On Quantum Error Correcting Codes

Pedro Patrício
CMAT- Centro de Matemática, Universidade do Minho, Portugal

Q Days, 2019

$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, |\psi\rangle|\phi\rangle = |\psi\rangle \otimes |\phi\rangle$, and concatenation of symbols denotes the concatenation of *kets*, i.e., $|01\rangle = |0\rangle|1\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

For $H = \frac{\sqrt{2}}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ then

$$\begin{aligned} H|0\rangle &= \frac{\sqrt{2}}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle =: |+\rangle \\ H|1\rangle &= \frac{\sqrt{2}}{2}|0\rangle - \frac{\sqrt{2}}{2}|1\rangle =: |-\rangle \end{aligned}$$

$|0\rangle = \left[\begin{array}{c} 1 \\ 0 \end{array}\right], |1\rangle = \left[\begin{array}{c} 0 \\ 1 \end{array}\right], |\psi\rangle|\phi\rangle = |\psi\rangle \otimes |\phi\rangle$, and concatenation of symbols denotes the concatenation of *kets*, i.e.,
$|01\rangle = |0\rangle|1\rangle = |0\rangle \otimes |1\rangle = \left[\begin{array}{c} 1 \\ 0 \end{array}\right] \otimes \left[\begin{array}{c} 0 \\ 1 \end{array}\right]$.
For $H = \frac{\sqrt{2}}{2}\left[\begin{array}{cc} 1 & 1 \\ 1 & -1 \end{array}\right]$ then

$$\begin{aligned} H|0\rangle &= \frac{\sqrt{2}}{2}\left[\begin{array}{cc} 1 & 1 \\ 1 & -1 \end{array}\right]\left[\begin{array}{c} 1 \\ 0 \end{array}\right] = \frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle =: |+\rangle \\ H|1\rangle &= \frac{\sqrt{2}}{2}|0\rangle - \frac{\sqrt{2}}{2}|1\rangle =: |-\rangle \end{aligned}$$

Take $|\psi\rangle = \frac{\sqrt{2}}{2}|00\rangle + \frac{\sqrt{2}}{2}|11\rangle$ and suppose we want to H the 1st qbit and keep the 2nd qbit intact.
We use the fact $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$ and $A \otimes (B + C) = A \otimes B + A \otimes C$.

$$
\begin{aligned}
& (H \otimes I)\left(\frac{\sqrt{2}}{2}|0\rangle \otimes |0\rangle + \frac{\sqrt{2}}{2}|1\rangle \otimes |1\rangle\right) \\
= \; & (H \otimes I)\left(\frac{\sqrt{2}}{2}|0\rangle \otimes |0\rangle\right) + (H \otimes I)\left(\frac{\sqrt{2}}{2}|1\rangle \otimes |1\rangle\right) \\
= \; & \frac{\sqrt{2}}{2}\left(H|0\rangle\right) \otimes |0\rangle + \frac{\sqrt{2}}{2}\left(H|1\rangle\right) \otimes |1\rangle \\
= \; & (\dots) = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle.
\end{aligned}
$$

Pauli matrices

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = i\sigma_x\sigma_z$$

Note that $\sigma_a\sigma_b = -\sigma_b\sigma_a$ for $a \neq b, a, b \in \{x, y, z\}$.

$$\sigma_x|0\rangle = |1\rangle, \sigma_x|1\rangle = |0\rangle$$

$$\sigma_z|0\rangle = |0\rangle, \sigma_z|1\rangle = -|1\rangle$$

For instance,

$$(\sigma_x \otimes \sigma_z)(|01\rangle) = (\sigma_x|0\rangle) \otimes (\sigma_z|1\rangle) = |1\rangle \otimes (-|1\rangle) = -|11\rangle.$$

Pauli matrices

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = i\sigma_x\sigma_z$$

Note that $\sigma_a\sigma_b = -\sigma_b\sigma_a$ for $a \neq b, a, b \in \{x, y, z\}$.

$$\sigma_x|0\rangle = |1\rangle, \sigma_x|1\rangle = |0\rangle$$

$$\sigma_z|0\rangle = |0\rangle, \sigma_z|1\rangle = -|1\rangle$$

For instance,

$$(\sigma_x \otimes \sigma_z)(|01\rangle) = (\sigma_x|0\rangle) \otimes (\sigma_z|1\rangle) = |1\rangle \otimes (-|1\rangle) = -|11\rangle.$$

