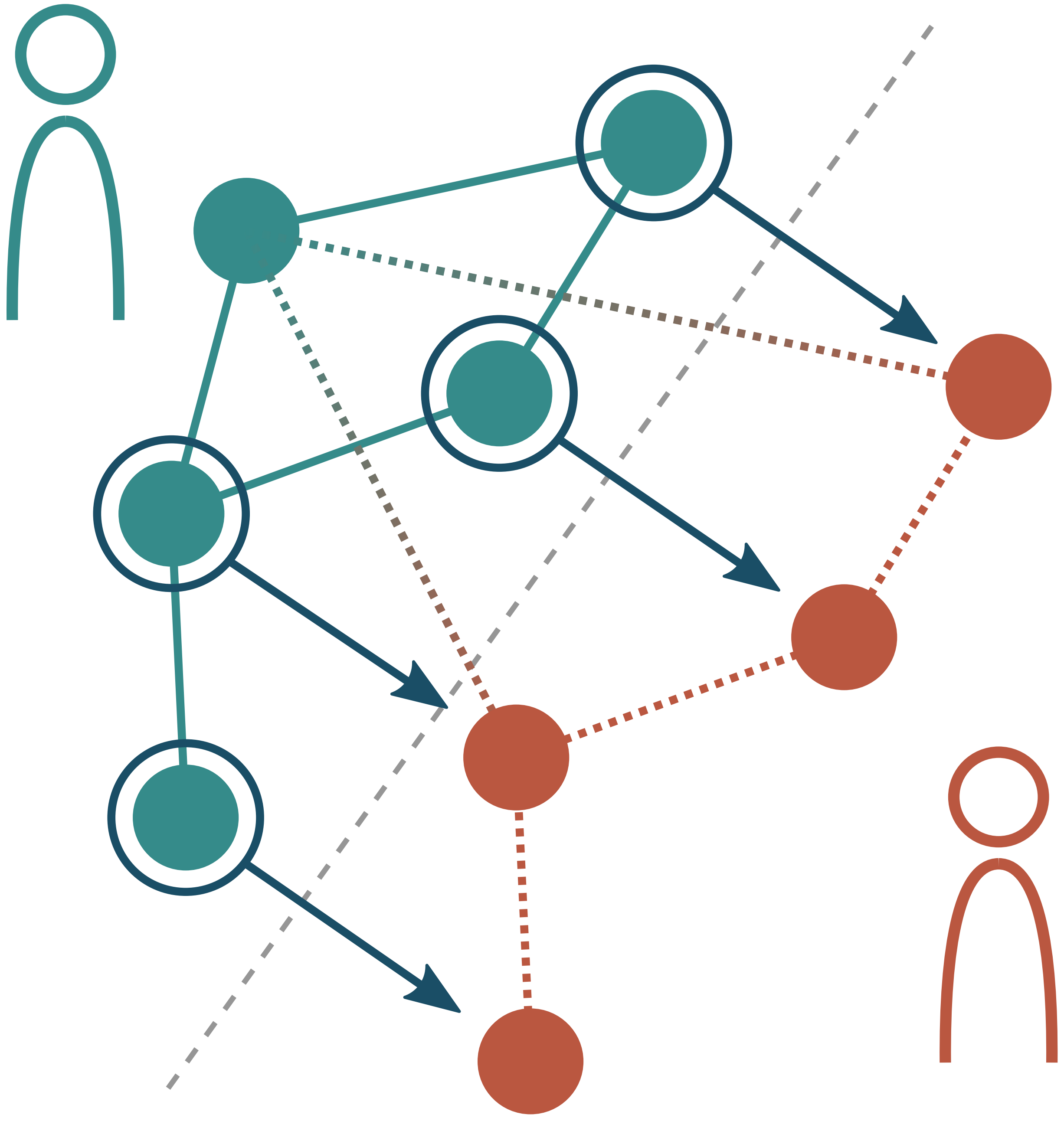
Beyond IID 8 - extended talk November 6, 2020

Error thresholds for arbitrary Pauli noise

arXiv:1910.00471



Felix Leditzky

IQC, University of Waterloo

Perimeter Institute

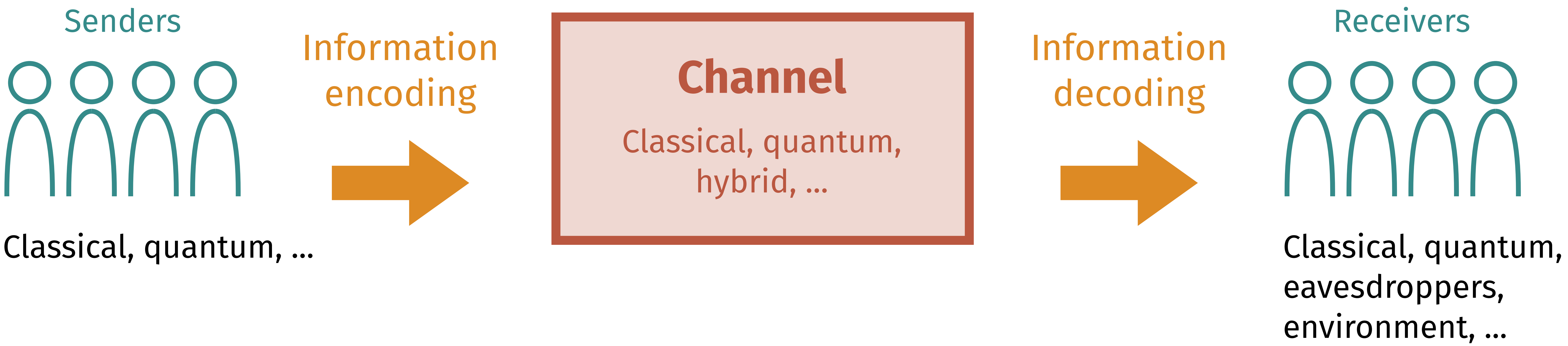
Institute for Quantum Computing

PERIMETER INSTITUTE

(joint work with J. Bausch, University of Cambridge)

Channel coding in information theory

Many communication tasks can be formalized as a channel coding problem:



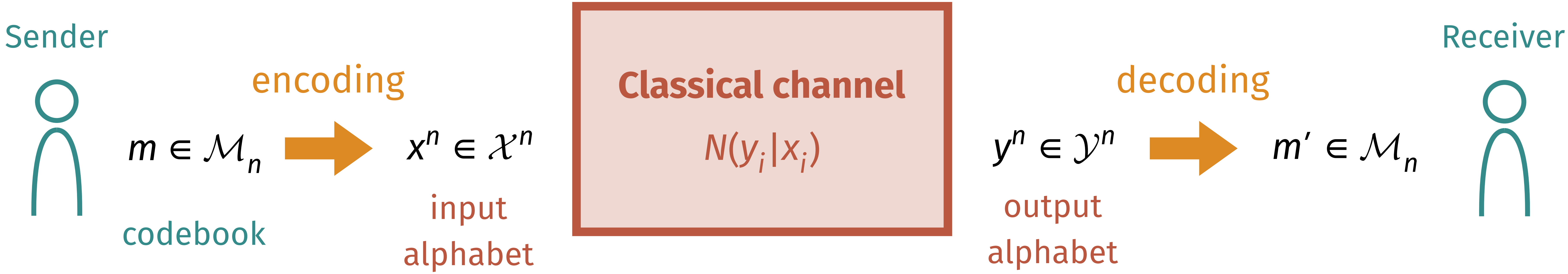
Central notions in information theory:

→ **Capacity of a channel:** quantifies information-processing capabilities of a channel.

→ **Coding theorem:** expresses capacity as (optimization over) entropic quantities.

Channel coding in information theory

Prototypical (and first) example: classical point-to-point channel



Capacity:

$$\mathcal{C}(N) := \sup\{ \tfrac{1}{n} \log |\mathcal{M}_n| : \ \Pr(M \neq M') \to 0\}.$$

Shannon entropy: $H(X) = -\sum_{x \in \mathcal{X}} p_X(x) \log p_X(x)$

Mutual information: $\mathcal{I}(X;Y) = H(X) + H(Y) - H(XY)$

Shannon's noisy channel coding theorem

$$\mathcal{C}(N) = \max_{p_X} \mathcal{I}(X;Y)$$

[Shannon '48]

Channel coding in information theory

Point-to-point classical communication is **extremely well understood**:

Shannon's formula is **single-letter**, i.e., a bounded optimization problem.

$$\mathcal{C}(N) = \max_{p_X} \mathcal{I}(X;Y)$$

[Shannon '48]

Shannon's theorem can be phrased as a **geometric program**, a type of convex program.

[Chiang, Boyd '04]

Capacity of a classical channel can be **efficiently computed** in time

$$O(|\mathcal{Y}||\mathcal{X}| \log |\mathcal{X}| \varepsilon^{-1}).$$

[Arimoto '72; Blahut '72]

There are families of **capacity-achieving codes** with efficient encoding/decoding: LDPC codes, turbo codes, polar codes.

[Gallager '60; Berrou '91; Arıkan '09]

Channel coding in information theory

Problematic settings

- → Network information theory (anything beyond 1 sender → 1 receiver)
- → Quantum resources: quantum channels, quantum information, …

Complications

- → Increased complexity of algorithms
- → Non-convex optimization problems
- → Unbounded optimization problems (multi-letter formulas)

This talk: Quantum information transmission through quantum channel

- → Relevant capacity: **Quantum capacity** of a quantum channel
- → **Non-convexity** and **multipartite entanglement** main problems/objects of study.
- → Use mathematical/numerical tools, in particular **symmetries** and **optimization techniques,** to study quantum capacity.

