L'ordinateur quantique à l'épreuve des erreurs

Christophe Vuillot

Inria

SIESTE - 23 octobre 2024

About Me

Current Position (Jan. 2021 - now)

Permanent, "Chargé de Recherche", at Inria Nancy, *Mocqua* team

About Me

Current Position (Jan. 2021 - now)

Permanent, “Chargé de Recherche”, at Inria Nancy, *Mocqua* team

Previous Research Experience

Postdoc	PhD	internships		
2019 - 2020	2015 - 2019	2015	2014	2012

Education

Upcoming Update

Future Position

Will be on (temporary) leave from Inria to work at Alice&Bob on trying to build a quantum computer

Computation

Computability

Church-Turing Thesis (20th): *Computability* $=$ Turing machines

Computation

Computability

Church-Turing Thesis (20th): *Computability* = Turing machines

What can be computed ?

- *Complexity* theory → accounts for time-scale and resources
- "Reasonable" complexity classes: P, BPP, ...

Computation

Computability

Church-Turing Thesis (20th): *Computability* = Turing machines

What can be computed ?

- *Complexity* theory → accounts for time-scale and resources
- "Reasonable" complexity classes: P, BPP, ...

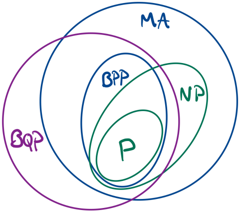
Physics of Computation Conference in 1981

Quantum processes $\notin$ *BPP*, (although $\in$ *PSPACE*).

Quantum Computation

Some Striking Quantum Algorithms

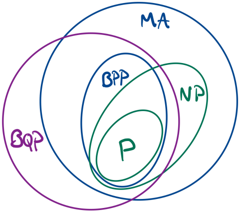
- Shor (1994) factors in polynomial time (break RSA).
- Grover (1996) searches an unstructured list in $\sqrt{N}$ queries.



Quantum Computation

Some Striking Quantum Algorithms

- Shor (1994) factors in polynomial time (break RSA).
- Grover (1996) searches an unstructured list in $\sqrt{N}$ queries.



Quantum Computer Model

Assume *idealized* perfect quantum computers!

Error Correction and Fault-Tolerance

Quantum Error Correction

- Encode quantum information redundantly
- Extract information about errors, process it and correct

Fault-Tolerant Quantum Computation

- Compute directly on encoded quantum information without weakening the protection
- Works when every quantum process is unreliable

Error Correction and Fault-Tolerance

Quantum Error Correction

- Encode quantum information redundantly
- Extract information about errors, process it and correct

Fault-Tolerant Quantum Computation

- Compute directly on encoded quantum information without weakening the protection
- Works when every quantum process is unreliable

Threshold Theorems (informal)

Given an error model there exist so-called fault-tolerant protocols and a threshold such that any computation can be simulated to any desired precision if the noise strength is below the threshold.

The Quantum Stack

FTQC Aware Compilation

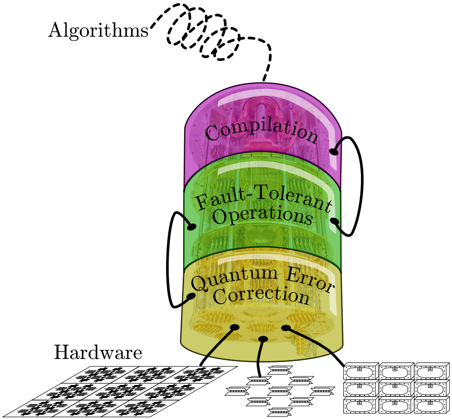
Specific gate sets

Fault-Tolerant Logic

Transversal gates, code deformation

Quantum Error Correction

Finite as well as infinite dimensional systems



Quantum Bit

A physical system with two perfectly distinguishable states:

Examples

- Electron around an atom/ion
- Photon in one of two paths
- Spin of a particle
- Collective degree of freedom
- ...

Notation

$$|0\rangle \qquad |1\rangle$$

Superposition

Qubit Hilbert Space

Quantum states live in a Hilbert space, $|\Psi\rangle \in \mathcal{H}$:

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle, \qquad |\alpha|^2 + |\beta|^2 = 1, \qquad \alpha, \beta \in \mathbb{C}.$$

Superposition

Qubit Hilbert Space

Quantum states live in a Hilbert space, $|\Psi\rangle \in \mathcal{H}$:

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \qquad |\alpha|^2 + |\beta|^2 = 1, \qquad \alpha, \beta \in \mathbb{C}.$$

Standard Orthonormal Basis

$$\langle 0|0\rangle = \langle 1|1\rangle = 1, \qquad \langle 0|1\rangle = 0$$

Superposition

Qubit Hilbert Space

Quantum states live in a Hilbert space, $|\Psi\rangle \in \mathcal{H}$:

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \qquad |\alpha|^2 + |\beta|^2 = 1, \qquad \alpha, \beta \in \mathbb{C}.$$

Standard Orthonormal Basis

$$\langle 0|0\rangle = \langle 1|1\rangle = 1, \qquad \langle 0|1\rangle = 0$$

Dual Basis

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

defines a perfectly valid basis

$$\langle +|+\rangle = \langle -|-\rangle = 1, \qquad \langle +|-\rangle = 0.$$

Standard Measurement

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \rightarrow \quad \{|0\rangle\,,|1\rangle\}? \begin{array}{l} \nearrow \quad |0\rangle \text{ with proba } |\alpha|^2 \\ \searrow \quad |1\rangle \text{ with proba } |\beta|^2 \end{array}$$

Dual Measurement

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow \{|+\rangle, |-\rangle\}?$$

$\nearrow$ $|+\rangle$ with proba $\frac{|\alpha+\beta|^2}{2}$

$\searrow$ $|-\rangle$ with proba $\frac{|\alpha-\beta|^2}{2}$

Quantum Gates

Unitary Transformations

Quantum transformations are linear and *unitary* (consistent with probabilistic interpretation of measurements)

