*$	2
$x_{i_2 j_{k'}}$	γ	2	δ	$\cdots$	2	ν

In every coordinate where 2 occurs in any of these three codewords, there is a repetition of some symbol. This implies that these three codewords cannot exhibit the trifference condition, which contradicts $\mathcal{C}$ being a trifferent code. Hence G must be $K_{3,65}$-free. From the Kővári-Sós-Turán theorem, $|E| \leq c' \times n^{5/3}$ for some constant c'. Since $|E| \geq \frac{1}{2}|\mathcal{C}|$, we have $|\mathcal{C}| \leq c \times n^{5/3}$ for some constant c. □

Using Corollary 1 and observing that $|S_2| = \binom{n}{2} \times 2^{n-2}$, we obtain the following result as a corollary, which is already an improvement to the prevailing upper bound.

Corollary 2. *There exists a positive constant c such that*

$$T(n) \leq c \times n^{-1/3} \times \left(\frac{3}{2}\right)^n.$$

The next theorem is a generalization of Bhandari and Khetan's [BK25] theorem for $r = 3$:

Theorem 3.7. *Let $T_b(n, r)$ be defined as before with $r > 2$. There exists a constant c such that*

$$T_b(n, r) \leq c \times n^{r-2/5}.$$

To prove this theorem, we first state a version of the KST Theorem given by Hyltén-Cavallius [HC58].

Theorem 3.8 (KST theorem due to Hyltén-Cavallius [HC58])**.** *The Zarankiewicz function $z(u, v; s, t)$ denotes the maximum possible number of edges in a bipartite graph $G = (U \cup V, E)$ for which $|U| = u$ and $|V| = v$, but which does not contain a subgraph of the form $K_{s,t}$ where s vertices come from U and t from V (here $K_{s,t}$ denotes the complete bipartite graph with s and t vertices in the two sets of the bipartition). Then,*

$$z(u, v; s, t) < (t-1)^{\frac{1}{s}}(u - s + 1)v^{1-\frac{1}{s}} + (s-1)v. \tag{3.3}$$

Proof of 3.7. Suppose $\mathcal{C} \subseteq \{0, 1, 2\}^n$ is an r-bounded trifferent code and $a < r$ a positive integer. Let $G = (V, E)$ be a graph with vertex set $V = \binom{[n]}{r-a} \cup \binom{[n]}{a}$. Let (S, T) be an edge in G with $S = \{x_1, x_2, \ldots, x_{r-a}\}$ and $T = \{y_1, y_2, \ldots, y_a\}$ if there exists $c \in \mathcal{C}$ such that x has 2's in the each of the coordinates $x_1, x_2, \ldots, x_{r-a}$ and $y_1, y_2, \ldots, y_a$ where $x_1 < x_2 < \cdots < x_{r-a} < y_1 < y_2 < \cdots < y_a$. Denote such a codeword as c_{ST}.

Further, if $a = r/2$, make G bipartite with equal-sized parts. This can be done by removing at most half of its edges, as per Lemma 3.1. In all other cases, G is bipartite by construction.

Note that due to trifference, at most 2 codewords can have 2s occurring in the same set of coordinates and thus, $|E| \geq \frac{1}{4}|\mathcal{C}|$ (where the second $1/2$ factor is in case G needs to be made bipartite).

Now, we will show G is $K_{s,t}$-free for $s = 2^a + 1$ and some large t, where the 's' vertices come from the set $\binom{[n]}{r-a}$, and the 't' vertices from $\binom{[n]}{a}$.

Suppose not. Assume the vertices $S_1, S_2, \ldots, S_s$ and $T_1, T_2, \ldots, T_t$ form $K_{s,t}$ as a subgraph in G. This implies the existence of codewords $c_{S_iT_k} \in \mathcal{C}$ for each $i \in [s], k \in [t]$. Note that while $c_{S_iT_k}$ may not denote a unique codeword for a fixed i, k, we pick one arbitrarily.

For a fixed $k \in [t]$, consider the set of codewords $J_k = \{c_{S_1T_k}, c_{S_2T_k}, \ldots, c_{S_sT_k}\}$. For $i \in [s]$, denote by F_i the set of coordinates $(\cup_{j\in[s]\setminus\{i\}} S_j) \setminus S_i$. It is easy to see that $|F_i| \leq (s-1)(r-a)$ where the maximum size is attained when all the sets $S_1, S_2, \ldots, S_s$ are pairwise disjoint. Further, for each i, the codeword $c_{S_iT_k}$ has only 0s and 1s present in the set of coordinates F_i.

Now consider the tuple of elements present in the set of coordinates F_1 of $c_{S_1T_k}$, the set of coordinates F_2 of $c_{S_2T_k}$ and so on till the set of coordinates F_s of $c_{S_sT_k}$. These are at most $s(s-1)(r-a)$ binary symbols (since each $|F_i| \leq (s-1)(r-a)$) corresponding to a fixed $k \in [t]$.

So, if $t > 2^{s(s-1)(r-a)}$, by PHP, there must exist at least two vertices, say $T_{k'}$and $T_{k''}$, where $k', k'' \in [t]$, in which symbols at all these coordinates are exactly the same.

Then the set of codewords $J_{k'}$ can be written as in Table 3.2 (for simplicity, we assume the sets $S_1, \ldots S_s$ are pairwise disjoint so that $F_i = \cup_{j\in[s]\setminus\{i\}} S_j$).

Codeword/Coordinates	S_1	S_2	$\cdots$	S_s	$\cdots$	$T_{k'}$	$T_{k''} \setminus T_{k'}$
$c_{S_1T_{k'}}$	$22\ldots2$	Λ	$\cdots$	Γ	$\cdots$	$22\ldots2$	$*\,*\cdots*$
$c_{S_2T_{k'}}$	Φ	$22\ldots2$	$\cdots$	Ω	$\cdots$	$22\ldots2$	$*\,*\cdots*$
$\vdots$							
$c_{S_sT_{k'}}$	Δ	Ψ	$\cdots$	$22\ldots2$	$\cdots$	$22\ldots2$	$*\,*\cdots*$

Table 3.2: Set of codewords $J_{k'}$

Here, each of the capital Greek letters signifies a tuple of binary symbols, i.e., lies in the set $\{0, 1\}^{r-a}$. Note that $|T_{k''} \setminus T_{k'}| \leq a$ and in the set of codewords J_k, elements present in the set of coordinates $T_{k''} \setminus T_{k'}$ must be either 0 or 1. Since $|T_{k''} \setminus T_{k'}| \leq a$ and $s = 2^a + 1$, by PHP, there must be at least two codewords in $J_{k'}$ which have the same elements present in this set of coordinates. For simplicity and without loss of generality, say codewords $c_{S_1T_{k'}}$ and $c_{S_2T_{k'}}$ have the same tuple of elements, Θ, in $T_{k''} \setminus T_{k'}$. Then the three codewords $c_{S_1T_{k'}}$, $c_{S_1T_{k''}}$ and $c_{S_2T_{k'}}$ can be written as in Table 3.3.

Codeword/Coordinates	S_1	S_2	$\cdots$	S_s	$\cdots$	$T_{k'}$	$T_{k''} \setminus T_{k'}$
$c_{S_1T_{k'}}$	$22\ldots2$	Λ	$\cdots$	Γ	$\cdots$	$22\ldots2$	Θ
$c_{S_1T_{k''}}$	$22\ldots2$	Λ	$\cdots$	Γ	$\cdots$	$*\,*\cdots*$	$22\ldots2$
$c_{S_2T_{k'}}$	Φ	$22\ldots2$	$\cdots$	Ω	$\cdots$	$22\ldots2$	Θ

Table 3.3: The three codewords $c_{S_1T_{k'}}$, $c_{S_1T_{k''}}$ and $c_{S_2T_{k'}}$

As before, we note that in every coordinate where 2 occurs in any of these three codewords, there is a repetition of some symbol. This implies that these three codewords cannot exhibit the trifference condition, which contradicts $\mathcal{C}$ being a trifferent code. Hence G must be $K_{s,t}$-free for $s = 2^a + 1$ and $t = 2^{s(s-1)(r-a)} + 1$.

From (3.3), we have that $|E| \leq c' \times (n^{r-a})(n^a)^{1-\frac{1}{2^a+1}} = c' \times n^{r-\frac{a}{2^a+1}}$. Here, we use the well-known bound $\binom{n}{a} \leq n^a$ for bounding the sizes of the two parts in the biparition of G. Since, we had $|\mathcal{C}| \leq 4|E|$, we get that $|\mathcal{C}| \leq c \times n^{r-\frac{a}{2^a+1}}$ for some constant c.

Finally, by noting that the quantity $\frac{a}{2^a+1}$ is largest when $a = 2$ for integral a and choosing $a = 2$ makes sense for all $r > 2$, we obtain the required result. □

Using this bound and Corollary 1, we get the next corollary:

Corollary 3. *Using this method, the best upper bound obtained for $T(n)$ is*

$$T(n) \leq c \times n^{-2/5} \times \left(\frac{3}{2}\right)^n$$

for some constant c.

This bound has already been shown by Bhandari and Khetan [BK25] by using a similar argument as in the proof of Theorem 3.7 for $r = 3$. Hence, we also conclude that a direct generalization of their proof for larger r does not yield an improvement in the bound for $T(n)$.

3.2. Lower bounds of r-bounded trifferent codes

We have already seen how new upper bounds for $T_b(n, r)$ can provide better upper bounds for $T(n)$ from Corollary 1.

From the same corollary, lower bounds for $T_b(n, r)$ indicate how tight an upper bound for $T(n)$ we can obtain using this method. As a result, we are also interested in knowing some lower bounds for the largest size of r-bounded trifferent codes, especially for $r = 2, 3$.

The following lower bound is obtained trivially.

Proposition 3.9. *We have $T_b(n, 2) \geq 2n - 2$.*

Proof. Consider the optimal 1-bounded trifferent code of block length $n-1$ having length $2n-2$. Append a 2 as the n^{th} coordinate for each of the codewords in it to obtain a 2-bounded trifferent code of size $2n-2$ and length n. The code continues to remain trifferent since any three codewords attain trifference in one of the first $n - 1$ coordinates by construction. □

Interestingly, there has been no improvement to this trivial lower bound for $T_b(n, 2)$. We will address this further in Chapter 5.

We now look at constructing lower bounds for $T_b(n, 3)$ and for also for $T_b(n, r)$ for general $r > 3$. Both these constructions are built upon ideas given by Anurag Bishnoi and Benedek Kovács.

Definition 3.2. An r-uniform hypergraph is said to be (v, e)-*free* if it contains no e hyperedges spanned by v vertices, i.e. any set of e edges comprise of at least $v + 1$ vertices. Let $f_r(n, v, e)$ denote the maximum number of edges in a (v, e)-free r-uniform hypergraph on n vertices.

Clearly, if a hypergraph is (v, e)-free, it is also $(v - a, e)$-free for every $0 < a < v$. Hence $f_r(n, v, e)$ is a decreasing function in v.

Recall that an r-uniform hypergraph is said to be *linear* if every two hyperedges share at most one vertex. Then two hyperedges in such a graph must be spanned by at least $2r - 1$ vertices and such

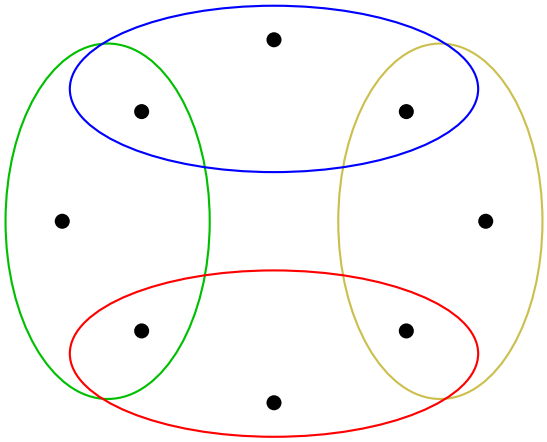


Figure 3.1: A (6,3)-free 3-uniform hypergraph

graphs are thus $(2r-2,2)$-free. By similar reasoning, any three hyperedges are spanned by at least $3r-3$ vertices and thus they are also $(3r-4,3)$-free.

For the simple case $r=3, v=6$, the problem of determining $f_3(n,6,3)$ is called the (6,3)-problem or the Rusza-Szemerédi problem.

Example 3.1. Consider the simple 3-uniform hypergraph in Figure 3.1 having 8 vertices and 4 hyperedges. It is easy to see that the union of any 3 hyperedges in this hypergraph contains exactly 7 vertices. Hence, this is a (6,3)-free 3-uniform hypergraph.

Proposition 3.10. *For n large enough, we have*

$$T_b(3n,3) \geq f_3(n,6,3).$$

Proof. Let $H=(V,E)$ be a (6,3)-free 3-uniform hypergraph on n vertices. Let the vertex set V be $\{1,2,\ldots,n\}$. Associate with each vertex i the vector $x_i \in S_1 \subseteq \{0,1,2\}^n$ given by $x_i(j)=0$ for $j<i$, $x_i(i)=2$ and $x_i(j)=1$ for $j>i$. We will construct a 3-bounded code $\mathcal{C} \subseteq S_3 \subseteq \{0,1,2\}^{3n}$ from the hyperedges of H as follows. For each hyperedge connecting vertices i,j,k with $i<j<k$, let x_{ijk} be a codeword in $\mathcal{C}$ formed by concatenating the vectors $x_ix_jx_k$. Clearly $x_{ijk} \in S_3$ for each $ijk \in E$, and $|\mathcal{C}|=|E|$.
Claim: $\mathcal{C}$ is trifferent.
This further implies that $T_b(3n,3) \geq |E|$ for any (6,3)-free 3-uniform hypergraph on n vertices and in particular, $T_b(3n,3) \geq f_3(n,6,3)$, which proves the proposition.
Proof of claim: By construction of $\mathcal{C}$, if the first vertex of the hyperedge corresponding to any three codewords is different in all three of them, then by similar reasoning as used in the proof of Proposition 3.4, the codewords must be trifferent. A similar logic follows for the second and third corresponding vertices of any three codewords. This means that for three codewords to violate the trifference condition, they must correspond to at most two distinct vertices in each of the n-length blocks, which further implies that the three corresponding hyperedges are spanned by at most 6 vertices. This is not possible since H is (6,3)-free and so, $\mathcal{C}$ must be trifferent. □

Bhandari and Khetan [BK25], and Sős et.al. [BETS73] both used properties of the finite projective plane PG$(2,q)$ to show $f_3(n,6,3) \geq c \times n^{3/2}$ for some constant c , and hence we have $T_b(n,3) \geq c' \times n^{3/2}$ for some constant c' from Proposition 3.10 (the factor 1/3 can be absorbed in the constant term).

Ruzsa and Szemerédi [RS78] resolved the (6,3)-problem by proving that

$$n^{2-o(1)} < f_3(n,6,3) = o(n^2).$$

They proved the lower bound using Behrend's [Beh46] construction of large 3-AP-free sets. The upper bound can be proved using Szemerédi regularity lemma. Since it is convulated and not directly relevant to trifferent codes, we omit it in this thesis. We present the proof of the lower bound later in this chapter.

First, we provide a small background on 3-AP free sets.

3.2.1. 3-AP-free sets

In an abelian group G, a 3-term arithmetic progression, or a 3-AP, is a set of three distinct elements of the form $\{x, x+d, x+2d\}, d \neq 0$ where $x, d \in G$. A subset $A \subseteq G$ is said to be *3-AP-free* if it does not contain any 3-AP.

Example 3.2. In the additive group of positive integers, the set $A = \{1, 2, 4, 5, 10\}$ is 3-AP-free while the set $A' = \{1, 2, 4, 5, 9\}$ is not, since it contains the 3-AP $\{1, 5, 9\}$.

In 1936, Erdös and Turán [ET36] conjectured that every set of positive integers with positive upper density[3] contains a non-trivial 3-AP. This was proved by Roth in 1953 [Rot53] and is now known as Roth's theorem. Let $r_3(N)$ denote the maximum size of a subset of $\{1, \ldots, N\}$ with no non-trivial three-term arithmetic progressions. Then Roth's theorem states the following:

Theorem 3.11 (Roth)**.** *We have that* $r_3(N) = o(N)$.

Since then the problem of finding large 3-AP-free sets and determining better bounds for $r_3(N)$ has become one of the most significant problems in additive combinatorics. It is also worth noting that in the field $\mathbb{F}_3^n$, a 3-AP-free set is equivalent to a *cap-set*, which is a subset of the field containing no three points in a line. As a result, the *cap-set* problem, another important problem in combinatorics to determine the largest size of cap-sets, is inherently connected to 3-AP-free sets.

Roth's proof of his theorem resulted in the upper bound $r_3(N) \lesssim N/\log\log N$. In 2020, Bloom and Sisask [BS20] were able to surpass the logarithmic barrier by proving an upper bound of $r_3(N) \lesssim N/(\log N)^{1+c}$ for some constant $c > 0$. In a further major breakthrough in 2023, Kelley and Meka [KM23] broke the quasi-polynomial barrier in this upper bound and proved that $r_3(N) \lesssim N/\exp(\Omega((\log N)^c))$ for a constant $c = 1/12$, which was improved by Bloom and Sisask [BS23] to $c = 1/9$.

Vis-à-vis the lower bounds, Salem and Spencer [SS42] proved $r_3(N) \gtrsim N/N^{(\log 2+\epsilon)/\log\log N}$ for every $\epsilon > 0$. In 1946, Behrend [Beh46] proposed a significant improvement.

Lemma 3.12 (Behrend's construction)**.** *There exists a constant* $C > 0$ *such that for every positive integer* N*, there exists a* 3*-AP-free set* $A \subseteq N$ *with* $|A| \geq N^{1-\frac{C}{\sqrt{\log N}}}$*. In other words,* $r_3(N) \gtrsim N^{1-\frac{C}{\sqrt{\log N}}}$*.*

Ever since Behrend's construction in 1946, the lower bound has retained the form of $N/\exp(O((\log N)^{1/2}))$, with improvements coming only in lower-order terms. For a more detailed survey on this problem, refer to [Pel23].

We now move on to prove the lower bound in the theorem of Ruzsa and Szemerédi.

