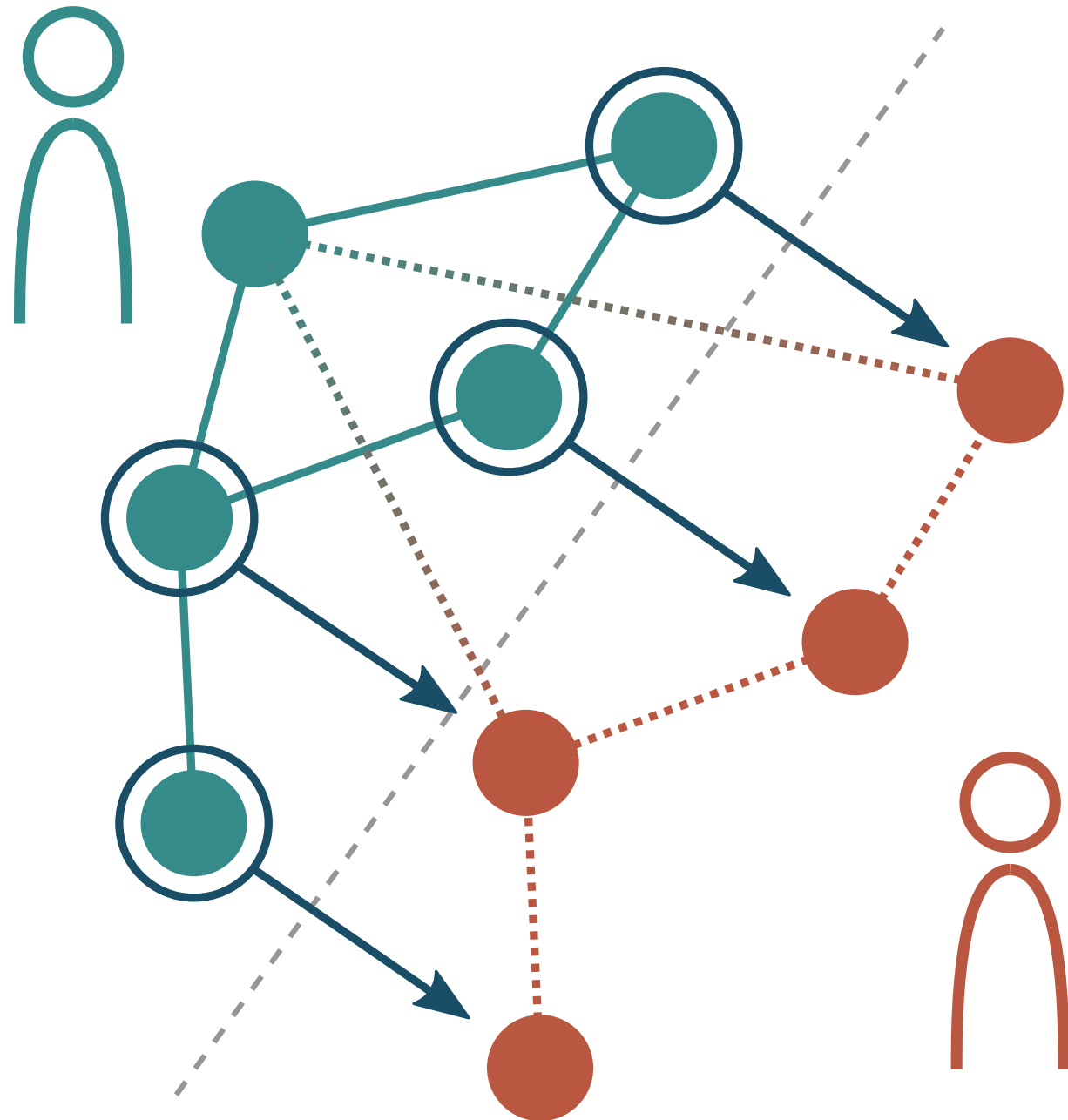


Symmetries and entanglement in channel coding problems



Felix Leditzky

IQC, University of Waterloo

Perimeter Institute

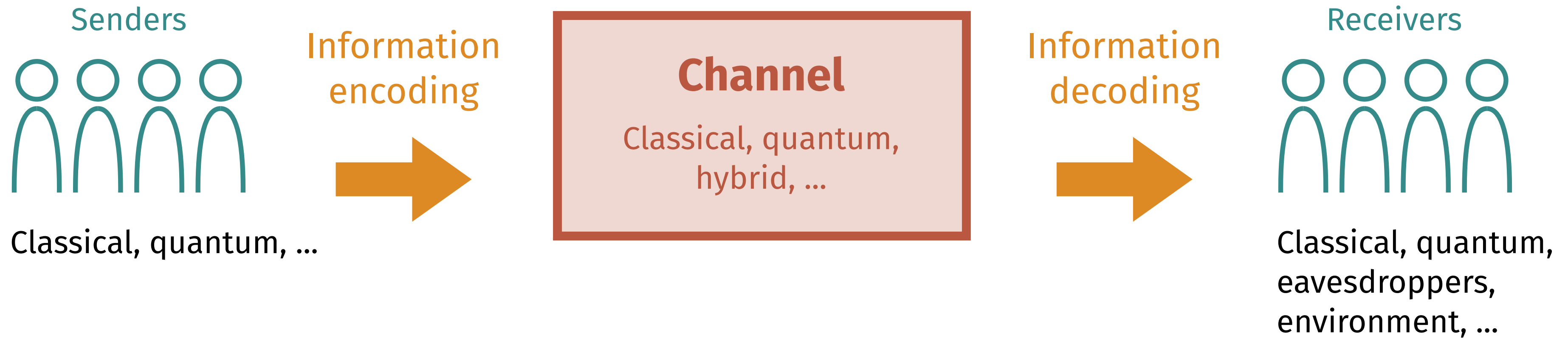
partly based on **arXiv:1910.00471**

(joint work with J. Bausch)



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 example: classical point-to-point channel

Shannon's channel coding theorem

[Shannon '48]

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

Single-letter: bounded optimization problem

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

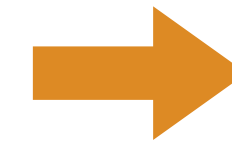
[Chiang, Boyd '04]

Sender



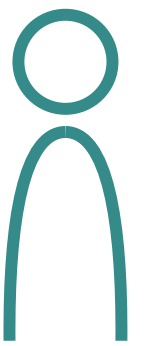
$$x^n \in \mathcal{X}^n$$

$$N(y_i | x_i)$$



$$y^n \in \mathcal{Y}^n$$

Receiver



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

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

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

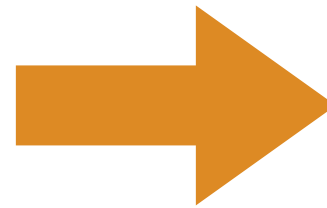
$$O(|\mathcal{Y}| |\mathcal{X}| \log |\mathcal{X}| \varepsilon^{-1}).$$

[Arimoto '72; Blahut '72]

Channel coding in information theory

More general 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)

Focus of my research

- **Non-convexity** and **multipartite entanglement** are the main problems/objects of study.
- Use mathematical/numerical tools, in particular **symmetries** and **optimization techniques**, to study channel coding tasks.

Example in this talk: Quantum capacity of a quantum channel

Talk outline

- Quantum information 101
- Quantum capacity of quantum channels
- Pauli channels, stabilizer states and graph states
- Decoherence properties of graph states
- Exploiting graph symmetries
- Results: repetition codes
- Conclusion

Talk outline

- Quantum information 101
- Quantum capacity of quantum channels
- Pauli channels, stabilizer states and graph states
- Decoherence properties of graph states
- Exploiting graph symmetries
- Results: repetition codes
- Conclusion

Quantum information terminology

$\mathcal{H}$ (finite-dim.) Hilbert space, $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ for quantum systems A, B .