Table of contents

Quantum capacity of a quantum channel

Quantum channel models:

Information theory

Noisy communication link between quantum parties.

Error correction

Environmental noise in a quantum device.

Quantum capacity characterizes:

How much quantum information can be sent faithfully?

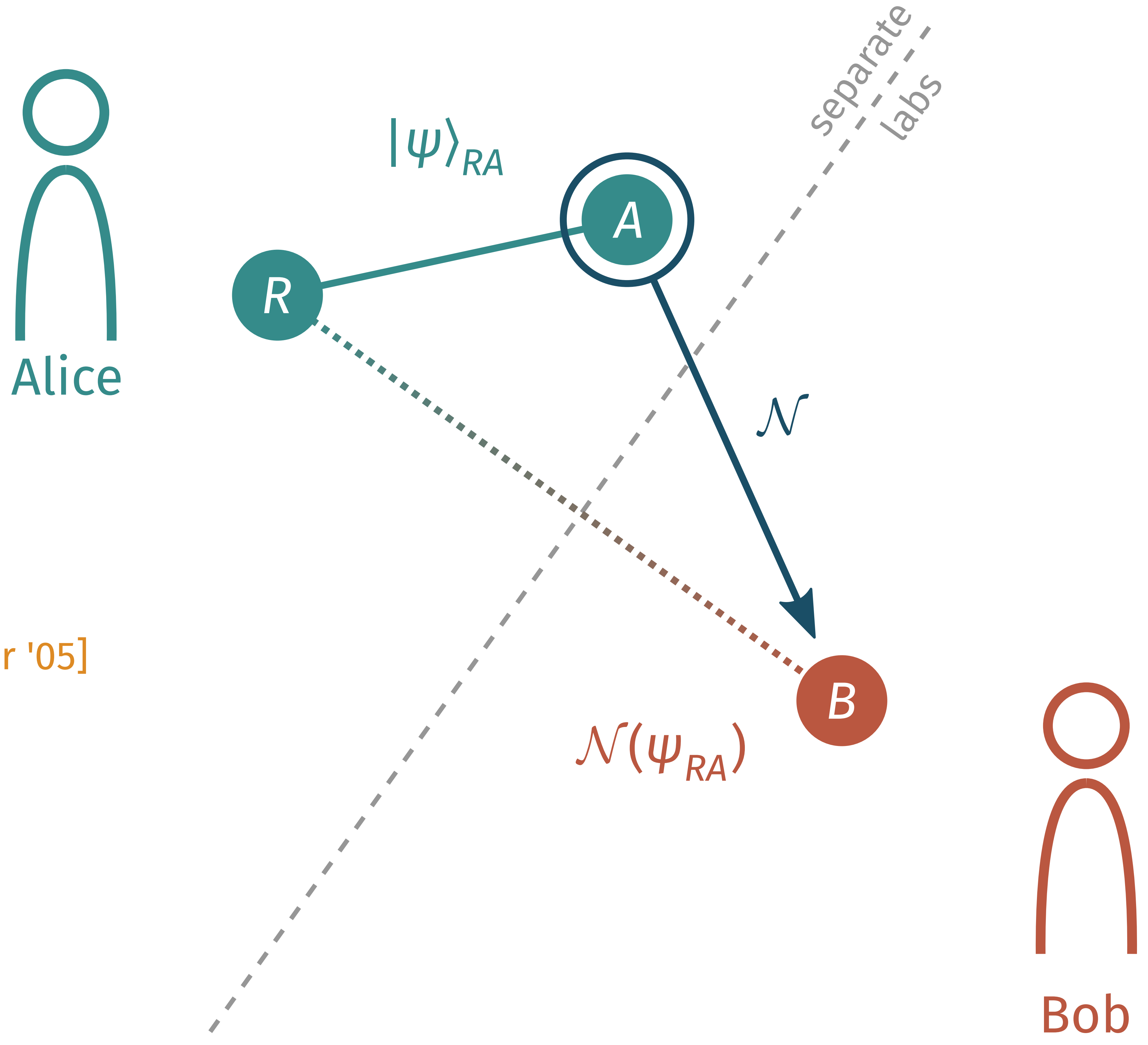
How much quantum information can be protected against noise?

Quantum capacity of a quantum channel

Entanglement generation:

→ Share k identical copies of pure bipartite state ψ_{RA} via channel $\mathcal{N}$.

→ Distill EPR pairs $|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B$ from $\mathcal{N}(\psi_{RA})^{\otimes k}$ using **local operations** and **forward classical communication** with vanishing error. [Devetak '05; Devetak, Winter '05]



Achievable rate: coherent information

$$\mathcal{I}(\psi,\mathcal{N}) = S(\mathcal{N}(\psi_A)) - S(\mathcal{N}(\psi_{RA}))$$

Von Neumann entropy: $S(\rho) = -\operatorname{tr}(\rho \log \rho)$

Quantum capacity of a quantum channel

Idea:

→ Distribute a multipartite state ψ_{RA^n} via n identical and independent copies of $\mathcal{N}$.

→ Rate for distilling from $[\mathcal{N}^{\otimes n}(\psi_{RA^n})]^{\otimes k}$:

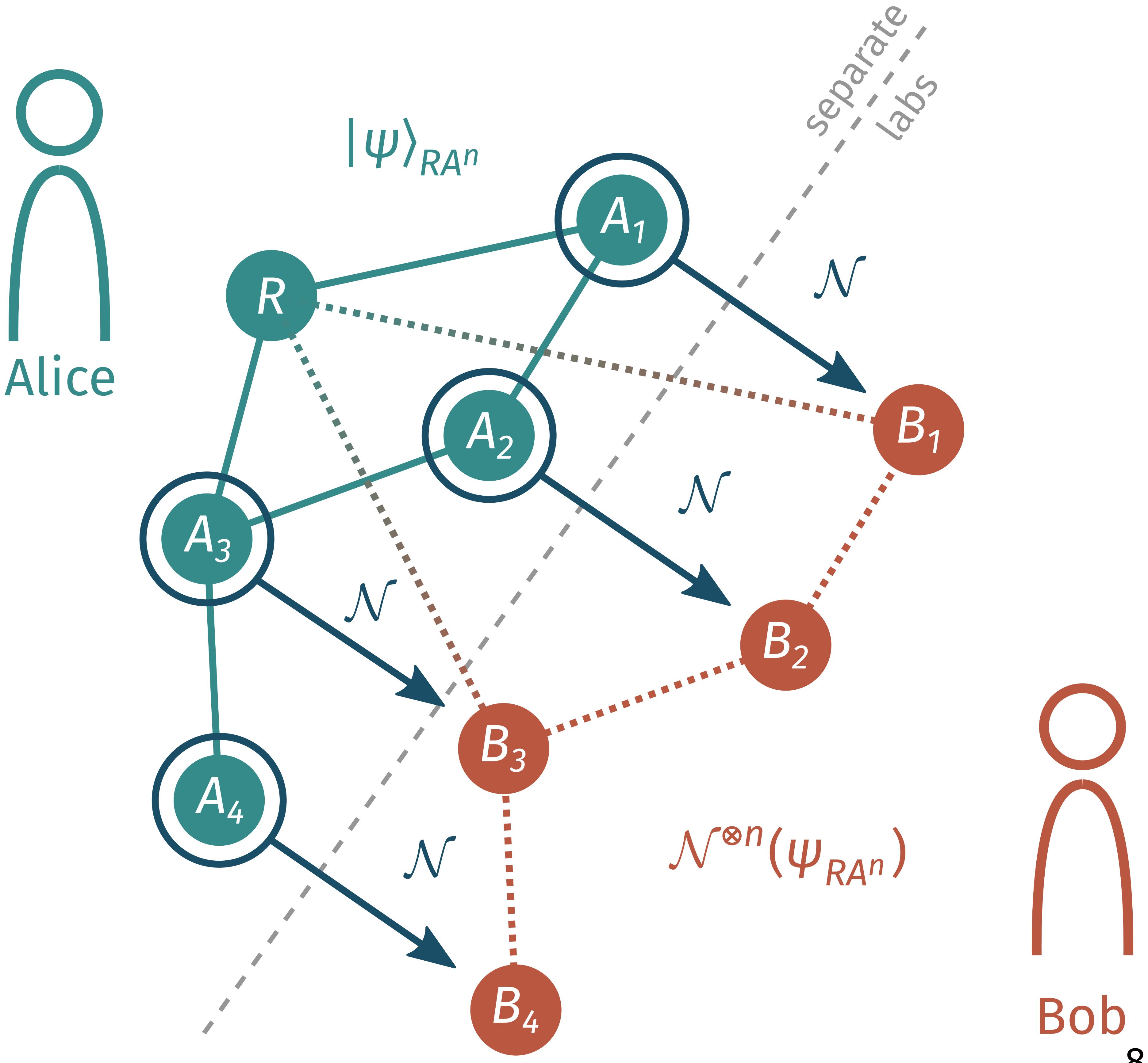
$$\frac{1}{n}\mathcal{I}_c(\psi_n, \mathcal{N}^{\otimes n})$$

Superadditivity of coherent information

There are ψ_n and $\mathcal{N}$ such that

$$\frac{1}{n}\mathcal{I}_c(\psi_n, \mathcal{N}^{\otimes n}) > \max_{\phi} \mathcal{I}_c(\phi, \mathcal{N}).$$

[Shor, Smolin '96; DiVincenzo et al. '98]



Quantum capacity of a quantum channel

Quantum capacity $Q(\mathcal{N})$**:** largest rate at which EPR pairs can be generated with asymptotically vanishing error.

