QECC

Quantum Error Correction Codes

Alessandro Tomasi
2017.03.31.
BINARY ECC

An elementary introduction
Sending and receiving

- The sender intends to transmit a message $m$ to a recipient
- The message crosses a channel introducing random errors $e$
- The receiver reads $m'$
Sending and receiving bits

- The sender intends to transmit a message $m \in (\mathbb{F}_2)^k$ to a recipient.
- The message crosses a channel introducing random errors $e$.
- The receiver reads $m' = m \oplus e$.
Encoding and decoding

- The sender intends to transmit a message $m \in (\mathbb{F}_2)^k$ to a recipient.
- The encoded message $c = E(m)$ crosses a channel introducing random errors $e$.
- The receiver reads a noisy codeword $c' = c \oplus e$ and decodes $m' = D(E(m) \oplus e)$.
The nature of errors

- The encoding/decoding functions should be chosen based on the nature of the messages to be transmitted, and the nature of the errors that can occur on the channel.

- The simplest model is the Binary Symmetric Channel: each bit transmitted has an equal and independent probability $p$ of being flipped:

- We will not consider: burst errors, erasures, insertions, etc.
Errors as a process

- The Binary Symmetric Channel can be seen as a Markov process with an evolution matrix
  \[ E = \begin{pmatrix} (1 - p) & p \\ p & (1 - p) \end{pmatrix} \]

- A bit with probability mass function \( \begin{bmatrix} p_0 \\ p_1 \end{bmatrix} \) exits the channel as
  \[ \begin{bmatrix} q_0 \\ q_1 \end{bmatrix} = E \begin{bmatrix} p_0 \\ p_1 \end{bmatrix} \]

- Completeness: for the output to be a valid probability mass,
  \[ \sum_c E_{rc} = 1 \]
Detecting and correcting

- Redundancy: encode messages in a larger space in order to notice errors by receiving invalid messages. Example: the [2,1] repetition code allows the detection of a single error.

\[
\begin{array}{c}
0 \rightarrow 00 \\
1 \rightarrow 11 \\
01 \\
\end{array}
\]

- Noticing errors have occurred is easier than correcting them: the [3,1] repetition code allows the detection of two errors and the correction of a single error.

\[
\begin{array}{c}
0 \rightarrow 000 \\
1 \rightarrow 111 \\
010 \\
011 \\
\end{array}
\]
Linear codes

- An \([n, k, d]\) binary linear code \(\mathcal{C}\) is a subspace of \((\mathbb{F}_2)^n\).
  - \(n\): length
  - \(k\): dimension
  - \(d\): minimum distance

- The message space \(\mathcal{M} = (\mathbb{F}_2)^k\) can be mapped into the code space by the code generator matrix \(G\):
  \[
  Gm = c
  \]
  \[
  (n \times k)(k \times 1) = (n \times 1)
  \]

- The columns of \(G\) are a basis of \(\mathcal{C}\), and it can be written in systematic form by Gaussian elimination
  \[
  G^T = [I_k \quad P]
  \]
  \[
  (k \times n) = (k \times k | k \times n-k)
  \]
Distance

- Hamming distance
  \[ H(c_0, c_1) = \# \{ i | c_0(i) \neq c_1(i) \} \]

- Hamming weight
  \[ H(c_0) = H(c_0, 0) \]

- The minimum distance of an \([n, k, d]\) binary linear code \(C\) is
  \[ d = \min_{c_0 \neq c_1 \in C} H(c_0, c_1) = \min_{c \in C} H(c) \]

- An \([n, k, d]\) binary linear code \(C\) can surely at most
  - detect \(d - 1\) errors
  - correct \(\left\lfloor \frac{d-1}{2} \right\rfloor\) errors
Distance

- Intuitively:

\[ C \in (\mathbb{F}_2)^n \]

\[ d \geq \left\lfloor \frac{d - 1}{2} \right\rfloor \]
Syndrome decoding

- Parity check matrix $H$
  
  \[
  Hc = 0 \quad \forall \quad c \in C
  \]
  \[
  H^T = \left[ -P^T \quad I_{n-k} \right]
  \]
  
  \[(n - k \times n) = (n-k \times k \mid n - k \times n - k)\]

