I. Introduction

What is Quantum Information Theory?

→ The study of information processing using the laws of quantum mechanics

Quantum mechanics / quantum theory:
The most general framework to describe matter at the fundamental (microscopic) level.

Quantum theories exist for almost all classical physical theories: mechanics (i.e. motion of particles subject to forces), electrodynamics, ... – except gravity.

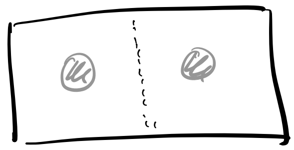
Here, q. mechanics (or q. theory, or q. physics) always refers to the <u>general framework</u>.

Why should we study information processing in the framework of quantum theory?

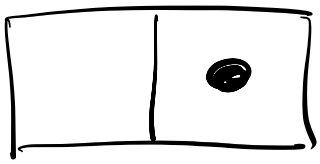
Even <u>further</u>: Why should we study information processing in the context of <u>physics</u>?

Information is a priori a concept unrelated to its physical realization (modern computers, punchcard, relays, paper, ...) – classical information theory (Shannon theory) never talks about physics.

Landauer (1961): Erasing information creates heat:



particle in box at unknown position:
1 bit of information
entropy $S_0 = k \ln 2$



particle in box at known position
bit erased (reset)
entropy $S_1 = 0$

$$\Delta S_{sys} = -k \ln 2 \Rightarrow \Delta Q_{env} = -T \Delta S_{sys} = kT \ln 2$$

$\Rightarrow$ Erasing 1 bit releases $\Delta Q = kT \ln 2$ heat – independent of realization!

Landauer: "Information is physical"

(i.e. we need to take at least the fundamental phys. principles into account when thinking about info. processing in <u>real systems</u>.)

On the other hand: <u>"Moore's Law"</u>

→ # transistors/chip doubles every 18 months

→ transistor size eventually approaches atomic size!

→ must take quantum effects into account: either fight them or <u>use them</u>.

→ Quantum Information Theory

→ information processing taking into account the fundamental principles of q. theory

— <u>independent</u> of specific physical realization.

Basic principles, ideas, and applications of QI

Classical information: <u>bit</u> $b = 0, 1$

Quantum info: <u>quantum bit</u> (<u>qubit</u>)

with two basis vectors $\vec{e}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\vec{e}_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

General qubit configuration ("state") is a <u>superposition</u>

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2 \quad , \quad |\alpha|^2 + |\beta|^2 = 1$$

For simplicity, consider $\alpha = \cos \varphi/2$, $\beta = \sin \varphi/2$:

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \cos \varphi/2 \\ \sin \varphi/2 \end{pmatrix} \qquad (\varphi \in [0, \pi))$$

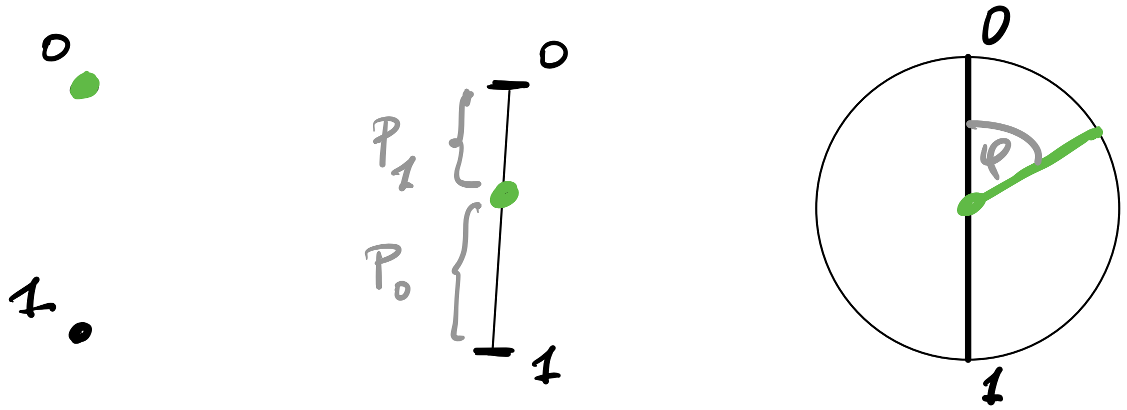
Has <u>similarities</u> to prob. distributions over classical bits,

$\begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$ with $p_0, p_1 \geq 0$, $p_0 + p_1 = 1$, but also

key <u>differences</u>.

