

Title: Adding entanglement to quantum error-correcting codes

Date: Apr 14, 2010 04:00 PM

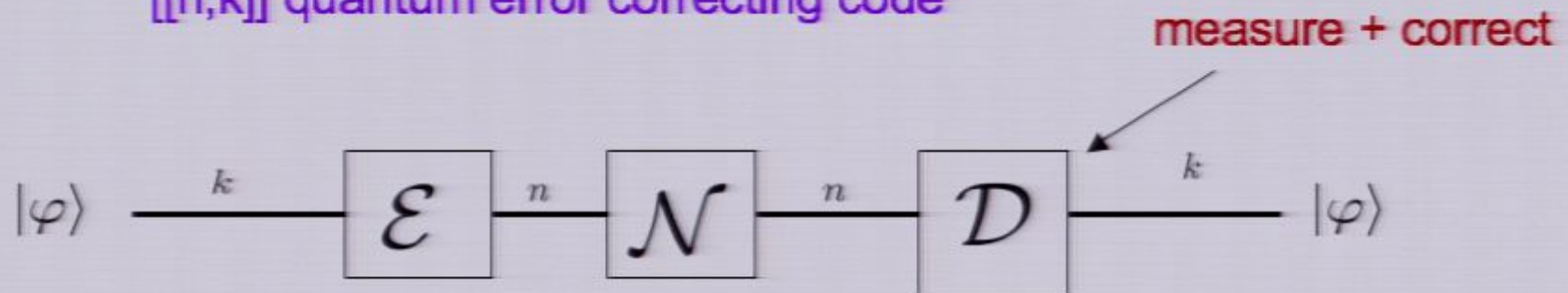
URL: <http://pirsa.org/10040029>

Abstract: Shared entanglement between sender and receiver can enable more errors to be corrected than with a standard quantum error-correcting code. This extra error correction can be used either to boost the rate of the code--commonly seen in quantum codes constructed from classical linear codes--or to increase the error-correcting power of the code (as represented by, for example, the code distance). We will see how adding extra entanglement to a given quantum code can increase its distance, and discuss the optimization problem in maximizing the effectiveness of a given amount of added entanglement. We will also briefly examine some applications of entanglement-assistance to particular types of codes, such as LDPC codes and convolutional codes.

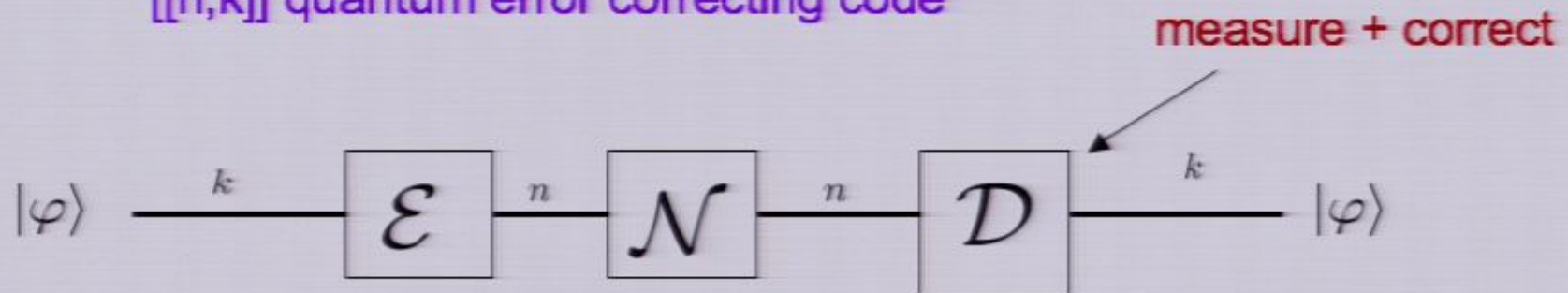
Adding Entanglement to Quantum Error-Correcting Codes

Todd A. Brun and Ching-Yi Lai
Communication Sciences Institute

[[n,k]] quantum error correcting code



[[n,k]] quantum error correcting code



Discretization
of errors

$$\boxed{\mathcal{N}} = \left\{ \boxed{N_u} : u \in S \subset \mathbb{Z}_2^{2n} \right\} \text{ Pauli group}$$

$$n=3 \quad N_{\underbrace{011}_Z \underbrace{110}_X} = Z^0 X^1 \otimes Z^1 X^1 \otimes Z^1 X^0 := X \otimes Y \otimes Z$$

Pauli unitaries

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

- The **symplectic** product $\odot : \mathbb{Z}_2^{2n} \times \mathbb{Z}_2^{2n} \rightarrow \mathbb{Z}_2^{2n}$ is defined by

$$(z|x) \odot (z'|x')^T = zx'^T + xz'^T$$

e.g. $(010|001) \odot (101|111)^T = 1 + 1 = 0$

- The **symplectic** product $\odot : \mathbb{Z}_2^{2n} \times \mathbb{Z}_2^{2n} \rightarrow \mathbb{Z}_2^{2n}$ is defined by

$$(z|x) \odot (z'|x')^T = zx'^T + xz'^T$$

e.g. $(010|001) \odot (101|111)^T = 1 + 1 = 0$

- N_u and N_v commute (anti-commute) iff $u \odot v^T = 0$ (1)

$N_{(010|001)} = IZX$ **and** $N_{(101|111)} = YXY$ **commute**

- The **symplectic** product $\odot : \mathbb{Z}_2^{2n} \times \mathbb{Z}_2^{2n} \rightarrow \mathbb{Z}_2^{2n}$ is defined by

$$(z|x) \odot (z'|x')^T = zx'^T + xz'^T$$

e.g. $(010|001) \odot (101|111)^T = 1 + 1 = 0$

- N_u and N_v commute (anti-commute) iff $u \odot v^T = 0$ (1)

$N_{(010|001)} = IZX$ **and** $N_{(101|111)} = YXY$ **commute**

- ★ An $[[n,k]]$ quantum error correcting code is described by a $(n-k) \times 2n$ parity check matrix H . Its rowspace $B(H)$ is an **isotropic** subspace of \mathbb{Z}_2^{2n}

$$u \odot v^T = 0, \quad \forall u, v \in B(H)$$

Classical symplectic codes

- The **symplectic** product $\odot : \mathbb{Z}_2^{2n} \times \mathbb{Z}_2^{2n} \rightarrow \mathbb{Z}_2^{2n}$ is defined by

$$(z|x) \odot (z'|x')^T = zx'^T + xz'^T$$

e.g. $(010|001) \odot (101|111)^T = 1 + 1 = 0$

- N_u and N_v commute (anti-commute) iff $u \odot v^T = 0$ (1)

$N_{(010|001)} = IZX$ and $N_{(101|111)} = YXY$ commute

- ★ An $[[n,k]]$ quantum error correcting code is described by a $(n-k) \times 2n$ parity check matrix H . Its rowspace $B(H)$ is an **isotropic** subspace of \mathbb{Z}_2^{2n}

$$u \odot v^T = 0, \quad \forall u, v \in B(H)$$

$n=5, k=1$

e.g. $H = \left(\begin{array}{ccccc|ccccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{array} \right) \sim \left(\begin{array}{ccccc} Z & Z & X & I & X \\ X & Z & Z & X & I \\ I & X & Z & Z & X \\ X & I & X & Z & Z \end{array} \right)$

commuting
stabilizer
generators

★ $C = B^\perp = \{u : u \odot v^T = 0, \quad \forall v \in B\}$

$B \subseteq B^\perp \iff C^\perp \subseteq C$ dual containing code

Quantum stabilizer codes

- The code space $\mathcal{E}(\mathcal{H}_2^{\otimes k}) \subset \mathcal{H}_2^{\otimes n}$ is defined as the simultaneous +1 eigenspace of the stabilizer operators $\{N_u : u \in C^\perp\} \equiv S$

- The correctable error set E is defined by: 

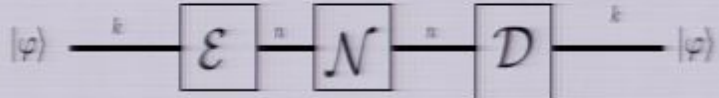


If E_1 and E_2 are in E , then at least one of the two conditions hold:

- $E_2^t E_1 \notin Z(S)$ distinct error syndromes
- $E_2^t E_1 \in S$ degenerate code

Quantum stabilizer codes

- The code space $\mathcal{E}(\mathcal{H}_2^{\otimes k}) \subset \mathcal{H}_2^{\otimes n}$ is defined as the simultaneous +1 eigenspace of the stabilizer operators $\{N_u : u \in C^\perp\} \equiv S$

- The correctable error set E is defined by: 



If E_1 and E_2 are in E , then at least one of the two conditions hold:

1) $E_2^t E_1 \notin Z(S)$ distinct error syndromes

2) $E_2^t E_1 \in S$ degenerate code

e.g. error $u = (00010|00010)$ Y error on 4th q-bit

$$\left(\begin{array}{ccccc|ccccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{array} \right) \odot (00010|00010)^T = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

Quantum stabilizer codes

- The code space $\mathcal{E}(\mathcal{H}_2^{\otimes k}) \subset \mathcal{H}_2^{\otimes n}$ is defined as the simultaneous +1 eigenspace of the stabilizer operators $\{N_u : u \in C^\perp\} \equiv S$

