Purely quantum polar codes

Frédéric Dupuis *Université de Montréal*

Joint work with:

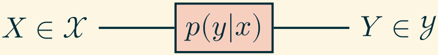
Ashutosh Goswami *Université Grenoble-Alpes*
Mehdi Mhalla *CNRS, Université Grenoble-Alpes*
Valentin Savin *CEA, Grenoble*

Outline

1. Introduction: error-correcting codes
2. Classical polar codes
3. Quantum error-correcting codes
4. Quantum polar codes

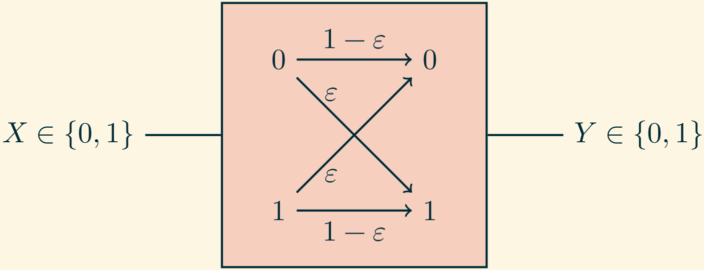
Error correcting codes

- We want to use noisy channels for sending messages with low probability of error.
- Noisy channel:



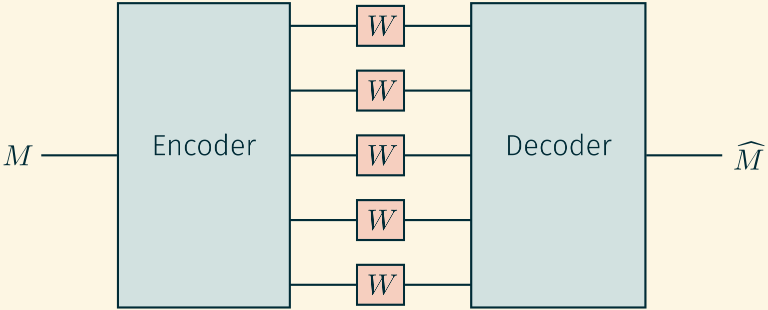
Channel capacity

Example: binary symmetric channel:



This channel flips its input with probability ε.

Error correcting codes



- Need a code such that $M = \widehat{M}$ with high probability.
- Capacity of W:

$$C(W) = \lim_{n\to\infty} \sup_{\text{encoder, decoder}} \left(\frac{1}{n} \log |M| \right).$$

Channel capacity

- Symmetric capacity of W:
  $C_S(W) = I(W) := H(X) - H(X|Y)$ for X uniform.
- Equal to the capacity for channels with symmetry in the input value, like the binary symmetric channel.

Error-correcting codes

What do we want from an error correcting code?

- Achieves capacity
- Efficiently encodable
- Efficiently decodable (ideally linear!)
- Efficiently constructible

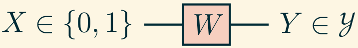
Provably fulfilling all of these was a long-standing open problem.

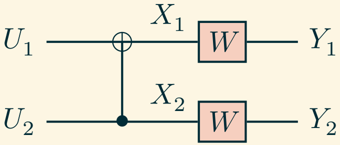
- Arıkan introduced polar codes in 2009, which fulfills all of the above.

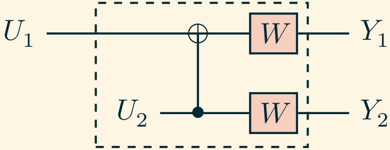
Classical polar codes: main idea

Main idea: channel polarization

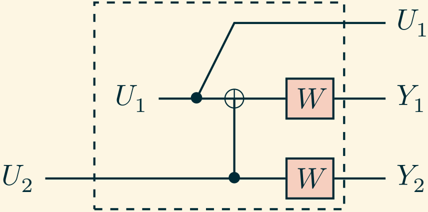
- Take n copies of a channel, turn them into n logical channels
- Each channel is either almost perfect or almost useless
- Proportion of almost-perfect channels $\rightarrow$ symmetric capacity





