Quantum Computation & Cryptography
Day 5

Fault tolerance and the future

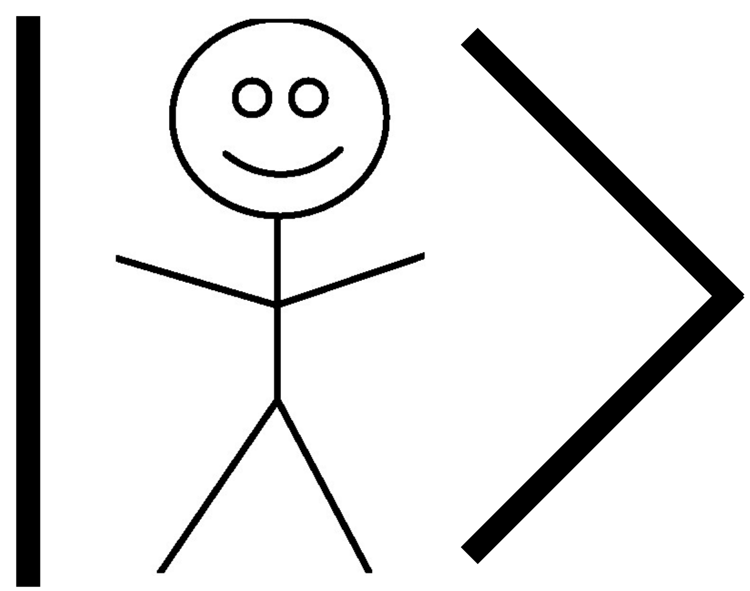
Andru Gheorghiu

Understanding decoherence

Suppose we have a qubit that we want to measure

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

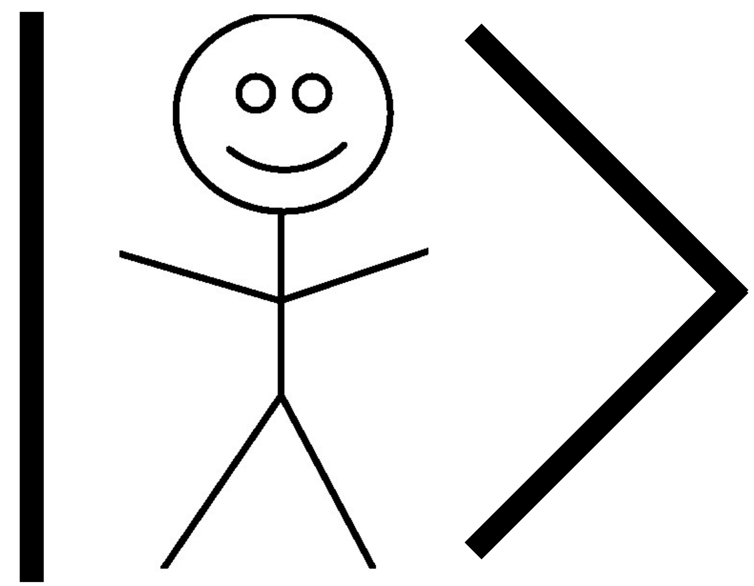
What does the state of the universe (me + qubit) look like?



$|\psi\rangle$

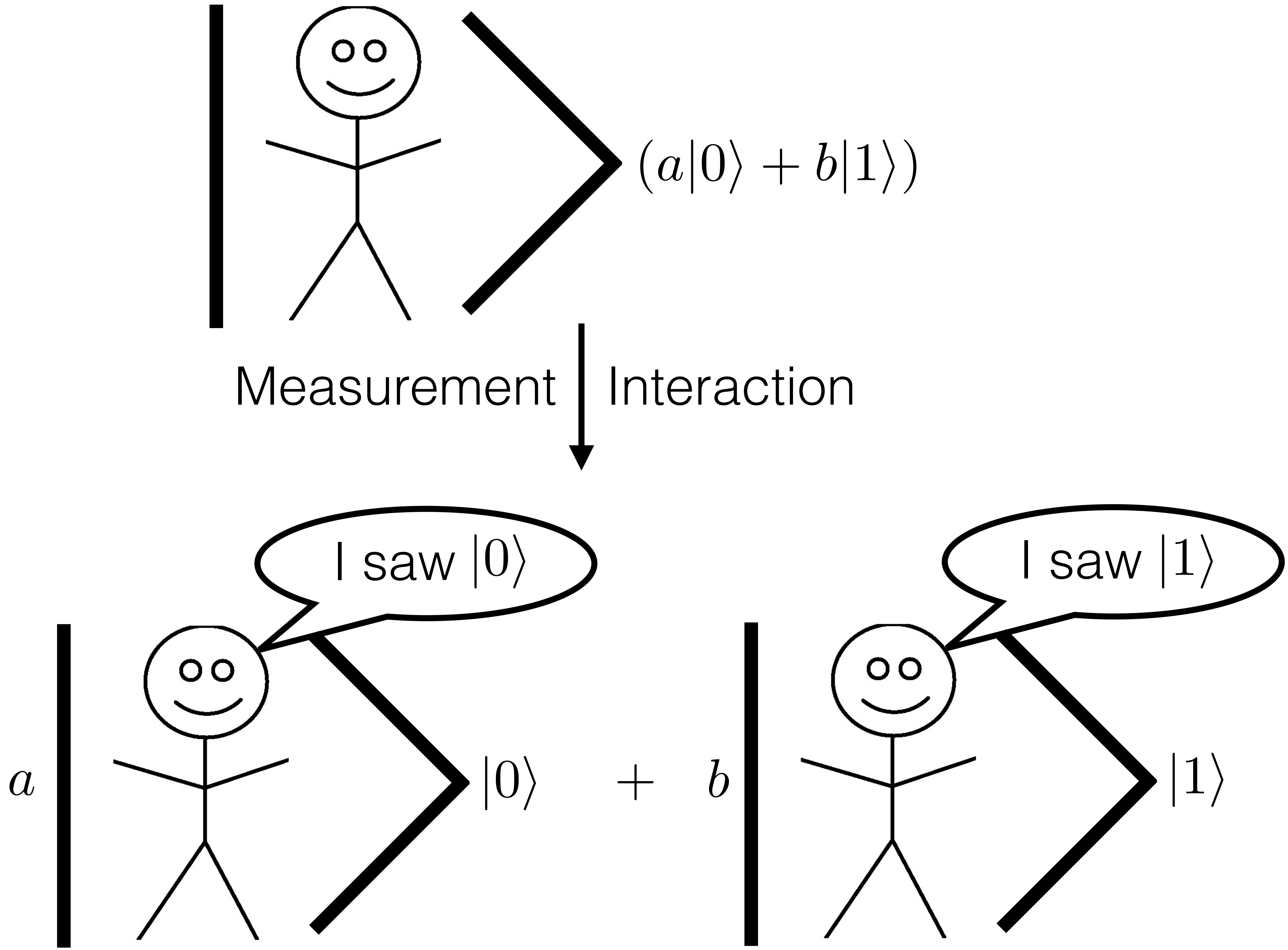
Measuring the qubit means interacting with it

