Vector Trifference

Siddharth Bhandari* Abhishek Khetan†

October 7, 2025

Abstract

We investigate a geometric generalization of *trifference*, a concept introduced by Elias [Eli88] in the study of zero-error channel capacity. In the discrete setting, a code $\mathcal{C} \subseteq \{0,1,2\}^n$ is *trifferent* if for any three distinct codewords $x, y, z \in \mathcal{C}$, there exists a coordinate $i \in [n]$ where x_i, y_i, z_i are mutually distinct. Determining the maximum size of such codes remains a central open problem; the classical upper bound $|\mathcal{C}| \leq 2 \cdot (3/2)^n$ from [Eli88], proved via a simple 'pruning' argument, has resisted significant improvement.

Motivated by the search for new techniques, and in line with the *vectorial extensions* of other classical combinatorial notions, we introduce the concept of *vector trifferent* codes. Consider $\mathcal{C} \subseteq (S^2)^n$, where the alphabet is the unit sphere $S^2 = \{v \in \mathbb{R}^3 : \|v\| = 1\}$. We say the code $\mathcal{C}$ is vector trifferent if for any three distinct $x, y, z \in \mathcal{C}$, there is an index i where the vectors x_i, y_i, z_i are mutually orthogonal. A direct reduction of the vectorial problem to the discrete setting appears infeasible, making it difficult to replicate Elias's pruning argument. Nevertheless, we develop a new method to establish the following upper bound for the size of a vector trifferent code:

$$|\mathcal{C}| \leq (\sqrt{2} + o(1)) \cdot (3/2)^n.$$

Interestingly, our approach, when modified and adapted back to the discrete setting, yields a polynomial improvement to Elias's bound: $|\mathcal{C}| \lesssim n^{-1/4} \cdot (3/2)^n$, This improvement arises from a technique that parallels, but is not identical to, the method of [BK25]. However, it still falls short of the sharper $n^{-2/5}$ factor obtained there. We also generalize the concept of vector trifferent codes to richer alphabets and prove a vectorial version of the Fredman-Komlós theorem [FK84] for general k-separating codes.

*Toyota Technological Institute at Chicago (Work done prior to author joining Amazon). Email: siddharth@ttic.edu

†Ashoka University, Dept. of Mathematics. Email: abhishek.khetan@ashoka.edu

1 INTRODUCTION

In this work we study a geometrical generalization of the concept of 'trifference' define below.

§ Definition (Trifferent Codes) For an integer $n > 0$ we say three distinct strings x, y and z all belonging to $\{0,1,2\}^n$ are *trifferent* if there exists a coordinate $i \in \{1,\dots,n\}$ where the entries x_i, y_i, z_i are mutually distinct. A *trifferent code* of block length n is a subset $\mathcal{C} \subseteq \{0,1,2\}^n$ such that any three distinct codewords $x, y, z \in \mathcal{C}$ are trifferent.

The problem of finding the maximum possible size of a trifferent code of block length n was first introduced by Elias [Eli88] and has occupied an important position at the intersection of zero-error information theory and combinatorics of hash functions. Upper bounding the maximum possible size of such a code, and understanding this question has drawn considerable attention. (See for instance the 2014 Shannon Lecture: 'On The Mathematics of Distinguishable Difference' by János Körner.) Elias [Eli88] established an initial upper bound, showing that $|\mathcal{C}| \leq 2(\frac{3}{2})^n$: on the other hand the current best lower-bound is $|\mathcal{C}| \gtrsim \left(\frac{9}{5}\right)^{n/4}$ obtained via a semi-random construction in [KM88]. Numerous results on the extensions of the trifference problem to richer alphabets and under varied hashing requirements have been obtained since, including the seminal result on k-separating codes (which are k-ary analogues of trifferent codes) in [FK84] (for a more detailed discussion please see the introduction in [BK25]). However, it has remained challenging to substantially improve the original bound of Elias. Subsequent works have managed to refine this bound via a computer search for low-dimensional trifferent codes: [FGP22] and later [Kur24] leading to the improved upper bound of $0.6937\left(\frac{3}{2}\right)^n$. A polynomial factor improvement was later obtained in [BK25]: more precisely, the bound was improved to $cn^{-2/5}\left(\frac{3}{2}\right)^n$, where c is an absolute constant. Some variants of trifferent codes have also been considered: such as linear trifferent codes where we think of $\{0,1,2\}$ as $\mathbb{F}_3$ and $\mathcal{C}$ is a linear subspace ([PZ22, BDGP23, DFD24, FD25]); and more recently in [BKK$^+$25] where the demand is that there exist multiple coordinates where any three different code words are mutually distinct (as opposed to a single coordinate in the usual setting).

This article investigates a natural geometric generalization of the concept of trifference, motivated by the aim of introducing new techniques, and of independent interest in its own right. Borrowing from *vectorial extensions* of other classical combinatorial notions (such as *vector chromatic number* in graph coloring, and semidefinite relaxations of discrete optimization problems [Lov79, GW94]), we extend the discrete alphabet $\{0,1,2\}$ to a continuous one: the set of unit vectors in $\mathbb{R}^3$, which form the 2-dimensional sphere S^2. Furthermore, the combinatorial notion of "trifference" is replaced with the geometric condition of pairwise orthogonality. This leads to the following definition.

§ Definition (Vector Trifferent Codes) Let $S^2 = \{v \in \mathbb{R}^3 : \|v\| = 1\}$. Consider an integer $n \geq 1$. We say that three points x, y and z, all belonging to $(S^2)^n$, are *vector trifferent* if there is an index $i \in \{1,\dots,n\}$ for which the vectors x_i, y_i, z_i are mutually orthogonal. A

vector trifferent code of block length n is a subset $\mathcal{C} \subseteq (S^2)^n$ such that any three distinct codewords $x, y, z \in \mathcal{C}$ are vector trifferent.

The primary goal of this work is to determine the largest possible size of a vector trifferent code. This geometric variant presents unique challenges that prevent a straightforward application of methods from the discrete setting. We document these challenges below.

1. A natural approach is to reduce the geometric problem to its discrete counterpart. To this end, consider the graph G whose vertices are the points on S^2 and we join two points on S^2 if the corresponding vectors are orthogonal. If the chromatic number of G were 3 then we could have easily created a discrete trifferent code of size $|\mathcal{C}|$: consider any proper coloring of G using the colors $\{0, 1, 2\}$, say χ, and transform $x \in \mathcal{C}$ to $(\chi(x_1), \ldots, \chi(x_n)) \in \{0, 1, 2\}^n$. It is easy to see that the transformed code satisfies the original definition of trifference discussed above.

   Hence, if the above were true we would have deduced that $|\mathcal{C}| \leq 2\left(\frac{3}{2}\right)^n$ (or a stronger bound using [BK25]). However, perhaps surprisingly, the chromatic number of G is 4 (see [GZ12] for a proof). Therefore, the above method transforms a vector trifferent code to a trifferent code over a quaternary alphabet: in other words, a code over $\{0, 1, 2, 3\}^n$ such that for every three distinct codewords x, y and z there is an $i \in [n]$ such that x_i, y_i and z_i are pairwise distinct. However, the best known upper bound for such a code is of the order 2^n (following the same argument as in [Eli88]), which is exponentially worse then Elias' original bound.