Quantum capacity coding theorem

$$Q(\mathcal{N}) = \sup_{n\in\mathbb{N}} \frac{1}{n} \max_{\psi_n} \mathcal{I}_c(\psi_n, \mathcal{N}^{\otimes n})$$

Unbounded optimization problem (because of superadditivity) and known pathological behavior.

Non-concave maximization problem for channels with superadditive coherent information.

[Schumacher '96; Schumacher, Nielsen '96; Lloyd '97; Shor '02; Devetak '05; Watanabe '12; Cubitt '15]

Quantum capacity of a quantum channel

Quantum capacity

$$Q(\mathcal{N}) = \sup_{n\in\mathbb{N}} \frac{1}{n} \max_{\psi_n} \mathcal{I}_c(\psi_n, \mathcal{N}^{\otimes n})$$

→ **Multipartite entanglement** in code state ψ_{RA^n} causes superadditivity.

→ Characterizing multipartite entanglement is hard for growing n due to **exponential scaling** of Hilbert space dimension.

→ For fixed n, objective function is non-concave and hard to optimize.

Possible computational ansatz

Restrict quantum states to **polynomial subspace** of Hilbert space with sufficiently rich entanglement structure, such as quantum neural network states.

[Bausch, FL '18]

Possible mathematical ansatz

For specific quantum channels, consider **symmetric codes** and exploit symmetries to compute coherent information.

➙ Permutation invariance [Kern, Renes '08]

➙ **Graph symmetries** [Bausch, FL '19]

Table of contents

Pauli channels and stabilizer states

Pauli channels

$\mathcal{N}_{\mathrm{p}}(\rho) = p_0\rho + p_1 X\rho X + p_2 Y\rho Y + p_3 Z\rho Z$

→ $\mathbf{p} = (p_0, p_1, p_2, p_3)$ probability distribution.

→ X, Y, Z Pauli matrices.

Important examples:

depolarizing noise $\mathbf{p}_{\mathrm{dep}} = (1-p, \frac{p}{3}, \frac{p}{3}, \frac{p}{3})$

BB84 channel $\mathbf{p}_{\mathrm{BB84}} = ((1-p)^2, p-p^2, p^2, p-p^2)$

→ QEC: Ability to correct X, Y, Z errors is sufficient for correcting **arbitrary unitary errors**. [Shor '95; Steane '96]

→ For Pauli channels of the form $\mathrm{p}_x = (1-x, xp_1, xp_2, xp_3)$ we are interested in the **threshold**:

$$\text{Supremum over all } x \text{ such that } Q(\mathcal{N}_{\mathrm{p}_x}) > 0.$$

QIT: $Q(\mathcal{N}) > 0 \Leftrightarrow$
faithful quantum communication possible.

QEC: $Q(\mathcal{N}) > 0 \Leftrightarrow$
perfect error-correcting code exists.

Pauli channels and stabilizer states

→ Pauli channel: $\mathcal{N}_{\mathbf{p}}(\rho) = p_0\rho + p_1 X\rho X + p_2 Y\rho Y + p_3 Z\rho Z$.

→ Tensor powers: $\mathcal{N}_{\mathrm{p}}^{\otimes n}(\rho_n) = \sum_{j^n} p_{j^n} E_{j^n} \rho_n E_{j^n}$,

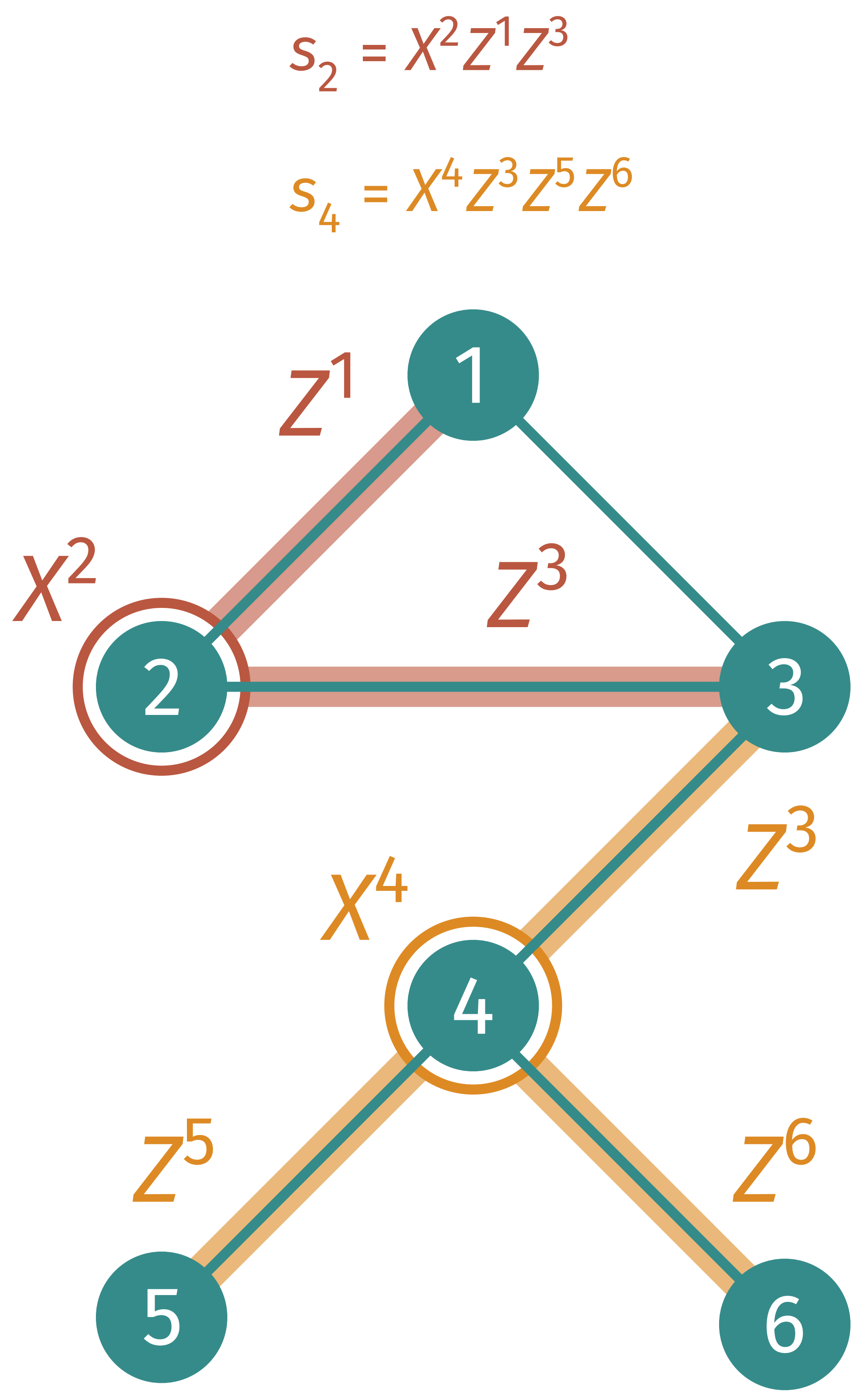
with n-qubit Pauli operators $E_{j^n} \in \mathcal{P}_n = \{I, X, Y, Z\}^{\otimes n} \cup \{\pm 1, \pm i\}$.

→ Restrict to **stabilizer states** $|\psi_k\rangle$ which are stabilized by

k pairwise commuting stabilizer generators $s_i \in \mathcal{P}_k$:

$$s_i|\psi_k\rangle = |\psi_k\rangle \quad \text{for } i = 1, \dots, k.$$

[Gottesman '97]



Graph states

Let $\Gamma = (V, E)$ be a graph and $N_i = \{j \in V : (i,j) \in E\}$.

For each vertex i define stabilizers $s_i = X^i \prod_{j \in N_i} Z^j$.

The **graph state** $|\Gamma\rangle$ is the unique pure state stabilized by $s_1, \dots, s_k$.

Graph states

Every stabilizer state is local unitary (LU) equivalent to a graph state: [van den Nest et al. '04]

For all stab's $|\psi_k\rangle$ there exist $\Gamma = (V, E)$ and unitaries $U_1, \dots, U_k$ s.t. $U_1 \otimes \dots \otimes U_k |\psi_k\rangle = |\Gamma\rangle$.