Understanding decoherence



$|\psi\rangle$

Understanding decoherence



Understanding decoherence

This leads to the many-worlds interpretation of QM
but we won't talk about that :)

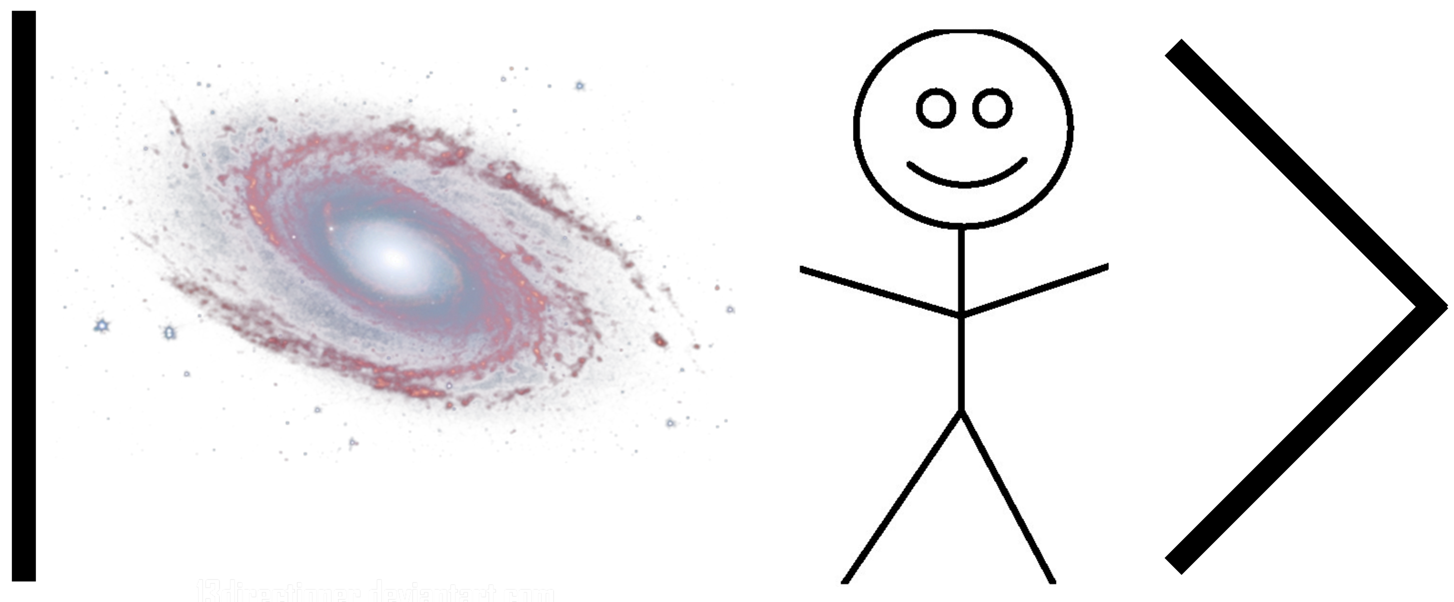
In reality our starting state is more like

$|\psi\rangle$

Environment User Quantum system

Understanding decoherence

Actually it's more like this…



$|\psi\rangle$

Because we are part of the environment
(correlated with it)

But it's easier to imagine things divided into 3 systems

$$|E\rangle|Me\rangle|\psi\rangle$$

Understanding decoherence

$$|Me\rangle|\psi\rangle|E\rangle$$

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

Decoherence is essentially the environment measuring my state

$$|Me\rangle(a|0\rangle + b|1\rangle)|E\rangle \rightarrow |Me\rangle(a|0\rangle|E_0\rangle + b|1\rangle|E_1\rangle)$$

Imagine a stray gamma ray from space entering an ion trap

The gamma photon can become entangled with the ion

Understanding decoherence

Measuring this $|\psi\rangle = a|0\rangle + b|1\rangle$

Is different from measuring the first qubit of

$$a|0\rangle|E_0\rangle + b|1\rangle|E_1\rangle$$

As an example, take

$$|\psi\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Vs

$$\frac{1}{\sqrt{2}}(|0\rangle_\psi|0\rangle_E + |1\rangle_\psi|1\rangle_E)$$

Understanding decoherence

$$|\psi\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Vs

$$\frac{1}{\sqrt{2}}(|0\rangle_\psi |0\rangle_E + |1\rangle_\psi |1\rangle_E)$$

In the first case, if I measure in $(|+\rangle, |-\rangle)$

I will get + with probability 1

But in the second case, we know that we can rewrite the state as

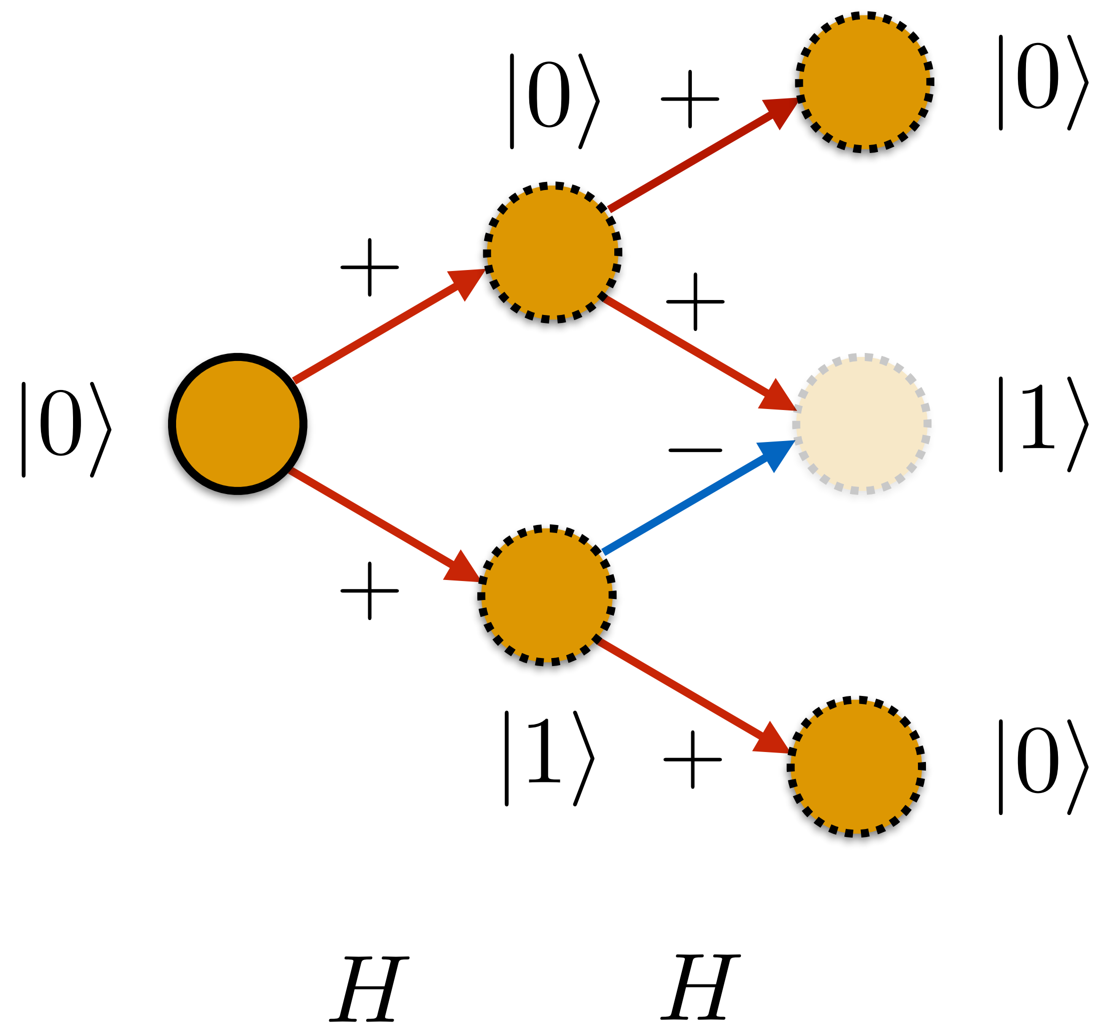
$$\frac{1}{\sqrt{2}}(|+\rangle_\psi |+\rangle_E + |-\rangle_\psi |-\rangle_E)$$

