Numerical estimate of the threshold for quantum expander codes

Antoine Grospellier (INRIA Paris)
&
Anirudh Krishna (Université de Sherbrooke)

October 11, 2018

Content of the talk

Outline

Alice

Bob

$|\varphi\rangle \in \mathbb{C}^{2^k}$
$|\varphi\rangle$: k qubits state

Alice

Bob

- Bit: $b \in \mathbb{F}_2$
- k-bit message: $m \in \mathbb{F}_2^k$

- Qubit: $|b\rangle \in \mathbb{C}^2$, $\| |b\rangle \|_2 = 1$
- k-qubits quantum state: $|\varphi\rangle \in \mathbb{C}^{2^k}$, $\| |\varphi\rangle \|_2 = 1$

$|\varphi\rangle \in \mathbb{C}^{2^k}$
$|\varphi\rangle$: k qubits state

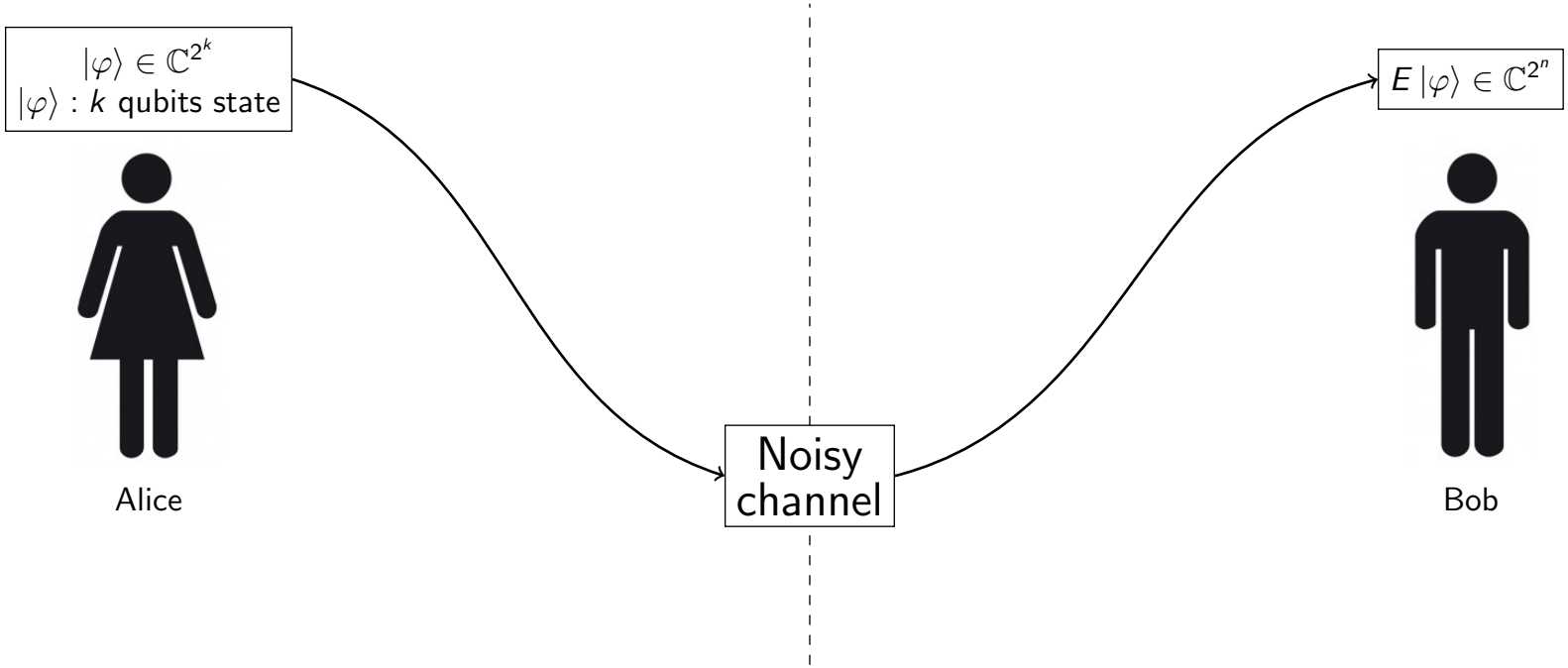
Alice

Noisy channel

Bob

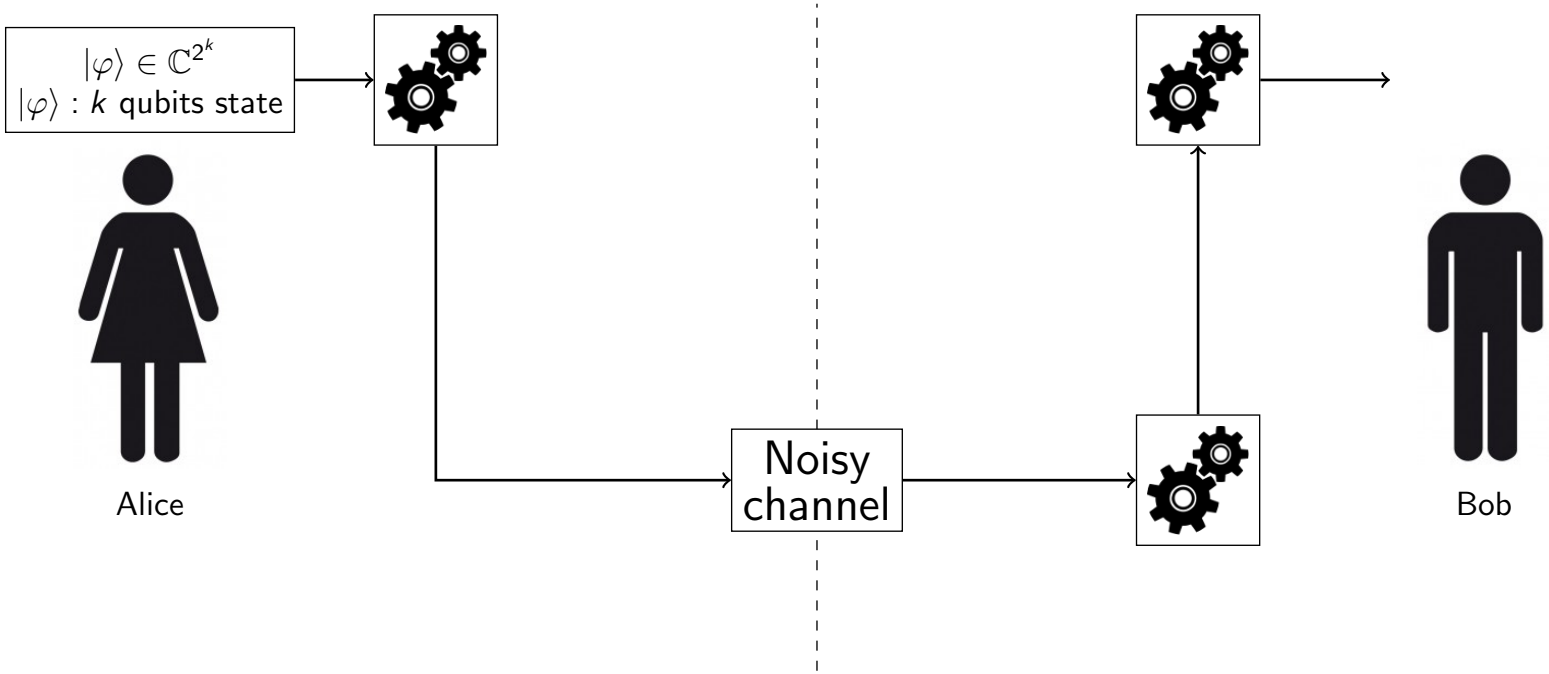
- Bit: $b \in \mathbb{F}_2$
- k-bit message: $m \in \mathbb{F}_2^k$

- Qubit: $|b\rangle \in \mathbb{C}^2$, $\| |b\rangle \|_2 = 1$
- k-qubits quantum state: $|\varphi\rangle \in \mathbb{C}^{2^k}$, $\| |\varphi\rangle \|_2 = 1$



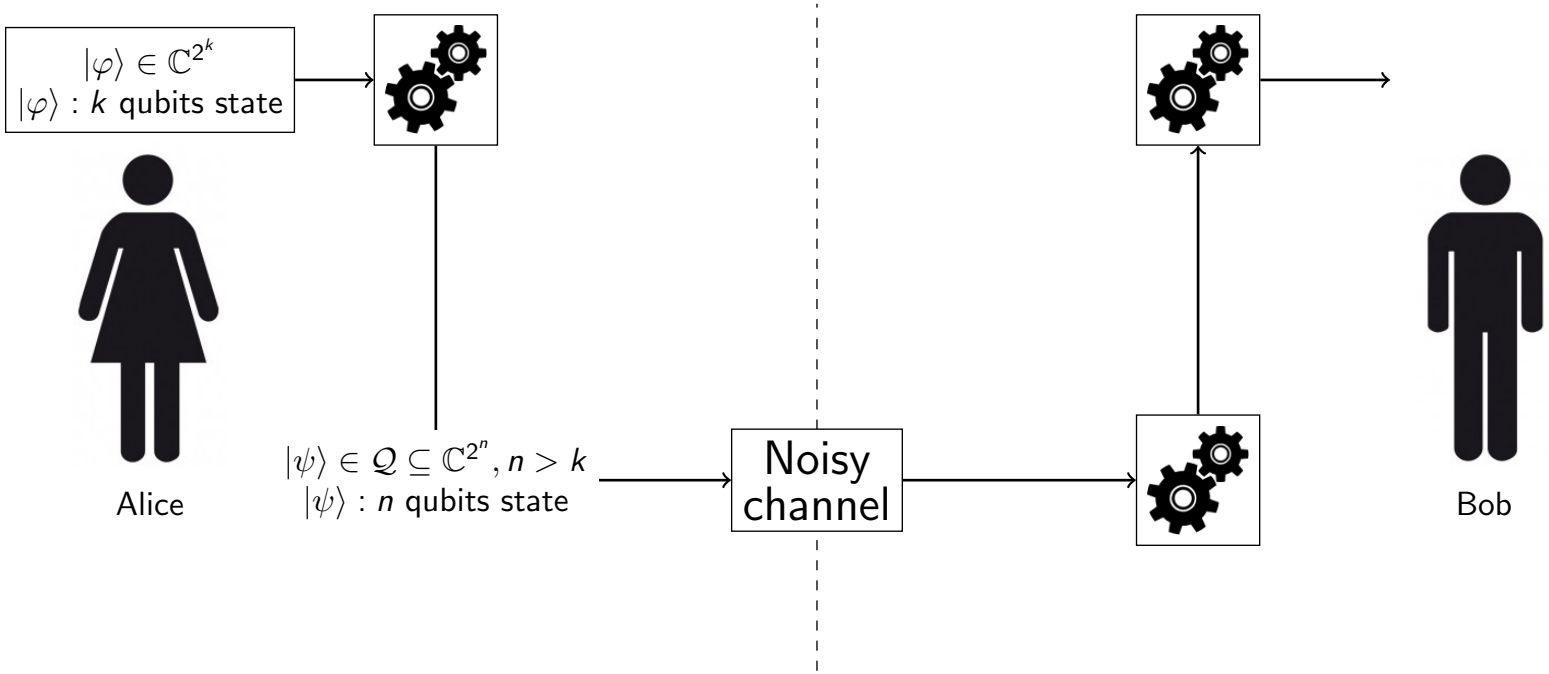
- Bit: $b \in \mathbb{F}_2$
- k-bit message: $m \in \mathbb{F}_2^k$