   Interestingly, [GZ12] also shows that if we restrict only to the set of the *rational points* of S^2 (which is a dense subset of S^2) then the graph that we get has chromatic number 3. This leads to another attempt where we transform each coordinate of each codeword to a symbol in $\{0, 1, 2\}$ using the color of a rational point 'close' to x_i. However, in order for our transformation to produce a trifferent code we would need to know the chromatic number of the graph where not only orthogonal vectors are neighbors but also 'almost' orthogonal vectors. Thus, in some sense the obstruction to reducing from the vector setting to the familiar discrete setting is "infinitesimal in nature."

2. Another natural attempt revolves around the following proof technique for the discrete setting. Consider a trifferent code $\mathcal{C} \subseteq \{0, 1, 2\}^n$. Now, let $A = \{0, 1\}^n$, then we know that $|\mathcal{C} \cap A| \leq 2$ as any three strings in A are non-trifferent. Combining this with the observation that trifference is a translationally invariant property (translating by $u \in \{0, 1, 2\}^n$ gives $\mathcal{C} \oplus u = \{x +_{\mathbb{F}_3} u \mid x \in \mathcal{C}\}$), we can say that the expected size of the intersection of A with a random translate of C is at most 2: on the other hand it is $|\mathcal{C}| \cdot 2^{-n}$. Hence, we get $|\mathcal{C}| \leq 2 \cdot (3/2)^n$. This is just a reinterpretation of the classical 'pruning' style argument for Elias' bound[1] but was, in fact, exploited in [BK25] to get a polynomial improvement.

   Adopting the above to the vector trifference question involves finding a large subset $A \subseteq S^2$ such that there do not exist three mutually orthogonal points in A. Say the Lebesgue measure of A, $\mu(A)$, is α. Then, we get an upper bound on the size of a vector trifferent code $\mathcal{C}$ of block length n as

$$|\mathcal{C}| \leq 2\left(\frac{1}{\alpha}\right)^n.$$

[1] Let $\mathcal{C}_0 = \mathcal{C} \subseteq \{0, 1, 2\}^n$ be trifferent. For each $i = 1$, pick a least-frequent symbol $a_i \in \{0, 1, 2\}$ in coordinate i of $\mathcal{C}_{i-1}$ and delete all codewords with a_i in that coordinate to form $\mathcal{C}_i$. Then, $|\mathcal{C}_i| \geq (2/3)\,|\mathcal{C}_{i-1}|$. Recursively apply the above process on the pruned set of codewords: this leads to $|\mathcal{C}_n| \geq (2/3)^n|\mathcal{C}|$. Since no three distinct words in $\mathcal{C}_n$ can all differ in any fixed coordinate, $|\mathcal{C}_n| \leq 2$. Hence, $2 \geq |\mathcal{C}_n| \geq (2/3)^n|\mathcal{C}|$ which gives $|\mathcal{C}| \leq 2 \cdot (3/2)^n$.

To see why, note that rotating $\mathcal{C}$ by a unitary in $(\mathbb{R}^3)^{\otimes n}$, preserves the vector trifference property of $\mathcal{C}$. Also, the expected number of codewords from $\mathcal{C}$ which land in A^n is $\alpha^n \cdot |\mathcal{C}|$. But this number cannot exceed 2 as any three points x, y, z in A^n

So the question is what can be the largest mass of A: the larger the better for our upper bound above. This question was studied in [Per19] as a natural variant of Wistenhausen's *double cap conjecture* [Wit74]. In [Per19] it was found that there is an A such that $0.594 \leq \mu((A))$. If we apply this result to upper bound the size of a vector trifferent code we get an answer exponentially worse than $(3/2)^n$ which is the approximate bound for the discrete variant.

In fact, it is actually easy to put an upper bound on α of $2/3$ (simple random argument). This shows that even in the limit this method will not yield upper bounds on vector trifferent codes beyond $2 \cdot (3/2)^n$. Thus, the problem of vector trifference intersects with some interesting geometrical problems. A recent interesting result towards the higher dimensional generalization of this problem appears in [Zak25].

Despite these challenges, this paper establishes an upper bound for vector trifferent codes that is analogous to the bound in the discrete case. Our main result demonstrates that the size of such a code is similarly constrained, and notably, achieves a better leading constant than the standard pruning argument provides for the discrete problem which leads to Elias' original bound for trifferent codes $(2 \cdot (3/2)^n)$. In fact, before the result of [BK25], the improvements to Elias' bound relied on searching for optimal trifferent codes of low block lengths.

Theorem 1.1 ***(Main Result).*** *Let $\mathcal{C}$ be a vector trifferent code of block length n. Then, as $n \to \infty$,*

$$|\mathcal{C}| \leq (\sqrt{2} + o(1)) \left(\frac{3}{2}\right)^n.$$

The proof appears in Section 3. As discussed, the proof requires techniques distinct from those used in the discrete setting, reflecting the challenges posed by the geometric formulation. Along the way we prove a geometrical lemma, Lemma 2.2, which might be of independent interest: it concerns the maximum probability that two independently drawn vectors from the same distribution over $\mathbb{R}^d$, are orthogonal. *Subsequently, we transfer these techniques to the discrete setting and demonstrate that they yield an alternative—similar in spirit yet distinct in method—for improving Elias's original bound, as achieved in [BK25].* Please see Section 5 for more details.

✍ **1.2 Proof overview.** Our proof of Theorem 1.1 proceeds by translating the combinatorial "trifference" condition into a statement about the geometry of certain tensor-product subspaces. The central idea is to associate to each *pair* of distinct codewords $(x, y) \in \mathcal{C}^2$ a structured subspace

$$E_{x,y} \subset (\mathbb{R}^3)^{\otimes n}$$

that captures the coordinates where x_i and y_i are not orthogonal. The argument unfolds in three main steps:

1. **Pairwise subspace construction and orthogonality constraints.** For each coordinate i, we define a 1- or 2-dimensional subspace $f(x_i, y_i) \subset \mathbb{R}^3$ depending on whether x_i is orthogonal to y_i. The tensor product of these subspaces across all coordinates yields $E_{x,y}$. The vector trifference property ensures that for any two *distinct* pairs $(x, y) \neq (a, b)$, the subspaces $E_{x,y}$ and $E_{a,b}$ are orthogonal.

2. **Direct sum decomposition and dimension bound.** The orthogonality property above implies that the collection $\{E_{x,y} : x < y\}$ forms a direct sum inside the ambient space $(\mathbb{R}^3)^{\otimes n}$, whose total dimension is 3^n. Summing dimensions over all pairs $\{x, y\}$ yields the key inequality

$$\binom{|\mathcal{C}|}{2} \cdot \mathop{\mathbb{E}}_{\{x,y\}\in\binom{\mathcal{C}}{2}} \left[\, 2^{A(x,y)} \,\right] \;\leq\; 3^n,$$

where $A(x, y)$ counts the coordinates where x_i and y_i are *not* orthogonal, and the expectation is over a uniformly random draw of x and y from $\mathcal{C}$ without replacement.

3. **Lower-bounding the expectation.** The quantity $\mathbb{E}_{\{x,y\}\in\binom{\mathcal{C}}{2}}[\, 2^{A(x,y)} \,]$ is first approximate by $\mathbb{E}_{\{x,y\}\in\mathcal{C}\times\mathcal{C}}[\, 2^{A(x,y)} \,]$ (so x and y are drawn uniformly at random from $\mathcal{C}$ with replacement) and then expanded over subsets $S \subseteq [n]$ of coordinates. For each S, the probability that $x_i \not\perp y_i$ for all $i \in S$ is bounded below in two ways:

   - *Trivial bound:* at least $1/|\mathcal{C}|$, since equality $x = y$ guarantees the event.
   - *Geometric bound:* appropriately using Corollary 2.3 we can show that for any given $S \subseteq [n]$, the probability that $x_i \not\perp y_i$ for all $i \in S$ is at least $(1/3)^{|S|}$.