50% probability!

Understanding decoherence

Entangling with an external system destroys interference

$$|0\rangle \rightarrow_H \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \rightarrow_H |0\rangle$$



Understanding decoherence

Entangling with an external system destroys interference

$$|E\rangle|0\rangle \rightarrow_H |E\rangle\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \rightarrow_{ent} \frac{1}{\sqrt{2}}(|E_0\rangle|0\rangle + |E_1\rangle|1\rangle)$$

$$\rightarrow_H \frac{1}{\sqrt{2}}(|E_0\rangle|+\rangle + |E_1\rangle|-\rangle) = \frac{1}{\sqrt{2}}(|E_0'\rangle|0\rangle + |E_1'\rangle|1\rangle)$$

50% chance of seeing 0

No interference!

This again explains why we don't see quantum interference with everyday objects

Understanding decoherence

Some good news as well

Decoherence is typically a gradual process

Decoherence time is (roughly) how long it takes for the state to become maximally entangled with the environment

We can also disentangle things from the environment

How?

Let’s look at a very silly example

Understanding decoherence

$$|Me\rangle(a|0\rangle + b|1\rangle)|E\rangle \longrightarrow |Me\rangle(a|0\rangle|E_0\rangle + b|1\rangle|E_1\rangle)$$

Suppose I measure in computational basis

$$(a|Me_0\rangle|0\rangle|E_0\rangle + b|Me_1\rangle|1\rangle|E_1\rangle)$$

If I see 0 do nothing; if I see 1 flip it!

$$(a|Me_0\rangle|E_0\rangle + b|Me_1\rangle|E_1\rangle)|0\rangle$$

I've made a qubit that is disentangled from both me and the environment

Of course, we've lost the original information so this isn't very useful (except for initialising system)

Understanding decoherence

While this entangling view of decoherence tells us why it happens, it's not very useful "practically"

Can be shown that it's equivalent to

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

Decoherence $\Big\downarrow$ Interaction with environment

25%	25%	25%	25%
$\|\psi\rangle$	$X\|\psi\rangle$	$Z\|\psi\rangle$	$XZ\|\psi\rangle$

Understanding decoherence

While this entangling view of decoherence tells us why it happens, it's not very useful "practically"

Can be shown that it's equivalent to

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

Decoherence ↓ Interaction with environment

$(1-p)$	$p/3$	$p/3$	$p/3$
$\|\psi\rangle$	$X\|\psi\rangle$	$Z\|\psi\rangle$	$XZ\|\psi\rangle$

Fault tolerance

$|\psi\rangle$ $X|\psi\rangle$ $Z|\psi\rangle$ $XZ|\psi\rangle$

Our goal will be to detect when an error happens
(quantum error detection)

We also want to know what type of error, to undo it
(quantum error correction)

Is this even possible?

Quantum threshold theorem

If $p \leq p_{th}$ there exists a procedure for fault tolerant QC

Time for some error correction, but first…

Measurements

$$O$$

Possible measurement outcomes

$$\lambda_1 \longrightarrow |v_1\rangle$$
$$\lambda_2 \longrightarrow |v_2\rangle$$
$$\lambda_3 \longrightarrow |v_3\rangle$$
$$\lambda_4 \longrightarrow |v_4\rangle$$
$$\vdots$$
$$\lambda_n \longrightarrow |v_n\rangle$$

State after measurement

Real numbers

Orthonormal vectors

What if $\lambda_1 = \lambda_2$?

