Coding theory: into the quantum world

Robin Simoens

Universitat Polytècnica de Catalunya & Ghent University

10 January 2024

SIMBa seminar

North:	00
East:	01
South:	10
West:	11

North:	00
East:	01
South:	10
West:	11

- Does not detect mistakes

North:	000
East:	011
South:	101
West:	110

- Detects 1 mistake

North:	00000
East:	01101
South:	10110
West:	11011

- Detects 2 mistakes
- Corrects 1 mistake

Classical coding theory

Coding theory, not to be confused zith cryptogrqphy, is q brqnch of informqtion theory thqt qdds redundqnt informqtion such thqt the informqtion is better protected qgqinst possible mistqkes thqt occur during trqnsmission.

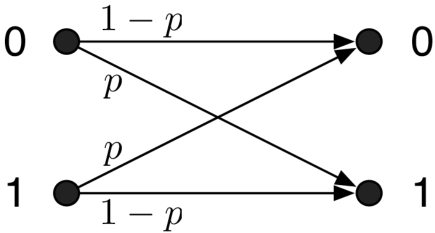
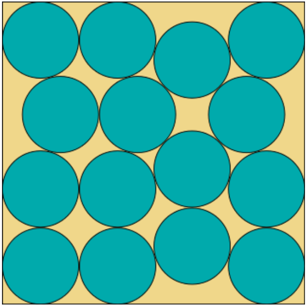


Figure: Binary symmetric channel

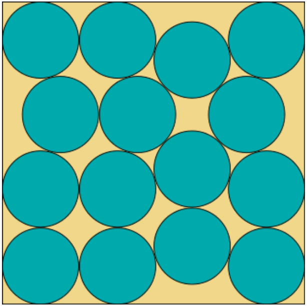
Definition

The **distance** between two codewords is the number of positions in which they differ.



Definition

The **distance** between two codewords is the number of positions in which they differ.



- A code with minimum distance d can detect $d-1$ errors.
- A code with minimum distance d can correct $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors.

Repetition code:

$$0 \mapsto \underbrace{000000000}_{9}$$

$$1 \mapsto \underbrace{111111111}_{9}$$

Repetition code:

$$0 \mapsto \underbrace{000000000}_{9}$$
$$1 \mapsto \underbrace{111111111}_{9}$$

- 2 codewords

Repetition code:

$$0 \mapsto \underbrace{000000000}_{9}$$
$$1 \mapsto \underbrace{111111111}_{9}$$

- 2 codewords
- length $n = 9$

Repetition code:

$$0 \mapsto \underbrace{000000000}_{9}$$
$$1 \mapsto \underbrace{111111111}_{9}$$

- 2 codewords
- length $n = 9$
- minimum distance $d = 9$

Repetition code:

$$0 \mapsto \underbrace{000000000}_{9}$$
$$1 \mapsto \underbrace{111111111}_{9}$$

- 2 codewords
- length $n = 9$
- minimum distance $d = 9$

- Detects 8 errors
- Corrects 4 errors

Problem (Main problem of coding theory)

Given

- *length* n
- *minimum distance* d

what is the maximum number of codewords that you can construct?

$A_2(n,d)$		d									
		1	2	3	4	5	6	7	8	9	10
n	1	2	/	/	/	/	/	/	/	/	/
	2	4	2	/	/	/	/	/	/	/	/
	3	8	4	2	/	/	/	/	/	/	/
	4	16	8	2	2	/	/	/	/	/	/
	5	32	16	4	2	2	/	/	/	/	/
	6	64	32	8	4	2	2	/	/	/	/
	7	128	64	16	8	2	2	2	/	/	/
	8	256	128	20	16	4	2	2	2	/	/
	9	512	256	40	20	6	4	2	2	2	/
	10	1024	512	72	40	12	6	2	2	2	2

Definition

A **linear code** is a subspace of $\mathbb{F}_2^n$.