- The syndrome of a received $c' = c \oplus e$,

  \[
  H(c \oplus e) = He
  \]

  is specific to the error, not the codeword. Recovering $e$ from $He$,

  \[
  c = c' \ominus e
  \]

- $C$ is the kernel of $H$; $H^T$ generates the dual code $C^\perp$. 
Dual identity

\[ \sum_{u \in \mathcal{C}} (-1)^{u \cdot v} = \begin{cases} 2^k & v \in \mathcal{C}^\perp \\ 0 & v \notin \mathcal{C}^\perp \end{cases} \]

Proof: recall the Walsh transform;

\[ \sum_{\alpha \in (\mathbb{F}_2)^k} (-1)^{\alpha \cdot \beta} = 0, \quad \beta \neq 0 \]

\[ \sum_{u \in \mathcal{C}} (-1)^{u \cdot v} = \sum_{\alpha \in (\mathbb{F}_2)^k} (-1)^{\alpha \cdot Gv} = 0 \]

for \( Gv = H_{\mathcal{C}^\perp} v \neq 0 \), i.e. for \( v \notin \mathcal{C}^\perp \).
Example: [3,1] repetition

- For the [3,1] repetition code, $G = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

- To construct $H$, pick $3 - 1 = 2$ linearly independent vectors orthogonal to the columns of $G$, e.g. $H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$

- $Hx = 0$ only for $x = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ or $x = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$. 
Example: $[7,4,3]$ Hamming

- Integer $r \geq 2$, take all $2^r - 1$ strings of length $r$ that are not identically equal to 0 as columns of $H$; this defines a $[2^r - 1, 2^r - 1 - r]$ linear code. For $r = 3$,

$$H = \begin{bmatrix}
0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1
\end{bmatrix}$$
Hamming bound

- Hamming ball: $B(x, t) = \{y | d(x, y) \leq t\}$, $x, y \in (\mathbb{F}_2)^n$.

$$|B(x, t)| = \sum_{j=0}^{t} \binom{n}{j}$$

- Hamming balls of size $t$ are disjoint but may not cover the entire space: $B(c_1, t) \cap B(c_2, t) = \emptyset$

$$2^n \geq \left| \bigcup_{c \in C} B(c, t) \right| = \sum_{c \in C} |B(c, t)| = 2^k \sum_{j=0}^{t} \binom{n}{j}$$

$$n \geq k + \log_2 \left( \sum_{j=0}^{t} \binom{n}{j} \right)$$
QUANTUM BIT FLIPS

An introduction to the correction of a quantum error
Bit flip as quantum channel noise

- The Pauli gate $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ acts as NOT or bit flip:

  $$\sigma_x \begin{bmatrix} z_0 \\ z_1 \end{bmatrix} = \begin{bmatrix} z_1 \\ z_0 \end{bmatrix}$$

- For a block of $k$ qubits, denote the action of $\sigma_x$ on the $j^{th}$ qubit only as $X_j$. For instance,

  $$X_2 |000\rangle = I \otimes \sigma_x \otimes I |000\rangle = |010\rangle$$
Quantum repetition?

- Single qubit message: $|z\rangle = z_0|0\rangle + z_1|1\rangle$
- There is no algorithm that will take a generic unknown $|z\rangle$ and return $|z\rangle|z\rangle|z\rangle$ (no cloning).
- We could however encode $|z\rangle$ as $|\bar{z}\rangle^3 = z_0|000\rangle + z_1|111\rangle$ using CNOT.
Explicitly

\[ |z\rangle |z\rangle = |z\rangle \otimes |z\rangle = \begin{bmatrix} z_0^2 \\ z_0 z_1 \\ z_0 z_1 \\ z_1^2 \end{bmatrix} \rightarrow \begin{cases} |00\rangle : |z_0|^4 \\
|01\rangle : |z_0 z_1|^2 \\
|10\rangle : |z_0 z_1|^2 \\
|11\rangle : |z_1|^4 \end{cases} \]

\[ |\bar{z}\rangle^2 = z_0 |00\rangle + z_1 |11\rangle = \begin{bmatrix} z_0 \\ 0 \\ 0 \\ z_1 \end{bmatrix} \rightarrow \begin{cases} |00\rangle : |z_0|^2 \\
|11\rangle : |z_1|^2 \end{cases} \]
Controlled NOT encoding