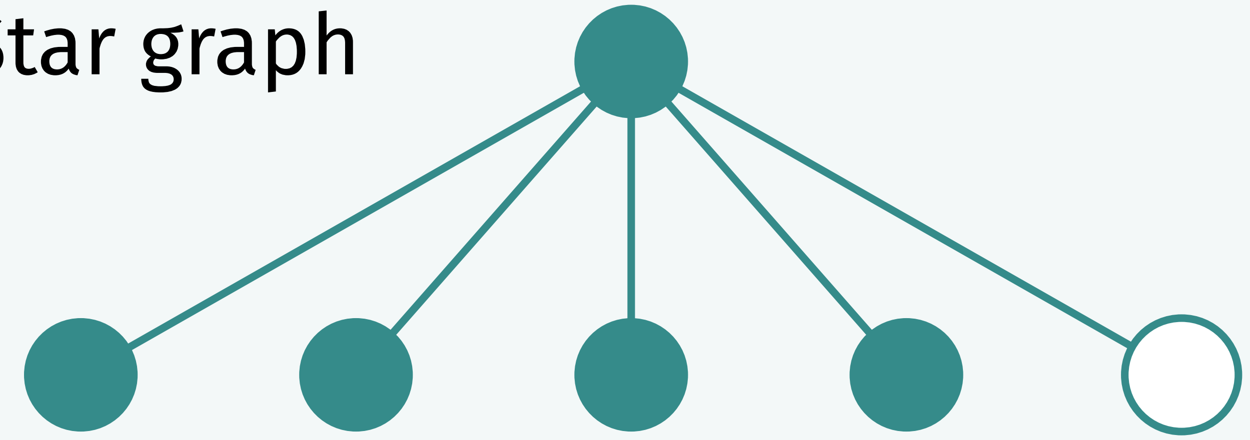
Important quantum codes as graph states:

● system qubits A_i ○ reference qubit R

Repetition code (GHZ state)

$|0\rangle_R \otimes |0\rangle_A^{\otimes n} + |1\rangle_R \otimes |1\rangle_A^{\otimes n}$

Star graph



Cat code (Shor code)

Concatenation of Z-type and X-type rep code.

X-type rep: $|+\rangle^{\otimes n} + |-\rangle^{\otimes n}$,

where $|\pm\rangle \sim |0\rangle \pm |1\rangle$.

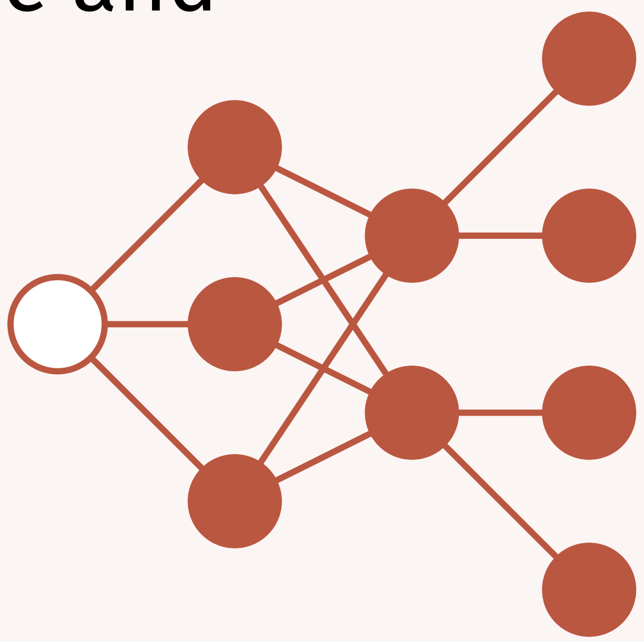
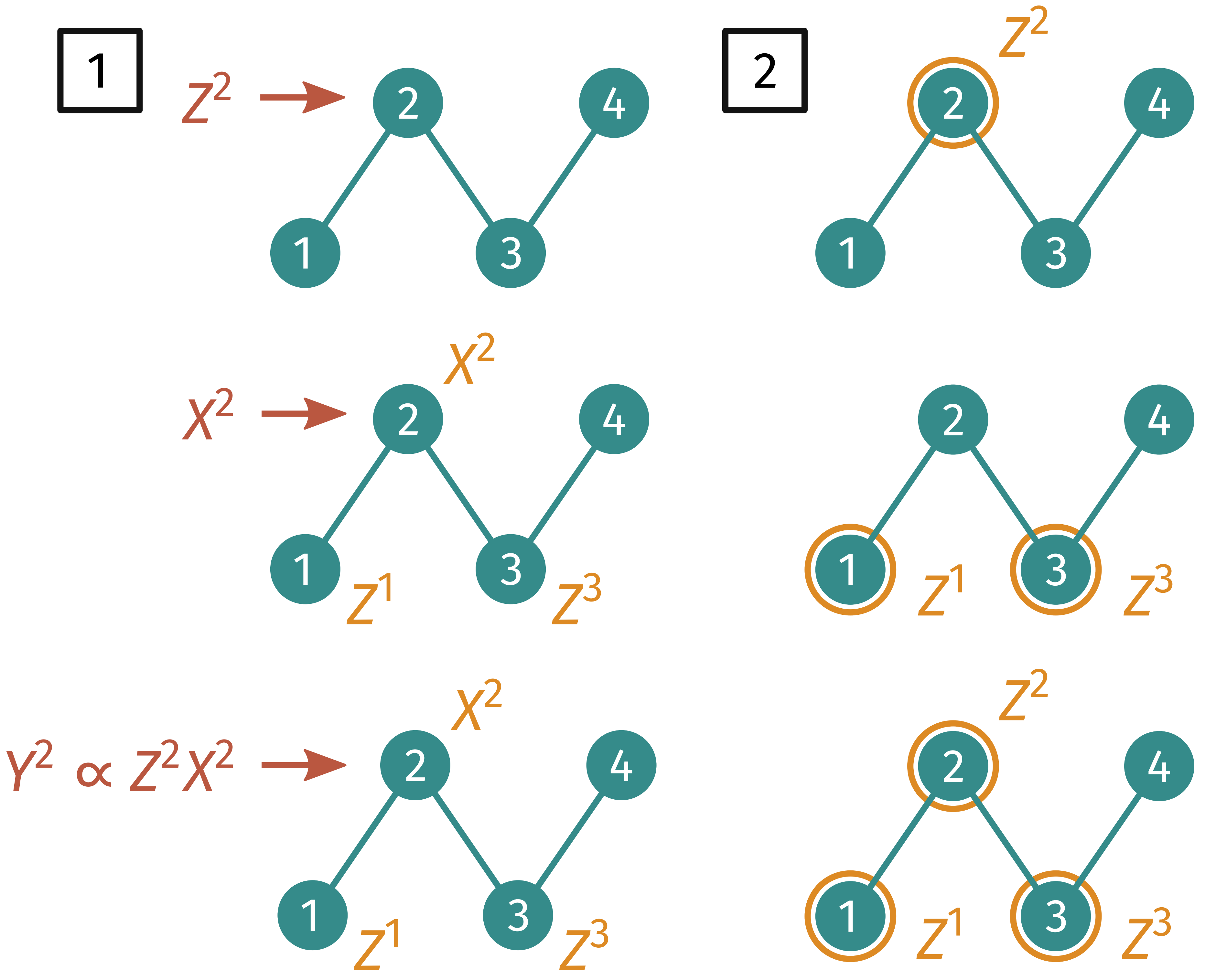


Table of contents

Decoherence of graph states

Quantum capacity: $Q(\mathcal{N}) = \sup_{n \in \mathbb{N}} \frac{1}{n} \max_{\psi_n} \mathcal{I}_c(\psi_n, \mathcal{N}^{\otimes n})$ $\Rightarrow$ $Q(\mathcal{N}) \geq \frac{1}{n} \mathcal{I}_c(\psi_n, \mathcal{N}^{\otimes n})$ for all ψ_n and $n \in \mathbb{N}$.

Coherent information: $\mathcal{I}_c(\phi, \mathcal{N}) = S(\mathcal{N}(\phi_A)) - S(\mathcal{N}(\phi_{RA}))$



Goal

Compute the tensor action of a Pauli channel

$$\mathcal{N}_{\mathbf{p}}(\rho) = p_0 \rho + p_1 X \rho X + p_2 Y \rho Y + p_3 Z \rho Z$$

on a graph state $|\Gamma\rangle$.

Observation

Graph states translate (products of) Pauli errors into Z-type errors.

Decoherence of graph states

Decoherence of graph states:

$$Z^i|\Gamma\rangle\langle\Gamma|Z^i = Z^i|\Gamma\rangle\langle\Gamma|Z^i \qquad X^i|\Gamma\rangle\langle\Gamma|X^i = Z^{N_i}|\Gamma\rangle\langle\Gamma|Z^{N_i} \qquad Y^i|\Gamma\rangle\langle\Gamma|Y^i = Z^{i\oplus N_i}|\Gamma\rangle\langle\Gamma|Z^{i\oplus N_i}$$

Graph states subjected to Pauli noise

For a Pauli channel, output state is of the form

$$\mathcal{N}^{\otimes n}(|\Gamma\rangle\langle\Gamma|) = \sum_{U\subset V} \lambda_U |U\rangle\langle U|,$$

where the $|U\rangle = Z^U|\Gamma\rangle$ form the **graph state basis**.

Computing coherent information

Determine coefficients λ_U

for all subset vertices $U \subset V$

using the decoherence rules above.