Definition

A **linear code** is a subspace of $\mathbb{F}_2^n$.

Generator matrix:

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Code: 00000
11100
10011
01111

Definition

A **linear code** is a subspace of $\mathbb{F}_2^n$.

Generator matrix:

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Parity check matrix:

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

Code: 00000
11100
10011
01111

Definition

A **linear code** is a subspace of $\mathbb{F}_2^n$.

Generator matrix:

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

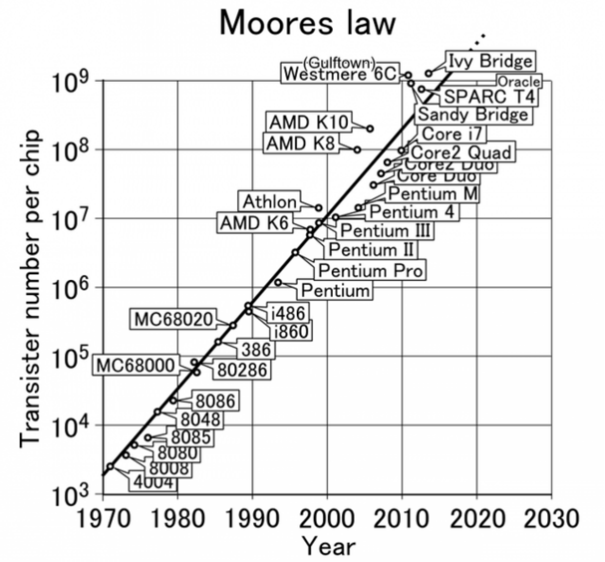
Parity check matrix:

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

Code: 00000
11100
10011
01111

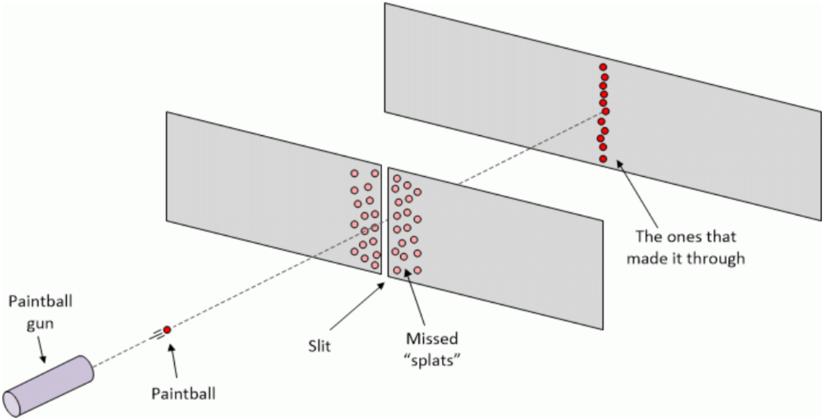
Error syndrome: $c \cdot H^T$
$c \cdot H^T = 0 \Leftrightarrow c$ is a codeword

