The injective norm of CSS code states

Stéphane Dartois (w/ Gilles Zémor)

February 4, 2026

CMLS, École Polytechnique

Context: geometric entanglement & QEC

Multipartite entanglement via the injective norm

For an n-partite pure state $|\psi\rangle \in \bigotimes_{i=1}^{n} \mathcal{H}_i$, the **injective norm** is

$$\| \, |\psi\rangle \, \|_{\mathrm{inj}} := \max_{|\phi_i\rangle \in \mathcal{H}_i, \ \langle \phi_i | \phi_i \rangle = 1} \left| \langle \psi | \overset{\in \mathcal{H}_1}{\phi_1} \cdots \overset{\in \mathcal{H}_n}{\phi_n} \rangle \right| .$$

The associated **geometric entanglement** is

$$E(|\psi\rangle) := -\log_2 \left(\| \, |\psi\rangle \, \|_{\mathrm{inj}}^2 \right) .$$

- $\| \, |\psi\rangle \, \|_{\mathrm{inj}} = 1$ or $E = 0$ iff $|\psi\rangle$ is a product state.
- Bipartite case ($n = 2$): E is the $\alpha \to \infty$ Rényi entropy (largest Schmidt coefficient).
- Computing $\| \cdot \|_{\mathrm{inj}}$ is NP-hard in general .

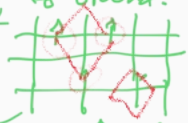
In physics: topological order and "topological GE"

local block

is a CSS code.

Orús & Wei.

$\mathcal{H}$ a Ground.



In topologically ordered fixed-point models Orús et al (2011-2014) show

Kitaev's toric code

$$E = \underbrace{E_0}_{} - \underbrace{E_\gamma}_{}, \qquad E_\gamma = S_\gamma \text{ (topological entanglement entropy).}$$

some cases are CSS codes

with E_0 a boundary-law term scaling like (# blocks)×(boundary size), and E_γ a constant dependent on the topological phase.

- This uses block product states and a block-spin disentangling viewpoint. **proof is intrinsically local**
- In particular models, E can be computed exactly.

For QI/QEC: entanglement as protection of information

IBM

In a more recent work (Bravyi et al. 2025): for a distance-d($=$ number of errors it can correct) stabilizer code, *any logical state* has nontrivial geometric entanglement:

CSS codes

$$E(|\psi\rangle) \geq \boxed{d-1},$$

qubits

equivalently any overlap with a product state is at most 2^{1-d}. (in fact this part was known to hold already for all non-degenerate codes, see e.g. Preskill notes)

They also introduce depth-h generalizations

$$E_h(|\psi\rangle) = -\max_{U \text{ depth}=h} \log_2 |\langle\psi|U|0^n\rangle|^2$$

qLDPC
sparsity

replace
product

and prove tradeoffs for several code families.

What we do: In yet another direction, compute $E = E_1$ *exactly* for a large structured family of states: *CSS basis states* (**and get rid of locality**).

CSS codes and their basis states

Classical codes basics

Let $\mathbb{F}_2 = (\{0,1\}, +, *)$ denote the two elements field (reminder: $0 * 0 = 0 * 1 = 0, 1 * 1 = 1, 0 + 0 = 1 + 1 = 0, 1 + 0 = 1$).

A *classical linear (binary) code* C of length n is a sub-vector space of $\mathbb{F}_2^n$. As such it has a dimension over $\mathbb{F}_2$ and can be seen as the image of a linear map

$$G : \mathbb{F}_2^k \to \mathbb{F}_2^n, \quad G \text{ is the generator matrix of the code}$$

(in fact: lot of freedom on linear map: we'll skip on this)

Codes are used to protect classical computers and classical communications against errors (random bit flips $0 \leftrightarrow 1$).

Useful in many other field (cryptography, computational complexity theory, randomness amplification...).

Bonus for physicists: Any such a code is the set of ground states of some Ising systems on hypergraphs.

Operations on code: puncturing and shortening

Let $C \subset \mathbb{F}_2^n$ a classical linear code. Given $A \subset [n]$, we define:

- **Puncturing** on A: $C_A := \{c_A : c \in C\} \subset \mathbb{F}_2^{|A|}$ (keep only coordinates in A). Equivalently, C_A is the image of the linear map

$$\mathbb{F}_2^n \to \mathbb{F}_2^A, \quad (x_1, \dots, x_n) \mapsto (x_i)_{i \in A}.$$

- **Shortening** on A: $\mathrm{sh}_A(C) := \{c_A : c \in C,\ c_{\overline{A}} = 0\}$ (keep only codewords zero outside A, then restrict to A). Equivalently, $\mathrm{sh}_A(A)$ is the kernel of the linear map

$$\mathbb{F}_2^n \to \mathbb{F}_2^{\overline{A}}, \quad (x_1, \dots, x_n) \mapsto (x_i)_{i \in \overline{A}}.$$

Puncturing and shortening: examples

Consider the length $n = 5$ linear code

2 x 5

$$C = \{uG : u \in \mathbb{F}_2^2\} \subset \mathbb{F}_2^5, \qquad G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

C has 4 codewords:

u	$c = uG$
00	00000
10	10110
01	01101
11	11011

Puncturing and shortening: examples

Let $A = \{1,3,4\}$ (so $\overline{A} = \{2,5\}$).