Visualization:

Classical: **probabilistic:**



0 or 1 $\qquad \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} \qquad \begin{pmatrix} \cos \varphi/2 \\ \sin \varphi/2 \end{pmatrix}$

Key process: "measurement":

i.e. check (test, measure, read out) the value of a classical bit (e.g., a coin in a box) prepared in a state $\begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$.

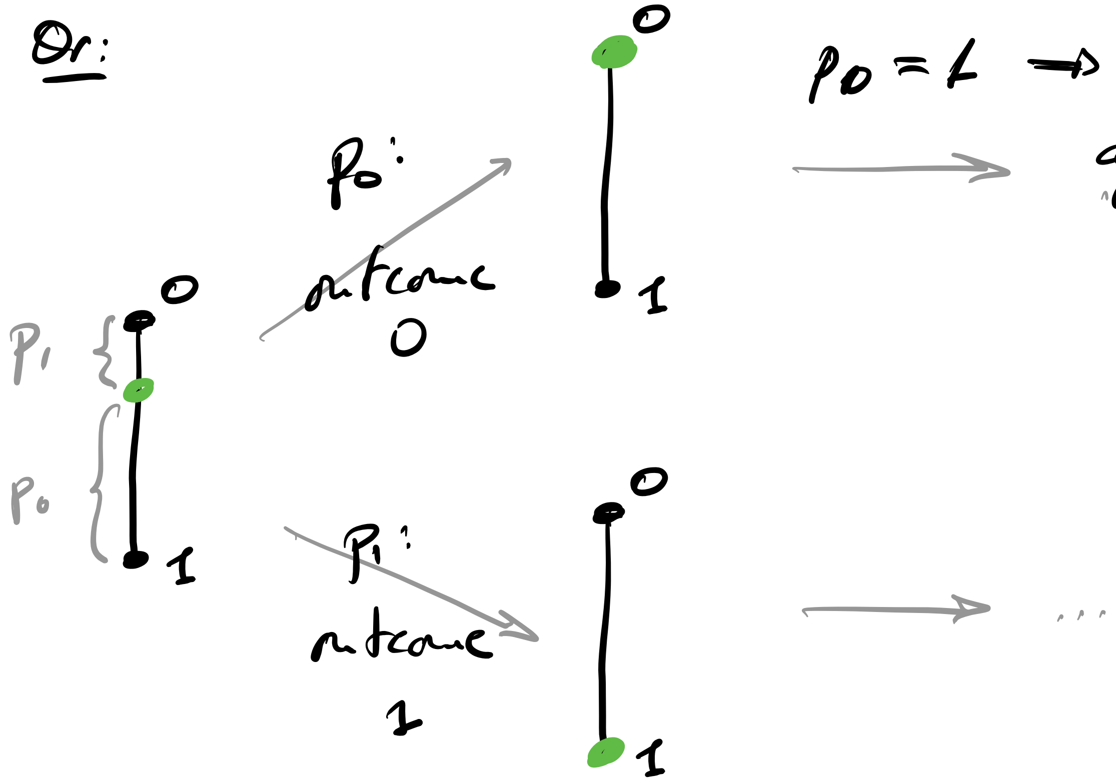
$$\begin{pmatrix} p_0 \\ p_1 \end{pmatrix} \xrightarrow[\text{meas.}]{\text{prob. } p_0} \text{result "0"} \longrightarrow \text{updated state } \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} p_0 \\ p_1 \end{pmatrix} \xrightarrow[\text{meas.}]{\text{prob. } p_1} \text{result "1"} \longrightarrow \text{updated state } \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

(2nd measurement gives same result (no new info).

$\rightarrow$ measurement "collapses" state.