- The correctable error set E is defined by: $|\varphi\rangle \xrightarrow{k} \boxed{\mathcal{E}} \xrightarrow{n} \boxed{\mathcal{N}} \xrightarrow{n} \boxed{\mathcal{D}} \xrightarrow{k} |\varphi\rangle$



If E_1 and E_2 are in E , then at least one of the two conditions hold:

1) $E_2^t E_1 \notin Z(S)$ distinct error syndromes

2) $E_2^t E_1 \in S$ degenerate code

e.g. error $u = (00010|00010)$ Y error on 4th q-bit

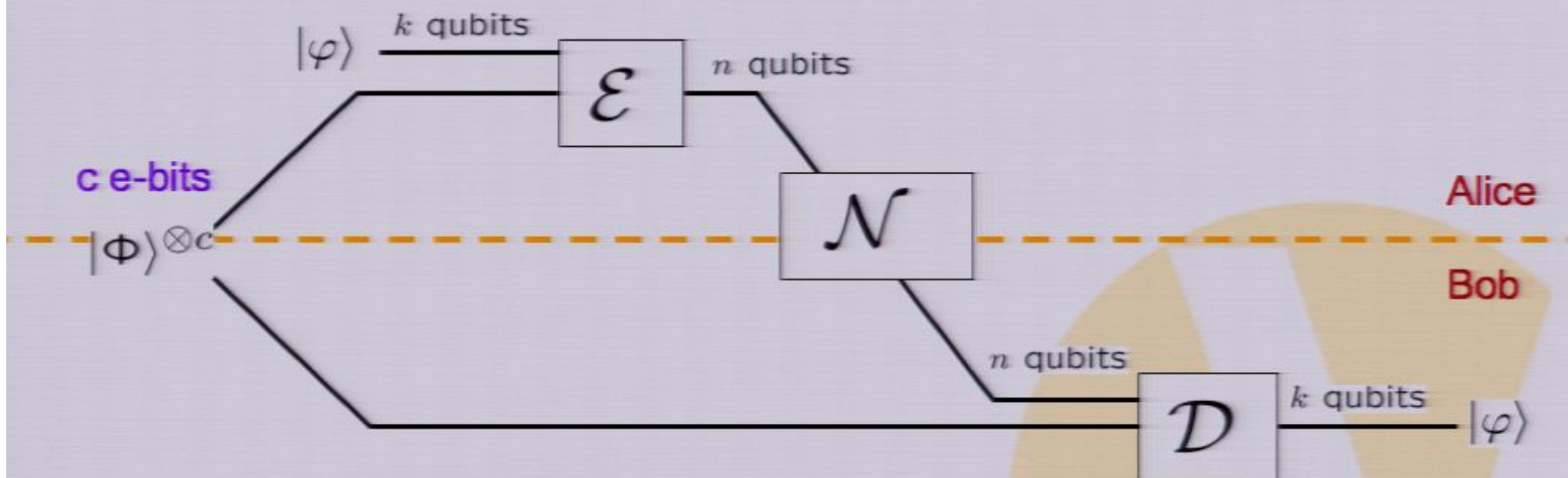
$$\left(\begin{array}{ccccc|ccccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{array} \right) \odot (00010|00010)^T = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

- Correction involves measuring the "error syndrome" (i.e. the simultaneous eigenvector of the stabilizer generators), $H \odot u^T$

Entanglement-assisted error correction

$[[n,k;c]]$ EA quantum error correcting code

non-local



$$|\Phi\rangle = \frac{1}{\sqrt{2}} (|0\rangle^A |0\rangle^B + |1\rangle^A |1\rangle^B) \quad \text{e-bit}$$

It turns out that we can establish a simple extension of the usual stabilizer formalism to describe entanglement-assisted codes. We again establish a “stabilizer” which is a subgroup of the Pauli group on n q-bits; but we no longer require this subgroup to be Abelian. For such a subgroup, we can find a set of generators which fall into two groups:

Isotropic generators, which commute with all other generators; and

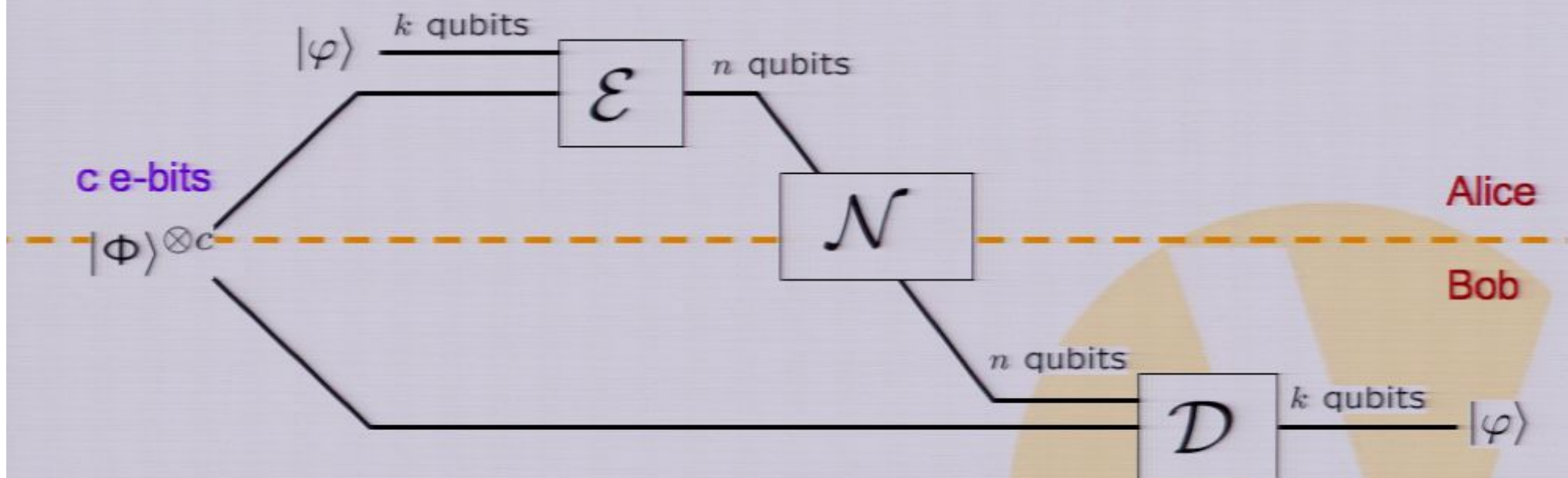
Symplectic generators, which come in anticommuting pairs; each pair commutes with all other generators.

The anticommutation of the symplectic generators is resolved by adding operators on the receiver’s side. This requires pre-shared entanglement.

Entanglement-assisted error correction

$[[n,k;c]]$ EA quantum error correcting code

non-local



$$|\Phi\rangle = \frac{1}{\sqrt{2}} (|0\rangle^A |0\rangle^B + |1\rangle^A |1\rangle^B) \quad \text{e-bit}$$

It turns out that we can establish a simple extension of the usual stabilizer formalism to describe entanglement-assisted codes. We again establish a “stabilizer” which is a subgroup of the Pauli group on n q-bits; but we no longer require this subgroup to be Abelian. For such a subgroup, we can find a set of generators which fall into two groups:

Isotropic generators, which commute with all other generators; and

Symplectic generators, which come in anticommuting pairs; each pair commutes with all other generators.

The anticommutation of the symplectic generators is resolved by adding operators on the receiver’s side. This requires pre-shared entanglement.

- An $[[n,k;c]]$ EA quantum error correcting code is described by a $(n-k) \times 2n$ parity check matrix H . $B = \text{rowspace}(H)$. Again, $C = B^\perp$
- Take a **general** symplectic matrix H . Its rowspace B can be written as

$$B = \underbrace{\text{iso}(B)}_{\text{symplectic pairs}} \oplus \underbrace{\bigoplus_{i=1}^c \text{span}\{e_i, f_i\}}_{\text{symplectic pairs}}$$

