Quantum Error Correction: part 1

FATMA ÇİÇEK

July 2024

Algorithms assume that qubits are perfect. Ideal qubits are called logical qubits. Actual qubits are noisy physical qubits.

Possible issues

- Idle qubits pick up noise from environment.
- Interaction of qubits with the environment.
- Measurements are not 100% correct.
- Gates are not perfect.

We will only focus on single qubit state errors, rather than gate errors or measurement errors.

Goal: Approximate a circuit of logical qubits by a circuit of physical qubits as close as possible. Many physical qubits are needed per each logical one.

Threshold theorem: It is possible to create a quantum computer to perform an arbitrary quantum computation provided the error rate per physical gate or time step is below some constant threshold value.

Classical Error Correction

An error correction code is called a $[k, n, d]$ code, where

k : number of bits of the message

n : number of bits of the encoding/encoded message, $\quad n > k$

d : distance

d is the minimum number of errors that would be undetectable with our code.
Example. If we repeat one qubit 3 times, so $|0\rangle \to |000\rangle$ and $|1\rangle \mapsto |111\rangle$, then we can't detect 3-bit errors.
Summary. Encode k logical qubits in n physical qubits with distance d.
Goals:

- Make d big.
- Reduce the redundancy and make the rate R big. Rate of an $[n, k, d]$-code is defined as $R = k/n$.

Decoding methods:

- Hamming codes (parity checks, linear codes, generator matrices)
- Reed-Muller codes (generator polynomials)

Parity check codes (Classical)

Idea: Instead of redundancy, encode the message as message plus parity check bits.

An example of a parity check code:

Encoding: n bits into $n+1$ bits.

$$a_1 a_2 \dots a_n \mapsto a_1 a_2 \dots a_n z \quad \text{for} \quad z = a_1 + \cdots + a_n \mod 2.$$

$z = 0$ for even number of 1 in $a_1 a_2 \dots a_n$, $z = 1$ for odd number of 1 in $a_1 a_2 \dots a_n$.
This code detects any single bit error except its location. It is a $[n+1, n, 2]$-code.

Hamming codes (Classical)

Hamming code: Hamming code is a $[7, 4, 3]$-code, $n = 4$, $k = 7$, $d = 3$.
Encoding: $n = 4$ bits into $k = 7$ bits ($2^r - r - 1$ bits into $2^r - 1$ bits).

$$abcd \mapsto abcdz_1z_2z_3$$

for $z_1 = a + b + d$, $z_2 = a + c + d$, $z_3 = b + c + d \mod 2$.
Any single bit error is detected and located.
Hamming codes are $[2^r - 1, 2^r - r - 1, 3]$-codes.

Quantum error correction (QEC)

Types of errors

Pauli matrices:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

(bit flip) (phase flip) (bit and phase flip)

All satisfy $A^2 = I$ and have eigenvalues ± 1. X, Y, Z (pairwise) anticommute.
Note:

$$X(\alpha |0\rangle + \beta |1\rangle) = \alpha |1\rangle + \beta |0\rangle , \qquad Z(\alpha |0\rangle + \beta |1\rangle) = \alpha |0\rangle - \beta |1\rangle .$$

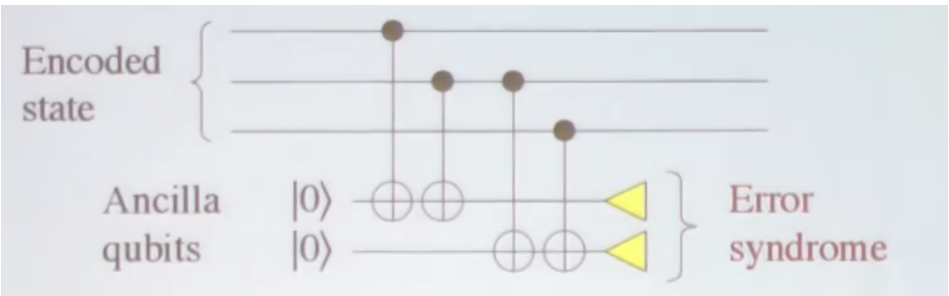
Bit flip errors are called **X-errors**, phase flip errors are called **Z-errors**, **Y-errors** can be understood from bit and phase flip errors, since

$$Y = -i\, XZ.$$

Other errors: Decoherence errors, rotation errors, etc.