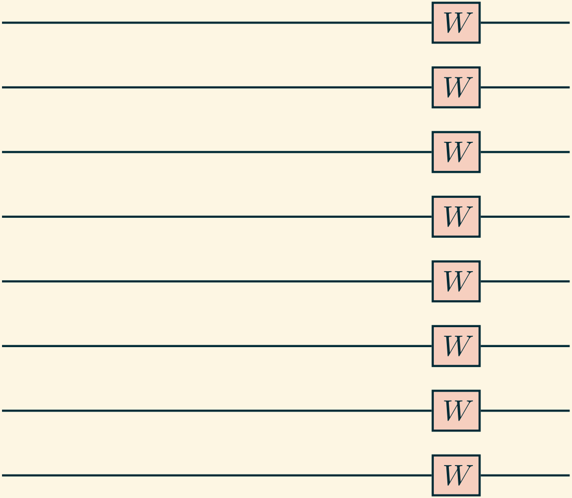


“Bad” channel

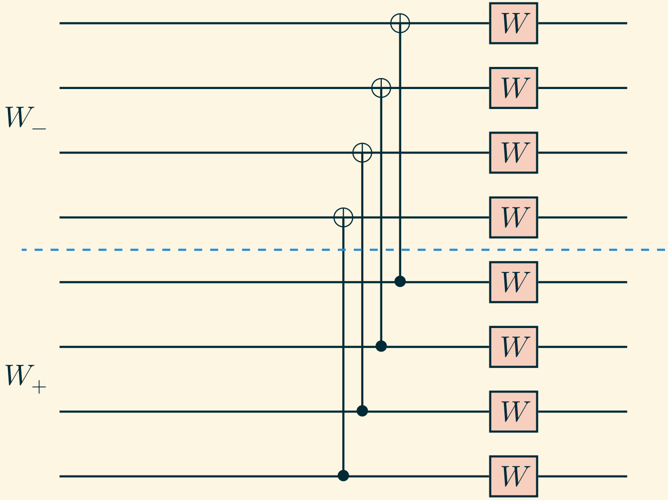


“Good” channel

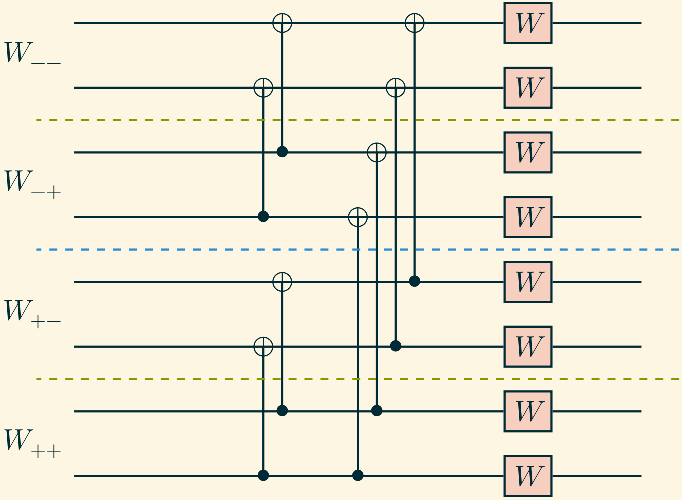
Polar encoder



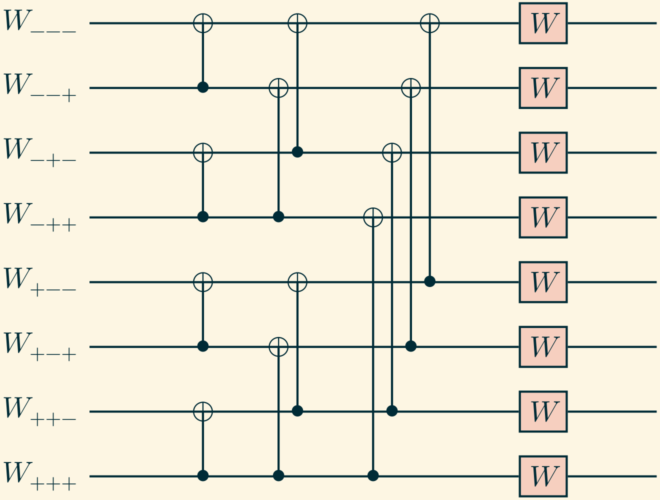
Polar encoder



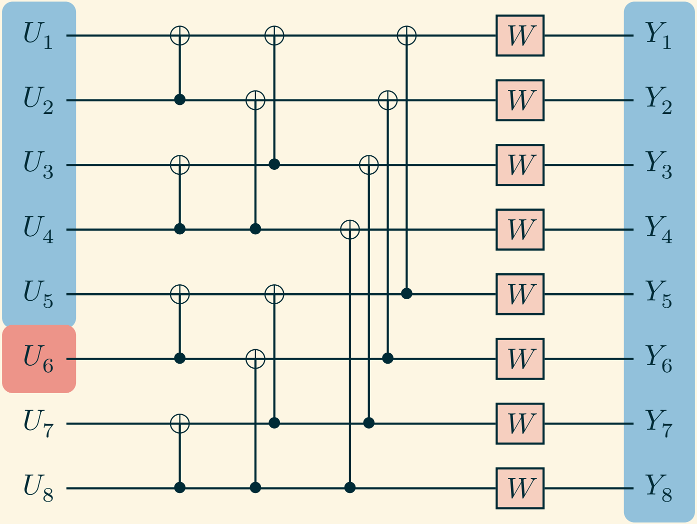
Polar encoder



Polar encoder



Channel polarization



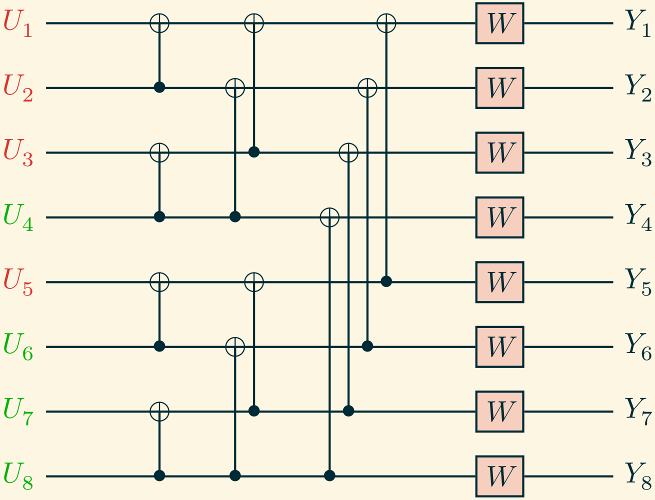
Channel polarization

The following can be shown:

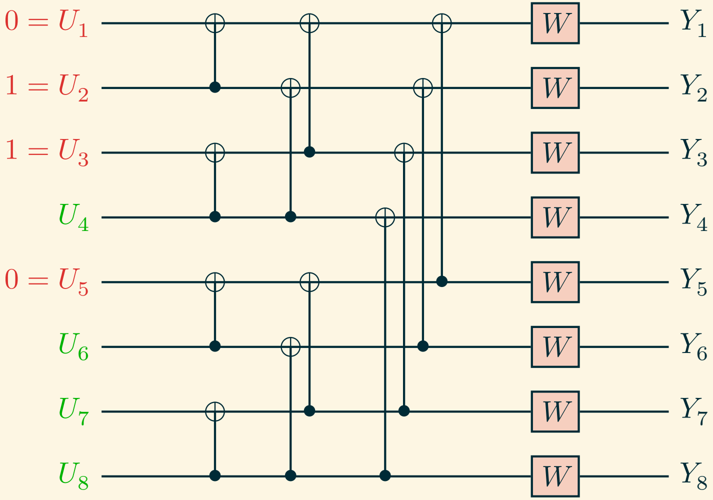
- If we add enough layers, each logical channel is either almost perfect or almost useless.
- The fraction of almost perfect channels is nearly $I(W)$.

Our coding strategy: send data through good channels, freeze bad channels to known values.

Coding strategy



Coding strategy



How to prove polarization?

How do we prove that the channels polarize?

- Select a logical channel at random, view it like the result of a random process consisting of choosing from { good, bad } n times.
- Use results about convergence of random processes.
- To make things simple, we'll assume that our channel has binary output.

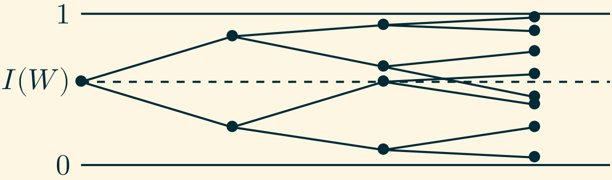
Proving polarization

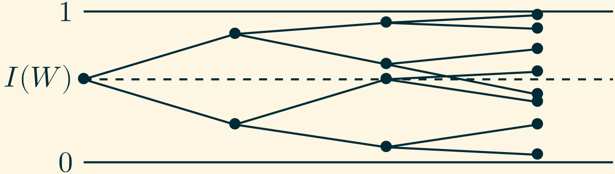
Definition (Stochastic process)

A stochastic process is a sequence of random variables $\{X_n : n \geq 0\}$.