   Taking the maximum of these bounds and summing over all S yields a combinatorial expression that can be controlled using Proposition 2.4. Optimizing over a cutoff parameter balances the two regimes and leads to the asymptotic bound

$$|\mathcal{C}| \;\leq\; (\sqrt{2} + o(1)) \left(\frac{3}{2}\right)^n.$$

♢

Vector k-separating codes

In the discrete setting it is natural to generalize the notion of trifference over alphabets of size larger than 3.

§ Definition (k-separating Codes) Let $k \geq 2$ be an integer. A subset $\mathcal{C} \subseteq \{0, 1, 2, \ldots, k-1\}^n$ is called k-separating if for any k distinct codewords in $\mathcal{C}$ there exists a coordinate $i \in [n]$ such that the symbols of the codewords in the i^{th} coordinate are all mutually distinct.

Hence, the usual trifferent codes are 3-separating codes in the above terminology. In the same spirit, we can define *vector k-separating codes*.

§ Definition (Vector k-separating Codes) Let $k \geq 2$ be an integer and consider S^{k-1} the unit sphere in $\mathbb{R}^k$. A subset $\mathcal{C} \subseteq (S^{k-1})^n$ is called vector k-separating if for any k distinct codewords in $\mathcal{C}$ there exists a coordinate $i \in [n]$ such that the vectors in the i^{th} coordinate of the codewords are all mutually orthogonal.

Hence, vector trifferent codes are vector 3-separating codes. The setting of k-separating codes for $k > 3$ has been widely (see Subsection 1.4). The seminal result of [FK84] states that any such code is of size at most

$$\frac{\log_2 |\mathcal{C}|}{n} \leq \frac{k!}{k^{k-1}} + o(1) \quad \text{as } n \to \infty.$$

We would like to establish an analogous result for vector k-separating codes. A natural approach is to attempt a reduction to the discrete setting; however, as in the case of vector trifferent codes, this strategy encounters the same fundamental obstacles. In particular, the chromatic number of orthogonality graphs on spheres grows exponentially with the dimension [BD25], which prevents a straightforward reduction. Nevertheless, by adapting the proof technique originally developed for k-separating codes to the vectorial setting, and making use of Lemma 2.2, we are able to obtain the desired result (see Section 4).

Theorem 1.3 ***(Upper Bound for Vector k-separating Codes).*** *Let $\mathcal{C}$ be a vector k-separating code of block length n. Then,*

$$\frac{\log_2 |\mathcal{C}|}{n} \leq \frac{k!}{k^{k-1}} + o(1)$$

as $n \to \infty$.

✍ **1.4 Discussion & Open Questions.** As mentioned, the motivation for introducing vector trifferent codes is to develop new techniques that are applicable to the original discrete setting and that may, in turn, lead to improvements on the long-standing bounds. Our proof technique proceeds by pairing codewords of a vector trifferent code and showing that the corresponding vector spaces associated with these pairs form a direct sum within a 3^n-dimensional ambient space. This approach already yields tangible progress: a similar pairing-based analysis can, in fact, be carried out in the discrete setting, leading to an upper bound of $(3/2)^n$, where the leading constant of 1. Moreover, by incorporating ideas from [BK25], this bound can be further refined to $O\left(n^{-1/4} \cdot (3/2)^n\right)$, which, although weaker than the best-known bounds in the above work, remains of interest as it highlights an alternative line of reasoning towards the problem. (See Section 5 for more details.) This naturally raises the question:

> *Q1. Can the leading constant (currently $\sqrt{2}$) in the bound for vector trifferent codes be improved, perhaps by adapting the discrete pairing-based proof or by other means, and can such a refinement also yield a polynomial improvement (in the spirit of [BK25]) over the current upper bound on the size of vector trifferent codes?*

From the complementary direction, the construction of large trifferent codes has also remained a challenging problem. A simple random construction shows that there exist trifferent codes in of size approximately $(9/7)^{n/2}$. In [KM88], a stronger construction was given, producing trifferent codes of size $\gtrsim (9/5)^{n/4}$ via a random concatenation technique applied to an inner code of block length 4 (the so-called *tetra code*). Since every trifferent code is, by definition, also a vector trifferent code, one might expect that constructing vector trifferent codes should be at least as feasible. This naturally raises the question:

> *Q2. Does the continuous geometry of S^2 allow for the construction of vector trifferent codes that are exponentially larger than the best-known discrete ones?*

Finally, many refinements of the classical bound for k-separating codes are known, some tailored to specific values of k and others applying more generally [Ari94, DGR20, GR22, CD21]. Further extensions have also been explored in which the hashing or separation requirements are relaxed.

In particular, one may require only that for some integer $\ell \geq k$, whenever ℓ distinct codewords are considered, there exists a coordinate in which all k symbols appear [CRRS06, BR22].

Q3. Can we adapt these more sophisticated techniques to the vectorial setting?

♢

2 TECHNICAL PRELIMINARIES

✍ **2.1 Notation.** If μ is a probability measure on a space X, then we write $\mu \otimes \mu$ to denote the product measure (of μ with itself) on X^2. More generally, for any positive integer ℓ, we write

$$\underbrace{\mu \otimes \cdots \otimes \mu}_{\ell \text{ times}} = \mu^{\otimes \ell}$$

to denote the ℓ-fold product of μ with itself, which is a probability measure on X^ℓ. ♢

Next, we state a lemma that determines the maximum probability of obtaining mutually orthogonal vectors when ℓ vectors are drawn i.i.d. from a distribution μ over the $(d-1)$-dimensional sphere. This lemma plays a crucial role in the proofs of Theorems 1.1 and 1.3.

Lemma 2.2 ***(Maximum Probability of Mutual Orthogonality Under IID Draws).*** *Let $d \geq 1$ and $\mu \in \mathcal{P}(S^{d-1})$. Let $2 \leq \ell \leq d$ be arbitrary. Then*

$$\mu^{\otimes \ell}(\{(u_1, \ldots, u_\ell) \in (S^{d-1})^\ell : u_i \perp u_j \text{ for all } i \neq j\}) \leq \frac{d!}{(d-\ell)! \cdot d^\ell}$$

Proof. Let

$$p = \mu^{\otimes \ell}(\{(u_1, \ldots, u_\ell) \in (S^{d-1})^\ell : u_i \perp u_j \text{ for all } i \neq j\})$$

Fix $n \geq \ell$ arbitrarily. Let $V_1, V_2, \ldots, V_n$ be n independent random points drawn from S^{d-1} according to the distribution μ. Define a graph G on $[n]$ as follows: we join i and j with an edge if $V_i \perp V_j$. Let $I_1, \ldots, I_\ell$ be ℓ random points chosen from $[n]$ such that $\{I_1, \ldots, I_\ell\}$ is a uniformly random element of $\binom{[n]}{\ell}$. Let the probability that the ℓ points $V_{I_1}, \ldots, V_{I_\ell}$ are pairwise orthogonal be p_n. Then the expected number of ℓ-cliques in G is $p_n \cdot \binom{n}{\ell}$. Fix a choice $v_1, \ldots, v_n$ of elements in S^{d-1} such that the corresponding graph G on $[n]$ has at least $p_n \cdot \binom{n}{\ell}$ ℓ-cliques.