Pauli group

Recall that σ_x, σ_z and σ_y anticommute.
Let

$$\mathcal{G}_n = \{\alpha A_1 \otimes \cdots \otimes A_n : A_i \in P, \alpha \in \{\pm 1, \pm i\}\},$$

called the (n-qubit) Pauli group.
Then $\mathcal{G}_n$ consists of the 4^n tensor products of $I, \sigma_x, \sigma_y, \sigma_z$ and an overall phase of ± 1 or $\pm i$, for a total of $4^n + 1$ elements.

$\mathcal{G}_n$ is **not** abelian! This will be very usefull!

In any case, if $A, B \in \mathcal{G}_n$ then **either** $[A, B] = 0$ or $\{A, B\} = 0$. Also, $A^2 = \pm I$.

The weight of A, $wt(A)$, is the number of factors different from I_2.
Eg, $wt(\sigma_x \otimes I \otimes \sigma_Z) = 2$.

Pauli group

Recall that σ_x, σ_z and σ_y anticommute.
Let

$$\mathcal{G}_n = \{\alpha A_1 \otimes \cdots \otimes A_n : A_i \in P, \alpha \in \{\pm 1, \pm i\}\},$$

called the (n-qubit) Pauli group.
Then $\mathcal{G}_n$ consists of the 4^n tensor products of $I, \sigma_x, \sigma_y, \sigma_z$ and an overall phase of ± 1 or $\pm i$, for a total of $4^n + 1$ elements.

$\mathcal{G}_n$ is **not** abelian! This will be very usefull!

In any case, if $A, B \in \mathcal{G}_n$ then **either** $[A, B] = 0$ or $\{A, B\} = 0$. Also, $A^2 = \pm I$.

The weight of A, $wt(A)$, is the number of factors different from I_2.
Eg, $wt(\sigma_x \otimes I \otimes \sigma_Z) = 2$.

The theory of error-correcting codes, namely algebraic coding theory, is well established. *But it doesn't apply here*, at least not directly. A simple classical code is the repetition code:

$$0 \mapsto 000$$
$$1 \mapsto 111$$

Try a quantum repetition code:

$$|\psi\rangle \mapsto |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle$$

That would violate the No-Cloning Theorem.

The theory of error-correcting codes, namely algebraic coding theory, is well established. *But it doesn't apply here*, at least not directly. A simple classical code is the repetition code:

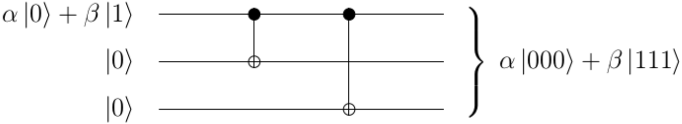
$$\begin{aligned} 0 &\mapsto 000 \\ 1 &\mapsto 111 \end{aligned}$$

Try a quantum repetition code:

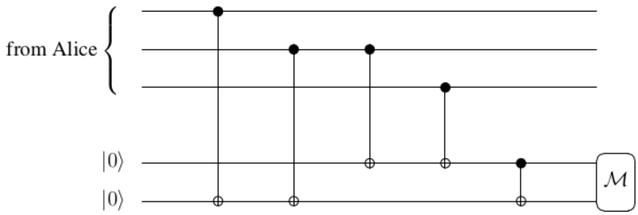
$$|\psi\rangle \mapsto |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle$$

That would violate the No-Cloning Theorem.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \mapsto \alpha|000\rangle + \beta|111\rangle$$



Alice sends $\alpha|000\rangle + \beta|111\rangle$ to Bob.
Bob receives $\alpha|010\rangle + \beta|101\rangle$ (i.e. there is a bit flip on the 2nd bit).



$$\begin{aligned}(\alpha|010\rangle + \beta|101\rangle)|00\rangle &= \alpha|010\rangle|00\rangle + \beta|101\rangle|00\rangle \\ &\mapsto \alpha|010\rangle|10\rangle + \beta|101\rangle|10\rangle \\ &= (\alpha|010\rangle + \beta|101\rangle)|10\rangle\end{aligned}$$