Theorem 3.13 (Ruzsa-Szemerédi)**.** *For any large enough* n*, there exists constant* c *such that*

$$f_3(n, 6, 3) > c \times n^{2-o(1)}. \tag{3.4}$$

Proof. Suppose n is a large enough positive integer. We use $r_3(n)$ to denote the size of the largest 3-AP-free subset of $\{1, \ldots, n\}$. Let $A = \{a_1, \ldots, a_m\}$ be the largest 3-AP-free set such that $\frac{n}{4} < a_i < \frac{n}{4} + \frac{n}{8}$ for each $1 \leq i \leq m$. Since x, y, z are in an AP if and only if $x+a, y+a, z+a$ are in an AP for some fixed a, A can be identified with a 3-AP-free subset of $\{1, \ldots, n/8\}$ and hence $m = r_3\left(\frac{n}{8}\right)$. We now construct a 3-uniform hypergraph $H = (V, E)$ on the vertex set $V = \{1, \ldots, n\}$. For each integer $t \in (0, n/8]$ and each $a_i \in A$, let $(t, t+a_1, t+2a_1)$ be a hyperedge of H. Clearly, $|E| = m \times n/8$.

Now suppose H is not (6,3)-free. From the bounds on t and a_i, the first vertex of any hyperedge, $t \in (0, n/8]$, the second vertex, $t + a_i \in (n/4, n/2)$ and the third vertex, $t + 2a_i \in (n/2, 7n/8)$, which implies H is a 3-partite 3-uniform hypergraph. Since any two vertices of a hyperedge in H uniquely determine the third by construction, no two hyperedges can share two vertices. This, along with H being 3-partite, implies that the only way 3 hyperedges in H can be spanned by 6 vertices is if the hyperedges are of the form $(x', y, z), (x, y', z)$ and (x, y, z'). This means the three hyperedges must be of the form $(u, u+a_i, u+2a_i), (t, t+a_j, t+2a_j)$ and $(t, t+a_k, t+2a_k)$ with $u + a_i = t + a_k$ and $u + 2a_i = t + 2a_j$. Subtracting these two equations gives $a_i = 2a_j - a_k$, or equivalently, $2a_j = a_i + a_k$.

[3] The upper density of a subset $A \subseteq \mathbb{Z}_+$ of positive integers is defined as $\limsup_{n\to\infty} \frac{|A\cap\{1,2,\ldots,N\}|}{N}$.

This is not possible since A is 3-AP-free and hence, H must be (6,3)-free. This means that

$$\begin{aligned} f_3(n,6,3) &\geq |E| \\ &= \frac{n}{8} \times r_3\left(\frac{n}{8}\right) \\ &\geq \frac{n}{8} \times \left(\frac{n}{8}\right)^{1-\frac{c'}{\sqrt{\log n/8}}} && \text{(From Behrend's construction)} \\ &> c \times n^{2-\frac{c'}{\sqrt{\log n/8}}} && (\exists c > 0 : (n/8)^{2-\delta} > c \times n^{2-\delta}) \\ &= c \times n^{2-o(1)} && (\because 1/\log(n/8) \to 0 \text{ as } n \to \infty) \end{aligned}$$

This proves the required lower bound. □

Using Proposition 3.10, this gives the following result.

Theorem 3.14. *For some constant c, we have*

$$T_b(n,3) \geq c \times n^{2-o(1)}.$$

For $e = 3$ and some specific values of v, we have the following result by Alon and Shapira [AS06] -

Theorem 3.15. *For any fixed $2 \leq k < r$ we have,*

$$n^{k-o(1)} < f_r(n, 3(r-k)+k+1, 3) = o(n^k). \tag{3.5}$$

Corollary 4. *For fixed $r \geq 3$ and n large enough, we have*

$$f_r(n, 2r, 3) > n^{\lceil \frac{r}{2} \rceil - o(1)}.$$

Proof. If $r \geq 3$ is even, using $k = r/2 \geq 2$ in Theorem 3.15, we get $f_r(n, 2r+1, 3) > n^{\frac{r}{2}-o(1)}$, which implies $f_r(n, 2r, 3) > n^{\frac{r}{2}-o(1)}$, since $f_r(n, v, e)$ is a decreasing function in v. If r is odd, use $k = (r+1)/2 \geq 2$ in Theorem 3.15 to get $f_r(n, 2r, 3) > n^{\frac{r+1}{2}-o(1)}$. Combining the two inequalities, we get $f_r(n, 2r, 3) > n^{\lceil \frac{r}{2} \rceil - o(1)}$. □

Note that the result by Ruzsa and Szemerédi can also be seen as a corollary of Theorem 3.15 by taking $k = 2$ and $r = 3$.

This result can also be used to generate lower bounds for maximum size of r-bounded trifferent codes by the following generalization of Proposition 3.10:

Proposition 3.16. *For n large enough,*

$$T_b(rn, r) \geq f_r(n, 2r, 3).$$

This proposition can be proved by trivially extending the proof of 3.10 using r blocks of 1-bounded trifferent codes rather than 3 blocks and an identical argument to show trifference.

The following result is then immediate using Proposition 3.16 and Corollary 4.

Theorem 3.17. *For any $r \geq 3$, we have*

$$T_b(n, r) \geq n^{\lceil \frac{r}{2} \rceil - o(1)}.$$

4

Linear Trifferent Codes

In this chapter, we focus on linear trifferent codes and establish their connections with minimal codes and strong blocking sets.

4.1. Error-correcting codes

In this section, we introduce some basic concepts in coding theory (see [GRS25] for a standard reference).

Definition 4.1. For a vector $v \in \mathbb{F}_q^n$, its support, $\sigma(v)$, is the set

$$\sigma(v) := \{i \in [n] \mid v(i) \neq 0\}.$$

The Hamming weight of v is the size of its support, i.e.

$$w(v) := |\sigma(v)|$$

The metric induced by the Hamming weight on the space $\mathbb{F}_q^n$ is called the Hamming distance, i.e. for any two vectors $u, v \in \mathbb{F}_q^n$, the Hamming distance between them, $d_H(u,v) := w(u-v)$. It can alternatively be seen as the number of coordinates in which the two vectors differ.

Definition 4.2. An $[n,k]_q$ code $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_q^n$. Its minimum distance $d(\mathcal{C})$ is defined as

$$d(\mathcal{C}) := \min\{d_H(u,v) \mid u, v \in \mathcal{C}\} = \min\{w(v) \mid v \in \mathcal{C}\}$$

where the second equality is true because of the linearity of $\mathcal{C}$.

If the minimum distance of an $[n,k]_q$ code is known to be d, it is referred to as an $[n,k,d]_q$ code.

The elements of $\mathcal{C}$ are called *codewords*. A *generator matrix* of $\mathcal{C}$ is a matrix $G \in \mathbb{F}_q^k$ such that its rows span $\mathcal{C}$, or in other words, $\mathcal{C} = \{u^T G \mid u \in \mathbb{F}_q^k\}$.

The following simple bound, called the *singleton bound*, is one of many bounds which restricts the choices of the various parameters of a linear code.

Proposition 4.1. *(Singleton bound). Let $\mathcal{C}$ be an $[n,k,d]_q$ code. Then $k \leq n - d + 1$.*

Proof. The result follows trivially if $k = 0$. Suppose $k > 0$. Let $I = \{1, 2, \ldots, n-d+1\}$. We claim that the projection of $\mathcal{C}$ onto the set of coordinates I is injective. Suppose not. Then there exist distinct codewords $c, c' \in \mathcal{C}$ with $\pi_I(c) = \pi_I(c')$, where π_I is a standard notation to denote the projection map onto the set of coordinates indexed by I. But this means that $\sigma(x-y) \subseteq \{n-d+2, n-d+3, \ldots, n\}$, which implies $w(x-y) \leq d-1$, a contradiction to the minimum distance being d. Hence, π_S is injective on $\mathcal{C}$.

This means that the code obtained by only considering the first $n-d+1$ coordinates of codewords in $\mathcal{C}$ has the same size as $\mathcal{C}$, i.e. has dimension k. Since the dimension is at most the length for any code, we have $k \leq n-d+1$, and we are done. □

Definition 4.3. An $[n,k,d]_q$ code $\mathcal{C}$ is said to be *nondegenerate* if there is no coordinate $i \in [n]$ such that $c(i) = 0$ for all codewords $c \in \mathcal{C}$. It is said to be *projective* if no two columns in its generator matrix are proportional (or linearly dependent).

Remark. A projective code is necessarily nondegenerate.

4.2. Linear trifferent codes

We now define linear trifferent codes using the definitions and notation used in the previous section.

Definition 4.4. A trifferent code $\mathcal{C}$ of block length n is said to be a *linear trifferent code* if it is a linear subspace of $\mathbb{F}_q^n$, i.e. it is also a linear code.

Analogous to the general case, $T_L(n)$ denotes the largest size of a linear trifferent code of block length n.

Example 4.1. The trifferent code in Example 1.1 is actually a linear trifferent code with generating matrix, $G = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix}$.

Linear codes have been widely studied in coding theory. The added structure of linearity in linear trifferent codes gives rise to interesting results and reconciles equivalent notions in different fields of mathematics.

More specifically, as we will soon show, linear trifferent codes are equivalent, in some sense, to 'minimal codes' in coding theory which have been studied for their applications in cryptology, and via this equivalence, also to 'strong blocking sets' in finite geometry.

These equivalences help us in using established bounds on these seemingly different combinatorial objects to derive bounds on sizes of linear trifferent codes.

4.3. Minimal Codes

In this section, we define minimal codes, provide a small background on them and their significance and lastly prove the equivalence of linear trifferent codes and certain minimal codes.

4.3.1. Background on Minimal Codes

Suppose $\mathcal{C}$ is an $[n,k]_q$ code. A codeword $c \in \mathcal{C}$ is called *minimal* if its support $\sigma(c)$ does not contain the support of another independent codeword. The study of the minimal codewords of a linear code finds application in the analysis of the Voronoi region for decoding purposes [Agr02], in secret sharing schemes [Mas93] and in secure two-party communication [ABCH95]. However, finding the minimal codewords of a general linear code is a challenging task in general, even for the binary case. In fact, the knowledge of the minimal codewords is related with the complete decoding problem which is known to be NP-hard [BMVT78]. To tackle this, a special class of codes called 'minimal' codes were introduced, which are essentially linear codes where each codeword is minimal.

Definition 4.5. Let $\mathcal{C}$ be an $[n,k,d]_q$ code. A nonzero codeword $c \in \mathcal{C}$ is called *minimal* if every codeword $c' \in \mathcal{C}$ with $\sigma(c') \subseteq \sigma(c)$ is a multiple of c. We say that the code $\mathcal{C}$ is *minimal* if all its codewords are minimal.

Example 4.2. Consider the $[4,2]_3$ codes $\mathcal{C}_1, \mathcal{C}_2$ with generator matrices $G_1 = \begin{pmatrix} 2 & 1 & 0 & 2 \\ 1 & 0 & 2 & 2 \end{pmatrix}$ and $G_2 = \begin{pmatrix} 2 & 0 & 0 & 1 \\ 1 & 0 & 2 & 2 \end{pmatrix}$ respectively. In case of $\mathcal{C}_2$, the codeword 1022 is not minimal since there exists codeword 2001 with $\sigma(2001) \subsetneq \sigma(1022)$. This implies that $\mathcal{C}_2$ is not a minimal code.

On the other hand, it is easy to check that all the codewords of $\mathcal{C}_1 = \{0000, 2102, 1201, 1022, 2011, 0121, 0212, 2220, 1110\}$ are minimal and so $\mathcal{C}_1$ is a minimal code.

Remark. Note that while any codeword c in a minimal code is *minimal*, it is also *maximal*, that is, every other codeword $c' \in \mathcal{C}$ with $\sigma(c') \supseteq \sigma(c)$, is a multiple of c.

The following simple result bounds the weight of a minimal codeword in a linear code.

Proposition 4.2. *Let $\mathcal{C}$ be an $[n,k]_q$ code. Every minimal codeword $c \in \mathcal{C}$ has $w(c) \leq n - k + 1$.*

Proof. Consider the code $\mathcal{C}'$ obtained by puncturing $\mathcal{C}$ on the support of c, i.e. $\mathcal{C}' = \pi_{[n]\setminus\sigma(c)}(\mathcal{C})$. Then $\mathcal{C}'$ has length $n - w(c)$ and dimension $k-1$, since any non-multiple of c continues to be a codeword of $\mathcal{C}'$ (due to the minimality of c) while any multiple of c vanishes in $\mathcal{C}'$. Since the dimension of any code is bounded above by its length, we get $k-1 \leq n-w(c)$, which gives the required result on rearranging. □

Ashikhmin and Barg [AB02] provided the first sufficient condition for a linear code to be minimal.

Lemma 4.3. *Let $\mathcal{C}$ be an $[n,k]_q$ code, $w_{\min}$, $w_{\max}$ be the minimum and the maximum Hamming weights of any codeword in $\mathcal{C}$, respectively. Then $\mathcal{C}$ is minimal if*

$$\frac{w_{\min}}{w_{\max}} > \frac{q-1}{q}. \tag{4.1}$$

In 2018, Heng et.al. [HDZ18] were able to provide a necessary and sufficient condition for an $[n,k]_q$ code to be minimal -

Lemma 4.4. *An $[n,k]_q$ code $\mathcal{C}$ is minimal if and only if for every pair of linearly indpendent codewords $u, v \in \mathcal{C}$, the following holds:*

$$\sum_{\lambda \in \mathbb{F}_q^*} w(u+\lambda v) \neq (q-1)w(u) - w(v)$$

In the same paper, the authors constructed an infinite family of minimal linear codes not satisfying condition (4.1).

The following theorem, proved in [ABNR22], provides a lower bound on the length of a minimal code. The proof requires various techniques from coding theory and is beyond the scope of this thesis.

Theorem 4.5. *Let $\mathcal{C}$ be an $[n,k]_q$ minimal code. We have $n \geq (q+1)(k-1)$.*

While the Hamming distance d does not appear in the definition of minimal codes, the following two theorems provide lower bounds on d for an $[n,k,d]_q$ minimal code. The first is from [ABN22], and the second from [ABNR22]. We only prove the first bound here.

Theorem 4.6. *Let $\mathcal{C}$ be an $[n,k,d]_q$ minimal code with $k \geq 2$. Then $d \geq k+q-2$.*

Proof. Let $c \in \mathcal{C}$ be such that $w(c) = d$. Consider the code $\mathcal{C}'$ obtained by projecting $\mathcal{C}$ onto the set of coordinates $\sigma(c)$. We claim that $\mathcal{C}'$ is a $[d,k,d']_q$ code with $d' \geq q-1$. Moreover, since $\mathcal{C}$ is minimal and the $k \geq 2$, it must be that $d' < d$.

To see why the dimension of $\mathcal{C}'$ is k, suppose it is not and is strictly less than k. Then there exists a codeword x such that its support is disjoint from the support of c. But this means that $\sigma(c) \subsetneq \sigma(c+x)$ where $c+x \in \mathcal{C}$ due to linearity. This contradicts the minimality of $\mathcal{C}$.

To see why $d' \geq q-1$, let $c' \in \mathcal{C}'$ denote the projection of c onto its support and so $w(c') = d$. Suppose $u \in \mathcal{C}$ is such that $\pi_{\sigma(c)}(u) = u' \in \mathcal{C}'$ has weight d' in $\mathcal{C}'$. Consider the set of codewords $\{c' + \lambda u' \mid \lambda \in \mathbb{F}_q^*\} \subseteq \mathcal{C}'$. If $d < q-1$, then at least one of the codewords in this set must have weight d due to uniqueness of additive inverses in a field and the pigeonhole principle. Then its corresponding codeword in $\mathcal{C}$ must have support containing $\sigma(c)$. Moreover, it cannot be a multiple of c since u' is not a multiple of c' ($d' < d$). This again contradicts the minimality of $\mathcal{C}$.

Now applying the Singleton bound on $\mathcal{C}'$ gives $d \geq k + d' - 1$ and since $d' \geq q-1$, we get $d \geq k+q-2$. □

Theorem 4.7. *Let $\mathcal{C}$ be an $[n,k,d]_q$ code and $c \in \mathcal{C}$ a maximal codeword. Then $w(c) > (q-1)(k-1)+1$. In particular, if $\mathcal{C}$ is minimal, then $d > (q-1)(k-1)+1$.*

Remark. The bound in Theorem 4.7 is a better bound than the one in Theorem 4.6 in almost all cases.

4.3.2. Minimal Codes and Linear Trifferent Codes

We conclude this section by establishing an equivalence between linear trifferent codes and minimal codes.

Proposition 4.8. *A linear code $\mathcal{C} \leq \mathbb{F}_3^n$ is trifferent if and only if it is minimal.*

Proof. Suppose $\mathcal{C}$ is not a minimal code. Then there exist two linearly independent codewords $x, y \in \mathcal{C}$ such that $\sigma(y) \subseteq \sigma(x)$. Since $\mathcal{C}$ is linear, the codeword $-y$ lies in $\mathcal{C}$ as well. From the linear independence of x and y, $x \neq -y$. Consider an arbitrary index $i \in [n]$ and the set $\{x_i, y_i, -y_i\}$. If $x_i = 0$, $\sigma(y) \subseteq \sigma(x)$ implies that both y_i and $-y_i$ are 0 too. If $x_i \neq 0$, either both y_i and $-y_i$ are zero or neither is. In all cases, $|\{x_i, y_i, -y_i\}| \leq 2$, and hence, $\mathcal{C}$ cannot be trifferent.

Now suppose $\mathcal{C}$ is not trifferent. Then there exist three distinct codewords $x, y, z \in \mathcal{C}$ such that for each $i \in [n]$, $\{x_i, y_i, z_i\} \subsetneq \mathbb{F}_3$. Since the trifference condition is invariant under translation and $\mathcal{C}$ is linear, we may assume $x = 0$. This implies both $y, z \neq 0$. Since $x(= 0)$, y, z violate the trifference condition, at no index $i \in [n]$, $\{y_i, z_i\} = \{1, 2\}$. Therefore, at any coordinate i, where either y_i or z_i is non-zero, their sum is non-zero too, which implies $\sigma(y + z) = \sigma(y) \cup \sigma(z)$ and also that $\sigma(y) \neq \sigma(z)$ since y, z are distinct. However, this means that either $\sigma(y)$ or $\sigma(z)$ (or both) is strictly contained in $\sigma(y + z)$. Since $y + z \in \mathcal{C}$ due to its linearity, $\mathcal{C}$ cannot be minimal. □

4.4. Blocking Sets

In this section, we first lay down some fundamental notation and concepts of finite geometry and more specifically, finite affine projective spaces. We then introduce the notions of blocking strong blocking sets and later prove the equivalence of strong blocking sets with minimal codes and also trifferent codes.