CNOT: \[
\begin{bmatrix}
1 & 1 \\
1 & 1
\end{bmatrix}
\]

|00\rangle \rightarrow |00\rangle
|01\rangle \rightarrow |01\rangle
|10\rangle \rightarrow |11\rangle
|11\rangle \rightarrow |10\rangle

\[ |z\rangle \rightarrow z_0 |00\rangle + z_1 |11\rangle \]
Controlled NOT encoding

\[
\begin{bmatrix}
1 & 1 \\
1 & 1
\end{bmatrix}
\]

\[
|00\rangle \rightarrow |00\rangle \\
|01\rangle \rightarrow |01\rangle \\
|10\rangle \rightarrow |11\rangle \\
|11\rangle \rightarrow |10\rangle
\]
Quantum channel bit flips

Assume a single bit flip occurs: the codewords and corrupted transmissions are all orthogonal subspaces of $(\mathbb{C}^2)^{\otimes 3}$:

\[
|z\rangle^3 = z_0|000\rangle + z_1|111\rangle \\
X_0|z\rangle^3 = z_0|100\rangle + z_1|011\rangle \\
X_1|z\rangle^3 = z_0|010\rangle + z_1|101\rangle \\
X_2|z\rangle^3 = z_0|001\rangle + z_1|110\rangle
\]
Quantum channel bit flip decoding

- We could use the following four measurement (projection) operators to detect errors:

  \[ P_1 = |000\rangle\langle 000| + |111\rangle\langle 111| \]
  \[ P_0 = |100\rangle\langle 100| + |011\rangle\langle 011| \]
  \[ P_1 = |010\rangle\langle 001| + |101\rangle\langle 101| \]
  \[ P_2 = |001\rangle\langle 001| + |110\rangle\langle 110| \]

- Each would result in a +1 if the error corresponding to the measurement did occur, but in any case would leave the quantum state unaltered.

- If \( \langle z|P_j|z \rangle = 1 \), we could correct by applying \( X_j \), that is by flipping the corresponding qubit.
Quantum channel bit flip decoding

Rather than asking which of the four possible states the received word is in, we can simplify the procedure by asking whether the received qubits are equal two-by-two:

\[ P_{01} = \begin{bmatrix} 1 & -1 & -1 \end{bmatrix} \otimes I, \quad P_{12} = I \otimes \begin{bmatrix} 1 & -1 & -1 \end{bmatrix} \]

This results in the following combinations:

\[
\begin{array}{cccc}
I & X_0 & X_1 & X_2 \\
+ & - & - & + \\
P_{01} & + & - & - & + \\
+ & + & - & - \\
P_{12}
\end{array}
\]
CCNOT decoding

\[
\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}
\]

\[
|110\rangle \rightarrow |111\rangle \\
|111\rangle \rightarrow |110\rangle
\]

\[\mathcal{E}_{bit}|z\rangle^3 \]

\[\{\text{syndrome}\}\]
Full bit flip circuit
QUANTUM ERROR CORRECTION
New challenges

**bits**
- Storage is highly robust
- Checking the state of storage is quick and inexpensive
- Redundant copies can easily be made
- Bit flips are (almost) the only kind of error

**qubits**
- Any environment interaction whatsoever introduces errors
- Measurement changes the state, and the outcome is stochastic
- No cloning: no encoding by repetition
- Bit flips, phase flips, arbitrary phase rotations...
Phase flip circuit

- Suppose the channel $\mathcal{E}_{\text{phase}}$ can introduce a single phase flip error. A phase flip $\sigma_z = Z$ is equivalent to a bit flip in phase space, i.e. in the Hadamard basis: $HZH = X$, $HIH = I$

- Phase flips can thus be corrected in the same way as bit flips.
The Shor code

- Combines the bit flip and phase flip codes: first applies phase, then bit flip
  
  \[
  |0\rangle \rightarrow |+++\rangle \quad |1\rangle \rightarrow |---\rangle \\
  |+\rangle \rightarrow (|000\rangle + |111\rangle)/\sqrt{2} \quad \langle-\rangle \rightarrow (|000\rangle - |111\rangle)/\sqrt{2}
  \]

- Final codewords:
  
  \[
  |0\rangle \rightarrow \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}
  \]
  
  \[
  |1\rangle \rightarrow |---3\rangle |---3\rangle |---3\rangle
  \]