We can define a stochastic process for our channels:

- $\{I_n : n \geq 0\}$, where I_n is the symmetric capacity of a randomly chosen logical channel after n layers of polar encoding.

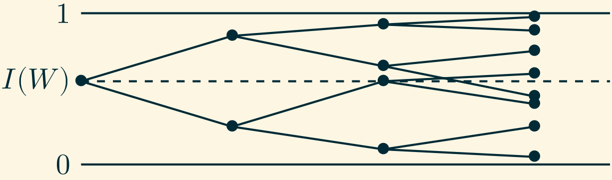




The goal: show that as $n \to \infty$:

$$I_n \to \begin{cases} 1 & \text{with probability } I(W) \\ 0 & \text{with probability } 1 - I(W) \end{cases}$$

Proving polarization



- General results about stochastic processes say that the process must converge to some distribution I_∞
- Properties of $I(W)$ say that $\mathbb{E}[I_\infty] = I(W)$.
- Tough part: show that all the probability of I_∞ is concentrated on $\{0, 1\}$.

Proving polarization

Proof idea: define a second stochastic process based on the *Bhattacharyya parameter*:

$$Z(W) = \sum_y \sqrt{W(y|0)W(y|1)}$$

- $Z(W)$: a sort of classical fidelity between the output of the channel if the input is 0 and if the input is 1.
- We have that

$$Z(W) = \begin{cases} 0 & \text{if } W \text{ is perfect} \\ 1 & \text{if } W \text{ is useless} \end{cases}$$

- Define second stochastic process Z_n.

Proving polarization

Key properties of Z:

- I_n is polarized iff Z_n is polarized.
- $Z(W_{\text{good}}) = Z(W)^2$.

Rough idea:

- Suppose I_∞ has some positive probability in the middle zone between 0 and 1.
- Then, for some big enough n, this probability will remain stable for the rest of the process.
- But the event that we get k good channels in a row happens infinitely often, which forces the middle channels to be good.
- $\Rightarrow$ contradiction

Decoding polar codes

To decode polar codes, we recursively compute the *likelihood ratio*:

$$L = \frac{\Pr[\text{input} = 0|\text{output}]}{\Pr[\text{input} = 1|\text{output}]}.$$

- Very big number $\rightarrow$ input very likely to be zero
- Very small number $\rightarrow$ input very likely to be one

Decoding polar codes

- Base case: if the channel is W, there is some expression for L that depends on W.
- Formulas for good and bad channel in terms of previous layer.
- Apply this recursively to get the L for the logical channels given the observed outputs. When we need the L for a frozen channel, substitute by $\{0, \infty\}$ depending on the frozen value.

Complexity of polar coding

What is the complexity of polar coding?

- Encoding: $O(n)$ per layer, $O(\log n)$ layers $\Rightarrow O(n \log n)$.
- Decoding: Also $O(n \log n)$: by reusing previously computed values in the recursive algorithm.
- Constructing:
  - How do we determine where the good channels are?
  - Efficient algorithm by Tal and Vardy (2013)

Quantum error-correcting codes

- We want to use noisy channels for sending qubits with low probability of error.
- Noisy quantum channel:

Here, $\mathcal{N}$ is a CPTP map from $\mathcal{H}_A$ to $\mathcal{H}_B$.

Example: depolarizing channel

$$\rho \;\longrightarrow\; \boxed{\mathcal{N}(\rho) = \begin{cases} \rho & \text{with prob } 1-\varepsilon \\ \frac{\mathrm{id}}{2} & \text{with prob } \varepsilon \end{cases}} \;\longrightarrow\; \mathcal{N}(\rho)$$

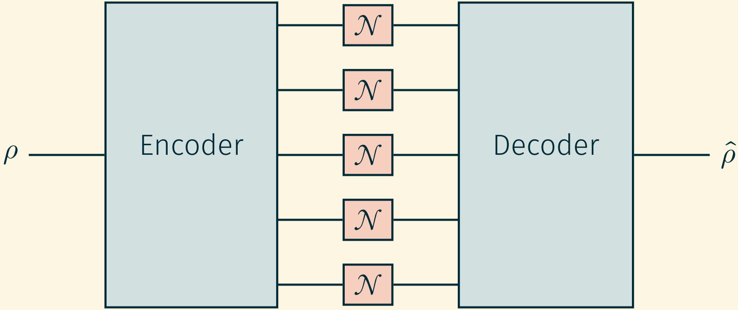
This channel replaces its input with noise with probability ε, like the depolarizing channel.