Quantum Gates

Unitary Transformations

Quantum transformations are linear and *unitary* (consistent with probabilistic interpretation of measurements)

Examples: Pauli Operators

- Bit-flip: $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$

Quantum Gates

Unitary Transformations

Quantum transformations are linear and *unitary* (consistent with probabilistic interpretation of measurements)

Examples: Pauli Operators

- Bit-flip: $X\left|0\right\rangle = \left|1\right\rangle$, $X\left|1\right\rangle = \left|0\right\rangle$
- Phase-flip: $Z\left|0\right\rangle = \left|0\right\rangle$, $Z\left|1\right\rangle = -\left|1\right\rangle$,

Quantum Gates

Unitary Transformations

Quantum transformations are linear and *unitary* (consistent with probabilistic interpretation of measurements)

Examples: Pauli Operators

- Bit-flip: $X\left|0\right\rangle = \left|1\right\rangle$, $X\left|1\right\rangle = \left|0\right\rangle$
- Phase-flip: $Z\left|0\right\rangle = \left|0\right\rangle$, $Z\left|1\right\rangle = -\left|1\right\rangle$,
- or $Z\left|+\right\rangle = \left|-\right\rangle$, $Z\left|-\right\rangle = \left|+\right\rangle$

Quantum Gates

Unitary Transformations

Quantum transformations are linear and *unitary* (consistent with probabilistic interpretation of measurements)

Examples: Pauli Operators

- Bit-flip: $X\left|0\right\rangle = \left|1\right\rangle$, $X\left|1\right\rangle = \left|0\right\rangle$
- Phase-flip: $Z\left|0\right\rangle = \left|0\right\rangle$, $Z\left|1\right\rangle = -\left|1\right\rangle$,
- or $Z\left|+\right\rangle = \left|-\right\rangle$, $Z\left|-\right\rangle = \left|+\right\rangle$

Pauli Operators form a basis

$$\forall M, \quad M = \alpha_{\mathbb{1}}\mathbb{1} + \alpha_X X + \alpha_Z Z + \alpha_{XZ} XZ$$

Several Quantum Systems

Tensor Product of Hilbert Spaces

The joint Hilbert space of two quantum systems described by $|\Psi\rangle \in \mathcal{H}_1$ and $|\Phi\rangle \in \mathcal{H}_2$ is given by the tensor product

$$\mathcal{H}_1 \otimes \mathcal{H}_2.$$

A basis for $\mathcal{H}_1 \otimes \mathcal{H}_2$ can be obtained by the carthesian product of a basis of $\mathcal{H}_1$ and a basis of $\mathcal{H}_2$.

Several Quantum Systems

Tensor Product of Hilbert Spaces

The joint Hilbert space of two quantum systems described by $|\Psi\rangle \in \mathcal{H}_1$ and $|\Phi\rangle \in \mathcal{H}_2$ is given by the tensor product

$$\mathcal{H}_1 \otimes \mathcal{H}_2.$$

A basis for $\mathcal{H}_1 \otimes \mathcal{H}_2$ can be obtained by the carthesian product of a basis of $\mathcal{H}_1$ and a basis of $\mathcal{H}_2$.

Entangled States

Entangled states are states that cannot be factorized as a single product state

$$\alpha |\Psi_1\rangle \otimes |\Phi_1\rangle + \beta |\Psi_2\rangle \otimes |\Phi_2\rangle \neq |\Psi\rangle \otimes |\Phi\rangle .$$

Many Qubits

We consider having $n \in \mathbb{N}^*$ qubits

Hilbert Space

This is a 2^n dimensional space with standard basis

$$\{|\boldsymbol{b}\rangle \,|\forall \boldsymbol{b} \in \mathbb{F}_2^n\}, \qquad \mathbb{F}_2 = \{0, 1\}.$$

Quantum States

Quantum states are given by

$$|\Psi\rangle = \sum_{\boldsymbol{b}\in\mathbb{F}_2^n} \alpha_{\boldsymbol{b}} |\boldsymbol{b}\rangle, \qquad \sum_{\boldsymbol{b}\in\mathbb{F}_2^n} |\alpha_{\boldsymbol{b}}|^2 = 1.$$

Multi-Qubit Pauli Operators

Single Qubit X and Z

$$X_j |\boldsymbol{b}\rangle = |\boldsymbol{b} \oplus \boldsymbol{e}_j\rangle, \qquad \boldsymbol{e}_j = \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix}$$

$$Z_j |\boldsymbol{b}\rangle = (-1)^{b_j} |\boldsymbol{b}\rangle = (-1)^{\boldsymbol{b}\cdot\boldsymbol{e}_j} |\boldsymbol{b}\rangle .$$

Multi-Qubit X and Z

$$X(\boldsymbol{x}) = \prod_{j=1}^{n} X_j^{x_j}, \quad \boldsymbol{x} \in \mathbb{F}_2^n \qquad Z(\boldsymbol{z}) = \prod_{j=1}^{n} Z_j^{z_j}, \quad \boldsymbol{z} \in \mathbb{F}_2^n.$$

acting on states

$$X(\boldsymbol{x}) |\boldsymbol{b}\rangle = |\boldsymbol{b} \oplus \boldsymbol{x}\rangle ,$$

$$Z(\boldsymbol{z}) |\boldsymbol{b}\rangle = (-1)^{\boldsymbol{b}\cdot\boldsymbol{z}} |\boldsymbol{b}\rangle .$$

Multi-Qubit Pauli Operators

Single Qubit X and Z

$$X_j \left|\boldsymbol{b}\right\rangle = \left|\boldsymbol{b} \oplus \boldsymbol{e}_j\right\rangle, \qquad \boldsymbol{e}_j = \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix}$$

$$Z_j \left|\boldsymbol{b}\right\rangle = (-1)^{b_j} \left|\boldsymbol{b}\right\rangle = (-1)^{\boldsymbol{b}\cdot\boldsymbol{e}_j} \left|\boldsymbol{b}\right\rangle.$$