Quantum states

A **quantum state** ρ is a linear operator on $\mathcal{H}$ with $\rho \geq 0$ and $\text{Tr}(\rho) = 1$. A state ψ is called **pure** if $\text{rank } \psi = 1$, then $\psi = |\psi\rangle\langle\psi|$ for a $|\psi\rangle \in \mathcal{H}$.

Quantum channels

A **quantum channel** $\mathcal{N}: A \rightarrow B$ is a linear, completely positive, trace-preserving map from $\mathcal{B}(\mathcal{H}_A)$ to $\mathcal{B}(\mathcal{H}_B)$.

Partial trace

The **partial trace** $\text{Tr}_B(\cdot)$ is the unique operation s.t. for a state ρ_{AB} on $\mathcal{H}_{AB}$ with $\rho_A = \text{Tr}_B \rho_{AB}$, $\text{Tr}(\rho_A X_A) = \text{Tr}(\rho_{AB}(X_A \otimes I_B))$ for all X_A .

Von Neumann entropy

The **von Neumann entropy** of a state ρ is defined as $S(\rho) = -\text{Tr}(\rho \log \rho)$.

$$S(\rho) = - \sum_{\lambda \in \text{spec}(\rho)} \lambda \log \lambda.$$

Entanglement

A **product state** is of the form $\rho_A \otimes \sigma_B \rightarrow$ no correlation between A and B .

The set $\text{SEP}(A : B) = \text{conv}\{\rho_A \otimes \sigma_B : \rho_A, \sigma_B \text{ states}\}$ of **separable states** consists of states with only **classical correlation**, e.g., $\omega_{AB} = \sum_i \lambda_i \rho_A^i \otimes \sigma_B^i$.

Entangled states

A $\psi_{AB} \notin \text{SEP}(A : B)$ is called **entangled**.

Multipartite entangled states

- GHZ state $\frac{1}{\sqrt{2}}(|0\rangle^{\otimes k} + |1\rangle^{\otimes k}) \in (\mathbb{C}^2)^{\otimes k}$
- Stabilizer states

Prototypical example

Let $\{|i\rangle\}_{i=0}^{d-1}$ be a basis for $\mathbb{C}^d$, then

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_A \otimes |i\rangle_B$$

is called a **maximally entangled state**.

$d = 2$: EPR pair $\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$

Talk outline

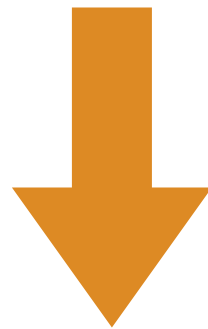
- Quantum information 101
- **Quantum capacity of quantum channels**
- Pauli channels, stabilizer states and graph states
- Decoherence properties of graph states
- Exploiting graph symmetries
- Results: repetition codes
- Conclusion

Quantum capacity of a quantum channel

Quantum channel models:

Information theory

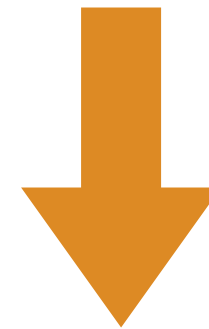
Noisy communication link
between quantum parties.



How much quantum information
can be sent through channel?

Error correction

Environmental noise in a
quantum device.



How much quantum information
can be protected against noise?

Quantum capacity characterizes:

Quantum capacity of a quantum channel

Quantum information transmission
is equivalent to **entanglement generation**.

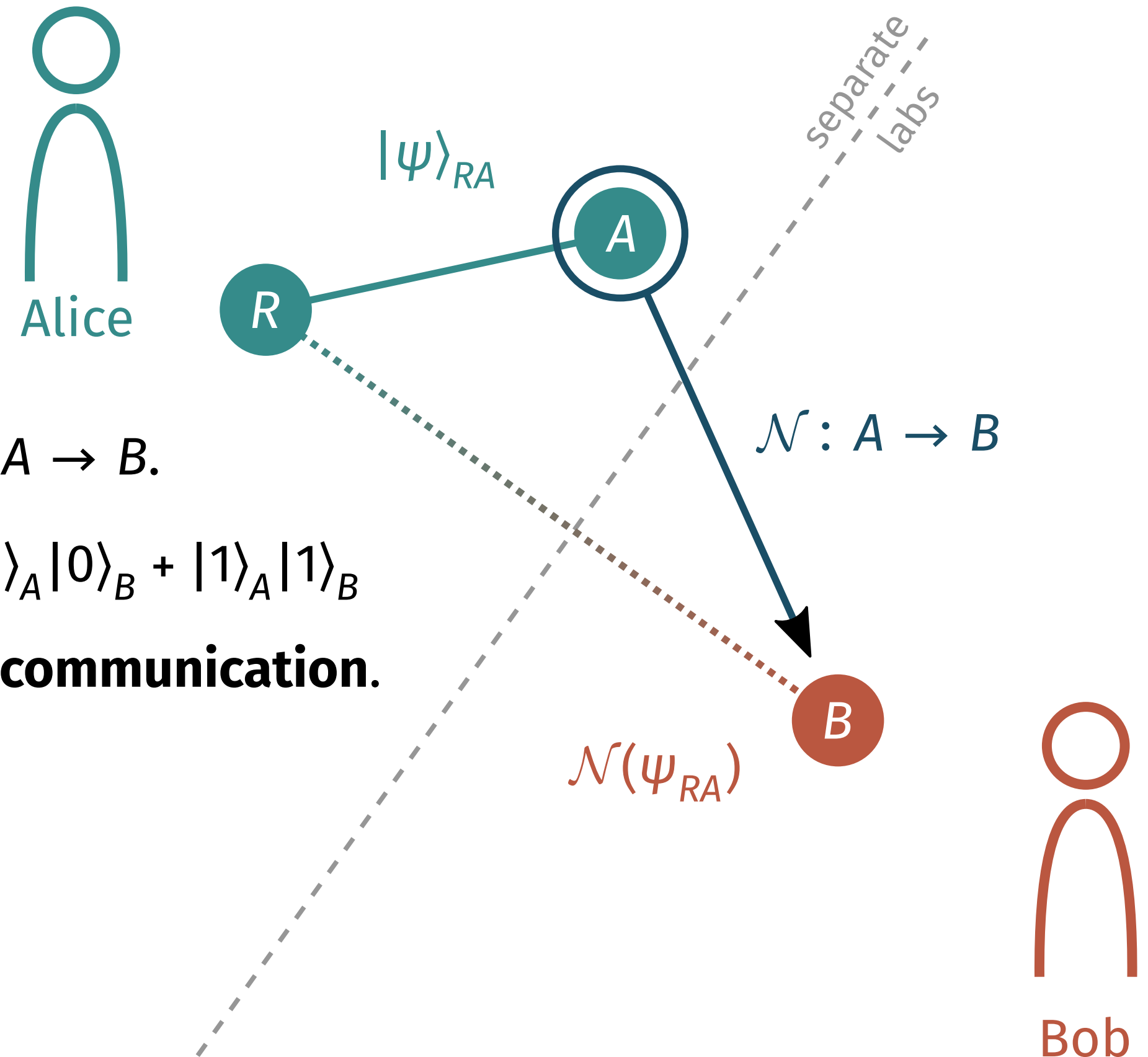
Protocol:

- Share k identical copies of pure bipartite state ψ_{RA} via quantum channel $\mathcal{N} : A \rightarrow B$.
- Convert $\mathcal{N}(\psi_{RA})^{\otimes k}$ into m “clean” EPR pairs $|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B$ using **local operations** and **forward classical communication**.