Punctured code $C|_A$*:* restrict each $c \in C$ to coordinates $(1,3,4)$:

$c \in C$	$c_{(1,3,4)}$
00000	000
10110	111
01101	010
11011	101

$\Rightarrow \quad C_A = \{000, 111, 010, 101\} \subset \mathbb{F}_2^3.$

Shortened code $\mathrm{sh}_A(C)$*:* keep only codewords with $c_2 = c_5 = 0$:

$$c_{\overline{A}} = 00 \iff c \in \{00000,\ 10110\} \quad \Rightarrow \quad \mathrm{sh}_A(C) = \{000, 111\}.$$

Quick intro to CSS code

Let $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ be the Hilbert space of n qubits. A CSS code $\mathcal{Q} \subset \mathcal{H}$ is specified by two classical binary linear codes

$$C_2 \subset C_1 \subset \mathbb{F}_2^n.$$

A standard orthonormal basis of the CSS code space $\mathcal{Q}$ is indexed by cosets $z \in C_1/C_2$:

$\mathcal{Q} = \mathrm{span}\{|z\rangle\}$

$$|z\rangle := \frac{1}{\sqrt{|C_2|}} \sum_{y \in z} |y\rangle\,,$$

pdt qubit states

$y \in C_1$, $y, y' \in z$

$y - y' \in C_2$

where $|y\rangle$ are computational basis states (bitstrings).

- These are (subcases of) stabilizer states for stabilizer group generated by commuting Pauli X, Z generator.
- Many topological codes have CSS descriptions (Kitaev toric code, color codes, etc.).

The code state $|C\rangle$

Given a k-dimensional classical code $C \subset \mathbb{F}_2^n$, define the normalized **code state**

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

$|C\rangle = |GHZ\rangle$

This includes GHZ as the repetition code case.

$C = \{000\cdots0,\ 111\cdots1\}$

Key remark: every CSS basis state is a coset state $|x + C_2\rangle$, for $x = x_1 \ldots x_n$, $x_i \in \mathbb{F}_2$, and there exists local unitaries $U_1, \ldots U_n \in U(2)$ s.t. $U_i |0\rangle = |x_i\rangle$, $U_i |1\rangle = |1 + x_i\rangle$ (*ie* U_i is the identity Id or Pauli X matrix).

Hence by local unitary invariance:

$$\| \, |x + C_2\rangle \, \|_{\mathrm{inj}} = \| (U_1 \otimes \ldots \otimes U_n) \, |C_2\rangle \, \|_{\mathrm{inj}} = \| \, |C_2\rangle \, \|_{\mathrm{inj}}$$

Therefore all CSS basis states have the same injective norm.

Main theorem and discussion

Main parameter: $j(C)$

Let $C \subset \mathbb{F}_2^n$ have dimension k.

Define $j(C)$ as the *smallest* integer j such that there exists a partition $[n] = A \sqcup B$ with:

- the punctured code on A has dimension k (all information is visible in A),
- the punctured code on B has dimension $k - j$.

Intuition: $j(C)$ counts how many dimensions of C *cannot* be simultaneously "seen" on both sides.

Theorem (injective norm of code states)

Theorem (Dartois–Zémor). Let $C \subset \mathbb{F}_2^n$ be a linear code of dimension k. Then

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

Equivalently,

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

Corollary. For a CSS code $CSS(C_1, C_2)$, every standard basis state $|z\rangle$ has

$$\| \, |z\rangle \, \|_{\mathrm{inj}} = 2^{-\frac{1}{2}(k_2 - j(C_2))}$$

(where $k_2 = \dim C_2$).

Examples

$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ A

$G_A = G$

1. Product state: $C = \mathbb{F}_2^n$ has $k = n$, and $|C\rangle = |+\rangle^{\otimes n}$.

   Here $j(C) = n$ so $-2\log_2(\| \, |C\rangle \, \|_{\mathrm{inj}}) = E(|C\rangle) = 0$.