$$e_i \odot f_i = 1$$

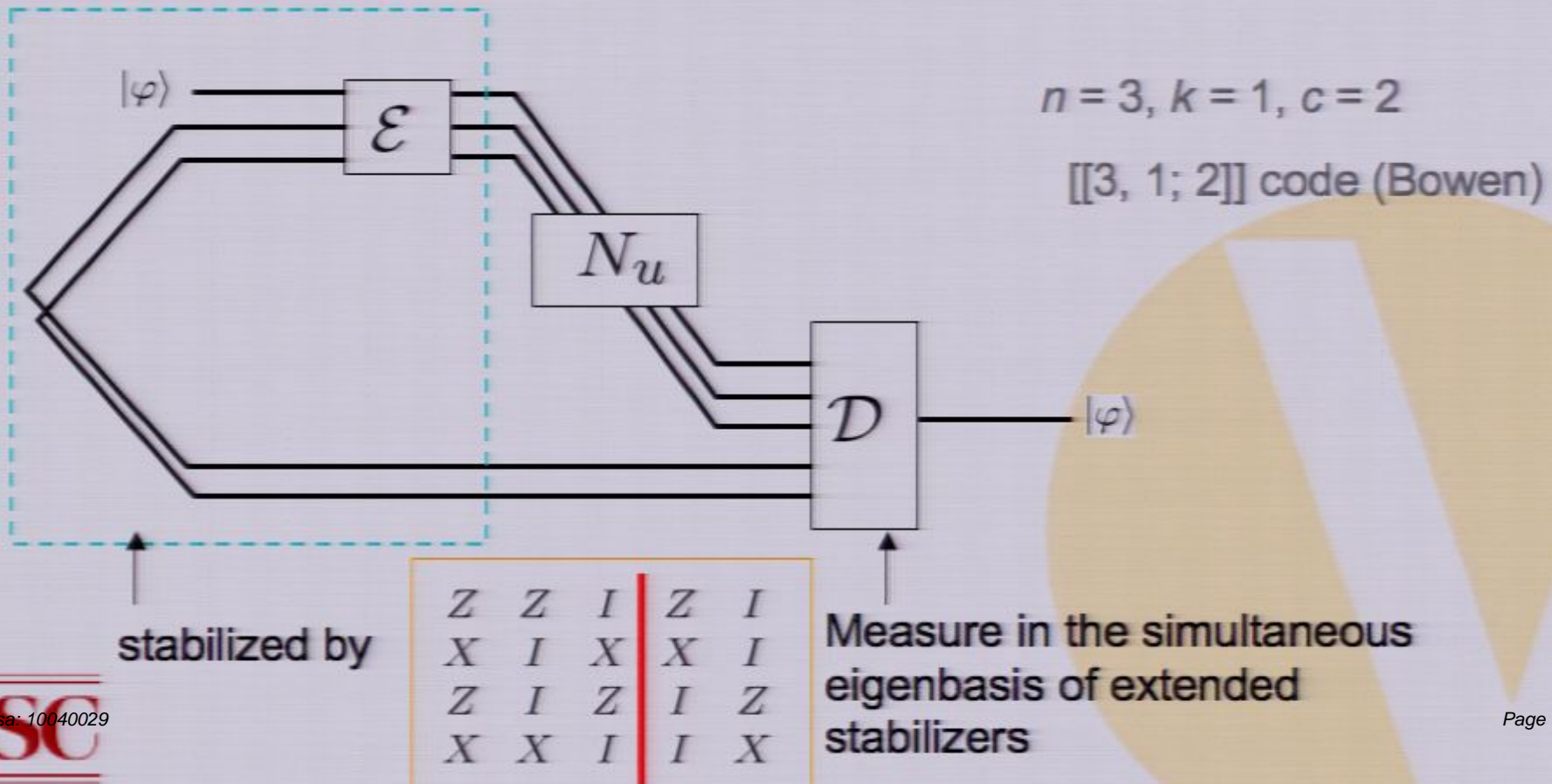
$$e_i, f_i \odot u = 0, \text{ otherwise}$$

- Canonical example

$$H = \left(\begin{array}{cc|cc|cc|cc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array} \right) \begin{matrix} e_1 \\ f_1 \\ e_2 \\ f_2 \end{matrix} \sim \left(\begin{array}{cc|cc|cc|cc} Z & I & I & I & I & I \\ I & Z & I & I & I & I \\ \hline I & I & Z & I & I & I \\ I & I & X & I & I & I \\ \hline I & I & I & Z & I & I \\ I & I & I & X & I & I \end{array} \right) \begin{matrix} \text{iso} \\ \text{symp} \end{matrix}$$

The isotropic generators generate S_I and the symplectic generators generate S_F .

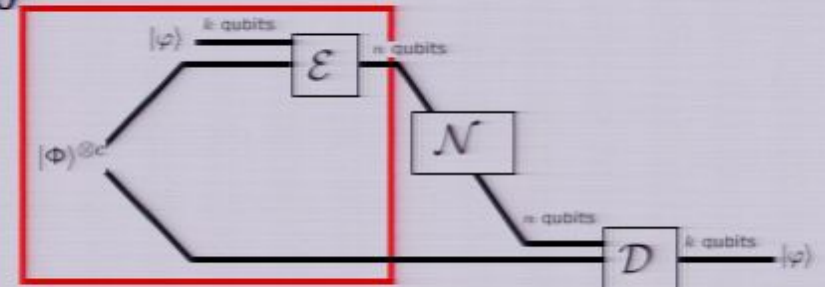
$$H = \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{array} \right) \begin{array}{l} e_1 \\ e_2 \\ f_2 \\ f_1 \end{array} \sim \begin{pmatrix} Z & Z & I \\ Z & I & Z \\ X & X & I \\ X & I & X \end{pmatrix}$$



- The correctable error set E is defined by:

If E_1 and E_2 are in E , then at least one of the two conditions hold:

- $E_2^t E_1 \notin Z(\langle S_I, S_E \rangle)$
- $E_2^t E_1 \in S_I$ **degenerate code**



- The code space $\mathcal{E}(\mathcal{H}_2^{\otimes k})$ is defined as the simultaneous +1 eigenspace of the stabilizer generators

$$\underbrace{\{N_u \otimes I^{\otimes c} : u \in \text{iso}(C^\perp)\}}_{\substack{n \\ c}} \cup \bigcup_{i=1}^c \underbrace{\{N_{e_i} \otimes Z_i, N_{f_i} \otimes X_i\}}_{\substack{n \\ c \quad n \\ c}}$$

- Decoding involves measuring the "error syndrome" (i.e. the simultaneous eigenvector of the stabilizer generators), $H \odot u^T$

- Natural isometry between $GF(4)$ and $(\mathbb{Z}_2)^2$
- Any **dual containing** classical $[n,k,d]_4$ code can be made into a $[[n,2k-n,d]]$ QECC
- Now: **Any classical $[n,k,d]_4$ code can be made into a $[[n,2k-n+c,d;c]]$ catalytic QECC for some c**

$$c = \text{rank}(H_4 \overline{H}_4^T).$$

- When the classical code attains the Singleton bound $n-k \geq d-1$ the quantum code attains the quantum Singleton bound $n-k+c \geq 2(d-1)$
- When the classical code attains the Shannon limit $2 - H_4(1 - 3p, p, p, p)$ on a quaternary symmetric channel, the quantum code attains the Hashing limit $1 - H_2(1 - 3p, p, p, p)$.
- Modern classical codes (LDPC, turbo) can now be made quantum without having to be dual-containing.

A helpful way to think about how resources (ancillas, ebits, gauge qubits, etc.) are used in error correction is with the canonical representation. For a standard code this looks like:

$$\underbrace{|0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle}_{n-k} \otimes \underbrace{|\psi\rangle}_k$$

This is, essentially, the form of the code *before* encoding. Each of these ancillas can hold one bit of info about any errors that occur:

$$\underbrace{e^{i\theta} |s_1\rangle \otimes |s_2\rangle \otimes \dots \otimes |s_{n-k}\rangle}_{n-k} \otimes \underbrace{E_s |\psi\rangle}_k$$

Each of these ancillas corresponds to a single stabilizer generator that is measured in the correction procedure.

In an entanglement-assisted code, we replace some or all of the ancillas with ebits.

$$\underbrace{|\Phi_+\rangle \otimes \dots \otimes |\Phi_+\rangle}_c \otimes \underbrace{|0\rangle \otimes \dots \otimes |0\rangle}_{s=n-k-c} \otimes \underbrace{|\psi\rangle}_k$$

These ebits can hold *two* bits of information about errors, via superdense coding. So replacing an ancilla with an ebit can increase the number of correctable errors.

Each ebit corresponds to *two* generators of the stabilizer--a symplectic pair. For the unencoded ebits these would take the form $Z|Z$ and $X|X$, where the first operator is on Alice's side and the second on Bob's.

A helpful way to think about how resources (ancillas, ebits, gauge qubits, etc.) are used in error correction is with the canonical representation. For a standard code this looks like:

$$\underbrace{|0\rangle \otimes |0\rangle \otimes \cdots |0\rangle}_{n-k} \otimes \underbrace{|\psi\rangle}_k$$

This is, essentially, the form of the code *before* encoding. Each of these ancillas can hold one bit of info about any errors that occur:

$$\underbrace{e^{i\theta} |s_1\rangle \otimes |s_2\rangle \otimes \cdots |s_{n-k}\rangle}_{n-k} \otimes \underbrace{E_s |\psi\rangle}_k$$

Each of these ancillas corresponds to a single stabilizer generator that is measured in the correction procedure.

In an entanglement-assisted code, we replace some or all of the ancillas with ebits.

$$\underbrace{|\Phi_+\rangle \otimes \dots \otimes |\Phi_+\rangle}_c \otimes \underbrace{|0\rangle \otimes \dots \otimes |0\rangle}_{s=n-k-c} \otimes \underbrace{|\psi\rangle}_k$$

These ebits can hold *two* bits of information about errors, via superdense coding. So replacing an ancilla with an ebit can increase the number of correctable errors.

Each ebit corresponds to *two* generators of the stabilizer--a symplectic pair. For the unencoded ebits these would take the form $Z|Z$ and $X|X$, where the first operator is on Alice's side and the second on Bob's.

When we constructed an EAQECC from a classical linear code, we saw that this increased error-correcting power manifested itself as an increased *rate*: $2k-n+c$.