Quantum repetition code for bit flip error at a single qubit (3 qubits)

- Encode $\alpha|0\rangle + \beta|1\rangle$ as $\alpha|000\rangle + \beta|111\rangle$.
- A bit flip error (X-error) on the second qubit will be $|000\rangle \to |010\rangle$ and $|111\rangle \to |101\rangle$.
- Measure that one qubit is different than the other two qubits, rather than measuring the state.
- Check whether each two adjacent qubits are the same by using auxiliary qubits called **ancilla qubits** .



Measurement from ancilla qubits (measurements done to detect errors / not the state) are called **syndromes**.
Syndrome is 0 if two qubits are the same, 1 otherwise.

Parity check matrices

For n logical bits encoded with parity checks into k bits, there is a matrix of dimension $k \times n$, called generator matrix, G.

$$G = \begin{bmatrix} I_n \\ A \end{bmatrix}.$$

Parity check matrix of $(k-n) \times k$ is

$$H = \begin{bmatrix} A & I_{k-n} \end{bmatrix}.$$

Example. For the Hamming code

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

For vectors of encoded multi-bits $y = [abcdz_1z_2z_3]^T$, $Hy = 0$.

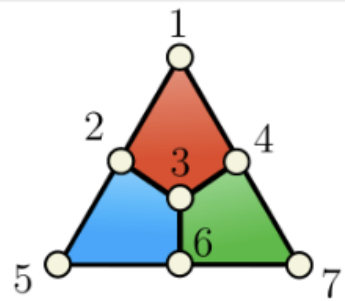
Steane code (7 qubits)

This is a $[7, 1, 3]$ code and an example of quantum Hamming codes with parameters $[2^r - 1, 2^r - 2r - 1, 3]$. It detects both Z-errors and X-errors.

$$\boldsymbol{H} = \left(\begin{array}{ccccccc|ccccccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{array}\right)$$

7-qubit color code

$$S_x^{(1)} = X_1X_2X_3X_4 \quad S_z^{(1)} = Z_1Z_2Z_3Z_4$$
$$S_x^{(2)} = X_2X_3X_5X_6 \quad S_z^{(2)} = Z_2Z_3Z_5Z_6$$
$$S_x^{(3)} = X_3X_4X_6X_7 \quad S_z^{(3)} = Z_3Z_4Z_6Z_7$$
$$X_L = X_1X_2X_3X_4X_5X_6X_7$$
$$Z_L = Z_1Z_2Z_3Z_4Z_5Z_6Z_7$$



$$\mathcal{S}_X = \langle X_1X_2X_3X_4I_5I_6I_7, I_1X_2X_3I_4X_5X_6I_7, I_1I_2X_3X_4I_5X_6X_7 \rangle$$

$$\mathcal{S}_Z = \langle Z_1Z_2Z_3Z_4I_5I_6I_7, I_1Z_2Z_3I_4Z_5Z_6I_7, I_1I_2Z_3Z_4I_5Z_6Z_7 \rangle$$

Observation Elements of $\mathcal{S}_X$ and $\mathcal{S}_Z$ commute:
Fact: Two Pauli operators P and P' commute if they intersect on an even number of qubits with a different Pauli element. Otherwise, they anticommute.
Example. The 3-qubit bit-flip code has stabilizer generators Z_1Z_2 and Z_2Z_3 .

