CS 599 P1: Introduction to Quantum Computation — Boston University, Fall 2025
Instructor: Alexander Poremba

LECTURE # 21: QUANTUM ERROR CORRECTION & FAULT TOLERANCE

In the last lecture, we covered the 9-qubit Shor code, a mechanism for encoding a single *logical* qubit into 9 *physical* qubits; these help protect the logical information against an *arbitrary* single-qubit error. Can we build more sophisticated codes that can correct more than a single error? What about multiple errors? It turns out that we can build much more powerful quantum codes using classical error-correcting codes as building blocks. In this lecture, we will introduce a powerful class of quantum codes called Calderbank-Steane-Shor (CSS) codes which make use of classical linear codes. Sophisticated quantum codes, such as CSS codes, can correct multiple errors and offer a pathway towards fault-tolerant quantum computation.

1 Classical coding theory

A code $\mathcal{C} \subseteq \mathbb{F}_2^n$ is an additive *subspace* of the ambient space $\mathbb{F}_2^n$—the vector space over bit-strings $\{0,1\}^n$ equipped with addition modulo 2.

Linear codes. A simple example of a $[n,k]$ code $\mathcal{C}$ mapping k *logical* bits into codewords of length n is

$$\mathcal{C} = \left\{ \mathbf{c} \in \mathbb{F}_2^n \,:\, \mathbf{c} = \mathbf{G} \cdot \mathbf{x} \pmod 2, \text{ for } \mathbf{x} \in \mathbb{F}_2^k \right\}$$

where $\mathbf{G} \in \mathbb{F}_2^{n \times k}$ is the so-called *generator matrix* which is assumed to have full (column) rank; thus, multiplication by $\mathbf{G}$ is *injective* and no two messages get mapped to the same codeword.

A $[n,k]$ code $\mathcal{C}$ has two important characteristics:

- **Rate:** The rate of $\mathcal{C}$ is defined as $R = \frac{k}{n}$. It captures rate at which codewords are packed into the ambient space $\mathbb{F}_2^n$: if the rate is high, i.e., $R \approx 1$, the codewords are very dense, whereas if the rate is very low, i.e. $R \approx 0$, then the codewords only occupy a sparse subset of $\{0,1\}^n$.
- **Distance:** The distance d of $\mathcal{C}$ captures how far apart any two codewords in $\mathcal{C}$ are. It is defined as

$$d = \min_{\substack{\mathbf{c},\mathbf{c}' \in \mathcal{C} \\ \mathbf{c} \neq \mathbf{c}'}} \mathrm{wt}(\mathbf{c} \oplus \mathbf{c}')\,,$$

  where $\mathrm{wt}(\cdot)$ denotes the Hamming weight of a string.[1] Because $\mathcal{C}$ is a *subspace* of the ambient space (under addition modulo 2), it is easy to see that d can be equivalently described as the length of the shortest non-zero codeword:

$$d = \min_{\substack{\mathbf{c} \in \mathcal{C} \\ \mathbf{c} \neq \mathbf{0}}} \mathrm{wt}(\mathbf{c}).$$

[1] The Hamming weight of a bit-string is the number of non-zero entries, i.e., the number of entries which are equal to 1.

Another (and equivalent) way of specifying a linear code is via the *dual* representation, where we write

$$\mathcal{C} = \left\{ \mathbf{c} \in \mathbb{F}_2^n \,:\, \mathbf{H} \cdot \mathbf{c} = \mathbf{0} \pmod 2 \right\}$$

and where $\mathbf{H} \in \mathbb{F}_2^{(n-k)\times n}$ is the so-called *parity check matrix*. Note that $\mathbf{H}$ has $n-k$ many rows to ensure that the kernel (and thus the codespace) has dimension k by the rank-nullity theorem.

