

THE INJECTIVE NORM OF CSS QUANTUM ERROR-CORRECTING CODES

STEPHANE DARTOIS

*École Polytechnique, Institut Polytechnique de Paris, Centre de Mathématiques Laurent Schwartz,
91120 Palaiseau, France*

GILLES ZÉMOR

*Institut de Mathématiques de Bordeaux, UMR 5251, 351 Cours de la Libération, 33400 Talence,
France*

Institut Universitaire de France

ABSTRACT. In this paper, we compute the injective norm — *a.k.a.* geometric entanglement — of standard basis states of CSS quantum error-correcting codes. The injective norm of a quantum state is a measure of genuine multipartite entanglement. Computing this measure is generically NP-hard. However, it has been exactly computed in condensed matter theory — notably in the context of topological phases — for the Kitaev code and its extensions, in works by Orús and collaborators. We extend these results to all CSS codes and thereby obtain the injective norm for a nontrivial, infinite family of quantum states. In doing so, we uncover an interesting connection to matroid theory and Edmonds’ intersection theorem.

Keywords: Geometric entanglement, CSS codes, injective norm, matroids, Edmonds’ intersection theorem

1. INTRODUCTION

1.1. Context. We are interested in the multipartite entanglement of the standard basis states of arbitrary CSS quantum error-correcting codes [CS96, Ste96]. Such families of quantum states are of great importance in quantum information and computation, and some of them also appear frequently in condensed matter theory, indeed, LDPC codes can often be seen as phases of matter [KL10, Haa13, Yos15, YL24, PRBK24]. We show that the exact value of the geometric entanglement for these states is entirely dictated by the dimensions of the shortened codes of the classical X code. Our work can be seen as a broad generalization of results obtained in the physics literature [OW11, OWBVdN14], with the key distinction that our arguments do not rely on any specific geometric or locality structure, and therefore apply to all CSS codes.

Among the motivations for this work lies the fact that the structure of many-body or multipartite entanglement is only poorly understood in spite of its importance for many applications.

E-mail addresses: `stephane.dartois@polytechnique.edu`, `zemor@math.u-bordeaux.fr`.

One of the well-known measures of multipartite entanglement is the injective norm, whose definition we recall in equation (1) below. The goal of this work is to benchmark the injective norm against a family of interesting quantum states provided by quantum error correcting codes. Computing the injective norm of a quantum state is an NP-hard problem [HL13], therefore finding families of states for which it can be explicitly computed is an interesting problem by and for itself. In fact, there are a number of works in the literature which study the behavior of the injective norm of families of simple enough quantum states [WG03, ZCH10] or focus on finding maximally entangled multipartite states with respect to the injective norm [AMM10, SG24].

A series of strong results were recently obtained concerning the typical behavior of the injective norm of random tensors and random quantum states, both in mathematics [DM24, BGJ⁺24, Boe24, BS25, Sto25] and from the viewpoint of physicists [Sas24]. The methods used in these studies broadly come from landscape complexity, statistical physics, and geometric functional analysis. The motivations range from questions about (classical) locally decodable codes, quantum information, statistical physics of spin glasses, and data analysis. Moreover, the injective norm has been extensively studied numerically in [FLN22] for different families of random and deterministic states.

In this context, our work can both be seen as contributing to a program aimed at better understanding tensor norms as well as to a program dedicated to the study of multipartite entanglement measures. The latter have been intensively studied in recent years for random states, with a particular focus on random tensor network states, due to their role as excellent toy models for Ryu-Takayanagi-like formulas. The studied measures of multipartite entanglement aim to generalize Rényi entropies [PWW23, AFLR24], and are constructed out of polynomial local unitary invariants of tensors [CGL23, Jin12, CCZ⁺17], mirroring how Rényi entropies arise from polynomial local unitary invariants of density matrices. In the multipartite case, the profusion of such invariants obscures their operational meaning and complicates the choice of a canonical family with good properties. By focusing on the injective norm, we step outside the polynomial framework and analyze a non-polynomial quantity.

Let n be a positive integer, let $(\mathcal{H}_i)_{i=1}^n$ be a collection of Hilbert spaces (of possibly different dimensions d_i). Given a quantum state $|\psi\rangle \in \bigotimes_{i=1}^n \mathcal{H}_i$, the injective norm of such a state is defined by

$$(1) \quad \|\psi\|_{\text{inj}} := \max_{|\varphi_i\rangle \in \mathcal{H}_i, \langle \varphi_i | \varphi_i \rangle = 1} |\langle \psi | \varphi_1 \dots \varphi_n \rangle|.$$

One often considers minus the logarithm of the above quantity, called the geometric entanglement,

$$E(|\psi\rangle) := -\log_2 \|\psi\|_{\text{inj}}^2.$$

Yet another equivalent quantity, which is just as natural from a geometric point of view, is the distance of $|\psi\rangle$ to the set of separable states, namely

$$d_{\text{SEP}}(|\psi\rangle) = \sqrt{2(1 - \|\psi\|_{\text{inj}})}.$$

This last quantity is sometimes called the Groverian [JHK⁺08]. We see in particular that the larger the injective norm of a state is, the closer this state is to a separable state.

In the $n = 2$ bipartite case, where $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$, the geometric entanglement is just the ∞ -Rényi entropy of the density matrix $\rho = \text{Tr}_2(|\psi\rangle\langle\psi|)$.