4.4.1. Preliminaries

Let V be a vector space of dimension $k \geq 1$ over a field $\mathbb{F}$. The *projective space* $\mathbf{P}(V)$ *induced by* V is the set $(V \setminus \mathbf{0})/\sim$ of equivalence classes of non-zero vectors in V under the equivalence relation $\sim$ defined for all $u, v \in V \setminus \mathbf{0}$ as,

$$u \sim v \quad \text{iff} \quad u = \lambda v, \text{ for some } \lambda \in \mathbb{F} \setminus 0.$$

The dimension of $\mathbf{P}(V)$ is $k - 1$. The process of obtaining the projective space from the underlying vector space is called *projectivization*.

More intuitively, points of $\mathbf{P}(V)$ are identified with the 1-dimensional linear subspaces of V, lines with 2-dimensional subspaces and so on. Note that while the dimension of a projective subspace is one less than the dimension of its corresponding vector subspace, the codimensions remain the same.

For a non-zero vector $v \in V$, the one-dimensional subspace containing v, or the equivalence class of v under $\sim$, is a point in $\mathbf{P}(V)$, denoted by $[v]$.

We focus more on the case when the vector space $V = \mathbb{F}^k$ over the field $\mathbb{F}$. In this context, the notation $\mathbb{FP}^{k-1}$ is used to denote the projective space $\mathbf{P}(\mathbb{F}^k)$.

As an example, consider the projective space $\mathbb{RP}^2$ obtained from the projectivization of $\mathbb{R}^3$ as illustrated in Figure 4.2. Interestingly, the motivation to study projective geometry also arises from a different way to arrive at the real projective plane $\mathbb{RP}^2$. The projective plane $\mathbb{RP}^2$ is in fact isomorphic to the *Extended Euclidean plane*, a plane obtained by adding a 'line at infinity' to the Euclidean plane and stipulating that each set of parallel lines in the plane intersects the line at infinity at a unique 'point at infinity'. It is easy to see that both the definitions of this projective plane lead to a geometry in which any two points lie on a unique line and any two lines intersect at a unique point.

In finite geometry, special emphasis is placed on the projective spaces induced by the vector spaces $\mathbb{F}_q^k$, where $\mathbb{F}_q$ denotes the finite field with q elements and q is a prime power. The notation PG$(k-1, q)$[1] is more commonly used to denote the projective space $\mathbb{F}_q\mathbb{P}^{k-1}$.

Example 4.3. The projective space PG(2,2) is commonly referred to as the Fano plane and is illustrated in Figure 4.1. Note that in representations of finite affine ($\mathbb{F}_q^k$) and projective (PG$(k-1, q)$) spaces, lines are often represented by arcs or circles, as seen in Figures 4.1,4.3 and 4.7.

The following result is called the *dimension formula* and is often an axiom for defining general projective spaces.

Lemma 4.9. *For any two subspaces $S_1, S_2 \subseteq$ PG$(k-1, q)$, we have*

$$\text{dim}(S_1 \oplus S_2) = \text{dim}(S_1) + \text{dim}(S_2) - \text{dim}(S_1 \cap S_2).$$

If the dimension formula is applied to any two distinct lines ℓ_1, ℓ_2 in a projective plane, we get

$$\text{dim}(\ell_1 \oplus \ell_2) = 2 - \text{dim}(\ell_1 \cap \ell_2).$$

Since ℓ_1, ℓ_2 are distinct, the subspace $\ell_1 \oplus \ell_2$ must strictly contain ℓ_1 and so dim$(\ell_1 \oplus \ell_2) > 1$. But the dimension of the projective plane is 2, and so we must have dim$(\ell_1 \oplus \ell_2) = 2$. This implies dim$(\ell_1 \cap$

[1] To avoid trivial cases, whenever we talk of the projective space PG$(k-1, q)$, we assume $k \geq 3$.

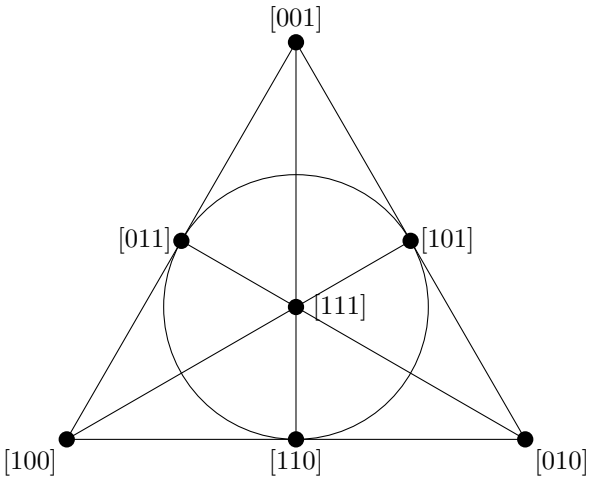


Figure 4.1: PG(2,2) or the Fano plane

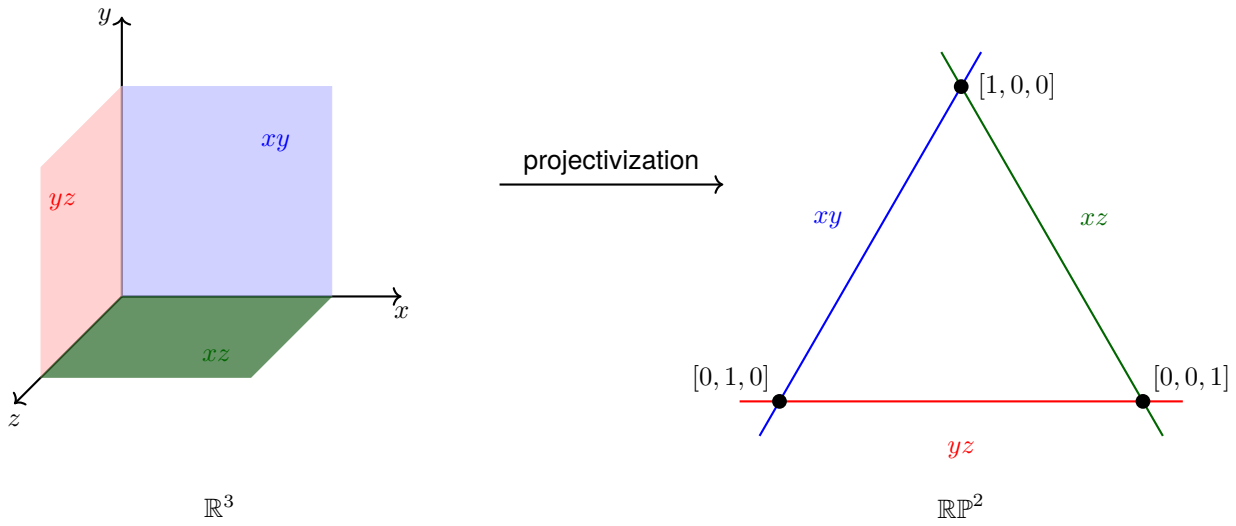


Figure 4.2: Projectivization of $\mathbb{R}^3$ - a line in $\mathbb{R}^3$ passing through the origin represents a point in $\mathbb{RP}^2$ while a plane through the origin represents a line. Thus, the coordinate planes in $\mathbb{R}^3$ represent a triangle in $\mathbb{RP}^2$ upon projectivization.

$\ell_2) = 1$, which leads us to an important observation: **Two distinct lines in a projective plane always intersect.**

For a set of points $S \subseteq \mathsf{PG}(k-1,q)$, the subspace formed by taking the linear span of the points in S is often denoted as $\langle S\rangle$. Abusing notation, for two subsets of points $S, T \subseteq \mathsf{PG}(k-1,q)$, $\langle S, T\rangle$ is used to denote the subspace $\langle S \cup T\rangle$. Note that if $S \leq \mathsf{PG}(k-1,q)$ is already a subspace, then $\langle S\rangle = S$.

These two notations can be reconciled by observing that for two subsets $S, T \subseteq \mathsf{PG}(k-1,q)$, we have $\langle S\rangle \oplus \langle T\rangle = \langle S, T\rangle$. The dimension formula can then be stated as

$$\mathsf{dim}(\langle S, T\rangle) = \mathsf{dim}(\langle S\rangle) + \mathsf{dim}(\langle T\rangle) - \mathsf{dim}(\langle S\rangle \cap \langle T\rangle).$$

The book [Cas06] serves as a standard reference in projective geometry.

Definition 4.6. For integers $0 \leq s \leq k$, the $q-$*binomial coefficient* is defined as:

$$\begin{bmatrix} k \\ s \end{bmatrix}_q = \frac{\left(q^k-1\right)\left(q^{k-1}-1\right)\cdots\left(q^{k-s+1}-1\right)}{\left(q^s-1\right)\left(q^{s-1}-1\right)\cdots(q-1)}$$

where the empty product is defined to be 1 and for other values of s and k, the coefficient is defined to be 0.

The quantity $\begin{bmatrix} k \\ s \end{bmatrix}_q$ is also known as the Gaussian coefficient. It is easy to see that $\begin{bmatrix} k \\ s \end{bmatrix}_q = \begin{bmatrix} k \\ k-s \end{bmatrix}_q$.

The following lemma illustrates the need for using this coefficient in the context of projective and affine spaces.

Lemma 4.10.

i. The number of codimension-s subspaces of PG$(k-1,q)$ is $\begin{bmatrix} k \\ s \end{bmatrix}_q$.

ii. The number of s-dimensional affine subspaces of $\mathbb{F}_q^k$ is equal to $q^{k-s}\begin{bmatrix} k \\ s \end{bmatrix}_q$.

Proof. *i.* The number of codimension-s subspaces of $\mathsf{PG}(k-1,q)$ is the same as the number of codimension-s linear subspaces of $\mathbb{F}_q^k$ (since we have remarked before that the codimensions of subspaces remain the same on projectivization). Since a codimension-s subspace in $\mathbb{F}_q^k$ has dimension $k-s$, we calculate the number of $(k-s)$-dimensional subspaces of $\mathbb{F}_q^k$ by its basis. For choosing the first vector v in the basis, we have $q^k - 1$ choices ($\mathbb{F}_q^k \setminus \mathbf{0}$). To choose the second linearly independent vector, we need to avoid all multiples of v and thus are left with $(q^k - q)$ choices. By a similar argument of choosing linearly independent vectors repeatedly, we get that there are $(q^k-1)(q^k-q)(q^k-q^2)\ldots(q^k-q^{k-s-1})$ ways of choosing a (ordered) basis. However, out of these, many represent the same linear subspace. To calculate the number of (ordered) basis which give the same $(k-s)$-dimensional space, we use the same method as before and get $(q^{k-s}-1)(q^{k-s}-q)(q^{k-s}-q^2)\ldots(q^{k-s}-q^{k-s-1})$. This implies that the number of codimension-s subspaces of $\mathsf{PG}(k-1,q) = \frac{(q^k-1)(q^k-q)\ldots(q^k-q^{k-s-1})}{(q^{k-s}-1)(q^{k-s}-q)\ldots(q^{k-s}-q^{k-s-1})}$, which can be reduced to $\frac{(q^k-1)(q^{k-1}-1)\ldots(q^{s+1}-1)}{(q^{k-s}-1)(q^{k-s-1}-1)\ldots(q-1)} = \begin{bmatrix} k \\ k-s \end{bmatrix}_q$ which is equal to $\begin{bmatrix} k \\ s \end{bmatrix}_q$, as noted before.

ii. From *i.*, the number of s-dimensional subspaces of $\mathbb{F}_q^k$ is equal to $\begin{bmatrix} k \\ k-s \end{bmatrix}_q = \begin{bmatrix} k \\ s \end{bmatrix}_q$. An s-dimensional affine space is obtained by translating an s-dimensional linear subspace $S \leq \mathbb{F}_q^k$ by a vector $v \in \mathbb{F}_q^k$. Since the two affine spaces $S + v$ and $S + v'$ are the same if and only if there exist $s, s' \in S$ such that $s + v = s' + v'$, we get that the same affine subspace is generated by $|S| = q^s$ many vectors. Since there are q^k choices for choosing a vector $v \in \mathbb{F}_q^k$, we get that the number of affine subspaces generated from a fixed s-dimensional linear subspace is $q^k/q^s = q^{k-s}$. Hence, the total number of s-dimensional affine subspaces of $\mathbb{F}_q^k$ is equal to $q^{k-s}\begin{bmatrix} k \\ s \end{bmatrix}_q$.

□

The following estimates on Gaussian coefficients will be used later. The proof of this lemma can be found in [BDGP24].

Lemma 4.11. *Let q be a prime power and $1 \leq s \leq k$ be integers. Then the following holds,*

$$1 \leq q^{-s(k-s)}\begin{bmatrix} k \\ s \end{bmatrix}_q \leq \frac{q}{q-1}e^{\frac{q}{(q^2-1)(q-1)}}.$$

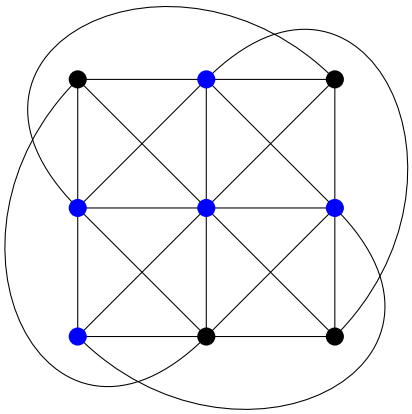


Figure 4.3: A 1-blocking set in $\mathbb{F}_3^2$ denoted by blue points

4.4.2. Background on Blocking Sets

A blocking set in a projective or affine space is a set of points which intersects every subspace of a fixed dimension. The problem of finding blocking sets was first introduced by Richardson [Ric56] who referred to such sets in projective spaces as *blocking coalitions*, since he studied them from a game-theoretic perspective. The study of blocking sets has now become a well-known topic in finite geometry. It finds various applications in the fields of coding theory, combinatorics as well as computer science.

A *strong blocking set* refers to a stronger notion than that of a blocking set. It is a set of points that not only asks for the intersection with every fixed-dimension subspace to be non-empty but rather for it to span the entire subspace.

As an example, consider any projective plane. Since any two lines in a projective plane intersect, the set of points on any fixed line forms a blocking set for all lines (subspaces of codimension-1) in the projective plane. Similarly, it is easy to check that the set of points lying on three non-concurrent lines forms a strong blocking set for all lines in the projective plane.

Strong blocking sets have been recently shown to be equivalent to minimal codes in coding theory [ABN22]. This has also renewed the interest in studying these objects.

In this section, we provide a brief background and a small literature review of blocking and strong blocking sets, and later formalize the connections between strong blocking sets, minimal codes and linear trifferent codes. For a more detailed overview of results in this area, refer to [BSS12, BDGP24].

Definition 4.7. For, $0 \leq s \leq k$, an (affine) *s-blocking set* in $\mathbb{F}_q^n$ is a set of points that has a non-empty intersection with every affine subspace of dimension $k - s$.

Example 4.4. Consider the 1-blocking set in the affine plane $\mathbb{F}_3^2$ shown in Figure 4.3.

Let $b_q(k, s)$ denote the smallest possible size of an s-blocking set in $\mathbb{F}_q^k$.

If we consider the case $q = 3$ and $s = k-1$, then we require the $(k-1)$-blocking set to intersect every line in $\mathbb{F}_3^k$. This means that the complement of the $(k-1)$-blocking set cannot contain a line. However, for $q = 3$, each line only contains three points which means that the complement cannot contain any three points in a line. Recall that such a set $A \subseteq \mathbb{F}_3^k$ which does not contain any three collinear points is called a *cap set*. Then the complement of a $(k-1)$-blocking set must be a cap set in $\mathbb{F}_3^k$. So, if $r_3(\mathbb{F}_3^k)$ denotes the maximum size of a cap set in $\mathbb{F}_3^k$, we must have $b_3(k, k-1) = 3^k - r_3(\mathbb{F}_3^k)$. For the particular case $k = 2$ (illustrated in Figure 4.3), it is known that $r_3(\mathbb{F}_3^2) = 4$ and so, we must have $b_3(2, 1) = 5$. Some other known values of the maximum cardinalities of cap sets include $r_3(\mathbb{F}_3^3) = 9, r_3(\mathbb{F}_3^4) = 20$ [Pel70] and $r_3(\mathbb{F}_3^5) = 45$ [Hil73]. These give rise to the values $b_3(3, 2) = 18$, $b_3(4, 3) = 61$ and $b_3(5, 4) = 198$ respectively.

Bishnoi et.al. [BDGP24] proved the following upper bounds for the general quantity $b_q(k, s)$. We provide a proof for the case $q = 2$. The proof of the other case $q \geq 3$ is along similar probabilistic arguments but requires use of non-trivial inequalities and much more careful counting and so we avoid it here.

Theorem 4.12. *Let s, k be integers such that $2 \leq s \leq k$ and let q be a prime power. If $q = 2$, then*

$$b_q(k,s) \leq \frac{s(k-s)+s+2}{\log_q \frac{q^s}{q^s-1}} + 1.$$

If $q \geq 3$,

$$b_q(k,s) \leq (q^s-1) \cdot \frac{s(k-s)+s+2}{\log_q \frac{q^4}{q^3-q+1}} + 1$$

Proof. ($q = 2$). Suppose B is a set of t points in $\mathbb{F}_2^k$ chosen uniformly and independently at random. We will calculate the probability that P is an s-blocking set. Let $U \subseteq \mathbb{F}_2^k$ be an arbitrary affine subspace of codimension-s. Then the probability that B does not intersect with U is

$$\begin{aligned}
\mathbb{P}(B \cap U = \emptyset) &= \mathbb{P}\Big(\bigcap_{p \in B} (p \notin U) \Big) \\
&= \prod_{p \in B} \mathbb{P}(p \notin U) \\
&= \prod_{p \in B} (1 - \mathbb{P}(p \in U)) \\
&= \left(1 - \frac{|U|}{|\mathbb{F}_2^k|}\right)^{|B|} \\
&= \left(1 - \frac{2^{k-s}}{2^k}\right)^t \\
&= \left(1 - 2^{-s}\right)^t.
\end{aligned}$$

The probability that B is not a blocking set is equal to the probability that there exists a codimension-s subspace of $\mathbb{F}_q^k$ which does not intersect with B and can be calculated as

$$\begin{aligned}
\mathbb{P}(B \text{ is not a blocking set}) &= \mathbb{P}\Big(\bigcup_{\substack{U:\text{affine} \\ \text{codim-}s}} (B \cap U = \emptyset) \Big) \\
&\leq \mathbb{P}\Big(\sum_{\substack{U:\text{affine} \\ \text{codim-}s}} (B \cap U = \emptyset) \Big) \\
&= \left(1 - 2^{-s}\right)^t \cdot |\{U \subseteq \mathbb{F}_2^k \mid U \text{ is an affine codim-}s \text{ subspace}\}| \\
&= 2^s \begin{bmatrix} k \\ k-s \end{bmatrix}_q \left(1 - 2^{-s}\right)^t \\
&= 2^s \begin{bmatrix} k \\ s \end{bmatrix}_q \left(1 - 2^{-s}\right)^t.
\end{aligned}$$

We want this probability to be strictly less than 1 so that there is a positive probability that B is a blocking set.