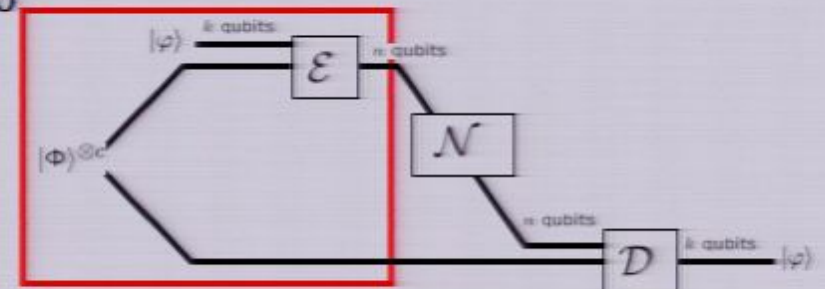
The canonical representation, however, raises a different question: what if we replace ancillas by ebits, *without* increasing the rate k/n ?

Is it possible, thereby, to increase the error-correcting power of the code--for example, to increase the minimal distance?

- The correctable error set E is defined by:

If E_1 and E_2 are in E , then at least one of the two conditions hold:

- $E_2^t E_1 \notin Z(\langle S_I, S_E \rangle)$
- $E_2^t E_1 \in S_I$ **degenerate code**



- The code space $\mathcal{E}(\mathcal{H}_2^{\otimes k})$ is defined as the simultaneous +1 eigenspace of the stabilizer generators

$$\underbrace{\{N_u \otimes I^{\otimes c} : u \in \text{iso}(C^\perp)\}}_{\substack{n \\ c}} \cup \bigcup_{i=1}^c \underbrace{\{N_{e_i} \otimes Z_i, N_{f_i} \otimes X_i\}}_{\substack{n \\ c \quad n \quad c}}$$

- Decoding involves measuring the "error syndrome" (i.e. the simultaneous eigenvector of the stabilizer generators), $H \odot u^T$

- Natural isometry between $GF(4)$ and $(\mathbb{Z}_2)^2$
- Any **dual containing** classical $[n,k,d]_4$ code can be made into a $[[n,2k-n,d]]$ QECC
- Now: **Any classical $[n,k,d]_4$ code can be made into a $[[n,2k-n+c,d;c]]$ catalytic QECC for some c**

$$c = \text{rank}(H_4 \overline{H}_4^T).$$

- When the classical code attains the Singleton bound $n-k \geq d-1$ the quantum code attains the quantum Singleton bound $n-k+c \geq 2(d-1)$
- When the classical code attains the Shannon limit $2 - H_4(1 - 3p, p, p, p)$ on a quaternary symmetric channel, the quantum code attains the Hashing limit $1 - H_2(1 - 3p, p, p, p)$.
- Modern classical codes (LDPC, turbo) can now be made quantum without having to be dual-containing.

In an entanglement-assisted code, we replace some or all of the ancillas with ebits.

$$\underbrace{|\Phi_+\rangle \otimes \dots \otimes |\Phi_+\rangle}_c \otimes \underbrace{|0\rangle \otimes \dots \otimes |0\rangle}_{s=n-k-c} \otimes \underbrace{|\psi\rangle}_k$$

These ebits can hold *two* bits of information about errors, via superdense coding. So replacing an ancilla with an ebit can increase the number of correctable errors.

Each ebit corresponds to *two* generators of the stabilizer--a symplectic pair. For the unencoded ebits these would take the form $Z|Z$ and $X|X$, where the first operator is on Alice's side and the second on Bob's.

When we constructed an EAQECC from a classical linear code, we saw that this increased error-correcting power manifested itself as an increased *rate*: $2k-n+c$.

The canonical representation, however, raises a different question: what if we replace ancillas by ebits, *without* increasing the rate k/n ?

Is it possible, thereby, to increase the error-correcting power of the code--for example, to increase the minimal distance?

In an entanglement-assisted code, we replace some or all of the ancillas with ebits.

$$\underbrace{|\Phi_+\rangle \otimes \dots \otimes |\Phi_+\rangle}_c \otimes \underbrace{|0\rangle \otimes \dots \otimes |0\rangle}_{s=n-k-c} \otimes \underbrace{|\psi\rangle}_k$$

These ebits can hold *two* bits of information about errors, via superdense coding. So replacing an ancilla with an ebit can increase the number of correctable errors.

Each ebit corresponds to *two* generators of the stabilizer--a symplectic pair. For the unencoded ebits these would take the form $Z|Z$ and $X|X$, where the first operator is on Alice's side and the second on Bob's.

A helpful way to think about how resources (ancillas, ebits, gauge qubits, etc.) are used in error correction is with the canonical representation. For a standard code this looks like:

$$\underbrace{|0\rangle \otimes |0\rangle \otimes \cdots |0\rangle}_{n-k} \otimes \underbrace{|\psi\rangle}_k$$

This is, essentially, the form of the code *before* encoding. Each of these ancillas can hold one bit of info about any errors that occur:

$$\underbrace{e^{i\theta} |s_1\rangle \otimes |s_2\rangle \otimes \cdots |s_{n-k}\rangle}_{n-k} \otimes \underbrace{E_s |\psi\rangle}_k$$

Each of these ancillas corresponds to a single stabilizer generator that is measured in the correction procedure.

In an entanglement-assisted code, we replace some or all of the ancillas with ebits.

$$\underbrace{|\Phi_+\rangle \otimes \dots \otimes |\Phi_+\rangle}_c \otimes \underbrace{|0\rangle \otimes \dots \otimes |0\rangle}_{s=n-k-c} \otimes \underbrace{|\psi\rangle}_k$$

These ebits can hold *two* bits of information about errors, via superdense coding. So replacing an ancilla with an ebit can increase the number of correctable errors.

Each ebit corresponds to *two* generators of the stabilizer--a symplectic pair. For the unencoded ebits these would take the form $Z|Z$ and $X|X$, where the first operator is on Alice's side and the second on Bob's.

When we constructed an EAQECC from a classical linear code, we saw that this increased error-correcting power manifested itself as an increased *rate*: $2k-n+c$.

The canonical representation, however, raises a different question: what if we replace ancillas by ebits, *without* increasing the rate k/n ?

Is it possible, thereby, to increase the error-correcting power of the code--for example, to increase the minimal distance?

In an entanglement-assisted code, we replace some or all of the ancillas with ebits.

$$\underbrace{|\Phi_+\rangle \otimes \dots \otimes |\Phi_+\rangle}_c \otimes \underbrace{|0\rangle \otimes \dots \otimes |0\rangle}_{s=n-k-c} \otimes \underbrace{|\psi\rangle}_k$$

These ebits can hold *two* bits of information about errors, via superdense coding. So replacing an ancilla with an ebit can increase the number of correctable errors.

Each ebit corresponds to *two* generators of the stabilizer--a symplectic pair. For the unencoded ebits these would take the form $Z|Z$ and $X|X$, where the first operator is on Alice's side and the second on Bob's.

When we constructed an EAQECC from a classical linear code, we saw that this increased error-correcting power manifested itself as an increased *rate*: $2k-n+c$.

The canonical representation, however, raises a different question: what if we replace ancillas by ebits, *without* increasing the rate k/n ?

Is it possible, thereby, to increase the error-correcting power of the code--for example, to increase the minimal distance?

Example: the repetition code

Consider the code on n qubits with the following generators:

$$n = 5: \quad ZZIII, \quad IZZII, \quad IIZZI, \quad IIIZZ$$

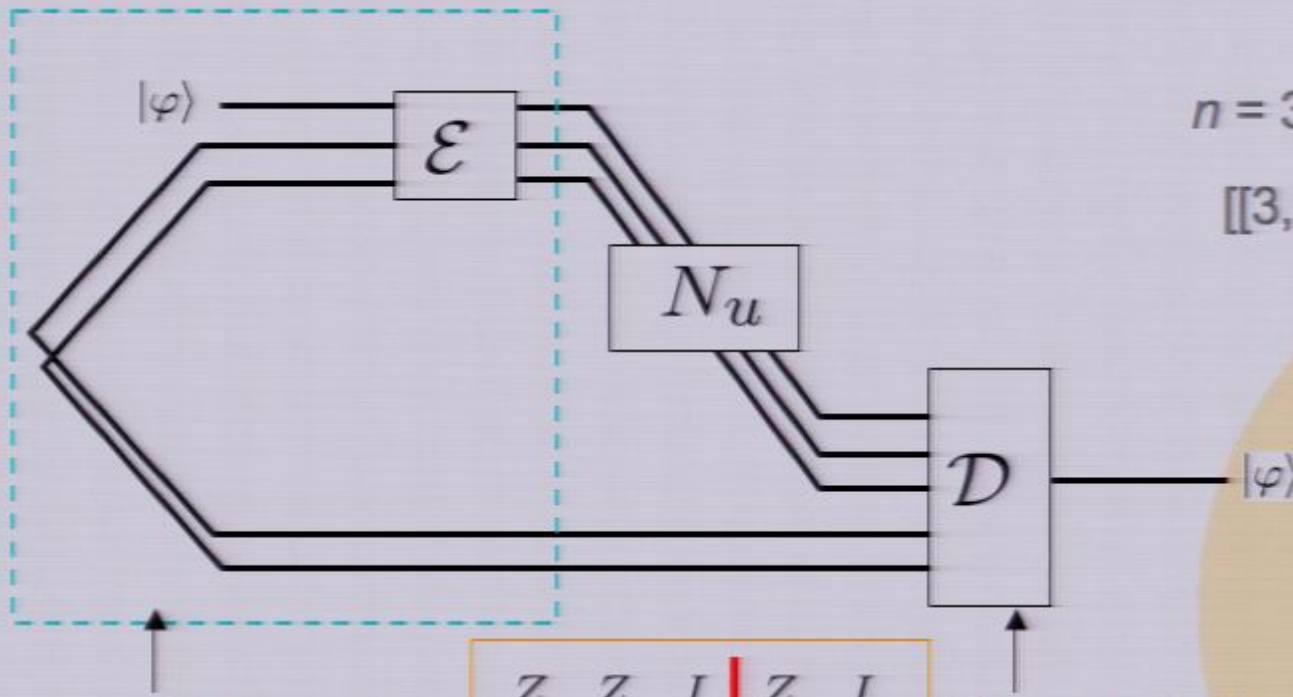
This is just the repetition code, which protects against bit flips. This code has distance $d=1$, because it cannot correct even a single phase flip error.