1.2. Results. Following standard coding theory practice, we call a subvector space of $\mathbb{F}_2^n$ a *classical linear code* over n bits, where $\mathbb{F}_2$ denotes the finite field on two elements. We shall require very little coding theory background, but for a textbook treatment of classical error-correcting codes, see [MS77], while [NC00] treats the quantum case.

Let C be a k -dimensional linear code over $\mathbb{F}_2^n$. We are interested in the associated quantum state that we denote by $|C\rangle$ defined as,

$$(2) \quad |C\rangle = \frac{1}{\sqrt{|C|}} \sum_{y \in C} |y\rangle \in (\mathbb{C}^2)^{\otimes n}.$$

Let $A \subset [n]$ be a subset of coordinate positions. We define the *punctured code* on A to be the code on $|A|$ bits consisting of all codewords of C restricted to coordinates of A . Define $j(C)$ to be the smallest integer j such that there exists a partition of $[n] = A \sqcup B$ for which the punctured code on A is of dimension k while the punctured code on $B = [n] \setminus A$ is of dimension $k - j$.

Theorem 1.1 (Main theorem). *Let $C \subset \mathbb{F}_2^n$ be a linear code of dimension k . Then the injective norm of $|C\rangle$ is given by*

$$\| |C\rangle \|_{\text{inj}} = 2^{-\frac{1}{2}(k-j(C))}.$$

Theorem 1.1 will be derived by proving matching upper and lower bounds on the injective norm of the state $|C\rangle$. The upper bound reads $\| |C\rangle \|_{\text{inj}} \leq 2^{-\frac{1}{2}(k-j(C))}$ while the lower bound is expressed in terms of an additional quantity $\delta(C)$. One obtains that $\| |C\rangle \|_{\text{inj}} \geq 2^{-\frac{1}{2}(k-\delta(C))}$, with $\delta(C) := \max_{C_0} 2k_0 - \ell(C_0)$ where the maximum is over shortened codes C_0 of C (see definition 3.4), k_0 is the dimension of C_0 and $\ell(C_0)$ its length. Proving the upper and lower bounds is the object of Section 4.

The most technical part of the proof is to show that the upper and lower bounds match, namely that $j(C) = \delta(C)$. This last equality is the content of Theorem 5.1 and Section 5 is devoted to its proof. The core argument involves using matroid theory and notably Edmonds' intersection theorem, an abstract version of the max flow-min cut principle.

Remark 1.2. *The family of states of the form*

$$(3) \quad |C\rangle = \frac{1}{\sqrt{|C|}} \sum_{y \in C} |y\rangle$$

captures a number of states that we are commonly interested in. An observation is that the celebrated GHZ states,

$$|GHZ_n\rangle = \frac{1}{\sqrt{2}} (|\underbrace{0 \dots 0}_{n \text{ times}}\rangle + |\underbrace{1 \dots 1}_{n \text{ times}}\rangle),$$

belong to this family: indeed, they correspond to the case when C is the well-known repetition code. On the other hand, some canonical examples fall outside this class. For instance, the W state,

$$|W\rangle = \frac{1}{\sqrt{3}} (|100\rangle + |010\rangle + |001\rangle),$$

cannot be written in the form (3), since the words 100, 010, 001 do not form a linear subspace of $\mathbb{F}_2^3$

Moreover, we will make the case that Theorem 1.1 extends and gives a formula for the injective norm of all basis states of any quantum CSS code. To be specific, let $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ be the total Hilbert space of n qubits. Let $C_1 \subseteq \mathbb{F}_2^n, C_2 \subseteq \mathbb{F}_2^n$ be two classical binary linear codes satisfying $C_2 \subset C_1$. We recall that (C_1, C_2) defines a *quantum CSS code* [CS96, Ste96] that consists of the subspace of $\mathcal{H}$ equal to the linear span of all states

$$(4) \quad |z\rangle := \frac{1}{\sqrt{|C_2|}} \sum_{y \in z} |y\rangle$$

where z ranges over all cosets $z \in C_1/C_2$. A simple consequence of Proposition 3.6 below and Theorem 1.1 is that,

Corollary 1.3. *Let C_2 be a code of dimension k in $\mathbb{F}_2^n$. For all $x \in C_1/C_2$, $\| |x\rangle \|_{\text{inj}} = 2^{-\frac{1}{2}(k-j(C_2))}$.*

This means that standard basis states of a CSS code all have the same injective norm.

Relation to previous results:

The geometric entanglement of the state $|C\rangle$ is

$$E(|C\rangle) = k - j(C).$$

In the case of the Kitaev toric code, we have a code C of length n and the dimension $n - 1$, and the work [OW11] of Orús and Wei shows that the geometric entanglement of basis states is $n - 1$, that is $j(C)$ vanishes for the Kitaev code. Therefore, the Kitaev code produces basis states which are maximally entangled for the geometric entanglement among basis states of CSS codes. The work [OW11] went further and computed the topological geometric entanglement by grouping qubits in larger and larger clusters. Their clustering method (reminiscent of block spin renormalization) is highly dependent on a locality property, which is not obviously generalized in the case of general CSS codes. We therefore postpone the study of the relevant generalization of topological geometric entanglement for CSS codes to further work.