- Encodes a single qubit using a 9-qubit register. Corrects bit flips and phase flips – and more – on a single qubit.
The Shor code
Noise as quantum operation

- Describe the channel noise $\mathcal{E}$ as any quantum operation sending an input state $z$ to 
  $$z' = \mathcal{E}(z)$$

- Typical quantum operations: unitary transform $U$ and measurement $M_m$ such that $\sum_m M_m = 1$
  $$\mathcal{E}(z) = U|z\rangle\langle z|U^\dagger$$

- $\mathcal{E}_m(z) = M_m|z\rangle\langle z|M_m^\dagger$ leads to measurement $m$ with probability $\text{tr}(\mathcal{E}_m(z))$ and leaves the state 
  $$\frac{\mathcal{E}_m(z)}{\text{tr}(\mathcal{E}_m(z))}$$
Noise as an open system interaction

\[ \mathcal{E}(z) = tr_e(U(z \otimes e)U^+) \]
Operator-sum representation

- Environment initial state $|e_0\rangle\langle e_0|$ with orthonormal basis $|e_k\rangle$

$$\mathcal{E}(z) = \sum_k \langle e_k | U(z \otimes |e_0\rangle\langle e_0|) U^\dagger |e_k\rangle$$

$$= \sum_k E_k z E_k^\dagger$$

- $E_k = \langle e_k | U | e_0 \rangle$ is an operator on the state space of $z$.

- Completeness: for trace-preserving operations,

$$tr(\mathcal{E}(z)) = 1 = tr \left( \sum_k E_k^\dagger E_k z \right)$$

$$\sum_k E_k^\dagger E_k = I$$
A quantum error-correcting code is defined as a subspace $\mathcal{C}$ of some larger Hilbert space with projector $P$ onto the code space $\mathcal{C}$.

- For the three-qubit bit flip code, $P = |000\rangle\langle 000| + |111\rangle\langle 111|.$

In order to perform a syndrome measurement and recover the message, the syndromes must correspond to copies of $\mathcal{C}$:

- orthogonal, to be distinguished by the syndrome; and
- undeformed, so errors take orthogonal codewords to orthogonal states
QECC Assumptions

- The noise is described by a quantum operation $\mathcal{E}$ with operation elements $\{E_i\}$.
- The complete error-correction procedure is effected by a trace-preserving quantum operation $\mathcal{R}$, which may both detect and correct the errors in one step, or otherwise.
- For any state $z$ whose support lies in the code $\mathcal{C}$, 
  $$(\mathcal{R} \circ \mathcal{E})(z) \propto z$$
- $\mathcal{E}$ may not be trace-preserving, e.g. measurement
QEC conditions

■ A set of equations that can be checked to determine whether a quantum error-correcting code protects against a particular type of noise $\mathcal{E}$.

■ Theorem 10.1 [NC10]: (Quantum error-correction conditions) A necessary and sufficient condition for the existence of an error-correction operation $\mathcal{R}$ correcting $\mathcal{E}$ on $\mathcal{C}$ is that

$$PE_i^\dagger E_j P = \alpha_{ij} P$$

for some Hermitian matrix $\alpha$ of complex numbers.

■ We call the operation elements $\{E_i\}$ for the noise $\mathcal{E}$ errors, and if such an $\mathcal{R}$ exists we say that $\{E_i\}$ constitutes a correctable set of errors.

[NC10]
Conditions and Ancilla

■ An alternative way to express the action of an error on code and environment basis states $|c\rangle, |e\rangle$ is

$$ |c\rangle \otimes |0\rangle \rightarrow \sum_{m} M_{m} |c\rangle \otimes |e\rangle $$

for linear combinations $M_{j}$ of the Pauli operators with operator-sum normalization $\sum_{m} M_{m}^{\dagger} M_{m} = I$

■ The error can be reversed if there exist $\sum_{r} R_{r}^{\dagger} R_{r} = I$ such that

$$ \sum_{r,m} R_{r} M_{m} |c\rangle \otimes |m\rangle_{e} \otimes |r\rangle_{a} = |c\rangle \otimes \perp c\rangle_{ea} $$

■ $|r\rangle_{a}$ an orthonormal basis for the ancilla, and whatever remains of the correction procedure in environment and ancilla is independent of $|c\rangle$.