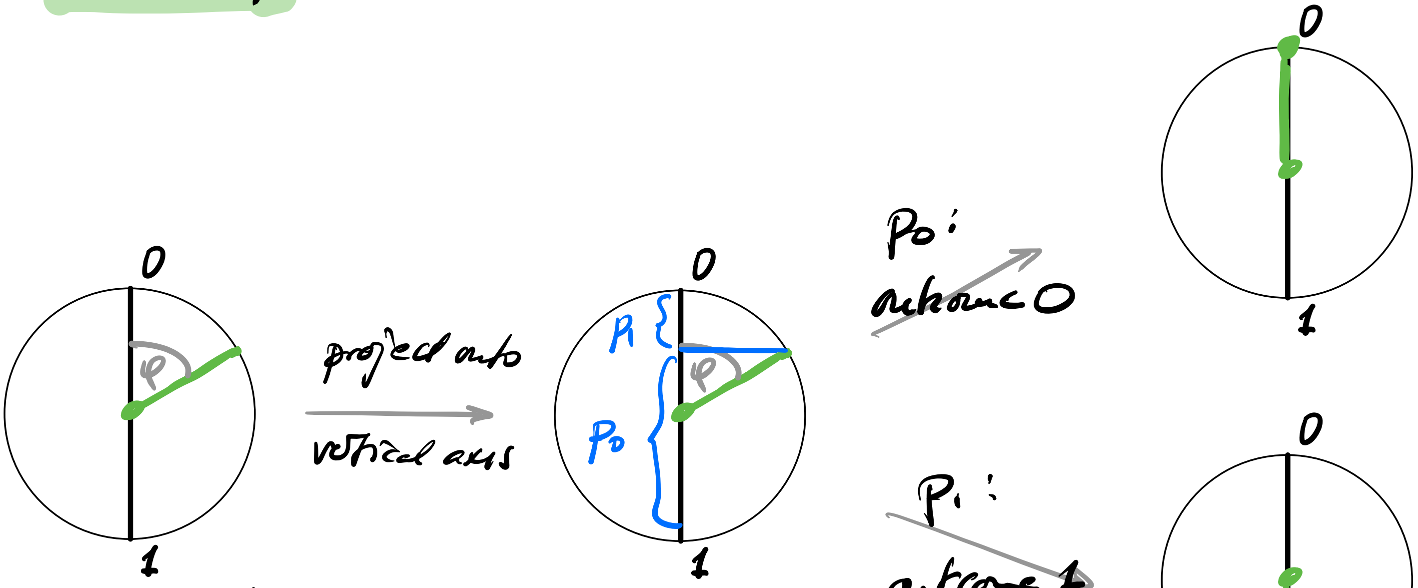
Or:



$p_0 = 1$ → further meas. again return 0.

Measurement of a quantum st:

Case a) Measurement in the "computational basis"