Multi-Qubit Pauli Operators

Single Qubit X and Z

$$X_j \left|\boldsymbol{b}\right\rangle = \left|\boldsymbol{b} \oplus \boldsymbol{e}_j\right\rangle, \qquad \boldsymbol{e}_j = \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix}$$

$$Z_j \left|\boldsymbol{b}\right\rangle = (-1)^{b_j} \left|\boldsymbol{b}\right\rangle = (-1)^{\boldsymbol{b}\cdot\boldsymbol{e}_j} \left|\boldsymbol{b}\right\rangle.$$

Multi-Qubit X and Z

$$X(\boldsymbol{x}) = \prod_{j=1}^{n} X_j^{x_j}, \quad \boldsymbol{x} \in \mathbb{F}_2^n \qquad Z(\boldsymbol{z}) = \prod_{j=1}^{n} Z_j^{z_j}, \quad \boldsymbol{z} \in \mathbb{F}_2^n.$$

Multi-Qubit Pauli Operators

Single Qubit X and Z

$$X_j\,|\boldsymbol{b}\rangle = |\boldsymbol{b} \oplus \boldsymbol{e}_j\rangle\,, \qquad \boldsymbol{e}_j = \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix}$$
$$Z_j\,|\boldsymbol{b}\rangle = (-1)^{b_j}\,|\boldsymbol{b}\rangle = (-1)^{\boldsymbol{b}\cdot\boldsymbol{e}_j}\,|\boldsymbol{b}\rangle\,.$$

Multi-Qubit X and Z

$$X(\boldsymbol{x}) = \prod_{j=1}^{n} X_j^{x_j}, \quad \boldsymbol{x} \in \mathbb{F}_2^n \qquad Z(\boldsymbol{z}) = \prod_{j=1}^{n} Z_j^{z_j}, \quad \boldsymbol{z} \in \mathbb{F}_2^n.$$

acting on states

$$X(\boldsymbol{x})\,|\boldsymbol{b}\rangle = |\boldsymbol{b} \oplus \boldsymbol{x}\rangle\,,$$
$$Z(\boldsymbol{z})\,|\boldsymbol{b}\rangle = (-1)^{\boldsymbol{b}\cdot\boldsymbol{z}}\,|\boldsymbol{b}\rangle\,.$$

Pauli Measurements

Z Parity Measurement

Given $\boldsymbol{z} \in \mathbb{F}_2^n$, it splits in half $\boldsymbol{b} \in \mathbb{F}_2^n$ between:

- $(-1)^{\boldsymbol{b}\cdot\boldsymbol{z}} = 1$
- $(-1)^{\boldsymbol{b}\cdot\boldsymbol{z}} = -1$

There is a quantum measurement that measures the parity of $\boldsymbol{z} \cdot \boldsymbol{b}$

Pauli Measurements

Z Parity Measurement

Given $\boldsymbol{z} \in \mathbb{F}_2^n$, it splits in half $\boldsymbol{b} \in \mathbb{F}_2^n$ between:

- $(-1)^{\boldsymbol{b}\cdot\boldsymbol{z}} = 1$
- $(-1)^{\boldsymbol{b}\cdot\boldsymbol{z}} = -1$

There is a quantum measurement that measures the parity of $\boldsymbol{z} \cdot \boldsymbol{b}$

$$|\Psi\rangle = \sum_{\boldsymbol{b}\in\mathbb{F}_2^n} \alpha_{\boldsymbol{b}} |\boldsymbol{b}\rangle \underset{M_{\boldsymbol{z}}=m\in\{0,1\}}{\longrightarrow} |\psi'_m\rangle \propto \sum_{\boldsymbol{b},\, \boldsymbol{z}\cdot\boldsymbol{b}=m} \alpha_{\boldsymbol{b}} |\boldsymbol{b}\rangle$$

$$\Rightarrow Z(\boldsymbol{z}) |\Psi'_m\rangle = (-1)^m |\Psi'_m\rangle$$

Pauli Measurements

Z Parity Measurement

Given $\boldsymbol{z} \in \mathbb{F}_2^n$, it splits in half $\boldsymbol{b} \in \mathbb{F}_2^n$ between:

- $(-1)^{\boldsymbol{b}\cdot\boldsymbol{z}} = 1$
- $(-1)^{\boldsymbol{b}\cdot\boldsymbol{z}} = -1$

There is a quantum measurement that measures the parity of $\boldsymbol{z} \cdot \boldsymbol{b}$

$$|\Psi\rangle = \sum_{\boldsymbol{b}\in\mathbb{F}_2^n} \alpha_{\boldsymbol{b}} |\boldsymbol{b}\rangle \underset{M_{\boldsymbol{z}}=m\in\{0,1\}}{\longrightarrow} |\psi'_m\rangle \propto \sum_{\boldsymbol{b},\, \boldsymbol{z}\cdot\boldsymbol{b}=m} \alpha_{\boldsymbol{b}} |\boldsymbol{b}\rangle$$

$$\Rightarrow Z(\boldsymbol{z}) |\Psi'_m\rangle = (-1)^m |\Psi'_m\rangle$$

X Parity Measurement

Same but in the dual basis $\{|+\rangle, |-\rangle\}$ and after measurement:

$$X(\boldsymbol{x}) |\Psi'_m\rangle = (-1)^m |\Psi'_m\rangle .$$

Classical Error Correction

3-bit Repetition Code

Define the code $\mathcal{C} = \{\boldsymbol{b}_0, \boldsymbol{b}_1\}$

$$
\begin{aligned}
0 &\to \boldsymbol{b}_0 = \begin{pmatrix} 0 & 0 & 0 \end{pmatrix}, \\
1 &\to \boldsymbol{b}_1 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}.
\end{aligned}
$$