But note that the graph G if K_{d+1}-free since there cannot be more than d pairwise orthogonal vectors in $\mathbb{R}^d$. By a generalization of Turán's theorem due to Zykov [Zyk49] (see Turán's Theorem for Maximizing Other Quantities), we know that the number of ℓ-cliques in G is at most

$$\binom{n}{\ell} \cdot \frac{d!}{(d-\ell)! \cdot d^\ell}$$

Therefore

$$\left\lceil p_n \binom{n}{\ell} \right\rceil \leq \binom{n}{\ell} \cdot \frac{d!}{(d-\ell)! \cdot d^\ell} \qquad \Rightarrow \qquad p_n + o(1) \leq \frac{d!}{(d-\ell)! \cdot d^\ell}$$

Finally, since $p_n \to p$ as $n \to \infty$, we have the claim. ■

An immediate consequence of the above is the following, which we record separately.

Corollary 2.3. *Let $d \geq 1$ and $\mu \in \mathcal{P}(S^{d-1})$. Then*

$$\mu \otimes \mu(\{(u,v) \in (S^{d-1})^2 : u \perp v\}) \leq \frac{d-1}{d}$$

Below we state a simple proposition concerning the growth of binomial coefficients, which plays an important role in bounding a key quantity that arises in the proof of Theorem 1.1.

Proposition 2.4. *Let $q \geq 2$ be an integer and let $\alpha > \frac{1}{q+1}$. Then there exists a constant $c_\alpha > 0$ (depending only on α) such that*

$$\sum_{m=0}^{\alpha n} \binom{n}{m} q^{-m} \;\geq\; \left(\frac{q+1}{q}\right)^n \left(1 - \exp(-c_\alpha n)\right)$$

for all sufficiently large n.

Proof. Let $p = \frac{1}{q+1}$ and write $\alpha = p + \varepsilon$ with $\varepsilon > 0$. Let $X_1, \ldots, X_n$ be independent Bernoulli random variables with $X_i \sim \mathrm{Be}(p)$, and set $X = \sum_{i=1}^n X_i$. Then $\mathbb{E}[X] = np$. By the Chernoff bound,

$$\Pr\big[X > n\alpha\big] = \Pr\big[X > n(p+\varepsilon)\big] \;\leq\; \exp(-2n\varepsilon^2),$$

and hence

$$\Pr\big[X \leq n\alpha\big] \;\geq\; 1 - \exp(-2n\varepsilon^2).$$

On the other hand,

$$\Pr\big[X \leq n\alpha\big] = \sum_{m=0}^{\alpha n} \Pr[X = m] = \sum_{m=0}^{\alpha n} \binom{n}{m} p^m (1-p)^{n-m}.$$

Rewriting,

$$\Pr[X \leq n\alpha] = \left(\frac{q}{q+1}\right)^n \sum_{m=0}^{\alpha n} \binom{n}{m} q^{-m}.$$

Combining the inequalities gives

$$\sum_{m=0}^{\alpha n} \binom{n}{m} q^{-m} \;\geq\; \left(\frac{q+1}{q}\right)^n \Big(1 - \exp(-2n\varepsilon^2)\Big).$$

Setting $c_\alpha := 2(\alpha - \frac{1}{q+1})^2$ completes the proof. ∎

3 PROOF OF THEOREM 1.1

Proof of Theorem 1.1. We begin by defining the key local construction that encodes the relationship between two vectors into a subspace of $\mathbb{R}^3$. Let $\mathcal{S}(\mathbb{R}^3)$ denote the set of all the linear subspaces of $\mathbb{R}^3$ and

$$f : \mathbb{R}^3 \setminus \{0\} \times \mathbb{R}^3 \setminus \{0\} \;\to\; \mathcal{S}(\mathbb{R}^3)$$

be given by

$$f(u,v) = \begin{cases} u^\perp \cap v^\perp, & \text{if } u \perp v, \\ u^\perp, & \text{otherwise.} \end{cases}$$

Here $u^\perp$ denotes the orthogonal complement of u in $\mathbb{R}^3$. For $x, y \in C$, define the *pair subspace*

$$E_{x,y} \;:=\; \bigotimes_{i=1}^{n} f(x_i, y_i) \;\subset\; \bigotimes_{i=1}^{n} \mathbb{R}^3,$$

where $\otimes$ denotes the tensor product of spaces. By construction,

$$\dim E_{x,y} \;=\; 2^{A(x,y)},$$

where

$$A(x,y) \;:=\; \big|\{\, i \in [n] : \langle x_i, y_i \rangle \neq 0 \,\}\big|$$

is the number of coordinates where x_i and y_i are *not* orthogonal. For any subspace $S \subset \mathbb{R}^3$, let $P_S : \mathbb{R}^3 \to \mathbb{R}^3$ denote the orthogonal projection onto S. For $x, y \in C$, define

$$P_{x,y} \;:=\; \bigotimes_{i=1}^{n} P_{f(x_i,y_i)}.$$

We now equip C with a fixed total order.

Proposition 3.1. *Let $x, y, a, b \in C$ with $x < y$ and $a < b$ in the total order. Then*

$$P_{x,y}(E_{a,b}) \;=\; \begin{cases} \{0\}, & \text{if } (a,b) \neq (x,y), \\ E_{a,b}, & \text{if } (a,b) = (x,y). \end{cases}$$

Proof. We consider cases.

Case 1: $a \neq x$ and $a \neq y$.

In this case, a, x, y are pairwise distinct. By the vector trifference property, there exists $k \in [n]$ such that a_k, x_k, y_k are mutually orthogonal. In this coordinate, $f(x_k, y_k) = x_k^\perp \cap y_k \perp= \operatorname{span}(a_k)$, while $f(a_k, b_k) \subset a_k^\perp = \operatorname{span}\{x_k, y_k\}$. Thus $P_{f(x_k,y_k)}(f(a_k, b_k)) = \{0\}$, forcing $P_{x,y}(E_{a,b}) = \{0\}$.

Case 2: $a \neq x$ but $a = y$.

Here x, a, b are pairwise distinct. Again, vector trifference gives a coordinate k where x_k, a_k, b_k are mutually orthogonal. Here $f(a_k, b_k) = a_k^\perp \cap b_k^\perp$, and the projection is onto $f(x_k, y_k) = \operatorname{span}(a_k)$, so the projection is zero.

Case 3: $a = x$ but $b \neq y$.

A symmetric argument to Case 2 applies.