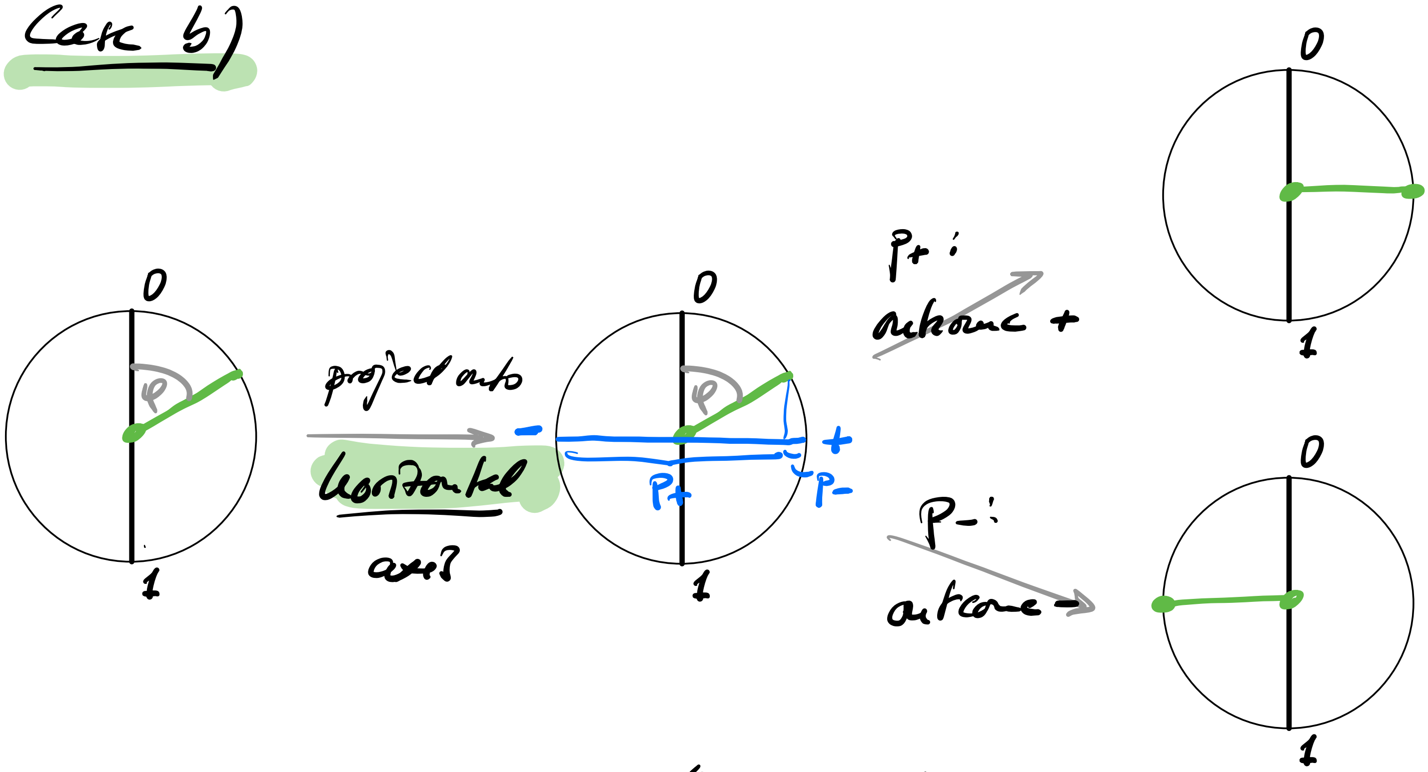


$$\begin{pmatrix} \cos \varphi/2 \\ \sin \varphi/2 \end{pmatrix}$$

measurement changes ("collapses") state:
subsequent measurements will reproduce outcome.

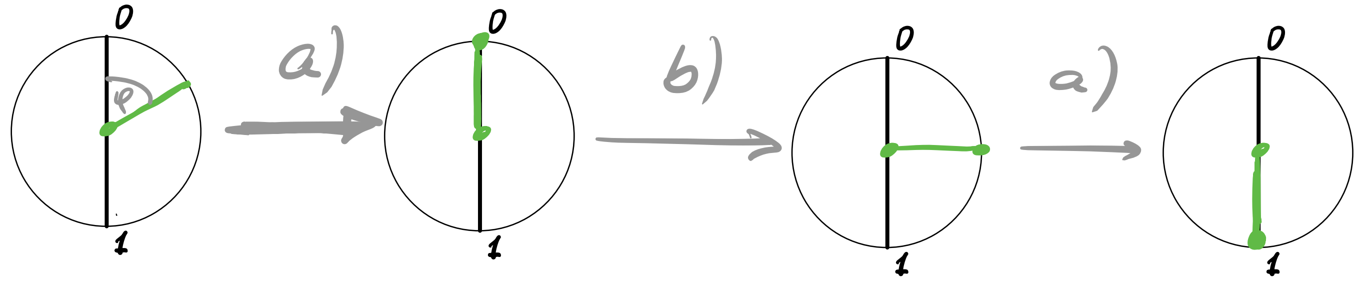
But: In quantum theory, other measurements exist, e.g.

Case b)



Again, measurement "collapses" state in a way where subsequent identical measurements give the same outcome.

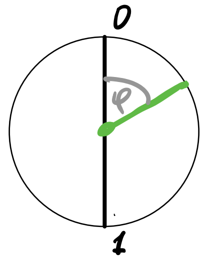
What if we alternate "Case a)" and "Case b)" meas.?



probability: $\frac{1}{2}$ $\frac{1}{2}$

Measuring one "property" can affect others:

- Properties are <u>not independent</u>.
- There is no 1-to-1 correspondence between the numbers $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ or point on the circle and properties we can measure.