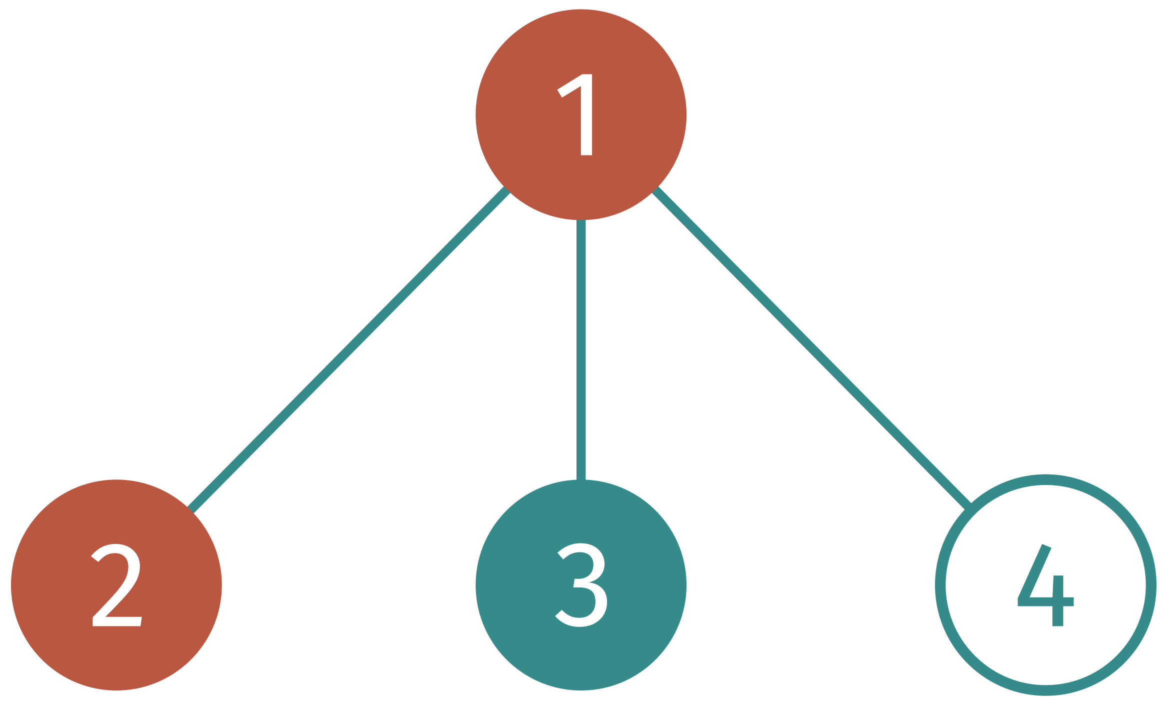
[Hein et al. '05]

Decoherence of graph states

Example: star graph on 4 vertices, $U = \{1,2\}$.

$$\mathcal{N}^{\otimes n}(|\Gamma\rangle\langle\Gamma|) = \sum_{U \subset V} \lambda_U |U\rangle\langle U|$$

Pauli error operators generating U:



$$\begin{array}{cccc} Z^1Z^2 & Y^2 & Z^2X^3 & Z^1Y^2X^3 \\ \downarrow & \downarrow & \downarrow & \downarrow \end{array}$$

$$\lambda_{\{1,2\}} = p_0^2 p_3^2 + p_0^3 p_2 + p_0^2 p_1 p_3 + p_0 p_1 p_2 p_3$$

$$\mathcal{N}_{\mathbf{p}} : \rho \longmapsto p_0\rho + p_1 X\rho X + p_2 Y\rho Y + p_3 Z\rho Z$$

PROBLEM

Exponential scaling:

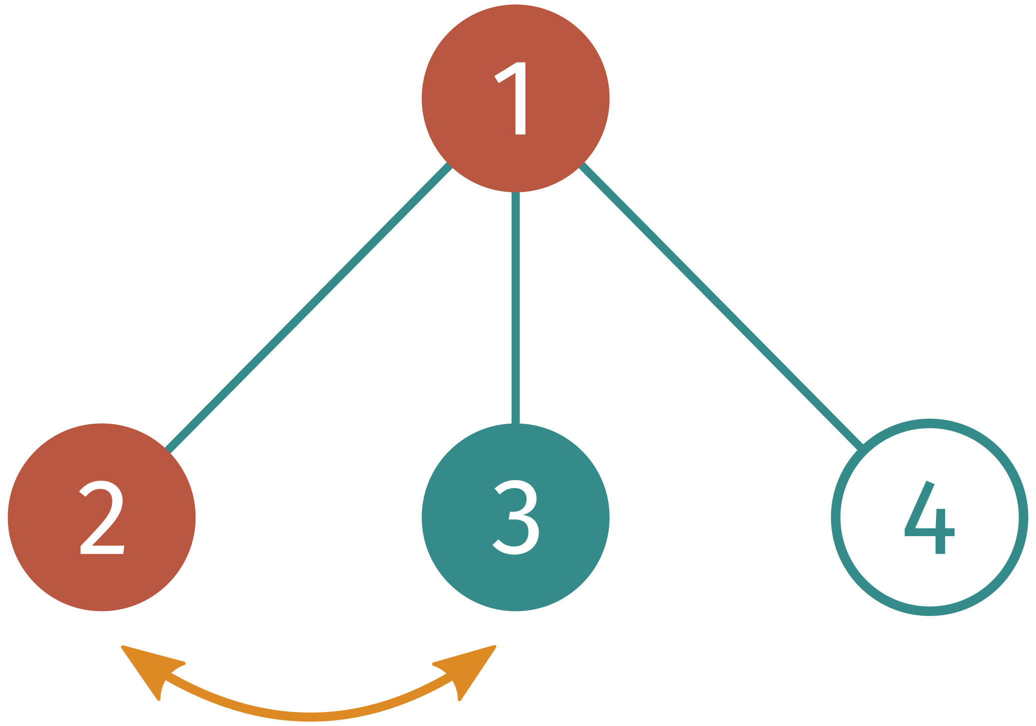
$$|V| = n, U \subset V$$

Table of contents

Exploiting graph symmetries

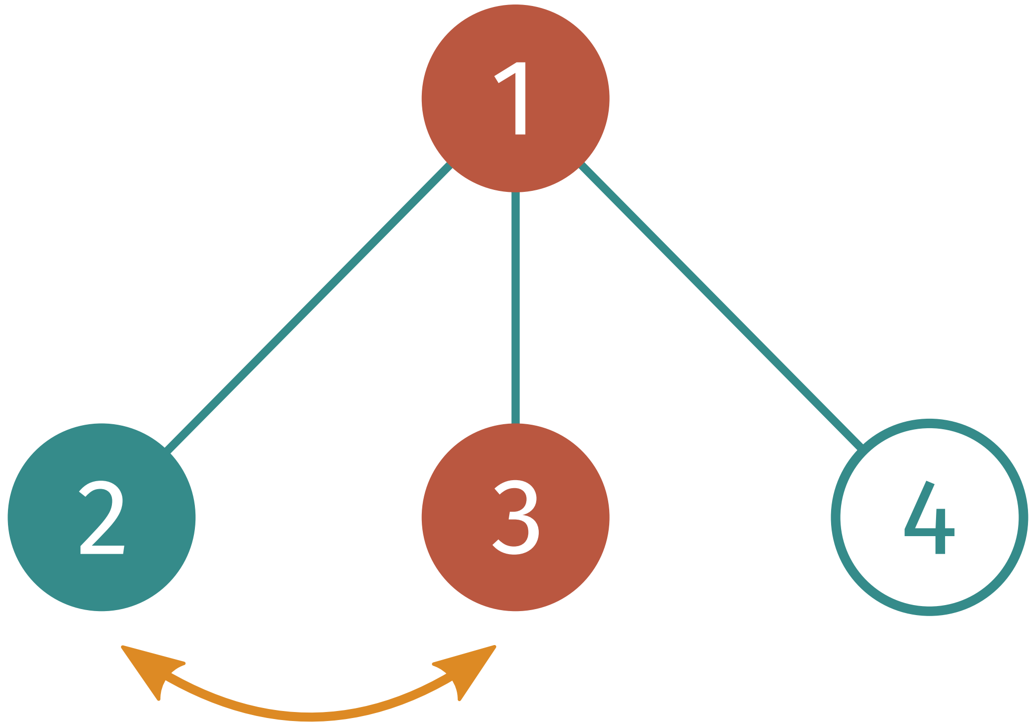
Revisit example: star graph on 4 vertices, $U = \{1, 2\}$.

$$\mathcal{N}^{\otimes n}(|\Gamma\rangle\langle\Gamma|) = \sum_{U \subset V} \lambda_U |U\rangle\langle U|$$



Graph automorphism

$2 \rightleftharpoons 3$



$Z^1Z^2 \quad Y^2 \quad Z^2X^3 \quad Z^1Y^2X^3$

$Z^1Z^3 \quad Y^3 \quad Z^3X^2 \quad Z^1Y^3X^2$

$$p_0^2p_3^2 + p_0^3p_2 + p_0^2p_1p_3 + p_0p_1p_2p_3 = \lambda_{\{1,2\}} = \lambda_{\{1,3\}} = p_0^2p_3^2 + p_0^3p_2 + p_0^2p_1p_3 + p_0p_1p_2p_3$$

Exploiting graph symmetries

Let $G = \mathrm{Aut}(\Gamma, |A|)$ be the **2-colored graph automorphism group** of the graph Γ.