   $\Rightarrow \mathrm{rk}\, G_A = n$ B

   max $\mathrm{rk}\, G_B = 0$

   $k - j = 0$

   $j = k = n$

2. GHZ: $C =$ repetition code $\{0^n, 1^n\}$ has $k = 1$.

   One can take a bipartition with A, B both nonempty, giving $j(C) = 0$, hence $-2\log_2(\| \, |C\rangle \, \|_{\mathrm{inj}}) = E(|C\rangle) = 1$.

   $G = (1 \, --- \, 1)$

   $\left.\begin{array}{l} k=1 \\ k-j=1 \end{array}\right\} \Rightarrow j=0$ $\quad (1 \cdots 1)$ $\quad \mathrm{rk}\, G_B = 1$

3. Toric code (Kitaev) X-code: for the relevant code C one has $k = n - 1$ and $j(C) = 0$, so $E(|C\rangle) = n - 1$. *Recover old results of Orus et al.*

   ↳ Now a parity code

Remarks

- The definition of $\| \, |\psi\rangle \, \|_{\text{inj}}$ is a *continuous* optimization over a product of spheres.
- For code states, the answer collapses to a *discrete* invariant of a classical code. $G = (\quad)$
- Moreover, $j(C)$ is computable in *polynomial time* via matroid intersection.

Fact: the closest product state can be chosen in a very structured way (built from $|+\rangle$ and $|0\rangle$ on selected qubits).

Proof strategy

Upper bound proof idea: operator norm of flattening/bipartition

General fact: for any bipartition $A \sqcup B$ and the corresponding flattening matrix $M(|\psi\rangle)$,

$n=6$ $\quad |\varphi\rangle \Rightarrow M(|\varphi\rangle)$

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

$\|M(|\varphi\rangle)\|_{op} = \max_{\substack{u,v \\ u \in (\mathbb{C}^2)^{\otimes A} \\ v \in (\mathbb{C}^2)^{\otimes B}}} \mathrm{Tr}\left(M(|\varphi\rangle)\, u v^*\right) = \langle v | M(|\varphi\rangle) | u \rangle$

For $|C\rangle$, choose an *information set* A of size k so that codewords split as

$$\text{prefix } (k \text{ bits}) \oplus \text{suffix } (n-k \text{ bits}).$$

$G = (G_A \mid G_B)$

Proof structure: *Information set property*: prefixes determine full codeword $\Rightarrow$ allows for counting argument $\Rightarrow$ determines dimension of kernel of B sub-block of flattening $\Rightarrow$ Ker dimension $\leftrightarrow$ suffix multiplicity $= 2^{j(C)} \Rightarrow$ density matrix $M(|\psi\rangle)^\dagger M(|\psi\rangle)$: proportional to identity$= \frac{1}{|C|}\mathrm{diag}(2^{j(C)})$ This implies

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

Lower bound proof idea

Given a partition $[n] = A \sqcup B$, consider the product state

$$|+_A 0_B\rangle := \bigotimes_{i \in A} |+\rangle \bigotimes_{i \in B} |0\rangle \, .$$

Then, by pure counting,

$$\langle +_A 0_B | C \rangle = 2^{-\frac{1}{2}(k - 2k_0 + |A|)},$$

$\forall A, B \quad \| |C\rangle \|_{inj} \geq 2^{-\frac{1}{2}(k-2k_0+|A|)}$

where k_0 is the dimension of the shortened code supported on A. Optimizing over A yields

$$\| \, |C\rangle \, \|_{\text{inj}} \geq 2^{-\frac{1}{2}(k - \delta(C))}, \qquad \delta(C) = \max_{C_0} \left(2 \dim C_0 - \ell(C_0) \right).$$

Matching the bounds?

We now have

$$2^{-\frac{1}{2}(k-j(C))} \geq \| \, |C\rangle \, \|_{\mathrm{inj}} \geq 2^{-\frac{1}{2}(k-\delta(C))}.$$

To finish, prove

$$\boxed{j(C) = \delta(C)}$$

which is the technically nontrivial part.

max flow / min cut

Use matroid intersection: turn the matching condition into a max–min statement.

Matroid proof ingredients

Matroid definitions

A **matroid** $M = (X, \mathcal{I})$ abstracts linear independence:

- X is a finite ground set.
- $\mathcal{I} \subseteq 2^X$ are the "independent" subsets.
- Axioms mimic independence in vector spaces (hereditary + augmentation)
  1. $\emptyset \in \mathcal{I}$
  2. $I \in \mathcal{I},\ J \subset I \Rightarrow J \in \mathcal{J}$
  3. if $I, J \in \mathcal{I}, |I| > |J|,\ \exists x \in I$ s.t. $J \cup \{x\} \in \mathcal{I}$

.