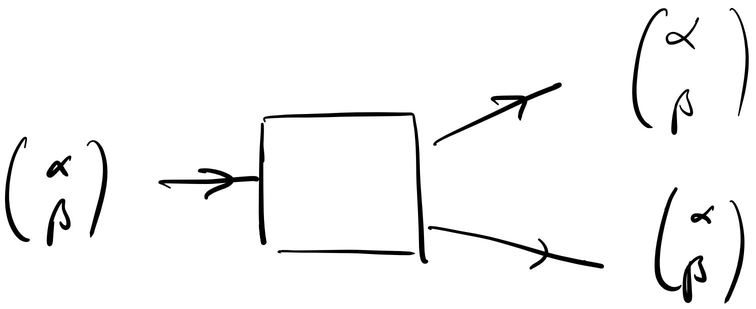


- "Incompatible" properties cannot be measured simultaneously.

Consequences:

- <u>"No-cloning-theorem"</u>

  Quantum information cannot be copied, i.e. a device



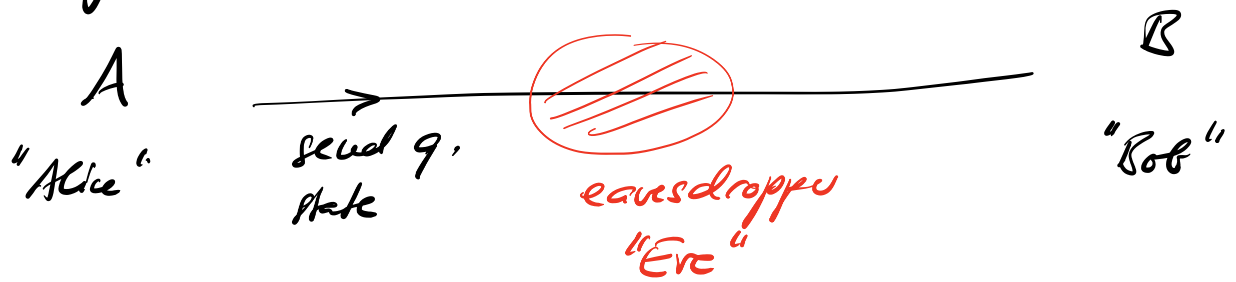
does not exist!

(Otherwise, we <u>could</u> determine $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ exactly, and measure diff. quantities at the same time.)

(Note: The same hold for class. prob. distributions.)

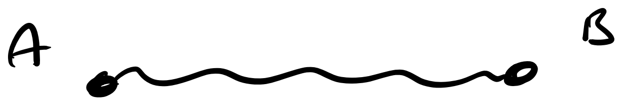
∘ Quantum Cryptography

Doing meas. disturbs quantum state:



Measurement disturbs state ⟶
Eve cannot obtain information about state sent
without A & B noticing ⟶ can be used to establish
secret keys.

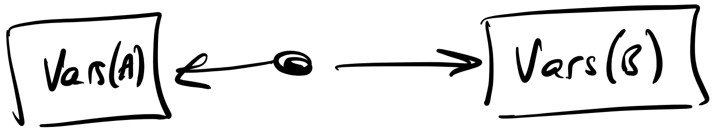
∘ Entanglement, teleportation, Bell inequalities



A & B share <u>joint</u> state: distribution over
00, 01, 10, 11: $\begin{array}{cc} \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} & \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} \end{array}$

Can choose state such that outcomes are perfectly correlated
for <u>all</u> measurements.

This can also happen in a classical theory:
A "hidden variable model" has an independent pre-determined outcome for every test (like a coin).
But: A local hidden variable (LHV) model



where the boxes cannot communicate (→ relativity!)
satisfies special inequalities ("Bell inequalities")
which are violated by quantum states!

→ "Entanglement"