Achievable rate m/k :
coherent information

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

[Devetak '05; Devetak, Winter '05]



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 $[\mathcal{N}^{\otimes n}(\psi_{RA^n})]^{\otimes k}$:

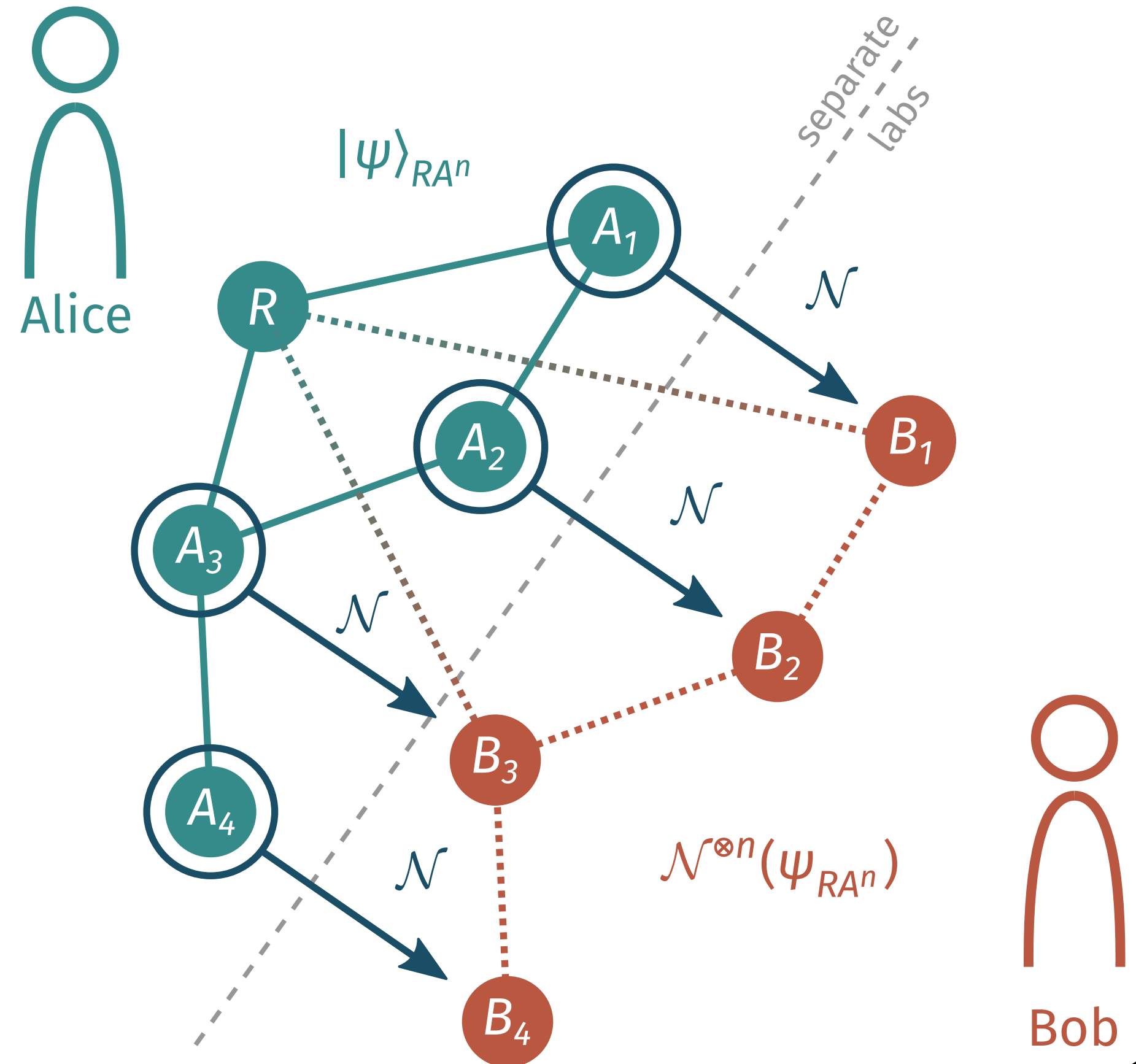
$$\frac{1}{n} \mathcal{I}_c(\psi_n, \mathcal{N}^{\otimes n})$$

Superadditivity of coherent information

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

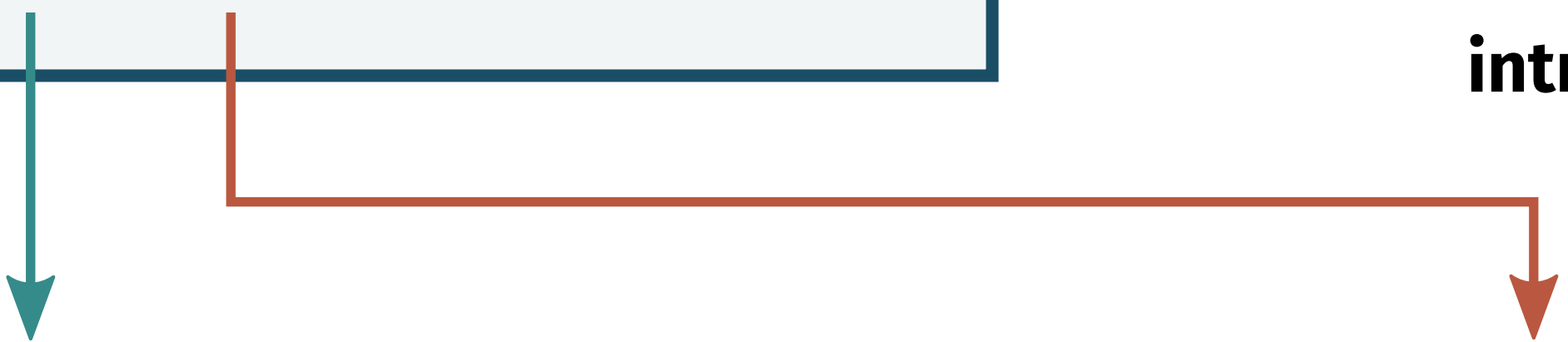
$$\frac{1}{n} \mathcal{I}_c(\psi_n, \mathcal{N}^{\otimes n}) > \max_{\phi} \mathcal{I}_c(\phi, \mathcal{N}).$$

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



Quantum capacity of a quantum channel

Quantum capacity of a quantum channel

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


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

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

Quantum capacity is given by **multi-letter formula** and in general **intractable** to compute.

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

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.

Mathematical ansatz for approximate solution

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

By the above theorem, this yields lower bounds on the true capacity.

Talk outline

- Quantum information 101
- Quantum capacity of quantum channels
- **Pauli channels, stabilizer states and graph states**
- Decoherence properties of graph states
- Exploiting graph symmetries
- Results: repetition codes
- Conclusion

Pauli channels and stabilizer states

Qubit-qubit Pauli channels

$$\mathcal{N}_{\mathbf{p}}(\rho) = p_0\rho + p_1X\rho X + p_2Y\rho Y + p_3Z\rho Z$$

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

→ $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ Pauli matrices.

Important examples:

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

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

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

define **threshold** as the largest x such that $Q(\mathcal{N}_{\mathbf{p}_x}) > 0$.

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: $\mathcal{N}_{\mathbf{p}}(\rho) = p_0\rho + p_1X\rho X + p_2Y\rho Y + p_3Z\rho Z$.

→ Tensored Pauli channel: $\mathcal{N}_{\mathbf{p}}^{\otimes n}(\rho_n) = \sum_{j^n} p_{j^n} E_{j^n} \rho_n E_{j^n}$,

where $E_{j^n} \in \mathcal{P}_n = \{I, X, Y, Z\}^{\otimes n}$, the n -**qubit Pauli group** (modulo phases).

→ Restrict to **stabilizer states** $|\psi_k\rangle$:

[Gottesman '97]

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

where $s_i \in \mathcal{P}_k$ are independent and pairwise commuting stabilizers.