Measurements

$$O$$

Possible measurement outcomes

$$\lambda_1 \longrightarrow span(|v_1\rangle, |v_2\rangle)$$

$$\lambda_3 \longrightarrow |v_3\rangle$$

$$\lambda_4 \longrightarrow |v_4\rangle$$

$$\vdots$$

$$\lambda_n \longrightarrow |v_n\rangle$$

State after measurement

Real numbers

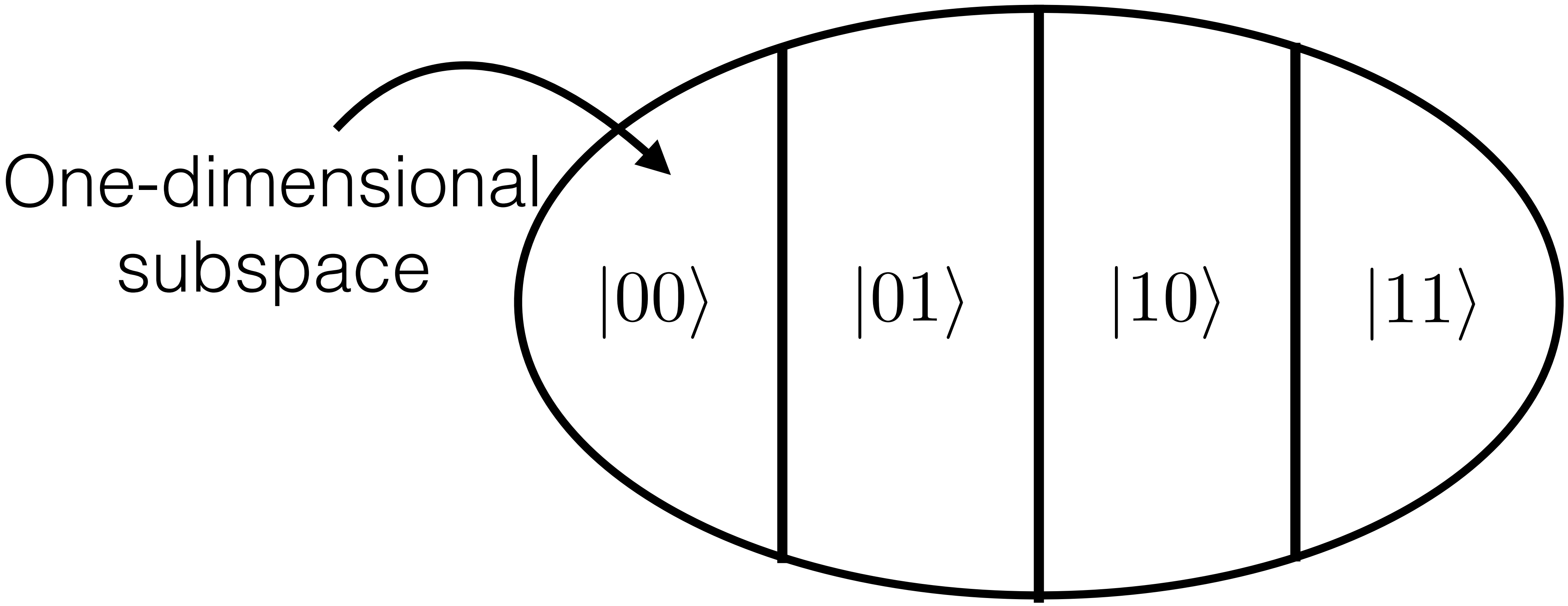
Orthonormal vectors

What if $\lambda_1 = \lambda_2$?