- Qubit: $|b\rangle \in \mathbb{C}^2$, $\| |b\rangle \|_2 = 1$
- k-qubits quantum state: $|\varphi\rangle \in \mathbb{C}^{2^k}$, $\| |\varphi\rangle \|_2 = 1$



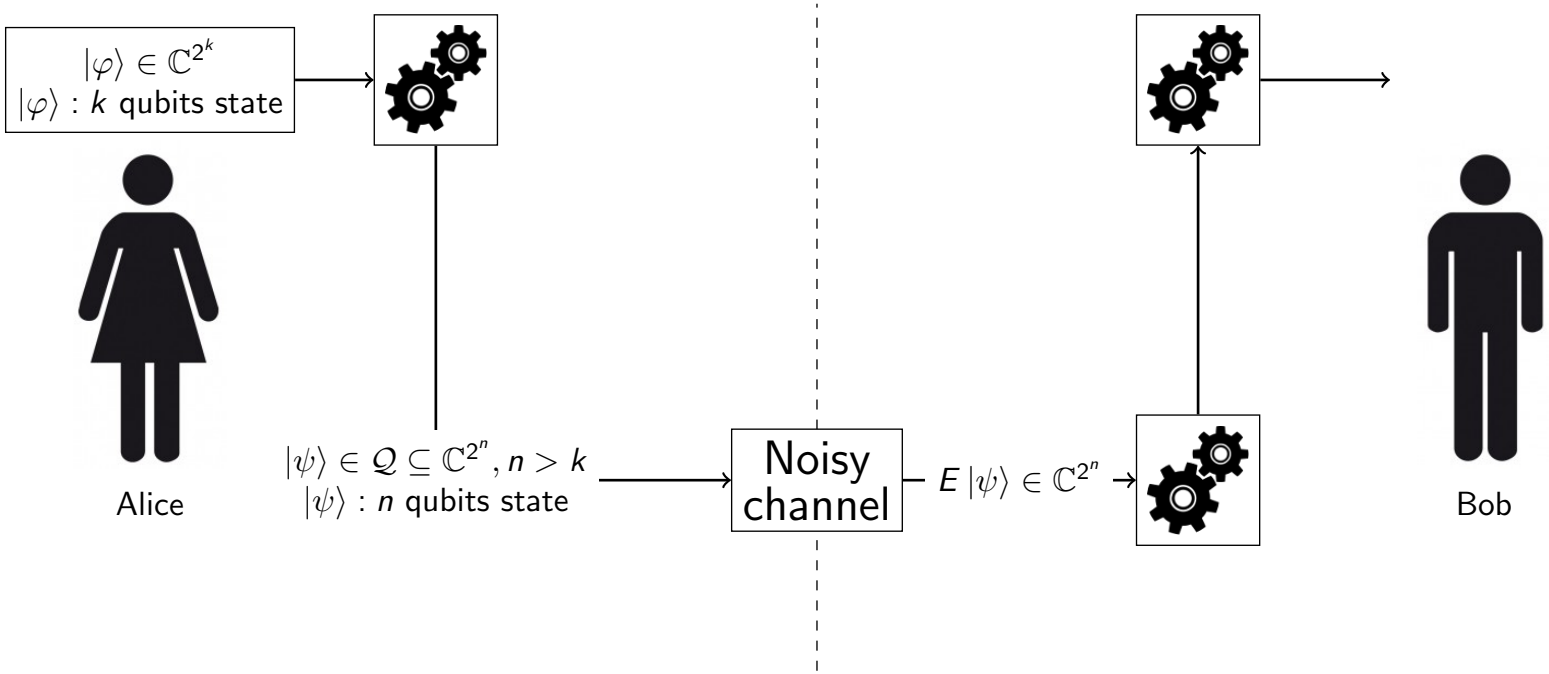
- Bit: $b \in \mathbb{F}_2$
- k-bit message: $m \in \mathbb{F}_2^k$

- Qubit: $|b\rangle \in \mathbb{C}^2$, $\| |b\rangle \|_2 = 1$
- k-qubits quantum state: $|\varphi\rangle \in \mathbb{C}^{2^k}$, $\| |\varphi\rangle \|_2 = 1$