Graph states

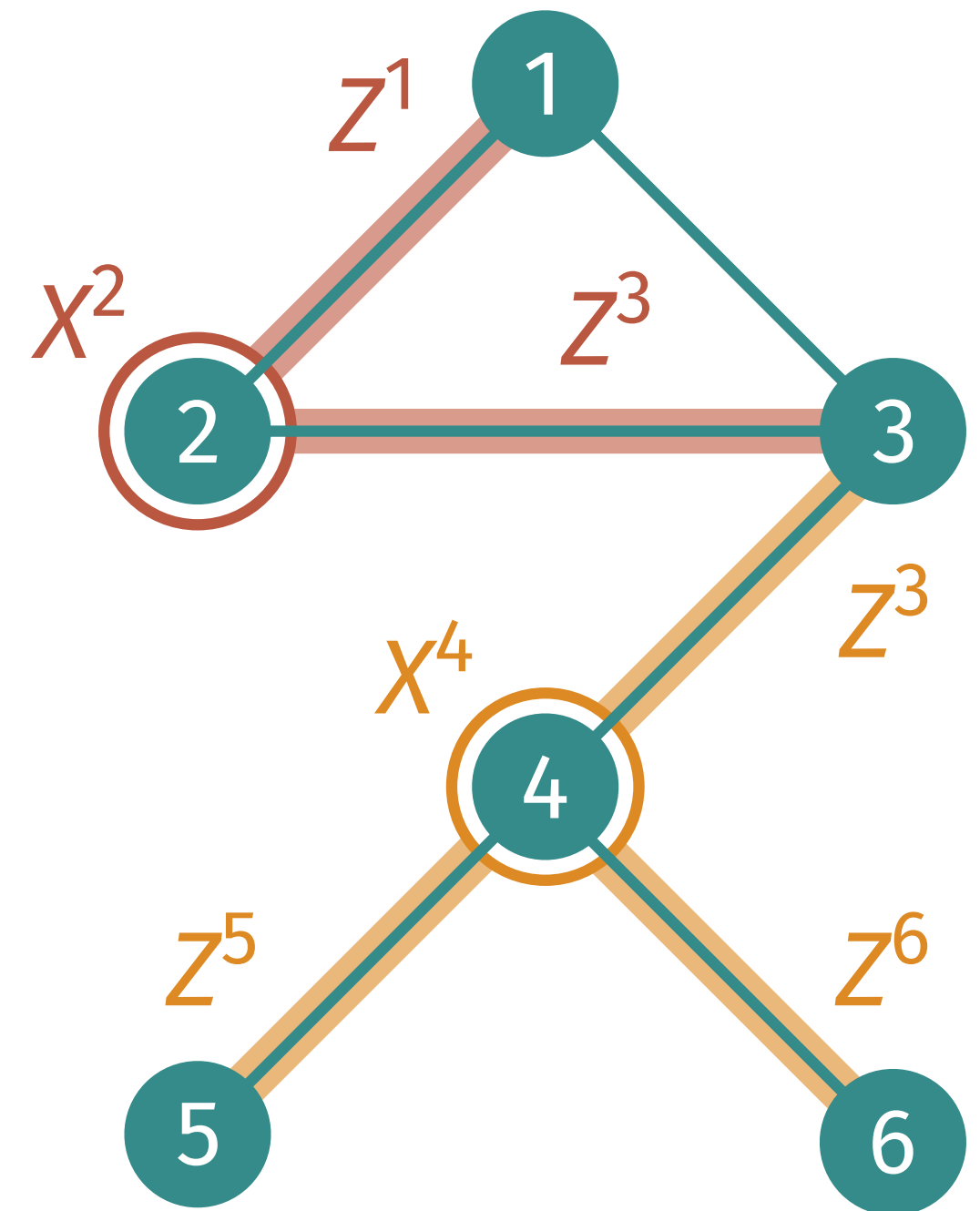
Let $\Gamma = (V, E)$ be a graph and $N_i = \{j \in V : (i, j) \in E\}$.

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 $s_1, \dots, s_k$.

$$s_2 = X^2 Z^1 Z^3$$

$$s_4 = X^4 Z^3 Z^5 Z^6$$



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. $U_1 \otimes \dots \otimes U_k |\psi_k\rangle = |\Gamma\rangle$.

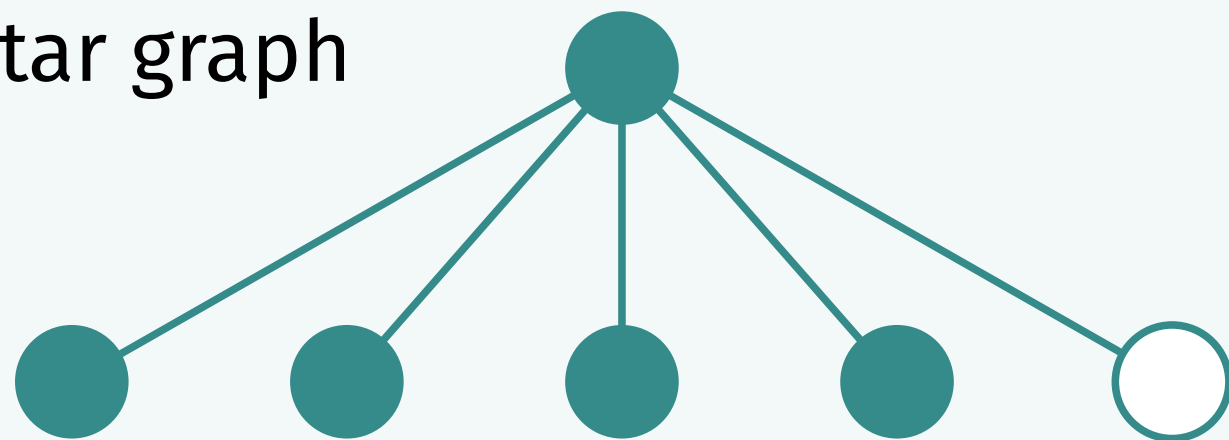
Important quantum codes as graph states:

● system qubits A_i ○ reference qubit R

Repetition code (GHZ state)

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

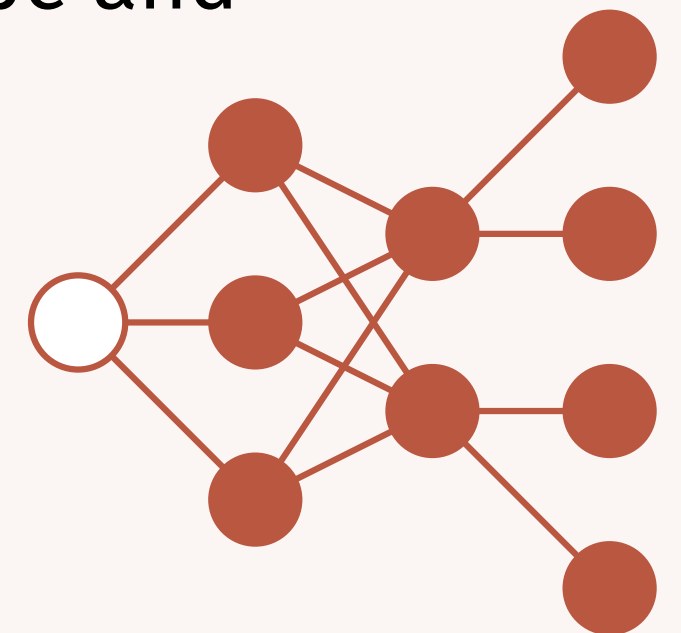
Star graph



Cat code (Shor code)

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

X-type rep: $|+\rangle^{\otimes n} + |-\rangle^{\otimes n}$,
where $|\pm\rangle \sim |0\rangle \pm |1\rangle$.



