Quantum Error Correction / CO639

Prepared by Annika Niehage

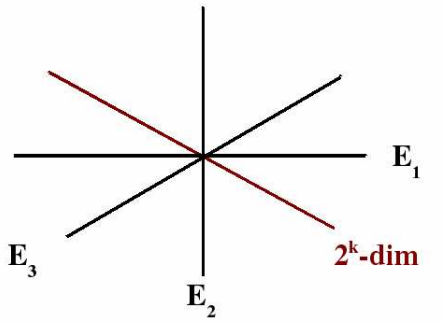
Edited by Daniel Gottesman lecture: 2004-02-05

1 Equivalence of the two 5-qubit codes

$$
\begin{array}{ccccc|c|ccccc|l}
X & Z & Z & X & I & \to & I & Z & Y & Y & Z & \\
I & X & Z & Z & X & \nearrow & I & X & Z & Z & X & \\
X & I & X & Z & Z & \searrow & X & I & X & Z & Z & \\
Z & X & I & X & Z & \to & Z & I & Z & Y & Y & \\
 & & & & & & & & \downarrow & \downarrow & & Y \to Z,\ Z \to X \\
I & X & X & X & X & \nwarrow & I & Z & Z & Z & Z & \\
I & Z & Z & Z & Z & \swarrow & I & X & X & X & X & \\
X & I & X & Z & Y & & X & I & Y & X & Z & \searrow \\
Z & I & Z & Y & X & \searrow & Z & I & X & Z & Y & \to \quad X \to Y,\ Y \to Z \\
 & & & & & \searrow & Y & I & Y & X & Z &
\end{array}
$$

First we replace generators of one version of the 5-qubit code with products of generators (top). Then we perform unitary operations on the third and fourth qubits (right). Then we replace the last generator of the second version of the 5-qubit code with the product of the last two generators (bottom). Finally, we perform a unitary operation on the first qubit (far right) to prove the equivalence of these two 5-qubit codes.

2 Upper and lower bounds on quantum error-correcting codes



For a non-degenerate code

N_E errors occur; each gives a $2^k - dim$ subspace of a $2^n - dim$ total space (n qubits). So we get

$$N_E \, 2^k \leq 2^n$$

2.1 Quantum Hamming bound (QHB)

Theorem: A non-degenerate QECC correcting t errors with n qubits and k encoded qubits satisfies

$$\underbrace{\left[\sum_{j=0}^{t} \binom{n}{j} 3^j\right]}_{N_E} 2^k \leq 2^n$$

Example:

Take $t = 1$: $(1 + 3n)2^k \leq 2^n$

If you set $k = 1$, you get: $1 + 3n \leq 2^{n-1}$

The smallest possible n is $n = 5$.

$\Rightarrow$ 5-qubit code saturates QHB and is called "**perfect**". In general a code is called **perfect**, if we have $=$ in the QHB.

$$1 + 3n = 2^{n-k}$$
$$2^{2s} \equiv 1 \; mod \; 3$$
$$n = \tfrac{4^3-1}{3}, \quad n - k = s$$

For certain values of s we get:

$$s = 2: \quad n = 5$$
$$s = 3: \quad n = 21$$
$$s = 4: \quad n = 85$$

What happens if $n \to \infty$?

The rates $\frac{t}{n}$ and $\frac{k}{n}$ should be constant. Then we get:

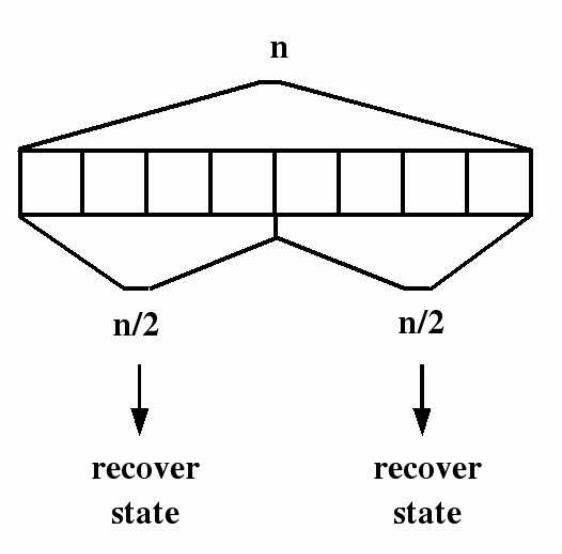
$$\log_2 N_E \approx \underbrace{\log_2 \binom{n}{t}}_{n\, h(\frac{t}{n})} + t \log_2 3$$