From Lemma 4.11, we have

$$\begin{aligned}
2^s \begin{bmatrix} k \\ s \end{bmatrix}_q \left(1 - 2^{-s}\right)^t &\leq 2^s 2^{s(k-s)} \frac{2}{2-1} e^{\frac{2}{(2^2-1)(2-1)}} \left(1 - 2^{-s}\right)^t \\
&= 2^{s(k-s)+s+1} e^{2/3} \left(1 - 2^{-s}\right)^t.
\end{aligned}$$

So, if the quantity on the right hand side of the above equation is less than 1, there is a positive probability that B is a blocking set.

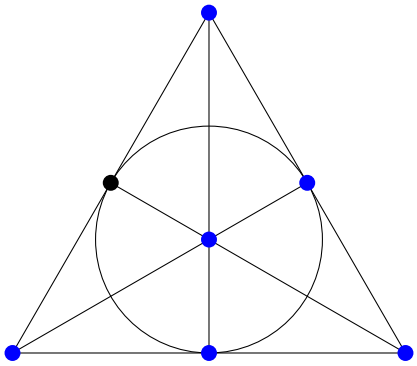


Figure 4.4: A strong blocking set for PG(2,2) or the Fano plane, denoted by blue points

$$
\begin{aligned}
& 2^{s(k-s)+s+1} e^{2/3} \left(1-2^{-s}\right)^t < 1 \\
& \quad \iff \left(1-2^{-s}\right)^t < 2^{-s(k-s)-s-1} e^{-2/3} \\
& \quad \iff t \log_2 \frac{2^s-1}{2^s} < -s(k-s)-s-1-2/3 \log_2 e \\
& \quad \impliedby t \log_2 \frac{2^s}{2^s-1} \geq s(k-s)+s+2 \qquad (\because 2/3 \log_2 e < 1) \\
& \quad \iff t \geq \frac{s(k-s)+s+2}{\log_2 \frac{2^s}{2^s-1}}.
\end{aligned}
$$

Therefore, there is a positive probability of choosing a set of points of size $\left\lceil \frac{s(k-s)+s+2}{\log_2 \frac{2^s}{2^s-1}} \right\rceil$ and it being an affine s-blocking set, which proves that there exists a collection of points of the same size which is an affine s-blocking set in $\mathbb{F}_2^k$ and we are done. □

We now define blocking and strong blocking sets for projective spaces.

Definition 4.8. For $0 \leq s \leq k-1$, an s-blocking set in PG$(k-1,q)$ is a set of points that has a non-empty intersection with every codimension-s subspace of PG$(k-1,q)$. For $s=1$, such sets are simply called blocking sets.

Since a blocking set remains a blocking set if any point is added to it, we are more interested in studying *minimal* blocking sets.

Note that in a projective plane, codimension-1 subspaces are lines and since any two lines intersect, the set of points on a fixed line naturally form a blocking set. A blocking set of PG$(2,q)$ is called *trivial* if it contains a line.

It was observed by von Neumann and Morgenstern [NM44] that there are no non-trivial blocking sets in the Fano plane. Richardson [Ric56] later showed that any non-trivial blocking set in PG$(2,q)$ must have size greater than $q+1$, which is the number of points on a line in PG$(k-1,q)$. Hence the set of points on a line forms the smallest blocking set for PG$(2,q)$ for every prime power q.

For a more detailed overview of s-blocking sets in projective spaces, refer to [BSS12].

Definition 4.9. A set of points in PG$(k-1,q)$ is called a *strong t-blocking set* if it intersects every codimension-t subspace in a set of points which spans the subspace.

For $t=1$, such sets are simply called *strong blocking sets*.

Example 4.5. Consider a strong blocking set of the Fano plane illustrated in Figure 4.4.

Strong blocking sets have also been studied under the name *generator sets*[FS14] or *cutting blocking sets*[ABNR22] in literature.

Let $b_q^*(k,t)$ denote the smallest possible size of a strong t-blocking set in PG$(k-1,q)$.

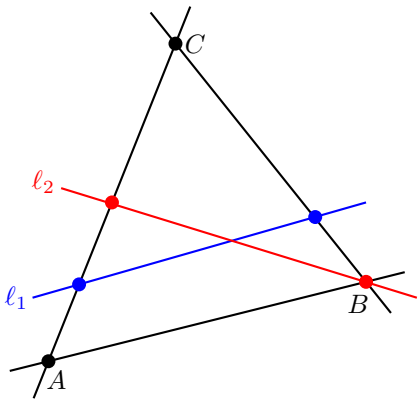


Figure 4.5: $AB \cup BC \cup CA$ forms a strong blocking set in the projective plane PG$(2, q)$.

A line in a projective space is spanned by any two points on it. Since any line in PG(2,2) (which is a hyperplane here) only has three points, each line can have at most one point not in a strong blocking set. Since any two lines in a projective space lie on a line, there can be at most one point not in the strong blocking set for PG(2,2) and thus we have $b_2^*(2,1) = 6$. Other known values, computed using an ILP approach in [BDGP24], include $b_3^*(2,1) = 4, b_3^*(3,1) = 9, b_3^*(4,1) = 14$ and $b_3^*(5,1) = 19$.

The first general bound $b_q^*(k,1) \leq \binom{k}{2}(q-1)+k$ is from the following well-known construction of strong blocking sets in $\mathbb{F}_q^k$: **The union of all lines joining pairs of k points in general position forms a strong blocking set in** PG$(k-1, q)$.

Example 4.6. Consider the projective plane PG$(2, q)$. Then the statement claims that the union of lines joining any three vertices of a triangle in the plane forms a strong blocking set. Since a hyperplane in this context is a line, this just says that the set of lines forming a triangle intersects any line in the plane at least twice. But a simple case analysis (an arbitrary line in PG$(2, q)$ either passes through no vertices of the triangle, one vertex of the triangle or coincides with an edge of the triangle) shows that this is true, as illustrated in Figure 4.5.

Let us first state a lemma which will be useful to prove the statement, stated formally as Proposition 4.14 later.

Lemma 4.13. *Let $p_1, p_2, \ldots, p_k$ be k points in general position in PG$(k-1, q)$ and $S_\mathcal{I}$ denote the subspace $\langle \cup_{i\in\mathcal{I}} p_i \rangle$ for some index set $\mathcal{I} \subseteq \{1, 2, \ldots, k\}$. Then*

i. For any subspace S and a point p, dim$(\langle S, p\rangle) \leq$ dim$(S)+1$. *Further, the inequality is tight if $p \notin S$.*

ii. For an index set $\mathcal{I} \subseteq \{1, 2, \ldots, k\}$, dim$(S_\mathcal{I}) = |\mathcal{I}| - 1$.

iii. For two disjoint index sets $\mathcal{I}, \mathcal{J} \subseteq \{1, 2, \ldots, k\}$, $S_\mathcal{I} \cap S_\mathcal{J} = \emptyset$.

Proof. *i.* Note that $S \cap p \leq p$ and hence dim$(S \cap p) \in \{-1, 0\}$. Further, if $p \notin S$, dim$(S \cap p) = -1$. Applying the dimension formula on $\langle S, p\rangle$ then gives the required result.

ii. If $\mathcal{I} = [k]$, then by definition of points being in general position, dim$(S_\mathcal{I}) = k - 1$. Now consider p_j for some $j \in [k] \setminus \mathcal{I}$. From i., we have

$$\text{dim}(\langle S_\mathcal{I}, p_j\rangle) \leq \text{dim}(S_\mathcal{I}) + 1.$$

Doing this iteratively over all points p_i where $i \in [k] \setminus \mathcal{I}$ gives

$$\text{dim}(\langle S_\mathcal{I}, S_{[k]\setminus\mathcal{I}}\rangle) \leq \text{dim}(S_\mathcal{I}) + |[k] \setminus \mathcal{I}|.$$

Since $S_\mathcal{I} \cup S_{[k]\setminus\mathcal{I}} = \cup_{i\in[k]} p_i$, the dimension of $\langle S_\mathcal{I} \cup S_{[k]\setminus\mathcal{I}}\rangle$ is $(k-1)$ as observed before. So,

$$\begin{aligned} k - 1 &\leq \text{dim}(S_\mathcal{I}) + k - |\mathcal{I}| \\ \implies \text{dim}(S_\mathcal{I}) &\geq |\mathcal{I}| - 1. \end{aligned}$$

Using a similar iterative argument, this time over points p_i for $i \in \mathcal{I}$ and using the fact that the dimension of a point is 0, we also get

$$\dim(S_{\mathcal{I}}) \leq |\mathcal{I}| - 1.$$

Combining the two inequalities finally gives us

$$\dim(S_{\mathcal{I}}) = |\mathcal{I}| - 1.$$

iii. The dimension formula applied on the subspaces $S_{\mathcal{I}}$ and $S_{\mathcal{J}}$ gives

$$\dim(\langle S_{\mathcal{I}}, S_{\mathcal{J}} \rangle) = (|\mathcal{I}| - 1) + (|\mathcal{J}| - 1) - \dim(S_{\mathcal{I}} \cap S_{\mathcal{J}}).$$

Since $S_{\mathcal{I}} \cup S_{\mathcal{J}} = \cup_{i \in \mathcal{I} \cup \mathcal{J}} p_i$, from ii, we get

$$\dim(\langle S_{\mathcal{I}}, S_{\mathcal{J}} \rangle) = |\mathcal{I}| + |\mathcal{J}| - 1.$$

This implies that $\dim(S_{\mathcal{I}} \cap S_{\mathcal{J}}) = -1$, or in other words, $S_{\mathcal{I}} \cap S_{\mathcal{J}} = \emptyset$.

□

Proposition 4.14. *Suppose the points $p_1, p_2, \ldots, p_k \in PG(k-1, q)$ lie in general position. Let $l_{ij} = \langle p_i, p_j \rangle$ denote the unique line passing through points p_i and p_j for any $i, j \in [k]$ with $i \neq j$. Then $B = \cup_{i,j \in [k], i<j} l_{ij}$ is a strong blocking set in PG$(k-1, q)$ of size $\binom{k}{2}(q-1) + k$.*

Proof. Let H be an arbitrary hyperplane in PG$(k-1, q)$, i.e. $\dim(H) = k-2$. It suffices to show that B intersects plane H in at least $k-1$ points in general position (since H has dimension $k-2$, it is generated by any $k-1$ points in general position on it). Equivalently, it suffices to produce a set of points in $B \cap H$ whose direct sum has dimension at least $k-2$.

If H contains $k-1$ of the simplex points, say $p_1, \ldots, p_{k-1}$, then from Lemma 4.13, $\dim(\langle \cup_{i \in [k-1]} p_i \rangle) \geq k-2$ and thus points $p_1, \ldots, p_{k-1} \in B \cap H$ span H and we are done.

So suppose H contains exactly t simplex points for $0 \leq t \leq k-2$, say $p_1, \ldots, p_t$. So, $S_{[t]} \leq H$. Let ℓ be a line in PG$(k-1, q)$. Then $\dim(H \oplus \ell) = k - 2 + 1 - \dim(H \cap \ell)$, and since $\dim(H \oplus \ell) \leq k-1$ (the dimension of the underlying space), we get $\dim(H \cap \ell) \geq 0$. So, each line intersects H in at least one point. Let p_{ij} denote a point of intersection of l_{ij} and H. Then each $p_{ij} \in B \cap H$. Thus it suffices to show that $\dim(\langle \cup_{i,j} p_{ij} \rangle) \geq k-2$.

Since $t \leq k-2$, p_{t+1} exists and $p_{t+1} \notin B$. Consider $\langle (\cup_{i,j} p_{ij}), p_{t+1} \rangle$. From Lemma 4.13,

$$\dim(\langle (\cup_{i,j} p_{ij}), p_{t+1} \rangle) \leq \dim(\langle \cup_{i,j} p_{ij} \rangle) + 1$$

$$\implies \dim(\langle \cup_{i,j} p_{ij} \rangle) \geq \dim(\langle (\cup_{i,j} p_{ij}), p_{t+1} \rangle) - 1.$$

Claim: $\dim(\langle (\cup_{i,j} p_{ij}), p_{t+1} \rangle) = k-1$.
Then this would imply $\dim(\langle \cup_{i,j} p_{ij} \rangle) \geq k-2$, and we are done.
Proof of Claim: We will prove the claim by showing that the space $S = \langle (\cup_{i,j} p_{ij}), p_{t+1} \rangle$ contains each of the points $p_1, p_2, \ldots p_k$. Consider an arbitrary simplex point p_m for some $m \in \{1, \ldots, k\}$. The point $p_{m(t+1)}$ is the intersection of $l_{m(t+1)}$ with H and by definition lies in S. Further $S \ni p_{t+1} \neq p_{m(t+1)}$ since $p_{t+1} \notin H$. Since S is a linear subspace, the subspace $\langle p_{m(t+1)}, p_{t+1} \rangle$ lies in S as well. Since both these points lie on $l_{m(t+1)}$ and there is a unique line passing through two points, $\langle p_{m(t+1)}, p_{t+1} \rangle = l_{m(t+1)}$. But this implies that the point $p_m \in l_{m(t+1)}$ also lies on S. Since m was chosen arbitrarily, we are done.
□

The following lemma, proved in [BDGP24], relates strong blocking sets with affine blocking sets. It is illustrated with an example in Figure 4.6.

Lemma 4.15. *Let $\mathcal{L}$ be a set of points in PG$(k-1, q)$. Then $\mathcal{L}$ is a strong $(s-1)$-blocking set if and only if the set $B = \cup_{\ell \in \mathcal{L}} \ell \subseteq \mathbb{F}_q^k$ is an affine s-blocking set.*

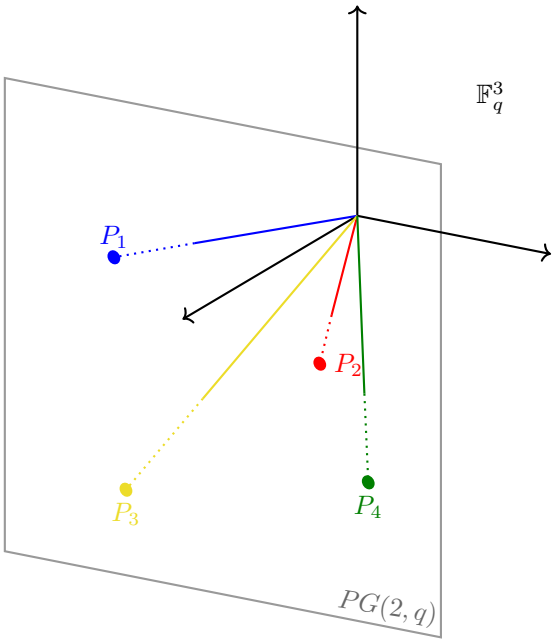


Figure 4.6: Example illustration of Lemma 4.15 - A set of points in PG$(2,q)$ (represented here by $\{P_1,P_2,P_3,P_4\}$) is a strong blocking set if and only if the union of the corresponding lines in $\mathbb{F}_q^3$ forms an affine 2-blocking set, i.e. intersects every line in $\mathbb{F}_q^3$.

Proof. Suppose $\mathcal{L}$ is a strong $(s-1)$-blocking set in PG$(k-1,q)$. Let $U \subseteq \mathbb{F}_q^k$ be a codimension-s subspace and $v \in \mathbb{F}_q^k \setminus U$. Then it suffices to show that $(U+v)\cap B \neq \emptyset$. Let $W \subseteq \mathbb{F}_q^k$ be the codimension-$(s-1)$ subspace spanned by $U \cup \{v\}$. Then W meets $\mathcal{L}$ in a spanning set. Since $\dim(W) > \dim(U)$ and W is spanned by $\mathcal{L}$, there exists $b \in B$ such that $b \in W \setminus U$. This means $b = u + \lambda v$ for some $u \in U$ and $\lambda \neq 0$. Then $b' = \lambda^{-1}b \in B$ since B is a collection of lines. Moreover, $b' \in U + v$ since $b' = \lambda^{-1}(u+\lambda v) = \lambda^{-1}u + v$ and $\lambda^{-1}u \in U$ since U is a linear subspace. Hence $b' \in B \cap (U+v)$ and we are done.

Now, suppose B is an affine s-blocking set in $\mathbb{F}_q^k$ but $\mathcal{L}$ is not a strong $(s-1)$-blocking set in PG$(k-1,q)$. Then there exists H of codimension-$(s-1)$ in PG$(k-1,q)$ such that $H \cap \mathcal{L} \subseteq H'$, where $H' \subsetneq H$ is a subspace of codimension-s in PG$(k-1,q)$. Let $v \in H \setminus H'$. Consider the affine codimension-s subspace $H'+v$ and let $w \in (H'+v)\cap B$ (this is non-empty since B is a blocking set). Then $[w] \in H \setminus H'$ and $[w] \in \mathcal{L}$. But this is a contradiction, since $H \cap \mathcal{L} \subseteq H'$. So, $\mathcal{L}$ must be a strong $(s-1)$-blocking set in PG$(k-1,q)$. □

In lieu of this lemma and Theorem 4.12, Bishnoi et.al. [BDGP24] also managed to improve the then prevailing upper bound for $b_q^*(k,1)$ by proving the following theorem.

Theorem 4.16. *Let $k \geq 2$ be an integer. Then $b_q^*(k,1)$ satisfies*

$$b_q^*(k,1) \leq (q+1) \cdot \frac{2k}{\log_q \frac{q^4}{q^3-q+1}}.$$

Further, Bishnoi et.al. [BDGP24] also proved the following lower bound on the quantity $b_3^*(k,1)$ (they in fact proved a more general result for arbitrary q). Since the proof uses highly non-trivial results from coding theory, we omit it here.

Theorem 4.17. *Every strong blocking set in PG$(k-1,3)$ has size at least $4(c_3 - o(1))(k-1)$, where $o(1)$ only depends on k, and $c_3 > 1.1375$. In other words, $b_3^*(k,1) > 4.55(k-1)$.*

4.4.3. Blocking Sets and Minimal Codes

To see the equivalence between minimal codes and strong blocking sets, we first define certain multi-sets of points in a projective space.