Syndrome decoding. The parity matrix representation is especially useful as a means of diagnosing and correcting errors. Suppose we have a codeword $\mathbf{c} \in \mathcal{C}$ which is perturbed by some error $\mathbf{e} \in \mathbb{F}_2^n$. The perturbed string can then be written as

$$\mathbf{c} + \mathbf{e} \pmod 2.$$

To diagnose whether our codeword has been corrupted, we can use the parity check matrix $\mathbf{H} \in \mathbb{F}_2^{(n-k)\times n}$ of the codespace $\mathcal{C}$, and multiply from the left as follows:

$$\begin{aligned} \mathbf{c} + \mathbf{e} \pmod 2 \qquad \overset{\mathbf{H}}{\mapsto} \qquad & \mathbf{H} \cdot (\mathbf{c} + \mathbf{e}) \pmod 2 \\ & = \underbrace{\mathbf{H} \cdot \mathbf{c}}_{=0} + \mathbf{H} \cdot \mathbf{e} \pmod 2 \\ & = \mathbf{H} \cdot \mathbf{e} \pmod 2. \end{aligned}$$

In other words, a corrupted codeword carries an error syndrome $\mathbf{H} \cdot \mathbf{e} \pmod 2$ which we can be detect. If we manage to infer the error $\mathbf{e}$ given the syndrome $\mathbf{y}$, we can easily correct the error by once again shifting the noisy codeword by $\mathbf{e}$.

Formally, we can define the syndrome decoding problem as the following computational task.

Syndrome Decoding Problem

Given: A parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{(n-k)\times n}$ and a syndrome

$$\mathbf{y} = \mathbf{H} \cdot \mathbf{e} \pmod 2,$$

arising from an unknown error vector $\mathbf{e} \in \mathbb{F}_2^n$.

Promise: The error vector $\mathbf{e}$ has low Hamming weight, i.e.,

$$\mathrm{wt}(\mathbf{e}) \leq t,$$

for some small and known parameter t.

Goal: Recover a low-weight error vector in $\mathbb{F}_2^n$ consistent with the syndrome $\mathbf{y}$.

The syndrome decoding problem is a *constraint satisfaction problem* and can, in general, be quite difficult to solve. Efficient syndrome decoding for linear codes often requires clever insights into code design. In the worst-case, the decision variant of the problem is known to be NP-complete. Nevertheless, there exist many families of codes which admit polynomial-time decoders, such as Reed-Muller or Reed-Solomon codes.

Dual codes. Given an $[n, k]$ code $\mathcal{C}$ we can define another related code—the *dual code* $\mathcal{C}^\perp$ given by

$$\mathcal{C}^\perp = \left\{ \mathbf{y} \in \mathbb{F}_2^n \,:\, \langle \mathbf{y}, \mathbf{c} \rangle = 0 \pmod 2,\ \forall \mathbf{c} \in \mathcal{C} \right\}$$

where we define the "inner product" modulo 2 as $\langle \mathbf{y}, \mathbf{c} \rangle := y_1 \cdot c_1 \oplus \cdots \oplus y_n \cdot c_n$. In other words, the dual code $\mathcal{C}^\perp$ consists of all vectors in the ambient space $\mathbb{F}_2^n$ which are "orthogonal" to $\mathcal{C}$. It is easy to check that $\mathcal{C}^\perp$ is an $[n, n-k]$ code since it is the code whose generator matrix is $\mathbf{H}^\intercal \in \mathbb{F}_2^{n \times (n-k)}$, i.e., the parity check matrix of the underlying code $\mathcal{C}$.

2 Multi-qubit errors

We will think of a general, multi-qubit, error of weight t acting on an n-qubit state as some product

$$\mathbf{E} = I \otimes E_1 \otimes E_2 \otimes I \otimes \cdots \otimes I \otimes E_t$$

of t many non-identity Pauli operators $E_i \in \{X, Y, Z\}$. As in the previous lecture, we will once again use that $Y = iXZ$. This motivates the shorthand notation

$$E \equiv X^{\mathbf{e}} \cdot Z^{\mathbf{f}} \qquad \text{(up to a phase)}$$

where, for bit-strings $\mathbf{e}, \mathbf{f} \in \{0,1\}^n$, we write

$$X^{\mathbf{e}} = X^{e_1} \otimes X^{e_2} \otimes \cdots \otimes X^{e_n}$$
$$Z^{\mathbf{f}} = Z^{f_1} \otimes Z^{f_2} \otimes \cdots \otimes Z^{f_n}$$

In other words, we can separately focus on X and Z-type errors. We will use the following properties:

Identities for multi-qubit Pauli operators

For all $\mathbf{e}, \mathbf{f} \in \{0,1\}^n$, the following identities hold:

- $X^{\mathbf{e}} Z^{\mathbf{f}} = (-1)^{\langle \mathbf{e}, \mathbf{f} \rangle} Z^{\mathbf{f}} X^{\mathbf{e}}$
- $H^{\otimes n} X^{\mathbf{e}} = Z^{\mathbf{e}} H^{\otimes n}$
- $H^{\otimes n} Z^{\mathbf{f}} = X^{\mathbf{f}} H^{\otimes n}$

where $H^{\otimes n} = H \otimes \cdots \otimes H$ is a product of n single-qubit Hadamard operators.

