Fault-tolerant Preparation of Stabilizer States for Quantum Calderbank-Shor-Steane Codes by Classical Error-Correcting Codes

Ching-Yi Lai

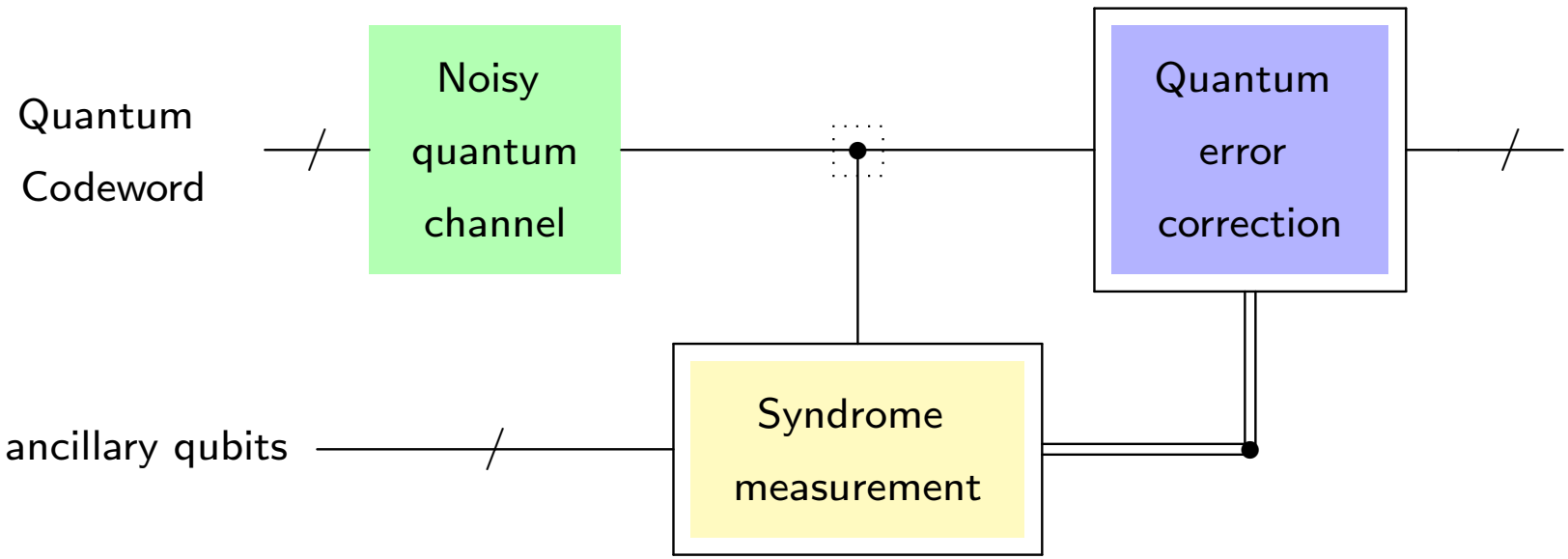
Institute of Information Science, Academia Sinica

September 1, 2016

Joint work with Yicong Zheng (Centre for Quantum Technology, Singapore)
and Todd Brun (University of Southern California)

arXiv:1605.05647

Outline


Quantum
Codeword
Noisy
quantum
channel
Quantum
error
correction
ancillary qubits
Syndrome
measurement

Qubit and Pauli Matries

- Consider the two-level quantum system: qubits. A qubit (quantum bit) is the quantum state (a unit vector) in a 2-dimensional complex vector space $\mathbb{C}^2$ with an orthonormal basis $\{|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\}$.
- The Pauli matrices

$$\{I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, Y = -iXZ\}$$

form a basis of the linear operators on a single-qubit state space.

$$X|0\rangle = |1\rangle, \ Z|1\rangle = -|1\rangle.$$

- The eigenvalues of X, Y, or Z are ± 1.
- $XY = -YX$, $XZ = -ZX$, $YZ = -ZY$.

Qubit and Pauli Matries

- Consider the two-level quantum system: qubits. A qubit (quantum bit) is the quantum state (a unit vector) in a 2-dimensional complex vector space $\mathbb{C}^2$ with an orthonormal basis $\{|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\}$.
- The Pauli matrices

$$\{I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, Y = -iXZ\}$$

form a basis of the linear operators on a single-qubit state space.

$$X|0\rangle = |1\rangle,\ Z|1\rangle = -|1\rangle.$$

- The eigenvalues of X, Y, or Z are ± 1.
- $XY = -YX$, $XZ = -ZX$, $YZ = -ZY$.

Qubit and Pauli Matries

- Consider the two-level quantum system: qubits. A qubit (quantum bit) is the quantum state (a unit vector) in a 2-dimensional complex vector space $\mathbb{C}^2$ with an orthonormal basis $\{|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\}$.
- The Pauli matrices

$$\{I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, Y = -iXZ\}$$

  form a basis of the linear operators on a single-qubit state space.

$$X|0\rangle = |1\rangle,\ Z|1\rangle = -|1\rangle.$$

- The eigenvalues of X, Y, or Z are ± 1.
- $XY = -YX$, $XZ = -ZX$, $YZ = -ZY$.

n-fold Pauli group

- n-fold Pauli group:

$$\mathcal{G}_n = \{cM_1 \otimes \cdots \otimes M_n : M_j \in \{I, X, Y, Z\}, c \in \{\pm 1, \pm i\}\}.$$

- Any elements in $\mathcal{G}_n$ has eigenvalues ± 1.
- Any two elements $g, h \in \mathcal{G}_n$ either commute or anticommute with each other.
- The weight of $E \in \mathcal{G}_n$ is the number of its nonidentity components. Ex. the weight of $X \otimes Y \otimes Z \otimes I \otimes I$ is three.

n-fold Pauli group

- n-fold Pauli group:

$$\mathcal{G}_n = \{cM_1 \otimes \cdots \otimes M_n : M_j \in \{I, X, Y, Z\}, c \in \{\pm 1, \pm i\}\}.$$

- Any elements in $\mathcal{G}_n$ has eigenvalues ± 1.
- Any two elements $g, h \in \mathcal{G}_n$ either commute or anticommute with each other.
- The weight of $E \in \mathcal{G}_n$ is the number of its nonidentity components. Ex. the weight of $X \otimes Y \otimes Z \otimes I \otimes I$ is three.

n-fold Pauli group

- n-fold Pauli group:

$$\mathcal{G}_n = \{cM_1 \otimes \cdots \otimes M_n : M_j \in \{I, X, Y, Z\}, c \in \{\pm 1, \pm i\}\}.$$

- Any elements in $\mathcal{G}_n$ has eigenvalues ± 1.
- Any two elements $g, h \in \mathcal{G}_n$ either commute or anticommute with each other.
- The weight of $E \in \mathcal{G}_n$ is the number of its nonidentity components. Ex. the weight of $X \otimes Y \otimes Z \otimes I \otimes I$ is three.