Suppose now that we replace *all* the ancillas of this code with ebits. The new set of generators is:

$$n = 5: \quad \begin{array}{l} ZZIII, \quad IZZII, \quad IIZZI, \quad IIIZZ, \\ IXXXX, \quad XXIII, \quad IIIXX, \quad XXXXI. \end{array}$$

This code has distance n . It is an $[[n,1,n;n-1]]$ EAQECC. Note that our example of a $[[3,1,3;2]]$ code from before lies in this class of codes!

$$H = \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{array} \right) \begin{array}{l} e_1 \\ e_2 \\ f_2 \\ f_1 \end{array} \sim \left(\begin{array}{ccc} Z & Z & I \\ Z & I & Z \\ X & X & I \\ X & I & X \end{array} \right)$$



$$n = 3, k = 1, c = 2$$

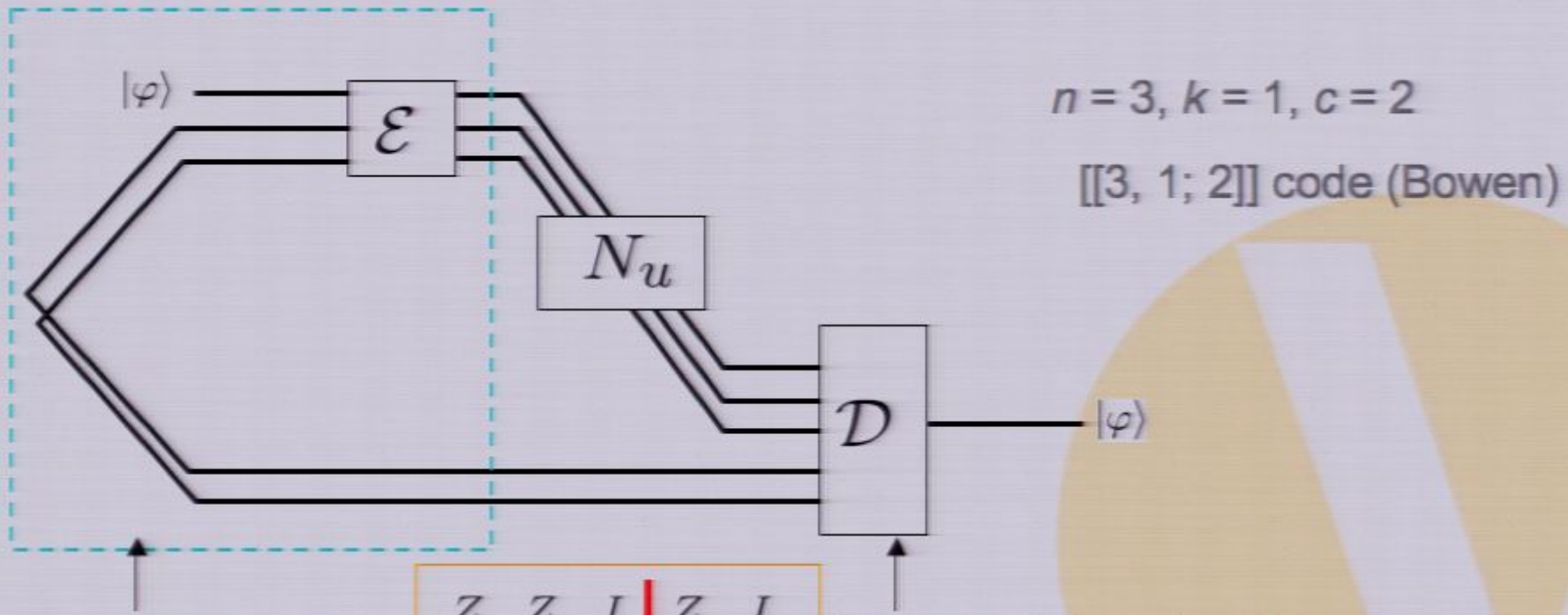
[[3, 1; 2]] code (Bowen)

stabilized by

Z	Z	I	Z	I
X	I	X	X	I
Z	I	Z	I	Z
X	X	I	I	X

Measure in the simultaneous
eigenbasis of extended
stabilizers

$$H = \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{array} \right) \begin{array}{l} e_1 \\ e_2 \\ f_2 \\ f_1 \end{array} \sim \left(\begin{array}{ccc} Z & Z & I \\ Z & I & Z \\ X & X & I \\ X & I & X \end{array} \right)$$

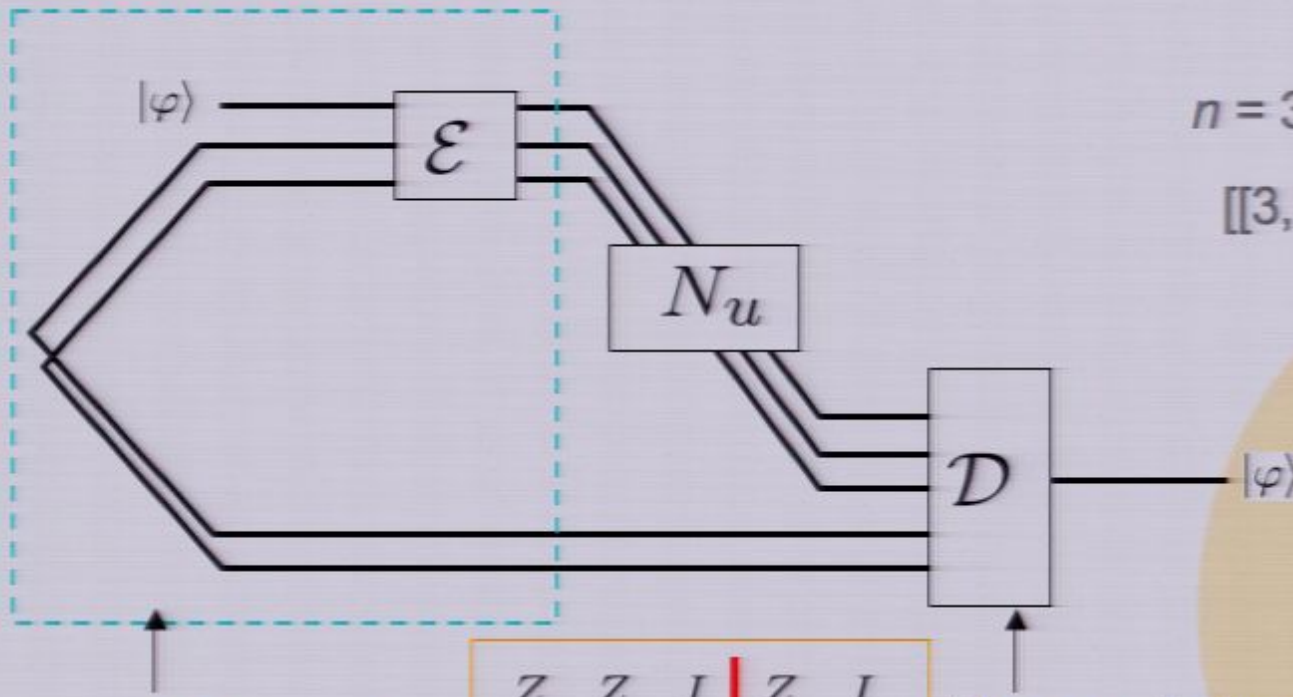


stabilized by

Z	Z	I	Z	I
X	I	X	X	I
Z	I	Z	I	Z
X	X	I	I	X

Measure in the simultaneous
eigenbasis of extended
stabilizers

$$H = \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{array} \right) \begin{array}{l} e_1 \\ e_2 \\ f_2 \\ f_1 \end{array} \sim \left(\begin{array}{ccc} Z & Z & I \\ Z & I & Z \\ X & X & I \\ X & I & X \end{array} \right)$$



$$n = 3, k = 1, c = 2$$

[[3, 1; 2]] code (Bowen)

stabilized by

Z	Z	I	Z	I
X	I	X	X	I
Z	I	Z	I	Z
X	X	I	I	X

Measure in the simultaneous
eigenbasis of extended
stabilizers

In an entanglement-assisted code, we replace some or all of the ancillas with ebits.

$$\underbrace{|\Phi_+\rangle \otimes \dots \otimes |\Phi_+\rangle}_c \otimes \underbrace{|0\rangle \otimes \dots \otimes |0\rangle}_{s=n-k-c} \otimes \underbrace{|\psi\rangle}_k$$

These ebits can hold *two* bits of information about errors, via superdense coding. So replacing an ancilla with an ebit can increase the number of correctable errors.