Measurements

A 2-qubit example

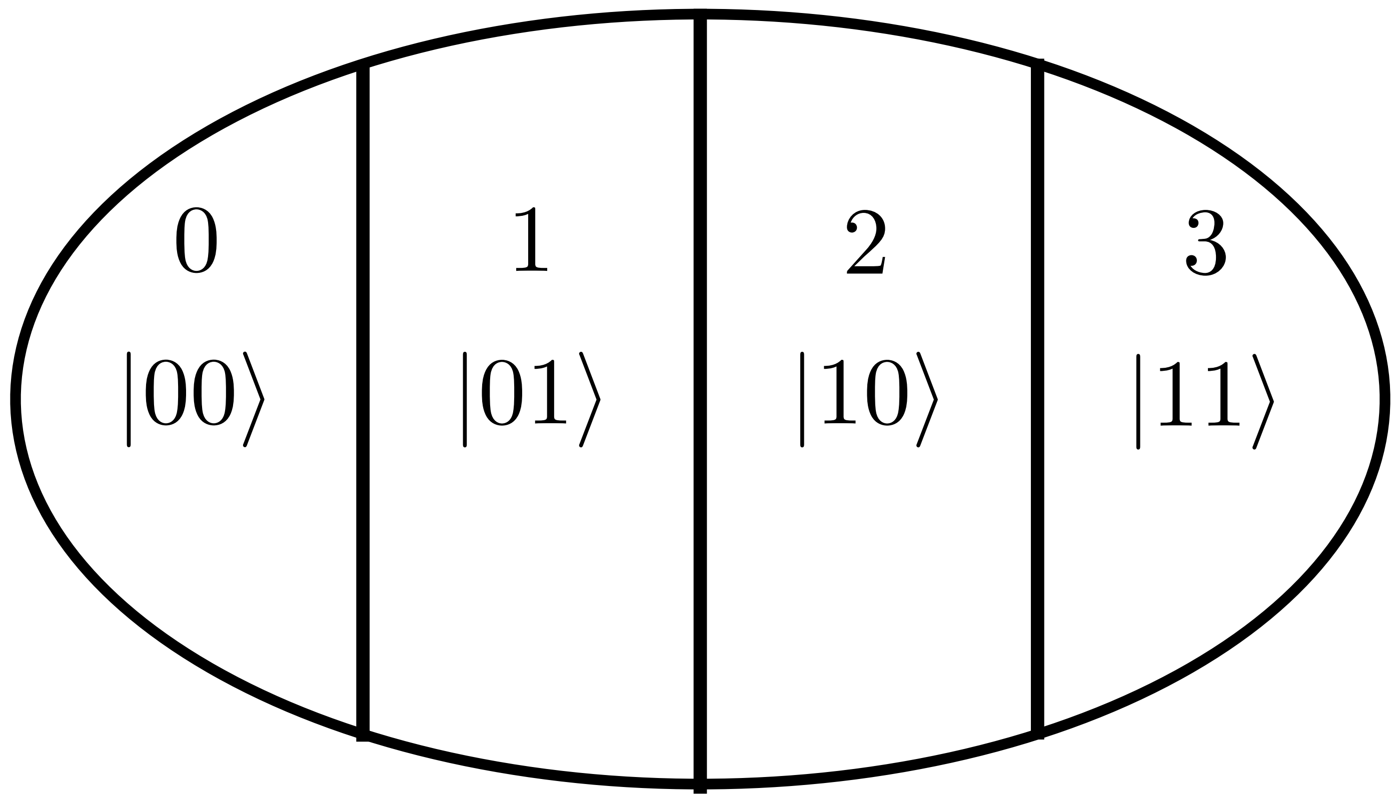
Consider the 4-dimensional space



Measurements

A 2-qubit example

Consider the 4-dimensional space



Eigenvalues: $0, 1, 2, 3$

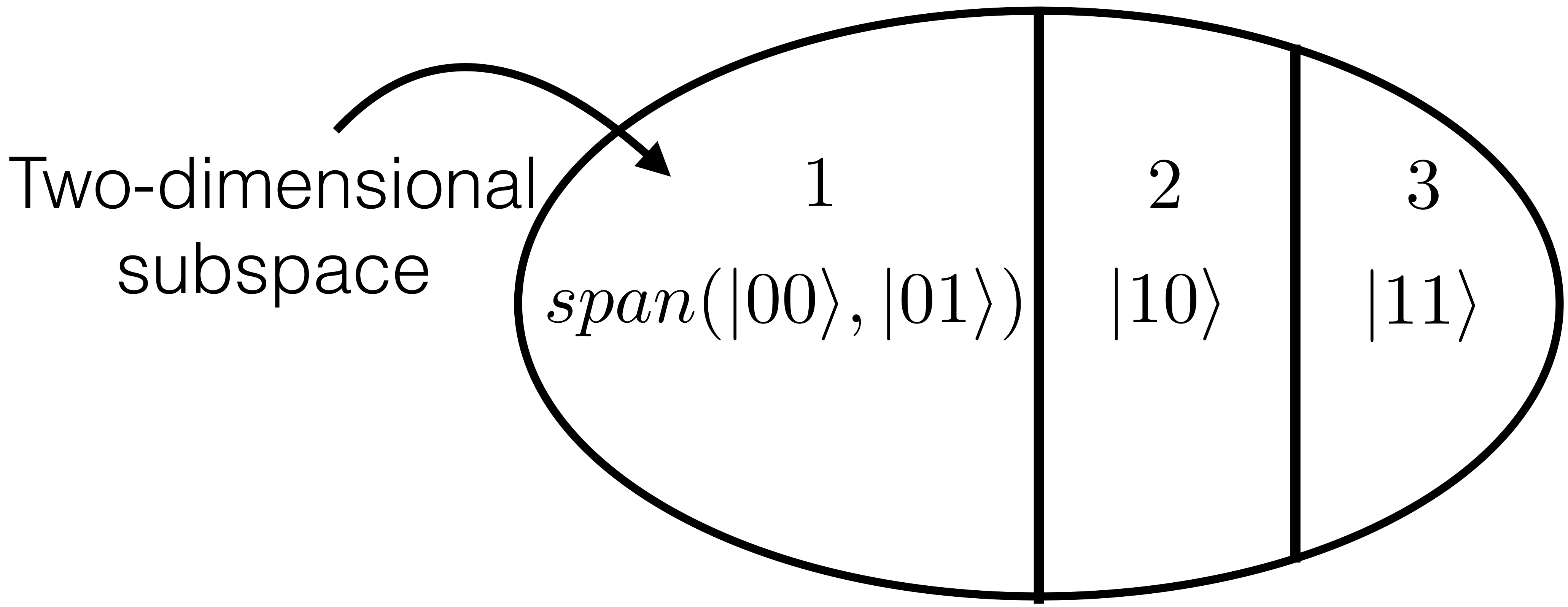
Eigenvectors: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$

Now suppose first 2 eigenvalues are the same

Measurements

A 2-qubit example

Consider the 4-dimensional space



Eigenvalues: $1, 2, 3$

Eigenvectors: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$

Now suppose first 2 eigenvalues are the same

Measurements

So if I were to measure the state

$$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

I would get outcome 1 with probability

$$|a|^2 + |b|^2$$

And my new state would be

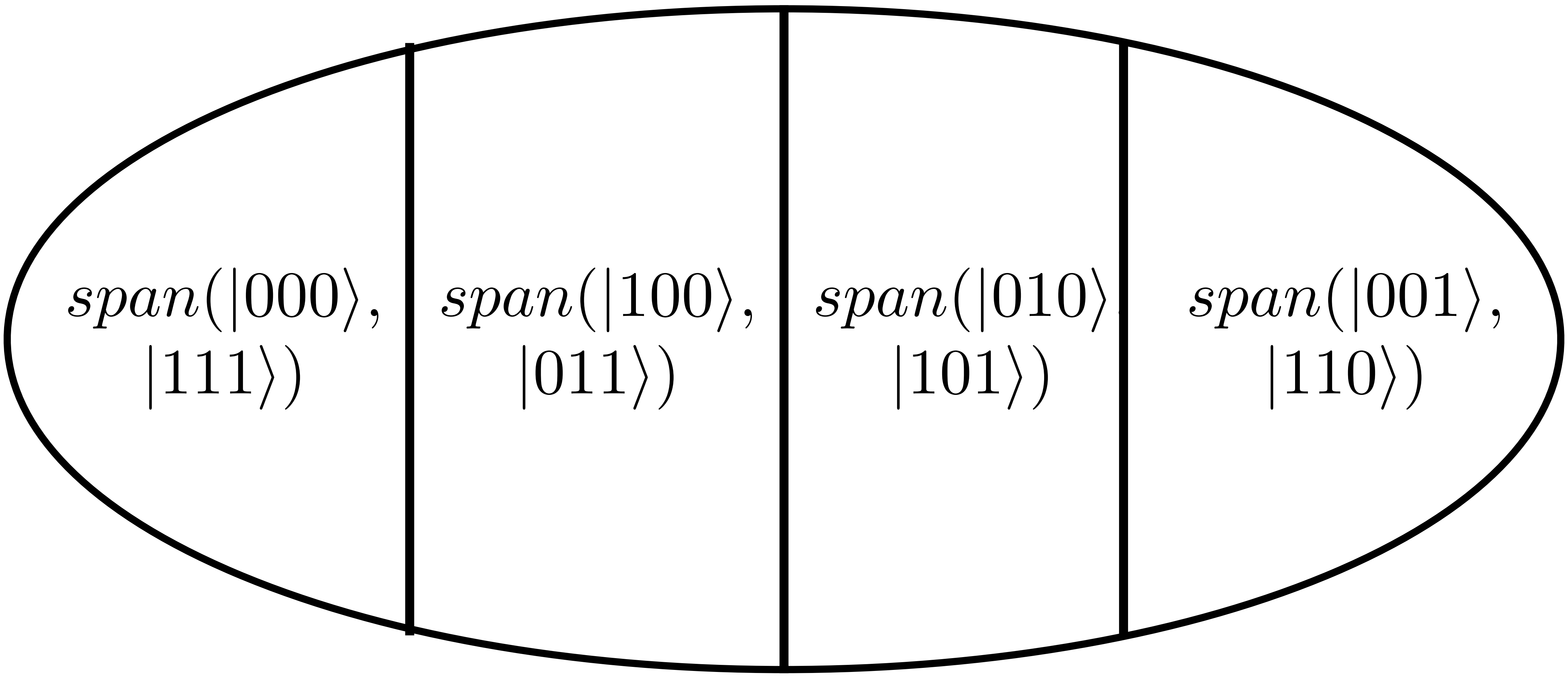
$$\frac{1}{\sqrt{|a|^2 + |b|^2}}(a|00\rangle + b|01\rangle)$$

Had I started with $\alpha|00\rangle + \beta|01\rangle$

The measurement will **always** give outcome 1 and the state remains unchanged

Our first error correcting code

Now let's divide the 8-dimensional space of 3 qubits



All of these subspaces are 2-dimensional

What lives in a 2-dimensional subspace?

Our first error correcting code

The logical qubit

$$|\psi\rangle = a|000\rangle + b|111\rangle$$

$$X \otimes I \otimes I|\psi\rangle = a|100\rangle + b|011\rangle$$

$$I \otimes X \otimes I|\psi\rangle = a|010\rangle + b|101\rangle$$

$$I \otimes I \otimes X|\psi\rangle = a|001\rangle + b|110\rangle$$

If we perform the measurement on the previous slide
we can detect an X error on a quantum state!

