Quantum Error Correction
Notes for lecture 9

Prepared by Casey Myers
Edited by Daniel Gottesman

February 10th, 2004

Quantum MacWilliams identity

Let $E_d \in \{\text{Pauli operators with weight } wt = d\}$. Eg. $E_0 = \{I\}$, $E_1 \in \{X_1, X_2, Z_1, Y_1, \cdots\}$.
Two Hermitian operators θ_1, θ_2

$$A_d = \frac{1}{\text{tr}\theta_1 \text{tr}\theta_2} \sum_{E_d} \text{tr}(E_d\theta_1)\text{tr}(E_d^\dagger\theta_2) \tag{1}$$

$$B_d = \frac{1}{\text{tr}\theta_1\theta_2} \sum_{E_d} \text{tr}\big(E_d\theta_1 E_d^\dagger\theta_2\big) \tag{2}$$

For a QECC, $\theta_1 = \theta_2 = \pi$ (Projector on coding space).
For a stabilizer code $\pi = \frac{1}{2^{n-k}} \sum_{M\in S} M$ ($\text{tr}I = 2^n$, $\text{tr}E = 0, E \neq I$).

$$\begin{aligned} A_d &= \frac{1}{2^{2k}} \sum_{E_d} \Big(\text{tr}\big(\frac{1}{2^{n-k}} \sum_{M\in S} E_d M\big)^2\Big) \qquad (3) \\ &= \frac{1}{2^{2k}} \frac{1}{(2^{n-k})^2} \sum_{E_d} \{0 \text{ if } E_d \notin S \text{ OR } 2^n \text{ if } E_d \in S\}^2 \\ &= \#\text{ Pauli operators of weight } d \text{ in } S. \end{aligned}$$

$$\begin{aligned} B_d &= \frac{1}{2^k}\sum_{E_d}\sum_{M,N\in S}\frac{1}{2^{2(n-k)}}\mathrm{tr}\big(E_d M E_d^\dagger N\big) \qquad (4) \\ &= \frac{1}{2^{2n-k}}\sum_{E_d}\sum_{M,N\in S}\delta_{MN}2^n(-1)^{C(M,E_d)} \\ &= \frac{1}{2^{n-k}}\sum_{E_d}\Big[\sum_{M\in S}(-1)^{C(M,E_d)}\Big] \end{aligned}$$

where $C(M,E_d)=0$ if $[M,E_d]=0$ OR 1 if $\{M,E_d\}=0$

and $\sum_{M\in S}(-1)^{C(M,E_d)}=2^{n-k}$ if $[E_d,M]=0\ \forall M\in S\ \Leftrightarrow E_d\in N(S)$ OR 0 if $E_d\notin N(S)$.

Suppose $E_d\notin N(S)\Rightarrow\exists M\in S,\ \{M,E_d\}=0$.

$NE_d=(-1)^{C(N,E_d)}E_dN$

$(MN)E_d=(-1)^{C(N,E_d)+1}E_d(MN)$

Pair $N\in S$ with $MN\in S$

1 of pair commutes with E_d

1 of pair anti-commutes

$\Rightarrow$ exactly $\frac{1}{2}$ of S anti-commutes with E_d.

So $B_d=\#$ Pauli operators of weight d in $N(S)$.

For a general code with distance d: $A_c=B_c$ $(c<d)$ (But $\Leftarrow$ need not hold).

And $A_d\le B_d,\ A_d\ge 0,\ A_0=B_0=1$.

Definition:

- Weight enumerator $A(z)=\sum_d A_d z^d$
- Dual weight enumerator $B(z)=\sum_d B_d z^d$
- Quantum MacWilliams Identity (QMWI) : $B_z=\frac{\mathrm{tr}\theta_1\mathrm{tr}\theta_2}{2^n\mathrm{tr}\theta_1\theta_2}(1+3z)^nA\big(\frac{1-z}{1+3z}\big)$

Use the QMWI to give "linear programming bounds"

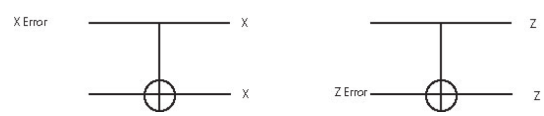
For $\theta_1=\theta_2=\pi$, $\mathrm{tr}\pi=2^k$

$$B(z)=\frac{1}{2^{n-k}}(1+3z)^nA\Big(\frac{1-z}{1+3z}\Big)$$

For classical weight enumerators, distance $d \Rightarrow A_c = B_c = 0,\ 0 < c < d$.
Can be $\neq 0$ in quantum case due to degenerate codes.
If $A_c = B_c = 0, \forall\, 0 < c < d$, code is pure, otherwise impure.

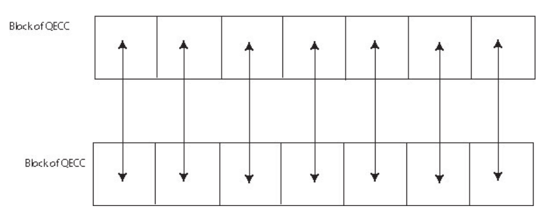
Fault Tolerance

1. How do we convert one encoded state to a different encoded state? (without leaving the code space)
2. Error propagation



Even perfect gates can cause pre-existing errors to spread.
Tensor product U of one-qubit gates takes E (error) to $UEU^\dagger$, which has same weight as E.

Transversal operations



jth qubit of each block only interacts with jth qubit of other blocks.
E.g. 2-qubit error becomes 2 2-qubit errors in separate blocks. Must line up qubits in the same way, otherwise causes interactions of "neighbours".
E.g. $\overline{X}$ and $\overline{Z}$ operations.
Look at $\mathcal{C}$
Hadamard H: $X \leftrightarrow Z$

M_1	X	X	X	X	I	I	I
M_2	X	X	I	I	X	X	I
M_3	X	I	X	I	X	I	X
M_4	Z	Z	Z	Z	I	I	I
M_5	Z	Z	I	I	Z	Z	I
M_6	Z	I	Z	I	Z	I	Z
$\overline{X}$	X	X	X	X	X	X	X
$\overline{Z}$	Z	Z	Z	Z	Z	Z	Z

$H^{\otimes 7}$ takes S into itself (for 7-qubit code), and $H^{\otimes 7}\overline{X}H^{\otimes 7} = \overline{Z}$, $H^{\otimes 7}\overline{Z}H^{\otimes 7} = \overline{X}$. So $H^{\otimes 7}$ performs encoded $H = \overline{H}$.

Phase gate $P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$. $P: \; X \to Y, \; Z \to Z$.

$P^{\otimes 7}: \; S \to S$

$P^{\otimes 7}\overline{Z}(P^{\dagger})^{\otimes 7} = \overline{Z}$

$P^{\otimes 7}\overline{X}(P^{\dagger})^{\otimes 7} = Y \otimes Y \otimes \cdots \otimes Y = -\overline{Y}$. $\overline{Y} = \pm i\overline{XZ}$, $\overline{Y}^{\otimes 7} = (\pm i)^7(\overline{XZ})$

$\Rightarrow$ $P^{\otimes 7}$ does logical $P^{\dagger}$.