Computational complexity for $j(C)$:

Regarding the problem of computing the injective norm of tensors, one noticeable fact is that, when specialised to the basis states of a CSS quantum error-correcting code, the problem becomes discrete, whereas the initial optimization problem on a product of spheres is of a continuous nature.

A natural question is whether this discretization reduced the difficulty of computing the injective norm. It turns out that our matroid formulation of the problem implies the existence of an efficient (polynomial in the number of qubits n) greedy augmenting path algorithm that computes $j(C)$: this is a consequence of the work of Edmonds [Edm71].

2. ACKNOWLEDGMENTS

S.D. is grateful to the Institut de Mathématiques de Bordeaux for their hospitality, where part of this work was carried out. The work of S.D. was partly supported by the ANR grants ANR-25-CE40-1380 and ANR-25-CE40-5672. G.Z. was supported by Plan France 2030 through the project NISQ2LSQ, ANR-22-PETQ-0006.

3. PRELIMINARIES

3.1. General facts on injective norm. Let $\mathcal{H}$ be a Hilbert space of the general form $\mathcal{H} = \bigotimes_{i=1}^n \mathcal{H}_i$. Let us start by pointing out that the injective norm (1) of a state clearly satisfies *local unitary invariance*, namely:

Proposition 3.1. *Let $U_i \in U(\mathcal{H}_i)$, then $\| |\psi\rangle \|_{\text{inj}} = \|(U_1 \otimes \dots \otimes U_n) |\psi\rangle \|_{\text{inj}}$, where each U_i is a unitary operator acting separately on each Hilbert space $\mathcal{H}_i$.*

Next we mention a generic method for deriving upper bounds on the injective norm.

Pick a basis $\{|\alpha_{m_i}^{(i)}\rangle_{i=1}^{d_i}\}$ for each $\mathcal{H}_i$. Using these bases, $|\psi\rangle = \sum_{m_i \in \llbracket 1, d_i \rrbracket} t_{m_1, \dots, m_n} |\alpha_{m_1}^{(1)} \dots \alpha_{m_n}^{(n)}\rangle$. The elements $T = (t_{m_1, \dots, m_n}) \in \bigotimes_{i=1}^n \mathbb{C}^{d_i}$ form a tensor.

Definition 3.2. *Let $A \sqcup B = \llbracket 1, n \rrbracket$ be a non-trivial bipartition of $[n] := \llbracket 1, n \rrbracket$. Then a flattening of a tensor T is the matrix $M(T) = (M(T)_{a,b})$ such that a, b are multi-indices taking values in*

$a \in \prod_{i_A \in A} [d_{i_A}]$, $b \in \prod_{i_B \in B} [d_{i_B}]$, and the elements $M(T)_{a,b} := t_{a \sqcup b}$, where $a \sqcup b$ is the multi-index in $\prod_{i=1}^n [d_i]$ whose elements $i_j, j \in A$ produce a and elements $i_j, j \in B$ produce b .

The bipartition above induces a bipartition of the total Hilbert space $\mathcal{H} = \bigotimes_{i=1}^n \mathcal{H}_i$ as $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ with $\mathcal{H}_A := \bigotimes_{i_A \in A} \mathcal{H}_{i_A}$ and $\mathcal{H}_B := \bigotimes_{i_B \in B} \mathcal{H}_{i_B}$. A flattening is just the reinterpretation of a multipartite quantum state in $\bigotimes_{i=1}^n \mathcal{H}_i$ as a bipartite state in $\mathcal{H}_A \otimes \mathcal{H}_B$.

We shall use:

Lemma 3.3. *Let T be a tensor, and $M(T)$ a flattening associated to a bipartition A, B as above. Then*

$$(5) \quad \|T\|_{\text{inj}} \leq \|M(T)\|_{\text{op}}.$$

Note that the operator norm of $M(T)$ is its largest singular value. This largest singular value can be accessed as the square root of the largest eigenvalue of $\rho_A = M(T)M(T)^*$. It is interesting to remark that ρ_A is the partial trace over B of the density matrix $\rho_{AB} = |T\rangle\langle T|$ associated to T .

In the rest of the paper, we shall focus on the case when $d_i = 2$ for every i , so that every component Hilbert space $\mathcal{H}_i$ is isomorphic to $\mathbb{C}^2$. The ambient Hilbert space will hereafter be equal to $\mathcal{H} = \bigotimes_{i=1}^n \mathcal{H}_i$. Following standard practice we write the canonical basis of $\mathbb{C}^2$ as $|0\rangle, |1\rangle$ and elementary product states as $|x\rangle$ for $x \in \mathbb{F}_2^n$. We shall also use the notation $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

3.2. Coding Theory. A binary linear code of length n is an $\mathbb{F}_2$ -subvector space of the ambient space $\mathbb{F}_2^n$. It will be useful to have coordinates of a binary vector not necessarily indexed by consecutive integers $1, 2, \dots, n$, therefore we will sometimes identify the ambient space $\mathbb{F}_2^n$ with $\mathbb{F}_2^E$ where E is a finite set of cardinality n . When a code C is defined in the ambient space $\mathbb{F}_2^E$, we will refer to the *length* of C as $\ell(C) = |E|$. A *generator matrix* for the code C is a matrix $\mathbf{G}$ whose rows form a basis of C as an $\mathbb{F}_2$ -vector space. The *rate* $R(C)$ of a code C is defined as the ratio of its dimension relative to its length: $R(C) = \dim C / \ell(C)$.