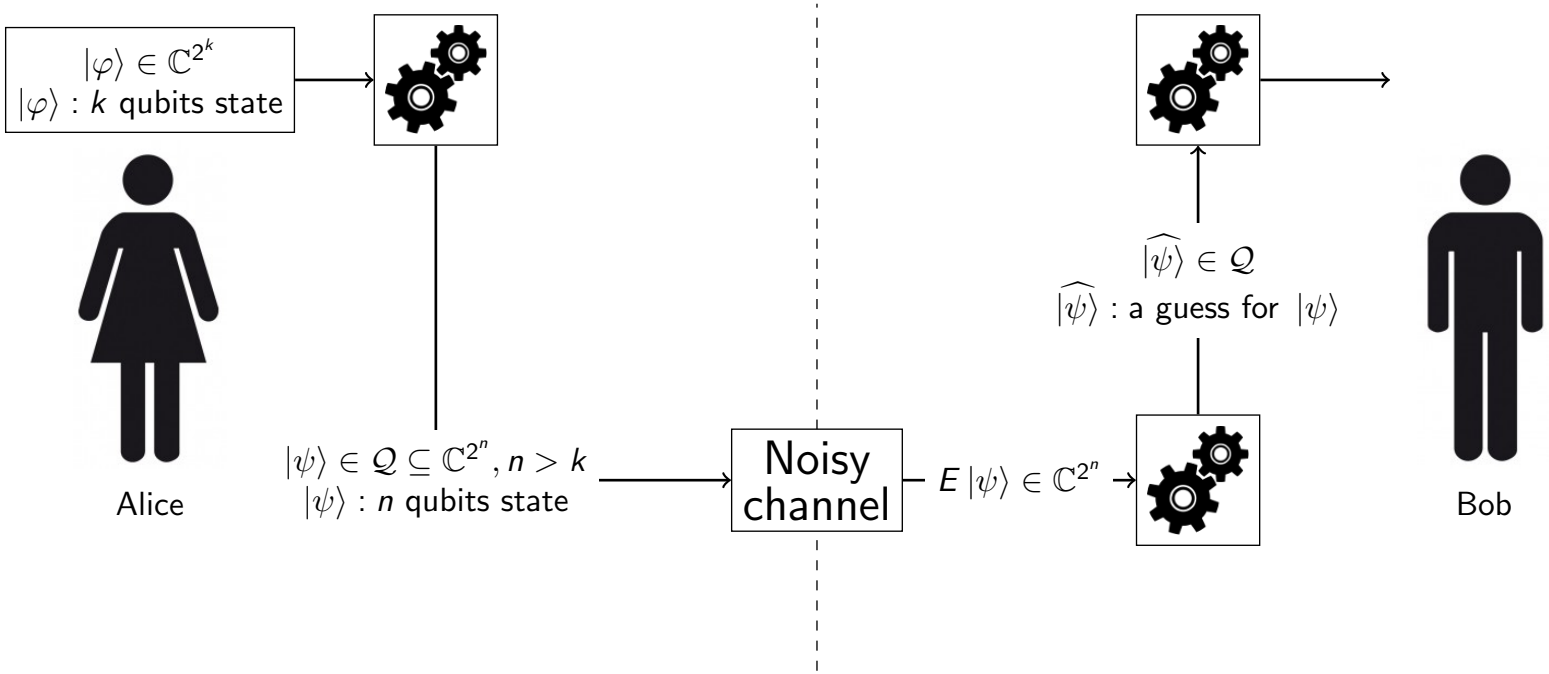
- Bit: $b \in \mathbb{F}_2$
- k-bit message: $m \in \mathbb{F}_2^k$
- A $[n, k]$-code is a k-dimensional subspace of $\mathbb{F}_2^n$

- Qubit: $|b\rangle \in \mathbb{C}^2$, $\| |b\rangle \|_2 = 1$
- k-qubits quantum state: $|\varphi\rangle \in \mathbb{C}^{2^k}$, $\| |\varphi\rangle \|_2 = 1$
- A $[\![n, k]\!]$-code is a 2^k-dimensional subspace of $\mathbb{C}^{2^n}$



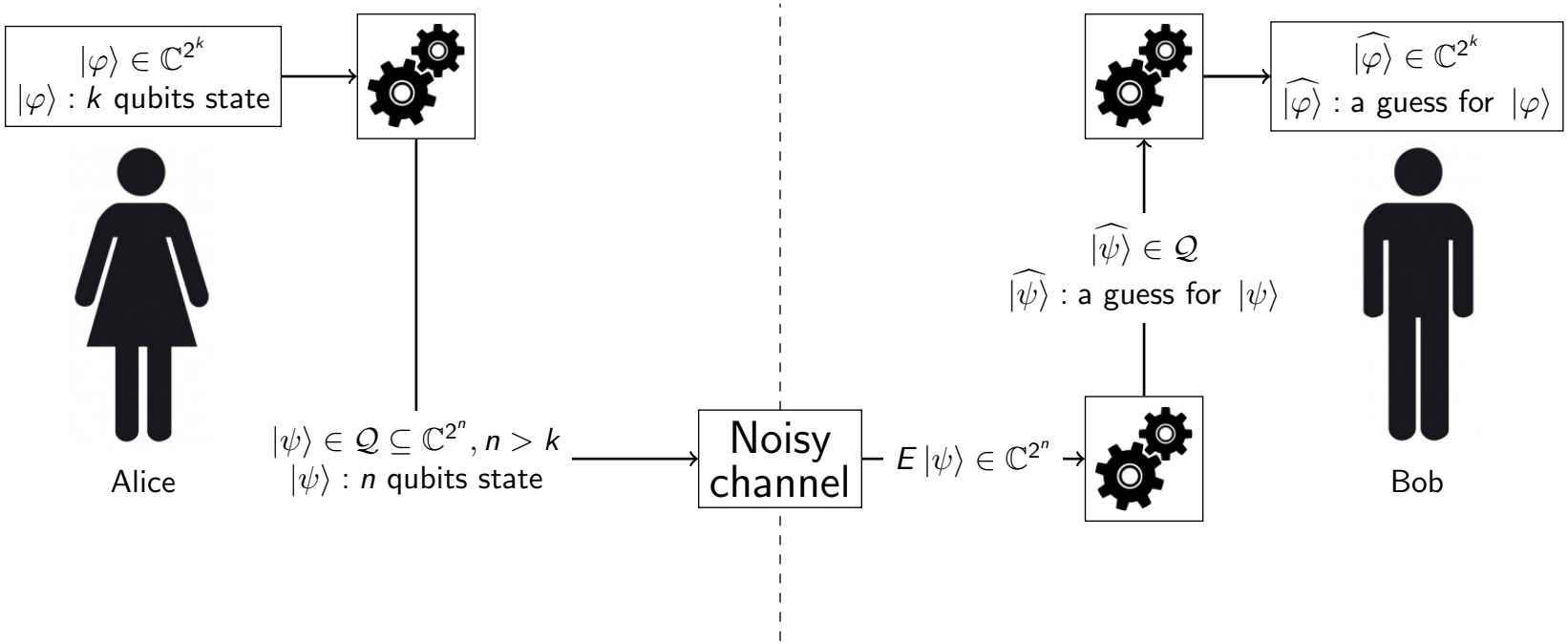
- Bit: $b \in \mathbb{F}_2$
- k-bit message: $m \in \mathbb{F}_2^k$
- A $[n, k]$-code is a k-dimensional subspace of $\mathbb{F}_2^n$
- Classical error: Flip