Classical Error Correction

3-bit Repetition Code

Define the code $\mathcal{C} = \{\boldsymbol{b}_0, \boldsymbol{b}_1\}$

$$0 \to \boldsymbol{b}_0 = \begin{pmatrix} 0 & 0 & 0 \end{pmatrix},$$
$$1 \to \boldsymbol{b}_1 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}.$$

Parity-check matrix

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \qquad H\boldsymbol{b}_0^{\mathrm{T}} = H\boldsymbol{b}_1^{\mathrm{T}} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Classical Error Correction

3-bit Repetition Code

Define the code $\mathcal{C} = \{\boldsymbol{b}_0, \boldsymbol{b}_1\}$

$$\begin{aligned} 0 \rightarrow \boldsymbol{b}_0 &= \begin{pmatrix} 0 & 0 & 0 \end{pmatrix}, \\ 1 \rightarrow \boldsymbol{b}_1 &= \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}. \end{aligned}$$

Parity-check matrix

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \qquad H\boldsymbol{b}_0^{\mathrm{T}} = H\boldsymbol{b}_1^{\mathrm{T}} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Syndrome of bit-flip error $\boldsymbol{e}$

The parity checks give information about errors only

$$H(\boldsymbol{b}_0 + \boldsymbol{e})^{\mathrm{T}} = H(\boldsymbol{b}_1 + \boldsymbol{e})^{\mathrm{T}} = H\boldsymbol{e}^{\mathrm{T}}$$

Linear Error Correcting Code

Definition

A linear code $\mathcal{C} \subset \mathbb{F}_2^n$ can be defined by a parity check matrix $H \in \mathbb{F}_2^{r \times n}$ with

$$\mathcal{C} = \left\{ \boldsymbol{b} \in \mathbb{F}_2^n \middle| \, H\boldsymbol{b}^{\mathrm{T}} = \mathbf{0} \right\}.$$

Linear Error Correcting Code

Definition

A linear code $\mathcal{C} \subset \mathbb{F}_2^n$ can be defined by a parity check matrix $H \in \mathbb{F}_2^{r \times n}$ with

$$\mathcal{C} = \left\{ \boldsymbol{b} \in \mathbb{F}_2^n \middle| \, H\boldsymbol{b}^{\mathrm{T}} = \boldsymbol{0} \right\}.$$

Syndrome and Decoding

$$\forall \boldsymbol{c} \in \mathcal{C}, \; H(\boldsymbol{c} + \boldsymbol{e})^{\mathrm{T}} = H\boldsymbol{e}^{\mathrm{T}}$$

Given $\boldsymbol{s}$ find the smallest $\boldsymbol{e}$ such that $H\boldsymbol{e}^{\mathrm{T}} = \boldsymbol{s}$.

Linear Error Correcting Code

Definition

A linear code $\mathcal{C} \subset \mathbb{F}_2^n$ can be defined by a parity check matrix $H \in \mathbb{F}_2^{r \times n}$ with

$$\mathcal{C} = \left\{ \boldsymbol{b} \in \mathbb{F}_2^n \middle| \, H\boldsymbol{b}^{\mathrm{T}} = \boldsymbol{0} \right\}.$$

Syndrome and Decoding

$$\forall \boldsymbol{c} \in \mathcal{C},\, H(\boldsymbol{c} + \boldsymbol{e})^{\mathrm{T}} = H\boldsymbol{e}^{\mathrm{T}}$$

Given $\boldsymbol{s}$ find the smallest $\boldsymbol{e}$ such that $H\boldsymbol{e}^{\mathrm{T}} = \boldsymbol{s}$.

Parameters $[n, k, d]$

The length of the codewords, n, the dimension of $\mathcal{C}$, k, the minimum distance, d,

$$k = n - \mathrm{rank} H, \qquad d = \min_{\boldsymbol{c} \in \mathcal{C},\, \boldsymbol{c} \neq \boldsymbol{0}} |\boldsymbol{c}|.$$

Quantum Error Correcting Code

General Idea

- Correct for bit-flips and phase-flips separately with X and Z parity measurements
- Problem: not all X and Z parity measurements are compatible because $XZ = -ZX$

Quantum Error Correcting Code

General Idea

- Correct for bit-flips and phase-flips separately with X and Z parity measurements
- Problem: not all X and Z parity measurements are compatible because $XZ = -ZX$

Quantum Commutation Constraint

$$
\begin{gathered}
Z(\boldsymbol{z})\,|\Psi\rangle = |\Psi\rangle \quad \wedge \quad X(\boldsymbol{z})\,|\Psi\rangle = |\Psi\rangle \\
\Rightarrow X(\boldsymbol{x})Z(\boldsymbol{z}) = Z(\boldsymbol{z})X(\boldsymbol{x}) \\
\Rightarrow \boldsymbol{x} \cdot \boldsymbol{z} = 0
\end{gathered}
$$

Quantum Error Correcting Code

Definition

Given two parity check matrices $H_Z \in \mathbb{F}_2^{r_X \times n}$ and $H_X \in \mathbb{F}_2^{r_X \times n}$ such that

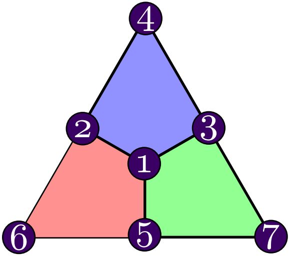
$$H_Z H_X^{\mathrm{T}} = 0,$$

We define the quantum error correcting code $\mathcal{C}(H_Z, H_X)$ on n qubits as the quantum states satisfying the Z and X parities defined by H_Z and H_X:

$$\mathcal{C} = \{|\Psi\rangle \,|\, \forall \boldsymbol{s}_Z \in \mathbb{F}_2^{r_Z}, \forall \boldsymbol{s}_X \in \mathbb{F}_2^{r_X},\ Z(\boldsymbol{s}_Z H_Z)\,|\Psi\rangle = X(\boldsymbol{s}_X H_X)\,|\Psi\rangle = |\Psi\rangle\}$$