Definition 4.10. A projective $[n,k,d]_q$ system $\mathcal{P}$ is a finite set of n points (counted with multiplicity) of PG$(k-1,q)$ that do not all lie on a hyperplane and such that

$$d = n - \max\{|H \cap \mathcal{P}| : H \subseteq \text{PG}(k-1,q),\ \dim(H) = k-2\}.$$

The following lemma describes a standard correspondence between the equivalence classes of projective $[n,k,d]_q$ systems and the equivalence classes of nondegenerate $[n,k,d]_q$ codes. We follow the proof given by Alfarano et.al. [ABNR22].

Lemma 4.18. *Let $\mathcal{C}$ be a nondegenerate $[n,k,d]_q$ code and let $G = (g_1 \mid g_2 \mid \ldots \mid g_n) \in \mathbb{F}_q^{k\times n}$ be any of its generator matrices. Then the (multi-)set of points $\mathcal{P} = \{[g_1],[g_2],\ldots,[g_n]\}$ in PG$(k-1,q)$ is a projective $[n,k,d]_q$ system.*

Conversely, for $d > 0$, let $\mathcal{P} = \{g_1,g_2,\ldots,g_n\}$ be a projective $[n,k,d]_q$ space (where elements are listed with multiplicity). Then the linear code $\mathcal{C}$ with generator matrix $G = (g_1 \mid g_2 \mid \ldots \mid g_n)$ is a nondegenerate $[n,k,d]_q$ code.

Proof. For the first part, it suffices to show that for the set of points $\mathcal{P}$ in PG$(k-1,q)$, we have

$$\max\{|H \cap \mathcal{P}| : H \subseteq \text{PG}(k-1,q),\ \dim(H) = k-2\} = n - d.$$

Let $x_1,x_2,\ldots,x_k$ be the points in PG$(k-1,q)$ corresponding to the standard basis of $\mathbb{F}_q^k$ and H' be an arbitrary hyperplane of $\mathbb{F}_q^k$ with equation $u_1x_1 + u_2x_2 + \ldots + u_kx_k = 0$. Clearly, its projection H has codimension-1 in PG$(k-1,q)$. Then $|H \cap \mathcal{P}| = |\{i \in [n] : u^T g_i = 0\}|$. Since $u^TG = (u^Tg_1 \mid u^Tg_2 \mid \ldots \mid u^Tg_n)$, $|H \cap \mathcal{P}| = n - w(u^TG)$. This implies

$$\begin{aligned}\max\{|H \cap \mathcal{P}| : H \subseteq \text{PG}(k-1,q),\ \dim(H) = k-2\} &= n - \min\{w(u^TG) : u \in \mathbb{F}_q^k\}\\ &= n - \min\{w(x) : x \in \mathcal{C}\}\\ &= n - d.\end{aligned}$$

For the converse, first note that the all-zero vector is not a point in the projective space and hence the resulting code must be nondegenerate. Now let $u \in \mathbb{F}_q^k$ be an arbitrary vector and let H be the projection of the hyperplane in $\mathbb{F}_q^k$ whose equation is given by $\sum_i u_ix_i = 0$. As argued before, we have $w(u^TG) = n - |H \cap \mathcal{P}|$ and so,

$$\begin{aligned}\min\{w(x) : x \in \mathcal{C}\} &= \min\{w(u^TG) : u \in \mathbb{F}_q^k\}\\ &= n - \max\{|H \cap \mathcal{P}| : H \subseteq \text{PG}(k-1,q),\ \dim(H) = k-2\}\\ &= d.\end{aligned}$$

□

Tang et.al. [TQLZ21] showed that this correspondence extends to provide an equivalence between strong blocking sets and minimal codes.

Theorem 4.19. *Let $\mathcal{C}$ be a non-degenerate $[n,k,d]_q$ code and $G = (g_1 \mid \ldots \mid g_n) \in \mathbb{F}_q^{k\times n}$ be any of its generator matrices. The following are equivalent:*

(i) $\mathcal{C}$ is a minimal code.

(ii) The set $\mathcal{P} = \{[g_1],\ldots,[g_n]\}$ is a strong blocking set in PG$(k-1,q)$.

Proof. For a non-zero vector $u \in \mathbb{F}_q^k$, let H_u denote the projection of the hyperplane of $\mathbb{F}_q^k$ given by the set $\{w \in \mathbb{F}_q^k \mid u^Tw = 0\}$. So, H_u is a hyperplane in PG$(k-1,q)$.

Conversely, suppose $H \subseteq$ PG$(k-1,q)$ is a hyperplane. Then there exists vector $v_H \in \mathbb{F}_q^k$ such that its equation as a hyperplane in $\mathbb{F}_q^k$ is $\sum_i (v_H)_i x_i = 0$, and thus $H = H_{v_H}$.

Suppose $c \in \mathcal{C}$ is a non-zero codeword. Then there exists $v_c \in \mathbb{F}_q^k \setminus \{\mathbf{0}\}$ such that $c = v_c^TG = (v_c^Tg_1 \mid \ldots \mid v_c^Tg_n)$. Thus,

$$\sigma(c) = [n] \setminus \{i \in [n] \mid [g_i] \in H_{v_c} \cap \mathcal{P}\}. \tag{4.2}$$

Again conversely, for any $v \in \mathbb{F}_q^k$, there exists $c_v = v^T G \in \mathcal{C}$ such that

$$\sigma(c_v) = [n] \setminus \{i \in [n] \mid [g_i] \in H_v \cap \mathcal{P}\}. \tag{4.3}$$

(i) $\implies$ (ii) : Suppose $\mathcal{C}$ is a minimal code and $\mathcal{P}$ is not a strong blocking set. Then there exists a hyperplane H of PG$(k-1,q)$ such that $H \cap \mathcal{P} \subseteq H'$, for some $H' < H$, a proper subspace of H of codimension-2.

Suppose $\mathcal{P}$ is a set of size $m \leq n$ (since $\mathcal{C}$ need not be projective). Since G is a full-rank matrix, its columns span $\mathbb{F}_q^k$ and hence $\mathcal{P} \not\subseteq H$. This means that there exists $p \in \mathcal{P}$ which does not lie in H.

Consider the hyperplane $\langle H', p\rangle$. From Lemma 4.13, since $p \notin H'$, dim$(\langle H', p\rangle) =$ dim$(H') + 1 = k-2$ and thus $H_1 := \langle H', p\rangle$ is a hyperplane which is different from H since $p \notin H$. Also by construction, $H_1 \cap \mathcal{P} \supsetneq H \cap \mathcal{P}$. Then (4.3) implies that $\sigma(c_{v_{H_1}}) \subsetneq \sigma(c_{v_H})$. This again contradicts the minimality of $\mathcal{C}$.

(ii) $\implies$ (i) : Suppose $\mathcal{P}$ is a strong blocking set in PG$(k-1,q)$ and $\mathcal{C}$ is not a minimal code. Then there exist non-zero codewords $c, c' \in \mathcal{C}$ such that $\sigma(c) \subseteq \sigma(c')$ and $c \neq \lambda c'$ for any $\lambda \in \mathbb{F}_q^*$. From (4.2), $H_{v_{c'}} \cap \mathcal{P} \subseteq H_{v_c} \cap \mathcal{P}$. Since c, c' are not proportional, $v_c, v_{c'}$ are also not proportional and hence $H_{v_c} \neq H_{v_{c'}}$. This implies that $H_{v_c} \cap H_{v_{c'}}$ is a codimension-2 subspace in PG$(k-1,q)$ which contains $H_{v_{c'}} \cap \mathcal{P}$. This means that $H_{v_{c'}} \cap \mathcal{P}$ does not span $H_{v_{c'}}$, which is in contradiction to $\mathcal{P}$ being a strong blocking set. □

4.4.4. Strong Blocking Sets and Linear Trifferent Codes

In this section, we finally establish a link between strong blocking sets and linear trifferent codes and also state come results arising from this connection.

Combining Theorem 4.19 and Proposition 4.8, we get the following corollary.

Corollary 5. *For all positive integers k, n, we have*

$$T_L(n) \geq 3^k \iff b_3^*(k,1) \leq n.$$

Proof. For the forward direction, let $\mathcal{C} \leq \mathbb{F}_3^n$ be a linear trifferent code of dimension k. Then by Proposition 4.8, $\mathcal{C}$ is an $[n,k]_3$ minimal code. In case G has degenerate columns, remove them. Then from Theorem 4.19, the lines corresponding to the columns of the truncated generator matrix forms a strong blocking set of PG$(k-1,3)$ of size at most n.

For the reverse direction, suppose $\mathcal{P} = \{[g_1], \ldots, [g_n]\}$ is a strong blocking set in PG$(k-1,3)$. From Theorem 4.19, the linear code $\mathcal{C} \leq \mathbb{F}_3^n$ with generator matrix $G = (g_1 \mid \ldots \mid g_n)$ is a minimal code of dimension k and by Proposition 4.8, also a linear trifferent code of dimension k. □

Example 4.7. It is well-known that the value $b_q^*(3,1) = 9$ (also computed in [BDGP24]). From Corollary 5, we get that $T_L(9) \geq 3^3$. This means that there exists a linear trifferent code of length 9 and dimension 3. This equivalence is illustrated in Figure 4.7 by showing how a specific strong blocking set in PG(2,3) of size 9 gives rise to a linear trifference code of dimension 3 and length 9.

Finally, as a consequence of Corollary 5, the following bounds were established in [BDGP24].

Theorem 4.20. *For n large enough, the largest size of a linear trifferent code, $T_L(n)$, has the following bounds -*

$$\frac{1}{3}\left(\frac{9}{5}\right)^{n/4} \leq T_L(n) \leq 3^{\frac{n}{4.55}}. \tag{4.4}$$

Proof. For the lower bound: Theorem 4.16 implies that

$$b_3^*(k,1) \leq \frac{8k}{\log_3(81/25)}.$$

Let $k = \left\lfloor n\frac{\log_3(81/25)}{8} \right\rfloor$. Then $b_3^*(k,1) \leq n$. Corollary 5 then implies that

$$T_L(n) \geq 3^k \geq 3^{n\frac{\log_3(81/25)}{8}-1} \geq \frac{1}{3}3^{\frac{n}{4}\log_3(9/5)} = \frac{1}{3}\left(\frac{9}{5}\right)^{n/4}.$$

For the upper bound: Suppose $\mathcal{C} \leq \mathbb{F}_3^n$ is a largest linear trifferent code of length n and dimension k, i.e. $T_L(n) = 3^k$. From Proposition 4.8, $\mathcal{C}$ is a linear minimal code of dimension k and thus from Theorem

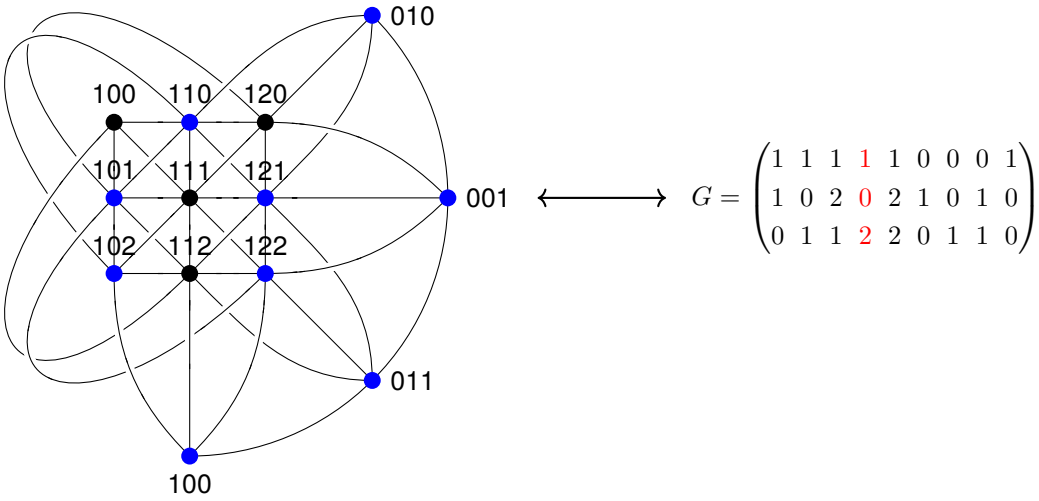


Figure 4.7: A strong blocking set of size 9 in PG(2,3) (denoted by blue points) is equivalent to a linear trifferent code of dimension 3 in $\mathbb{F}_3^9$ with a generator matrix having columns as the points of PG(2,3) belonging to the strong blocking set.

4.19, there is a strong blocking set in PG$(k-1,3)$ of size $m \leq n$, since $\mathcal{C}$ can be made non-degenerate by deleting a finite set of columns from its generator matrix. Hence, we have $b_3^*(k,1) \leq m$. For large enough k, an application of Theorem 4.17 yields $n \geq m > 4.55(k-1)$. This gives $k \leq (n/4.55)$.

□

5
Computational Results

In Chapter 2, we saw that the following bounds have been established for 3-bounded linear trifferent codes after recent significant improvements in both lower and upper bounds -

$$c \times n^{2-o(1)} \leq T_b(n,3) \leq c' \times n^{13/5}.$$

As a result, the asymptotic behaviour of the quantity $T_b(n,3)$ is known to lie in a small exponential-factor window.

However, the same cannot be said for 2-bounded trifferent codes, for which the best known bounds are

$$2n-2 \leq T_b(n,2) \leq c \times n^{5/3}.$$

The lower bound has not been studied beyond this trivially obtained one and hence, there appears to be scope for improving it.

As mentioned before, while better upper bounds on these quantities can directly improve upper bounds on $T(n)$, the lower bounds can help estimate how good an upper bound this method can potentially provide for $T(n)$.

In this chapter, we focus on different formulations to construct 2-bounded trifferent codes of different block lengths in an attempt to improve the lower bound for the quantity $T_b(n,2)$.

We will mostly focus on two main formulations viz., ILP formulation as an independent set problem and SAT formulation.

5.1. ILP Approach

Consider a 3-uniform hypergraph G with vertex set $S_2 := \{v \in \mathbb{F}_3^n : |\{i \in [n] \mid v(i) = 2\}| = 2\}$. In other words, S_2 contains all the ternary vectors of length n in which the symbol 2 appears exactly twice.

Three vectors or codewords $u, v, w \in S_2$ form a hyperedge $(u,v,w) \in E(G)$ if they do not satisfy the trifference condition, i.e. if for each coordinate $i \in [n], \{u(i), v(i), w(i)\} \subsetneq \mathbb{F}_3$.

Then an independent set in this graph contains no three codewords which violate the trifference condition and hence corresponds to a trifferent code.

Thus, $T_b(n,2) = \alpha(G)$, where $\alpha(G)$ denotes the *independence number* or the size of a largest independent set in graph G. This enables us to now use the following well-known ILP formulation to compute the independence number of this graph for a fixed n.

Suppose $x_1, \ldots, x_{|V(G)|}$ (where $V(G) = S_2$) are binary variables representing each vertex and therefore each 2-bounded ternary vector. The variable x_i is assigned value 1 if the corresponding codeword in S_2 lies in the trifferent code $\mathcal{C}$ corresponding to a largest independent set of G.

Then the ILP formulation to compute the independence number of G and thus the value $T_b(n,2)$ is

$$\begin{aligned} \alpha(G) \quad = \quad & \max \quad \sum_{i=1}^{|V(G)|} x_i & \\ & \text{s.t.} \quad x_u + x_v + x_w \leq 2 & \forall (u,v,w) \in E(G) \\ & \qquad x_i \in \{0,1\} & \forall i \in \{1, \ldots, |V(G)|\} \end{aligned}$$

Using this computational approach, we obtain the optimal values, $T_b(4,2) = 6$ and $T_b(5,2) = 10$. [1]

[1] We used a basic Gurobi ILP optimization algorithm on a local computer for these computations.

However, for $n > 5$, this approach becomes intractable. This is due to multiple reasons. Firstly, this ILP computation is known to be NP-hard since finding the independence number of a graph is NP-hard [Kar09], and even for $n = 6$, the number of edges in G are close to $500,000$. Secondly, for such a large problem, this computation is riddled with a lot of redundancy arising from the highly symmetric nature of the problem. This causes the program to not even compute the value $T_b(6, 2)$ optimally.

While in theory, we can introduce many more constraints to enforce the symmetry in the structure and speed up the computations, we thought of using an entirely different approach which inherently takes into account the specific requirements and symmetries of our problem.

This approach of using a SAT solver, is explained in the following section.

5.2. SAT Approach

Let us first see a small example to understand how the trifference condition can be modeled into a satisfiability problem.

Example 5.1. Let $u, v, w \in \mathbb{F}_3^5$ be 2-bounded ternary vectors and assume it is known in which coordinates 2s are present in each of the codewords x, y, z. Suppose $u(1) = u(2) = 2$, $v(1) = v(3) = 2$ and $w(4) = w(5) = 2$. Then the three codewords look like

$$\begin{array}{ccccc} 2 & 2 & x_1 & x_2 & x_3 \\ 2 & x_4 & 2 & x_5 & x_6 \\ x_7 & x_8 & x_9 & 2 & 2 \end{array}$$

Note that each of the x_i's can only be either 0 or 1 (since the codewords are 2-bounded) and can thus be treated as boolean variables. Clearly, it is only possible to achieve trifference in the coordinates where a single 2 is present. In this case, it can only happen in either the second, third or fourth coordinates. For trifference to occur in one of these coordinates, one of the binary symbols must be 0 and the other must be 1. In other words, the XOR of both the boolean variables must be true. Then for the three codewords to be trifferent, at least one of the XOR's of the two boolean symbols present in each of the coordinate where a single 2 occurs, must be true.

In the example, this translates to the following logical statement:

$$(x_4 \text{ XOR } x_8) \text{ OR } (x_1 \text{ XOR } x_9) \text{ OR } (x_2 \text{ XOR } x_5),$$

which is written more formally as

$$\Big((x_4 \wedge \neg x_8) \vee (\neg x_4 \wedge x_8)\Big) \vee \Big((x_1 \wedge \neg x_9) \vee (\neg x_1 \wedge x_9)\Big) \vee \Big((x_2 \wedge \neg x_5) \vee (\neg x_2 \wedge x_5)\Big).$$

This can be easily turned into a statement in conjunctive normal form (required by SAT solvers) by applying distributivity and de Morgan's laws.

5.2.1. Graph of a 2-bounded trifferent code

As motivated by the example above, to compute 2-bounded trifferent codes of a fixed length, we wish to have information about the coordinates in which 2s occur in each codeword.

Since we are dealing with 2-bounded trifferent codes, this information can be captured by a graph having the coordinates from 1 to n as the set of vertices and each edge representing a codeword with the 2s present in the coordinates corresponding to its endpoints.

