CMPT 476 Lecture 28

Quantum error-correcting codes

Last class we showed that quantum bit flip errors can be corrected by encoding the computational basis states (NOT the quantum state itself) in an ECC – code (error correcting)

Expectation	Reality
$\|47147147\rangle$	$\alpha\|1000\rangle + \beta\|1111\rangle$

Today we delve into the theoretical and general construction of QECCs and why this model suffices to correct the entire continuum of quantum errors.

(Quantum error models)

In the last lecture we noted that quantum errors are remarkably **free**. That is, we have a continuum of errors where any unitary may theoretically be applied. Our first order of business is to **discretize** the set of possible errors to a finite set which we can then focus on correcting. This is possible roughly because:

1. We can write error operators as linear combinations over a (finite) basis, and
2. We can use (projective) measurements to **project** a linear combination of errors down to **one particular error** without **destroying the state**.

As in last class, we make one **BIG** assumption:

Errors on individual qubits are independent

That is, the **bit flip channel** for instance applies **individually** and **independently** to each qubit in a system.

(Quantum bit flip channel)

Like in the classical case, the quantum bit flip channel is a **probabilistic process** that sends a state $|\psi\rangle$ to $|\psi\rangle$ with probability $1-p$, and $X|\psi\rangle$ (i.e. with a bit flip error) with probability p. We can represent the state afterwards as a **mixed state** or **ensemble**

$$\{(1-p, |\psi\rangle), (p, |\psi\rangle)\}$$

Since multiple consecutive bit flip channels may be applied, the input itself may be a mixed state, so as a function of a density matrix we can define the bit flip channel $\mathcal{E}_X$ as

$$\mathcal{E}_X(\rho) = (1-p)\rho + pX\rho X$$

Recall in particular that given a density matrix ρ, we apply a unitary U to ρ as $U\rho U^+$, so $\mathcal{E}_X$ can be viewed as sending $\rho \to I\rho I$ with probability $1-p$ and $\rho \to X\rho X$ with probability p.

(Quantum Channels)

The bit flip channel is an example of a **quantum channel**, which is a process that sends **density matrices to density matrices**

$$\mathcal{E}: \rho \longmapsto \mathcal{E}(\rho)$$

The most general types of quantum errors correspond to quantum channels. If the error is in fact **unitary**, such as a slow persistent rotation around the **x-axis**:

$$\mathcal{E}(\rho) = R_X^+(\theta)\,\rho\, R_X(\theta)$$

then it is called **coherent** and can often be corrected by proper calibration. **Stochastic** errors like the bit-flip channel on the other hand are called **incoherent**.

Mathematically, we can model channels in **many** ways, but the one with the closest intuition to stochastic errors uses **kraus operators**.

(Kraus operators)

Let $\mathcal{E}$ be a quantum channel on a Hilbert space $\mathcal{H}$. Then there exists a finite set of operators $\{M_a\}$ on $\mathcal{H}$ such that

1. $\sum_a M_a^\dagger M_a = I$
2. $\mathcal{E}(\rho) = \sum_a M_a \rho M_a^\dagger$

Such a set (which is not unique) $\{M_a\}$ is called a set of Kraus operators for $\mathcal{E}$.

Ex.

The bit flip channel $\mathcal{E}_X(\rho) = (1-p)\rho + pX\rho X$ has Kraus operators

$$\{\sqrt{1-p}\, I, \sqrt{p}\, X\}$$

Ex.

Measurement in the computational (or any basis) is a quantum channel. Recall that measurement of a qubit ρ produced the state $P_0\rho P_0 + P_1 \rho P_1$ where $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$ satisfied $P_0^\dagger P_0 + P_1^\dagger P_1 = I$. Hence measurement is a channel with Kraus operators

$$\{P_0, P_1\}$$

Ex.

A Pauli channel is one with Kraus operators

$$\{\sqrt{p_i}\, I, \sqrt{p_x}\, X, \sqrt{p_y}\, Y, \sqrt{p_z}\, Z\}$$

which sends $\rho \longmapsto p_i\rho + p_x X\rho X + p_y Y\rho Y + p_z Z\rho Z$.

As we explore now it turns out that it suffices to consider only Pauli channels when correcting errors.