This output string is called the *syndrome*; in this case it tells us that a bit-flip error occurred on qubit number 2 (or 10 in binary). So, Bob corrects the error by applying σ_x to the 2nd qubit:

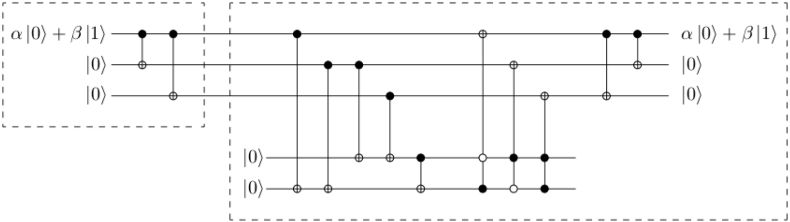
$$\alpha|010\rangle + \beta|101\rangle \mapsto \alpha|000\rangle + \beta|111\rangle$$

The same procedure works in the case that we have a bit-flip in the first or third qubits:

State	$\|000\rangle$	$\|001\rangle$	$\|010\rangle$	$\|011\rangle$	$\|100\rangle$	$\|101\rangle$	$\|110\rangle$	$\|111\rangle$
Syndrome	00	11	10	01	01	10	11	00

If no errors occur, or a single bit-flip occurs, the syndrome will correctly diagnose the errors (or lack of errors):

- No errors $\rightarrow$ Syndrome $= 00$
- σ_x applied to qubit number $j \in \{1, 2, 3\} \rightarrow$ Syndrome $= j$ (in binary).



The code corrects up to one bit-flip error. If two or more bit-flip errors occurred, there are no guarantees...

Suppose we have a *phase-flip* error. For instance, we have

$$\alpha|000\rangle + \beta|111\rangle \mapsto \alpha|000\rangle - \beta|111\rangle$$

if any odd number of phase-flips occur.

This error is represented by $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

We could change the encoding

$$\alpha|0\rangle + \beta|1\rangle \mapsto \alpha|+++\rangle + \beta|---\rangle$$

Just encode as previously and then apply a Hadamard transform on each qubit. The effect of a phase-flip on the basis $\{|+\rangle, |-\rangle\}$ is similar to the effect of a bit-flip on the standard basis $\{|0\rangle, |1\rangle\}$:

$$\sigma_z|+\rangle = |-\rangle,\ \sigma_z|-\rangle = |+\rangle.$$

Bob can easily correct against a phase-flip on a single qubit by first applying Hadamard transforms to all three qubits, and then correcting as before.

For instance, if a phase-flip happens on the 1st qubit, then

$$\alpha|+++\rangle + \beta|---\rangle$$

becomes

$$\alpha|-++\rangle + \beta|+--\rangle.$$

Bob applies Hadamard transforms to all three qubits and obtains

$$\alpha|100\rangle + \beta|011\rangle$$

and he then corrects just as before to obtain $\alpha|0\rangle + \beta|1\rangle$.
Although the new code protects against phase-flips, it fails to protect against bit-flips.
Is there any way to protect against both bit flips and phase flips simultaneously?

The 9-qubit Shor algoritm encodes

$$\begin{aligned} |0\rangle &\mapsto |\bar{0}\rangle = (|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) \\ |1\rangle &\mapsto |\bar{1}\rangle = (|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle) \end{aligned}$$

Suppose the channel flips a single qubit, i.e., $|0\rangle \leftrightarrow |1\rangle$; assume it flips the 1st qubit. We compare the first 2 qbits, and then the 1st and 3rd qbits. Note that we **do not actually measure** the first and second qubits, since this would destroy the superposition in the codeword.
So, how do we compare?
Recall that $\sigma_z|0\rangle = |0\rangle$ and $\sigma_z|1\rangle = -|1\rangle$. Then

$$\begin{aligned} (\sigma_z \otimes \sigma_z \otimes I)\,|100\rangle &= -|100\rangle \\ (\sigma_z \otimes I \otimes \sigma_z)\,|100\rangle &= -|100\rangle \\ (\sigma_z \otimes \sigma_z \otimes I)\,|011\rangle &= -|011\rangle \\ (\sigma_z \otimes I \otimes \sigma_z)\,|011\rangle &= -|011\rangle \end{aligned}$$