Identify Pauli operators with

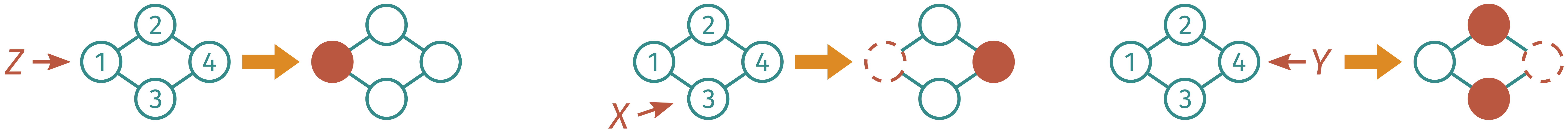
quaternary strings $Q = \{0, 1, 2, 3\}^n$.

Example: $Z^1 X^3 Y^4 \longleftrightarrow \texttt{3012}$

Identify subsets $U \subset V$

with **binary strings** $B = \{0, 1\}^n$.

Example: $U = \{2, 3\} \longleftrightarrow \texttt{0110}$



Group action of G on Q and B by permuting strings is **homomorphic**:

Decoherence rules induce G-equivariant surjective map $\theta : Q \to B$.

$\theta(\texttt{3012}) = \texttt{0110}, \pi = (23)$

$\theta(\pi(\texttt{3012})) = \theta(\texttt{3102}) = \texttt{0110} = \pi(\texttt{0110})$

Exploiting graph symmetries

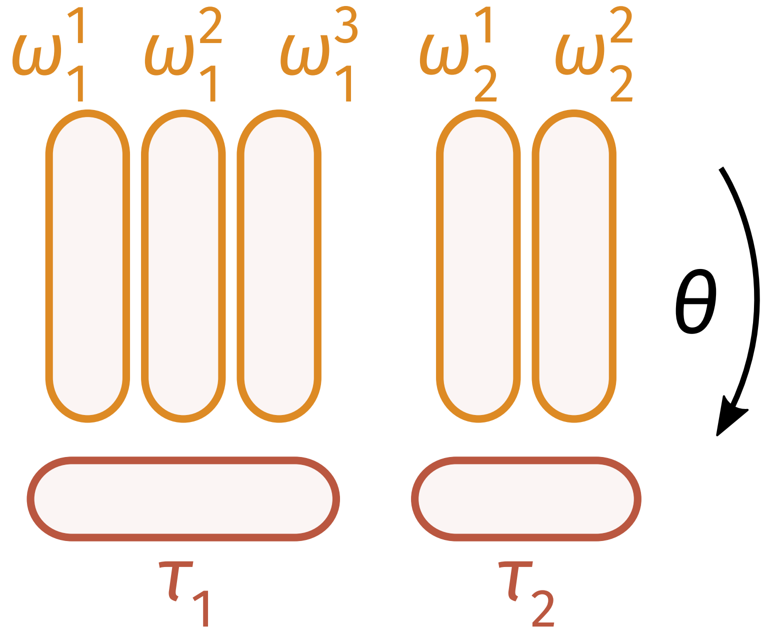
$Q = \{0,1,2,3\}^n, B = \{0,1\}^n$, automorphism group G acts on Q, B by permuting strings.

G-equivariant surjective map $\theta : Q \to B$ defined by decoherence rules.

Homomorphic group actions

→ For each orbit $\omega \in Q/G$ there exists a unique $\tau \in B/G$ such that $\omega \cap \theta^{-1}(\tau) \neq \{\}$.

→ For an orbit $\tau \in B/G$ and subsets $U, U' \in \tau$ we have $|\theta^{-1}(U)| = |\theta^{-1}(U')|$.



To compute $\mathcal{N}^{\otimes n}(|\Gamma\rangle\langle\Gamma|) = \sum_{U \subset V} \lambda_U |U\rangle\langle U|$

and partial trace $\mathrm{Tr}_R\, \mathcal{N}^{\otimes n}(|\Gamma\rangle\langle\Gamma|)$

Symmetry-aware algorithm

Loop over orbit representatives of Q/G

and collect contributions and multiplicities to get λ_U.

Yields **analytical expression** for $\mathcal{I}_c(\Gamma, \mathcal{N}^{\otimes n})$ in the p_i's.

Table of contents

Numerical method

Given: Pauli channel $\mathcal{N}_{\mathrm{p}_x}$, where $\mathrm{p}_x = (1 - x, xp_1, xp_2, xp_3)$, and a graph state $|\Gamma\rangle$ on $n + 1$ qubits.

Goal: compute coherent information $\mathcal{I}_c(\Gamma, \mathcal{N}^{\otimes n})$ from the output state

$$\mathcal{N}^{\otimes n}(|\Gamma\rangle\langle\Gamma|) = \sum_{U \subset V} \lambda_U |U\rangle\langle U|.$$

Our algorithm yields an **analytical expression** of the coherent information

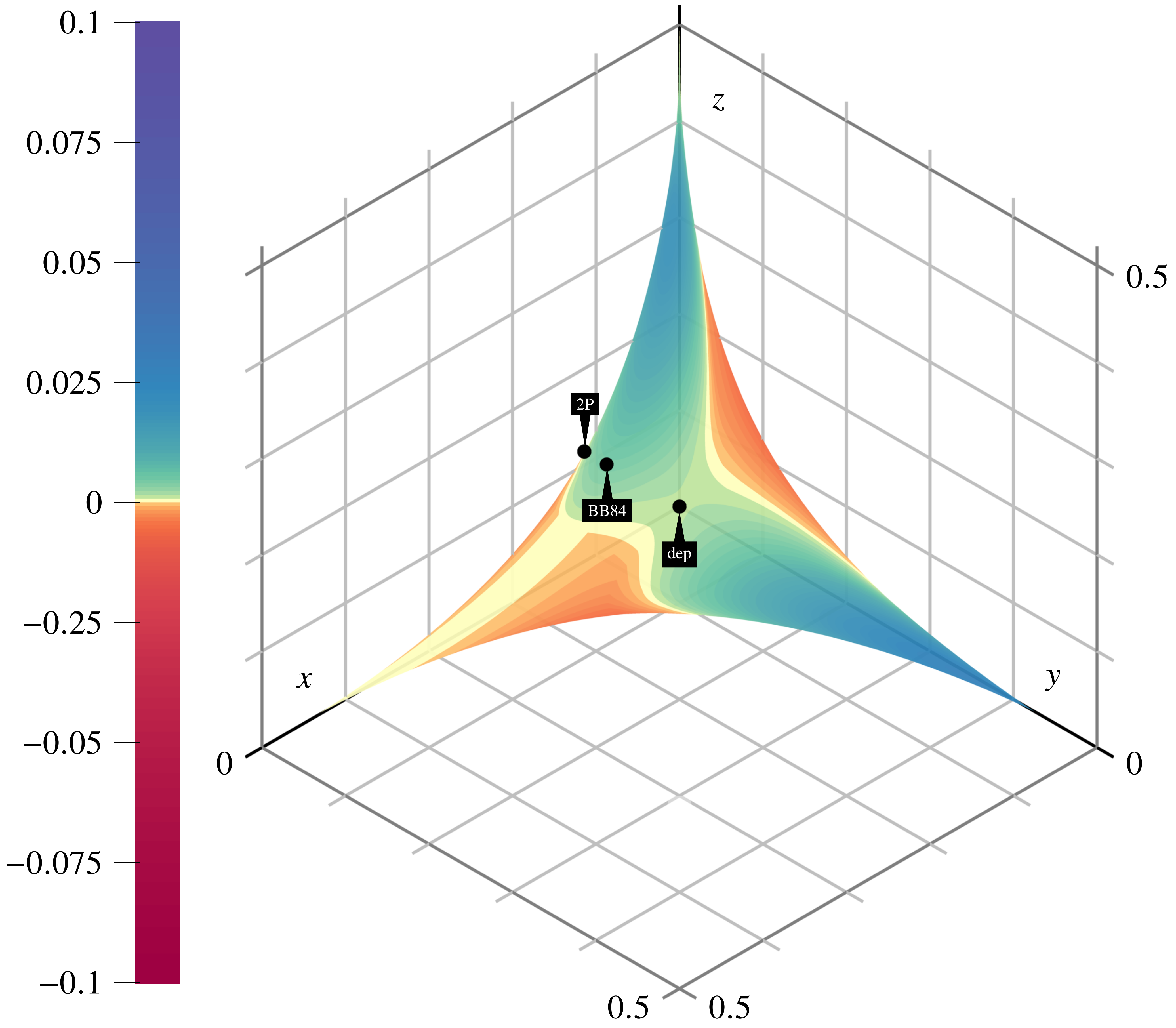
in terms of Pauli probabilities $(1 - x, xp_1, xp_2, xp_3)$, i.e., a function $f(x)$.

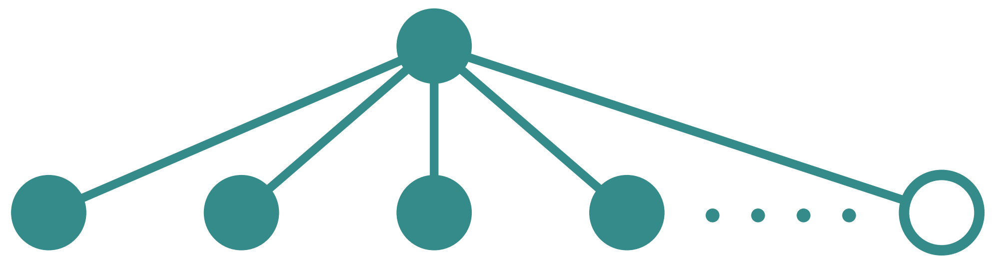
This function $f(x)$ is **non-increasing** in x, so the **error threshold** is given by the **first root of** f.