Pauli channels

An important class of channels: Pauli channels

$$\rho \longrightarrow \boxed{\mathcal{N}(\rho) = \begin{cases} \rho & \text{with prob } p_I \\ X\rho X & \text{with prob } p_X \\ Y\rho Y & \text{with prob } p_Y \\ Z\rho Z & \text{with prob } p_Z \end{cases}} \longrightarrow \mathcal{N}(\rho)$$

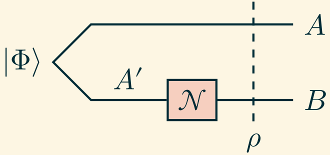
Quantum error-correcting codes



- Need a code such that $F(\rho, \hat{\rho})$ for all ρ.
- Capacity of $\mathcal{N}$:

$$Q(\mathcal{N}) = \lim_{n\to\infty} \sup_{\text{encoder, decoder}} \left(\frac{1}{n} \log \dim \mathcal{H}_{\text{in}} \right).$$

Quantum symmetric coherent information

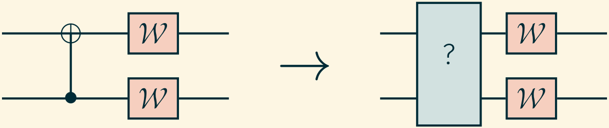


- Symmetric coherent information of $\mathcal{N}$: $Q_S(\mathcal{N}) = I(\mathcal{N}) := -H(A|B)_\rho \in [-1, 1]$.
- *Not* necessarily equal to the capacity even for symmetric channels: we could entangle the inputs between channel uses.

Quantum polar codes?

Can we make polar codes for sending qubits?

- Can we still use the basic transform using CNOTs?
- Do we need a new transformation?

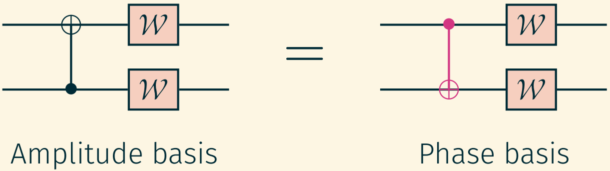


Quantum polar codes using CNOTs

- (Wilde, Guha 2011): Polar codes work as-is for classical-quantum channels
    - ...but we don't know how to decode them.
- (Wilde, Guha 2011 (second paper)): Can use correspondance between coding for wiretap channels and quantum coding to construct quantum polar codes.
    - ...but we don't know how to decode them.

Quantum polar codes using CNOTs

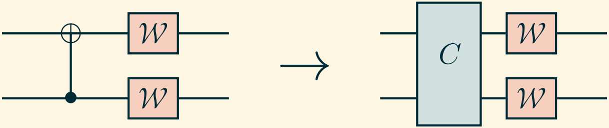
Approach in [Renes, Dupuis, Renner 2011]: use CNOTs, analyze amplitude and phase basis separately.



- So a polar code in the amplitude basis is a polar code in the phase basis with good and bad channels inverted.
- We can use the classical decoder coherently twice when the channel is a Pauli channel.

Purely quantum polar codes

This talk: we investigate the option of replacing the CNOTs:

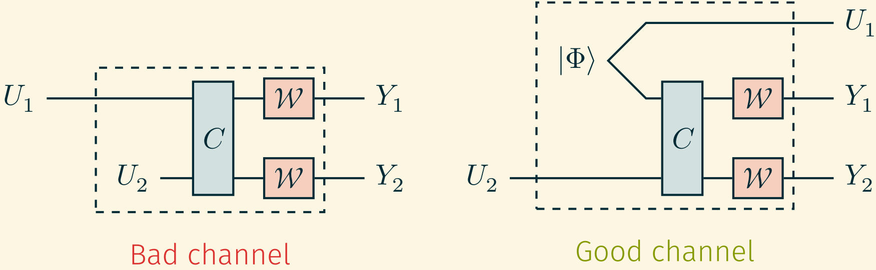


where all the C's in the encoding circuit are chosen independently at random from the two-qubit Clifford group (subgroup of the unitaries generated by $\{\mathrm{CNOT}, H, \sqrt{Z}\}$).

- Cliffords maps Paulis to Paulis by conjugation: if P is Pauli then, $CPC^{\dagger}$ is Pauli.