- Qubit: $|b\rangle \in \mathbb{C}^2$, $\| |b\rangle \|_2 = 1$
- k-qubits quantum state: $|\varphi\rangle \in \mathbb{C}^{2^k}$, $\| |\varphi\rangle \|_2 = 1$
- A $[\![n, k]\!]$-code is a 2^k-dimensional subspace of $\mathbb{C}^{2^n}$
- Quantum errors: $E \in \mathcal{U}(2^n)$



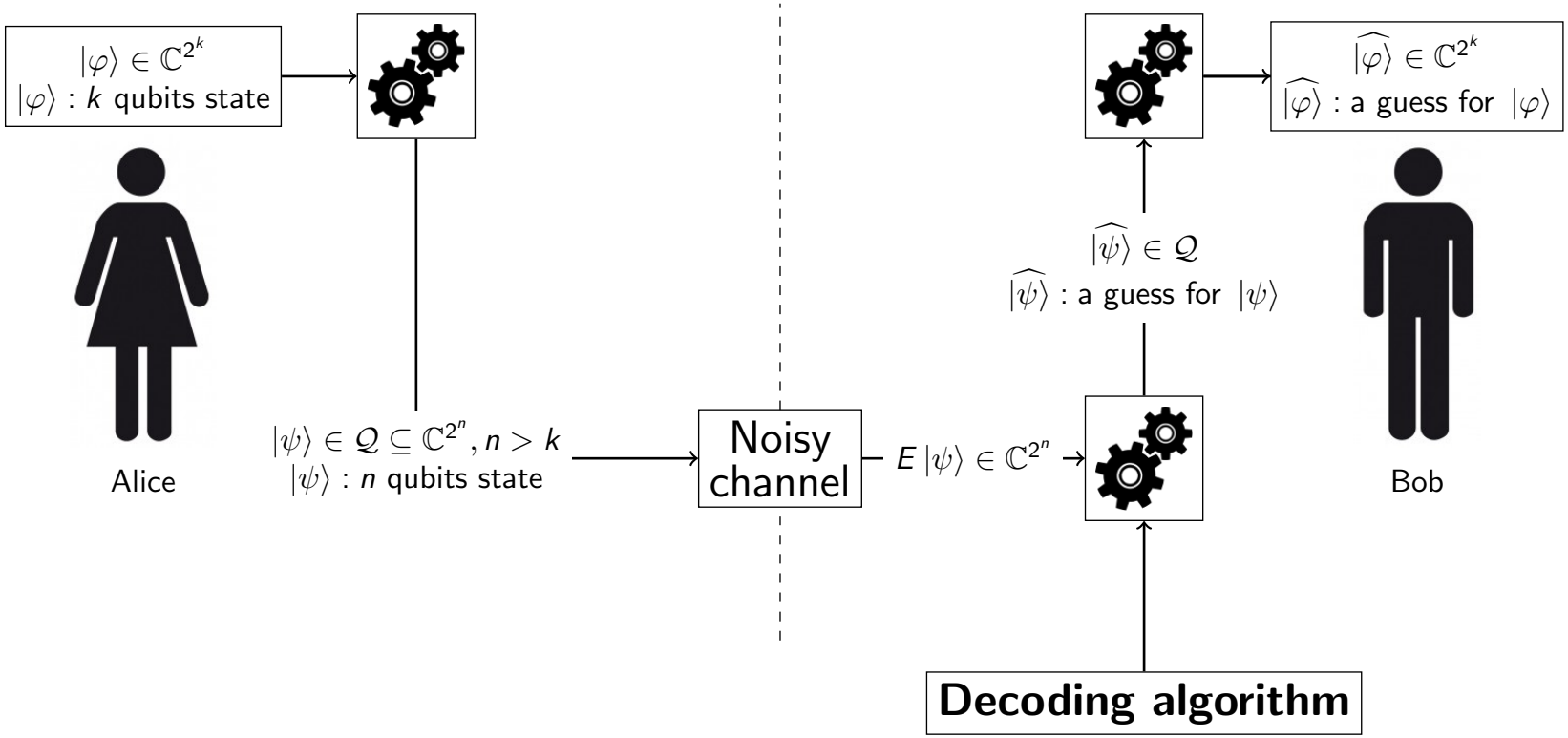
- Bit: $b \in \mathbb{F}_2$
- k-bit message: $m \in \mathbb{F}_2^k$
- A $[n, k]$-code is a k-dimensional subspace of $\mathbb{F}_2^n$
- Classical error: Flip

- Qubit: $|b\rangle \in \mathbb{C}^2$, $\| |b\rangle \|_2 = 1$
- k-qubits quantum state: $|\varphi\rangle \in \mathbb{C}^{2^k}$, $\| |\varphi\rangle \|_2 = 1$
- A $[\![n, k]\!]$-code is a 2^k-dimensional subspace of $\mathbb{C}^{2^n}$
- Quantum errors: $E \in \mathcal{U}(2^n)$



- Bit: $b \in \mathbb{F}_2$
- k-bit message: $m \in \mathbb{F}_2^k$
- A $[n, k]$-code is a k-dimensional subspace of $\mathbb{F}_2^n$
- Classical error: Flip