Each ebit corresponds to *two* generators of the stabilizer--a symplectic pair. For the unencoded ebits these would take the form $Z|Z$ and $X|X$, where the first operator is on Alice's side and the second on Bob's.

When we constructed an EAQECC from a classical linear code, we saw that this increased error-correcting power manifested itself as an increased *rate*: $2k-n+c$.

The canonical representation, however, raises a different question: what if we replace ancillas by ebits, *without* increasing the rate k/n ?

Is it possible, thereby, to increase the error-correcting power of the code--for example, to increase the minimal distance?

Example: the repetition code

Consider the code on n qubits with the following generators:

$$n = 5: \quad ZZIII, \quad IZZII, \quad IIZZI, \quad IIIZZ$$

This is just the repetition code, which protects against bit flips.
This code has distance $d=1$, because it cannot correct even a single phase flip error.

Suppose now that we replace *all* the ancillas of this code with ebits. The new set of generators is:

$$n = 5: \quad \begin{array}{l} ZZIII, \quad IZZII, \quad IIZZI, \quad IIIZZ, \\ IXXXX, \quad XXIII, \quad IIIXX, \quad XXXXI. \end{array}$$

This code has distance n . It is an $[[n,1,n;n-1]]$ EAQECC. Note that our example of a $[[3,1,3;2]]$ code from before lies in this class of codes!

For a *standard* QECC, we can choose any set of generators we like for the stabilizer. Going from one set to another is like doing a row operation in the symplectic description:

$$ZZI, IZZ, XXX \rightarrow ZZI, ZIZ, YXY$$

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{array} \right) \rightarrow \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{array} \right)$$

Different choices of generators describe the same code (though possibly not the same encoding circuit).

In an entanglement-assisted code, we replace some or all of the ancillas with ebits.

$$\underbrace{|\Phi_+\rangle \otimes \dots \otimes |\Phi_+\rangle}_c \otimes \underbrace{|0\rangle \otimes \dots \otimes |0\rangle}_{s=n-k-c} \otimes \underbrace{|\psi\rangle}_k$$

These ebits can hold *two* bits of information about errors, via superdense coding. So replacing an ancilla with an ebit can increase the number of correctable errors.

Each ebit corresponds to *two* generators of the stabilizer--a symplectic pair. For the unencoded ebits these would take the form $Z|Z$ and $X|X$, where the first operator is on Alice's side and the second on Bob's.

Example: the repetition code

Consider the code on n qubits with the following generators:

$$n = 5: \quad ZZIII, \quad IZZII, \quad IIZZI, \quad IIIZZ$$

This is just the repetition code, which protects against bit flips. This code has distance $d=1$, because it cannot correct even a single phase flip error.

Suppose now that we replace *all* the ancillas of this code with ebits. The new set of generators is:

$$n = 5: \quad \begin{array}{l} ZZIII, \quad IZZII, \quad IIZZI, \quad IIIZZ, \\ IXXXX, \quad XXIII, \quad IIIXX, \quad XXXXI. \end{array}$$

This code has distance n . It is an $[[n,1,n;n-1]]$ EAQECC. Note that our example of a $[[3,1,3;2]]$ code from before lies in this class of codes!

For a *standard* QECC, we can choose any set of generators we like for the stabilizer. Going from one set to another is like doing a row operation in the symplectic description:

$$ZZI, IZZ, XXX \rightarrow ZZI, ZIZ, YXY$$

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{array} \right) \rightarrow \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{array} \right)$$

Different choices of generators describe the same code (though possibly not the same encoding circuit).

For an EAQECC, however, one must maintain the commutation relations. Therefore, row operations on one set of generators must be matched by complementary row operations on the other.

$$ZZI, IZZ, IXX, XXI \rightarrow ZZI, ZIZ, XIX, XXI$$

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{array} \right) \rightarrow \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{array} \right)$$

For a code in which there are no isotropic generators--where every ancillas has been replaced by an ebit--row operations still do not change the code. However, if we replace only *some* of the ancillas, then the choice of generators can make a big difference.

For example, if we add one ebit to a standard QECC, that is the same as adding a symplectic partner for one generator. But the different ways of doing this are *not* interchangeable. For the code we have been considering, we used the standard generators ZZII IZZI IIZZ IIIZ. But there are 15 non-identity elements of the stabilizer group, each of which has a different symplectic partner:

XXII, IXXI, XIXI, IXXI, XXXI, IXIX, XIIX, IIIX, XXIX, IXXX, XIXX, IIXI, XXXI, IXIX, XIIX

All of these give different codes, with different correctable error sets. For a large block code, the number of ways of adding c ebits to the code can be combinatorially large.

Examples of increasing distance with entanglement

We have used numerical searches to see the effect of adding different amounts of entanglement to a QECC. The following table started with the $[[7,1,3]]$ quantum BCH code:

c	do	ds	No	combs
6	7	5	36	4096
5	5	5	31920	64512
4	5	5	39522	166656
3	5	4	4332	89280
2	5	3	14	10416
1	3	3	252	252

do and ds compare the best $[[n,1,do;c]]$ code to the best $[[n+c,1,ds]]$ code; No is the number of "optimal" encodings.

The following table started with the $[[9,1,3]]$ Shor code:

c	do	ds	No	combs
8	9	7	256	65536
7	7	6	330624	4.17×10^6
6	7	6	278904	4.42×10^7
5	7	6	17748	9.94×10^7
4	7	5	132	5.14×10^7
3	5	5	69777	6.21×10^6
2	5	5	201	1.72×10^5

In many ways, codes with maximal entanglement are particularly simple. In fact, in many ways their properties are exactly like classical linear codes.

- 1. These codes are strictly nondegenerate. All error correction is active--no errors can be passively corrected.**
- 2. They satisfy the bound $n-k \geq d-1$.**
- 3. Since the isotropic group is trivial, the logical operators of these codes are defined unambiguously.**
- 4. This lack of ambiguity means that these codes can be defined by their logical operators, just as classical linear codes can be defined by their generator matrix.**

In general, codes constructed in this way may use a great deal of entanglement. This means that they would only be useful if entanglement is essentially free, or at least readily available. While this is unlikely to be true in most practical situations, there may be some niche applications where these codes might prove beneficial.

Another potential application is to large, high-rate block codes. For these codes, adding a small amount of entanglement might well improve performance for a moderate cost. The combinatorial difficulty, however, has restricted us so far to looking at modest-sized codes.

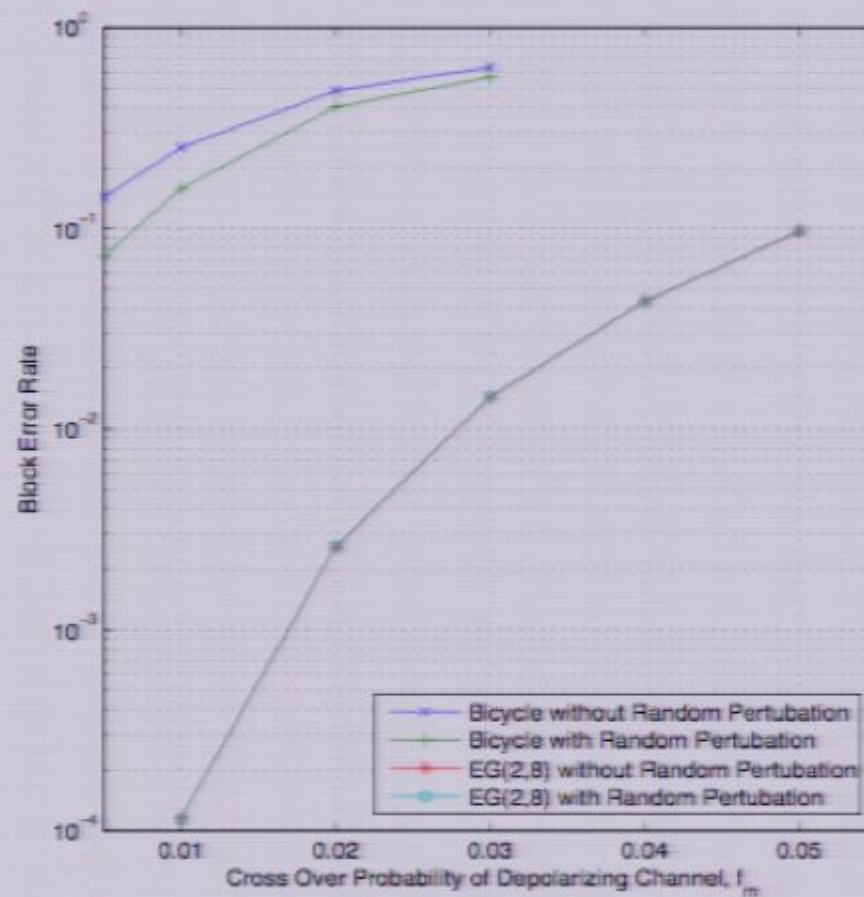
We are currently exploring algorithms to randomly search for good codes using a given amount of entanglement.