(Error correction and channels)

Let $\mathcal{H}_L$ and $\mathcal{H}_P$ be the logical and physical Hilbert space, respectively, and $\dim(\mathcal{H}_P) \geq \dim(\mathcal{H}_L)$. A quantum error correcting code is defined by an encoding of the basis $|i\rangle \in \mathcal{H}_L$ of $\mathcal{H}_L$ into orthogonal states $|i\rangle_L \in \mathcal{H}_P$ of $\mathcal{H}_P$.

(Note that $\text{span}(\{|i\rangle_L\})$ is a $\dim(\mathcal{H}_L)$ subspace of $\mathcal{H}_P$ called the codespace)

If $|\psi\rangle = \sum_i \alpha_i |i\rangle$, then the encoding of $|\psi\rangle$ is

$$|\psi\rangle_L = \sum_i \alpha_i |i\rangle_L$$

Let $\{E_a\}$ be a set of Kraus operators for a quantum error channel $\mathcal{E}^Q$ on $\mathcal{H}_P$. With the encoding $|i\rangle_L$, the errors $\{E_a\}$ are correctable or recoverable if and only if

$${}_L\langle i| E_a^\dagger E_b |j\rangle_L = \begin{cases} 0 & \text{if } i \neq j \\ c_{ab} & \text{otherwise} \end{cases}$$

In particular, errors are recoverable if and only if orthogonal states remain orthogonal after the application of errors.

Ex.

For the three-bit code we have the single bit flip errors

$$\{I \otimes I \otimes I, X \otimes I \otimes I, I \otimes X \otimes I, I \otimes I \otimes X\}$$

Graphing the states $E_a|0\rangle_L$ and $E_b|1\rangle_L$ we have

	$I\otimes I\otimes I$	$X\otimes I\otimes I$	$I\otimes X\otimes I$	$I\otimes I\otimes X$
$\|0\rangle_L = \|000\rangle$	$\|000\rangle$	$\|100\rangle$	$\|010\rangle$	$\|001\rangle$
$\|1\rangle_L = \|111\rangle$	$\|111\rangle$	$\|011\rangle$	$\|101\rangle$	$\|110\rangle$

It can be observed that ${}_L\langle 0|E_a^\dagger E_b|1\rangle_L = 0$ for every E_a, E_b from the table above, and hence a single bit flip is correctible (as we saw explicitly last class).

On the other hand,

$${}_L\langle 0|(X\otimes X\otimes I)(I\otimes I\otimes X)|1\rangle_L \neq 0$$

so two bit flips are not correctible with this encoding.

Proposition (linear combinations of errors)

Let $\{E_a\}$ be a set of correctible errors for some code. If $\{E_b'\}$ is a set of errors such that

$$E_b' = \sum_a \alpha_a E_a \quad \forall b$$

that is each E_b' is a linear combination of errors in $\{E_a\}$, then $\{E_b'\}$ is also correctible.

(Discretization of errors)

Since the Pauli operators $\{I, X, Y, Z\}$ form a basis for single-qubit operators, the above proposition tells us that we only need to correct Pauli errors to correct any single qubit error.

(Correcting Pauli errors)

We already know how to correct bit flip or X errors, so now let's think about how we could correct other Pauli errors, starting with Z. Z-type errors define the phase flip channel

$$\mathcal{E}_Z^Q : \rho \longrightarrow (1-p)\rho + pZ\rho Z$$

While a phase flip is un-classical, it's really no different from a bit flip, just in the Hadamard basis:

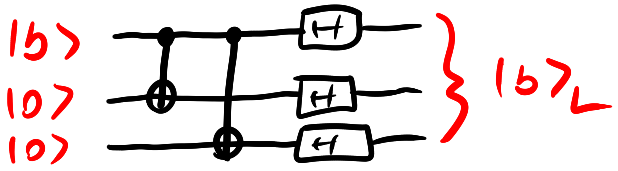
$$X : |0\rangle \longleftrightarrow |1\rangle$$

$$Z : |+\rangle \longleftrightarrow |-\rangle$$

Intuitively, we should be able to protect against Z errors by using the bit flip code over the Hadamard basis. In particular, we define a three-bit phase flip code by

$$|0\rangle_L = |+++\rangle \qquad |1\rangle_L = |---\rangle$$

Note that the encoder in this case is just the bit flip encoder followed by Hadamard gates on each qubit.