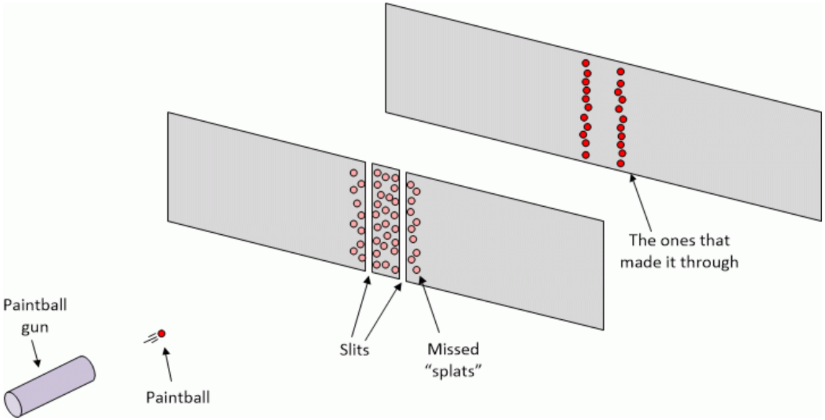
Moore’s law

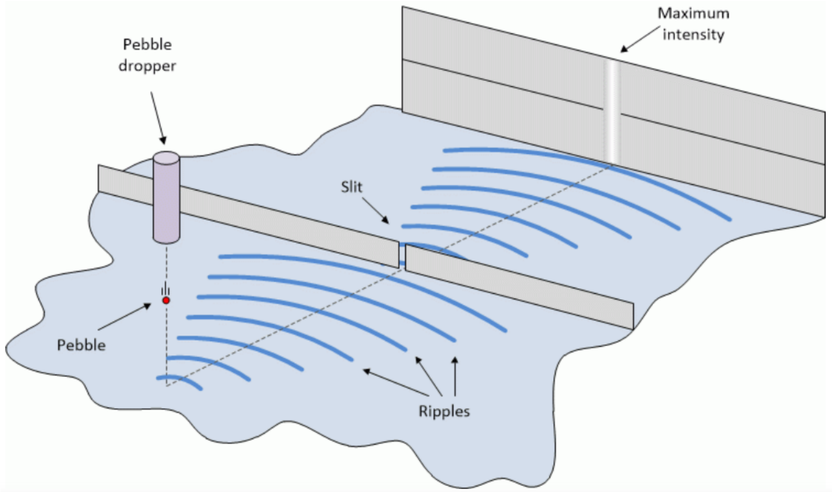


Moores law
Transister number per chip
Year
1970
1980
1990
2000
2010
2020
2030
10^3
10^4
10^5
10^6
10^7
10^8
10^9
4004
8008
8080
8085
8048
8086
MC68000
80286
386
MC68020
i486
i860
Pentium
Pentium Pro
Pentium II
Pentium III
AMD K6
Athlon
Pentium 4
Pentium M
Core Duo
Core2 Duo
Core2 Quad
Core i7
AMD K8
AMD K10
Sandy Bridge
Oracle
SPARC T4
(Gulftown)
Westmere 6C
Ivy Bridge