Entanglement-assisted quantum LDPC codes

One group of EAQECCs that show great promise are the quantum LDPC codes (and possibly Turbo codes as well). Classical low-density parity check codes use sparse check matrices together with a computationally efficient suboptimal decoder based on iterative decoding (or message passing). Classically these codes can approach capacity while still being efficiently decodable.

However, these iterative decoding algorithms don't perform as well if the Tanner Graph of the code has a smallest cycle (*girth*) of length 4. This is a problem for quantum codes, because any quantum code whose symplectic matrix is self-orthogonal *must* have girth 4.

Relaxing the need for self-orthogonality, by allowing entanglement-assistance, allows quantum codes with girth ≥ 6 . And there are classes of LDPC codes that achieve this using only a small, fixed or slowly growing amount of entanglement.

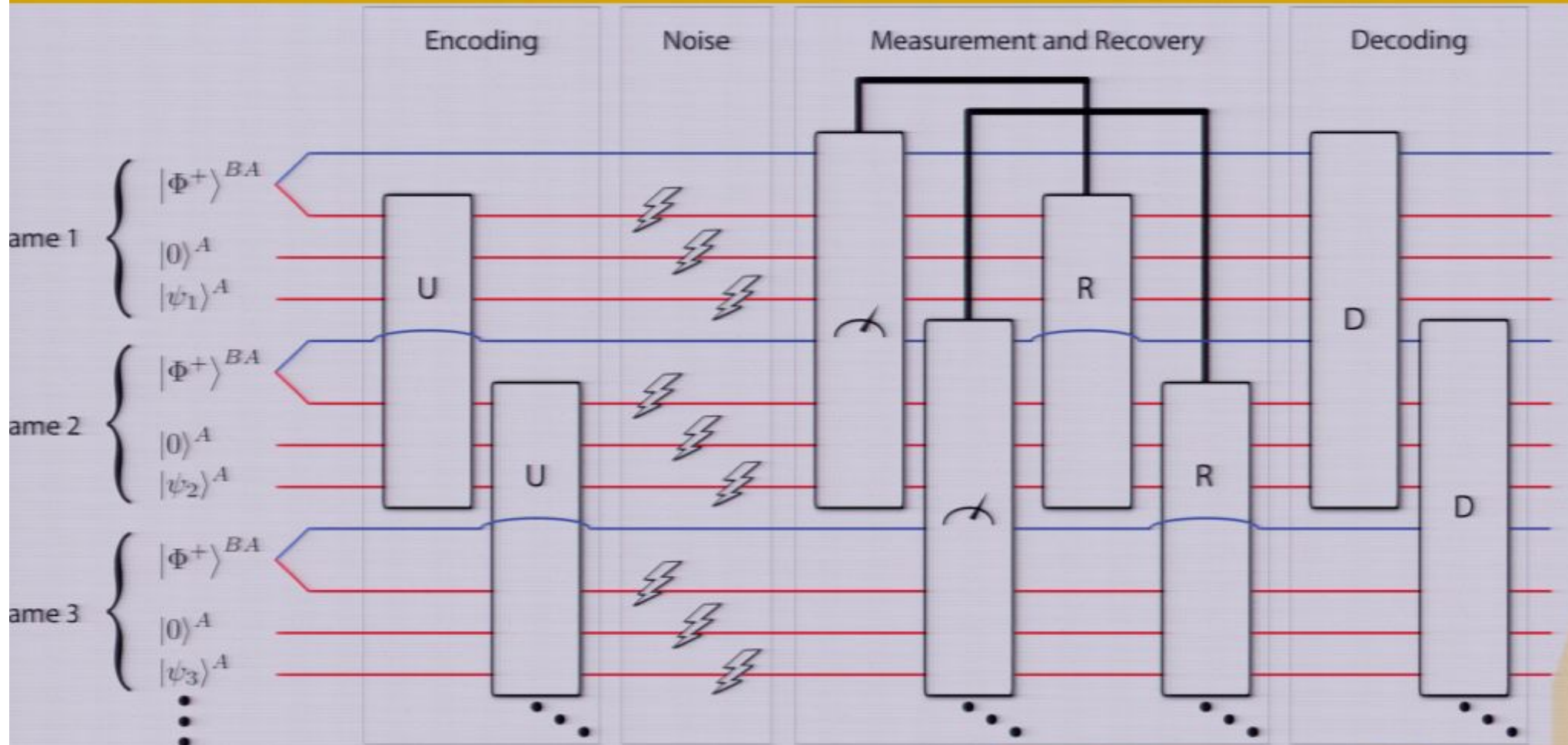


This graph compares the block error rate of EAQLDPC codes to standard QLDPC codes for the depolarizing channel. Almost all uncorrected errors are due to suboptimal decoding.

Convolutional codes, unlike block codes, encode information bits “on the fly” as a continuous process, and decode them the same way. Quantum convolutional codes work the same way, bringing in a continuous stream of information qubits and ancillas to the encoder and outputting a string of corrected qubits from the decoder.

To make such codes entanglement-assisted is straightforward, in principle--just allow an input stream of ebits as well as ancillas. But the algebraic description is much more complicated, with the symplectic check matrices becoming polynomial or rational-function valued.

$$\dots \begin{bmatrix} Z & X & Z & I \\ X & Y & X & I \end{bmatrix} \begin{bmatrix} Z & Z & I & Z \\ X & X & I & X \end{bmatrix} \dots \leftrightarrow \left(\begin{array}{cccc|cccc} 1+D & D & 1 & D & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1+D & 1+D & 1 & D \end{array} \right)$$

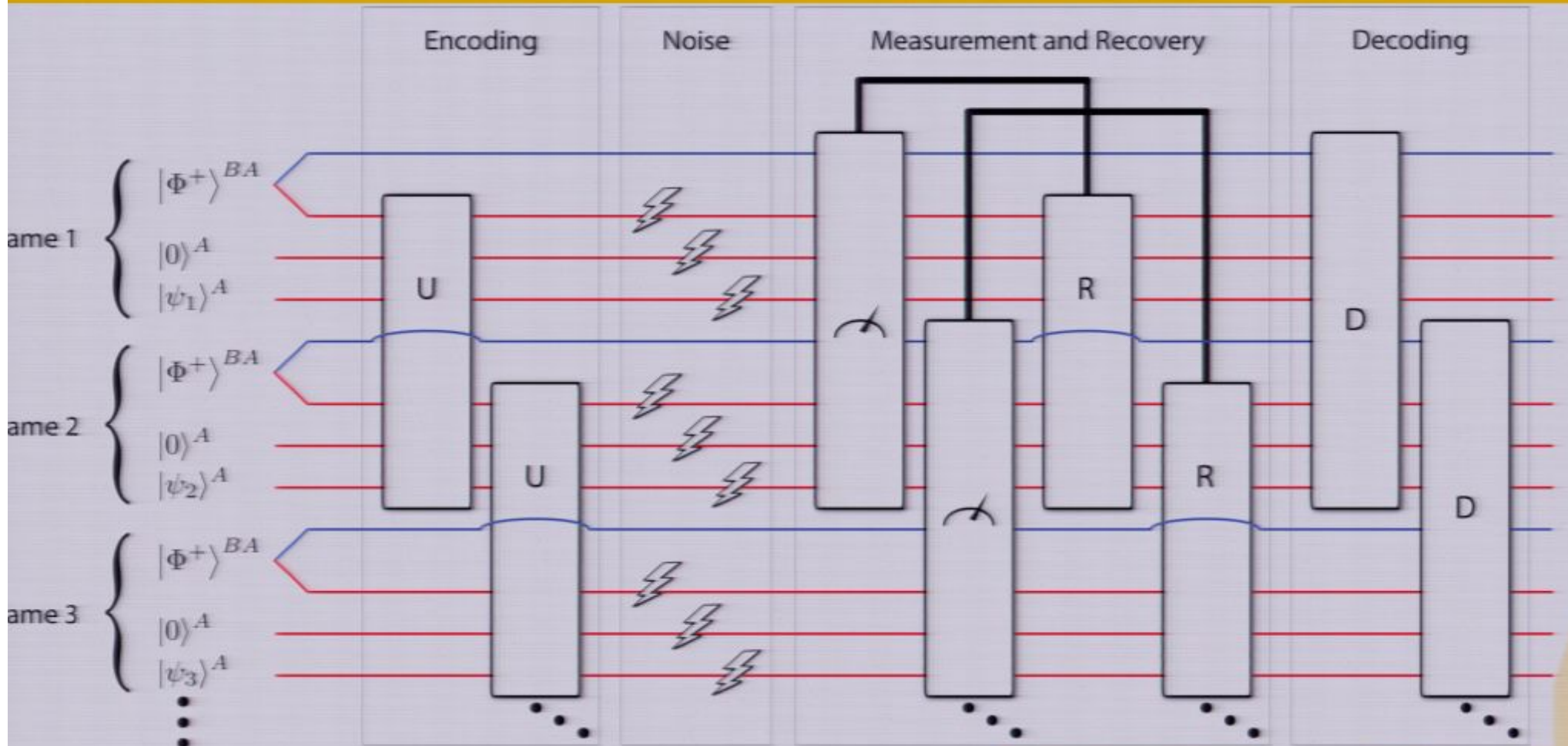


The use of EAQCCs may allow encoders and decoders that are recursive but noncatastrophic, impossible for standard QCCs.