Quantum Stabilizer Codes

- $\mathcal{S} = \langle g_1, g_2, \cdots, g_{n-k} \rangle$: an Abelian subgroup of $\mathcal{G}_n$ and $-I \notin \mathcal{S}$.
- An $[[n, k, d]]$ quantum stabilizer code $\mathcal{C}(\mathcal{S})$ corresponding to the stabilizer group $\mathcal{S}$ is the 2^k-dimensional subspace of the n-qubit state space $\mathbb{C}^{2^n}$ fixed by $\mathcal{S}$ so that any error $E \in \mathcal{G}_n$ of $\mathrm{wt}(E) \leq d-1$ is detectable.

$$\mathcal{C}(\mathcal{S}) = \{|\psi\rangle \in \mathbb{C}^{2^n} : g|\psi\rangle = |\psi\rangle, \forall g \in \mathcal{S}\}.$$

- An error $E \in \mathcal{G}_n$ can be detected if it anticommutes with some stabilizer $g_j \in \mathcal{S}$:

$$g_j(E|\psi\rangle) = -Eg_j|\psi\rangle = -(E|\psi\rangle).$$

- The error syndrome of E is the binary $(n-k)$-tuple corresponding to the eigenvalues of $g_1, \ldots, g_{n-k}$.

$$+1 :\rightarrow 0$$
$$-1 :\rightarrow 1$$

Quantum Stabilizer Codes

- $\mathcal{S} = \langle g_1, g_2, \cdots, g_{n-k} \rangle$: an Abelian subgroup of $\mathcal{G}_n$ and $-I \notin \mathcal{S}$.
- An $[[n, k, d]]$ quantum stabilizer code $\mathcal{C}(\mathcal{S})$ corresponding to the stabilizer group $\mathcal{S}$ is the 2^k-dimensional subspace of the n-qubit state space $\mathbb{C}^{2^n}$ fixed by $\mathcal{S}$ so that any error $E \in \mathcal{G}_n$ of $\mathrm{wt}(E) \leq d-1$ is detectable.

$$\mathcal{C}(\mathcal{S}) = \{|\psi\rangle \in \mathbb{C}^{2^n} : g|\psi\rangle = |\psi\rangle, \forall g \in \mathcal{S}\}.$$

- An error $E \in \mathcal{G}_n$ can be detected if it anticommutes with some stabilizer $g_j \in \mathcal{S}$:

$$g_j(E|\psi\rangle) = -Eg_j|\psi\rangle = -(E|\psi\rangle).$$

- The error syndrome of E is the binary $(n-k)$-tuple corresponding to the eigenvalues of $g_1, \ldots, g_{n-k}$.

$$+1 :\rightarrow 0$$
$$-1 :\rightarrow 1$$

Quantum Stabilizer Codes

- $\mathcal{S} = \langle g_1, g_2, \cdots, g_{n-k} \rangle$: an Abelian subgroup of $\mathcal{G}_n$ and $-I \notin \mathcal{S}$.
- An $[[n, k, d]]$ quantum stabilizer code $\mathcal{C}(\mathcal{S})$ corresponding to the stabilizer group $\mathcal{S}$ is the 2^k-dimensional subspace of the n-qubit state space $\mathbb{C}^{2^n}$ fixed by $\mathcal{S}$ so that any error $E \in \mathcal{G}_n$ of $\mathrm{wt}(E) \leq d-1$ is detectable.

$$\mathcal{C}(\mathcal{S}) = \{|\psi\rangle \in \mathbb{C}^{2^n} : g|\psi\rangle = |\psi\rangle, \forall g \in \mathcal{S}\}.$$

- An error $E \in \mathcal{G}_n$ can be detected if it anticommutes with some stabilizer $g_j \in \mathcal{S}$:

$$g_j(E|\psi\rangle) = -Eg_j|\psi\rangle = -(E|\psi\rangle).$$

- The error syndrome of E is the binary $(n-k)$-tuple corresponding to the eigenvalues of $g_1, \ldots, g_{n-k}$.

$$+1 :\rightarrow 0$$
$$-1 :\rightarrow 1$$

Quantum Stabilizer Codes

- $\mathcal{S} = \langle g_1, g_2, \cdots, g_{n-k} \rangle$: an Abelian subgroup of $\mathcal{G}_n$ and $-I \notin \mathcal{S}$.
- An $[[n, k, d]]$ quantum stabilizer code $\mathcal{C}(\mathcal{S})$ corresponding to the stabilizer group $\mathcal{S}$ is the 2^k-dimensional subspace of the n-qubit state space $\mathbb{C}^{2^n}$ fixed by $\mathcal{S}$ so that any error $E \in \mathcal{G}_n$ of $\mathrm{wt}(E) \leq d-1$ is detectable.

$$\mathcal{C}(\mathcal{S}) = \{|\psi\rangle \in \mathbb{C}^{2^n} : g|\psi\rangle = |\psi\rangle, \forall g \in \mathcal{S}\}.$$

- An error $E \in \mathcal{G}_n$ can be detected if it anticommutes with some stabilizer $g_j \in \mathcal{S}$:

$$g_j(E|\psi\rangle) = -Eg_j|\psi\rangle = -(E|\psi\rangle).$$

- The error syndrome of E is the binary $(n-k)$-tuple corresponding to the eigenvalues of $g_1, \ldots, g_{n-k}$.

$$+1 :\to 0$$
$$-1 :\to 1$$

- The eigenstate of $\mathcal{S} \subset \mathcal{G}_n$ is called a stabilizer state if $k = 0$ or $\mathcal{S} = \langle g_1, g_2, \cdots, g_n \rangle$.

- The eigenstate of $\mathcal{S} \subset \mathcal{G}_n$ is called a stabilizer state if $k = 0$ or $\mathcal{S} = \langle g_1, g_2, \cdots, g_n \rangle$.
- The Einstein-Podolsky-Rosen (EPR) pair

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

is stabilized by $X \otimes X$ and $Z \otimes Z$.

Calderbank-Shor-Steane (CSS) Codes

- For simplicity, we consider an $[[n = 2\gamma + 1, 1]]$ CSS code $\mathcal{Q}$ that encodes one logical qubit in n physical qubits.