3 Quantum CSS Codes

In this section, we will introduce CSS codes—more sophisticated codes that can correct more than a single-qubit error. At a high level, a quantum CSS code that can correct quantum errors of weight t is constructed by cleverly combining the following two building blocks:

- a classical linear code that can correct up to t many classical errors (used for X-type errors), and
- another suitable linear code that can correct up to t many classical errors (used for Z-type errors).

Setup. Let $C_1 \subseteq \mathbb{F}_2^n$ and $C_2 \subseteq \mathbb{F}_2^n$ be two linear codes such that

- C_1 is an $[n, k_1]$ code;
- C_2 is an $[n, k_2]$ code with $k_2 < k_1$ and $C_2 \subseteq C_1$.

Then, if C_1 and $C_2^\perp$ can each correct up to t many classical errors, the resulting quantum CSS code is an $[[n, k_1 - k_2]]$ code that can correct up to t many quantum errors.

CSS encoding. The encoding of logical information takes place as follows:

1. Let $N = 2^{k_1 - k_2}$. Find codewords $x_0, x_1, \ldots, x_{N-1} \in C_1$ such that

$$x_i \oplus x_j \notin C_2 \qquad (\text{for } i \neq j)$$

   Note that we can always find N-many such vectors as they correspond to *cosets*[2] of C_2: indeed, by Lagrange's Theorem, the number of cosets of C_2 is precisely given by $[C_1 : C_2] = \frac{|C_1|}{|C_2|} = \frac{2^{k_1}}{2^{k_2}} = N$; importantly, two vectors are in the same coset if and only if they sum to an element in C_2.

2. Identify the N different cosets with logical states $i \in \{0, 1, 2, \ldots, N-1\}$ such that

$$|\bar{i}\rangle = |x_i \oplus C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x_i \oplus y\rangle .$$

   The codewords $\{|\bar{i}\rangle\}$ are *orthogonal* such that $\langle \bar{i} | \bar{j} \rangle = \delta_{i,j}$, which follows from the fact that we selected distinct cosets: indeed, an overlap $x_i \oplus c^{(i)} = x_j \oplus c^{(j)}$ occurs if and only if

$$x_i \oplus x_j = c^{(i)} \oplus c^{(j)} \in C_2, \qquad \text{for } c^{(i)}, c^{(j)} \in C_2.$$

   By construction, however, we ensured that $x_i \oplus x_j \notin C_2$.

Then, we can encode an arbitrary state $|\psi\rangle$ on $k_1 - k_2$ many qubits into an n-qubit state $|\overline{\psi}\rangle$ via

$$|\psi\rangle = \sum_{i=0}^{N-1} \alpha_i |i\rangle \quad \mapsto \quad |\overline{\psi}\rangle = \sum_{i=0}^{N-1} \alpha_i |\bar{i}\rangle .$$

3.1 Error-correction.

Suppose that the physical n-qubit state $|\overline{\psi}\rangle$ gets corrupted by an error $E \equiv X^{\mathbf{e}} Z^{\mathbf{f}}$ where $\mathbf{e}, \mathbf{f} \in \{0,1\}^n$ are strings of weight t; in other words, we have

$$\begin{aligned} |\overline{\psi}\rangle \quad &\mapsto \quad X^{\mathbf{e}} Z^{\mathbf{f}} |\overline{\psi}\rangle \\ &= \sum_{i=0}^{N-1} \alpha_i X^{\mathbf{e}} Z^{\mathbf{f}} |\bar{i}\rangle \\ &= \sum_{i=0}^{N-1} \alpha_i (-1)^{\langle \mathbf{e}, \mathbf{f} \rangle} Z^{\mathbf{f}} |x_i \oplus C_2 \oplus \mathbf{e}\rangle . \end{aligned}$$

To correct the error $E \equiv X^{\mathbf{e}} Z^{\mathbf{f}}$, we will correct the X-errors and the Z-errors separately.