- Qubit: $|b\rangle \in \mathbb{C}^2$, $\| |b\rangle \|_2 = 1$
- k-qubits quantum state: $|\varphi\rangle \in \mathbb{C}^{2^k}$, $\| |\varphi\rangle \|_2 = 1$
- A $[\![n, k]\!]$-code is a 2^k-dimensional subspace of $\mathbb{C}^{2^n}$
- Quantum errors: $E \in \mathcal{U}(2^n)$



- Bit: $b \in \mathbb{F}_2$
- k-bit message: $m \in \mathbb{F}_2^k$
- A $[n, k]$-code is a k-dimensional subspace of $\mathbb{F}_2^n$
- Classical error: Flip

- Qubit: $|b\rangle \in \mathbb{C}^2$, $\| |b\rangle \|_2 = 1$
- k-qubits quantum state: $|\varphi\rangle \in \mathbb{C}^{2^k}$, $\| |\varphi\rangle \|_2 = 1$
- A $[\![n, k]\!]$-code is a 2^k-dimensional subspace of $\mathbb{C}^{2^n}$
- Quantum errors: $E \in \mathcal{U}(2^n)$

Definition: stabilizer codes ($\sim$ linear codes)

Pauli group:
$\mathcal{P}_n := \{I, X, Z, XZ\}^{\otimes n} \subseteq \mathcal{U}(2^n)$

Bit flip: $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Phase-flip: $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

The stabilizer code $\mathcal{Q}$ associated to $g_1, \cdots, g_{n-k} \in \mathcal{P}_n$ is:

$$\mathcal{Q} := \left\{ |\psi\rangle \in \mathbb{C}^{2^n} : g_1 |\psi\rangle = |\psi\rangle, \cdots, g_{n-k} |\psi\rangle = |\psi\rangle \right\}.$$

Definition: stabilizer codes ($\sim$ linear codes)

Pauli group:
$\mathcal{P}_n := \{I, X, Z, XZ\}^{\otimes n} \subseteq \mathcal{U}(2^n)$

Bit flip: $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Phase-flip: $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

The stabilizer code $\mathcal{Q}$ associated to $g_1, \cdots, g_{n-k} \in \mathcal{P}_n$ is:

$$\mathcal{Q} := \left\{ |\psi\rangle \in \mathbb{C}^{2^n} : g_1 |\psi\rangle = |\psi\rangle, \cdots, g_{n-k} |\psi\rangle = |\psi\rangle \right\}.$$

Communication scenario for a quantum code $\mathcal{Q} \subseteq \mathbb{C}^{2^n}$:

1) Alice sends $|\psi\rangle \in \mathcal{Q}$ through a noisy channel.
2) Bob receives $E|\psi\rangle$ with $E \in \mathcal{U}(2^n)$.
3) Bob measures $g_1, \cdots, g_{n-k} \in \mathcal{P}_n$
   $\rightarrow \sigma \in \mathbb{F}_2^{n-k}$ the syndrome.
4) Bob guesses a correction $\hat{E} \in \mathcal{P}_n$.

Is it possible to perform quantum error correction?

Bob needs to correct $E \in \mathcal{U}(2^n)$ given $\sigma \in \mathbb{F}_2^{n-k}$.

Is it possible to perform quantum error correction?

Bob needs to correct $E \in \mathcal{U}(2^n)$ given $\sigma \in \mathbb{F}_2^{n-k}$.

Answer: [Shor, '96]

Trick: Quantum measurements destruct the information.

Example: let $|\psi\rangle = \frac{1}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|1\rangle$ and let's measure Z:

- With probability $1/5$:
  - $\rightarrow$ Measurement output: 0
  - $\rightarrow$ $|\psi\rangle$ is projected onto $|\psi'\rangle = |0\rangle$
- With probability $4/5$:
  - $\rightarrow$ Measurement output: 1
  - $\rightarrow$ $|\psi\rangle$ is projected onto $|\psi'\rangle = |1\rangle$

The amplitudes are lost.

Communication scenario for a quantum code $\mathcal{Q} \subseteq \mathbb{C}^{2^n}$:

1) Alice sends $|\psi\rangle \in \mathcal{Q}$ through a noisy channel.
2) Bob receives $E|\psi\rangle$ with $E \in \mathcal{U}(2^n)$.
3) Bob measures $g_1, \cdots, g_{n-k} \in \mathcal{P}_n$
   - $\rightarrow$ $\sigma \in \mathbb{F}_2^{n-k}$ the syndrome (contains information about E but not about $|\psi\rangle$).
   - $\rightarrow$ $E|\psi\rangle$ is projected onto $E'|\psi\rangle$ with $E' \in \mathcal{P}_n$.
4) Bob guesses a correction $\hat{E} \in \mathcal{P}_n$.

Without loss of generality: $E \in \mathcal{P}_n$ or $E \in \{I, X\}^{\otimes n}$.

This work: Numerical study of quantum expander codes subject to iid X-type errors.

Outline

Fault-tolerant quantum computation

Fact: quantum information is fragile.

- Quantum storage is not stable.
- Quantum gates are noisy.

Question: Is it possible to build a quantum computer?

Fault-tolerant quantum computation

Fact: quantum information is fragile.

- Quantum storage is not stable.
- Quantum gates are noisy.

Question: Is it possible to build a quantum computer?
Answer: [Ben-Or & Aharonov, Gottesman, Shor, Preskill '96,'97, '13]

Threshold Theorem

Hypothesis: Are available noisy quantum gates whose noise is below some threshold.
Goal: Simulate a quantum circuit with m logical qubits.
Threshold theorem: We can build a fault-tolerant circuit with ηm physical qubits for some constant $\eta > 1$.

Idea: Use a quantum error correcting code with $\frac{m}{\text{polylog}(m)}$ logical qubits.