Calderbank-Shor-Steane (CSS) Codes

- For simplicity, we consider an $[[n = 2\gamma + 1, 1]]$ CSS code $\mathcal{Q}$ that encodes one logical qubit in n physical qubits.
- Suppose $\mathcal{Q}$ is defined by an $[n, n - \gamma]$ classical dual-containing code $\mathcal{C}_1(\supseteq \mathcal{C}_1^{\perp})$ and let H_1 be its binary parity-check matrix of dimension $n \times \gamma$. Let $[\mathrm{M}]_{i,j}$ denote the (i, j) entry of a matrix M. Then the Z and X stabilizer generators of $\mathcal{Q}$ are

$$g_i = \bigotimes_{j=1}^{n} Z^{[\mathrm{H}_1]_{i,j}}$$

and

$$g_{\gamma+i} = \bigotimes_{j=1}^{n} X^{[\mathrm{H}_1]_{i,j}},$$

respectively, for $i = 1, \cdots, \gamma$.

Calderbank-Shor-Steane (CSS) Codes

- For simplicity, we consider an $[[n = 2\gamma + 1, 1]]$ CSS code $\mathcal{Q}$ that encodes one logical qubit in n physical qubits.
- Suppose $\mathcal{Q}$ is defined by an $[n, n-\gamma]$ classical dual-containing code $\mathcal{C}_1(\supseteq \mathcal{C}_1^{\perp})$ and let H_1 be its binary parity-check matrix of dimension $n \times \gamma$. Let $[\mathrm{M}]_{i,j}$ denote the (i,j) entry of a matrix M. Then the Z and X stabilizer generators of $\mathcal{Q}$ are

$$g_i = \bigotimes_{j=1}^{n} Z^{[\mathrm{H}_1]_{i,j}}$$

and

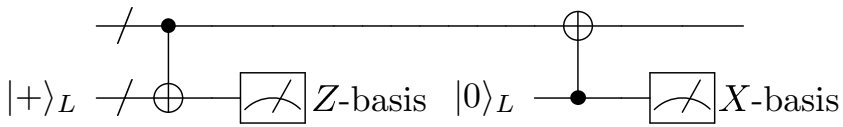
$$g_{\gamma+i} = \bigotimes_{j=1}^{n} X^{[\mathrm{H}_1]_{i,j}},$$

respectively, for $i = 1, \cdots, \gamma$.

- Let $|0\rangle_L, |1\rangle_L$ denote the encoded $|0\rangle, |1\rangle$. Let $|+\rangle_L = \frac{1}{\sqrt{2}}(|0\rangle_L + |1\rangle_L)$.
- Let $\bar{X}$, $\bar{Z}$ denote the logical operators of $\mathcal{Q}$.

Steane Syndrome Extraction

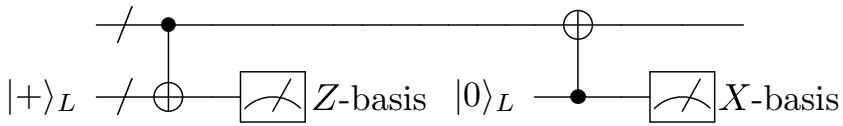
- Steane syndrome extraction



- Two ancilla states are required: $|+\rangle_L$, $|0\rangle_L$.

Steane Syndrome Extraction

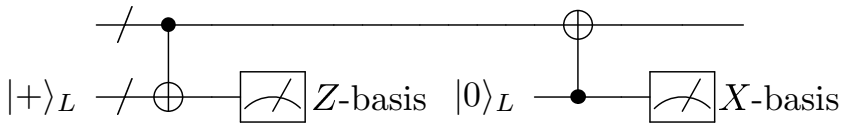
- Steane syndrome extraction



- Two ancilla states are required: $|+\rangle_L$, $|0\rangle_L$.
- Suppose a Pauli error X_e occurs on a quantum codeword, where $e \in \mathbb{Z}_2^n$ is a binary n-tuple (row vector) indicating which qubits have X errors.
- Ex. $X_{101} = X \otimes I \otimes X$.

Steane Syndrome Extraction

- Steane syndrome extraction



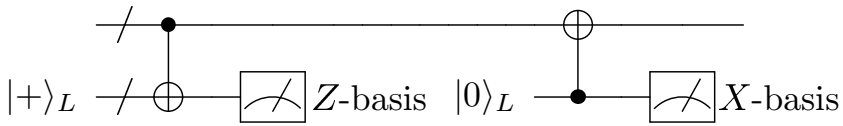
- Two ancilla states are required: $|+\rangle_L$, $|0\rangle_L$.
- Suppose a Pauli error X_e occurs on a quantum codeword, where $e \in \mathbb{Z}_2^n$ is a binary n-tuple (row vector) indicating which qubits have X errors.
- Ex. $X_{101} = X \otimes I \otimes X$.
- Then its (binary) error syndrome $s_X \in \mathbb{Z}_2^\gamma$, which corresponds to the eigenvalues of $g_1, \cdots, g_\gamma$, is given by

$$s_X^T = \mathrm{H}_1 m^T = \mathrm{H}_1 e^T,$$

where m is the binary measurement outcome vector.

Steane Syndrome Extraction

- Steane syndrome extraction



- Two ancilla states are required: $|+\rangle_L$, $|0\rangle_L$.
- Suppose a Pauli error X_e occurs on a quantum codeword, where $e \in \mathbb{Z}_2^n$ is a binary n-tuple (row vector) indicating which qubits have X errors.
- Ex. $X_{101} = X \otimes I \otimes X$.
- Then its (binary) error syndrome $s_X \in \mathbb{Z}_2^\gamma$, which corresponds to the eigenvalues of $g_1, \cdots, g_\gamma$, is given by

$$s_X^T = \mathrm{H}_1 m^T = \mathrm{H}_1 e^T,$$

  where m is the binary measurement outcome vector.
- The Z error syndrome is defined similarly: $s_Z \in \mathbb{Z}_2^\gamma$.

CSS State Preparation

- The two ancillas $|+\rangle_L$ and $|0\rangle_L$ are actually stabilizer states of $\mathcal{Q}$ by including logical operator $\bar{X}$ or $\bar{Z}$ in with the stabilizer generators. Namely, $|+\rangle_L$ is stabilized by

$$\langle g_1, \cdots, g_{n-1}, \bar{X} \rangle,$$

and $|0\rangle_L$ is stabilized by

$$\langle g_1, \cdots, g_{n-1}, \bar{Z} \rangle.$$

CSS State Preparation

- The two ancillas $|+\rangle_L$ and $|0\rangle_L$ are actually stabilizer states of $\mathcal{Q}$ by including logical operator $\bar{X}$ or $\bar{Z}$ in with the stabilizer generators. Namely, $|+\rangle_L$ is stabilized by

$$\langle g_1, \cdots, g_{n-1}, \bar{X} \rangle,$$

and $|0\rangle_L$ is stabilized by

$$\langle g_1, \cdots, g_{n-1}, \bar{Z} \rangle.$$

- The stabilizer states of any Calderbank-Shor-Steane (CSS) codes can be prepared by quantum circuits with CNOT and H gates only.