Convolutional codes, unlike block codes, encode information bits “on the fly” as a continuous process, and decode them the same way. Quantum convolutional codes work the same way, bringing in a continuous stream of information qubits and ancillas to the encoder and outputting a string of corrected qubits from the decoder.

To make such codes entanglement-assisted is straightforward, in principle--just allow an input stream of ebits as well as ancillas. But the algebraic description is much more complicated, with the symplectic check matrices becoming polynomial or rational-function valued.

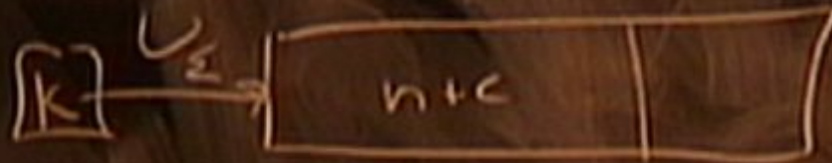
$$\dots \begin{bmatrix} Z & X & Z & I \\ X & Y & X & I \end{bmatrix} \begin{bmatrix} Z & Z & I & Z \\ X & X & I & X \end{bmatrix} \dots \leftrightarrow \left(\begin{array}{cccc|cccc} 1+D & D & 1 & D & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1+D & 1+D & 1 & D \end{array} \right)$$

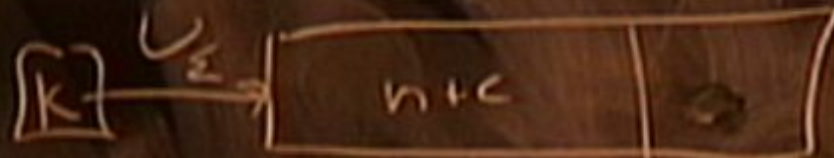


The use of EAQCCs may allow encoders and decoders that are recursive but noncatastrophic, impossible for standard QCCs.

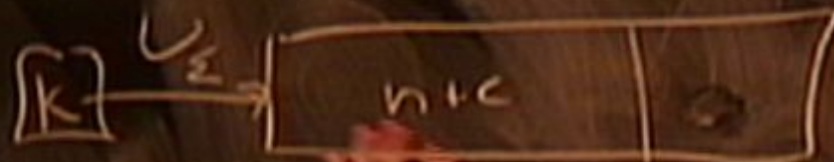


- **EAQECCs can be represented in different ways--in terms of stabilizers, using symplectic matrices, and in the canonical representation. The interplay between these representations helps us understand how entanglement can increase error-correcting power**
- **In constructing EAQECCs from classical linear codes, entanglement has the effect of boosting the rate.**
- **It is also possible to add entanglement to QECCs without increasing the rate. This increases the number of errors that can be corrected, as seen by (for example) the minimal distance.**
- **Added entanglement can also allow a simplified algebraic structure.**

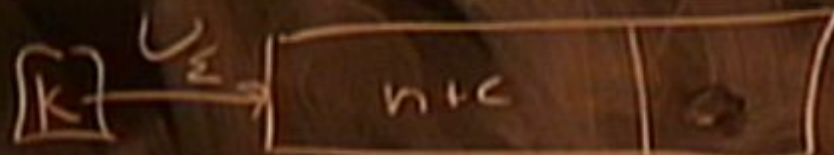




c on Bob's
Side



c on Bob's
side



c on Bob's
side

The following table started with the $[[9,1,3]]$ Shor code:

c	do	ds	No	combs
8	9	7	256	65536
7	7	6	330624	4.17×10^6
6	7	6	278904	4.42×10^7
5	7	6	17748	9.94×10^7
4	7	5	132	5.14×10^7
3	5	5	69777	6.21×10^6
2	5	5	201	1.72×10^5

- Natural isometry between $GF(4)$ and $(\mathbb{Z}_2)^2$
- Any **dual containing** classical $[n,k,d]_4$ code can be made into a $[[n,2k-n,d]]$ QECC
- Now: **Any classical $[n,k,d]_4$ code can be made into a $[[n,2k-n+c,d;c]]$ catalytic QECC for some c**

$$c = \text{rank}(H_4 \overline{H}_4^T).$$

- When the classical code attains the Singleton bound $n-k \geq d-1$ the quantum code attains the quantum Singleton bound $n-k+c \geq 2(d-1)$
- When the classical code attains the Shannon limit $2 - H_4(1 - 3p, p, p, p)$ on a quaternary symmetric channel, the quantum code attains the Hashing limit $1 - H_2(1 - 3p, p, p, p)$.
- Modern classical codes (LDPC, turbo) can now be made quantum without having to be dual-containing.

- Natural isometry between $GF(4)$ and $(\mathbb{Z}_2)^2$
- Any **dual containing** classical $[n,k,d]_4$ code can be made into a $[[n,2k-n,d]]$ QECC
- Now: **Any classical $[n,k,d]_4$ code can be made into a $[[n,2k-n+c,d;c]]$ catalytic QECC for some c**

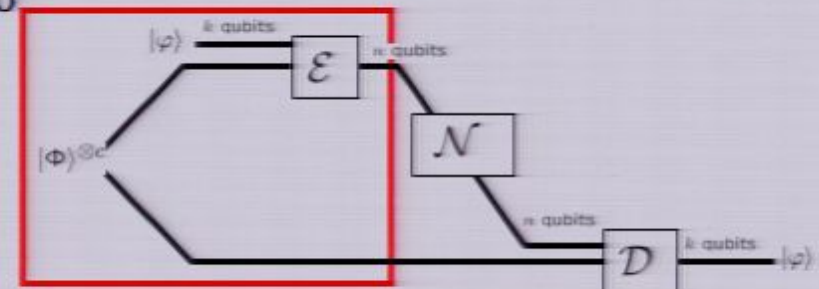
$$c = \text{rank}(H_4 \overline{H}_4^T).$$

- When the classical code attains the Singleton bound $n-k \geq d-1$ the quantum code attains the quantum Singleton bound $n-k+c \geq 2(d-1)$
- When the classical code attains the Shannon limit $2 - H_4(1 - 3p, p, p, p)$ on a quaternary symmetric channel, the quantum code attains the Hashing limit $1 - H_2(1 - 3p, p, p, p)$.
- Modern classical codes (LDPC, turbo) can now be made quantum without having to be dual-containing.

- The correctable error set E is defined by:

If E_1 and E_2 are in E , then at least one of the two conditions hold:

- $E_2^t E_1 \notin Z(\langle S_I, S_E \rangle)$
- $E_2^t E_1 \in S_I$ **degenerate code**



- The code space $\mathcal{E}(\mathcal{H}_2^{\otimes k})$ is defined as the simultaneous +1 eigenspace of the stabilizer generators

$$\underbrace{\{N_u \otimes I^{\otimes c} : u \in \text{iso}(C^\perp)\}}_{\substack{n \\ c}} \cup \bigcup_{i=1}^c \underbrace{\{N_{e_i} \otimes Z_i, N_{f_i} \otimes X_i\}}_{\substack{n \\ c \quad n \quad c}}$$

- Decoding involves measuring the "error syndrome" (i.e. the simultaneous eigenvector of the stabilizer generators), $H \odot u^T$

- Natural isometry between $GF(4)$ and $(\mathbb{Z}_2)^2$
- Any **dual containing** classical $[n,k,d]_4$ code can be made into a $[[n,2k-n,d]]$ QECC
- Now: **Any classical $[n,k,d]_4$ code can be made into a $[[n,2k-n+c,d;c]]$ catalytic QECC for some c**

$$c = \text{rank}(H_4 \overline{H}_4^T).$$

- When the classical code attains the Singleton bound $n-k \geq d-1$ the quantum code attains the quantum Singleton bound $n-k+c \geq 2(d-1)$
- When the classical code attains the Shannon limit $2 - H_4(1 - 3p, p, p, p)$ on a quaternary symmetric channel, the quantum code attains the Hashing limit $1 - H_2(1 - 3p, p, p, p)$.
- Modern classical codes (LDPC, turbo) can now be made quantum without having to be dual-containing.

In an entanglement-assisted code, we replace some or all of the ancillas with ebits.

$$\underbrace{|\Phi_+\rangle \otimes \dots \otimes |\Phi_+\rangle}_c \otimes \underbrace{|0\rangle \otimes \dots \otimes |0\rangle}_{s=n-k-c} \otimes \underbrace{|\psi\rangle}_k$$

These ebits can hold *two* bits of information about errors, via superdense coding. So replacing an ancilla with an ebit can increase the number of correctable errors.

Each ebit corresponds to *two* generators of the stabilizer--a symplectic pair. For the unencoded ebits these would take the form $Z|Z$ and $X|X$, where the first operator is on Alice's side and the second on Bob's.