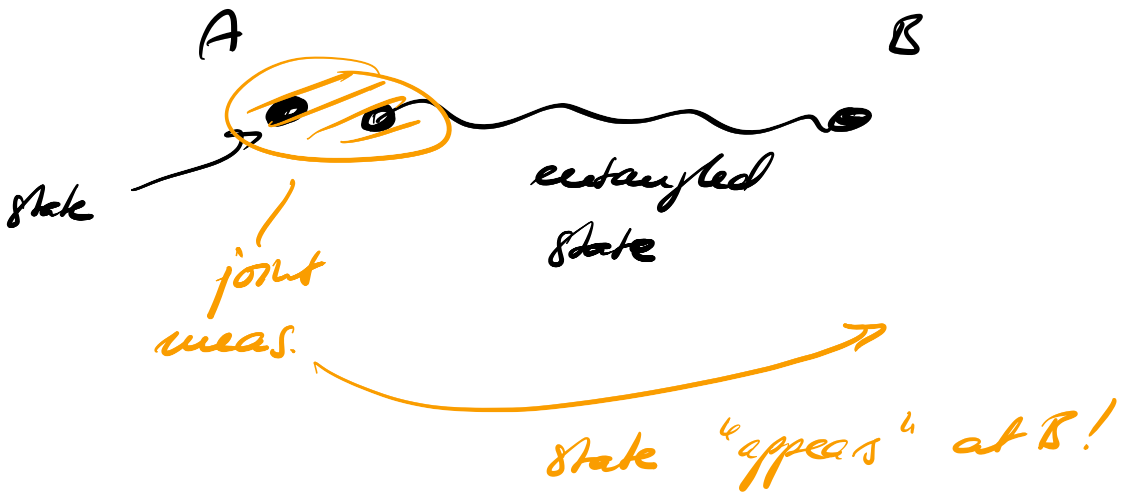
→ Q.M. states can display non-classical correlations.

But: No faster-than-light communication possible!!

This also highlights a fundamental difference between probability theory and quantum theory: In prob. th., values are real indep. of measurement, and the state $\begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$ merely signifies a lack of knowledge.
Quantum theory does not allow for such an interpretation.

Teleportation: A wants to get q. state to B, without risking to lose state. But: No-cloning theorem → A cannot make copies!

→ Teleportation:



→ Does this allow for faster-than-light comm.?

→ No! State on B's side is "scrambled", and requires A's meas. outcome (sent as classical info at speed of light) to be decoded!

Note: The state of the system is teleported, not the system itself.

(Asher Peres: "disembodied reincarnation")

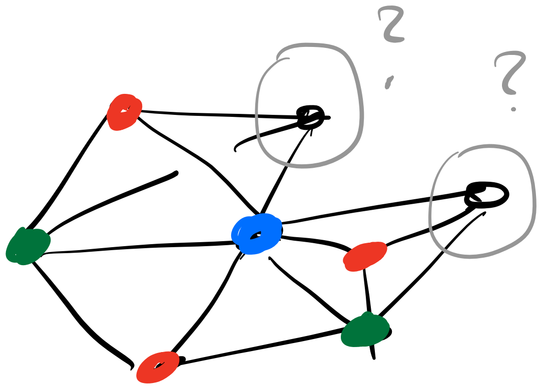
• Quantum Computing:

Typical hard computational problem:

"NP problems": Solution may be hard to find,

but easy to check.

E.g. graph coloring:



Can we color given graph with e.g. 3 colors w/out same color on adjacent vertices?

Given solution: easy to check!

Quantum computer: Work with quantum bits!

→ Superposition of all possibilities!

→ Might be able to check all solutions at the same time!

→ But: How can we single out the good solutions? Non-trivial problem!

(Note: For class. prob. distr. it also looks like we can test "all possibilities", but there, this is only describes randomly testing possibilities.

What is different in QI? → Negative numbers!)

Shor '94: Quantum computers can factor numbers exponentially faster than any known classical algorithm.

Quantum Error Correction:

Noise can destroy quantum information!

↑

Any kind of influence from the outside!

How can we protect Q.I. from errors (when storing, transmitting, processing it)?

Classical info: Copy!

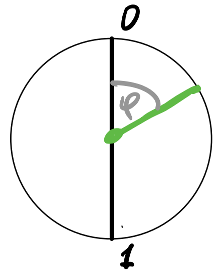
$$\begin{array}{ccccccc} 0 \rightarrow 000 & \xrightarrow[\text{flip bit 3}]{\text{error, e.g.}} & 001 & \xrightarrow[\text{maj. vote}]{\text{correction}} & 0 \\ 1 \rightarrow 111 & & 110 & & 1 \ \checkmark \end{array}$$

→ Decreases effective error rate!

Quantum Info: several issues!

- cloning impossible!
- meas. destroys q. state → how to do majority vote?
- errors can be continuous

  → is it even possible to identify the error?



→ Quantum Error Correction!

Use quantum superpositions to protect quantum superpositions!