As argued before, at most 2 codewords in a trifferent code can have 2s at the same set of coordinates and so we allow edges in this graph to have either weight 1 or weight 2, depending on whether that edge corresponds to 1 or 2 codewords in the code.

Further, if there exists a triangle in the graph, then any three codewords corresponding to these three edges violate the trifference condition (since 2s are repeated in each coordinate that they occur in) and hence the code cannot be trifferent. So, we require the graph to be triangle-free, or K_3-free.

We will now describe how we used this approach to compute some 2-bounded trifferent codes of various block lengths.

5.2.2. SAT Formulation

Let G be a K_3-free graph on n vertices, with edge weights 1 or 2. Let $L(G) = (e_1, \ldots, e_m)$ be a list of edges of G, where an edge of weight 2 is counted twice. Further for each $e_i \in L$, let c_i denote the corresponding codeword. Let $x_{i,p}$ denote the boolean variable representing the symbol present in coordinate p of c_i. If $e_i = (u_i, v_i)$, then the variables x_{i,u_i}, x_{i,v_i} do not exist since 2s are present in those coordinates. Thus there are exactly $n-2$ such variables for each codeword and $m(n-2)$ total boolean variables.

For each combination of three codewords c_i, c_j, c_k where $i, j, k \in \{1, \ldots, m\}$, denote by S'_{ijk} the (multi)set of coordinates given by the endpoints of e_i, e_j and e_k.

Then let $S_{ijk} \subseteq S'_{ijk}$ be the set of coordinates in S'_{ijk} which occur only once, or which occur with multiplicity one. This means each element in S_{ijk} is a vertex of G contributed by exactly one of e_i, e_j or e_k. So, for $s \in S_{ijk}$, let $\sigma_s \in \{i, j, k\}$ indicate which edge out of e_i, e_j or e_k has vertex s as an endpoint and τ_s, ω_s represent the other two indices present in $\{i, j, k\} \setminus \sigma(s)$ (the order of τ_s or ω_s does not matter).

Example 5.2. Suppose $n = 5$ and the three codewords c_i, c_j, c_k correspond to edges $e_i = (2, 4), e_j = (2, 3)$ and $e_k = (1, 4)$, then the multiset $S_{ijk} = \{1, 2, 2, 3, 4, 4\}$ and the set $S_{ijk} = \{1, 3\}$. Further, $\sigma(1) = k$, $\tau_1 = i$ or j, $\omega_1 = \{i, j\} \setminus \{\tau_1\}$ and $\sigma(3) = j$.

Then the trifference condition may only be satisfied at one of the coordinates in the set S_{ijk}.

Similar to the illustration in Example 5.1, the trifference condition for codewords c_i, c_j, c_k can be stated as

$$\text{OR}_{\, s \in S_{ijk}} \left(x_{\tau_s, s} \text{ XOR } x_{\omega_s, s} \right).$$

The logical statement to ensure that the graph G represents a 2-bounded trifferent code may then be written as

$$\text{AND}_{e_i, e_j, e_k \in L(G)} \text{ OR}_{\, s \in S_{ijk}} \left(x_{\tau_s, s} \text{ XOR } x_{\omega_s, s} \right). \tag{5.1}$$

Thus, given a K_3-free graph G on n vertices with edge weights 1 or 2, and sum of edge weights m, if a SAT solver provides a solution to (5.1), it implies that there exists a 2-bounded trifferent code of size m and block length n.

In the next section, we state some computational results obtained by SAT solvers[2] for constructing trifferent codes of different block lengths.

5.2.3. Results from SAT Formulation

In Table 5.1, we list new lower bounds of $T_b(n, 2)$ obtained for different values of n and also describe the underlying graph used for constructing the 2-bounded trifferent code of that size.

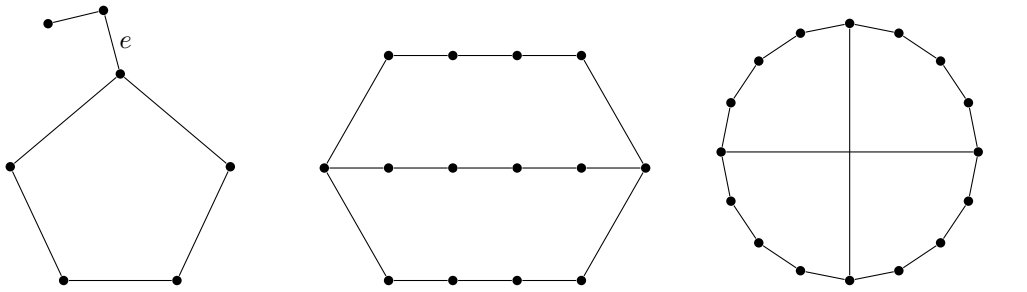
Here, C_n and P_n denote the cycle graph and path graph on n vertices, respectively. $K_{s,t}$ denotes the complete bipartite graph with sizes of sets in the bipartition s and t. Finally, $\Theta(n_1, n_2, \ldots, n_m)$ denotes a *Theta graph*, having m paths $P_{n_1+2}, P_{n_2+2}, \ldots, P_{n_m+2}$ each having the same two vertices as their endpoints, and all the other vertices disjoint from each other. As an example, the cycle C_6 may also be denoted as $\Theta(2, 2)$. The shorthand notation $\Theta(n^m)$ describes the Theta graph $\Theta(n, n, \ldots, n)$ with n appearing m times.

To better understand the notation in Table 5.1, we illustrate some of the graphs in Figure 5.1.

[2] We used pysat on a local computer to obtain these results.

n	(2n - 2)	Size of trifferent code	Graph G	Edge weights
5	8	10 (2n)	C_5	All 2
6	10	11 (2n-1)	$C_5 + P_2$ sharing common vertex	Non-cyclic edge 1, rest 2
7	12	13 (2n-1)	$C_5 + P_3$ sharing common vertex	Joining edge of P_3 1, rest 2
8	14	16 (2n)	C_8	All 2
9	16	18 (2n)	C_9	All 2
		20 (2n+2)	$K_{4,5}$	All 1
10	18	20 (2n)	C_{10}	All 2
		22 (2n+2)	Random 22-edge subgraph of $K_{5,5}$	All 1
12	22	24 (2n)	C_{12}	All 2
		26 (2n+2)	Random 26-edge subgraph of $K_{6,6}$	All 1
14	26	28 (2n)	C_{14}	All 2
		30 (2n+2)	$\Theta(4^3)$	All 2
		31 (2n+3)	$C_{14}+$ edges $(1,8),(5,11)$	$(5,11)$ 1, rest 2
16	30	32 (2n)	C_{16}	All 2
		36 (2n+4)	$C_{16}+$ edges $(1,9),(5,13)$	All 2
18	34	36 (2n)	C_{18}	All 2
		40 (2n+2)	$\Theta(4^4)$	All 2
22	42	44 (2n)	C_{22}	All 2
		50 (2n+6)	$\Theta(4^5)$	All 2

Table 5.1: Table detailing new lower bound values of $T_b(n,2)$ for different n given by SAT solver



(a) $C_5 + P_3$ sharing common vertex with e being the 'joining edge of P_3'

(b) Graph $\Theta(4,4,4)$ or $\Theta(4^3)$

(c) $C_{16}+$ edges $(1,9)$ and $(5,13)$

Figure 5.1: Some graphs appearing in Table 5.1

6

New Lower Bounds

In the section, we first analyze the computational results stated in Table 5.1 and then use them to construct 2-bounded trifferent codes. We provide two new constructions, both of which improve the current bound of $T_b(n, 2) \geq 2n - 2$.

6.1. Discussion of Computational Results

The first key observation that we see in the table is that for every $n > 4$, the lower bound of $2n - 2$ is not tight. Interestingly, the cycle graph on n vertices with each edge representing two codewords, gives a 2-bounded trifferent code of length n and size $2n$ for every $n > 7$ that was able to be computed (up to $n = 24$). This strongly suggests that the lower bound of $2n - 2$ can be improved upon. In fact, we exploit this cycle graph structure with all edge weights 2 in Construction 1.

The next observation from the table is that the best computational lower bound can be written in the form $2n + c$, where c increases with n. This also suggests that the constant 2 might not be the best constant for a linear lower bound.

In fact, if we were to consider 2-bounded trifferent codes of length $n = 4t + 2$, then the graph $\Theta(4^t)$ with all edge weights two seems to always provide a trifferent code of length $2n + 2(t - 2)$. This has been verified computationally for $t = 2, 3, \ldots, 8$. If this were to be true, the lower bound obtained from this for $T_b(n, 2)$ when $n = 4t + 2$, would be $(5/2)n - 5$.

Apart from the Theta graphs, even the cycle graph on n vertices in which some diagonals are added as n gets large, seem to provide lower bounds of the form $2n + c$, where c seems to increase as more diagonal edges can be added for increasing n. However, this is computationally very slow to verify and we were not able to show this beyond $n = 16$.

Interestingly, the graphs obtained from randomly sampling edges with weight 1 from the complete equi-bipartite graph seem to provide the best lower bound values for $n = 9, 10, 11$ and 12. Since the computation is much slower when the edge weights are 1, for $n > 13$, we cannot compute a lower bound using this method. However, the better results obtained from these graphs does indicate that the best constructions for lower bounds can also be obtained when each codeword has a unique pair of coordinates corresponding to the positions of 2 in it. We exploit this in Construction 2.

6.2. Construction 1

Inspired by the fact that the cyclic graph with all edge weights 2 always seems to give a trifferent code of size $2n$ computationally, Anurag Bishnoi and Jozefien D'haeseleer came up with a construction of size $2n$ for $n = 3m + 2$, for all $m > 0$. Their construction was all n cyclic shifts of the 2 codewords $c_0 = (22\ 110\ 110\ \cdots\ 110)$ with 110 appearing m times and $d_0 = (22\ 011\ 011\ \ldots\ 011)$, with 011 appearing m times. We were then able to prove the same linear bound for $n \equiv 1 \pmod 3$ and $n \equiv 0 \pmod 3$. As a result of this construction, we obtain the new bound $T_b(n, 2) \geq 2n$.

We present this construction and the proof of trifference of these codes in the following theorem.

Theorem 6.1. *For $n = 5, 8, 10, 11$ and $n \geq 13$, we have $T_b(n, 2) \geq 2n$.*

Proof. We will prove this statement in three cases:

Case I: **$n \equiv 2 \pmod 3$ and $n \geq 5$**
Let $n = 3m + 2, m \geq 1$. Consider the set of $2n$ 2-bounded codewords

$\mathcal{C}_n = \{c_0, c_1, \ldots, c_{n-1}, d_0, d_1, \ldots, d_{n-1}\} \subseteq \mathbb{F}_3^n$ obtained by the n cyclic shifts of the two codewords:

$$c_0 = 22\ \underbrace{110\ 110\ \cdots\ 110}_{m \text{ times}}$$
$$d_0 = 22\ \underbrace{011\ 011\ \cdots\ 011}_{m \text{ times}}$$

This set of codewords can also be defined coordinate-wise[1] as[2]:

$$c_i(j) = \begin{cases} 2 & \text{if } j = i, i+1; \\ 1 & \text{if } j = i + (3h-1), i+3h \text{ for } h = 1, \ldots, m; \\ 0 & \text{if } j = i + (3h+1) \text{ for } h = 1, \ldots, m. \end{cases}$$
$$d_i(j) = \begin{cases} 2 & \text{if } j = i, i+1; \\ 1 & \text{if } j = i + 3h, i + (3h+1) \text{ for } h = 1, \ldots, m; \\ 0 & \text{if } j = i + (3h-1) \text{ for } h = 1, \ldots, m. \end{cases}$$

for all $i, j \in \{0, 1, \ldots, n-1\}$.

Example 6.1. For $n = 5$, the code $\mathcal{C}_5$ is the set of codewords $\{c_0, c_1, c_2, c_3, c_4, d_0, d_1, d_2, d_3, d_4\} = \{22110, 02211, 10221, 11022, 21102, 22011, 12201, 11220, 01122, 20112\}$.

We will now prove, by case analysis, that $\mathcal{C}_n$ is a trifferent code. To make matters simpler, we make the following observation first:

Lemma 6.2. *The three codewords $c_i, c_j, c_k \in \mathcal{C}_n$ (or c_i, c_j, d_k) are trifferent if and only if the codewords $c_0, c_{j-i}, c_{k-i} \in \mathcal{C}_n$ (or c_0, c_{j-i}, d_{k-i}) are trifferent.*

This is true due to the cyclic nature of the construction since the codewords c_i, c_j, c_k are trifferent at coordinate ℓ if and only if the codewords c_0, c_{j-i}, c_{k-i} are trifferent at coordinate $\ell - i$.

To prove $\mathcal{C}_n$ is trifferent, consider three arbitrary codewords $x, y, z \in \mathcal{C}_n$. Following cases arise:

(i) $x = c_i, y = d_i, z = c_j$ or d_j. Due to Lemma 6.2, this is the same as checking the case $x = c_0, y = d_0, z = c_k$ or d_k for some $k > 0$:
If $k = 1$ or $n-1$, then the three codewords are trifferent at coordinate 2 or $n-1$ respectively, since by construction, both the sets $\{c_0(2), d_0(2)\}$ and $\{c_0(n-1), d_0(n-1)\}$ are equal to $\{0, 1\}$, while $c_1(2) = d_1(2) = 2$ and $c_{n-1}(n-1) = d_{n-1}(n-1) = 2$.
For any other k, the symbols at the coordinates k and $k+1$ for codewords c_0, d_0 are either 0 or 1 and by construction, either $\{c_0(k), d_0(k)\} = \{0, 1\}$ or $\{c_0(k+1), d_0(k+1)\} = \{0, 1\}$. By definition, 2 occurs in both these coordinates for both c_k and d_k, and so we are done.

(ii) $x = c_i, y = c_{i'}, z = c_{i''}$ with $i < i' < i''$. Following exhaustive subcases arise due to the cyclic nature of the construction:

(a) All pairs of 2s in the three codewords are disjoint:
By Lemma 6.2, we may assume $x = c_0, y = c_j, z = c_k$ with $2 < j+1 < k < n-1$. For illustration, the three codewords look something like:

$$c_0 = 22110110\ldots$$
$$c_j = \ldots 22110110\ldots$$
$$c_k = \quad \ldots 11022110\ldots$$

If in either coordinate j or $j+1$, we have different symbols in the codewords c_0 and c_k, then trifference is achieved in that coordinate and we are done. So assume $c_0(j) = c_k(j)$ and $c_0(j+1) = c_k(j+1)$. But for consecutive binary symbols to be the same in these two codewords, it is easy to see that the construction forces $k = 3m' + 2$ for some $m' > 0$.

[1] For the sake of convenience, coordinates here are defined starting from 0 and going up to $n-1$.
[2] Note that henceforth, addition and subtraction pertaining to codeword indices and coordinates will always be modulo n.

By similar logic, if in either coordinate k or $k+1$, we have different symbols in the codewords c_0 and c_j, then trifference is achieved in that coordinate and we are done. So again assume $c_0(k) = c_j(k)$ and $c_0(k+1) = c_j(k+1)$. By a similar argument as before, this can only happen if $j = 3m''$ for some $m'' > 0$.
However, with these class of values of j, k, we must have $c_j(0) = c_j(1) = 1, c_k(0) = 1, c_k(1) = 0$ and so trifference is achieved in coordinate 1, as shown in Example 6.2.

Example 6.2. Suppose $n = 11, j = 3, k = 8$. Then the three codewords look like

$$c_0 = 22110110110,$$
$$c_3 = 11022110110,$$
$$c_8 = 10110110221.$$

Note that $c_0(3) = c_8(3), c_0(4) = c_8(4), c_0(8) = c_3(8), c_0(9) = c_3(9)$ and so trifference is achieved at coordinate 1.

(b) Only two of the codewords share a coordinate in which 2 occurs.
By Lemma 6.2, we may assume $x = c_0, y = c_1$ and $z = c_k$ for $2 < k < n-1$. For illustration, the three codewords look something like:

$$c_0 = 22110110\ldots$$
$$c_1 = 02211011\ldots$$
$$c_k = \ldots 01122110\ldots$$

If $c_k(0) \neq c_1(0) = 0$ or $c_k(2) \neq c_0(2) = 1$, then we achieve trifference at coordinate 0 or 2 respectively. So suppose $c_k(0) = 0$ and $c_k(2) = 1$. This can only happen if $k = 3m' + 1$ for some $m' > 0$. But this implies $c_0(k) = 0$ and $c_1(k) = 1$ and so trifference is achieved in coordinate k.

(c) All the three codewords share a coordinate where 2 occurs with another codeword:
By construction and Lemma 6.2, we may assume $x = c_0, y = c_1, z = c_2$. The codewords then look like:

$$c_0 = 22110110\ldots$$
$$c_1 = 02211011\ldots$$
$$c_2 = 10221101\ldots$$

Clearly, trifference is achieved at coordinate 0.

(iii) $x = d_i, y = d_{i'}, z = d_{i''}$ with $i < i' < i''$. This is very similar to the previous case and has identical subcases and arguments which we omit for the sake of brevity.

(iv) $x = c_i, y = c_{i'}, z = d_{i''}$ with $i < i' < i''$. By the cyclic invariance of Lemma 6.2, this is equivalent to the cases $x = c_i, y = d_{i'}, z = c_{i''}$ as well as $x = d_i, y = c_{i'}, z = c_{i''}$ for $i < i' < i''$.
Again, by Lemma 6.2, we may assume $x = c_0, y = c_j, z = d_k$ with $0 < j < k$. The following subcases arise:

(a) All pairs of 2s are disjoint, i.e. $j > 1$ and $j + 1 < k < n - 1$:
The codewords look something like:

$$c_0 = 22110110\ldots$$
$$c_j = \ldots 22110110\ldots$$
$$d_k = \quad \ldots 01122011\ldots$$

Following similar reasoning as in previous cases, if either $c_0(j) \neq d_k(j)$ or $c_0(j+1) \neq d_k(j+1)$, then trifference is achieved in one of these two coordinates. Otherwise, we must have both $c_0(j) = d_k(j)$ or $c_0(j) = d_k(j)$, which is only possible if $k = 3m' + 1$ for some $m' > 0$. Similarly, if trifference is not achieved in coordinates k or $k+1$, we must have $j = 3m''$ for some $m'' > 0$.
But this implies $c_j(0) = c_j(1) = 1$ and $d_k(0) = 1, d_k(1) = 0$ and hence, trifference is achieved in coordinate 1, as shown in Example 6.3.