Bit flip code

Our first error correcting code

The logical qubit

$$|\psi\rangle = a|000\rangle + b|111\rangle$$

We write it like this

$$|\psi\rangle_L = a|0\rangle_L + b|1\rangle_L$$

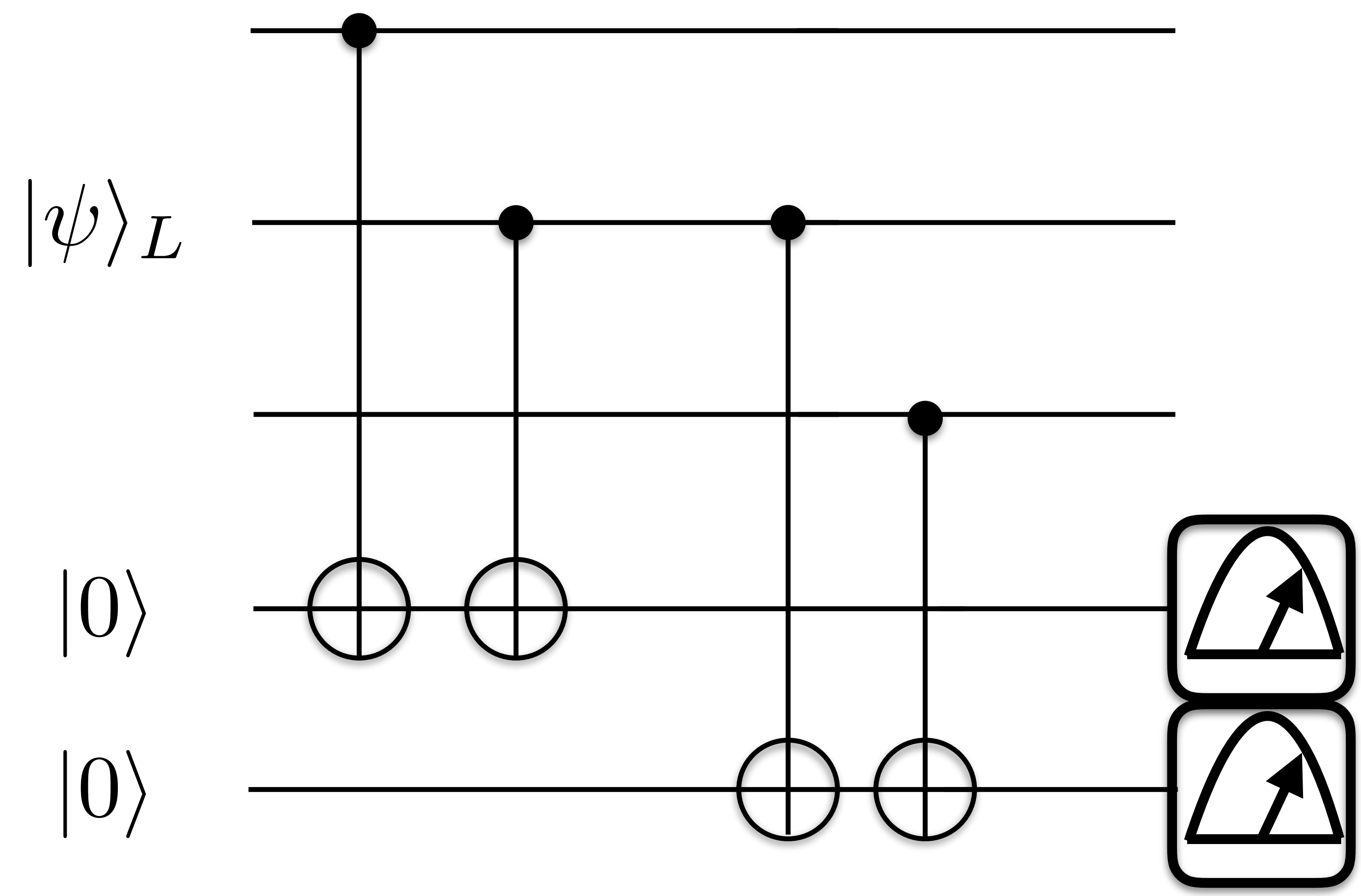
$$|0\rangle_L = |000\rangle \qquad |1\rangle_L = |111\rangle$$

Idea of error correction:
work in a small subspace of a larger space

Every now and then check to see
if you are still in that subspace

Our first error correcting code

How do we do that funky measurement?



These are called **syndrome measurements**

In reality the measurement is slightly more complicated but not by much :)

Our first error correcting code

What if we have 2 flip errors?

Say the probability flipping one particular qubit is p

(we'll assume errors are independent)

The probability of one qubit being flipped is at most $3p$

The probability of at least 2 qubits being flipped is at most

$$3p^2 + p^3$$

$$O(p) \xrightarrow[\text{correction}]{\text{Error}} O(p^2)$$

As long as $p \leq p_{th}$ this will be decreasing

Our first error correcting code

The logical state

$$|\psi\rangle_L = a|0\rangle_L + b|1\rangle_L$$

is also called encoded state

Imagine encoding this in a code as well!

$$|\phi\rangle_L = a|0\rangle_L|0\rangle_L|0\rangle_L + b|1\rangle_L|1\rangle_L|1\rangle_L$$