$$\mathrm{H} = [\mathrm{H}_X|\mathrm{H}_Z] = \left(\begin{array}{ccc|ccc} \mathrm{I}_r & \mathrm{A} & \mathrm{B} & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathrm{D} & \mathrm{I}_s & \mathrm{F} \end{array}\right),$$

$$\mathrm{H}' = \left(\begin{array}{ccc|ccc} \mathrm{I}_r & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathrm{I}_s & 0 \end{array}\right)$$

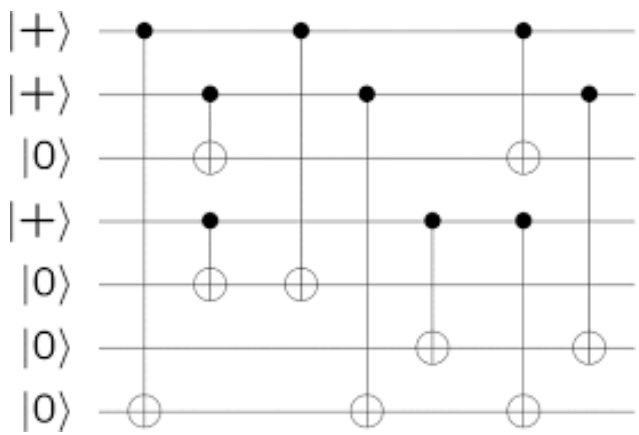
Example

- The $[[7, 1, 3]]$ Steane code has stabilizer generators

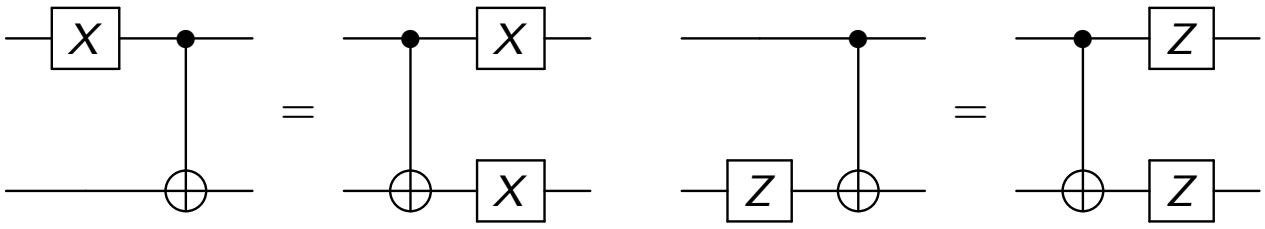
$$
\begin{aligned}
g_1 &= Z_1 Z_4 Z_5 Z_7, \\
g_2 &= Z_2 Z_4 Z_6 Z_7, \\
g_3 &= Z_3 Z_5 Z_6 Z_7, \\
g_4 &= X_1 X_4 X_5 X_7, \\
g_5 &= X_2 X_4 X_6 X_7, \\
g_6 &= X_3 X_5 X_6 X_7,
\end{aligned}
$$

  and logical operators $\bar{X} = X_1 X_2 X_4$, $\bar{Z} = Z_1 Z_2 Z_4$.

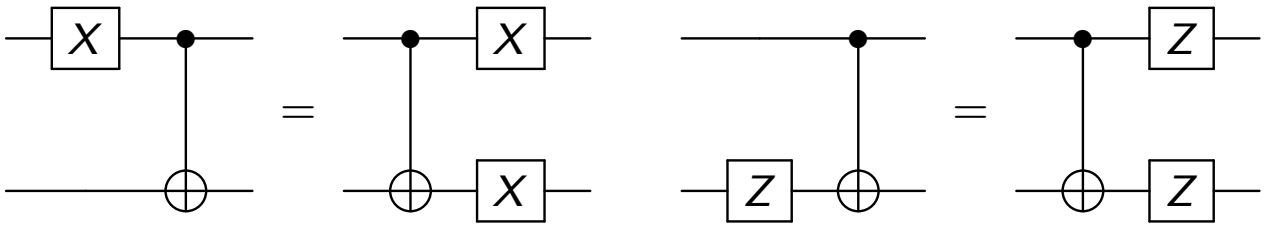
- $|\bar{0}\rangle$ of the $[[7, 1, 3]]$ Steane code: $(|+\rangle = H|0\rangle)$



Errors Propagate through *CNOT* Gates

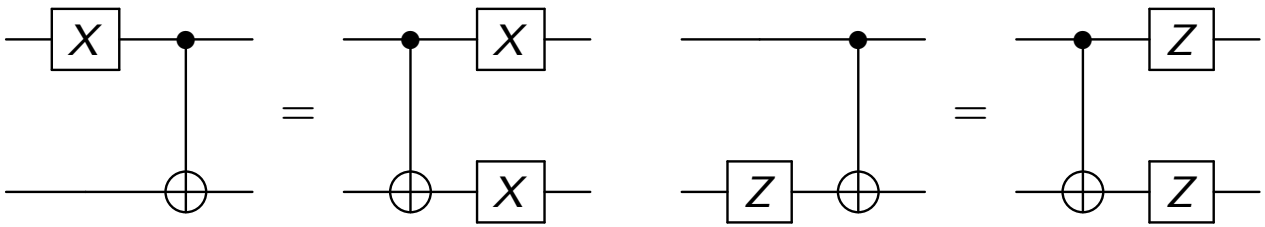


Errors Propagate through *CNOT* Gates



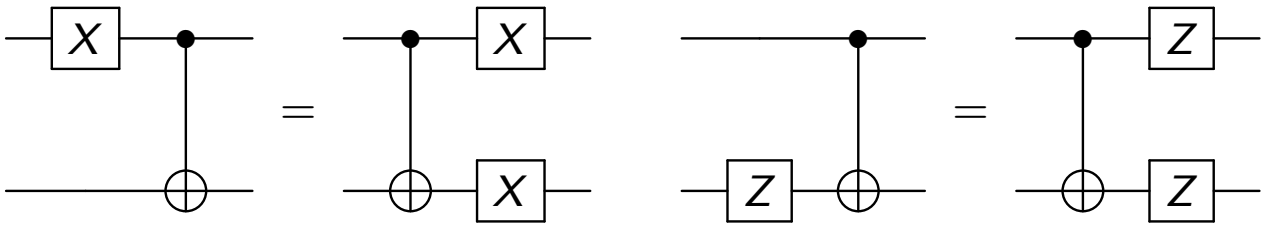
- A procedure is fault-tolerant if it has the property that if only one component (or more generally, a small number of components) in the procedure fails, the errors produced by this failure are not transformed by the procedure into an uncorrectable error.