[2] A *coset* of the codespace $C_2 \subseteq C_1$ is an additive shift $x \oplus C_2 = \{x \oplus c : c \in C_2\}$ for some $x \in C_1$.

Correcting the X-errors. Let $H_1 \in \mathbb{F}_2^{(n-k_1)\times n}$ denote the parity check matrix for the linear code C_1. To correct the bit-flip error $X^{\mathbf{e}}$, we proceed as follows:

1. Coherently compute the C_1 error syndrome (resulting from multiplication by H_1) into an ancilla:

$$\sum_{i=0}^{N-1} \alpha_i \, (-1)^{\langle \mathbf{e},\mathbf{f}\rangle} \, Z^{\mathbf{f}} \, |x_i \oplus C_2 \oplus \mathbf{e}\rangle \quad \mapsto \quad \sum_{i=0}^{N-1} \alpha_i \, (-1)^{\langle \mathbf{e},\mathbf{f}\rangle} \, Z^{\mathbf{f}} \, |x_i \oplus C_2 \oplus \mathbf{e}\rangle \otimes |H_1 \cdot (x_i \oplus C_2 \oplus \mathbf{e})\rangle$$

   Recall that $C_2 \subseteq C_1$, and hence the second register simplifies as follows:

$$H_1 \cdot (x_i \oplus C_2 \oplus \mathbf{e}) = \underbrace{H_1 x_i}_{=0} \oplus \underbrace{H_1 C_2}_{=0} \oplus H_1 \mathbf{e} = H_1 \mathbf{e} \pmod 2.$$

   Crucially, the second system is now completely unentangled from the rest of the state.

2. Measure the second register in the computational basis to obtain the syndrome $H_1\mathbf{e}$.

3. Apply syndrome decoding to $H_1\mathbf{e}$ to recover $\mathbf{e}$. Note that $\mathbf{e}$ has weight t and C_1 can correct t errors.

4. Correct the error by applying $X^{\mathbf{e}}$.

At the end of this procedure, the state is now of the form

$$X^{\mathbf{e}} Z^{\mathbf{f}} \, |\overline{\psi}\rangle \quad \mapsto \quad Z^{\mathbf{f}} \, |\overline{\psi}\rangle \; = \; \sum_{i=0}^{N-1} \alpha_i \; Z^{\mathbf{f}} \, |x_i \oplus C_2\rangle \; = \; \sum_{i=0}^{N-1} \alpha_i \; Z^{\mathbf{f}} \, X^{x_i} \, |C_2\rangle \, .$$

Correcting the Z-errors. We now explain how to correct the phase-flip error $Z^{\mathbf{f}}$. Let $H_2 \in \mathbb{F}_2^{k_2\times n}$ denote a generator matrix for the code C_2, equivalently a parity check matrix for the dual code $C_2^{\perp}$. To diagnose the Z-errors, we proceed as follows:

1. Apply a transversal Hadamard transform $H^{\otimes n}$ to the data qubits. This yields

$$\begin{aligned} H^{\otimes n} Z^{\mathbf{f}} \, |\overline{\psi}\rangle &= \sum_{i=0}^{N-1} \alpha_i \; H^{\otimes n} Z^{\mathbf{f}} X^{x_i} \, |C_2\rangle \\ &= \sum_{i=0}^{N-1} \alpha_i \; X^{\mathbf{f}} Z^{x_i} H^{\otimes n} \, |C_2\rangle \\ &= \sum_{i=0}^{N-1} \alpha_i \; (-1)^{\langle \mathbf{f}, x_i\rangle} Z^{x_i} X^{\mathbf{f}} H^{\otimes n} \, |C_2\rangle \, . \end{aligned}$$

   Notice that the operator $Z^{\mathbf{f}}$ gets converted into a bit-flip $X^{\mathbf{f}}$ acting in the Hadamard basis. In other words, the phase error has been mapped to a classical bit-flip error, which can now be diagnosed and corrected using standard syndrome decoding techniques for the code $C_2^{\perp}$.

   Next, we require the following technical fact.