We can determine this threshold for a fixed graph state in the **whole Pauli channel simplex**

by varying (p_1, p_2, p_3), leading to a **threshold surface**.

Repetition code thresholds





Plot of the **threshold surface** of rep codes with $n \leq 60$.

$x \mapsto \mathbf{p}_x = (1 - x, xp_1, xp_2, xp_3)$

Color: Superadditivity magnitude

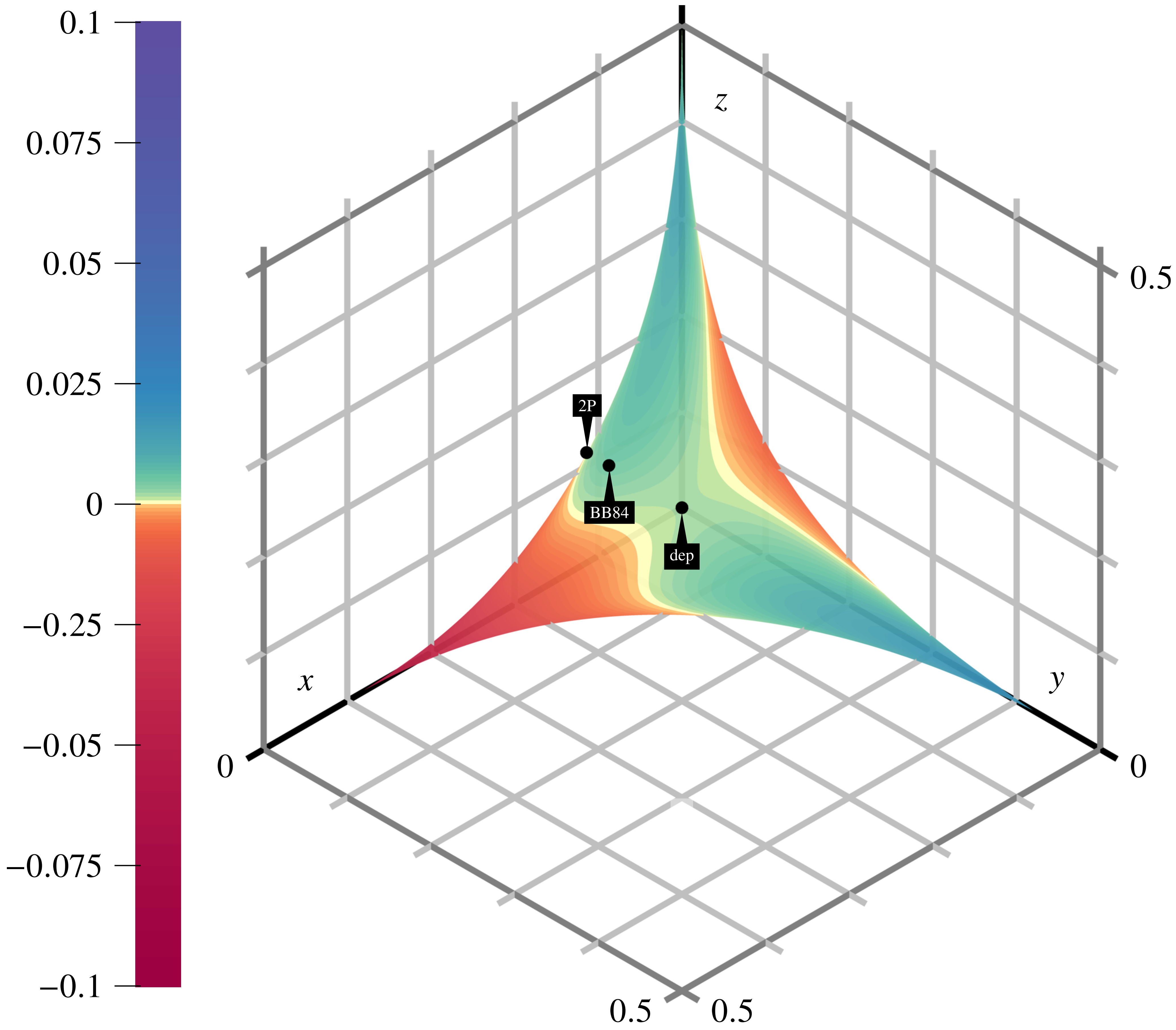
$$\frac{1}{n}\mathcal{I}_c(\Gamma, \mathcal{N}_{\mathbf{p}_x}^{\otimes n}) - \max_{\psi} \mathcal{I}_c(\psi, \mathcal{N}_{\mathbf{p}_x})$$

2P: $(1 - p, \frac{p}{2}, 0, \frac{p}{2})$

BB84: $((1 - p)^2, p - p^2, p^2, p - p^2)$

dep: $(1 - p, \frac{p}{3}, \frac{p}{3}, \frac{p}{3})$

Concatenated code thresholds



5-in-5 code

(graph state on the right)

Achieves best threshold

for depolarizing channel

for $n \leq 25$ channel copies.

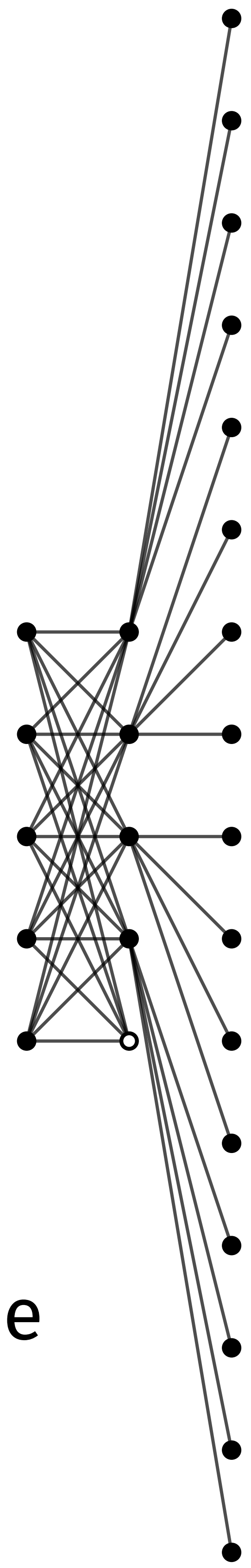
[DiVincenzo et al. '98]

[Smith, Smolin '07; Fern, Whaley '08]

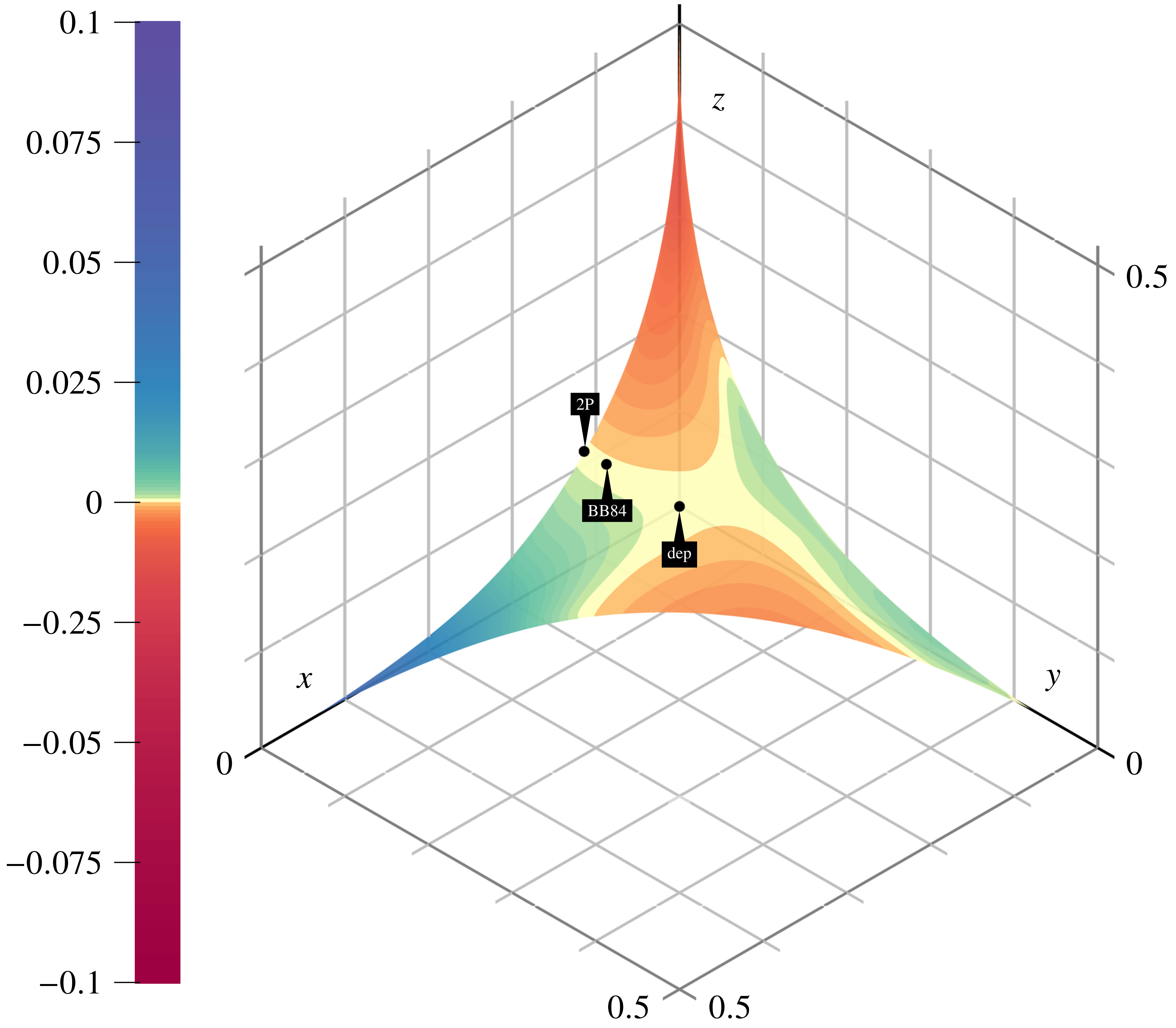
$$x \mapsto \mathbf{p}_x = (1 - x, xp_1, xp_2, xp_3)$$

Color: Superadditivity magnitude

$$\frac{1}{n}\mathcal{I}_c(\Gamma, \mathcal{N}_{\mathbf{p}_x}^{\otimes n}) - \max_{\psi} \mathcal{I}_c(\psi, \mathcal{N}_{\mathbf{p}_x})$$



A new code family: tree graph states



We found a new interesting code family based on **tree graphs with two levels**.