Example 6.3. Suppose $n = 11, j = 3, k = 7$. Then the three codewords look like

$$\begin{aligned} c_0 &= 22110110110, \\ c_3 &= 11022110110, \\ d_7 &= 10110112201. \end{aligned}$$

Since we have $c_0(3) = d_7(3), c_0(4) = d_7(4), c_0(7) = c_3(7)$ and $c_0(8) = c_3(8)$, trifference is achieved at coordinate 1.

(b) Only $c_i, c_{i'}$ share a coordinate in which 2 occurs, i.e. $j = 1$ and $2 < k < n - 1$:
The codewords look like:

$$\begin{aligned} c_0 &= 22110110\ldots \\ c_1 &= 02211011\ldots \\ d_k &= \ldots 01122011\ldots \end{aligned}$$

If either $d_k(0) = 1$ or $d_k(2) = 0$, trifference is achieved at one of these coordinates. So, suppose both $d_k(0) = 0$ and $d_k(2) = 1$. This can only happen if $k = 3m'$ for some $m' > 0$. But in this case $c_0(k+1) = 0$ and $c_1(k+1) = 1$ and thus trifference is achieved at coordinate $k + 1$.

(c) Only $c_i, d_{i''}$ share a coordinate in which 2 occurs, i.e. $1 < j < k - 1$ and $k = n - 1$:
The codewords look like:

$$\begin{aligned} c_0 &= 22110\ldots110 \\ c_j &= \ldots 22110\ldots \\ d_{n-1} &= 2011\ldots0112 \end{aligned}$$

If either $c_j(1) = 1$ or $c_j(n-1) = 1$, trifference is achieved at one of these coordinates. By construction, one of these must happen, since the minimum number of symbols between any two 0s in any codeword is 2.

(d) Only $c_{i'}, d_{i''}$ share a coordinate in which 2 occurs, i.e. $1 < j < n - 2$ and $k = j + 1$:
The codewords look like:

$$\begin{aligned} c_0 &= 22110110\ldots \\ c_j &= \quad \ldots 221101\ldots \\ d_{j+1} &= \quad \ldots 122011\ldots \end{aligned}$$

If $c_0(j) = 0$ or $c_0(j + 2) = 0$, trifference is achieved in one of these coordinates. If not, then $c_0(j) = c_0(j + 2) = 1$, which is only possible if $j = 3m'$ for some $m' > 0$. But this implies $c_j(1) = 1$ and $d_{j+1}(1) = 0$ and thus trifference is achieved at coordinate 1.

(e) All codewords share a coordinate in which 2 occurs, with $j = 1$ and $k = 2$:
The codewords look like:

$$\begin{aligned} c_0 &= 22110110\ldots \\ c_1 &= 02211011\ldots \\ d_2 &= 11220110\ldots \end{aligned}$$

Clearly, trifference is achieved at coordinate 0.

(f) All codewords share a coordinate in which 2 occurs, with $j = 1$ and $k = n - 1$:
The codewords look like:

$$\begin{aligned} c_0 &= 22110110\ldots110 \\ c_1 &= 02211011\ldots011 \\ d_{n-1} &= 2011011\ldots0112 \end{aligned}$$

Clearly, trifference is achieved at coordinate $n - 1$.

(g) All codewords share a coordinate in which 2 occurs, with $j = n-2$ and $k = n-1$: The codewords look like:

$$c_0 = 22110110\ldots110$$
$$c_{n-2} = 110110\ldots11022$$
$$d_{n-1} = 2011011\ldots0112$$

Clearly, trifference is achieved at coordinate 1.

(v) $x = d_i, y = d_{i'}, z = c_{i''}$ with $i < i' < i''$. By the cyclic invariance of Lemma 6.2, this is equivalent to the cases $x = c_i, y = d_{i'}, z = d_{i''}$ as well as $x = d_i, y = c_{i'}, z = d_{i''}$ for $i < i' < i''$.
Again, by Lemma 6.2, we may assume $x = d_0, y = d_j, z = c_k$ with $0 < j < k$. The subcases and arguments arising are identical to the previous case and we will again choose to omit them here.

Case II: **n $\equiv$ 1** $\pmod 3$ **and n $\geq$ 10**

In this case, we construct a 2-bounded trifferent code of length n and size $2n$ from two smaller 2-bounded codes of lengths $5 \equiv 2 \pmod 3$ (denoted $\mathcal{C}_5$) and $(n-5) \equiv 2 \pmod 3$ (denoted $\mathcal{C}_{n-5}$) and sizes 10 and $2n-10$, respectively, as constructed from Case I.

For the code $\mathcal{C}_5$ from Case I, denote the set of codewords as $\{c_1, \ldots, c_5, d_1, \ldots, d_5\}$ and for the code $\mathcal{C}_{n-5}$, denote the set of codewords as $\{c'_1, \ldots, c'_{n-5}, d'_1, \ldots, d'_{n-5}\}$.

Then the new code of length n and size $2n$, denoted $\mathcal{C}_n$, is constructed (by concatenation) as follows:

$$\left.\begin{array}{ll} c_1 & 0\ 0\ \cdots\ 0 \\ \vdots & \vdots \\ c_5 & 0\ 0\ \cdots\ 0 \\ d_1 & 1\ 1\ \cdots\ 1 \\ \vdots & \vdots \\ d_5 & 1\ 1\ \cdots\ 1 \end{array}\right\} \mathcal{C}_{n,1}$$

$$\left.\begin{array}{ll} 0\ 0\ 0\ 0\ 0 & c'_1 \\ \vdots & \vdots \\ 0\ 0\ 0\ 0\ 0 & c'_{n-5} \\ 1\ 1\ 1\ 1\ 1 & d'_1 \\ \vdots & \vdots \\ 1\ 1\ 1\ 1\ 1 & d'_{n-5} \end{array}\right\} \mathcal{C}_{n,2}$$

Clearly, $\mathcal{C}_n = \mathcal{C}_{n,1} \cup \mathcal{C}_{n,2}$. For convenience, we also divide $\mathcal{C}_{n,1} = \mathcal{C}_{n,1c} \dot\cup \mathcal{C}_{n,1d}$ and $\mathcal{C}_{n,2} = \mathcal{C}_{n,2c} \dot\cup \mathcal{C}_{n,2d}$ based on whether the codeword contains a smaller codeword of type c or d.

We now show that $\mathcal{C}_n$ is trifferent, for which we require the following lemma.

Lemma 6.3. *Suppose $n' \equiv 3 \pmod 2$ and $x, y \in \mathcal{C}_{n'}$ (from Case I) such that either $x = c_i$ and $y = c_j$ or $x = d_i$ and $y = d_j$ for some $0 \leq i < j \leq n-1$. Then there exist coordinates t, t' such that $\{x(t), y(t)\} = \{0, 2\}$ and $\{x(t'), y(t')\} = \{1, 2\}$.*

Proof. Consider the first case, i.e. $x = c_i, y = c_j$ for some $0 \leq i < j \leq n-1$. From similar reasoning as in Lemma 6.2, we may assume $x = c_0$ and $y = c_k$ for some $k > 0$.

If $k = 1$, we have $c_0(0) = 2, c_1(0) = 0, c_0(2) = 1$ and $c_1(2) = 2$; so $t = 0, t' = 2$ and we are done. The case $k = n-1$ is equivalent to this by a simple cyclic shift.

So, assume $0 < k < n-1$. This means that the pairs of 2s in c_0 and c_k are disjoint. Consider the coordinates 0 and 1. Clearly, $c_0(0) = c_0(1) = 2$. So if $c_k(0) \neq c_k(1)$, we have $\{t, t'\} = \{0, 1\}$ and we are done. So suppose $c_k(0) = c_k(1) \neq 2$. Since they are successive coordinates, they cannot both be 0, by construction. Hence, $c_k(0) = c_k(1) = 1$. This is only possible if $k = 3m'$ for some $m' > 0$. But this implies that $c_0(k) = 1$ and $c_0(k+1) = 0$, so $t = k+1, t' = k$ and we are done. For better understanding, this case is illustrated in Example 6.4.

For the second case, we may assume as before, $x = d_0, y = d_k$ for some $k > 0$. If $k = 1$, we have $t = 2, t' = 0$ and identically for $k = n-1$. For the remaining case $0 < k < n-1$, we can assume $d_k(0) = d_k(1) = 1$ (if not, we have $\{t, t'\} = \{0, 1\}$ as before). This implies $k = 3m' + 2$ for some $m' > 0$, which in turn implies $d_0(k) = 0$ and $d_0(k+1) = 1$. So $t = k, t' = k+1$, and we are done. □

Example 6.4. Let $n = 11$ and consider the codewords c_0, c_6:

$$c_0 = 22110110110$$
$$c_6 = 11011022110$$

Since $6 = 3m'$ for some $m' > 0$, we have both $c_6(0) = c_6(1) = 1$. However, we still have $c_0(6) = 1$ and $c_0(7) = 0$ and so $t = 7, t' = 6$.

To prove $\mathcal{C}_n$ is trifferent, let $x, y, z \in \mathcal{C}_n$ be arbitrary codewords. The following cases arise:

(i) All three codewords $x, y, z \in \mathcal{C}_{n,1}$. Then, they are trifferent in one of the first 5 coordinates since the code $\mathcal{C}_5$ is trifferent from Case I.

(i) All three codewords $x, y, z \in \mathcal{C}_{n,2}$. Then, they are trifferent in one of the last $n-5$ coordinates since the code $\mathcal{C}_{n-5}$ is trifferent from Case I.

(iii) $x, y \in \mathcal{C}_{n,1}$ and $z \in \mathcal{C}_{n,2}$. Three subcases arise:

  (a) $x \in \mathcal{C}_{n,1c}$ and $y \in \mathcal{C}_{n,1d}$. By construction, z has 2s occurring only in the last $n-5$ coordinates, which are all 0 for x and all 1 for y. Hence, the three codewords achieve trifference at any coordinate in which 2 occurs in z.

  (b) $x, y \in \mathcal{C}_{n,1c}$ or $x, y \in \mathcal{C}_{n,1d}$. From Lemma 6.3, there exist coordinates $t, t' \in [5]$ with $\{x(t), y(t)\} = \{0, 2\}$ and $\{x(t'), y(t')\} = \{1, 2\}$. Since z has all zeros or all ones in these set of coordinates, the three codewords achieve trifference at either one of the coordinates t or t'.

(iv) $x, y \in \mathcal{C}_{n,2}$ and $z \in \mathcal{C}_{n,1}$. Since the arguments of case (iii) hold regardless of the length of the codes C_5 and $\mathcal{C}_{n-5}$, these codewords are also trifferent by the same subcases and reasoning.

Remark. There is nothing special about having 0s trail and lead codewords of the form c_i/c_i' and 1s doing the same for d_i/d_i' to form the concatenated codewords of $\mathcal{C}_n$. The proof remains identical if we were to construct $\mathcal{C}_n$ with 1s trailing and leading c_i/c_i' and 0s trailing and leading d_i/d_i'. We call the code obtained by swapping 1s and 0s in these coordinate blocks (while keeping the positions of 1s and 0s inside $c_i/c_i'/d_i/d_i'$ intact) the 'dual' of $\mathcal{C}_n$ and denote it as $\bar{\mathcal{C}_n}$. As argued, $\bar{\mathcal{C}_n}$ is also a trifferent code of size $2n$ and length n, where $n \equiv 1 \pmod 3$.

Case III: **n $\equiv$ 0 (mod 3) and n $\geq$ 15**

In this case, we construct a 2-bounded trifferent code of length n and size $2n$ from three smaller 2-bounded codes, two of lengths $5 \equiv 2 \pmod 3$ (denoted $\mathcal{C}_5$) and one of length $(n-10) \equiv 2 \pmod 3$ (denoted $\mathcal{C}_{n-10}$) and sizes 10, 10 and $2n-20$, respectively, as constructed from Case I.

For the code $\mathcal{C}_5$ from Case I, denote the set of codewords as $\{c_1, \ldots, c_5, d_1, \ldots, d_5\}$ and for the code $\mathcal{C}_{n-10}$, denote the set of codewords as $\{c_1', \ldots, c_{n-10}', d_1', \ldots, d_{n-10}'\}$.

Then the new code of length n and size $2n$, denoted $\mathcal{C}_n$ is constructed (by concatenation of three 'blocks' of coordinates of lengths $5, 5$ and $n-10$) as follows:

$$
\begin{array}{cccc}
c_1 & 0\ 0\ 0\ 0\ 0 & 1\ 1\ \cdots\ 1 & \Bigg\} \mathcal{C}_{n,1} \\
\vdots & \vdots & \vdots & \\
c_5 & 0\ 0\ 0\ 0\ 0 & 1\ 1\ \cdots\ 1 & \\
d_1 & 1\ 1\ 1\ 1\ 1 & 0\ 0\ \cdots\ 0 & \\
\vdots & \vdots & \vdots & \\
d_5 & 1\ 1\ 1\ 1\ 1 & 0\ 0\ \cdots\ 0 &
\end{array}
$$

$$
\begin{array}{ccc}
1\ 1\ 1\ 1\ 1 & c_1 & 0\ 0\ \cdots\ 0 \\
\vdots & \vdots & \vdots \\
1\ 1\ 1\ 1\ 1 & c_5 & 0\ 0\ \cdots\ 0 \\
0\ 0\ 0\ 0\ 0 & d_1 & 1\ 1\ \cdots\ 1 \\
\vdots & \vdots & \vdots \\
0\ 0\ 0\ 0\ 0 & d_5 & 1\ 1\ \cdots\ 1
\end{array}
\Bigg\} \mathcal{C}_{n,2}
$$

$$
\begin{array}{ccc}
0\ 0\ 0\ 0\ 0 & 1\ 1\ 1\ 1\ 1 & c'_1 \\
\vdots & \vdots & \vdots \\
0\ 0\ 0\ 0\ 0 & 1\ 1\ 1\ 1\ 1 & c'_{n-10} \\
1\ 1\ 1\ 1\ 1 & 0\ 0\ 0\ 0\ 0 & d'_1 \\
\vdots & \vdots & \vdots \\
1\ 1\ 1\ 1\ 1 & 0\ 0\ 0\ 0\ 0 & d'_{n-10}
\end{array}
\Bigg\} \mathcal{C}_{n,3}
$$

Clearly, $\mathcal{C}_n = \mathcal{C}_{n,1} \cup \mathcal{C}_{n,2} \cup \mathcal{C}_{n,3}$. We also divide $\mathcal{C}_n = \mathcal{C}_{n,c} \dot\cup \mathcal{C}_{n,d}$ based on whether the codeword contains a smaller codeword of type c or d. From the illustration above, $\mathcal{C}_{n,c}$ contains the first 5 codewords of $\mathcal{C}_{n,1}$, the first 5 codewords of $\mathcal{C}_{n,2}$ and the first $(n-10)$ codewords of $\mathcal{C}_{n,3}$, while $\mathcal{C}_{n,d} = \mathcal{C}_n \setminus \mathcal{C}_{n,c}$.

To show $\mathcal{C}_n$ is trifferent, let $x, y, z \in \mathcal{C}_n$ be arbitrary codewords. Consider the following cases:

(i) All codewords $x, y, z \in \mathcal{C}_{n,i}$ for some $i \in \{1,2,3\}$. Then trifference is achieved in the i^{th} block of coordinates since the codewords $\mathcal{C}_5$ and $\mathcal{C}_{n-10}$ are trifferent, from Case I.

(ii) Two codewords, say x, y, lie in $\mathcal{C}_{n,i}$ and z lies in $\mathcal{C}_{n,j}$ for some $i \neq j \in \{1,2,3\}$. Then the three codewords, when restricted to the blocks of coordinates i, j are of some length $n' \equiv 1 \pmod 3$ and lie in either a code constructed in Case II or its dual. Hence, they are trifferent as well. For illustration, consider Example 6.5.

Example 6.5. Let $n = 18$, $x, y \in \mathcal{C}_{18,1}$ and $z \in \mathcal{C}_{18,3}$ be the codewords:

$$
\begin{aligned}
x &= 02211 \quad 00000 \quad 11111111, \\
y &= 11220 \quad 11111 \quad 00000000, \\
z &= 00000 \quad 11111 \quad 11220110
\end{aligned}
$$

Then the three codewords restricted to blocks $1, 3$ look like:

$$
\begin{aligned}
x\big|_{1,3} &= 02211 \quad 11111111, \\
y\big|_{1,3} &= 11220 \quad 00000000, \\
z\big|_{1,3} &= 00000 \quad 11220110
\end{aligned}
$$

Clearly, these are 2-bounded codewords of length $13 \equiv 1 \pmod 3$. Further, they are of the form $(c_i \quad 1 \cdots 1)$, $(d_j \quad 0 \ldots 0)$ and $(00000 \quad c'_k)$. So these codewords lie in the code $\bar{\mathcal{C}_{13}}$, where $\mathcal{C}_{13}$ refers to a code constructed in Case II; and are thus trifferent.

(iii) All three codewords lie in different $\mathcal{C}_{n,i}$'s. Suppose, wlog, $x \in \mathcal{C}_{n,1}, y \in \mathcal{C}_{n,2}$ and $z \in \mathcal{C}_{n,3}$. By PHP, at least two of these codewords must lie in either the set $\mathcal{C}_{n,c}$ or $\mathcal{C}_{n,d}$. Then, in the block where neither of these codewords have a 2, one of the codewords must have only 1s while the other must have only 0s, by construction. Hence, whenever a 2 occurs in this block of coordinates in the third codeword (which must happen, since the three codewords have 2s occurring in different blocks in this case), the three codewords achieve trifference, as illustrated in Example 6.6.

Example 6.6. Suppose $n = 15$, $x \in \mathcal{C}_{15,1c}, y \in \mathcal{C}_{15,2d}$ and $z \in \mathcal{C}_{15,3c}$ such that:

$$\begin{aligned} x &= 22110 \quad 00000 \quad 11111 \\ y &= 00000 \quad 12201 \quad 11111 \\ z &= 00000 \quad 11111 \quad 11022 \end{aligned}$$

Here, $x, z \in \mathcal{C}_{15,c}$ and thus trifference is achieved in block 2 in any coordinate in which a 2 occurs in codeword y.

□

6.3. Construction 2

This is a recursive construction suggested by Anurag Bishnoi. It uses k copies of a 2-bounded trifferent code of length n and size t, to create k disjoint blocks of this code leading to a larger 2-bounded trifferent code of length nk and size tk. As a base code, we use the trifferent code of size 20 and length 9, as obtained computationally from the graph $K_{4,5}$ (see Table 5.1). As a result of this construction, we obtain the new bound $T_b(n, 2) \geq (20/9)n - O(1)$, which is better than the one obtained from Construction 1.

We first state and prove the construction of these recursive codes.