Definition 3.4. *Let $C \subset \mathbb{F}_2^n$ be a linear code of length n . Let $A \subset [n]$. The punctured code of C on A is defined as the image of C by the map:*

$$\begin{aligned} \mathbb{F}_2^n &\rightarrow \mathbb{F}_2^A \\ (x_1, \dots, x_n) &\mapsto (x_i)_{i \in A} \end{aligned}$$

The shortened code of C on A (or supported by A) is defined to be the kernel C_0 of the map:

$$\begin{aligned} C &\rightarrow \mathbb{F}_2^{\bar{A}} \\ (x_1, \dots, x_n) &\mapsto (x_i)_{i \in \bar{A}} \end{aligned}$$

where $\bar{A} = [n] \setminus A$: the corresponding set A is referred to as the support of the shortened code. The code C_0 may also be thought of as code in the ambient space $\mathbb{F}_2^{\bar{A}}$, so that the length $\ell(C_0)$ of the shortened code will mean $\ell(C_0) = |\bar{A}|$ and its rate $R(C_0)$ will mean $R(C_0) = \dim C_0 / |\bar{A}|$.

Let C be a code in $\mathbb{F}_2^n$ and let $x \in \mathbb{F}_2^n$ be a vector in the ambient space. Extending the definition (2) of the state $|C\rangle$ to coset states (4), namely

$$|x + C\rangle = \frac{1}{\sqrt{|C|}} \sum_{y \in C} |x + y\rangle,$$

we obtain:

Proposition 3.5. *For every $x \in \mathbb{F}_2^n$ we have $\|x + C\|_{\text{inj}} = \|C\|_{\text{inj}}$.*

Proof. Let U_i be the unitary operator on the component Hilbert space $\mathcal{H}_i$ defined by $U_i|0\rangle = |x_i\rangle$ and $U_i|1\rangle = |1 + x_i\rangle$. We clearly have

$$(U_1 \otimes \dots \otimes U_n)|C\rangle = |x + C\rangle.$$

The result therefore follows from Proposition 3.1. $\square$

Recall that two classical codes C_1, C_2 such that $C_2 \subseteq C_1$ define a quantum CSS code $CSS(C_1, C_2)$ that is a subspace in $\mathcal{H}$, whose basis states are defined to be the states $|z\rangle$ for $z \in C_1/C_2$. Proposition 3.5 implies:

Proposition 3.6. *Let $\mathcal{Q} = CSS(C_1, C_2)$ be the quantum CSS code associated to two classical linear codes C_1, C_2 , $C_2 \subseteq C_1$. The injective norm $\|\cdot\|_{\text{inj}}$ is a constant function on the set of basis states for $\mathcal{Q}$.*

4. UPPER AND LOWER BOUNDS

Lower bound. We start with the lower bound.

Lemma 4.1 (Lower bound). *Let $C \subseteq \mathbb{F}_2^n$ a code of dimension k . Then,*

$$(6) \quad \| |C\rangle \|_{\text{inj}} \geq 2^{-\frac{1}{2}(k - \delta(C))},$$

with

$$(7) \quad \delta(C) := \max_{C_0} (2 \dim C_0 - \ell(C_0)) = \max_{C_0} \ell(C_0)(2R(C_0) - 1)$$

where the maximum is over all shortened codes C_0 of C , $\ell(C_0)$ is the length of C_0 , and $R(C_0)$ is its rate, according to Definition 3.4.

Proof. Given a partition $A \sqcup B = [n]$ we compute the scalar product

$$\langle +_A 0_B | C \rangle \leq \| |C\rangle \|_{\text{inj}},$$

where by $|+_A 0_B\rangle$ we mean $\bigotimes_{i \in A} |+\rangle \bigotimes_{i \in B} |0\rangle$. Let C_0 be the shortened code of C supported by A . We have:

$$\begin{aligned} \langle +_A 0_B | C \rangle &= \frac{1}{\sqrt{|C|}} \sum_{c \in C} \langle +_A 0_B | c \rangle \\ &= \frac{1}{\sqrt{|C|}} \sum_{c \in C_0} \langle +_A 0_B | c \rangle \\ &= \frac{1}{\sqrt{|C|}} \sum_{c \in C_0} \frac{1}{2^{|A|/2}} \sum_{x_A \in \mathbb{F}_2^A} \langle x_A 0_B | c \rangle \\ &= \frac{1}{\sqrt{|C|}} \frac{1}{2^{|A|/2}} |C_0| \\ &= 2^{-\frac{1}{2}(k - 2k_0 + \ell(C_0))} \end{aligned}$$

where $k = \dim C$, $k_0 = \dim C_0$, and $\ell(C_0) = |A|$. Optimizing over all shortened codes C_0 of C proves the claim. $\square$

Remark 4.2. $\delta(C)$ measures how well the dimension of C is distributed over subspaces. In fact, if there exists a shortened code C_0 whose rate is strictly larger than $1/2$ then $\delta(C) > 0$. In this case C has the property that a large number of its codewords (namely 2^{k_0} of them) has support on a restricted set of positions A .

If there is no such shortened code, $\delta(C) = 0$ (the maximum is attained for $A = \emptyset$, so that $k_0 = 0$, $\ell(C_0) = 0$), and the lower bound on the injective norm only depends on the dimension of k . In this case the codeword supports are more evenly spread inside C .