As in the bit flip code, a single phase flip is correctible

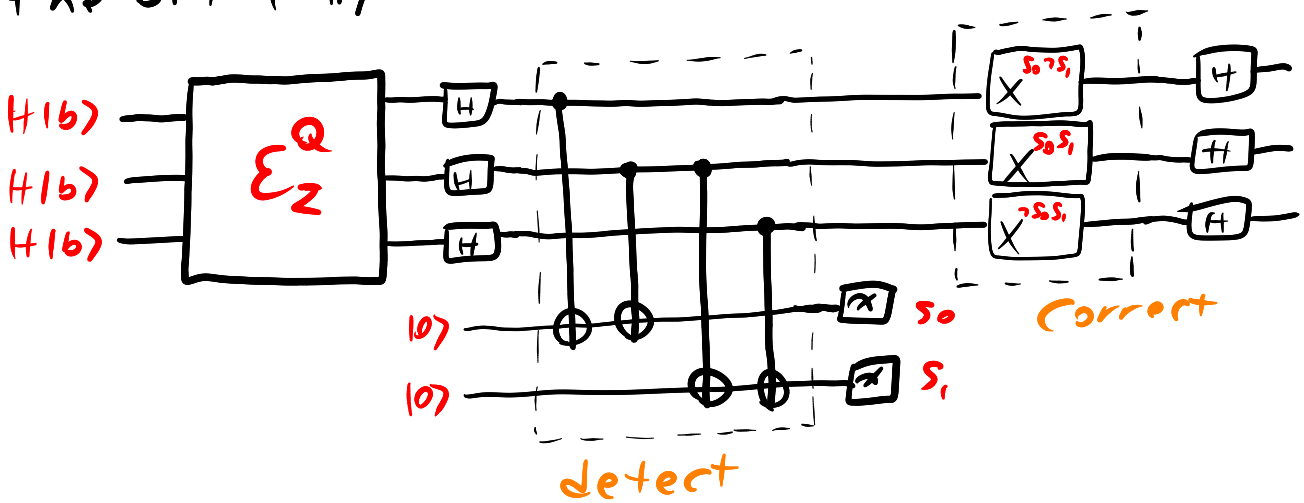
	$I\otimes I\otimes I$	$Z\otimes I\otimes I$	$I\otimes Z\otimes I$	$I\otimes I\otimes Z$
$\|0\rangle_L = \|+++\rangle$	$\|+++\rangle$	$\|-++\rangle$	$\|+-+\rangle$	$\|++-\rangle$
$\|1\rangle_L = \|---\rangle$	$\|---\rangle$	$\|+--\rangle$	$\|-+-\rangle$	$\|--+\rangle$

(Syndrome decoding)

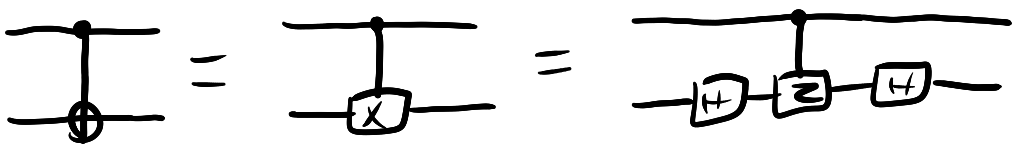
For the bit flip code, we corrected by measuring the syndrome — the parities of bits 1&2 and 2&3. One option to perform correction in the phase flip code is to simply switch back to the bit flip code using H gates and then use the bit flip decoder. This works because H maps Z errors to X errors:

$$HZ|+\rangle = H|-\rangle = |1\rangle = X|0\rangle = XH|+\rangle$$

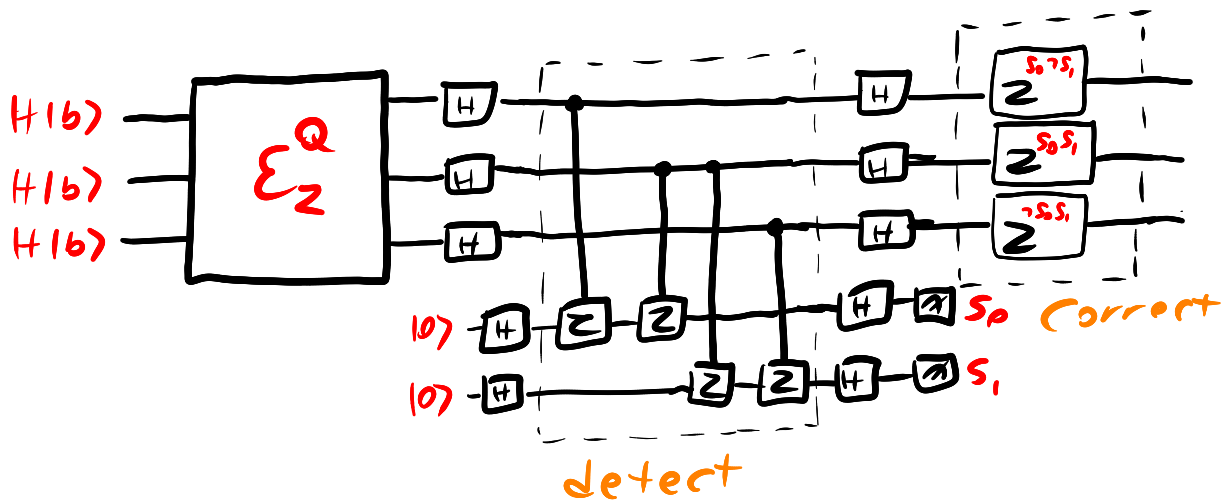
So we can write the correction procedure using the bit flip decoder as



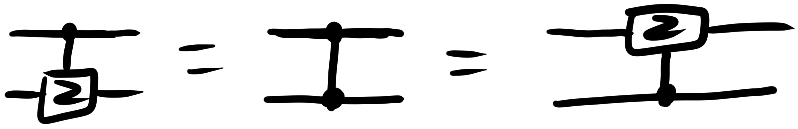
Noting that



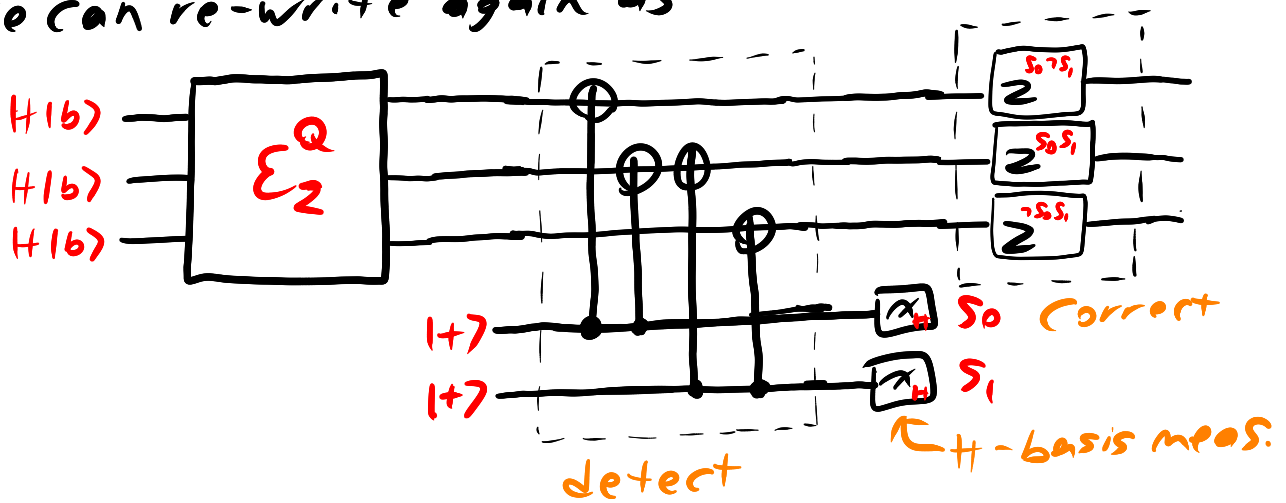
we can write the above instead as



Now using the fact that



we can re-write again as



Which is the in-basis syndrome measurement and correction for the phase flip code. In particular, it uses phase kickback to measure the phase parities of qubits 1&2 and 2&3.

(Correcting one bit and one phase flip)

While we've shown how to correct a bit or phase flip, the use different codes, so we can only protect against one kind of error at a time. As Peter Shor showed in the 90's however, if we concatenate the two codes we can in fact correct either (or both) error. This is the 9-qubit code.