$$O(p) \to O(p^2) \to O(p^4)$$

Concatenation

If we repeat this a small number of times, the error becomes negligible

Other codes

$$|\psi\rangle_L = a|+++\rangle + b|---\rangle$$

This code can correct single-qubit Z errors

Take each qubit of this state and encode it in the bit-flip code from before

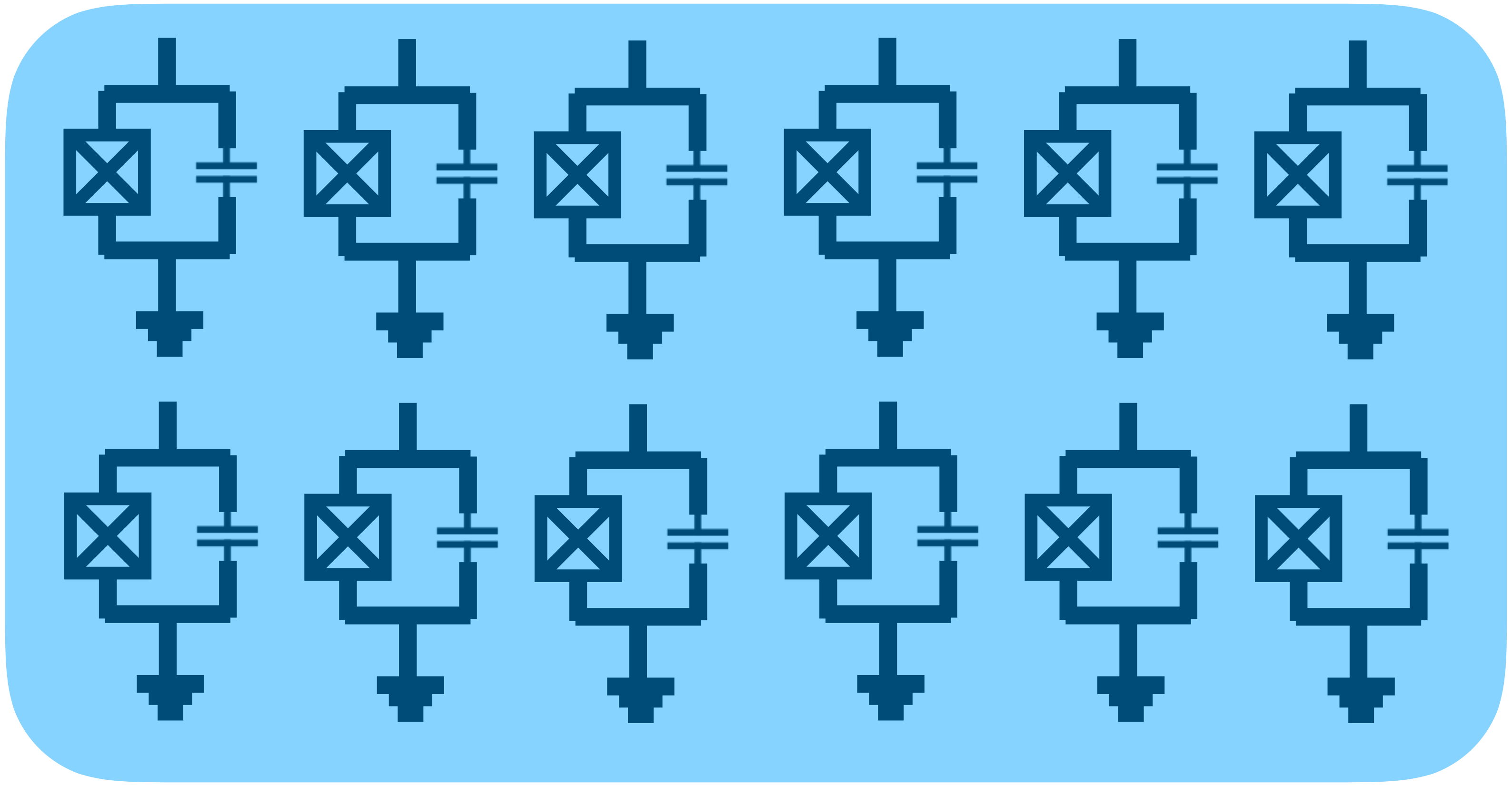
We will get a 9-qubit code that can correct for both X and Z errors

Can be shown that this is enough to detect any single-qubit error

Shor’s code

Fault tolerance in a nutshell

Use lots of physical qubits to encode fewer logical qubits



$|\psi\rangle_L$

Perform periodic syndrome measurements to detect errors

Apply appropriate correction procedures

Continue with quantum computation

Repeat

Thresholds

Thresholds depend a lot on assumptions about the error model

For a fairly typical error model
(independent depolarising noise errors)

Surface code

$$0.6\% - 1\%$$

However…

It requires 1000-10.000 physical qubits per logical qubit

Thresholds

Better thresholds for different noise models

If Z errors are 10 times more likely than other errors

$$28.2\%$$

But we still need large numbers of good qubits

Quality and quantity

Research into quantum error correction is ongoing,
we might find better codes

How many physical qubits to run Shor for 512-bit numbers?

This will be a very rough estimate :)

We saw that to factor an N-bit number, we need 2N qubits

$$\sum_x |x\rangle |f(x)\rangle$$

These should be logical qubits

Let's say 1000 physical qubits per logical qubit

Around one million physical qubits


ONE MILLION QUBITS

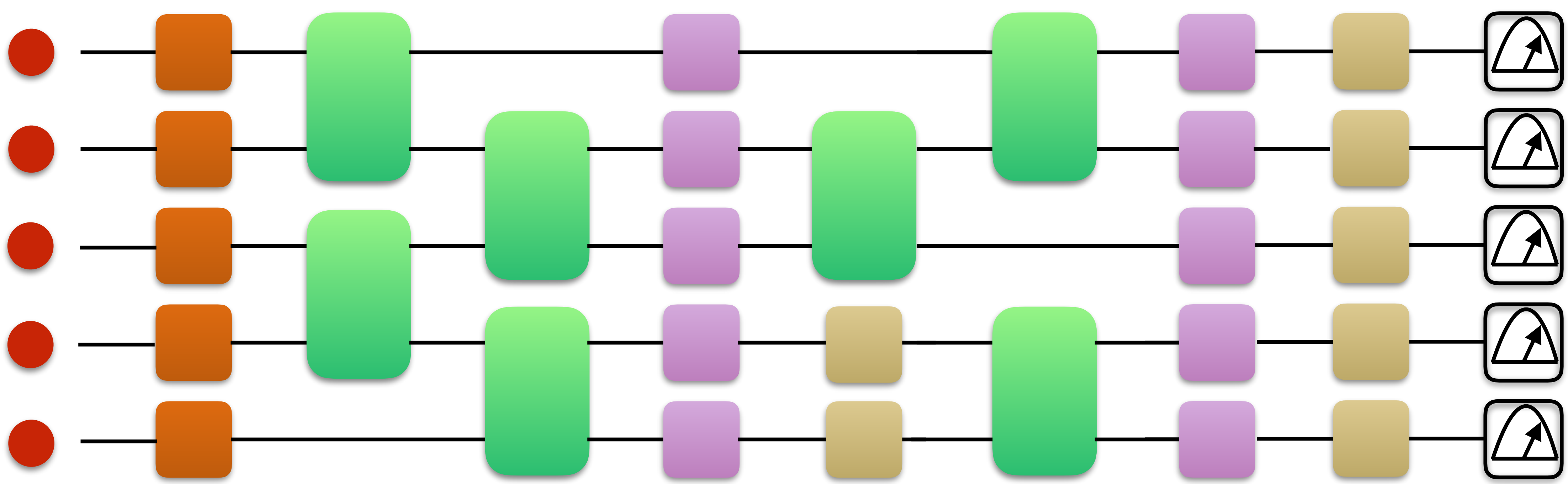

The Future
NEXT EXIT

Quantum computational supremacy

Solving a problem on a QC in less time than on the best classical computers with the best algorithms

