# Misc info

References on classical linear codes and CSS codes: NC Chp 10.4. In particular, I skipped most of 10.4.2 (a more concrete description of CSS codes) to make room for the stabilizer formalism, but you may want to be familiar with 10.4.2 in preparation for the Shor-Preskill security proof for QKD (and for the comprehensive).

References of the QECC criterion: Sevag Gharibian made scribe notes in the Fall 2006 lecture (available from Ashwin's homepage) which is very similar to the lecture, but including many many details in the derivation. You can also use NC Chp 10.3-10.3.1.

I added comments on degenerate codes. The 9-bit code example was essentially finished last class, so, I won't go back to it. I added a page of the 4-bit code in the notes.

# Nondegenerate and degenerate codes

**Definition:** Notations as in QECC conditions (1) and (2). For the error set $\mathbb{E}$, if $\mathcal{C}$ is called **non-degenerate** if $c$ has full rank, else, $\mathcal{C}$ is **degenerate**.

**Concept of degeneracy:** $\{E_i P\}$ is linearly dependent, ie, some errors act like a linear combination of others. The syndromes cannot be unique, yet error correction works (generally by changing to the $F_k$ error basis, but most known examples simply have errors acting identically on the codespace so that there's no need to distinguish them).

We have kept full generality when considering codes that correct for span($\mathbb{E}$) for the most general $\mathbb{E}$. For concreteness and for most practical purpose, we consider more specific $\mathbb{E}$.

# The Pauli Group

**Def:** The Pauli group, denoted $\mathcal{P}_n$, consists of all $n$-qubit tensor products of $I, X, Y, Z$ with overall phases $\pm 1, i$. Let $\tilde{\mathcal{P}}_n$ be the quotient set without the phases.

e.g. $X \otimes X \in \mathcal{P}_2$, $iI \otimes Y \otimes Z \otimes I \in \mathcal{P}_4$.

**Facts:** (1) $\forall p \in \mathcal{P}_N, p^2 = \pm I$.
(2) $\forall p, q \in \mathcal{P}_N$, $pq = \pm qp$.
(3) $\text{span}(\tilde{\mathcal{P}}_n) = \mathcal{B}(\mathbb{C}^{2 \otimes n})$.

**Def:** The wt of $p \in \mathcal{P}_n$ is the number of non-identity tensor factors. Let $\tilde{\mathcal{P}}_{n,t} \subset \tilde{\mathcal{P}}_n$ be the subset with wt $\leq t$.

NB The Pauli group is an important concept.

# Distance of QECC for the Pauli error basis

**Def:** consider $t$-qubit errors as CP maps (no T) with Kraus operators all in span($\tilde{\mathcal{P}}_{n,t}$).

e.g.1 if $\mathcal{E}$ is a qubit TCP map, then, $\mathcal{E}^{\otimes t} \otimes \mathcal{I}^{\otimes (n-t)}$ is a $t$-qubit error, but there are many others.

e.g.2 let $\mathcal{E}(\rho) = (1-\eta)\rho + \eta/3(X\rho X + Y\rho Y + Z\rho Z)$ and consider $\mathcal{E}^{\otimes n}$. There are $4^n$ terms in the Kraus rep, and $\sum_{i=0}^{t} \binom{n}{i} 3^i$ terms with Kraus operators in span($\tilde{\mathcal{P}}_{n,t}$). The latter form a $t$-qubit error, but not included in e.g.1.

**Def:** Distance of a QECC is the min wt $p \in \mathcal{P}$ s.t. $PpP \neq c(p)P$.

**Fact:** Distance $d$ QECC corrects for $t$-qubit errors with $t = \lfloor (d-1)/2 \rfloor$ errors, corrects for $d-1$ erasure errors, and detect $d-1$ errors.

# CSS code example 2: the 9-bit Shor code

$$|0_L\rangle = (|000\rangle + |111\rangle)^{\otimes 3}$$
$$|1_L\rangle = (|000\rangle - |111\rangle)^{\otimes 3}$$

By inspection, it is a CSS code with:

$$M_Z = \begin{bmatrix} Z & Z & I & I & I & I & I & I & I \\ I & Z & Z & I & I & I & I & I & I \\ I & I & I & Z & Z & I & I & I & I \\ I & I & I & I & Z & Z & I & I & I \\ I & I & I & I & I & I & Z & Z & I \\ I & I & I & I & I & I & I & Z & Z \end{bmatrix}$$

$$M_X = \begin{bmatrix} X & X & X & X & X & X & I & I & I \\ I & I & I & X & X & X & X & X & X \end{bmatrix}$$

# CSS code example 2: the 9-bit Shor code

The phase code has distance $d_P = 2$, but $\mathcal{C}$ still corrects for any phase error. e.g. $Z_{1,2,3}$ all have the same syndrome, but they also all act the same way (as the product of any two is a $Z$ stabilizer) so there is no need to distinguish them.

This is a **degenerate** code, and it has distance 3, correcting any 1-qubit error. Exercise: verify the QECC condition (2) for $\mathbb{E} = \tilde{\mathcal{P}}_{9,1}$.

We will see in the 3rd part of the course that degenerate codes prevent the quantum capacity in terms of the coherent information to have a single-letter expression.

# CSS code example: two 4-bit codes

Code 1: $|0_L\rangle = (|0000\rangle + |1111\rangle)$, $|1_L\rangle = (|0011\rangle + |1100\rangle)$

By inspection, it is a CSS code with:

$$M_Z = \begin{bmatrix} Z & Z & I & I \\ I & I & Z & Z \end{bmatrix}$$

$$M_X = \begin{bmatrix} X & X & X & X \end{bmatrix}$$

We're not yet there to understand how, but it can correct for 1 amplitude damping error. It is in the same family as the 9 bit Shor code (which corrects for 2 amplitude damping errors).

Code 2:

$M_Z = ZZZZ$, $M_X = XXXX$. It is a $[4, 2, 2]$ code instead (distance 2) which encodes 2-qubits in 4 and detects any 1-qubit error or corrects for any 1 erasure error. (Ex: check)