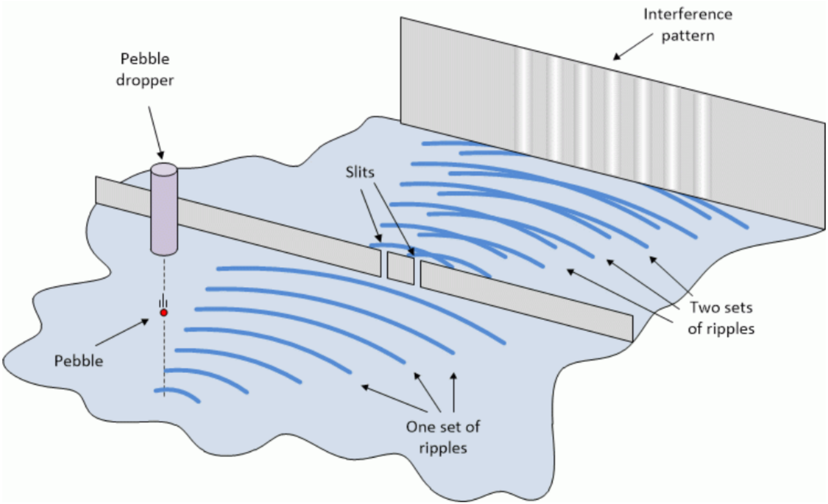
Quantum mechanics

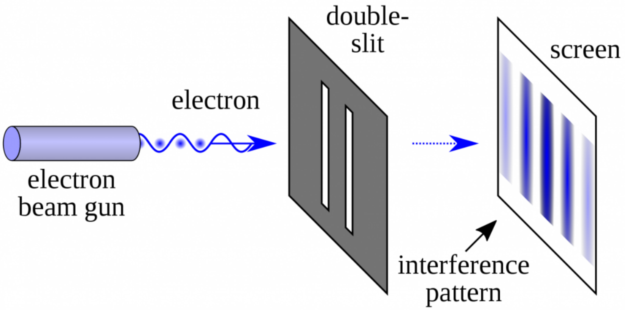



Paintball
gun
Paintball
Slits
Missed
"splats"
The ones that
made it through


Pebble
dropper
Maximum
intensity
Slit
Pebble
Ripples

Quantum mechanics



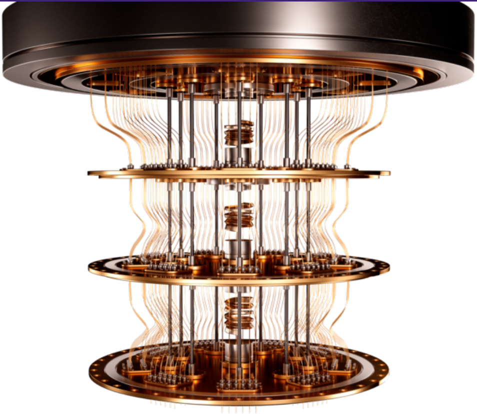

double-
slit
screen
electron
electron
beam gun
interference
pattern


SCHRODINGER'S
CAT
(maybe)

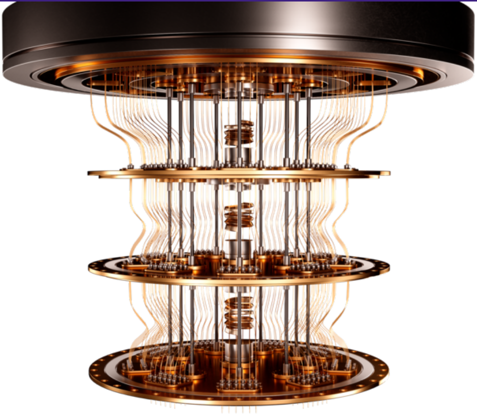
Quantum mechanics

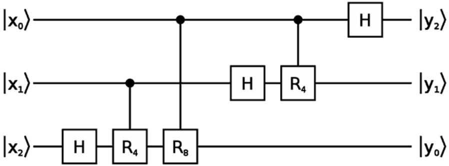
Anyone who is not shocked by quantum theory has not understood it.

Niels Bohr



Quantum coding theory



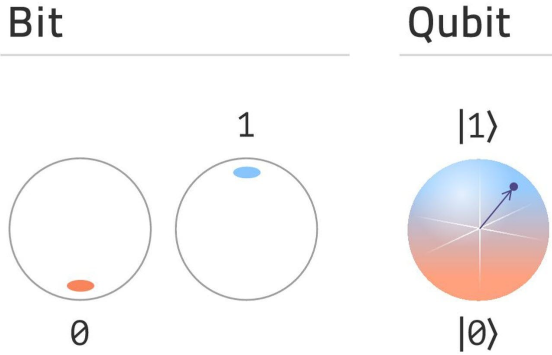


Qubits:

$$|0\rangle := \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle := \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$



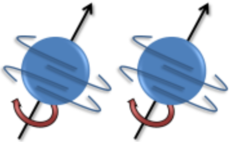
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Axioms of quantum mechanics

- **Axiom 1:** A physical system is described by a unit vector in $\left(\mathbb{C}^2\right)^{\otimes n}$.
- **Axiom 2:** An evolution on a closed system corresponds to a unitary operator acting on that vector.
- **Axiom 3:** A measurement causes a state to collapse and is probabilistic in nature.
- ...

Definition

A quantum code is a subspace of $\left(\mathbb{C}^2\right)^{\otimes n}$.