Upper bound. Let $C \subset \mathbb{F}_2^n$ be a linear code of length n and dimension k . We call $j(C)$ the smallest integer $0 \leq j \leq k$ such that there exists a partition $[n] = A \sqcup B$ for which the code C punctured on A (see Definition 3.4) is of dimension k and punctured on B is of dimension $k - j$. In other words, if we let $\mathbf{G}$ be a generator matrix of the code, the sub-matrix $\mathbf{G}_A$ consisting of columns indexed by A must be of rank k and the sub-matrix $\mathbf{G}_B$ must be of rank $k - j$.

Lemma 4.3. *Let $C \subset \mathbb{F}_2^n$ be a linear code of dimension k with $j(C) = j$ then $\| |C\rangle \|_{\text{inj}} \leq 2^{-\frac{1}{2}(k-j)}$.*

The proof relies on the decomposition of the coordinate set $[n]$ into an information set [Pra62] for C and its complement. An information set is a subset of positions such that the codeword coordinates at those positions uniquely identify the codeword. Given a codeword we call prefix the subword of positions corresponding to the chosen information set of the code, while we call suffix the subword made of the remaining positions. Rephrasing the above, for any given prefix c_{pre} of a codeword c of C , there is a unique associated suffix, allowing one to reconstruct the full codeword given one prefix.

Proof. We recall $|C\rangle := \frac{1}{\sqrt{|C|}} \sum_{c \in C} |c\rangle \in (\mathbb{C}^2)^{\otimes n}$. Let $\mathbf{G}$ be the generator matrix of the code C . We assume, without loss of generality, that it is in standard form

$$\mathbf{G} = \left(\begin{array}{ccc|c} 1 & \dots & 0 & \mathbf{A} \\ \vdots & \ddots & \vdots & \\ 0 & \dots & 1 & \end{array} \right)$$

meaning that the left sub-matrix is the $k \times k$ identity matrix, and the right submatrix is some $k \times (n - k)$ matrix $\mathbf{A}$ with $\text{rank}(\mathbf{A}) = k - j$. The first k positions thus form an information set, allowing us to split the words into prefix and suffix. This splitting induces a splitting of the Hilbert space into the Hilbert space of prefixes (of dimension 2^k) and the Hilbert space of suffixes (of dimension 2^{n-k}) so that we see $|C\rangle \in (\mathbb{C}^2)^{\otimes n} \simeq (\mathbb{C}^2)^{\otimes k} \otimes (\mathbb{C}^2)^{\otimes n-k}$. To this splitting is associated a flattening of $|C\rangle$ according to the partition $A = [k], B = [n] \setminus [k]$ (see definition 3.2). Denoting this flattening $M(|C\rangle)$ we have according to lemma 3.3,

$$\| |C\rangle \|_{\text{inj}} \leq \| M(|C\rangle) \|_{\text{op}}.$$

The matrix $M(|C\rangle) \in \text{Mat}_{2^k \times 2^{n-k}}(\mathbb{C})$ is the matrix whose lines are indexed by elements of $\mathbb{F}_2^k$, which is also the set of prefixes of all codewords of C , while columns are indexed by elements of $\mathbb{F}_2^{n-k}$. Let $\mathbf{a} \in \mathbb{F}_2^k$ and $\mathbf{b} \in \mathbb{F}_2^{n-k}$. There is a one at position $\mathbf{a}, \mathbf{b}$ of $\sqrt{|C|} M(|C\rangle)$ if the prefix $\mathbf{a}$ has for suffix $\mathbf{b}$ in C . Every other element is zero. The square of the operator norm of $M(|C\rangle)$ is the largest eigenvalue of $\rho_{\text{suffix}} := M(|C\rangle)^* M(|C\rangle)$. We have for $\mathbf{b}, \mathbf{b}' \in \mathbb{F}_2^{n-k}$

$$|C|(\rho_{\text{suffix}})_{\mathbf{b}, \mathbf{b}'} = |C| \sum_{\mathbf{a} \in \mathbb{F}_2^k} (M(|C\rangle)^*)_{\mathbf{b}, \mathbf{a}} (M(|C\rangle))_{\mathbf{a}, \mathbf{b}'} = N(\mathbf{b}) \delta_{\mathbf{b}, \mathbf{b}'},$$

where $N(\mathbf{b})$ is the number of prefixes having $\mathbf{b}$ as suffix. Indeed, the element $\mathbf{b}, \mathbf{b}'$ of $|C| \rho_{\text{suffix}}$ is the scalar product (over $\mathbb{C}$) of the line $\mathbf{b}$ of $\sqrt{|C|} M(|C\rangle)^*$ with the column $\mathbf{b}'$ of $\sqrt{|C|} M(|C\rangle)$ which is easily seen to count the number of prefixes having $\mathbf{b}, \mathbf{b}'$ as suffixes. But thanks to the information set property that a prefix has a unique suffix, we must have $\mathbf{b} = \mathbf{b}'$, otherwise the scalar product vanishes. Therefore the largest eigenvalue of ρ_{suffix} is the largest value of $N(\mathbf{b})$ (divided by $|C|$). The number of prefixes having the same suffix $\mathbf{b}$ counts the different linear combinations of lines of $\mathbf{A}$ leading to the same bitstring $\mathbf{b}$ or equivalently, (at the cost of adding $\mathbf{b}$ to those combinations),

the number of different vanishing linear combinations of lines of $\mathbf{A}$, that is $N(\mathbf{b}) = |\ker_{\mathbb{F}_2} \mathbf{A}| = 2^j$. In particular, if $\mathbf{b}$ is indeed a suffix of a codeword in C , then $N(\mathbf{b})$ does not depend on $\mathbf{b}$. We conclude that

$$\|M(|C\rangle)\|_{\text{op}} = \frac{2^{\frac{1}{2}j}}{\sqrt{|C|}} = 2^{-\frac{1}{2}(k-j)}. \quad \square$$