Fact: Hadamard transform of a code coset

Let $C \subseteq \mathbb{F}_2^n$ be a linear code and $|C\rangle = \frac{1}{\sqrt{|C|}} \sum_{c \in C} |c\rangle$. Then

$$H^{\otimes n} |C\rangle = \frac{1}{\sqrt{|C^\perp|}} \sum_{z \in C^\perp} |z\rangle .$$

Proof. Starting from the definition of $|C\rangle$ and applying the Hadamard transform, we obtain

$$\begin{aligned} H^{\otimes n} |C\rangle &= \frac{1}{\sqrt{|C|}} \sum_{c \in C} H^{\otimes n} |c\rangle \\ &= \frac{1}{\sqrt{|C|}} \sum_{c \in C} \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} |y\rangle \\ &= \frac{1}{\sqrt{|C|\, 2^n}} \sum_{y \in \{0,1\}^n} \left(\sum_{c \in C} (-1)^{\langle c, y \rangle} \right) |y\rangle . \end{aligned}$$

We now analyze the inner sum. If $y \in C^\perp$, then $\langle c, y \rangle = 0$ for all $c \in C$, and hence

$$\sum_{c \in C} (-1)^{\langle c, y \rangle} = |C|.$$

If $y \notin C^\perp$, then there exists some $c_0 \in C$ such that $\langle c_0, y \rangle = 1$, and the terms in the sum cancel pairwise, yielding

$$\sum_{c \in C} (-1)^{\langle c, y \rangle} = 0.$$

Therefore, the sum over y collapses to a sum over $C^\perp$, and we obtain

$$H^{\otimes n} |C\rangle = \frac{\sqrt{|C|}}{\sqrt{2^n}} \sum_{y \in C^\perp} |y\rangle .$$

Using $|C| \cdot |C^\perp| = 2^n$, this simplifies to the claimed expression. □

Applying the above fact to C_2, we conclude that

$$H^{\otimes n} |C_2\rangle = \frac{1}{\sqrt{|C_2^\perp|}} \sum_{z \in C_2^\perp} |z\rangle \; = \; |C_2^\perp\rangle .$$

Plugging this into the previous expression, this implies

$$H^{\otimes n} Z^{\mathbf{f}} |\overline{\psi}\rangle = \sum_{i=0}^{N-1} \alpha_i \; (-1)^{\langle \mathbf{f}, x_i \rangle} Z^{x_i} X^{\mathbf{f}} |C_2^\perp\rangle = \sum_{i=0}^{N-1} \alpha_i \; (-1)^{\langle \mathbf{f}, x_i \rangle} Z^{x_i} |C_2^\perp \oplus \mathbf{f}\rangle .$$

Thus, after the Hadamard transform, the encoded state becomes a superposition over the dual code $C_2^\perp$, and the error operator $X^{\mathbf{f}}$ acts as a classical bit-flip error on this superposition. This allows us to diagnose and correct $\mathbf{f}$ using standard syndrome decoding for the code $C_2^\perp$.

2. Coherently compute the $C_2^{\perp}$ error syndrome using the parity check matrix H_2:

$$\sum_{i=0}^{N-1} \alpha_i \, (-1)^{\langle \mathbf{f}, x_i \rangle} Z^{x_i} \, |C_2^{\perp} \oplus f\rangle \quad \mapsto \quad \sum_{i=0}^{N-1} \alpha_i \, (-1)^{\langle \mathbf{f}, x_i \rangle} Z^{x_i} \, |C_2^{\perp} \oplus \mathbf{f}\rangle \otimes |H_2 \cdot (C_2^{\perp} \oplus \mathbf{f})\rangle \, .$$

   Since H_2 generates C_2 and hence annihilates all elements of C_2, the second register simplifies to

$$H_2 \cdot (C_2^{\perp} \oplus \mathbf{f}) = \underbrace{H_2 C_2^{\perp}}_{=0} \oplus H_2 \mathbf{f} = H_2 \mathbf{f} \pmod 2,$$

   which is independent of i and thus unentangled from the logical state.

3. Measure the second register in the computational basis to obtain the syndrome $H_2\mathbf{f}$.

4. Apply syndrome decoding for the code $C_2^{\perp}$ to recover the error vector $\mathbf{f}$. This is possible since $\mathbf{f}$ has weight t and $C_2^{\perp}$ can correct up to t errors.

5. Apply the corrective operator $X^{\mathbf{f}}$, undo the Hadamard transform by applying $H^{\otimes n}$ again, thereby correcting the original Z-error.

After this procedure, all phase errors have been removed and the logical state $|\overline{\psi}\rangle$ is fully restored (up to an irrelevant global phase).