with $h(x) = -x \log_2 x - (1 - x) \log_2(1 - x)$, called the **binary entropy function**. So

$$\frac{k}{n} \leq 1 - h(\frac{t}{n}) - \frac{t}{n} \log_2 3$$

2.2 Quantum Singleton bound ("Knill-Laflamme" bound) (QSB)

Remember: Correcting t errors $\Leftrightarrow$ correcting $2t = d - 1$ erasure errors.



If we had an n-qubit code correcting $\geq \frac{n}{2}$ erasure errors, we could clone states, so $n > 2(d-1)$.

Theorem (QSB):

$$k \leq n - 2(d-1)$$

e.g. the following codes saturate the bound: $[[5,1,3]]$, $[[4,2,2]]$, $[[n, n-2, 2]]$ (n even).
Codes which saturate the QSB are called **"MDS" codes**. (MDS comes from the classical case and stands for "maximum distance separable codes").

Proof: Take a QECC and k EPR pairs. Encode $\frac{1}{2}$ of each pair in QECC, call the other half R. Then you have the following:

$$\overbrace{R}^{k} \quad \overbrace{A}^{d-1}\overbrace{B}^{d-1} \overbrace{C}^{n-2(d-1)}$$

The **entropy** is defined as the following: $S(\rho) = -tr\,\rho \log_2 \rho$.

$$\begin{aligned} S(RA) &= S(BC) \text{ (pure state)} \\ S(RB) &= S(AC) \end{aligned}$$

As the QECC has distance d

$\Rightarrow$ any $d-1$ qubits are independant of the encoded state

$$\begin{aligned} \Rightarrow \quad \rho(RA) &= \rho(R) \otimes \rho(A) \\ S(RA) &= S(R) + S(A) \\ S(RB) &= S(R) + S(B) \end{aligned}$$

Subadditivity gives us:

$$\begin{aligned} S(BC) &\leq S(B) + S(C) \\ S(AC) &\leq S(A) + S(C) \end{aligned}$$

Combining these results, we get:

$$\begin{aligned} k = S(R) &\leq S(C) + [S(B) - S(A)] \\ k = S(R) &\leq S(C) + [S(A) - S(B)] \\ \Rightarrow \qquad k &\leq S(C) \\ S(C) &\leq n - 2(d-1) \end{aligned}$$

■

2.3 Quantum Gilbert-Varshamov bound (QGVB)

Existence of QECC: Stabilizer code $[[n, k, d]]$

- Write down **all** $[[n, k]]$ stabilizer codes ($\sharp = N_C$)
- For each code, list all elements in $N(S) \backslash S$; each list has $2^{n+k} - 2^{n-k}$ elements.
- Each $E \in \mathcal{P} \backslash \{I\}$ appears on the **same** number of lists:

$$E,\ F \in \mathcal{P} \backslash \{I\}$$

$$\Rightarrow \exists\, U \in \mathcal{C} \ \text{ s.t. } U(E) = F$$

$$S \ \text{ stab. } \ [[n,k]] \quad \Leftrightarrow \quad U(S) \ \text{ stab. } \ [[n,k]] \ \text{ also}$$

$$E \in N(S) \backslash S \quad \Leftrightarrow \quad F \in N(U(S)) \backslash U(S)$$

- Each $E \in \mathcal{P} \backslash \{I\}$ appears on
$$\frac{N_C\,(2^{n+k} - 2^{n-k})}{4^n - 1}$$
lists.
- Cross off each code that fails to correct E with $wt(E) < d$.

In the end we crossed off at most $N_E \frac{N_C\,(2^{n+k} - 2^{n-k})}{4^n - 1}$ codes. If this is $< N_C$, then $\exists\, [[n, k, d]]$.

Theorem (QGVB): A QECC correcting t errors with n qubits and k encoded qubits exists, if

$$\left[\sum_{j=0}^{d-1} \binom{n}{j} 3^j\right] 2^k \leq 2^n$$

$$\Leftrightarrow \frac{k}{n} \leq 1 - h(\frac{d}{n}) - \frac{d}{n} \log_2 3$$