Steane's Code Example

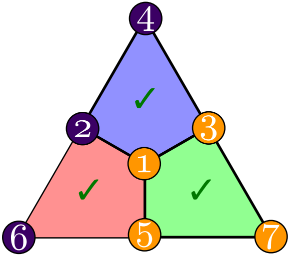
$$
\left.\begin{matrix} H_X \\ \| \\ H_Z \end{matrix}\right\} =
\begin{array}{cc}
 & \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{matrix} \\
\begin{matrix} c_1 \\ c_2 \\ c_3 \end{matrix} &
\begin{pmatrix}
1 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1
\end{pmatrix}
\end{array}
$$



Stabilizer checks

Steane's Code Example

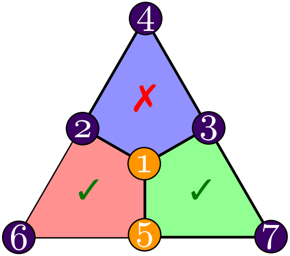
$$\begin{array}{c} H_X \\ \parallel \\ H_Z \end{array}\Bigg\} = \begin{array}{c} \\ c_1 \\ c_2 \\ c_3 \end{array} \begin{array}{c} \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$



Stabilizer checks

Steane's Code Example

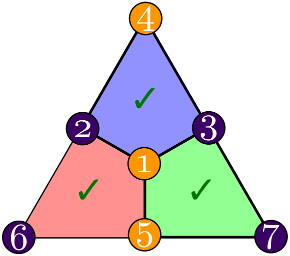
$$
\left.\begin{array}{c} H_X \\ \| \\ H_Z \end{array}\right\} = \begin{array}{c} \\ c_1 \\ c_2 \\ c_3 \end{array}
\begin{array}{c}
\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\
\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}
\end{array}
$$



Error

Steane's Code Example

$$
\begin{array}{c}
\left.\begin{array}{c} H_X \\ \parallel \\ H_Z \end{array}\right\} =
\end{array}
\begin{array}{c} \\ c_1 \\ c_2 \\ c_3 \end{array}
\begin{array}{c}
\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\
\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}
\end{array}
$$



Logical operator

Properties of Quantum Codes

Logical operators

Pauli operators which are not detectable but not stabilizers act non-trivial on the codespace

$$\mathcal{L}_X = \ker H_Z / \mathrm{im} H_X, \qquad \mathcal{L}_Z = \ker H_X / \mathrm{im} H_Z$$

Properties of Quantum Codes

Logical operators

Pauli operators which are not detectable but not stabilizers act non-trivial on the codespace

$$\mathcal{L}_X = \mathrm{ker} H_Z / \mathrm{im} H_X, \qquad \mathcal{L}_Z = \mathrm{ker} H_X / \mathrm{im} H_Z$$

Parameters $[[n, k, d]]$

The number of qubits, n, the number of logical qubits in $\mathcal{C}$, k, the minimum distance, d,

$$k = n - \mathrm{rank} H_Z - \mathrm{rank} H_X, \qquad d = \min_{\boldsymbol{c} \in \mathcal{L}_X \cup \mathcal{L}_Z, \, \boldsymbol{c} \neq \boldsymbol{0}} |\boldsymbol{c}|.$$

Desirable Properties of Quantum Codes

Given a quantum code $\mathcal{C}$ with parameters $[[n, k, d]]$ one might want it to have

- Large encoding rate: k/n
- Large distance: d
- Good and efficient syndrome decoding algorithm
- (Large) Threshold
- Easy implementation $\rightarrow$ sparse/local matrices H_Z and H_X
- Fault-tolerant quantum gates...

Desirable Properties of Quantum Codes

Given a quantum code $\mathcal{C}$ with parameters $[[n, k, d]]$ one might want it to have

- Large encoding rate: k/n
- Large distance: d
- Good and efficient syndrome decoding algorithm
- (Large) Threshold
- Easy implementation $\to$ sparse/local matrices H_Z and H_X
- Fault-tolerant quantum gates...

Good quantum LDPC codes exists

The existence of good quantum LDPC codes with efficient decoders has been established first in 2022, i.e $[[n, k = \Theta(n), d = \Theta(n)]]$.

Fruitful Connection to Homology

Chain Complex

$$\mathcal{C}: \quad C_2 \xrightarrow{\partial} C_1 \xrightarrow{\sigma} C_0 \quad \text{with } \sigma \circ \partial = 0$$

Fruitful Connection to Homology

Chain Complex

$$\mathcal{C}: \quad \begin{array}{ccccc} C_2 & \xrightarrow[H_X]{\partial} & C_1 & \xrightarrow[H_Z^T]{\sigma} & C_0 \\ \shortparallel & & \shortparallel & & \shortparallel \\ \mathbb{F}_2^{r_x} & & \mathbb{F}_2^{n} & & \mathbb{F}_2^{r_z} \end{array} \quad \text{with } \sigma \circ \partial = 0$$

Fruitful Connection to Homology

Chain Complex

$$\begin{array}{ccccccc} \mathcal{C}: & C_2 & \xrightarrow[H_X]{\partial} & C_1 & \xrightarrow[H_Z^T]{\sigma} & C_0 & \text{with } \sigma \circ \partial = 0 \\ & \shortparallel & & \shortparallel & & \shortparallel & \\ & \mathbb{F}_2^{r_x} & & \mathbb{F}_2^{n} & & \mathbb{F}_2^{r_z} & \\ & \shortparallel & & \shortparallel & & \shortparallel & \\ & \text{stabilizers} & & \text{operators} & & \text{syndrome} & \end{array}$$