3-qubit code for phase flip error at a single qubit

Note. Repetition codes can only detect bit flip errors.
Use the repetition code in Hadamard basis $\{|+\rangle, |-\rangle\}$, since H switches the role of X-errors and Z-errors:

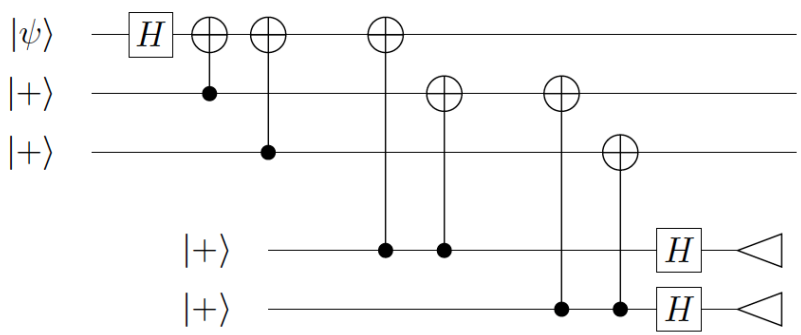
$$HXH = Z \quad \text{or} \quad HZH = X.$$

Also

$$Z|+\rangle = |-\rangle, \; Z|-\rangle = |+\rangle \quad \text{while} \quad X|+\rangle = |+\rangle, \; X|-\rangle = -|-\rangle.$$

Encoding:

$$|0\rangle \mapsto |+++\rangle \quad |1\rangle \mapsto |---\rangle.$$



Stabilizers

Pauli operators: $P = P_1 \otimes \ldots \otimes P_n$ with $P_j \in \{I, X, Y, Z\}$ for all j.
Pauli group is the group generated by them.
Any two elements of the Pauli group either commute or anticommute.
A **stabilizer group** is an abelian subgroup of the whole group of Pauli operators such that it does not contain $-I$.
Given a stabilizer group $\mathcal{S}$, we define its **codespace** ($+1$ eigenspace of all the stabilizers in $\mathcal{S}$) as

$$\mathcal{C}_{\mathcal{S}} := \{|\psi\rangle : S|\psi\rangle = |\psi\rangle \text{ for all } S \in \mathcal{S}\}.$$

Conversely, given an encoding, the stabilizer of the code is the Pauli operators M

$$\mathcal{S} = \{M : M|\psi\rangle = |\psi\rangle \quad \text{for all encoded states } |\psi\rangle\}.$$

This then turns out to be an abelian subgroup of all Pauli operators.

- Parity check matrices correspond to stabilizer generators and vice versa.
- To detect X-errors, we can use stabilizers made of Z operators, and to detect Z-errors, we can use stabilizers made of X operators.
- A CSS (Calderbank-Shor-Steane) code is a stabilizer code that can be generated by a set of pure X and pure Z stabilizers.

References

- https://ml4q.de/wp-content/uploads/2020/03/Top_Arch_Exercise-1-Steane-Code.pdf (Image 3)
- Daniel Gottesman, Surviving as a Quantum Computer in a Classical World (Image 2)
- Arthur Pesah's blog posts: arthurpesah.me
- Youtube: James Wootton, Quantum Error Correction using Repetition Codes, Qiskit Global Summer School, 2020
- Youtube: Daniel Gottesman - Quantum Error Correction and Fault Tolerance, CSSQI 2012 (Image 1)

Note.
No *exact* analog of parity checks due to
No-cloning theorem. There is no quantum operation which maps $|\psi\rangle$ to $|\psi\rangle\,|\psi\rangle$ for arbitrary ψ.

Proof. Suppose that such a unitary map $\mathcal{U} : \mathcal{H} \to \mathcal{H}^{\otimes 2}$ exists. Then $|0\rangle \mapsto |00\rangle$ and $|1\rangle \mapsto |11\rangle$ and

$$\mathcal{U}\,|+\rangle = \frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big),$$

which is not equal to

$$|+\rangle\,|+\rangle = \frac{1}{2}\big(\,|00\rangle + |01\rangle + |10\rangle + |11\rangle\,\big).$$