In all cases except $(a, b) = (x, y)$, the projection is zero. If $(a, b) = (x, y)$, the projection is the identity on $E_{x,y}$ by definition. ∎

Proposition 3.2.

$$\sum_{\substack{x,y \in C \\ x \leq y}} E_{x,y} \;=\; \bigoplus_{\substack{x,y \in C \\ x \leq y}} E_{x,y}.$$

Proof. Suppose $\sum_{x<y} v_{x,y} = 0$ with each $v_{x,y} \in E_{x,y}$. Applying $P_{x,y}$ and using the previous claim isolates $v_{x,y}$, forcing $v_{x,y} = 0$ for all pairs. Thus the sum is direct. ■

From this direct sum property, the sum of the dimensions is bounded by the ambient dimension:

$$\sum_{\{x,y\} \in \binom{C}{2}} \dim(E_{x,y}) \;\le\; \dim\left((\mathbb{R}^3)^{\otimes n}\right) \;=\; 3^n.$$

Since $\dim(E_{x,y}) = 2^{A(x,y)}$, we have

$$\binom{|C|}{2} \cdot \mathbb{E}_{\{x,y\}}[\, 2^{A(x,y)}\,] \;\le\; 3^n. \tag{1}$$

Next, note that

$$\mathop{\mathbb{E}}_{(x,y)\in C^2}[\, 2^{A(x,y)}\,] = \Pr[x \neq y] \cdot \mathop{\mathbb{E}}_{\{x,y\}\in\binom{C}{2}}[\, 2^{A(x,y)}\,] \quad + \quad \Pr[x = y] \cdot \mathop{\mathbb{E}}_{x\in C}[\, 2^{A(x,x)}\,].$$

Since $A(x,x) = n$, this becomes

$$\mathop{\mathbb{E}}_{(x,y)\in C^2}[\, 2^{A(x,y)}\,] = \frac{|C|-1}{|C|} \cdot \mathop{\mathbb{E}}_{\{x,y\}\in\binom{C}{2}}[\, 2^{A(x,y)}\,] + \frac{2^n}{|C|}.$$

Using (1), we deduce

$$\mathop{\mathbb{E}}_{(x,y)\in C^2}[\, 2^{A(x,y)}\,] \;\le\; \frac{2\cdot 3^n}{|C|^2} + \frac{2^n}{|C|}. \tag{2}$$

Now expand $2^{A(x,y)}$ as

$$2^{A(x,y)} \;=\; \prod_{k=1}^{n} \big(1 + 1[\, x_k \not\perp y_k\,]\big) \;=\; \sum_{S\subset[n]} \prod_{s\in S} 1[\, x_s \not\perp y_s\,].$$

Taking expectations,

$$\mathop{\mathbb{E}}_{(x,y)\in C^2}[\, 2^{A(x,y)}\,] = \sum_{S\subset[n]} \Pr_{(x,y)\in C^2}\big[\, x_s \not\perp y_s \;\forall s \in S\,\big].$$

For any $S \subset [n]$, two lower bounds hold:

- *Trivial bound:* If $x = y$, the event holds automatically, so

$$\Pr[\, x_s \not\perp y_s \;\forall s \in S\,] \;\ge\; \frac{1}{|C|}. \tag{3}$$

- *Geometric bound:* By Corollary 2.3, two independent vectors in $\mathbb{R}^3$ are non-orthogonal with probability at least $1/3$, hence

$$\Pr[\, x_s \not\perp y_s \;\forall s \in S\,] \;\ge\; \left(\frac{1}{3}\right)^{|S|} \tag{4}$$

  This requires some justification. We cannot apply Corollary 2.3 by "successively conditioning," since the independence clause needed by the lemma may not longer be satisfied as soon as we

condition even on a single $s \in S$. But, fortunately, we can get around this by passing to a suitable space, namely $\bigotimes_{s\in S} \mathbb{R}^3$. We equip $\bigotimes_{s\in S} \mathbb{R}^3$ with the natural inner product obtained by tensoring the usual innder product on $\mathbb{R}^3$. The crucial, yet simple observation is

$$\Pr[\, x_s \not\perp y_s \ \forall s \in S\,] = \Pr\left[\otimes_{s\in S} x_s \not\perp \otimes_{s\in S} y_s\right]$$

The vectors $\otimes_{s\in S} x_s$ and $\otimes_{s\in S} y_s$ are unit vectors in $\bigotimes_{s\in S} \mathbb{R}^3$. Also, if x and y were picked independently from C, then $\otimes_{s\in S} x_s$ and $\otimes_{s\in S} y_s$ are independently picked from the unit sphere in $\bigotimes_{s\in S} \mathbb{R}^3$, both affording the same distribution. Thus we can apply Corollary 2.3 and get

$$\Pr[\, x_s \not\perp y_s \ \forall s \in S\,] \;=\; \Pr\left[\otimes_{s\in S} x_s \not\perp \otimes_{s\in S} y_s\right] \;\geq\; \frac{1}{3^{|S|}}$$

Combining (3) and (4), we obtain for every $S \subset [n]$:

$$\Pr_{(x,y)\in C^2}\left[\, x_s \not\perp y_s \ \forall s \in S\,\right] \;\geq\; \max\left\{\frac{1}{3^{|S|}},\; \frac{1}{|C|}\right\}. \tag{5}$$

Substituting (5) into the expansion of $\mathbb{E}[2^{A(x,y)}]$ gives

$$\mathop{\mathbb{E}}_{(x,y)\in C^2}\left[\, 2^{A(x,y)}\,\right] \;\geq\; \sum_{S\subset[n]} \max\left\{\frac{1}{3^{|S|}},\; \frac{1}{|C|}\right\}.$$

Grouping terms by $k = |S|$ and introducing a cutoff parameter $0 < \alpha \leq 1$, we split the sum into two regimes:

$$\mathbb{E}_{(x,y)\in C^2}\left[\, 2^{A(x,y)}\,\right] \;\geq\; \sum_{0\leq k\leq \alpha n} \binom{n}{k}\frac{1}{3^k} \;+\; \sum_{\alpha n < k \leq n} \binom{n}{k}\frac{1}{|C|}. \tag{6}$$

Recall from (2) that

$$\mathop{\mathbb{E}}_{(x,y)\in C^2}\left[\, 2^{A(x,y)}\,\right] - \frac{2^n}{|C|} \;\leq\; \frac{2\cdot 3^n}{|C|^2}. \tag{7}$$

Combining (6) and (7) yields

$$\left[\sum_{0\leq k\leq \alpha n} \binom{n}{k}\frac{1}{3^k} \;+\; \frac{1}{|C|}\sum_{\alpha n < k \leq n} \binom{n}{k}\right] - \frac{2^n}{|C|} \;\leq\; \frac{2\cdot 3^n}{|C|^2}.$$

Rearranging the middle term by noting that

$$\sum_{\alpha n < k \leq n} \binom{n}{k} = 2^n - \sum_{0\leq k\leq \alpha n} \binom{n}{k},$$

we can rewrite the inequality as

$$\sum_{0\leq k\leq \alpha n} \binom{n}{k}\frac{1}{3^k} \;-\; \frac{1}{|C|}\sum_{0\leq k\leq \alpha n} \binom{n}{k} \;\leq\; \frac{2\cdot 3^n}{|C|^2}.$$

At this point we invoke Proposition 2.4: for any $\alpha > \frac{1}{4}$, there exists $c_\alpha > 0$ such that

$$\sum_{0\leq k\leq \alpha n} \binom{n}{k} 3^{-k} \;\geq\; \left(\frac{4}{3}\right)^n \left(1 - e^{-c_\alpha n}\right).$$

Moreover, for such α the hypergeometric sum $\sum_{0\le k\le \alpha n}\binom{n}{k}$ is $o(2^n)$, so the second term

$$\frac{1}{|C|}\sum_{0\le k\le \alpha n}\binom{n}{k}$$

is negligible compared to the first when $|C|$ is exponential in n. Thus, as $n\to\infty$,

$$\left(\frac{4}{3}\right)^n(1-o(1)) \;\le\; \frac{2\cdot 3^n}{|C|^2}.$$

Rearranging gives

$$|C|^2 \;\le\; 2\cdot\left(\frac{3}{2}\right)^n(1+o(1)),$$

and hence

$$|C| \;\le\; (\sqrt{2}+o(1))\left(\frac{3}{2}\right)^n.$$

as $n\to\infty$. This completes the proof. ■

4 PROOF OF THEOREM 1.3

We now turn our attention to vector k-separating codes as mentioned in subsection 1.4.