Errors Propagate through *CNOT* Gates



- A procedure is fault-tolerant if it has the property that if only one component (or more generally, a small number of components) in the procedure fails, the errors produced by this failure are not transformed by the procedure into an uncorrectable error.
- In general, we don't know how to fault-tolerantly prepare ancilla states of an arbitrary CSS code.

Errors Propagate through *CNOT* Gates



- A procedure is fault-tolerant if it has the property that if only one component (or more generally, a small number of components) in the procedure fails, the errors produced by this failure are not transformed by the procedure into an uncorrectable error.
- In general, we don't know how to fault-tolerantly prepare ancilla states of an arbitrary CSS code.
- If we have the correct error syndrome of a polluted ancilla, ex. $|0\rangle_L$, we can prepare a clean one.

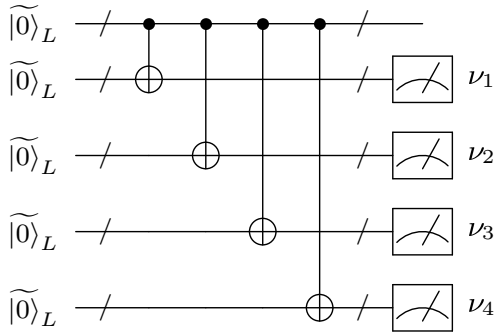
What do we do?

What do we do?

Main idea: Extract the correct error syndromes of some target ancillas from a bunch of noisy ancillas.

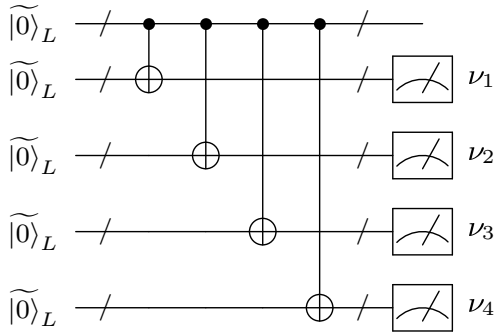
Distillation by Classical Codes

- Suppose we are given a bunch of imperfect ancillas of some CSS code defined by H_1.



Distillation by Classical Codes

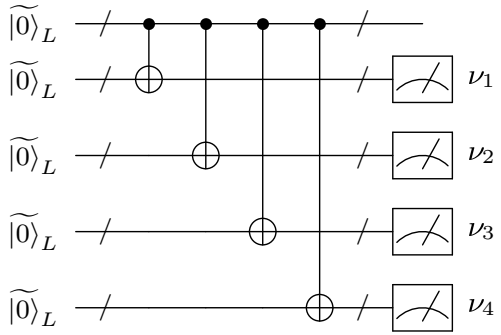
- Suppose we are given a bunch of imperfect ancillas of some CSS code defined by H_1.



- Let $H_2 = [A^T \ I_r]$ be a parity-check matrice of a classical $[m, r, 2t+1]$ linear block code $\mathcal{C}_2$ in the systematic form.

Distillation by Classical Codes

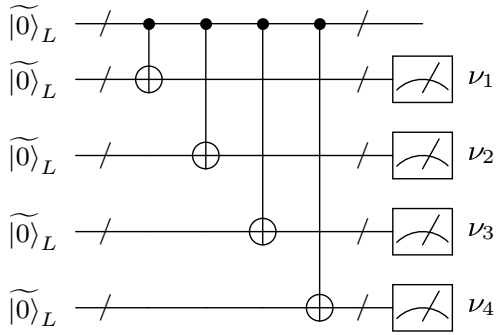
- Suppose we are given a bunch of imperfect ancillas of some CSS code defined by H_1.



- Let $H_2 = [A^T \ I_r]$ be a parity-check matrice of a classical $[m, r, 2t+1]$ linear block code $\mathcal{C}_2$ in the systematic form.
- If $[A]_{i,j} = 1$, we apply transversal CNOTs from the i-th ancilla to the $(k+j)$-th ancilla. As a consequence, X errors on the target ancillas will propagate to the parity-check ancillas via the CNOTs. Ex. the [5,1,5] repetition code.

Distillation by Classical Codes

- Suppose we are given a bunch of imperfect ancillas of some CSS code defined by H_1.



- Let $H_2 = [A^T \ I_r]$ be a parity-check matrice of a classical $[m, r, 2t+1]$ linear block code $\mathcal{C}_2$ in the systematic form.
- If $[A]_{i,j} = 1$, we apply transversal CNOTs from the i-th ancilla to the $(k+j)$-th ancilla. As a consequence, X errors on the target ancillas will propagate to the parity-check ancillas via the CNOTs. Ex. the [5,1,5] repetition code.
- The error syndrome of the target ancilla are hidden in the error syndromes of the other four parity-check ancillas.

$$\mathrm{H}_2 \begin{bmatrix} e_1 \mathrm{H}_1^T \\ \vdots \\ e_m \mathrm{H}_1^T \end{bmatrix} = \begin{bmatrix} \nu_1 \mathrm{H}_1^T \\ \vdots \\ \nu_r \mathrm{H}_1^T \end{bmatrix}.$$

- $\nu_1, \ldots, \nu_r$ are measured.
- $e_1 \mathrm{H}_1^T, \ldots, e_m \mathrm{H}_1^T$ are still unknown.

Distillation Protocol by Classical Codes

- Our distillation protocol for CSS stabilizer states by classical codes (Protocol I) involves two rounds of error corrections: one for X errors and one for Z errors.

Distillation Protocol by Classical Codes

- Our distillation protocol for CSS stabilizer states by classical codes (Protocol I) involves two rounds of error corrections: one for X errors and one for Z errors.
- Suppose we are using an $[m, r]$ code.

1 (encoding for the first round) Divide the noisy ancillas up into groups of m. Coupling the qubits according to the parity-check matrix. Then measure all the qubits of each of the parity-checking ancillas.

Distillation Protocol by Classical Codes

- Our distillation protocol for CSS stabilizer states by classical codes (Protocol I) involves two rounds of error corrections: one for X errors and one for Z errors.
- Suppose we are using an $[m, r]$ code.

1 (encoding for the first round) Divide the noisy ancillas up into groups of m. Coupling the qubits according to the parity-check matrix. Then measure all the qubits of each of the parity-checking ancillas.

2 (decoding) We can then use the classical codes $\mathcal{C}_1$ (or $\mathcal{C}_1^{\perp}$ if we are distilling $|0\rangle_L$ or $|1\rangle_L$) and $\mathcal{C}_2$ to locate X errors among the m ancillas, and correct them (or just keep track of them). The rate of X errors goes from p to cp^{t+1} for some c. The rate of Z errors on the remaining k ancillas will increase to $\sim (\beta + 1)p$.