The construction of the code uses 2-layers of encoding, called Concatenation. The outer layer constitutes the phase flip code, while the inner uses the bit flip code

Outer layer	Inner layer
$\|0\rangle_L = \|+++\rangle_I$	$\|+\rangle_I = \frac{1}{\sqrt{2}}(\|000\rangle + \|111\rangle)$
$\|1\rangle_L = \|---\rangle_I$	$\|-\rangle_I = \frac{1}{\sqrt{2}}(\|000\rangle - \|111\rangle)$

Writing the code out explicitly,

$$|0\rangle_L = \frac{1}{2\sqrt{2}} (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$|1\rangle_L = \frac{1}{2\sqrt{2}} (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$$

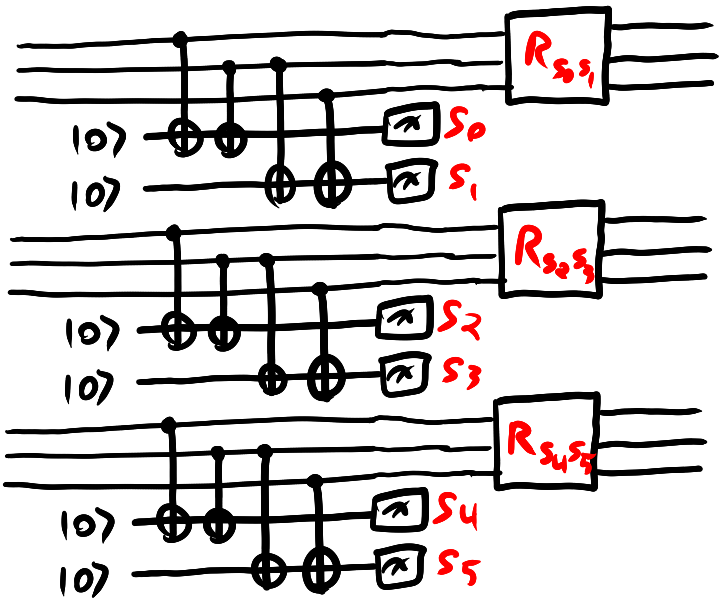
Intuitively, each set of 3 qubits encodes a state in the bit flip code, so we can correct a bit flip on any block:

we often drop $\otimes$ in QECC for brevity

$$IIXIIIIII\,|0\rangle_L = \frac{1}{2\sqrt{2}} (|001\rangle + |110\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$|001\rangle + |110\rangle$: correctible via syndrome decoding

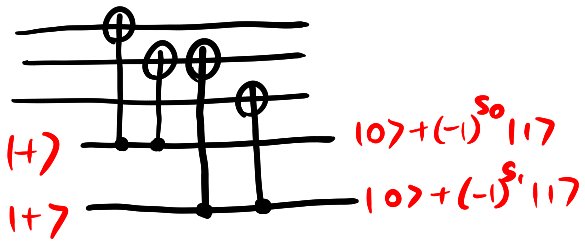
In particular, to correct X errors, we do syndrome decoding on each block:



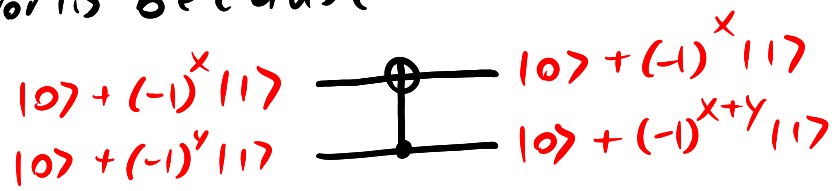
Phase errors are a little trickier to correct. Note that a Z error on any of the three blocks of 3 qubits swaps the encoded $|+\rangle \leftrightarrow |-\rangle$. E.g.

$$IIIIZIIIII\,|1\rangle_L = \frac{1}{2\sqrt{2}} (|000\rangle - |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle - |111\rangle)$$

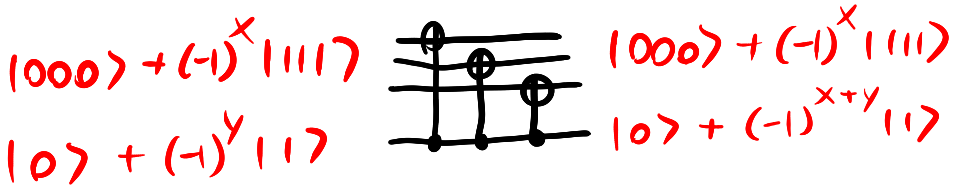
Since the blocks are in an encoded $|+/-\rangle$ state, we can't simply apply a hadamard and measure the bit flip syndrome. Recall that the in-basis syndrome measurement for the phase flip code used phase kickback