Theorem 6.4. *Suppose $\mathcal{C}$ is a 2-bounded trifferent code of size t and length n such that no two codewords in it have the same pair of coordinates in which 2 occurs. Then, we have $T_b(nk, 2) \geq tk$ for each positive integer k.*

Proof. Suppose $\mathcal{C} = \{c_1, \ldots, c_t\}$. Denote by c_i^0, the codeword obtained by replacing the 2s in the codeword $c_i \in \mathcal{C}$ by 0s. Similarly, denote the codeword obtained by replacing the 2s by 1s in codeword $c_i \in \mathcal{C}$, by c_i^1.

To prove $T_b(nk, 2) \geq tk$, we construct a 2-bounded trifferent code of size tk and length nk.

Let $\mathcal{C}_k$ be a 2-bounded code constructed by concatenating k blocks of codewords as follows:

Block 1	Block 2	Block 3	$\cdots$	Block k	
c_1	c_1^1	c_1^1	$\cdots$	c_1^1	$\mathcal{C}_k^{(1)}$
$\vdots$					
c_t	c_t^1	c_t^1	$\cdots$	c_t^1	
c_1^0	c_1	c_1^1	$\cdots$	c_1^1	$\mathcal{C}_k^{(2)}$
$\vdots$					
c_t^0	c_t	c_1^1	$\cdots$	c_t^1	
		$\vdots$			
c_1^0	c_1^0	c_1^0	$\cdots$	c_1	$\mathcal{C}_k^{(k)}$
$\vdots$					
c_t^0	c_t^1	c_t^0	$\cdots$	c_t	

Clearly, $\mathcal{C}_k = \mathcal{C}_k^{(1)} \cup \mathcal{C}_k^{(2)} \cup \cdots \cup \mathcal{C}_k^{(k)}$.

Example 6.7. Suppose $\mathcal{C} = \{0212, 1022, 2102\}$. Then, for $k = 3$, the code $\mathcal{C}_3$ is a code of length 9 and size 9, and looks like

$$\begin{array}{ccc} 0212 & 0111 & 0111 \\ 1022 & 1011 & 1011 \\ 2102 & 1101 & 1101 \end{array}$$

$$\begin{array}{ccc} 0010 & 0212 & 0111 \\ 1000 & 1022 & 1011 \\ 0100 & 2102 & 1101 \end{array}$$

$$\begin{array}{ccc} 0010 & 0010 & 0212 \\ 1000 & 1000 & 1022 \\ 0100 & 0100 & 2102 \end{array}$$

To prove $\mathcal{C}_k$ is a trifferent code, let $x, y, z \in \mathcal{C}_k$ be arbitrary codewords. The following cases need to be checked.

(i) All codewords $x, y, z \in \mathcal{C}_k^{(j)}$ for some $j \in \{1, \ldots, k\}$. Then the codewords, when restricted to block j (we use the notion $|_j$ to denote this), lie in the code $\mathcal{C}$ by construction, and thus must be trifferent in this block of coordinates.

(ii) Two codewords, say $x, y \in \mathcal{C}_k^{(j)}$, and $z \in \mathcal{C}_k^{(\ell)}$ for distinct $j, \ell \in \{1, \ldots, k\}$. Two subcases are possible in this case:

(a) $x|_j = c_i, y|_j = c_p, z|_\ell = c_q$ for distinct $i, p, q \in \{1, \ldots, t\}$.
Since $c_i, c_p, c_q \in \mathcal{C}$, a trifferent code, they must be trifferent. Suppose they attain trifference in coordinate s. If $c_i(s) = 2$, we clearly have $\{c_p, c_q\} = \{0, 1\}$. Then in the s coordinate of block j, where c_i and thus x has a 2, we have $y|_j(s) = c_p(s)$ as well as $z|_j(s) = c_q^0(s) = c_q^1(s) = c_q(s)$. So, the three codewords are trifferent in coordinate s of block j. The same logic holds if $c_p(s) = 2$. If $c_q(s) = 2$, we also have $\{c_i(s), c_p(s)\} = \{0, 1\}$. Since $x|_\ell(s) = c_i^0(s) = c_i^1(s) = c_i(s)$ and $y|_\ell(s) = c_p^0(s) = c_p^1(s) = c_p(s)$, the three codewords attain trifference in coordinate s of block ℓ.

(b) $x|_j = c_i, y|_j = c_p, z|_\ell = c_i$ for $i, p \in \{1, \ldots, t\}$.
Since no two codewords in $\mathcal{C}$ have the same pair of coordinates in which 2 occurs, there exists a coordinate, say s, such that $c_i(s) = 2$ and $c_p(s) \in \{0, 1\}$. Consider the symbols in coordinate s of blocks j and ℓ. We clearly have $x|_j(s) = c_i(s) = 2$, $y|_j(s) = c_p(s)$ and $z|_\ell(s) = c_i(s) = 2$, $y|_\ell(s) = c_p^1(s) = c_p^0(s) = c_p(s)$. Moreover, we have $\{z|_j(s), x|_\ell(s)\} = \{0, 1\}$ since either $j > \ell$ or $\ell > j$. Hence, the three codewords attain trifference in one of these coordinates.

(iii) $x \in \mathcal{C}_k^{(j)}, y \in \mathcal{C}_k^{(\ell)}$ and $z \in \mathcal{C}_k^{(m)}$ for distinct $j, \ell, m \in \{1, \ldots, k\}$. Three subcases arise in this case:

(a) $x|_j = c_i, y|_\ell = c_p, z|_m = c_q$ for distinct $i, p, q \in \{1, \ldots, t\}$.
Since $c_i, c_p, c_q \in \mathcal{C}$, a trifferent code, they are also trifferent. Suppose they attain trifference in coordinate s, in which wlog, c_i has a 2. Clearly, $\{c_p, c_q\} = \{0, 1\}$. Then in the block j, where c_i and thus x has a 2, we have $y|_j(s) = c_p^0(s) = c_p^1(s) = c_p(s)$ as well as $z|_j(s) = c_q^0(s) = c_q^1(s) = c_q(s)$. So, the three codewords are trifferent in coordinate s of block j.

(b) $x|_j = c_i, y|_\ell = c_i, z|_m = c_p$ for distinct $i, p \in \{1, \ldots, t\}$.
Since no two codewords in $\mathcal{C}$ have the same pair of coordinates in which 2 occurs, there exists a coordinate, say s, such that $c_i(s) = 2$ and $c_p(s) \in \{0, 1\}$. Consider the symbols in coordinate s of blocks j and ℓ. We clearly have $x|_j(s) = c_i(s) = 2$, $z|_j(s) = c_p^1(s) = c_p^0(s) = c_p(s)$ and $y|_\ell(s) = c_i(s) = 2$, $z|_\ell(s) = c_p^1(s) = c_p^0(s) = c_p(s)$. Moreover, we have $\{y|_j(s), x|_\ell(s)\} = \{0, 1\}$ since either $j > \ell$ or $\ell > j$. Hence, the three codewords attain trifference in one of these coordinates.

(c) $x|_j = c_i, y|_\ell = c_i, z|_m = c_i$ for some $i \in \{1, \ldots, t\}$.
Suppose wlog, $j < \ell < m$. Then, we have $x|_\ell = c_i^1, y|_\ell = c_i, z|_\ell = c_i^0$. Suppose $c_i(s) = 2$ for some coordinate s (the codewords are 2-bounded so this must happen). Then $y|_\ell(s) = 2$ and by construction, $x|_\ell = c_i^1(s) = 1$ and $z|_\ell = c_i^0(s) = 0$. So the three codewords are trifferent in coordinate s of block ℓ.

□

From the computational results of the SAT solver, outlined in Table 5.1, we know that there exists a trifferent code of length 9 and size 20. Moreover, the underlying graph of the computation is $K_{4,5}$ with all edge weights 1. This means each codeword has a unique pair of coordinates in which 2 occurs.

Using this code, denoted $\mathcal{C}_9$, as the base code in Theorem 6.4, we obtain the following result.

Proposition 6.5. *For all $n \geq 9$, we have*

$$T_b(n, 2) \geq (20/9)n - O(1).$$

Proof. Suppose $n = 9k$ for some positive integer k. Using code $\mathcal{C}_9$ as the base code in Theorem 6.4, we have $T_b(9k, 2) \geq 20k$, which implies $T_b(n, 2) \geq (20/9)n$.

Suppose $n = 9k + a$ for some $0 < a < 9$. Then, using (3.2) repeatedly (i.e. by appending a 1s in each of the coordinates of $\mathcal{C}_{9k}$), we get $T_b(9k + a, 2) \geq 20k$, which implies $T_b(n, 2) \geq (20/9)n - (20/9)a$. Since $a < 9$, we have $20a/9 = O(1)$, and we are done. □

7

Conclusion and Further Research

In this thesis, we explored some prevailing and recent improvements to asymptotic bounds on sizes of trifferent codes. Since the recent improvements in these bounds (by Bhandari and Khetan [BK25]) were obtained by considering r-bounded trifferent codes, we also studied these codes in more detail.

Inspired by the technique of the same paper, we proved the following upper bound on largest sizes of r-bounded trifferent codes:

$$T_b(n,2) \leq c \times n^{5/3} \quad \text{and}$$
$$T_b(n,r) \leq c' \times n^{r-2/5}.$$

for some positive constants c, c' and $r > 2$.

Using these, we were able to show that the bound obtained by Bhandari and Khetan,

$$T(n) \leq c \times n^{-2/5} \times \left(\frac{3}{2}\right)^n$$

is the best possible even after directly generalizing their proof technique for $r > 3$.

We were also able to prove new lower bounds on $T_b(n,r)$ from some existing hypergraph constructions by Ruzsa-Szemerédi[RS78] and Alon-Shapira [AS06], building upon ideas by Bishnoi and Kovács:

$$T_b(n,r) \geq n^{\lceil r/2 \rceil - o(1)}$$

for all $r \geq 3$.

Finally, we were able to come up with new constructions of 2-bounded trifferent codes which improved the current best lower bound of $T_b(n,2) \geq 2n-2$. In a joint work with Jozefien D'haeseleer, we first gave an explicit construction of 2-bounded trifferent codes of length n and size $2n$ for $n = 5, 8, 10, 11$ and all $n \geq 13$.

Using a SAT solver, we computed a trifferent code of length 9 and size 20 to show that $T_b(9,2) \geq 20$. Using this 2-bounded trifferent code (of length 9 and size 20) as a base code, we were able to provide a recursive construction for 2-bounded trifferent codes of longer lengths. This resulted in an even better bound of

$$T_b(n,2) \geq (20/9)n - O(1).$$

There is still huge scope to improve upon these bounds. Even though the technique of using forbidden subgraph for bounding r-bounded trifferent codes did not immediately improve bounds for $T(n)$, there is still a huge gap between the current best lower and upper bounds for $T_b(n,r)$. Any improvement made to the upper bound will result in a better bound on $T(n)$.

Further, the lower bounds obtained for $T_b(n,2)$ obtained from computations, can also see further improvement. If we are able to compute a lower bound $T_b(k,2) \geq t$ such that $t/k > 20/9$, then the recursive result we proved in Chapter 6 can directly improve the constant $(20/9)$ in our current best lower bound.

Lastly, the recently established connections between strong blocking sets, minimal codes and linear trifferent codes, which we have also elaborated on in Chapter 4, can also be investigated more to see if any bounds on $T_L(n)$ can be further improved.

Bibliography

[AB02] Alexei Ashikhmin and Alexander Barg. Minimal vectors in linear codes. *IEEE Transactions on Information Theory*, 44(5):2010–2017, 2002.

[ABCH95] A Ashikhmin, Alexander Barg, G Cohen, and L Huguet. Variations on minimal codewords in linear codes. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 96–105. Springer, 1995.

[ABN22] Gianira N. Alfarano, Martino Borello, and Alessandro Neri. A geometric characterization of minimal codes and their asymptotic performance. *Advances in Mathematics of Communications*, 16(1):115–133, 2022.

[ABNR22] Gianira N Alfarano, Martino Borello, Alessandro Neri, and Alberto Ravagnani. Three combinatorial perspectives on minimal codes. *SIAM Journal on Discrete Mathematics*, 36(1):461–489, 2022.

[Agr02] Erik Agrell. On the Voronoi neighbor ratio for binary linear block codes. *IEEE Transactions on Information Theory*, 44(7):3064–3072, 2002.

[AS06] Noga Alon and Asaf Shapira. On an extremal hypergraph problem of Brown, Erdos and Sós. *Combinatorica*, 26(6):627–646, 2006.

[BDGP24] Anurag Bishnoi, Jozefien D'haeseleer, Dion Gijswijt, and Aditya Potukuchi. Blocking sets, minimal codes and trifferent codes. *Journal of the London Mathematical Society*, 109(6):e12938, 2024.

[Beh46] F. A. Behrend. On sets of integers which contain no three terms in arithmetical progression. *Proceedings of the National Academy of Sciences*, 32(12):331–332, 1946.

[BETS73] William G Brown, Pál Erdős, and Vera T Sós. On the existence of triangulated spheres in 3-graphs and related problems. *Periodica Mathematica Hungarica*, 3:221–229, 1973.

[BK25] Siddharth Bhandari and Abhishek Khetan. Improved upper bound for the size of a trifferent code. *Combinatorica*, 45(1):2, 2025.

[BMVT78] Elwyn Berlekamp, Robert McEliece, and Henk Van Tilborg. On the inherent intractability of certain coding problems (corresp.). *IEEE Transactions on Information theory*, 24(3):384–386, 1978.

[BR21] Siddharth Bhandari and Jaikumar Radhakrishnan. Bounds on the zero-error list-decoding capacity of the $q/(q-1)$ channel. *IEEE Transactions on Information Theory*, 68(1):238–247, 2021.

[BS20] Thomas F. Bloom and Olof Sisask. Breaking the logarithmic barrier in Roth's theorem on arithmetic progressions, 2020.

[BS23] Thomas F. Bloom and Olof Sisask. An improvement to the Kelley-Meka bounds on three-term arithmetic progressions, 2023.

[BSS12] Aart Blokhuis, Péter Sziklai, and Tamás Szonyi. *Blocking sets in projective spaces*, pages 61–84. Nova Science Publisher Inc., 2012.

[Cas06] Rey Casse. *Projective geometry: An Introduction*. OUP Oxford, 2006.

[DFGP22] Stefano Della Fiore, Alessandro Gnutti, and Sven Polak. The maximum cardinality of trifferent codes with lengths 5 and 6. *Examples and Counterexamples*, 2:100051, 2022.

[DGR19] Marco Dalai, Venkatesan Guruswami, and Jaikumar Radhakrishnan. An improved bound on the zero-error list-decoding capacity of the 4/3 channel. *IEEE Transactions on Information Theory*, 66(2):749–756, 2019.

[Eli88] P. Elias. Zero error capacity under list decoding. *IEEE Transactions on Information Theory*, 34(5):1070–1074, 1988.

[ET36] Paul Erdös and Paul Turán. On some sequences of integers. *Journal of The London Mathematical Society-second Series*, pages 261–264, 1936.

[FK84] Michael L Fredman and János Komlós. On the size of separating systems and families of perfect hash functions. *SIAM Journal on Algebraic Discrete Methods*, 5(1):61–68, 1984.

[FS14] Szabolcs L. Fancsali and Péter Sziklai. Lines in higgledy-piggledy arrangement. *The Electronic Journal of Combinatorics*, 21, 2014.

[GR22] Venkatesan Guruswami and Andrii Riazanov. Beating Fredman-Komlós for perfect k-hashing. *Journal of Combinatorial Theory, Series A*, 188:105580, 2022.

[GRS25] Venkatesan Guruswami, Atri Rudra, and Madhu Sudan. *Essential Coding Theory*. University at Buffalo, 2025. Available online.

[HC58] C. Hyltén-Cavallius. On a combinatorical problem. *Colloquium Mathematicae*, 6:61–65, 1958.

[HDZ18] Ziling Heng, Cunsheng Ding, and Zhengchun Zhou. Minimal linear codes over finite fields. *Finite Fields and Their Applications*, 54:176–196, 2018.

[Hil73] Raymond Hill. On the largest size of cap in $S_{5,3}$. *Atti Accad. Naz. Lincei Rend.*, 54(3):378–384, 1973.

[Kar09] Richard M Karp. Reducibility among combinatorial problems. In *50 Years of Integer Programming 1958-2008: from the Early Years to the State-of-the-Art*, pages 219–241. Springer, 2009.

[KM88] J. Korner and K. Marton. New bounds for perfect hashing via information theory. *European Journal of Combinatorics*, 9(6):523–530, 1988.

[KM23] Zander Kelley and Raghu Meka. Strong bounds for 3-progressions. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 933–973, 2023.

[KST54] T. Kóvari, V. Sős, and P. Turán. On a problem of k. zarankiewicz. *Colloquium Mathematicae*, 3:50–57, 1954.

[Kur24] Sascha Kurz. Trifferent codes with small lengths. *Examples and Counterexamples*, 5:100139, 2024.

[Mas93] James L Massey. Minimal codewords and secret sharing. In *Proceedings of the 6th joint Swedish-Russian international workshop on information theory*, pages 276–279, 1993.

[NM44] J von Neumann and Oskar Morgenstern. *Theory of games and economic behavior*. Princeton university press Princeton, 1944.

[Pel70] Giuseppe Pellegrino. Sul massimo ordine delle calotte in $S_{4,3}$. *Matematiche (Catania)*, 25(10), 1970.

[Pel23] Sarah Peluse. Recent progress on bounds for sets with no three terms in arithmetic progression, 2023.

[Ric56] Moses Richardson. On finite projective games. *Proceedings of the American Mathematical Society*, 7(3):458–465, 1956.

[Rot53] K. F. Roth. On certain sets of integers. *Journal of the London Mathematical Society*, s1-28(1):104–109, 1953.

[RS78] Imre Z Ruzsa and Endre Szemerédi. Triple systems with no six points carrying three triangles. *Combinatorics (Keszthely, 1976), Coll. Math. Soc. J. Bolyai*, 18(939-945):2, 1978.

[SS42] Raphaël Salem and Donald C Spencer. On sets of integers which contain no three terms in arithmetical progression. *Proceedings of the National Academy of Sciences*, 28(12):561–563, 1942.

[TQLZ21] Chunming Tang, Yan Qiu, Qunying Liao, and Zhengchun Zhou. Full characterization of minimal linear codes as cutting blocking sets. *IEEE Transactions on Information Theory*, 67(6):3690–3700, 2021.

[XY23] Chaoping Xing and Chen Yuan. Beating the probabilistic lower bound on q-perfect hashing. *Combinatorica*, 43(2):347–366, 2023.