Talk outline

- Quantum information 101
- Quantum capacity of quantum channels
- Pauli channels, stabilizer states and graph states
- **Decoherence properties of graph states**
- Exploiting graph symmetries
- Results: repetition codes
- Conclusion

Decoherence of graph states

Goal

Compute the tensor action of a Pauli channel

$$\mathcal{N}_{\mathbf{p}}(\rho) = p_0\rho + p_1X\rho X + p_2Y\rho Y + p_3Z\rho Z$$

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

Observation

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

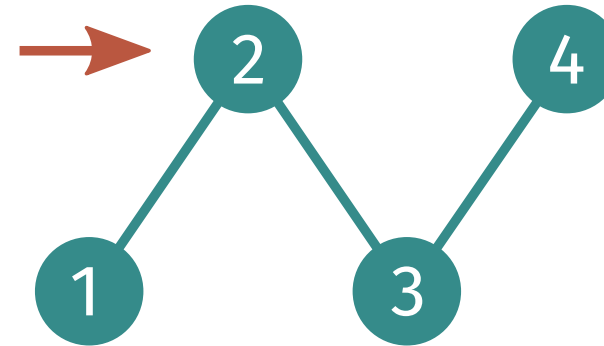
Quantum capacity: $Q(\mathcal{N}) = \sup_{n \in \mathbb{N}} \frac{1}{n} \max_{\psi_n} \mathcal{I}_c(\psi_n, \mathcal{N}^{\otimes n})$

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

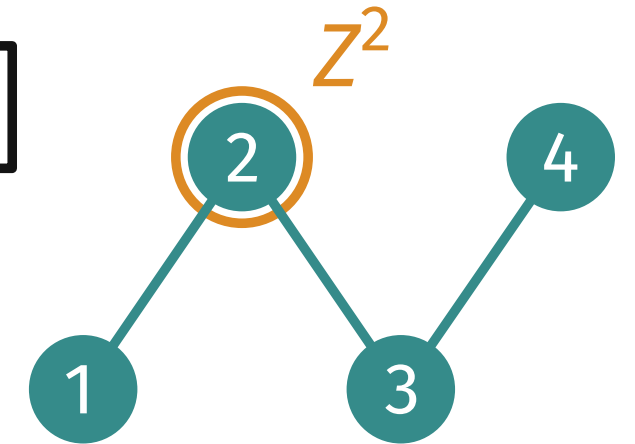
Von Neumann entropy: $S(\rho) = - \sum_{\lambda \in \text{spec}(\rho)} \lambda \log \lambda$

1

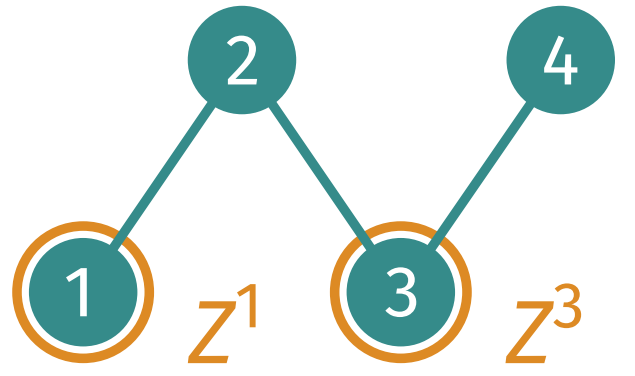
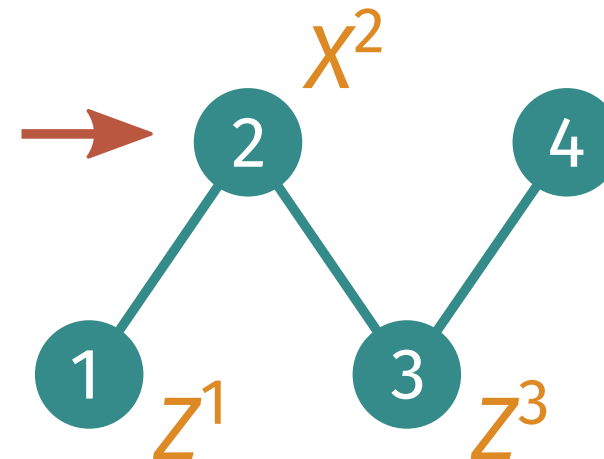
Z^2



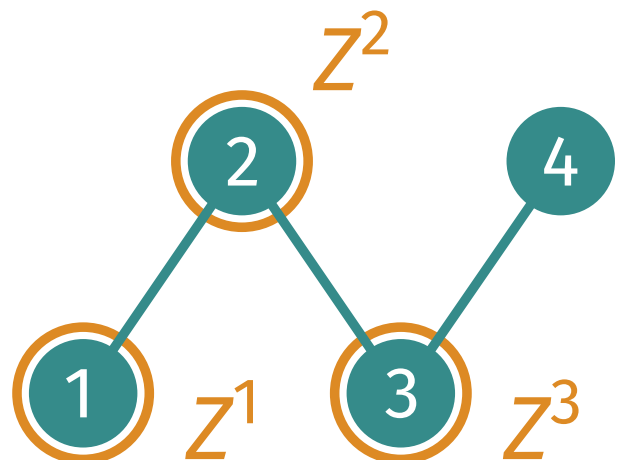
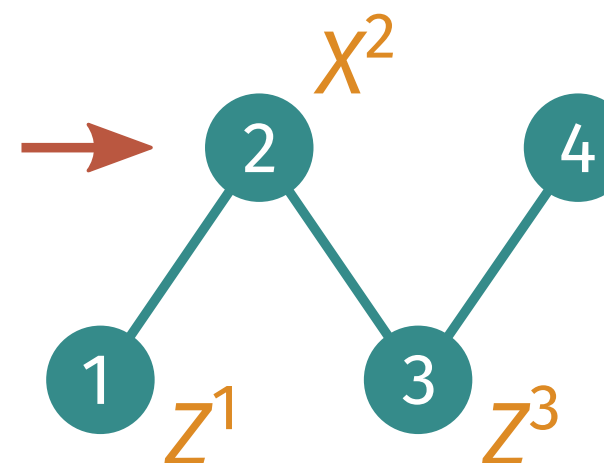
2



X^2



$Y^2 \propto Z^2 X^2$



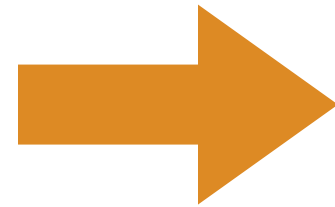
Decoherence of graph states

Decoherence of graph states:

$$Z^i |\Gamma\rangle\langle\Gamma| Z^i = Z^i |\Gamma\rangle\langle\Gamma| Z^i$$

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

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



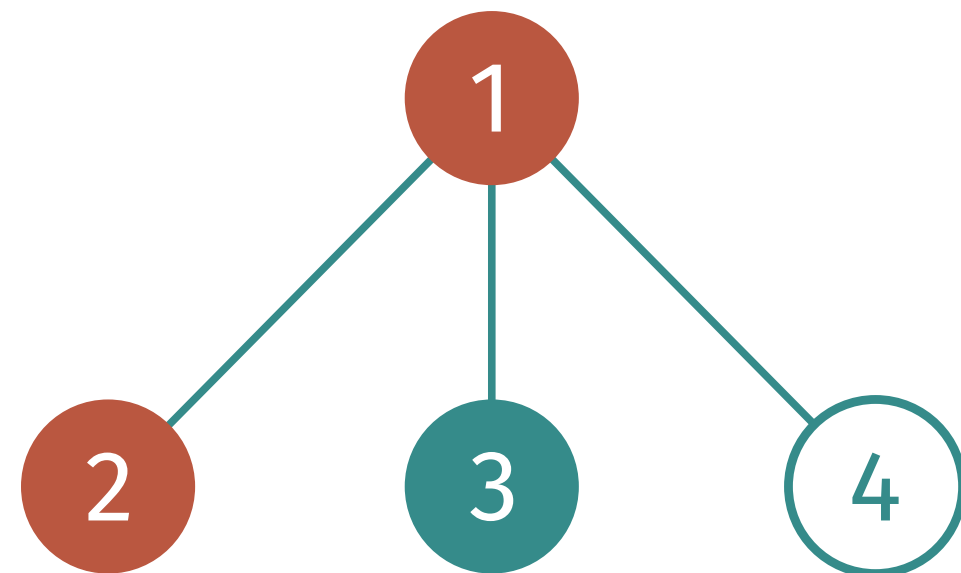
Graph states subjected to Pauli noise

$$\mathcal{N}^{\otimes n}(|\Gamma\rangle\langle\Gamma|) = \sum_{U \subset V} \lambda_U |U\rangle\langle U|, \quad [\text{Hein et al. '05}]$$

where the $|U\rangle = Z^U |\Gamma\rangle$ form a **basis** of $(\mathbb{C}^2)^{\otimes n}$.