Distillation Protocol by Classical Codes

- Our distillation protocol for CSS stabilizer states by classical codes (Protocol I) involves two rounds of error corrections: one for X errors and one for Z errors.
- Suppose we are using an $[m, r]$ code.

1 (encoding for the first round) Divide the noisy ancillas up into groups of m. Coupling the qubits according to the parity-check matrix. Then measure all the qubits of each of the parity-checking ancillas.

2 (decoding) We can then use the classical codes $\mathcal{C}_1$ (or $\mathcal{C}_1^{\perp}$ if we are distilling $|0\rangle_L$ or $|1\rangle_L$) and $\mathcal{C}_2$ to locate X errors among the m ancillas, and correct them (or just keep track of them). The rate of X errors goes from p to cp^{t+1} for some c. The rate of Z errors on the remaining k ancillas will increase to $\sim (\beta + 1)p$.

3 Of a fraction k/m, we again divide them up into groups of m. It is very important that ancillas that were grouped together in the first round are not grouped together in the second round, because their errors are correlated. Then do similar steps of 1 and 2.

Distillation Protocol by Classical Codes

- Our distillation protocol for CSS stabilizer states by classical codes (Protocol I) involves two rounds of error corrections: one for X errors and one for Z errors.
- Suppose we are using an $[m, r]$ code.

1 (encoding for the first round) Divide the noisy ancillas up into groups of m. Coupling the qubits according to the parity-check matrix. Then measure all the qubits of each of the parity-checking ancillas.

2 (decoding) We can then use the classical codes $\mathcal{C}_1$ (or $\mathcal{C}_1^{\perp}$ if we are distilling $|0\rangle_L$ or $|1\rangle_L$) and $\mathcal{C}_2$ to locate X errors among the m ancillas, and correct them (or just keep track of them). The rate of X errors goes from p to cp^{t+1} for some c. The rate of Z errors on the remaining k ancillas will increase to $\sim (\beta+1)p$.

3 Of a fraction k/m, we again divide them up into groups of m. It is very important that ancillas that were grouped together in the first round are not grouped together in the second round, because their errors are correlated. Then do similar steps of 1 and 2.

4 The rate of Z errors will go from $(\beta+1)p$ to $c((\beta+1)p)^{t+1} = c'p^{t+1}$, and the rate of X errors will go from cp^{t+1} to $(\beta+1)cp^{t+1} = c''p^{t+1}$. (So the rate of an arbitrary Pauli error is roughly $\tilde{c}p^{t+1}$ for some $\tilde{c}$.)

Example

- The $[[7, 1, 3]]$ Steane code has stabilizer generators

$$
\begin{aligned}
g_1 &= Z_1 Z_4 Z_5 Z_7, \\
g_2 &= Z_2 Z_4 Z_6 Z_7, \\
g_3 &= Z_3 Z_5 Z_6 Z_7, \\
g_4 &= X_1 X_4 X_5 X_7, \\
g_5 &= X_2 X_4 X_6 X_7, \\
g_6 &= X_3 X_5 X_6 X_7,
\end{aligned}
$$

  and logical operators $\bar{X} = X_1 X_2 X_4$, $\bar{Z} = Z_1 Z_2 Z_4$.

- Suppose we have three noisy Steane codewords $E_1|0\rangle_L$, $E_2|0\rangle_L$, and $E_3|0\rangle_L$, where $E_1 = X_1 X_2$, $E_2 = X_3$ and $E_3 = X_4$.
- Apparently E_1 is an uncorrectable error for Steane code.

- After the (perfect) distillation circuit by the $[3,1,3]$ code, the errors become $E_1' = E_1$, $E_2' = E_1E_2 = X_1X_2X_3$, and $E_3' = E_1E_3 = X_1X_2X_4 = \bar{X}$.
- Then measuring bitwise the second and the third codewords, and calculating the parities of g_1, g_2, g_3 and $\bar{Z}$, we have their syndrome bits

$$1111,$$
$$0001.$$

- Now we can use the parity check matrix of the $[3,1,3]$ repetition code to recover the four syndrome bits of the first codeword:

$$0001.$$

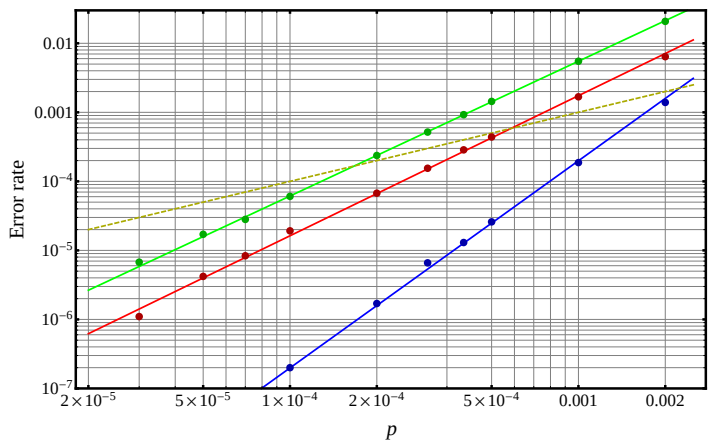
- Since the fourth bit is 1, we apply $\bar{X}$ to the first codeword to correct the logical error and the final state is

$$X_4|0\rangle_L,$$

which has a correctable residual error X_4. Thus we have fault-tolerantly prepared an ancilla $|0\rangle_L$ in this case.

Example

- Assume the distillation circuit is perfect.
- Depolarizing channel with parameter p: An error X, Y, or Z occurs with probability $p/3$ and no error occurs with probability $1-p$.
- Ancilla distillation by 1) $[7,4,3]$ Hamming code (green); 2) $[3,1,3]$ repetition code (red); 3) $[5,1,5]$ repetition code (blue). The dashed line is the rate without distillation.



- If p is small enough, our protocol will work. As can be seen in this logarithmic plot, each curve appears linear with slope $t+1$ and the "threshold" for each code is specified by $\log p_{\text{th}} = -\frac{1}{t}\log \tilde{c}$.

It is also possible to do distillation by using quantum CSS codes. See arXiv:1605.05647.

Let's go to its applications.