Error thresholds are competitive compared to 5-in-5 code (see left).

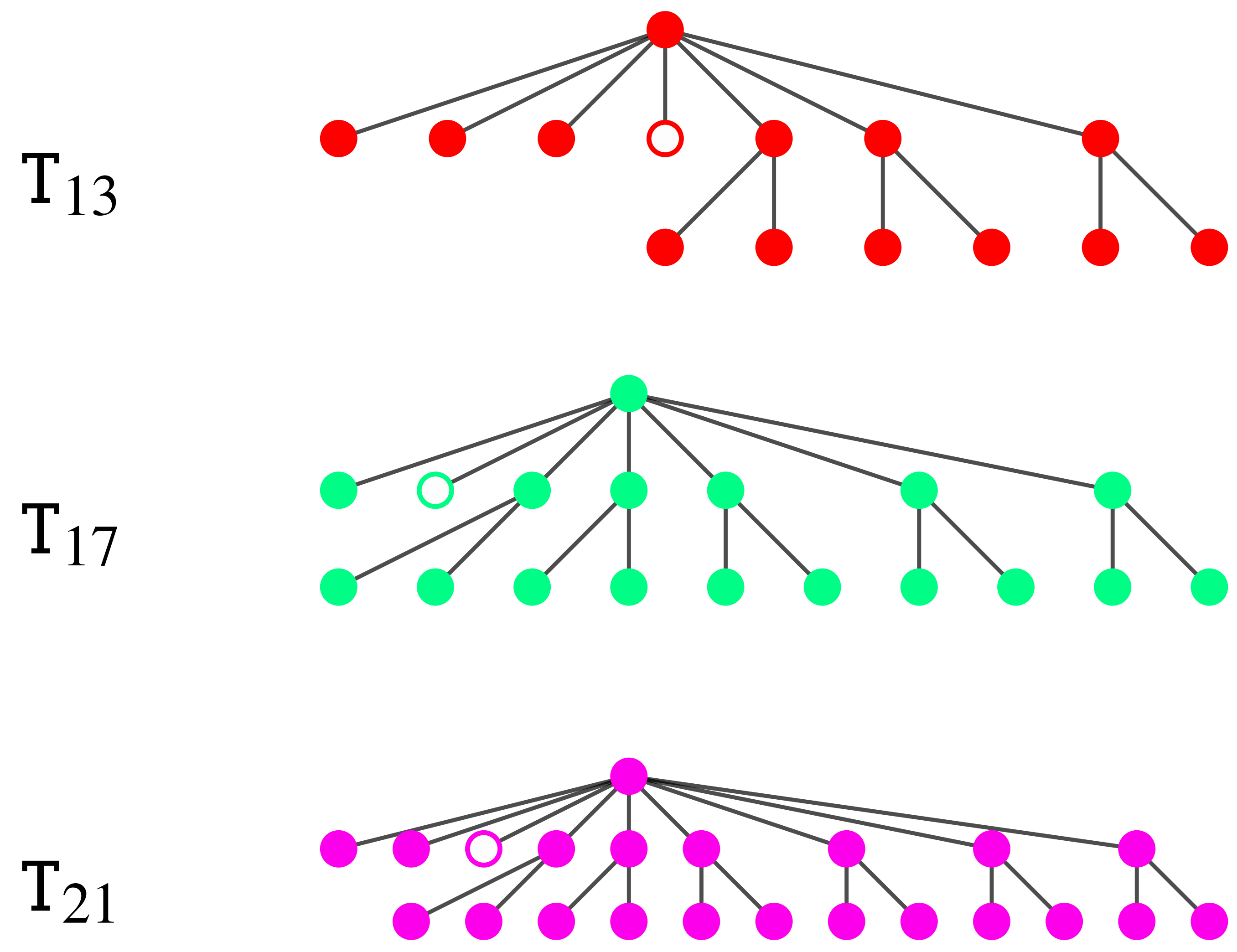
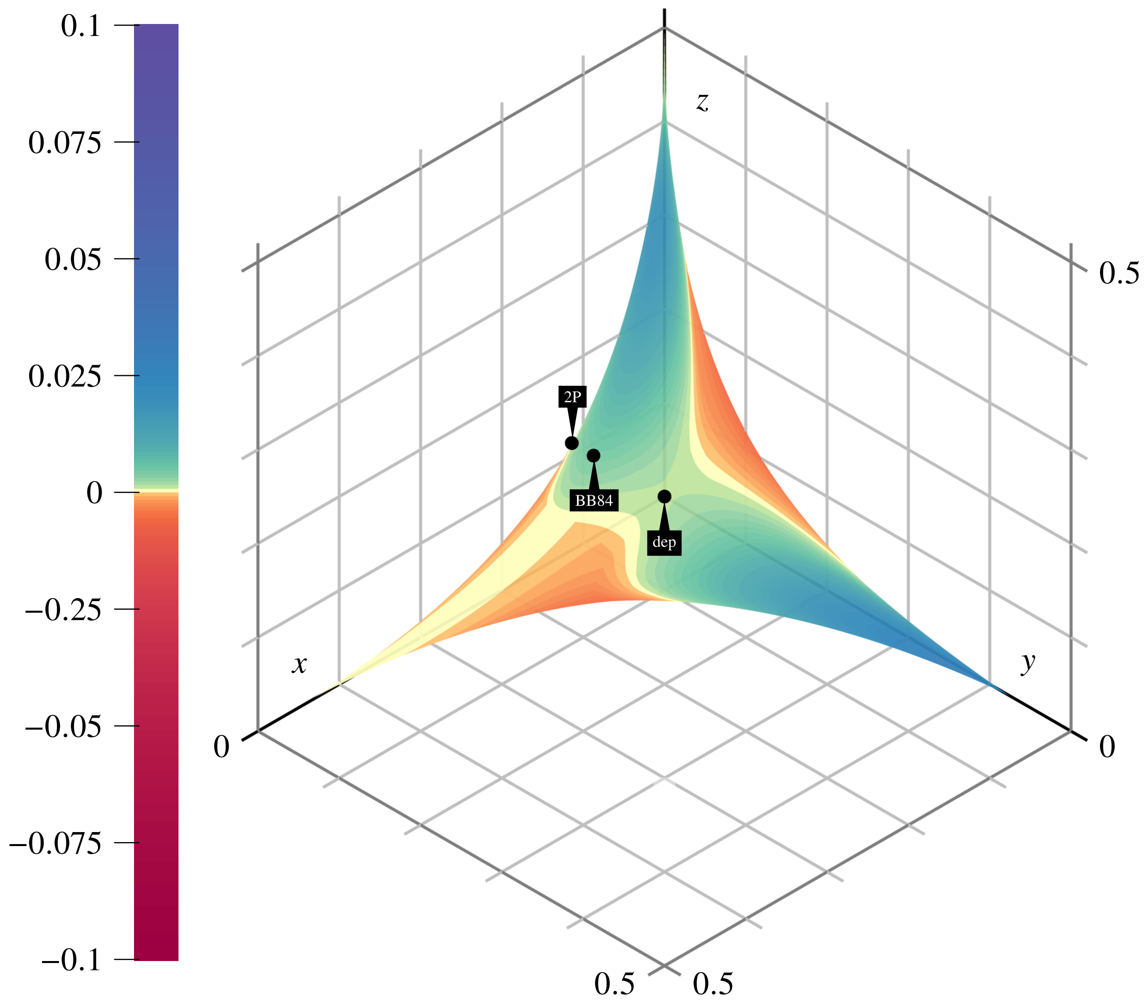


Table of contents

Symmetries in channel coding problems

Summary

We can use the graph state formalism and exploit **graph symmetries** and tools from **group theory** to approximate quantum capacity of interesting channels.



Ideas for future work:

➡ Generalize methods to handle more general quantum channels?

➡ Improve upon/adopt more tools from computational group theory (CGT)?

➡ Can we use the framework of group actions and CGT to analyze concrete quantum error correction codes and their decoders, thresholds, etc?

Our paper
on arXiv.org

Download
these slides

Contact
information

THANKS

for your attention!