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

Pauli error operators generating U :



$$\lambda_{\{1,2\}} = \begin{array}{c} Z^1 Z^2 \\ \downarrow \\ p_0^2 p_3^2 + \end{array} \begin{array}{c} Y^2 \\ \downarrow \\ p_0^3 p_2 + \end{array} \begin{array}{c} Z^2 X^3 \\ \downarrow \\ p_0^2 p_1 p_3 + \end{array} \begin{array}{c} Z^1 Y^2 X^3 \\ \downarrow \\ p_0 p_1 p_2 p_3 \end{array}$$

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

PROBLEM

Exponential scaling:

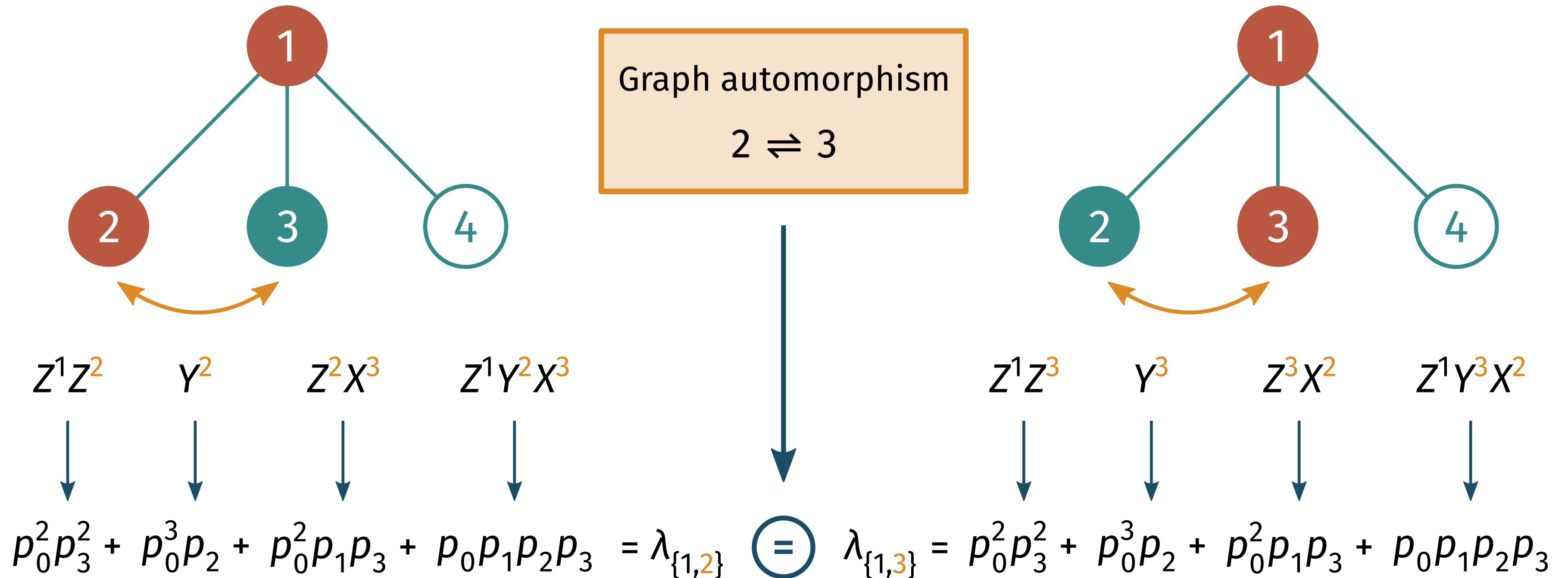
$$U \subset V, |V| = n$$

Talk outline

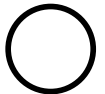
- Quantum information 101
- Quantum capacity of quantum channels
- Pauli channels, stabilizer states and graph states
- Decoherence properties of graph states
- **Exploiting graph symmetries**
- Results: repetition codes
- Conclusion

Exploiting graph symmetries

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



Exploiting graph symmetries

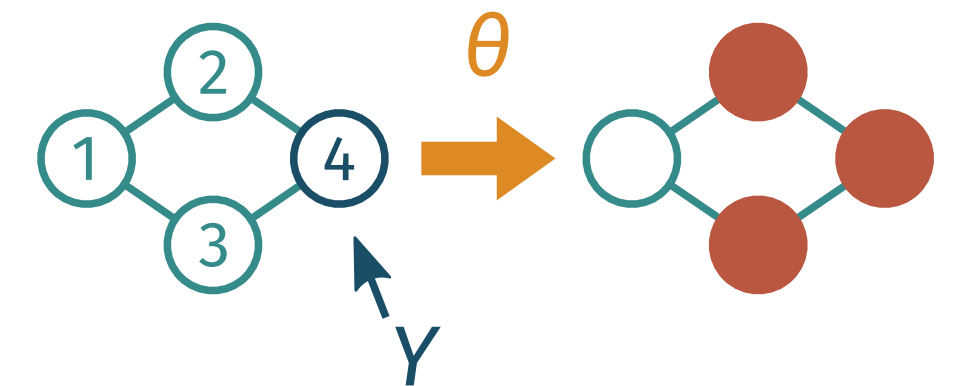
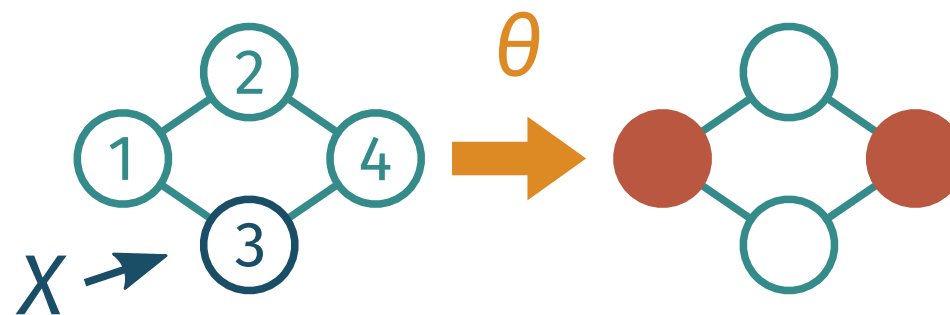
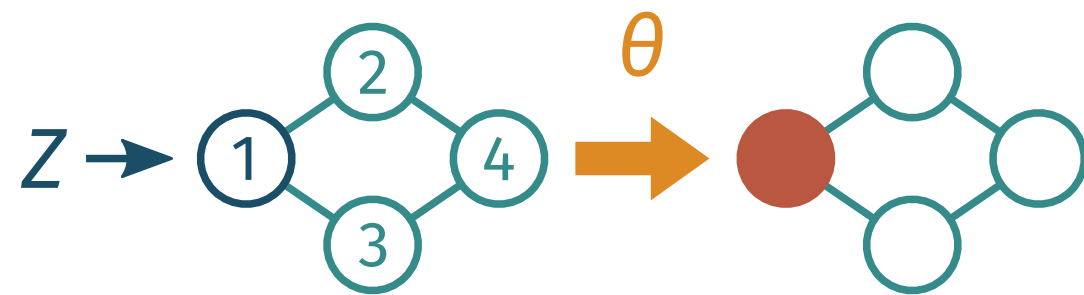
Let $G = \text{Aut}(\Gamma, |A|)$ be the **2-colored graph automorphism group** of the graph Γ .  system qubits  reference qubits

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

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

Identify subsets $U \subset V$
with **binary strings** $B = \{0, 1\}^n$.