Ancilla Saving Protocol

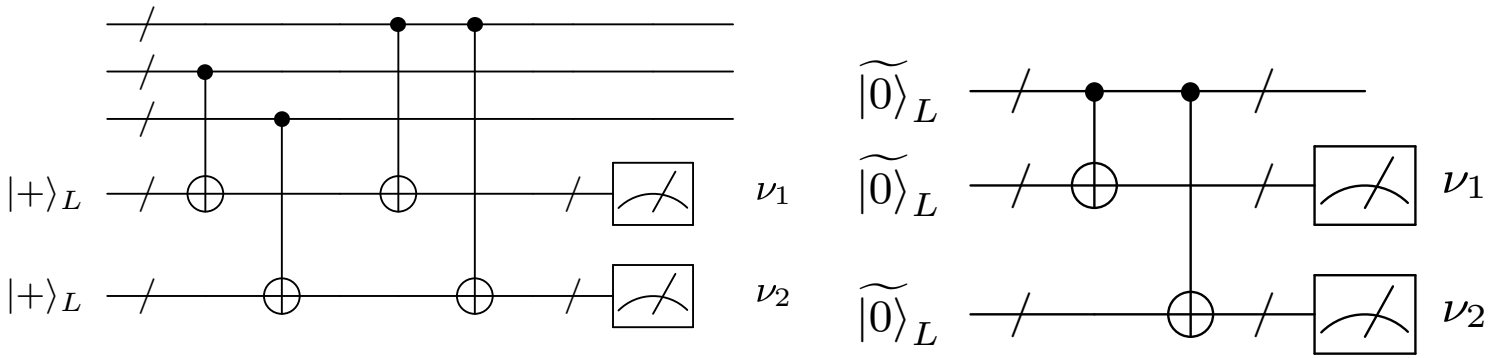
- Clean ancillas $|0\rangle_L$ and $|+\rangle_L$ are expensive resources. We would like to save them during syndrome measurement as long as errors do not accumulate seriously.

Ancilla Saving Protocol

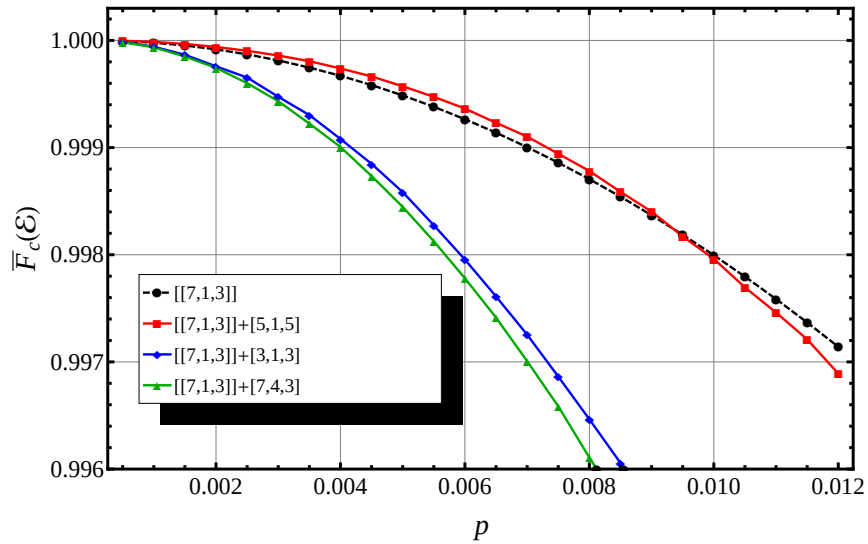
- Clean ancillas $|0\rangle_L$ and $|+\rangle_L$ are expensive resources. We would like to save them during syndrome measurement as long as errors do not accumulate seriously.
- Suppose we have m codewords $|\psi_1\rangle, \cdots, |\psi_m\rangle$ of the $[[n, 1]]$ CSS code $\mathcal{Q}$ defined by H_1. Our goal here is to estimate the m error syndromes by using only r $(< m)$ clean ancillas $|+\rangle_L$.

Ancilla Saving Protocol

- Clean ancillas $|0\rangle_L$ and $|+\rangle_L$ are expensive resources. We would like to save them during syndrome measurement as long as errors do not accumulate seriously.
- Suppose we have m codewords $|\psi_1\rangle, \cdots, |\psi_m\rangle$ of the $[[n, 1]]$ CSS code $\mathcal{Q}$ defined by H_1. Our goal here is to estimate the m error syndromes by using only r $(< m)$ clean ancillas $|+\rangle_L$.



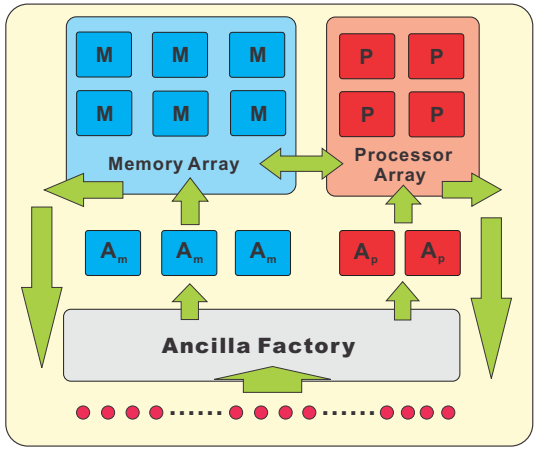
- When the ancilla consumption rate is fixed, we can increase the frequency of quantum error correction with the ancilla saving protocol, which is equivalent to lowering the error rate on the data qubits.



- As can be seen, applying the ancilla saving protocol with the $[5, 1, 5]$ is better than the original scheme for $p < 0.00925$. Of course, this fidelity gain was at the cost of some additional CNOT gates and classical decoding steps.

Teleportation-based FTQC Scheme

- T. A. Brun, Y.-C. Zheng, K.-C. Hsu, J. Job, and C.-Y. Lai, "Teleportation-Based Fault-tolerant Quantum Computation in Multi-qubit Large Block Codes," arXiv:1504.03913.



  - M: memory blocks of large stabilizer codes
  - P: concatenated $[[15, 1, 3]]$ punctured Reed-Muller codes.
  - Ancilla factory : constantly prepares the ancilla qubits for error correction and teleportation, such as $|\bar{0}\rangle$, which are CSS stabilizer states.

Measuring a Logical X or Z operator

1. Suppose we wish to measure $\bar{X}_i \bar{X}_j$. The logical qubits i and j of the X ancilla are prepared in the state

$$|\Phi_+\rangle_L = \frac{1}{\sqrt{2}}(|0_i 0_j\rangle_L + |1_i 1_j\rangle_L),$$

   which is a joint $+1$ eigenstate of $\bar{X}_i \bar{X}_j$ and $\bar{Z}_i \bar{Z}_j$, and the other logical qubits are prepared in the state $|0\rangle_L$.