Proof of Theorem 1.3. Let $\mathcal{C}\subseteq(S^{k-1})^n$ be a vector k-separating code of block length n. We want to put an upper bound on the size of $\mathcal{C}$. Let $\ell=k-2$ and $X_1,\dots,X_\ell$ be randomly chosen from $\mathcal{C}$ such that the set $\mathcal{X}=\{X_1,\dots,X_\ell\}$ is a uniformly random element of $\binom{\mathcal{C}}{\ell}$. Consider the complete graph $G_{\mathcal{X}}$ whose vertex-set is $\mathcal{C}\setminus\mathcal{X}$. For distinct vertices a and b of $G_{\mathcal{X}}$, we color the edge between a and b by the symbol j if j is the smallest element in $[n]$ such that $a_j, b_j, X_1,\dots,X_\ell$ are pairwise orthogonal. Such a j must exist because of the k-separating property of the code $\mathcal{C}$.

Let $G_{\mathcal{X}}^{(j)}$ denote the graph whose vertex-set is $\mathcal{C}\setminus\mathcal{X}$ and whose edge set consists of all the j-colored edges. Note that $G_{\mathcal{X}}^{(j)}$ is a bipartite graph. This is because, if there is at least one j-colored edge, then the vectors $X_1(j),\dots,X_\ell(j)$ span a $\ell(=k-2)$-dimensional subspace of $\mathbb{R}^k$, and the j-th entries of the endpoints any j-colored edge lie in the orthogonal complement of this subspace, which is just a copy of $\mathbb{R}^2$. It follows that any odd cycle in $G_{\mathcal{X}}^{(j)}$ produces an odd-length closed walk in the orthogonality graph of S^1. But this latter graph is bipartite since it is a disjoint union of 4-cycles. Therefore, there cannot be any odd cycle in $G_{\mathcal{X}}^{(j)}$ and hence it is a bipartite graph.

It is clear that

$$G_{\mathcal{X}} = G_{\mathcal{X}}^{(1)}\cup\cdots\cup G_{\mathcal{X}}^{(n)}$$

If $\tau_{\mathcal{X}}^{(j)}$ denote the fraction of non-isolated vertices of $G_{\mathcal{X}}^{(j)}$, then by Hansel lemma we know that

$$\log(|\mathcal{C}|-\ell)=\log|G_{\mathcal{X}}|\le\sum_{j=1}^{n}\tau_{\mathcal{X}}^{(j)}$$

Taking expectation, we can write

$$\log(|\mathcal{C}|-\ell)\le\sum_{j=1}^{n}\mathbb{E}[\tau_{\mathcal{X}}^{(j)}] \qquad (*)$$

Let us think about how to upper bound $\mathbb{E}[\tau_{\mathcal{X}}^{(j)}]$. This is same as the probability that a vertex in $G_{\mathcal{X}}$ selected uniformly at random is non-isolated in $G_{\mathcal{X}}^{(j)}$. This is clearly upper bounded by the probability that a vertex V in $G_{\mathcal{X}}^{(j)}$ selected uniformly at random is such that the vectors $X_1, \ldots, X_\ell, V$ are pairwise orthogonal. But $\{X_1, \ldots, X_\ell, V\}$ is just a uniformly random subset of $\binom{\mathcal{C}}{\ell+1}$. For the sake of more convenient notation, let $\mathcal{S} = \{S_1, \ldots, S_{\ell+1}\}$ be a uniformly random subset of $\mathcal{C}$ of size $\ell + 1$. Thus, form (*), we have

$$\log(|\mathcal{C}| - \ell) \leq n \Pr[S_i \perp S_j \text{ for all } i \neq j] \quad \Rightarrow \quad \frac{\log(|\mathcal{C}| - \ell)}{n} \leq \Pr[S_i \perp S_j \text{ for all } i \neq j] \qquad (**)$$

We would like to invoke Lemma 2.2 to upper bound the RHS of the above to finish the proof. But to do that we need to work with samples *with* replacement. To this end, let $Y_1, \ldots, Y_{\ell+1}$ be uniformly and independently chosen from $\mathcal{C}$. Noting that

$$\begin{aligned}
&\Pr[Y_i \perp Y_j \text{ for all } i \neq j] \\
&= \Pr[Y_i \perp Y_j \text{ for all } i \neq j |\ Y_1, \ldots, Y_{\ell+1} \text{ are pairwise distinct}] \cdot \Pr[Y_1, \ldots, Y_{\ell+1} \text{ are pairwise distinct}] \\
&= \Pr[S_i \perp S_j \text{ for all } i \neq j] \cdot \left[\left(1 - \frac{1}{|\mathcal{C}|}\right) \cdot \left(1 - \frac{2}{|\mathcal{C}|}\right) \cdot \cdots \cdot \left(1 - \frac{\ell}{|\mathcal{C}|}\right)\right] \\
&\geq \Pr[S_i \perp S_j \text{ for all } i \neq j] \cdot \left(1 - \frac{\ell}{|\mathcal{C}|}\right)^\ell
\end{aligned}$$

From this and (**) we get

$$\frac{\log(|\mathcal{C}| - \ell)}{n} \leq \Pr[Y_i \perp Y_j \text{ for all } i \neq j] \cdot \frac{1}{\left(1 - \frac{\ell}{|\mathcal{C}|}\right)^\ell} \leq \Pr[Y_i \perp Y_j \text{ for all } i \neq j] \cdot \frac{1}{1 - \frac{\ell^2}{|\mathcal{C}|}}$$

where we have used the fact that $(1 - x)^n \geq 1 - nx$ if $x \in (0, 1)$ and $n \geq 1$. This gives

$$\left(1 - \frac{\ell^2}{|\mathcal{C}|}\right) \cdot \frac{\log(|\mathcal{C}| - \ell)}{n} \leq \Pr[Y_i \perp Y_j \text{ for all } i \neq j]. \qquad (\dagger)$$

But by Lemma 2.2 we also know that

$$\Pr[Y_i \perp Y_j \text{ for all } i \neq j] \leq \frac{k!}{(k - (\ell + 1))! \cdot k^{\ell+1}} = \frac{k!}{k^{k-1}}$$

Using this in (†) we get

$$\left(1 - \frac{\ell^2}{|\mathcal{C}|}\right) \cdot \frac{\log(|\mathcal{C}| - \ell)}{n} \leq \frac{k!}{k^{k-1}}$$

The desired result is now obvious since $|\mathcal{C}|$ is large compared to ℓ. ■

5 REANALYZING THE DISCRETE SETTING USING THE PROOF OF THEOREM 1.1

We now focus our attention to classical discrete setting. Let $\Sigma = \{0, 1, 2\}^n$ and $\mathcal{C} \subseteq \Sigma^n$ be a trifferent code.

1. First, we show how the proof idea of Theorem 1.1 shows that $|\mathcal{C}| < (1 + o(1)) \cdot (3/2)^n$
2. Then, we show how we can import an idea from [BK25] to show $|\mathcal{C}| \lesssim (n^{-1/4} \cdot (3/2)^n)$.

Proposition 5.1. $|\mathcal{C}| \leq (1 + o(1)) \cdot (3/2)^n$.