Outline

Available quantum LDPC codes

	Dimension	Minimal distance	Efficient correction up to size
Toric code [Kitaev, '03]	2	$\Theta(\sqrt{n})$	$\Theta(\sqrt{n})$
Manifold-based codes [Freedman & Meyer & Luo '02]	1	$\Theta(\sqrt{n}\sqrt[4]{\log(n)})$	Not efficient
Hyperbolic 2D [Freedman & Meyer & Luo, '02]	$\Theta(n)$	$\Theta(\log n)$	$\Theta(\log n)$
Hyperbolic 4D [Guth & Lubotzky, '14], [Hastings, '13], [Londe & Leverrier, '17]	$\Theta(n)$	$\Omega(n^{0.2}), \mathcal{O}(n^{0.3})$	$\Theta(\log n)$
Expander codes [Leverrier & Tillich & Zémor, '15]	$\Theta(n)$	$\Theta(\sqrt{n})$	$\Theta(\sqrt{n})$

- Minimal distance: smallest weight for an error with zero syndrome.
- Some errors with weight $\Theta(\sqrt{n})$ cannot be corrected.
- Errors with weight $\Theta(n)$ are corrected with high probability [Fawzi & **Grospellier** & Leverrier, '18].

Quantum expander codes [Leverrier & Tillich & Zémor '15]

Steps to define a quantum expander codes $\mathcal{Q}$:

- H the parity check matrix of a classical expander code [Sipser & Spielman, '96].
- Hypergraph product of H with itself:

$$H_X = (\mathbb{1} \otimes H, H^T \otimes \mathbb{1}) \qquad H_Z = (H \otimes \mathbb{1}, \mathbb{1} \otimes H^T)$$

- $g_1, \cdots, g_{n-k} \in \mathcal{P}_n$ where g_i is an X-type or Z-type generator:
  - X-type: $g_i = \otimes_{i=1}^n X^{L_i}$ with L a line of H_X.
  - Z-type: $g_i = \otimes_{i=1}^n Z^{L_i}$ with L a line of H_Z.
- $\mathcal{Q} := \left\{ |\psi\rangle \in \mathbb{C}^{2^n} : g_1 |\psi\rangle = |\psi\rangle, \cdots, g_{n-k} |\psi\rangle = |\psi\rangle \right\}$

The small-set-flip algorithm for X-type errors:
Repeat until blocked:

- **Informally:** Flip a subset of one X-type g_i which decreases the syndrome weight
- **Formally:** Find $S \subseteq L_i$ for some $g_i = \otimes_{i=1}^n X^{L_i}$ such that applying $\otimes_{i=1}^n X^{S_i}$ reduces the syndrome weight.

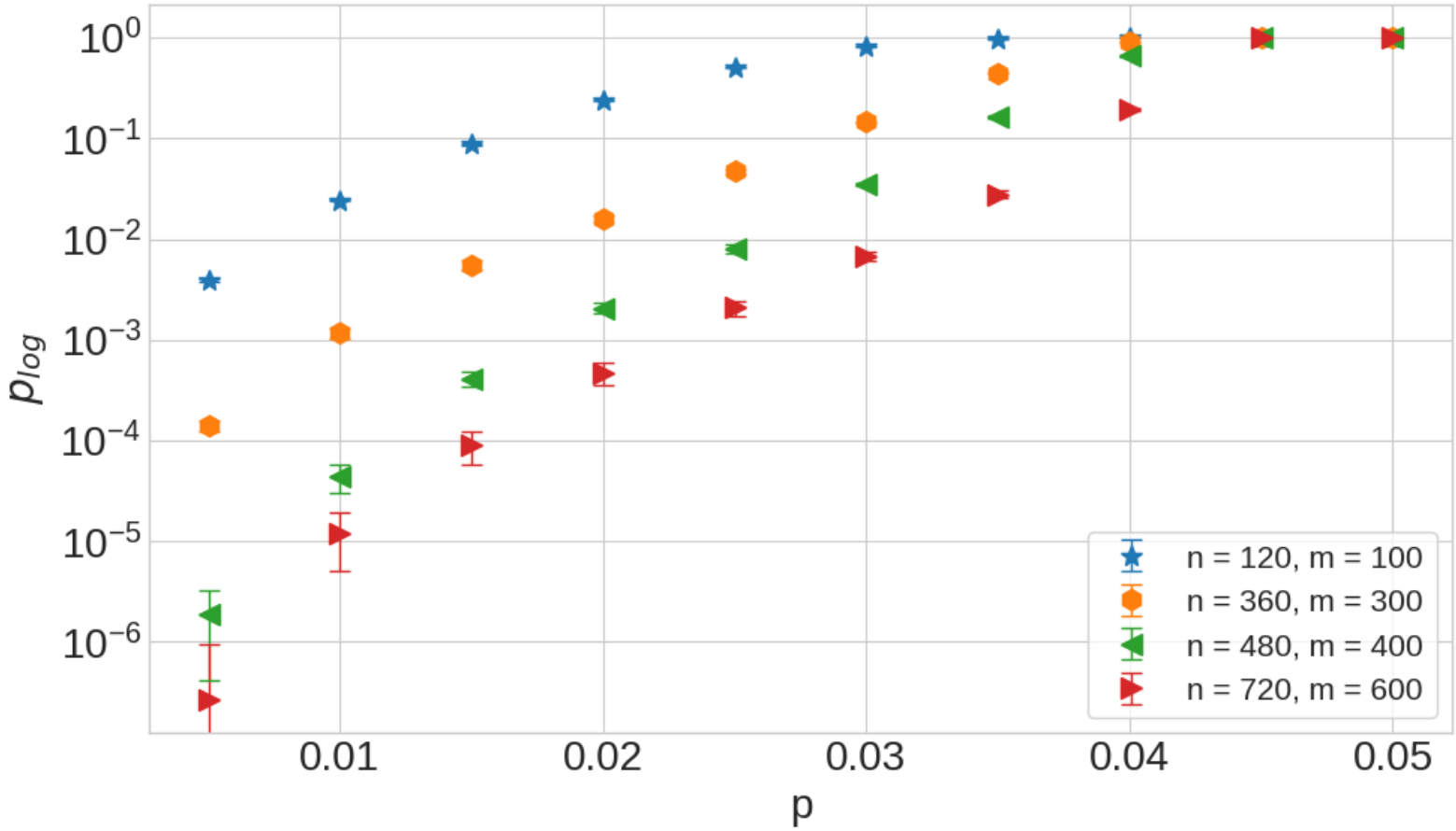
Outline

Protocol:

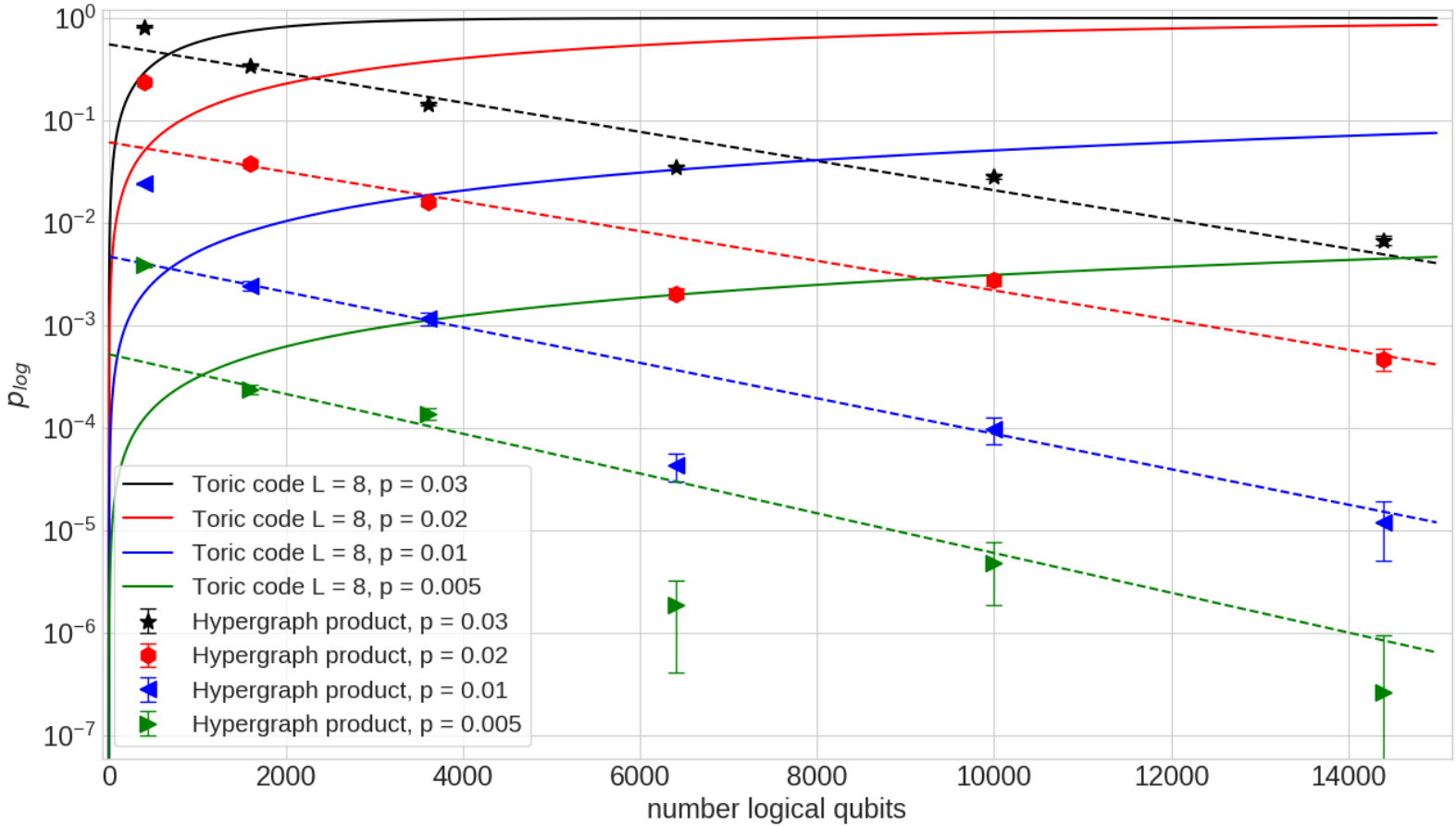
- Consider a quantum expander code.
- Estimation of logical failure rate with Monte-Carlo simulations:
  - Apply bit-flip on each qubit with probability p independently.
  - Run the small-set-flip decoder.
  - Check whether the error is corrected.

We expect to find a threshold p_{th}:

- If $p < p_{\mathrm{th}}$ then bigger codes have better performances.
- If $p > p_{\mathrm{th}}$ then smaller codes have better performances.



- No crossing point $\rightsquigarrow$ no obvious threshold.
- $p_{\mathrm{th}} \geq 4.5\%$



- Better to use toric code when ≤ 1000 logical qubits.
- Better to use expander codes when ≥ 1000 logical qubits.

Conclusion

- Quantum expander codes are very promising for large computations.

Future work:

- Run simulations for codes with higher rate.
- Improve the decoding algorithm.

Conclusion

- Quantum expander codes are very promising for large computations.

Future work:

- Run simulations for codes with higher rate.
- Improve the decoding algorithm.

Thank you for your attention.