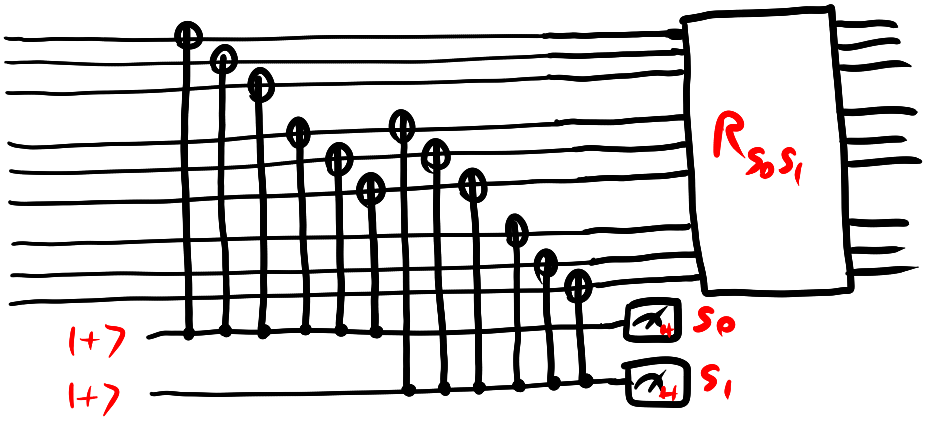
This works because



Likewise, observe that



Which we can now use to compute the syndrome for the outer (phase flip) code



Now, if we combine both corrections we can observe that either one X, one Z, or one X AND one Z error can be corrected, since the error corrections for one are invariant to errors of the other. Moreover, since $Y = iXZ$, this means the Shor code can correct a single Pauli error!

(Shor code adequacy for single-qubit errors)

Just restating what we've shown. The Shor 9-qubit code can correct a single error from the set $\{I, X, Y, Z\}$ of Pauli operators (taken as a single Pauli on a single qubit). Combined with the fact that any error that is expressible as a sum of Paulis is also correctible, Shor's code can hence correct any error of the form

$$|\psi\rangle \longmapsto I^{\otimes m} \otimes U \otimes I^{\otimes n-m-1} |\psi\rangle$$

where U is an arbitrary single-qubit unitary.

Shor's code is what showed that quantum error correction was even possible in principle, but there are some serious issues:

1. It's really a bad code...
2. We can't decode our state to compute on it without exposing it to errors

We'll cover 2. next class, but for 1. it suffices to know that many interesting and useful codes have been developed through an elegant formalism due to Daniel Gottesman called the stabilizer formalism. Among other things, the stabilizer formalism allows classical error correcting codes to be directly used as Pauli error correcting codes.

(Stabilizer formalism) (mostly for interest)

Stabilizer codes and the **stabilizer formalism** is the standard method of constructing and studying codes for quantum computers, and all the codes we have seen so far are examples of stabilizer codes.

(Stabilizer codes)

Let S be a set of n-qubit Pauli operators. The set S defines a **codespace**

$$C(S) = \{|\psi\rangle \mid P_i|\psi\rangle = |\psi\rangle \ \forall P_i \in S\}$$

which is the **simultaneous +1-eigenspace** of all $P_i \in S$. The term **Stabilizer** comes from group theory, where S is said to **stabilize** the codespace $C(S)$.

(Number of logical qubits from a stabilizer)

We say that a set S of Paulis is **independent** if

$$P_1 P_2 \cdots P_m \neq I \quad \leftarrow \text{up to global phase}$$

for any distinct $P_1 \cdots P_m \in S$. If S is a set of $n-k$ independent, **and commuting** Paulis, then

$$\dim(C(S)) = 2^k$$

In other words, $C(S)$ encodes the state of k logical qubits.

Ex.

shorthand for $I \otimes Z \otimes Z$

Let $S = \{ZZI, ZIZ, IZZ\}$. Observe that

$$P|000\rangle = |000\rangle$$
$$P|111\rangle = (-1)^2|111\rangle = |111\rangle \quad \forall P \in S$$

Note that S is not linearly independent, since

$$(ZZI)(ZIZ)(IZZ) = (ZZI)(ZZI) = I$$

If we take $S' = \{ZZI, ZIZ\}$ now we have a linear independent set of $2 = 3-1$ Paulis, which gives a codespace of dimension $2^1 = 2$. Hence

$$C(S') = \{\alpha|000\rangle + \beta|111\rangle \mid |\alpha|+|\beta| = 1\}$$

This is exactly the 3-bit bit flip code!