Proof. Define a bipartite graph $G = (U, V)$, where

$$U = \binom{\mathcal{C}}{2} \quad \text{and} \quad V = \Sigma^n,$$

and we join an edge between $\{x, y\} \in U$ with $a \in V$ if and only if both x and y differ from a in every coordinate. More precisely, we join an edge between $\{x, y\} \in U$ and $a \in V$ if

$$x_i \neq a_i \quad \text{and} \quad y_i \neq a_i$$

for all $i \in [n]$. The fact that $\mathcal{C}$ is a trifferent code implies that no vertex in V can have degree greater than 1. Also, for each $\{x, y\}$ in U we have

$$\deg(\{x, y\}) = 2^{A(x,y)}$$

where $A(x, y) = |\{i \in [n] : \ x_i = y_i\}|$. By double counting, we have

$$\sum_{u \in U} \deg(u) = \sum_{v \in V} \deg(v)$$

We will lower bound the left hand side and upper bound the right hand side to obtain the desired bound. The left hand side is

$$\sum_{u \in U} \deg(u) = \sum_{\{x,y\} \in \binom{\mathcal{C}}{2}} \deg(\{x, y\}) = \sum_{\{x,y\} \in \binom{\mathcal{C}}{2}} 2^{A(x,y)} = \binom{|\mathcal{C}|}{2} \mathop{\mathbb{E}}_{\{x,y\} \in \binom{\mathcal{C}}{2}} [2^{A(x,y)}] \tag{*}$$

Next, we show the following

$$\left(\frac{4}{3}\right)^n (1 - o(1)) \leq \mathop{\mathbb{E}}_{\{x,y\} \in \binom{\mathcal{C}}{2}} [2^{A(x,y)}].$$

The notion of randomness we have chooses a 2-element subset of $\mathcal{C}$ uniformly at random. It is convenient to convert this random model to the one where we choose two elements of $\mathcal{C}$ successively, with repetition allowed. To this end, we write

$$\mathop{\mathbb{E}}_{(x,y) \in \mathcal{C}^2} [2^{A(x,y)}] = \mathop{\mathbb{P}}_{(x,y) \in \mathcal{C}^2} [x \neq y] \cdot \mathop{\mathbb{E}}_{\{x,y\} \in \binom{\mathcal{C}}{2}} [2^{A(x,y)}] \quad + \mathop{\mathbb{P}}_{(x,y) \in \mathcal{C}^2} [x = y] \cdot 2^n$$

Thus

$$\mathop{\mathbb{E}}_{(x,y) \in \mathcal{C}^2} [2^{A(x,y)}] = \left(1 - \frac{1}{|\mathcal{C}|}\right) \mathop{\mathbb{E}}_{\{x,y\} \in \binom{\mathcal{C}}{2}} [2^{A(x,y)}] + \frac{2^n}{|\mathcal{C}|} \tag{1}$$

So we will lower bound the left hand side in the above. We have

$$2^{A(x,y)} = \prod_{i \in [n]} (1 + 1[x_i = y_i]) = \sum_{S \subseteq [n]} 1[x_S = y_S]$$

where "$x_S = y_S$" means that $x_s = y_s$ for all $s \in S$. Since the probability of $x_S = y_S$ is at least the collision probability for two uniformly and independently chosen elements from Σ^S, we have

$$\mathop{\mathbb{E}}_{(x,y)\in\mathcal{C}^2}[1[x_S = y_S]] \geq (1/3)^{|S|} \tag{5.1}$$

We also have the *trivial bound* that

$$\Pr[\, x_S = y_S \,] \geq \Pr[x = y] \geq \frac{1}{|\mathcal{C}|}.$$

Combining these, we obtain for every $S \subset [n]$:

$$\Pr_{(x,y)\in C^2}\left[\, x_S = y_S \,\right] \geq \max\left\{\frac{1}{3^{|S|}},\ \frac{1}{|\mathcal{C}|}\right\} \qquad \Rightarrow \qquad \mathop{\mathbb{E}}_{(x,y)\in C^2}[\, 2^{A(x,y)} \,] \geq \sum_{S\subset[n]} \max\left\{\frac{1}{3^{|S|}},\ \frac{1}{|\mathcal{C}|}\right\}.$$

Grouping terms by $k = |S|$ and introducing a cutoff parameter $0 < \alpha \leq 1$, we split the sum into two regimes:

$$\mathbb{E}_{(x,y)\in C^2}[\, 2^{A(x,y)} \,] \ \geq \ \sum_{0\leq k\leq \alpha n} \binom{n}{k}\frac{1}{3^k} \ + \ \sum_{\alpha n < k \leq n} \binom{n}{k}\frac{1}{|C|}. \tag{2}$$

Using this in (1) we get

$$\sum_{0\leq k\leq \alpha n} \binom{n}{k}\frac{1}{3^k} + \sum_{\alpha n < k \leq n} \binom{n}{k}\frac{1}{|C|} \leq \left(1 - \frac{1}{|\mathcal{C}|}\right) \mathop{\mathbb{E}}_{\{x,y\}\in\binom{\mathcal{C}}{2}}[2^{A(x,y)}] + \frac{2^n}{|\mathcal{C}|}$$

which gives

$$\sum_{0\leq k\leq \alpha n} \binom{n}{k}\frac{1}{3^k} + \left[\sum_{\alpha n < k \leq n} \binom{n}{k}\frac{1}{|\mathcal{C}|} - \frac{2^n}{|\mathcal{C}|}\right] \leq \left(1 - \frac{1}{|\mathcal{C}|}\right) \mathop{\mathbb{E}}_{\{x,y\}\in\binom{\mathcal{C}}{2}}[2^{A(x,y)}]$$

Writing 2^n as $\sum_{k=0}^{n}\binom{n}{k}$ we get

$$\sum_{0\leq k\leq \alpha n} \binom{n}{k}\frac{1}{3^k} + \sum_{0\leq k\leq \alpha n} \binom{n}{k}\frac{1}{|\mathcal{C}|} \leq \left(1 - \frac{1}{|\mathcal{C}|}\right) \mathop{\mathbb{E}}_{\{x,y\}\in\binom{\mathcal{C}}{2}}[2^{A(x,y)}]$$

The first term in the left hand side is $\left(\frac{4}{3}\right)^n(1 - o(1))$ (see Proposition 2.4) and the second term is $o(2^n)/|\mathcal{C}|$ whence the lemma follows.

From the above argument and from (*) we have

$$\binom{|\mathcal{C}|}{2}\left(\frac{4}{3}\right)^n(1 - o(1)) \leq \sum_{u\in U}\deg(u) \tag{**}$$

Now for the right hand side. We have

$$\sum_{v\in V}\deg(v) = \sum_{x\in\Sigma^n}\deg(x) = 3^n \mathop{\mathbb{E}}_{x\in\Sigma^n}[\deg(x)]$$

But note that, by definition of our bipartite graph and by the fact that $\mathcal{C}$ is a trifferent code, we have $\deg(v)$ is either 0 or 1 for any $v \in V$. In fact, if for any $v \in V$ we define

$$H_v = \{x \in \Sigma^n : \Delta(x, v) = n\} \quad \text{and} \quad h_v = |H_v \cap \mathcal{C}|$$

then $\deg(v) = \binom{h_v}{2}$. Thus

$$\sum_{v \in V} \deg(v) = 3^n \cdot \Pr_v[h_v = 2] = 3^n \cdot \mathbb{E}_v[1[h_v = 2]]$$

Applying Markov, we get

$$\begin{aligned}
\sum_{v \in V} \deg(v) &\leq 3^n \cdot \frac{\mathbb{E}_v[h_v]}{2} \\
&= \frac{3^n}{2} \cdot \mathop{\mathbb{E}}_v \left[\sum_{x \in \mathcal{C}} 1[x \in H_v] \right] \\
&= \sum_{x \in \mathcal{C}} \frac{3^n}{2} \cdot \Pr_v[x \in H_v] \\
&= \frac{3^n}{2} \cdot |\mathcal{C}| \cdot \left(\frac{2}{3}\right)^n = 2^{n-1} \cdot |\mathcal{C}|
\end{aligned}$$

Using this in (**) and using the double counting, we have

$$\binom{|\mathcal{C}|}{2} \cdot \left(\frac{4}{3}\right)^n \leq 2^{n-1}|\mathcal{C}| \qquad \Rightarrow \qquad |\mathcal{C}| - 1 \leq \left(\frac{3}{2}\right)^n$$

which shows that $|\mathcal{C}| = (1 + o(1)) \left(\frac{3}{2}\right)^n$. ■

Next, we give a brief proof sketch on adapting the idea in [BK25] to obtain a polynomial factor improvement.