Fruitful Connection to Homology

Chain Complex

$$
\begin{array}{ccccccl}
\mathcal{C}: & C_2 & \xrightarrow[H_X]{\partial} & C_1 & \xrightarrow[H_Z^T]{\sigma} & C_0 & \text{with } \sigma \circ \partial = 0 \\
& \shortparallel & & \shortparallel & & \shortparallel & \\
& \mathbb{F}_2^{r_x} & & \mathbb{F}_2^{n} & & \mathbb{F}_2^{r_z} & \\
& \shortparallel & & \shortparallel & & \shortparallel & \\
& \text{stabilizers} & & \text{operators} & & \text{syndrome} &
\end{array}
$$

Homology Group $=$ X Logical Operators

$$H_1(\mathcal{C}, \mathbb{Z}) = \ker \sigma / \mathrm{im} \partial = \ker (H_Z) / \mathrm{im} (H_X)$$

Fruitful Connection to Homology

Chain Complex

$$
\begin{array}{cccccccc}
\mathcal{C}: & C_2 & \xrightarrow{\partial} & C_1 & \xrightarrow{\sigma} & C_0 & & \text{with } \sigma \circ \partial = 0 \\
& \shortparallel & H_X & \shortparallel & H_Z^T & \shortparallel & & \\
& \mathbb{F}_2^{r_x} & & \mathbb{F}_2^{n} & & \mathbb{F}_2^{r_z} & & \\
& \shortparallel & & \shortparallel & & \shortparallel & & \\
& \text{stabilizers} & & \text{operators} & & \text{syndrome} & &
\end{array}
$$

Homology Group $=$ X Logical Operators

$$
\begin{aligned}
H_1(\mathcal{C}, \mathbb{Z}) = \ker \sigma / \mathrm{im} \partial &= \ker\left(H_Z\right) / \mathrm{im}\left(H_X\right) \\
&= \mathcal{L}_X
\end{aligned}
$$

Cohomology = Logical Z

Cochain Complex

$$
\begin{array}{ccccccc}
\mathcal{C}^* : & C_2^* & \xleftarrow[H_X^T]{\partial^*} & C_1^* & \xleftarrow[H_Z]{\sigma^*} & C_0^* \\
& \shortparallel & & \shortparallel & & \shortparallel \\
& \mathbb{F}_2^{r_x} & & \mathbb{F}_2^{n} & & \mathbb{F}_2^{r_z} \\
& \shortparallel & & \shortparallel & & \shortparallel \\
& \text{syndrome} & & \text{operators} & & \text{stabilizers}
\end{array}
$$

Cohomology $=$ Logical Z

Cochain Complex

$$\begin{array}{ccccccc}
\mathcal{C}^* : & C_2^* & \xleftarrow[H_X^T]{\partial^*} & C_1^* & \xleftarrow[H_Z]{\sigma^*} & C_0^* \\
& \parallel & & \parallel & & \parallel \\
& \mathbb{F}_2^{r_x} & & \mathbb{F}_2^{n} & & \mathbb{F}_2^{r_z} \\
& \parallel & & \parallel & & \parallel \\
& \text{syndrome} & & \text{operators} & & \text{stabilizers}
\end{array}$$

Cohomology Group $=$ Z Logical Operators

$$H^1(\mathcal{C}, \mathbb{T}) = \ker \partial^* / \mathrm{im} \sigma^* = \ker (H_X) / \mathrm{im} (H_Z)$$

Cohomology $=$ Logical Z

Cochain Complex

$$
\mathcal{C}^* : \quad \begin{array}{ccccc}
C_2^* & \xleftarrow[H_X^T]{\partial^*} & C_1^* & \xleftarrow[H_Z]{\sigma^*} & C_0^* \\
\shortparallel & & \shortparallel & & \shortparallel \\
\mathbb{F}_2^{r_x} & & \mathbb{F}_2^{n} & & \mathbb{F}_2^{r_z} \\
\shortparallel & & \shortparallel & & \shortparallel \\
\text{syndrome} & & \text{operators} & & \text{stabilizers}
\end{array}
$$

Cohomology Group $=$ Z Logical Operators

$$
\begin{aligned}
H^1(\mathcal{C}, \mathbb{T}) = \ker \partial^* / \mathrm{im} \sigma^* &= \ker \left(H_X\right) / \mathrm{im} \left(H_Z\right) \\
&= \mathcal{L}_Z
\end{aligned}
$$

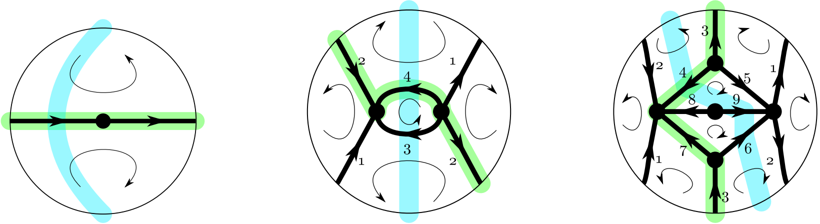
Codes from Cellular Homology in 2D

$$
\begin{array}{ccccccc}
\mathcal{C}: & C_2 & \xrightarrow{\partial} & C_1 & \xrightarrow{\sigma} & C_0 & \text{with } \sigma \circ \partial = 0 \\
 & \shortparallel & & \shortparallel & & \shortparallel & \\
 & \mathbb{F}_2^F & & \mathbb{F}_2^E & & \mathbb{F}_2^V & \\
 & \shortparallel & & \shortparallel & & \shortparallel & \\
 & \text{faces} & & \text{edges} & & \text{vertices} &
\end{array}
$$