[Preskill, J]
Steps

- Recovery after error on the code subspace is a multiple of $I$:
  \[ R_r M_m |c\rangle = \lambda_{rm} |c\rangle \]

- \[ M_n^\dagger M_m |c\rangle = M_n^\dagger (\sum R_r^\dagger R_r) M_m |c\rangle = \sum_r \lambda^*_r \lambda_{rm} |c\rangle \]

- So $M_n^\dagger M_m$ is also a multiple of $I$ on the code subspace
  \[ \langle d | M_n^\dagger M_m |c\rangle = C_{nm} \delta_{cd} \]

- $C_{nm} = \langle d | E_n^\dagger E_m |c\rangle$ an arbitrary Hermitian matrix.

- The recovery operation is then:
  \[ R_r : M_m |c\rangle \rightarrow \sqrt{C_r} \delta_{mr} |c\rangle \]

\[
\sum_{r,m} R_r M_m |c\rangle \otimes |m\rangle_e \otimes |r\rangle_a = |c\rangle \otimes \left( \sum_r \sqrt{C_r} |r\rangle_e \otimes |r\rangle_a \right)
\]
Significance of Ancilla

- Two-step procedure: a measurement is conducted to diagnose the error, and a unitary transformation is applied to reverse the error based on the measurement outcome.
- Measurement projects the damaged state into one of a discrete set of outcomes but is not indispensable.
- When the code block interacts with its environment, it becomes entangled with the environment, and the Von Neumann entropy of the environment increases (as does the entropy of the code block).
- We may apply a unitary transformation to the data and to an ancilla that we do control. This unitary can be chosen to transform the entanglement of the data with the environment into entanglement of ancilla with environment. The ancilla serves as a depository for the entropy inserted into the code block by the errors.
QEC linearity

- Theorem 10.2 [NC10]: Suppose $\mathcal{F}$ is a quantum operation with operation elements $\{\mathcal{F}_i\}$ that are linear combinations of the $E_i$, that is $\{\mathcal{F}_i\} = \sum_i m_{ji} E_i$ for some matrix $m_{ji}$ of complex numbers. Then the error-correction operation $\mathcal{R}$ also corrects for the effects of the noise process $\mathcal{F}$ on the code $\mathcal{C}$.

- Instead of talking about the class of error processes $\mathcal{E}$ correctable by a code $\mathcal{C}$ and error-correction operation $\mathcal{R}$ we can talk about a set of error operators (or simply errors) $\{E_i\}$ that are correctable.

- Any noise process $\mathcal{E}$ whose operation elements are built from linear combinations of these error operators $\{E_i\}$ will be corrected by the recovery operation $\mathcal{R}$. 
Channel operators

- Describe the channel noise $\mathcal{E}$ with elements $\{E_i\}$:
  - Bit flip:
    \[ \{E_i\} = \{\sqrt{1 - p} I, \sqrt{p} X\} \]
  - Phase flip:
    \[ \{E_i\} = \{\sqrt{1 - p} I, \sqrt{p} Z\} \]
  - Bit-phase flip:
    \[ \{E_i\} = \{\sqrt{1 - p} I, \sqrt{p} Y\} \quad Y = iXZ \]
  - Depolarizing:
    \[ \{E_i\} = \{\sqrt{1 - 3p/4} I, \sqrt{p/4} X, \sqrt{p/4} Y, \sqrt{p/4} Z\} \]
  - Amplitude damping:
    \[ \{E_i\} = \{\begin{bmatrix} 1 \\ \sqrt{\gamma} \end{bmatrix}, \begin{bmatrix} \sqrt{\gamma} \end{bmatrix}\} \]
Shor code redux

- Example: Suppose $\mathcal{E}$ is a quantum operation acting on a single qubit. Then its operation elements $\{E_i\}$ can each be written as a linear combination of the Pauli $\{\sigma_0, \sigma_x, \sigma_y, \sigma_z\}$.

- To check that the Shor code corrects against arbitrary single qubit errors on the first qubit it is sufficient to verify that the equations

  \[ P \sigma_i^{(0)} \sigma_j^{(0)} P = \alpha_{ij} P \]

  are satisfied.