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



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

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

$$\theta(3012) = 0110, \pi = (23)$$

$$\theta(\pi s) = \pi \theta(s) \text{ for all } s \in Q, \pi \in G$$

$$\theta(\pi(3012)) = \theta(3102) = 0110 = \pi(0110)$$

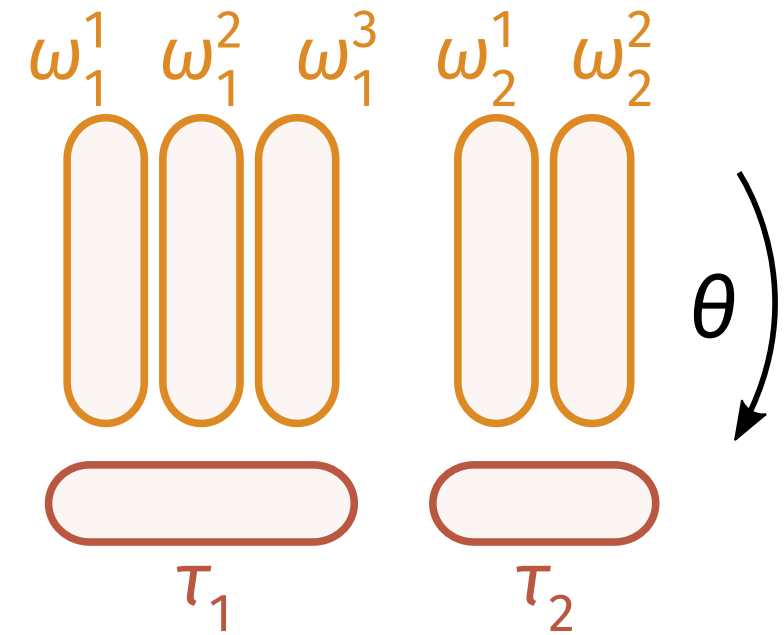
Exploiting graph symmetries

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

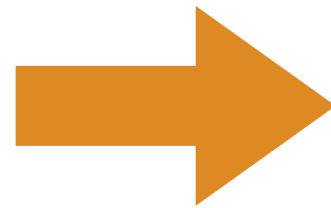
G -equivariant surjective map $\theta: Q \rightarrow B$ defined by decoherence rules.

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



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



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

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.

Orbit representatives

Group stabilizer chain

Define $G_i = \{\sigma \in G : \sigma(j) = j \text{ for } j \leq i\}$.

Then $\{\text{id}\} = G_n \leq G_{n-1} \leq \dots \leq G_1 \leq G_0 = G$

is called a *group stabilizer chain*.

Strong generating system

$T = \{T_1, \dots, T_n\}$, where T_i is a transversal of G_{i-1}/G_i .

Application to find orbit representatives

Use lexicographical order within orbits.

Given string $s \in [4]^n$, successively check in position i using T_i whether s is canonical.

Saves runtime by avoiding to test all group elements on each element!

[Borie '12]

Algorithm overview

1. Determine G -orbit representatives $\{\omega_i\}$ of $\{0, 1, 2, 3\}^n$.

2. For each orbit representative ω_i do:

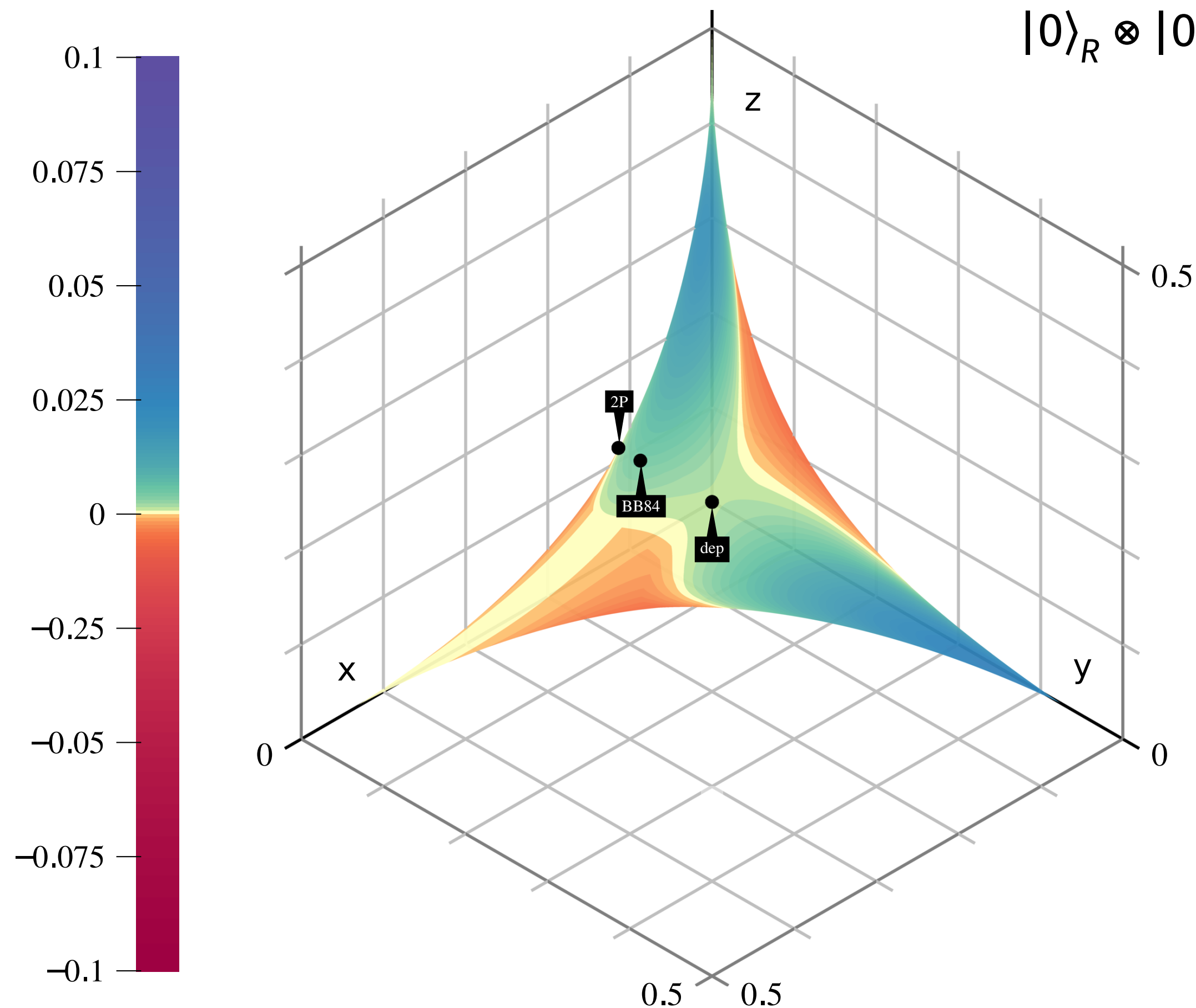
- (a) Compute weight contribution from ω_i .
- (b) Determine subset $V \supset U_i = \theta(\omega_i)$ onto which ω_i is mapped via θ .
- (c) Determine orbit representative τ_i of the orbit $\tau \ni U_i$.
- (d) Store coefficient λ_{τ_i} and its multiplicity in a hash table.