Now observe what an X error does — if $|\psi\rangle$ is in the $+1$-eigenspace of Z (i.e $Z|\psi\rangle = |\psi\rangle$), then X sends $|\psi\rangle$ to Z's -1-eigenspace:

$$Z(X|\psi\rangle) = ZX|\psi\rangle = -XZ|\psi\rangle = -X|\psi\rangle$$

In the case of S' we see

$$XII \longrightarrow \{-ZZI, -ZIZ\}$$
$$IXI \longrightarrow \{-ZZI, ZIZ\}$$
$$IIX \longrightarrow \{ZZI, -ZIZ\}$$

Denoting $s_0 = \begin{cases} 0 \text{ if } ZZI|\psi\rangle = |\psi\rangle \\ 1 \text{ if } ZZI|\psi\rangle = -|\psi\rangle \end{cases}$ and likewise for s_1 and ZIZ, we see that the bit string $s_0 s_1$ is a syndrome of $|\psi\rangle$.

Note: we previously used the generators ZZI, IZZ for the syndrome — either choice is equally valid as we can now see, and just results in a different correction.

(Syndrome of a stabilizer code)

Let $S \subseteq P_n$. The syndrome of $|\psi\rangle$ is the result of measuring each $P_i \in S$. That is, if $|S| = n-k$ then the syndrome of $|\psi\rangle$ is $s \in \mathbb{Z}_2^{n-k}$ such that

$$s_i = \begin{cases} 0 \text{ if } P_i|\psi\rangle = |\psi\rangle \\ 1 \text{ if } P_i|\psi\rangle = -|\psi\rangle \end{cases}$$

Ex.

Let $S = \{XXI, XIX\}$. Then

$$C(S) = \{\alpha|+++\rangle + \beta|---\rangle \mid |\alpha|^2 + |\beta|^2 = 1\}$$

To measure the syndrome, we need to measure the observables XXI, XIX. Let's consider XX. It's $+1$-eigenspace is

$$\text{span}\{|++\rangle, |--\rangle\} = P_+$$

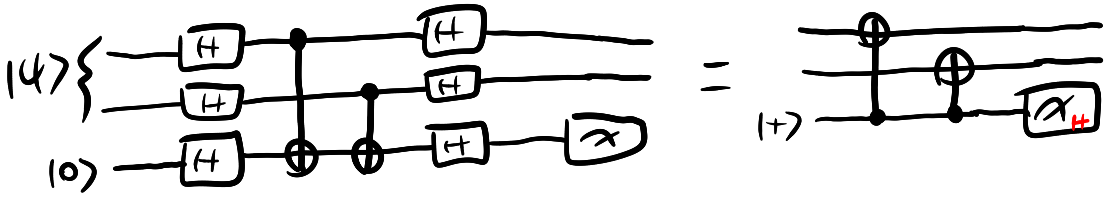
while its -1-eigenspace is

$$\text{span}\{|+-\rangle, |-+\rangle\} = P_-$$

To measure the XX observable, we hence do a projective measurement with projectors

$$\{P_+, P_-\}$$

Note that this is just a parity measurement in the hadamard basis, so we can do a basis change and measure the parity as before



Ex.

The Shor code has stabilizers

$$ZZI\ III\ III$$
$$ZIZ\ III\ III$$
$$III\ ZZI\ III$$
$$III\ ZIZ\ III$$
$$III\ III\ ZZI$$
$$III\ III\ ZIZ$$

$$XXX\ XXX\ III$$
$$XXX\ III\ XXX$$

Note that the stabilizers are in fact all independent and commute, since for example

$$(ZZI)(XXX) = (-1)^2 (XXX)(ZZI)$$
$$= (XXX)(ZZI)$$

It can also be readily verified that

$$P|0\rangle_L = |0\rangle_L$$
$$P|1\rangle_L = |1\rangle_L$$

for each stabilizer P above. Since we have 8 stabilizers on 9 qubits, the dimension of the codespace is 2, corresponding to 1 logical qubit as expected.