- Equally, any code able to correct errors on the depolarizing channel can correct an arbitrary single-qubit operation.
Degenerate codes

- The 9-qubit Shor code is a degenerate QECC: different errors result in identical received states, e.g. $Z_1|z\rangle = Z_2|z\rangle$.
- This has no classical equivalent: errors in different locations result in different received words.
Quantum Hamming bound

There are \( \binom{n}{j} \) possible locations for \( j \) errors in an \( n \)-qubit register, and 3 possible linearly independent errors, so the number of possible errors of weight up to \( t \) is

\[
N(t) = \sum_{j=0}^{t} 3^j \binom{n}{j}
\]

To encode each error in a \textbf{non-degenerate} way, each must map to an orthogonal \( 2^k \)-dimensional subspace; all of these must be contained in the \( 2^n \)-dimensional qubit space:

\[
2^n \geq 2^k \sum_{j=0}^{t} 3^j \binom{n}{j}
\]

\[
n \geq k + \log_2 \left( \sum_{j=0}^{t} 3^j \binom{n}{j} \right)
\]
Comparison

- Compared with the classical Hamming bound, the quantum version

\[ n \geq k + \log_2 \left( \sum_{j=0}^{t} \binom{n}{j} \right) \]

has not only a scaling difference – three possible errors rather than one – but most importantly does not take into account degenerate codes.

- Example: to encode 1 qubit and correct all errors on 1 transmitted qubit, the quantum Hamming bound \( 2(1 + 3n) \leq 2^n \) is satisfied for \( n \geq 5 \).
CSS codes

- Explicit construction: suppose $C_1$ and $C_2$ are $[n, k_1]$ and $[n, k_2]$ classical linear codes such that $C_2 \subseteq C_1$, and $C_1$ and $C_2^{\perp}$ both correct $t$ errors.

- $C_2$ defines an equivalence relation in $C_1$: $u \equiv v \in C_1 \iff \exists w \in C_2 | u + v = w$. The equivalence classes are cosets of $C_2$ in $C_1$.

- A CSS code is a $[[n, k_1 - k_2]]$ quantum code that associates a codeword with each equivalence class. For any $x \in C_1$:

$$|c\rangle = |x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x \oplus y\rangle$$

- There are $2^{k_1 - k_2}$ cosets, and hence $2^{k_1 - k_2}$ linearly independent codewords.
Suppose the bit flip errors are located by an indicator $e_b$, and the phase flip errors by an indicator $e_p$. The received word is

$$|c_e\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x \oplus y) \cdot e_p} |x \oplus y \oplus e_b\rangle$$

We can introduce an ancillary register of size $n - k_1$ and find a reversible operation $|x\rangle |0\rangle \rightarrow |x\rangle |Hx\rangle$ to get the syndrome, then locate and correct by applying NOT gates to $e_b$, leaving

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x \oplus y) \cdot e_p} |x \oplus y\rangle$$
CSS correcting phase flips

- Apply a Hadamard transform to get
  \[
  \frac{1}{\sqrt{|C_2|2^n}} \sum_z \sum_{y \in C_2} (-1)^{(x \oplus y) \cdot (z \oplus e_p)} |z\rangle
  \]

- If \( z' \in C_2^\perp \), then \( \sum_{y \in C_2} (-1)^{y \cdot z'} = |C_2| \), otherwise \( = 0 \), leaving
  \[
  \frac{1}{\sqrt{2^n / |C_2|}} \sum_{z' \in C_2^\perp} (-1)^{x \cdot z'} |z' \oplus e_p\rangle
  \]

which may be corrected in the same manner as a bit flip. The original state is recovered by another Hadamard transform.
The Steane code

- This example uses the Hamming [7,4,3] code as $C_1$, and its dual code as $C_1^\perp = C_2$:

- $H_{C_1} = \begin{bmatrix}
0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1
\end{bmatrix}$

- $H_{C_2} = (G_{C_1})^T \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1
\end{bmatrix}$
Thank you for your attention!
References


[NC10] Nielsen, MA; Chuang, IL: Quantum Computation and Quantum Information. CUP 2010. isbn: 9781107002173
Links

[Brun, T] Quantum Information Processing
[Mermin, D] Quantum Computation
[Preskill, J] Quantum Computation
[Trevisan, L] Quantum Computing
[Whaley, B; Vazirani, U] Qubits, Quantum Mechanics, and Computers
[Quantiki] Basic concepts in quantum computation