The **rank function** of a matroid is defined by:

$$\mathrm{rk} : 2^X \to \mathbb{N},\ \mathrm{rk}(A) = \max\{|I| : I \subseteq A, I \in \mathcal{I}\}$$

For a generator matrix G of a code C:

- M_1: *column matroid* of G (independent sets = linearly independent column subsets).

Edmonds' matroid intersection theorem

The **dual of a matroid** $M = (X, \mathcal{I})$ is the matroid $M^* = (X, \mathcal{I}^*)$ where $\mathcal{I}^*$ is the collection of $I \subseteq X$ s.t. $\bar{I}$ contains a maximal element of $\mathcal{I}$.

Theorem (Edmonds). For two matroids $M_1 = (X, \mathcal{I}_1)$ and $M_2 = (X, \mathcal{I}_2)$ on the same ground set,

$$\max_{I \in \mathcal{I}_1 \cap \mathcal{I}_2} |I| = \min_{S \subseteq X} \big(\mathrm{rk}_1(S) + \mathrm{rk}_2(X \setminus S)\big).$$

↳ can be computed

Proof structure. In our setting, one shows

$$\boxed{k - j(C) = \max_{I \in \mathcal{I}_1 \cap \mathcal{I}_2} |I|}$$

for M_1 the column matroid of the generator matrix G of C and $M_2 = M_1^*$ its dual. From Edmonds' theorem + some calculations we obtain that the shortened code C_O realizing $\delta(C)$ corresponds to S realizing the minimum above such that C_0 is supported on $\bar{S}$. Filling the details leads to $j(C)\delta(C)$.

Take away from the matroids

- Matroid intersection is the right abstraction of “columns independent” + “columns co-independent”.
- The theorem gives both:
  - a conceptual proof that the analytic bounds match,
  - an algorithm: polynomial-time augmenting paths (another theorem of Edmonds) to compute $j(C)$.
- A genuine multipartite entanglement measure becomes efficiently computable on this family.

Connections

Connection with Orús et al.

Orús et al. compute geometric entanglement for several topologically ordered fixed-point states and find

$$E_G = E_0 - E_\gamma, \qquad E_\gamma = S_\gamma.$$

Our result is different in scope:

- we compute *spin-level* geometric entanglement E_0 (i.e., product over individual qubits),
- for *all* CSS basis states, with no geometric/locality assumptions (includes all CSS lattice codes, but goes much further),
- giving an exact formula $E(|C\rangle) = k - j(C)$.

Future possible direction: extend the notion of *block* GE / topological GE beyond locality?

Connection to generalized Hamming weights of code (not in paper)

Let $C \subset \mathbb{F}_2^n$ be a length n, dimension k linear code. Recall $\delta(C)$:

$$\delta(C) = \max_{C_0 \text{ shortened code of } C} \big(2 \dim C_0 - \ell(C_0)\big), \qquad \text{and} \qquad j(C) = \delta(C).$$

Define the r-**th generalized Hamming weight** (a.k.a. weight hierarchy)

$$d_r(C) := \min\big\{\, |\mathrm{supp}(D)| : \; D \subseteq C, \; \dim D = r \,\big\}, \qquad r = 1, \ldots, k.$$

Standard quantities in classical code theory appearing in (classical) secret sharing schemes (control how much secret leaks from a given number of shares) and in code decoding complexity.

Claim: the variational definition of $\delta(C)$ is *equivalent* to

$$\boxed{\delta(C) = \max_{1 \le r \le k} \big(2r - d_r(C)\big)} \qquad \Longrightarrow \qquad \boxed{j(C) = \max_{1 \le r \le k} \big(2r - d_r(C)\big)}.$$

Code interpretation: $j(C) > 0$ iff C contains an r-dimensional subcode supported on *fewer* than $2r$ coordinates, i.e. a subcode on its support with *rate* $> 1/2$. So the injective norm / geometric entanglement is governed by the code's *weight hierarchy*, not just its minimum distance.

Summary

- Injective norm/geometric entanglement is generally hard, but CSS basis states are exactly solvable.
- For a classical code C of dimension k:

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

- The matching of bounds is a matroid intersection statement (Edmonds), implying an efficient algorithm for $j(C)$.

Outlook/future workds?

- A locality-free analogue of “block geometric entanglement” and a “topological correction” for general CSS codes.
- Extend beyond CSS basis states: can other stabilizer families be treated similarly?
- Compare with depth-h measures E_h and code complexity: do classical code invariants, like their weight hierarchy, control E_h for CSS basis states?

Related works:

- Orus & Wei: `https://arxiv.org/abs/1108.1537`
- Bravyi et al: `https://arxiv.org/abs/2405.01332` (of which we were not aware at the time we submitted our paper)

Our manuscript:

- Dartois & Zémor: `https://arxiv.org/abs/2510.23736`