5. MATCHING UPPER AND LOWER BOUNDS

Let $C \subset \mathbb{F}_2^n$ be a code such that $j(C) = 0$. Then Lemmas 4.3 and 4.1 together imply that $\delta(C) = 0$ so that the upper and lower bounds match. To prove Theorem 1.1 it will therefore be enough to prove:

Theorem 5.1. *Let $C \subset \mathbb{F}_2^n$ be a linear code, such that $j = j(C) \geq 1$, then there exists C_0 a shortened code of C of dimension $k_0 > 0$ and length $2k_0 - j$.*

Indeed, if such a shortened code C_0 exists, then by definition of $\delta(C)$ we must have $\delta(C) \geq 2k_0 - (2k_0 - j) = j$, but then Lemmas 4.3 and 4.1 imply that the corresponding upper and lower bounds are equal.

We shall prove Theorem 5.1 using arguments from matroid theory. To this aim, we introduce the relevant background and state one of the cornerstones of the theory and essential element of the proof of theorem 5.1, namely Edmonds' intersection theorem.

5.1. Elements of matroid theory. Matroids are combinatorial objects that are defined to abstract and generalize the concept of linear independence of vectors in linear algebra. They can also be seen as a way to generalize concepts from graph theory. For a gentle introduction to matroids and some of their applications, we refer to the notes [Oxl25] and the associated book [Oxl06]. For our purpose we need only a few concepts of matroid theory, that is the definition of a matroid, its bases, its dual, and the rank functions over a matroid. In particular, this allows us to state Edmonds' intersection theorem that we use in the next section to prove Theorem 5.1.

One way to define a matroid over a finite set X is through the data of independent subsets of X .

Definition 5.2. *Let X be a finite set, a finite matroid $\mathcal{M}(X, \mathcal{I})$ on X is a couple $(X, \mathcal{I})$ where $\mathcal{I} \subseteq 2^X$ is a subset of the powerset of X satisfying the following constraints*

- (1) $\emptyset \in \mathcal{I}$
- (2) if $J \in \mathcal{I}$ and $I \subset J$ then $I \in \mathcal{I}$
- (3) if $I, J \in \mathcal{I}$ such that $|I| < |J|$, there exists $x \in J \setminus I$ such that $I \cup \{x\} \in \mathcal{I}$.

The set $\mathcal{I}$ is called the set of independents, and its elements are the independent sets.

The archetypical example of a matroid is the following. Let V be a dimension N vector space over a field K endowed with a specific generating set of vectors $X = \{e_1, \dots, e_R\}$, $R > N$. Let $\mathcal{I}$ be the set of linearly independent subsets of X . This endows (V, X) with the structure of a matroid. Additionally, if one thinks of $\{e_1, \dots, e_R\}$ as the columns of a matrix M , then the above matroid structure is known as the column matroid of M .

We can now introduce bases of a matroid as

Definition 5.3. *Let $\mathcal{M}(X, \mathcal{I})$ be a finite matroid. A basis is a largest element $B \in \mathcal{I}$, that is for all $I \in \mathcal{I}$, $|B| \geq |I|$.*

It is straightforward to show that all bases of a matroid have the same cardinality.

We now define the dual of a matroid

Definition 5.4. *The dual $\mathcal{M}^*(X, \mathcal{I}^*)$ of a finite matroid $\mathcal{M}(X, \mathcal{I})$ is the matroid over X whose set of independents $\mathcal{I}^*$ is formed of subsets $I \subseteq X$ whose complement $\bar{I}$ contain a basis of $\mathcal{M}(X, \mathcal{I})$.*

Alternatively, the dual of a finite matroid $\mathcal{M}(X, \mathcal{I})$ on X is the matroid whose basis sets are the complements of the basis sets of $\mathcal{M}(X, \mathcal{I})$.

The rank function of a given matroid is defined on the subsets of X ,

$$(8) \quad \text{rk} : 2^X \rightarrow \mathbb{Z}_+$$

$$(9) \quad S \mapsto \max\{|I| : I \subseteq S, I \in \mathcal{I}\},$$

that is the size of the largest independent contained in S . One shows that the rank function of the dual matroid is

$$(10) \quad \text{rk}^*(S) = \text{rk}(X \setminus S) + |S| - \text{rk}(X)$$

The cornerstone theorem of matroid theory is arguably Edmonds' intersection theorem [Edm03]:

Theorem 5.5 (Edmonds' theorem - The matroid intersection theorem). *Let $\mathcal{M}_1(X, \mathcal{I}_1), \mathcal{M}_2(X, \mathcal{I}_2)$ be two matroids over the same set X . The following equality holds*

$$(11) \quad \max_{I \in \mathcal{I}_1 \cap \mathcal{I}_2} |I| = \min_{S \subseteq X} [\text{rk}_1(S) + \text{rk}_2(\bar{S})],$$

where the complement $\bar{S}$ of S is meant in X , that is $\bar{S} = X \setminus S$.