2. Suppose we wish to measure $\bar{X}_i \bar{Z}_j$ on logical qubits i and j.
   - If $i \neq j$, logical qubit i of the X ancilla and logical qubit j of the Z ancilla at step 1) are prepared in the entangled state

$$|\Omega_{ij}\rangle_L = 1/2\,(|0_i 0_j\rangle_L + |0_i 1_j\rangle_L + |1_i 0_j\rangle_L - |1_i 1_j\rangle_L)\,,$$

     which is a joint $+1$ eigenstate of $\bar{X}_i \bar{Z}_j$ and $\bar{Z}_i \bar{X}_j$, while the other logical qubits of the X or Z ancillas are prepared in the state $|0\rangle_L$ or $|+\rangle_L$, respectively.
   - If $i = j$, the ancilla is prepared in a joint $+1$ eigenstate of $\bar{Y}_i \bar{Z}_i$ and $\bar{Z}_i \bar{X}_i$.

Multipartite Entanglement Purification

- In the task of multipartite entanglement purification for CSS stabilizer states by local operations and classical communication (LOCC), each qubit is considered as a single party.

Multipartite Entanglement Purification

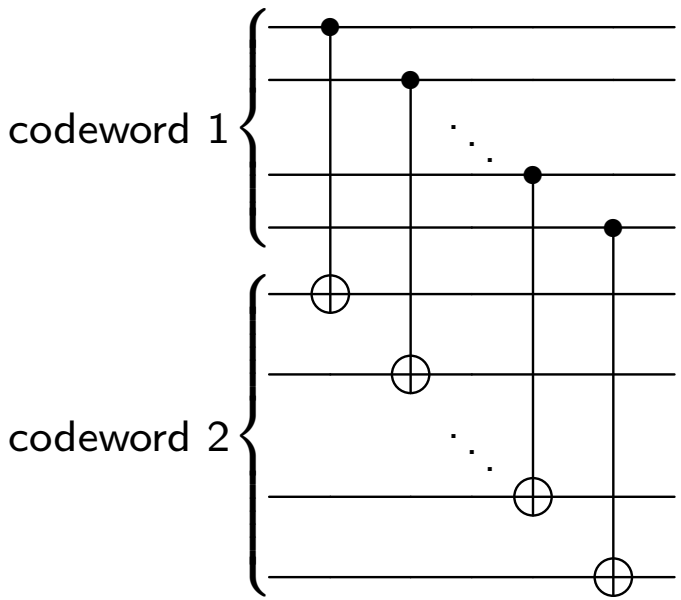
- In the task of multipartite entanglement purification for CSS stabilizer states by local operations and classical communication (LOCC), each qubit is considered as a single party.
- These parties share several copies of noisy CSS stabilizer states. The goal is to purify a small subset of these states by LOCC only.

Transversality and LOCC

- All the operations we need in our previous distillation protocols are transversal controlled-NOT (CNOT) gates, bitwise single-qubit measurements, classical decoding, and correction by Pauli operators.

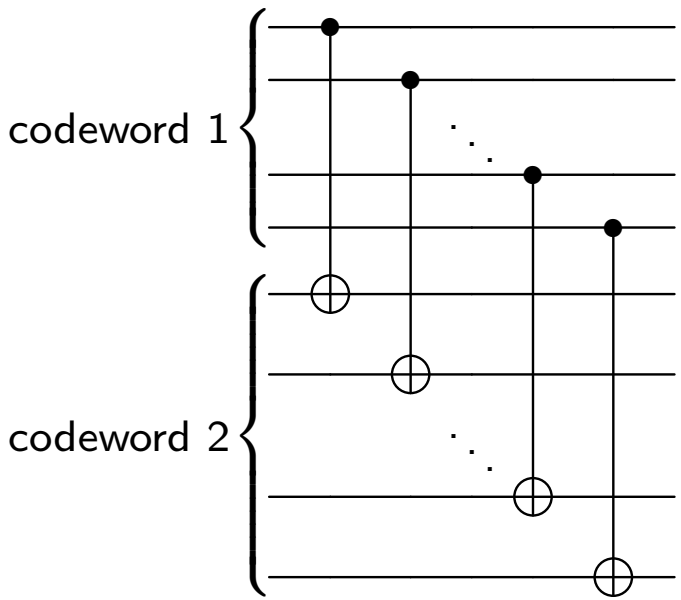
Transversality and LOCC

- All the operations we need in our previous distillation protocols are transversal controlled-NOT (CNOT) gates, bitwise single-qubit measurements, classical decoding, and correction by Pauli operators.
- The encoded CNOT gate is in a bitwise fashion.



Transversality and LOCC

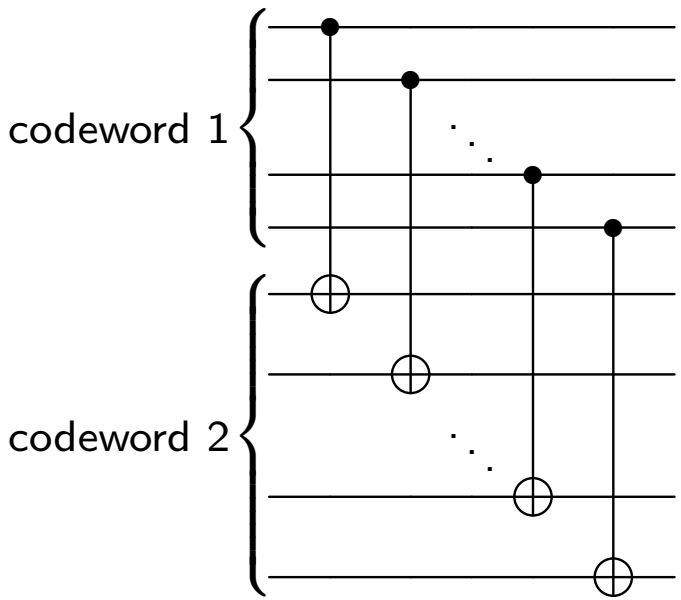
- All the operations we need in our previous distillation protocols are transversal controlled-NOT (CNOT) gates, bitwise single-qubit measurements, classical decoding, and correction by Pauli operators.
- The encoded CNOT gate is in a bitwise fashion.



- These features for fault-tolerance are similar to the constraint of LOCC in the multipartite protocol.

Transversality and LOCC

- All the operations we need in our previous distillation protocols are transversal controlled-NOT (CNOT) gates, bitwise single-qubit measurements, classical decoding, and correction by Pauli operators.
- The encoded CNOT gate is in a bitwise fashion.



- These features for fault-tolerance are similar to the constraint of LOCC in the multipartite protocol.
- Our CSS state distillation protocols are naturally also multipartite entanglement purification protocols for CSS states.

Conclusion

- When the circuit is imperfect, need another classical code to encode the error syndrome as in

  A. Ashikhmin, C.-Y. Lai, and T. A. Brun, "Robust quantum error syndrome extraction by classical coding," in Proceedings of IEEE International Symposium on Information Theory (ISIT 2014), pp. 546-550, June 2014 in Honolulu, Hawaii, USA.

  .... in Preparation.
- Relation between the distillation protocol and compressed sensing?

Thank You!