$\dots$

Quantum coding theory

Definition

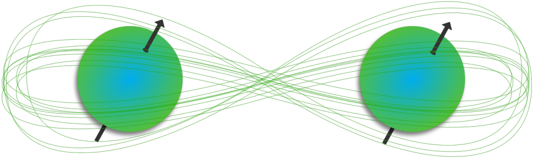
A quantum code is a subspace of $\left(\mathbb{C}^2\right)^{\otimes n}$.

$$|0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |0\rangle$$

Definition

A quantum code is a subspace of $\left(\mathbb{C}^2\right)^{\otimes n}$.

$$\frac{1}{\sqrt{2}}\,|0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle \otimes |1\rangle$$



Problems:

- **Measurement destroys information**

Problems:

- **Measurement destroys information**
  Solution: only measure *syndromes*.

Problems:

- **Measurement destroys information**
  Solution: only measure *syndromes.*
- **Errors are continuous**

Problems:

- **Measurement destroys information**
  Solution: only measure *syndromes*.
- **Errors are continuous**
  Solution: discretisation of errors.

Theorem (Discretisation of errors)

It suffices to correct the following errors:

- *Bit flips:*

$$|0\rangle \mapsto |1\rangle \ \textit{and} \ |1\rangle \mapsto |0\rangle\,, \ \textit{i.e.} \ \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \mapsto \begin{bmatrix}\beta\\ \alpha\end{bmatrix}$$

These errors are elements of the the **Pauli group**.

Theorem (Discretisation of errors)

It suffices to correct the following errors:

- *Bit flips:*

$$|0\rangle \mapsto |1\rangle \ \textit{and}\ |1\rangle \mapsto |0\rangle\,,\ \textit{i.e.}\ \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \mapsto \begin{bmatrix}\beta\\ \alpha\end{bmatrix}$$

- *Phase flips:*

$$|0\rangle \mapsto |0\rangle \ \textit{and}\ |1\rangle \mapsto -|1\rangle\,,\ \textit{i.e.}\ \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \mapsto \begin{bmatrix}\alpha\\ -\beta\end{bmatrix}$$

These errors are elements of the the **Pauli group**.

Theorem (Discretisation of errors)

It suffices to correct the following errors:

- *Bit flips:*

$$|0\rangle \mapsto |1\rangle \ \textit{and} \ |1\rangle \mapsto |0\rangle\,, \ \textit{i.e.} \ \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \mapsto \begin{bmatrix}\beta\\ \alpha\end{bmatrix}$$

- *Phase flips:*

$$|0\rangle \mapsto |0\rangle \ \textit{and} \ |1\rangle \mapsto -|1\rangle\,, \ \textit{i.e.} \ \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \mapsto \begin{bmatrix}\alpha\\ -\beta\end{bmatrix}$$

- *Both a bit flip and a phase flip.*

These errors are elements of the the **Pauli group**.

Repetition code:

$$
\begin{aligned}
|0\rangle &\mapsto |0\rangle \otimes |0\rangle \otimes |0\rangle \\
|1\rangle &\mapsto |1\rangle \otimes |1\rangle \otimes |1\rangle
\end{aligned}
$$

Repetition code:

$$|0\rangle \mapsto |0\rangle \otimes |0\rangle \otimes |0\rangle$$
$$|1\rangle \mapsto |1\rangle \otimes |1\rangle \otimes |1\rangle$$

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \mapsto \alpha\,|0\rangle \otimes |0\rangle \otimes |0\rangle + \beta\,|1\rangle \otimes |1\rangle \otimes |1\rangle$$

Repetition code:

$$|0\rangle \mapsto |0\rangle \otimes |0\rangle \otimes |0\rangle$$
$$|1\rangle \mapsto |1\rangle \otimes |1\rangle \otimes |1\rangle$$

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} \mapsto \alpha\,|0\rangle \otimes |0\rangle \otimes |0\rangle + \beta\,|1\rangle \otimes |1\rangle \otimes |1\rangle$$

No cloning

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} \not\mapsto \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \otimes \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \otimes \begin{bmatrix}\alpha\\ \beta\end{bmatrix}$$