5.2. Proof of Theorem 5.1.

Proof. Let $\mathbf{G}$ be a generator matrix of the code C of theorem 5.1. Let $j := j(C)$ be as announced, i.e. the smallest integer such that there exists a bipartition $A \sqcup \bar{A} = [n]$ inducing a submatrix $\mathbf{G}_A$ of rank k and another submatrix $\mathbf{G}_{\bar{A}}$ of rank $k - j$.

Let $\mathcal{M}_1$ be the column matroid of $\mathbf{G}$, meaning the matroid on $X = [n]$ whose independent sets are the subsets $I \subset [n]$ such that the columns of $\mathbf{G}$ indexed by I are linearly independent. We denote by rk_1 its rank function. We let $\mathcal{M}_2$ be the dual matroid of $\mathcal{M}_1$ and denote by rk_2 its rank function.

We remark that with those matroid structures, by definition of j , $k - j$ is the maximal value of rk_1 over the complements of bases of $\mathcal{M}_1$. Moreover, letting B be a basis of $\mathcal{M}_1(X, \mathcal{I}_1)$, we have $\text{rk}_1(\bar{B}) = \max\{|I| : I \in \mathcal{I}_1, I \subseteq \bar{B}\}$. Hence, by definition of the dual matroid such I 's are also independent in $\mathcal{M}_2$, $k - j$ is the largest size of a set $I \subset [n]$ such that I is independent in both $\mathcal{M}_1$ and $\mathcal{M}_2$. Therefore, letting $\mathcal{I}_1, \mathcal{I}_2$ be the sets of independents of respectively $\mathcal{M}_1, \mathcal{M}_2$, Edmonds' intersection theorem [Edm03] (Theorem 5.5) tells us that

$$(12) \quad k - j = \max_{I \in \mathcal{I}_1 \cap \mathcal{I}_2} |I| = \min_{S \subseteq [n]} [\text{rk}_1(S) + \text{rk}_2(\bar{S})].$$

Consider $S \subset [n]$ achieving the minimum of the right-hand side of (12). Since we have supposed $j \geq 1$, there must exist $k_0 > 0$ such that $\text{rk}_1(S) = k - k_0$. We now let $x = |\bar{S}|$ so that, applying (10), we have $\text{rk}_2(\bar{S}) = \text{rk}_1(S) + |\bar{S}| - k = x - k_0$.

Since S achieves the minimum of the right-hand side of (12) we now have $k - j = (k - k_0) + (x - k_0)$ so that $|\bar{S}| = x = 2k_0 - j$. We now subdivide the matrix $\mathbf{G}$ into the set of columns indexed by S and the set of columns indexed by $\bar{S}$. Assuming, without loss of generality, that the submatrix

$\mathbf{G}_S$ whose columns are indexed by S is the $k \times |S|$ leftmost submatrix of $\mathbf{G}$, we obtain, since $\text{rk}(\mathbf{G}_S) = k - k_0$, that $\mathbf{G}$ multiplied on the left by an appropriate invertible matrix is of the form

$$(13) \quad \mathbf{G}' = \left(\begin{array}{c|c} \mathbf{0} & \mathbf{G}_0 \\ \hline \mathbf{G}_1 & \mathbf{G}_2 \end{array} \right)$$

where the top left $k_0 \times |S|$ submatrix is the zero matrix. The top right submatrix $\mathbf{G}_0$ must therefore be a $k_0 \times (2k_0 - j)$ matrix, and it must be of rank k_0 for the rank of $\mathbf{G}'$ to be of rank k . Since $\mathbf{G}'$ is, like $\mathbf{G}$, a generator matrix for the code C , we have that the shortened code C_0 of C supported by $\bar{S}$ has dimension k_0 and length $2k_0 - j$. $\square$