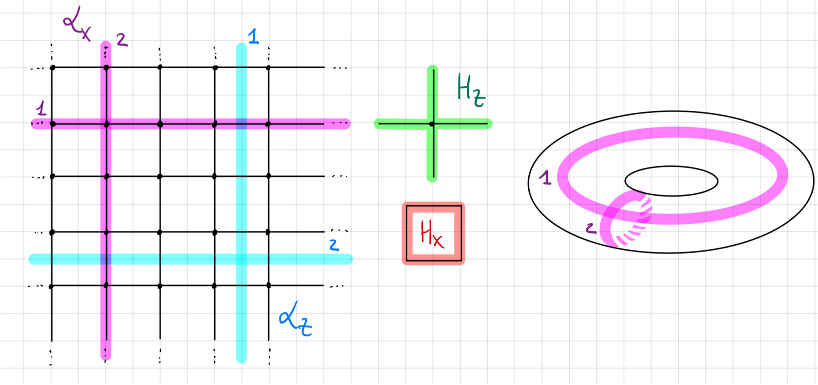
Codes from Cellular Homology in 2D

$$
\begin{array}{ccccccc}
\mathcal{C}: & C_2 & \xrightarrow{\partial} & C_1 & \xrightarrow{\sigma} & C_0 & \text{with } \sigma \circ \partial = 0 \\
 & \parallel & & \parallel & & \parallel & \\
 & \mathbb{F}_2^F & & \mathbb{F}_2^E & & \mathbb{F}_2^V & \\
 & \parallel & & \parallel & & \parallel & \\
 & \text{faces} & & \text{edges} & & \text{vertices} &
\end{array}
$$

Example: Projective Plane



The Toric Code (Kitaev 1997)



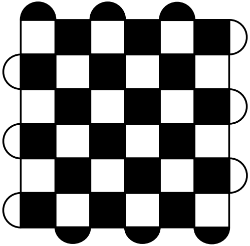
For a genus g surface, distance correspond to shortest non-trivial cycles and

$$H_1(\mathcal{C}, \mathbb{F}_2) = H^1(\mathcal{C}, \mathbb{F}_2) = \mathbb{F}_2^{2g}$$

The Surface Code: The Volkswagen of Quantum Codes

Many Advantages

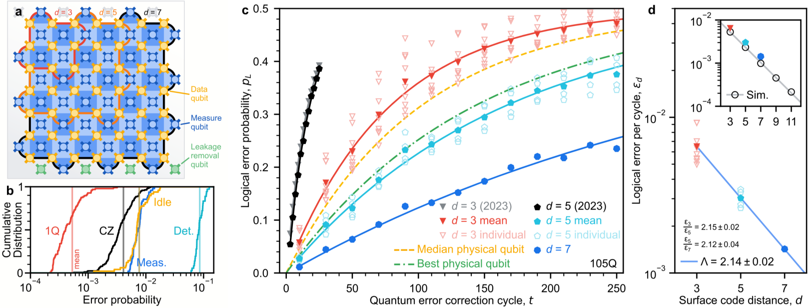
- 2D local connectivity with degree 4
- Good decoder with high threshold
- Fault-tolerant gates understood
- Experimentally demonstrated (2024)



One Weakness

Vanishing encoding rate!

Google's 2024 Surface Code Experiment



Bravyi-Poulin-Terhal Bound

The surface code is optimal for 2D, for any $[[n, k, d]]$ quantum code:

Constraints from 2D Locality

$$kd^2 = O(n)$$

Bravyi-Poulin-Terhal Bound

The surface code is optimal for 2D, for any $[[n, k, d]]$ quantum code:

Constraints from 2D Locality

$$kd^2 = O(n)$$

How to Improve

- Have to soften connectivity constraints

In the Lab

Physical Systems

Physical systems are often richer than qubits, for instance bosonic modes are infinite dimensional quantum systems

- photons in a cavity
- motion of an ion

In the Lab

Physical Systems

Physical systems are often richer than qubits, for instance bosonic modes are infinite dimensional quantum systems

- photons in a cavity
- motion of an ion

Error Correction

Can be formulated more generally as $\mathcal{H}_{\mathrm{code}} \subset \mathcal{H}$. Often just replacing $\mathbb{F}_2$ with the relevant G is enough

- $G = \mathbb{Z}/\mathbb{Z}_d \longrightarrow$ Qudit error correction
- $G = \mathbb{R} \longrightarrow$ Grid-state bosonic codes (GKP)
- $G = \mathbb{Z} \longrightarrow$ Quantum Rotor codes

Cat Qubits

Bosonic Codes

- Uses bosonic modes, i.e. $\mathcal{H} = \ell_2(\mathbb{N})$
- Can encodes a qubit
- Can features extremely biased noise

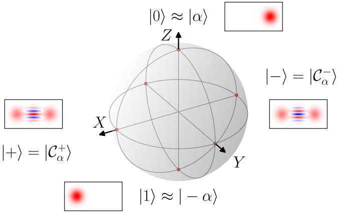
Cat Qubits

Bosonic Codes

- Uses bosonic modes, i.e. $\mathcal{H} = \ell_2(\mathbb{N})$
- Can encodes a qubit
- Can features extremely biased noise

Cat Qubit

- $|\overline{0}\rangle \simeq |\alpha\rangle$, $|\overline{1}\rangle \simeq |-\alpha\rangle$
- X-errors $\sim \mathrm{e}^{-2|\alpha|^2}$
- Z-errors $\sim c|\alpha|^2$



Repetition Cat Qubit

Assuming we can get negligible X errors $\rightarrow$ Classical code to correct remaining Z errors

Repetition Cat Qubit

Assuming we can get negligible X errors $\rightarrow$ Classical code to correct remaining Z errors

Repetition Cat

- use $[n, 1, n]$ repetition code
- 1D layout
- Degree 2 tanner graph

Repetition Cat Qubit

Assuming we can get negligible X errors $\rightarrow$ Classical code to correct remaining Z errors

Repetition Cat

- use $[n, 1, n]$ repetition code
- 1D layout
- Degree 2 tanner graph

Classical Bravyi-Poulin-Terhal bound in 2D

$$k\sqrt{d} = O(n)$$

Repetition Cat Qubit

Assuming we can get negligible X errors → Classical code to correct remaining Z errors