Repetition code:

$$|0\rangle \mapsto |0\rangle \otimes |0\rangle \otimes |0\rangle$$
$$|1\rangle \mapsto |1\rangle \otimes |1\rangle \otimes |1\rangle$$

$$\begin{bmatrix}\alpha \\ \beta\end{bmatrix} \mapsto \alpha\,|0\rangle \otimes |0\rangle \otimes |0\rangle + \beta\,|1\rangle \otimes |1\rangle \otimes |1\rangle$$

- code of dimension 2

Repetition code:

$$|0\rangle \mapsto |0\rangle \otimes |0\rangle \otimes |0\rangle$$
$$|1\rangle \mapsto |1\rangle \otimes |1\rangle \otimes |1\rangle$$

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \mapsto \alpha\,|0\rangle \otimes |0\rangle \otimes |0\rangle + \beta\,|1\rangle \otimes |1\rangle \otimes |1\rangle$$

- code of dimension 2
- length $n = 3$

Repetition code:

$$|0\rangle \mapsto |0\rangle \otimes |0\rangle \otimes |0\rangle$$
$$|1\rangle \mapsto |1\rangle \otimes |1\rangle \otimes |1\rangle$$

$$\begin{bmatrix}\alpha \\ \beta\end{bmatrix} \mapsto \alpha\,|0\rangle \otimes |0\rangle \otimes |0\rangle + \beta\,|1\rangle \otimes |1\rangle \otimes |1\rangle$$

- code of dimension 2
- length $n = 3$
- minimum distance $d = 1$ ($\neq 3$)

Repetition code:

$$|0\rangle \mapsto |0\rangle \otimes |0\rangle \otimes |0\rangle$$
$$|1\rangle \mapsto |1\rangle \otimes |1\rangle \otimes |1\rangle$$

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} \mapsto \alpha\,|0\rangle \otimes |0\rangle \otimes |0\rangle + \beta\,|1\rangle \otimes |1\rangle \otimes |1\rangle$$

- code of dimension 2
- length $n = 3$
- minimum distance $d = 1$ ($\neq 3$)

- Detects 2 flip errors
- Detects 0 phase errors

Problem (Main problem of quantum coding theory)

Given

- *length* n
- *minimum distance* d

what is the maximum dimension of a quantum code?

Definition (Stabiliser code)

$$\mathcal{C} = \{|\psi\rangle \in \left(\mathbb{C}^2\right)^{\otimes n} \mid E|\psi\rangle = |\psi\rangle \text{ for all } E \in S\} \quad \text{where } S \leqslant \mathcal{P}_n$$

$$S = \left\langle cX^{\vec{a}_i} Z^{\vec{b}_i} \right\rangle_{1 \leq i \leq r}$$

$$\mathcal{G} = \left(\begin{array}{ccc|ccc} a_{11} & \cdots & a_{1n} & b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{r1} & \cdots & a_{rn} & b_{r1} & \cdots & b_{rn} \end{array}\right)$$

CSS construction:

$$\mathcal{G} = \left(\begin{array}{c|c} G & O \\ \hline O & H \end{array} \right)$$

where G and H are the generator matrix and parity check matrix of a classical linear code.

Classical **Quantum**

Classical	**Quantum**
Intuitive	Weird

Classical	**Quantum**
Intuitive	Weird
Discrete	Continuous

Classical	**Quantum**
Intuitive	Weird
Discrete	Continuous
Mostly transmission	Mostly storage

Classical	**Quantum**
Intuitive	Weird
Discrete	Continuous
Mostly transmission	Mostly storage
Well-developed	Still a long way to go

Summary

Classical	**Quantum**
Intuitive	Weird
Discrete	Continuous
Mostly transmission	Mostly storage
Well-developed	Still a long way to go

Same fundamental principles:

Adding redundant information
Measuring syndromes

Thank you for listening!

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \otimes \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} & a_{12} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \\ a_{21} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} & a_{22} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{bmatrix}$$