REFERENCES

- [AFLR24] Chris Akers, Thomas Faulkner, Simon Lin, and Pratik Rath. Reflected entropy in random tensor networks. part iii. triway cuts. *Journal of High Energy Physics*, 2024(12):1–70, 2024. [2](#)
- [AMM10] Martin Aulbach, Damian Markham, and Mio Murao. The maximally entangled symmetric state in terms of the geometric measure. *New Journal of Physics*, 12(7):073025, 2010. [2](#)
- [BGJ⁺24] Afonso S Bandeira, Sivakanth Gopi, Haotian Jiang, Kevin Lucca, and Thomas Rothvoss. A geometric perspective on the injective norm of sums of random tensors. *arXiv preprint arXiv:2411.10633*, 2024. [2](#)
- [Boe24] March T Boedihardjo. Injective norm of random tensors with independent entries. *arXiv preprint arXiv:2412.21193*, 2024. [2](#)
- [BS25] Erik Bates and Youngtak Sohn. Balanced multi-species spin glasses. *arXiv preprint arXiv:2507.06522*, 2025. [2](#)
- [CCZ⁺17] Meiyu Cui, Jingmei Chang, Ming-Jing Zhao, Xiaofen Huang, and Tinggui Zhang. Local unitary invariants of quantum states. *International Journal of Theoretical Physics*, 56(11):3579–3587, 2017. [2](#)
- [CGL23] Benoît Collins, Razvan Gurau, and Luca Lionni. The tensor harish-chandra–itzkson–zuber integral i: Weingarten calculus and a generalization of monotone hurwitz numbers. *Journal of the European Mathematical Society*, 26(5):1851–1897, 2023. [2](#)
- [CS96] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098–1105, August 1996. [1](#), [3](#)
- [DM24] Stephane Dartois and Benjamin McKenna. Injective norm of real and complex random tensors i: From spin glasses to geometric entanglement. *arXiv preprint arXiv:2404.03627*, 2024. [2](#)
- [Edm71] Jack Edmonds. Matroids and the greedy algorithm. *Mathematical programming*, 1:127–136, 1971. [4](#)
- [Edm03] Jack Edmonds. Submodular functions, matroids, and certain polyhedra. In *Combinatorial Optimization—Eureka, You Shrink! Papers Dedicated to Jack Edmonds 5th International Workshop Aussois, France, March 5–9, 2001 Revised Papers*, pages 11–26. Springer, 2003. [9](#)
- [FLN22] Khurshed Fitter, Cecilia Lancien, and Ion Nechita. Estimating the entanglement of random multipartite quantum states. *arXiv preprint arXiv:2209.11754*, 2022. [2](#)
- [Haa13] Jeongwan Haah. *Lattice quantum codes and exotic topological phases of matter*. California Institute of Technology, 2013. [1](#)
- [HL13] Christopher J. Hillar and Lek-Heng Lim. Most tensor problems are NP-hard. *Journal of the ACM (JACM)*, 60(6):1–39, 2013. [2](#)
- [JHK⁺08] Eylee Jung, Mi-Ra Hwang, Hungsoo Kim, Min-Soo Kim, DaeKil Park, Jin-Woo Son, and Sayatnova Tamaryan. Reduced state uniquely defines the groverian measure of the original pure state. *Physical Review A—Atomic, Molecular, and Optical Physics*, 77(6):062317, 2008. [2](#)
- [Jin12] Naihuan Jing. On classes of local unitary transformations. In *Algebra Colloquium*, volume 19, pages 283–292. World Scientific, 2012. [2](#)
- [KL10] Alexei Kitaev and Chris Laumann. Topological phases and quantum computation. *Exact methods in low-dimensional statistical physics and quantum computing*, pages 101–125, 2010. [1](#)
- [MS77] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error-correcting codes*, volume 16. Elsevier, 1977. [2](#)
- [NC00] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 2000. [2](#)
- [OW11] Roman Orus and Tzu-Chieh Wei. Topological geometric entanglement. *arXiv preprint arXiv:1108.1537*, 2011. [1](#), [4](#)
- [OWBVdN14] Román Orús, Tzu-Chieh Wei, Oliver Buerschaper, and Maarten Van den Nest. Geometric entanglement in topologically ordered states. *New Journal of Physics*, 16(1):013015, 2014. [1](#)

- [Oxl06] James G Oxley. *Matroid theory*, volume 3. Oxford University Press, USA, 2006. 8
- [Oxl25] James Oxley. Briefly, what is a matroid? https://www.math.lsu.edu/~oxley/matroid_intro_summ.pdf, accessed 2025. 8
- [Pra62] Eugene Prange. The use of information sets in decoding cyclic codes. *IRE Transactions on Information Theory*, 8(5):5–9, 1962. 7
- [PRBK24] Benedikt Placke, Tibor Rakovszky, Nikolas P Breuckmann, and Vedika Khemani. Topological quantum spin glass order and its realization in qldpc codes. *arXiv preprint arXiv:2412.13248*, 2024. 1
- [PWW23] Geoff Penington, Michael Walter, and Freek Witteveen. Fun with replicas: tripartitions in tensor networks and gravity. *Journal of High Energy Physics*, 2023(5):1–30, 2023. 2
- [Sas24] Naoki Sasakura. Signed eigenvalue/vector distribution of complex order-three random tensor. *Progress of Theoretical and Experimental Physics*, 2024(5):053A04, 2024. 2
- [SG24] Jonathan Steinberg and Otfried Gühne. Finding maximal quantum resources. *Physical Review A*, 110(6):062428, 2024. 2
- [Ste96] A. M. Steane. Multiple-particle interference and quantum error correction. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 452(1954):2551–2577, November 1996. 1, 3
- [Sto25] Mihailo Stojnic. Ground state energies of multipartite p -spin models—partially lifted rdt view. *arXiv preprint arXiv:2509.05916*, 2025. 2
- [WG03] Tzu-Chieh Wei and Paul M Goldbart. Geometric measure of entanglement and applications to bipartite and multipartite quantum states. *Physical Review A*, 68(4):042307, 2003. 2
- [YL24] Chao Yin and Andrew Lucas. Low-density parity-check codes as stable phases of quantum matter. *arXiv preprint arXiv:2411.01002*, 2024. 1
- [Yos15] Beni Yoshida. Topological color code and symmetry-protected topological phases. *Physical Review B*, 91(24):245131, 2015. 1
- [ZCH10] Huangjun Zhu, Lin Chen, and Masahito Hayashi. Additivity and non-additivity of multipartite entanglement measures. *New Journal of Physics*, 12(8):083002, 2010. 2