Repetition Cat

- use $[n, 1, n]$ repetition code
- 1D layout
- Degree 2 tanner graph

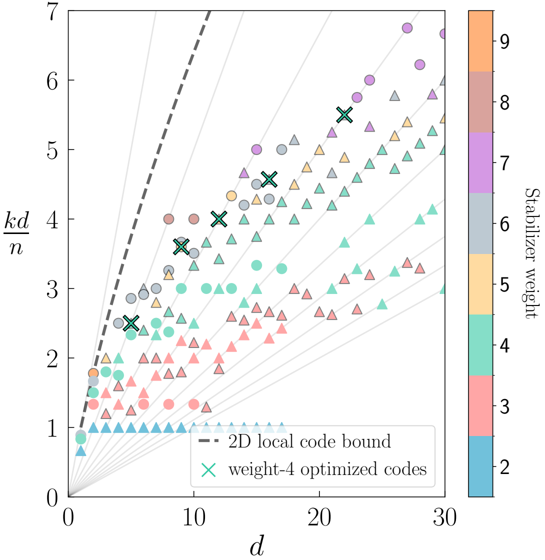
Classical Bravyi-Poulin-Terhal bound in 2D

$$k\sqrt{d} = O(n)$$

Repetition Code not Optimal

$$k\sqrt{d} = 1 \times \sqrt{n}$$

Exploring All Codes

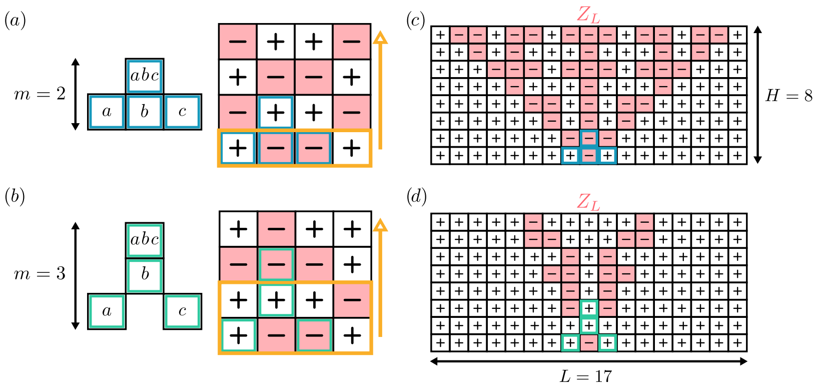


Cellular Automaton Codes

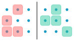
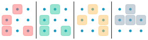
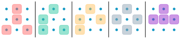
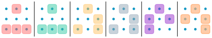
Characteristics

- $L \times H$ Cylinder
- Translation invariant check with “pointed” shape
- k linear in L
- d increases with H
- fixed $H \rightarrow$ fixed kd/n

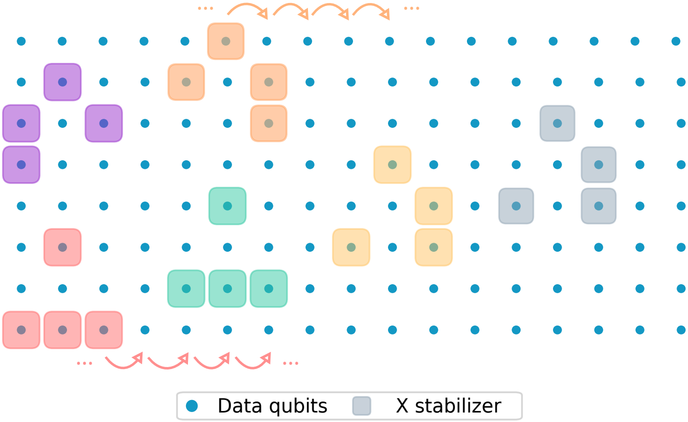
Cellular Automaton Codes Examples



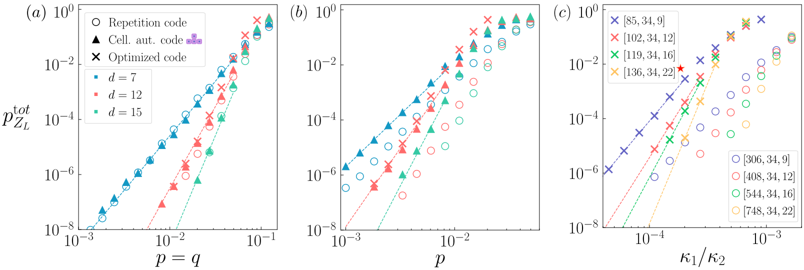
Relaxing Vertical Translation Invariance

$[n, k, d]$	kd/n	$(H, L = L^* + \ell)$	Stabilizer shapes (bottom to top)
$[20 + 4\ell, 10 + 2\ell, 5]$	2.5	$(4,\ 5 + \ell)$	
$[55 + 5\ell, 22 + 2\ell, 9]$	3.6	$(5,\ 11 + \ell)$	
$[78 + 6\ell, 26 + 2\ell, 12]$	4	$(6,\ 13 + \ell)$	
$[119 + 7\ell, 34 + 2\ell, 16]$	4.6	$(7,\ 17 + \ell)$	
$[136 + 8\ell, 34 + 2\ell, 22]$	5.5	$(8,\ 17 + \ell)$	

The Chosen One



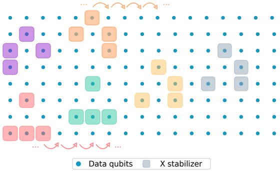
Numerical Simulations



LDPC-Cat Code

LDPC-Cat Code

- $[136 + 8\ell, 34 + 2\ell, 22]$ code
- 2D local
- Degree 4 tanner graph



Improvement over Surface code

In an intermediate regime (logical error rate$\sim 10^{-8}$) can get 44-fold reduction in resource cost.

Summary

- Concepts works in theory
- First experimental proofs are emerging
- Demonstrating that it scales in practice is still daunting
- Active area of research with lot to understand

Quantum in France

Quantum Programming Languages

Inria Nancy, Inria Saclay

Quantum Algorithms

Irif Paris

Quantum Info and Error Correction

Inria Paris, Lyon, Bordeaux, CEA Grenoble