"This is equivalent to measuring the eigenvalues of $\sigma_{z1}\sigma_{z2}$ and $\sigma_{z1}\sigma_{z3}$", where

$$\sigma_{z1}\sigma_{z2} = \sigma_z \otimes \sigma_z \otimes I^{\otimes^7} \text{ and } \sigma_{z1}\sigma_{z3} = \sigma_z \otimes I \otimes \sigma_z \otimes I^{\otimes^6}$$

If the first 2 qbits are the same, the eigenvalue of $\sigma_{z1}\sigma_{z2}$ is $+1$. If they are different, then the eigenvalue is -1.
In order to detect a phase-flip, we compare the signs of the 1st and 2nd block, and of the 1st and 3rd block. I.e. the eigenvalues of

$$\sigma_{x_1}\sigma_{x_2}\sigma_{x_3}\sigma_{x_4}\sigma_{x_5}\sigma_{x_6} \text{ and } \sigma_{x_1}\sigma_{x_2}\sigma_{x_3}\sigma_{x_7}\sigma_{x_8}\sigma_{x_9}.$$

If the signs agree, that corresponds to obtaining the eigenvalue $+1$; otherwise, we get -1.
In order to correct flip and phase errors we hence need 8 matrices.

$$
\begin{array}{c|ccccccccc}
M_1 & \sigma_z & \sigma_z & I & I & I & I & I & I & I \\
M_2 & \sigma_z & I & \sigma_z & I & I & I & I & I & I \\
M_3 & I & I & I & \sigma_z & \sigma_z & I & I & I & I \\
M_4 & I & I & I & \sigma_z & I & \sigma_z & I & I & I \\
M_5 & I & I & I & I & I & I & \sigma_z & \sigma_z & I \\
M_6 & I & I & I & I & I & I & \sigma_z & I & \sigma_z \\
M_7 & \sigma_x & \sigma_x & \sigma_x & \sigma_x & \sigma_x & \sigma_x & I & I & I \\
M_8 & \sigma_x & \sigma_x & \sigma_x & I & I & I & \sigma_x & \sigma_x & \sigma_x
\end{array}
$$

The codewords $|\bar{0}\rangle$ and $|\bar{1}\rangle$ are eigenvectors of these M_i corresponding **to the eigenvalue 1**.
Set $\mathcal{G}_n = \{\alpha A_1 \otimes \cdots \otimes A_n : A_i \in P, \alpha \in \{\pm 1, \pm i\}\}$, $wt(H)$ the number of factor different from I_2, for $H \in \mathcal{G}_n$.
If $H \in \mathcal{G}_8$ s.t. $H|\bar{0}\rangle = |\bar{0}\rangle, H|\bar{1}\rangle = |\bar{1}\rangle$ then $H \in \langle M_1, M_2, \ldots, M_7, M_8\rangle$.
These operators that fix $|\bar{0}\rangle$ and $|\bar{1}\rangle$ form a **group** $\mathcal{S}$, called the *stabilizer* of the code.

When we measure the eigenvalue of

$$M_1 = \sigma_z \otimes \sigma_z \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I$$

we determine if a bit flip error has occurred on qubit one or two, i.e., if σ_{x1} or σ_{x2} has occurred. Both of these errors anticommute with M_1, while $\sigma_{x3}, \dots, \sigma_{x9}$, which cannot be detected by just M_1, commute with it. Similarly, M_2 detects σ_{x1} or σ_{x3}, which anticommute with it, and M_7 detects σ_{z1} through σ_{z6}. In general,

$$\text{if } M \in \mathcal{S}, \{M, E\} = 0, |\psi\rangle \in T \text{ then } ME|\psi\rangle = -EM|\psi\rangle = -E|\psi\rangle$$

so $E|\psi\rangle$ is an eigenvector of M corresponding to the eigenvalue -1.

Theorem

If a quantum code corrects errors A and B, it also corrects any linear combination of A and B. In particular, if it corrects all weight t Pauli errors, then the code corrects all t-qubit errors.