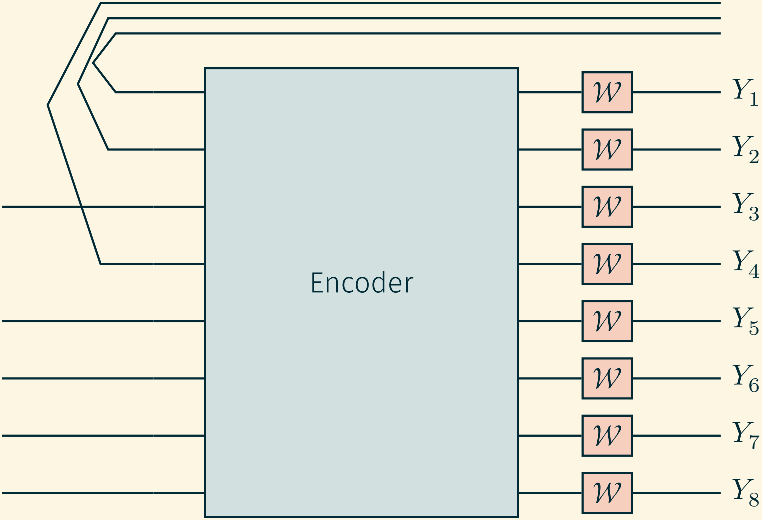
Purely quantum polar codes

The good and bad channels now look like this:



where we choose all the C's in the encoding circuit independently at random from the two-qubit Clifford group.

Coding strategy



(# of good channels) − (# of bad channels) $\approx nI(\mathcal{W})$

Proving polarization

How do we prove that this construction polarizes? Two stochastic processes:

- $I_n = \mathbb{E}_C I(\mathcal{W}_{\text{logical}})$: Symmetric coherent information of the channel
- Z_n: we need a quantum version of the Bhattacharyya parameter. Key properties required:
  - Polarizes iff I_n polarizes
  - Guarantees that if $\mathcal{W}$ is neither very good or very bad, and we look at the k-fold good channel produced from $\mathcal{W}$, we get Z nearly perfect.

Proving polarization

Solution: use the Rényi $\frac{1}{2}$ entropy:

$$Z(\mathcal{N}) = \mathbb{E}_C 2^{H^{\uparrow}_{\frac{1}{2}}(A|B)_{\mathcal{N}(\Phi_{AA'})}}$$

and we can prove the two properties needed.

Stronger results for Pauli channels

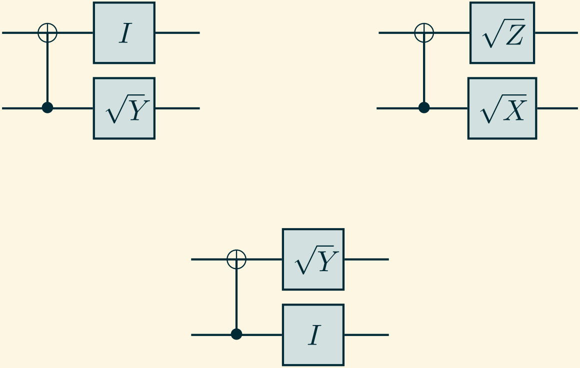
If $\mathcal{W}(\rho) = p_0\sigma_0\rho\sigma_0^\dagger + p_1\sigma_1\rho\sigma_1^\dagger + p_2\sigma_2\rho\sigma_2^\dagger + p_3\sigma_3\rho\sigma_3^\dagger$ is a Pauli channel, we can define the classical channel:

$$X \in \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\} \longrightarrow \boxed{\mathcal{W}^\#} \longrightarrow Y \in \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$$

- Transition prob: $\mathcal{W}^\#(\sigma_j|\sigma_i) = p_k, \sigma_k = \sigma_i\sigma_j \;\{\pm 1, \pm \iota\}$
- Mutual information: $I(\mathcal{W}^\#) = \frac{1+I(\mathcal{W})}{2}$.
- Can show polarization directly for these channels

Polarization with 3 Cliffords

For Pauli channels, we can choose the Cliffords from a set of 3 gates:



Decoding for Pauli channels

- **Efficient decoding:** For the Pauli construction, we can run a version of the classical decoder to deduce the Pauli operation applied by the channel and correct.

Open problems

Some open problems related to this construction:

- Get rid of entanglement assistance
- Efficient decoding for general channels
- Algorithm for constructing the codes (Tal-Vardy?)
- Polar codes for fault tolerant quantum computation?

Thanks!