3. Compute partial trace of $\mathcal{N}^{\otimes n}(|\Gamma\rangle\langle\Gamma|)$ in a similar manner (not discussed in this talk).

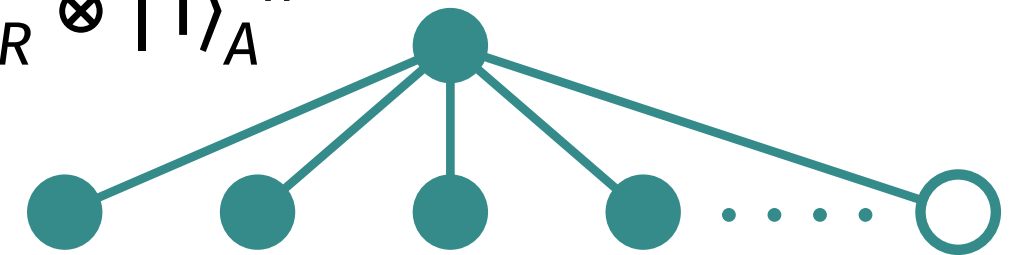
Talk outline

- Quantum information 101
- Quantum capacity of quantum channels
- Pauli channels, stabilizer states and graph states
- Decoherence properties of graph states
- Exploiting graph symmetries
- **Results: repetition codes**
- Conclusion

Repetition code thresholds



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



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

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

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

$$\mathbf{BB84}: ((1 - p)^2, p - p^2, p^2, p - p^2)$$

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

Talk outline

- Quantum information 101
- Quantum capacity of quantum channels
- Pauli channels, stabilizer states and graph states
- Decoherence properties of graph states
- Exploiting graph symmetries
- Results: repetition codes
- Conclusion

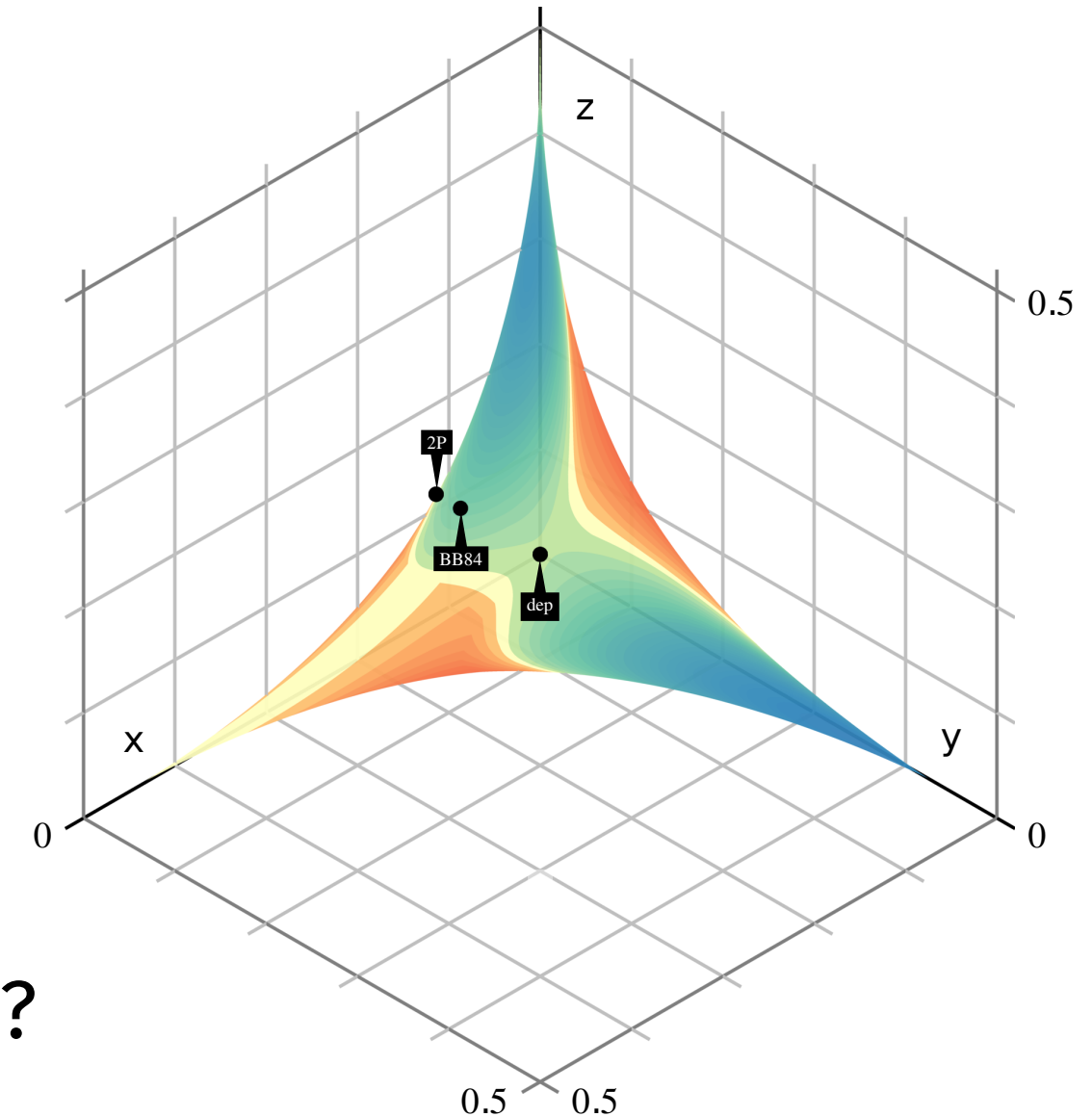
Symmetries in channel coding problems

Summary of arXiv:1910.00471

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?

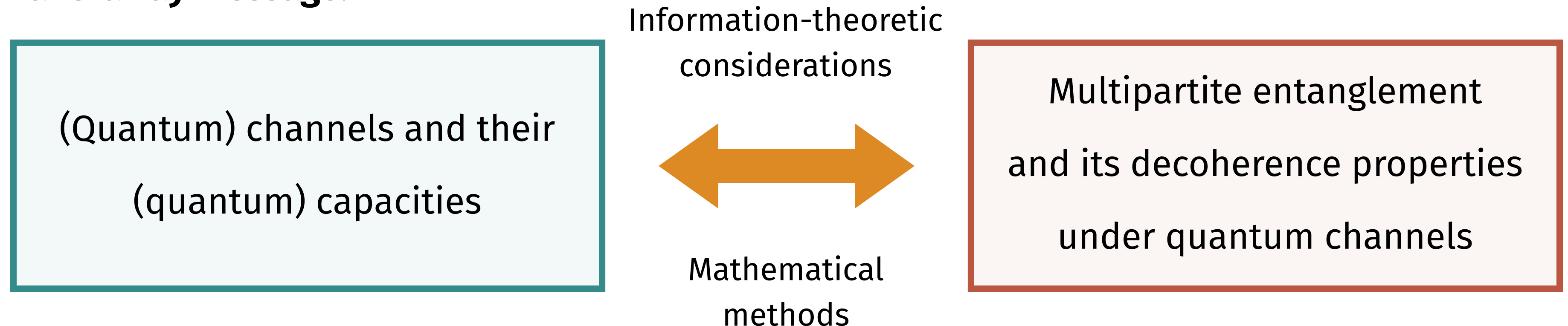


Conclusion

Channel capacities characterize **fundamental concepts** such as:

- Faithful communication using noisy resources
- Existence of error-correcting codes necessary for computations
- Secure key distribution

Take-away message:



THANKS

for your attention!