Suppose now that every qubit in our 9-qubit code has some small error. For instance, error $I + \epsilon E_i$ acts on qubit i , where E_i is some single qubit error. Then the overall error is

$$\bigotimes (I + \epsilon E_i) = I + \epsilon(E_1 \otimes I^{\otimes 8} + I \otimes E_2 \otimes I^{\otimes 7} + \cdots) + O(\epsilon^2)$$

To order ϵ, the actual error is the sum of single-qubit errors, which we can correct. While the code cannot completely correct this error, it still produces a significant improvement over not doing error correction when ϵ is small. A code correcting more errors would do even better.

The *stabilizer* $\mathcal{S}$ is some abelian subgroup of $\mathcal{G}$ (that is, all commute with each other, $I \in \mathcal{S}$ and it is closed under products) such that $-I \notin \mathcal{S}$.
The coding space T (also called the stabilizer subspace $\mathcal{H}$) is the space of vectors fixed by $\mathcal{S}$.

$$\mathcal{H} = T = \{|\psi\rangle : M|\psi\rangle = |\psi\rangle, \forall M \in \mathcal{S}\}$$

An example of a stabilizer group on three qubits is

$$\mathcal{S} = \{I \otimes I \otimes I, \sigma_z \otimes \sigma_z \otimes I, \sigma_z \otimes I \otimes \sigma_z, I \otimes \sigma_z \otimes \sigma_z\}.$$

We simplify the notation by

$$\mathcal{S} = \{III, ZZI, ZIZ, IZZ\}.$$

Note that $\mathcal{S} = \langle ZZI, ZIZ \rangle$.

A well known quantum code is the [[5, 1, 3]] code.

Its stabilizer is given by

$$\begin{matrix} X & Z & Z & X & I \\ I & X & Z & Z & X \\ X & I & X & Z & Z \\ Z & X & I & X & Z \end{matrix}$$

Of course, we should verify that it commutes.

Consider the parity check matrix of the Hamming code [7, 4, 3]:

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

and **replace** 1 by Z and 0 by I. The generated group identifies bit-flip errors (X).
Analogously, replacing 1 by X and 0 by I will detect phase-flip errors (Z). Y errors are distinguished by showing up in both halves.
The stabilizer group $\mathcal{S}$ is generated by

$$ZZZZIII$$
$$ZZIIZZI$$
$$ZIZIZIZ$$
$$XXXXIII$$
$$XXIIXXI$$
$$XIXIXIX$$

One needs to check: the stabilizer must be **abelian**; but that is easily verified.
The stabilizer has 6 generators on 7 qubits, so it encodes 1 qubit and the quantum code $\mathcal{H}_{\mathcal{S}}$ corrects 1 single qbit. It is a $[[7, 1, 3]]$ code.

This is the **Steane** 7 qubit quantum code.

For the 7-qubit code, we used the same classical code for both the X and Z generators.

But **we could have used any two classical codes**.

Remember: we need that the X and Z generators to commute. This corresponds to $C_2^{\perp} \subseteq C_1$.
If C_1 is an $[n, k_1, d_1]$ code, and C_2 is an $[n, k_2, d_2]$ code with $C_2^{\perp} \subseteq C_1$ then

the corresponding quantum code is an $[[n, k_1 + k_2 n, \min(d_1, d_2)]]$ code.

This gives a **CSS code**, due to Calderbank, Shor and Steane.

- D. Gottesman, *Stabilizer codes and quantum error correction*, Ph.D. thesis, Caltech, 2002.
- Daniel Gottesman, An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation, *Proceedings of Symposia in Applied Mathematics*, `https://arxiv.org/abs/0904.2557v1`, 2009.
- John Watrous, Notes of CPSC 519/619: Quantum Computation, University of Calgary, 2006.
- Dave Bacon, Notes of CSE 599d – Quantum Computing, University of Washington.
- Salah A. Aly, *On Quantum and Classical Error Control Codes: Constructions and Applications*, Ph.D. thesis, Department of Computer Science at Texas A&M University, 2007.
- Mark McMahon Wilde, *Quantum Coding with Entanglement*, Ph.D. thesis, University of Southern California, 2008.
- Lisa Steiner, *A $C*$-Algebraic Approach to Quantum Coding Theory*, Ph.D. thesis, Darmstadt, 2008.