Proposition 5.2. $|\mathcal{C}| \lesssim n^{-1/4} \cdot (3/2)^n$

Proof Sketch. To show this we adapt the proof of Proposition 5.1. We modify the definition of the bipartite graph $G = (U, V)$ as below. The modification is to relax the criterion used in the above proof which governs the edge structure. Let $Agr(x, y)$ denote the set of coordinates where x and y agree.

$$U = \binom{\mathcal{C}}{2} \quad \text{and} \quad V = \Sigma^n,$$

and we join an edge between $\{x, y\} \in U$ with $a \in V$ iff

$$|\{i \in Agr(x, y) \mid a_i \in \{x_i, y_i\}\}| = 2 \quad \text{and} \quad |\{i \notin Agr(x, y) \mid a_i \in \{x_i, y_i\}\}| = 0.$$

In the proof above, the condition was $|\{i \in [n] \mid a_i \in \{x_i, y_i\}\}| = 0$. Hence, we have relaxed the condition for edge existence whenever $i \in Agr(x, y)$. To understand this condition better let us take the example of $a = \mathbf{2}$, i.e., the all 2's string. By the above condition a pair of strings $\{x, y\}$ is joined to a iff there are at most two coordinates $i \in [n]$ such that the symbol 2 appears in x_i, y_i and in those coordinates $x_i = y_i$.

The questions now becomes what are the left and right degree of this bipartite graph.

1. For the left degree: this can be computed in a manner similar to the one used in Proposition 5.1. It turns out that there is roughly a quadratic increase in the left degree due to the relaxed conditions, i.e.,

$$n^2 \times \binom{|\mathcal{C}|}{2} \left(\frac{4}{3}\right)^n \lesssim \sum_{u \in U} \deg(u)$$

2. For the right degree: the fact that $\mathcal{C}$ is a trifferent code implies that no vertex in V can have degree greater than $\approx n^{3/2}$. To see this consider a string in V, say $a = \mathbf{2}$. Let $N(a)$ be the neighborhood of a. Construct a graph H where the vertex set is $[n]$ and we join i and j if there exists a pair $\{x, y\} \in N(a)$ such that $x_i = y_i = 2$. Hence, the number of edges in H is $|N(a)|$. Following the arguments from [BK25], it is possible to verfiy that H is 4-cycle free and then by the famous result of Kővári, Sós and Turán [KST54], known popularly as the KST theorem, we have our desired bound.

Combining the above observations yields the $n^{-1/4}$ improvement. ■

REFERENCES

[Ari94] Erdal Arikan. An upper bound on the zero-error list-coding capacity. *IEEE Trans. Inform. Theory*, 40(4):1237–1240, 1994.

[BD25] Matija Bucić and James Davies. Geometric graphs with exponential chromatic number and arbitrary girth. *The American Mathematical Monthly*, pages 1–12, 2025.

[BDGP23] Anurag Bishnoi, Jozefien D'haeseleer, Dion Gijswijt, and Aditya Potukuchi. Blocking sets, minimal codes and trifferent codes, 2023.

[BK25] Siddharth Bhandari and Abhishek Khetan. Improved upper bound for the size of a trifferent code. *Combinatorica*, 45(1):Paper No. 2, 14, 2025.

[BKK+25] Anurag Bishnoi, Bartłomiej Kielak, Benedek Kovács, Zoltán Lóránt Nagy, Gábor Somlai, Máté Vizer, and Zeyu Zheng. The generalized trifference problem. *arXiv preprint arXiv:2505.07706*, 2025.

[BR22] 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, 2022.

[CD21] Simone Costa and Marco Dalai. New bounds for perfect k-hashing. *Discrete Appl. Math.*, 289:374–382, 2021.

[CRRS06] Sourav Chakraborty, Jaikumar Radhakrishnan, Nandakumar Raghunathan, and Prashant Sasatte. Zero error list-decoding capacity of the $q/(q-1)$ channel. In S. Arun-Kumar and Naveen Garg, editors, *Proc. 26th IARCS Annual Conf. on Foundations of Software Tech. and Theoretical Comp. Science (FSTTCS)*, volume 4337 of *LNCS*, pages 129–138. Springer, 2006.

[DFD24] Stefano Della Fiore and Marco Dalai. Upper bounds on the rate of linear q-ary k-hash codes. In *2024 IEEE International Symposium on Information Theory (ISIT)*, pages 2610–2615. IEEE, 2024.

[DGR20] Marco Dalai, Venkatesan Guruswami, and Jaikumar Radhakrishnan. An improved bound on the zero-error list-decoding capacity of the 4/3 channel. *IEEE Trans. Inform. Theory*, 66(2):749–756, 2020.

[Eli88] Peter Elias. Zero error capacity under list decoding. *IEEE Trans. Inform. Theory*, 34(5):1070–1074, 1988.

[FD25] Stefano Della Fiore and Marco Dalai. Bounds on k-hash distances and rates of linear codes, 2025.

[FGP22] 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.

[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.

[GR22] Venkatesan Guruswami and Andrii Riazanov. Beating Fredman-Komlós for perfect k-hashing. *J. Combin. Theory Ser. A*, 188:Paper No. 105580, 21, 2022.

[GW94] Michel X. Goemans and David P. Williamson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. In *Proceedings of the 26th Annual ACM Symposium on Theory of Computing (STOC)*, pages 422–431, 1994.

[GZ12] C. D. Godsil and J. Zaks. Colouring the sphere. 2012.

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

[KST54] Tamás Kővári, Vera T. Sós, and Pál Turán. On a problem of K. Zarankiewicz. *Colloquium Mathematicum*, 3:50–57, 1954.

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

[Lov79] László Lovász. On the shannon capacity of a graph. *IEEE Transactions on Information Theory*, 25(1):1–7, 1979.

[Per19] AnaMaria Perez. On generalizations of the double cap conjecture, 2019.

[PZ22] Cosmin Pohoata and Dmitriy Zakharov. On the trifference problem for linear codes. *IEEE Transactions on Information Theory*, 68(11):7096–7099, 2022.

[Wit74] H. S. Witsenhausen. Spherical sets without orthogonal point pairs. *Amer. Math. Monthly*, 81:1101–1102, 1974.

[Zak25] Dmitrii Zakharov. Spherical sets avoiding orthonormal bases. 2025.

[Zyk49] A. A. Zykov. O nekotorykh svoistvakh lineinykh kompleksov. *Matematicheskii sbornik*, 24(2):163–188, 1949. Title translated as: "On some properties of linear complexes".