Sampling problems

Random circuit sampling

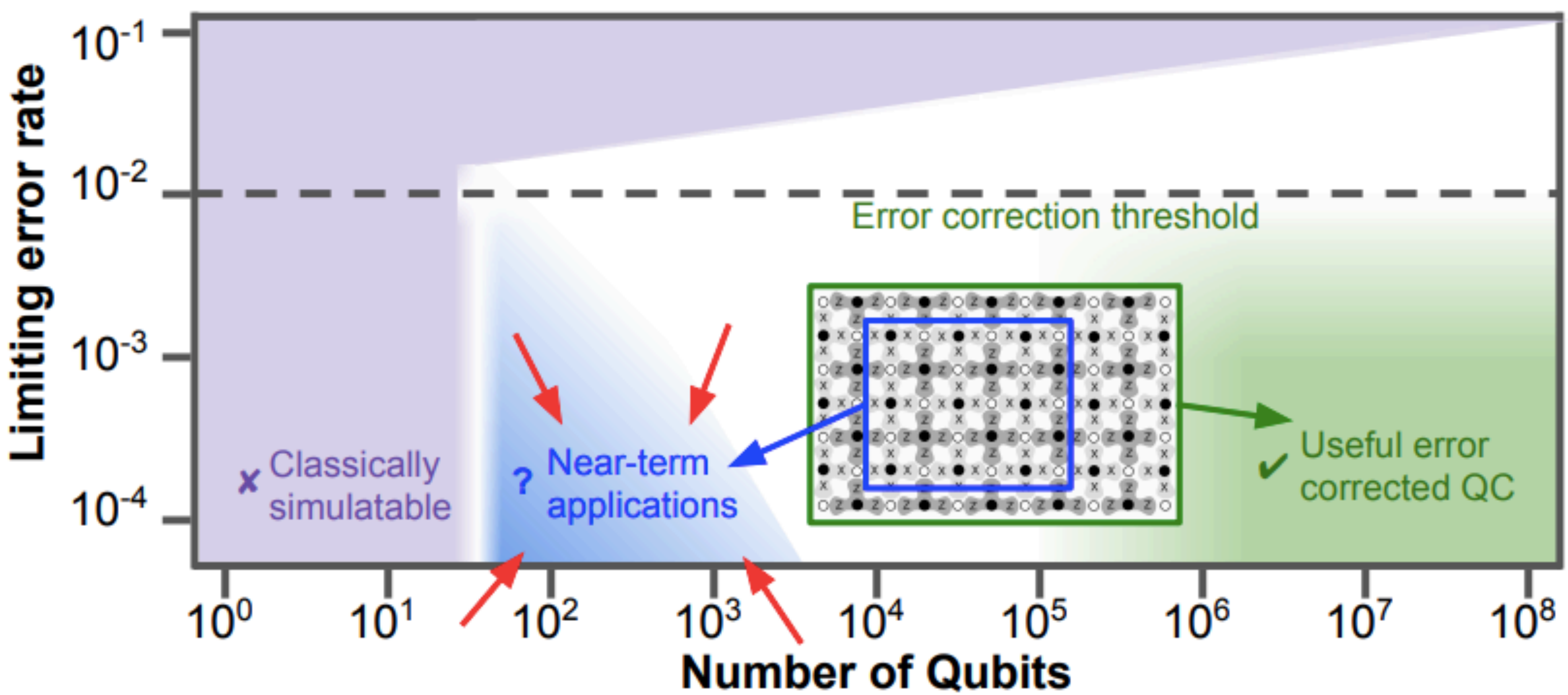


Complexity theoretic arguments for hardness

Quantum computational supremacy

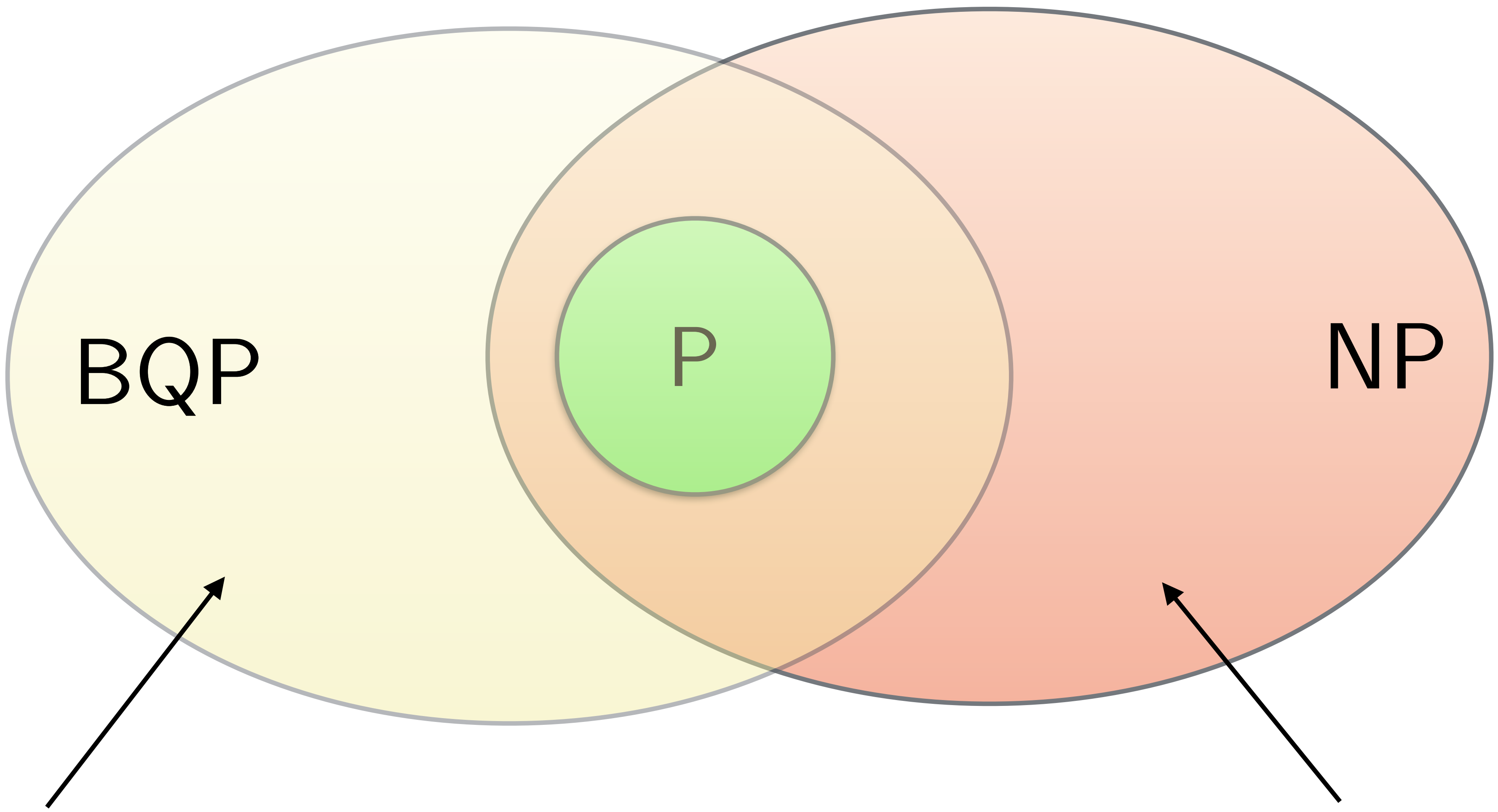
Might not require fault tolerance

You just need ~100 qubits and long enough coherence times and low enough errors to do (say) 10.000 gates



Verification of quantum computation

How do we verify the correctness of quantum computations?

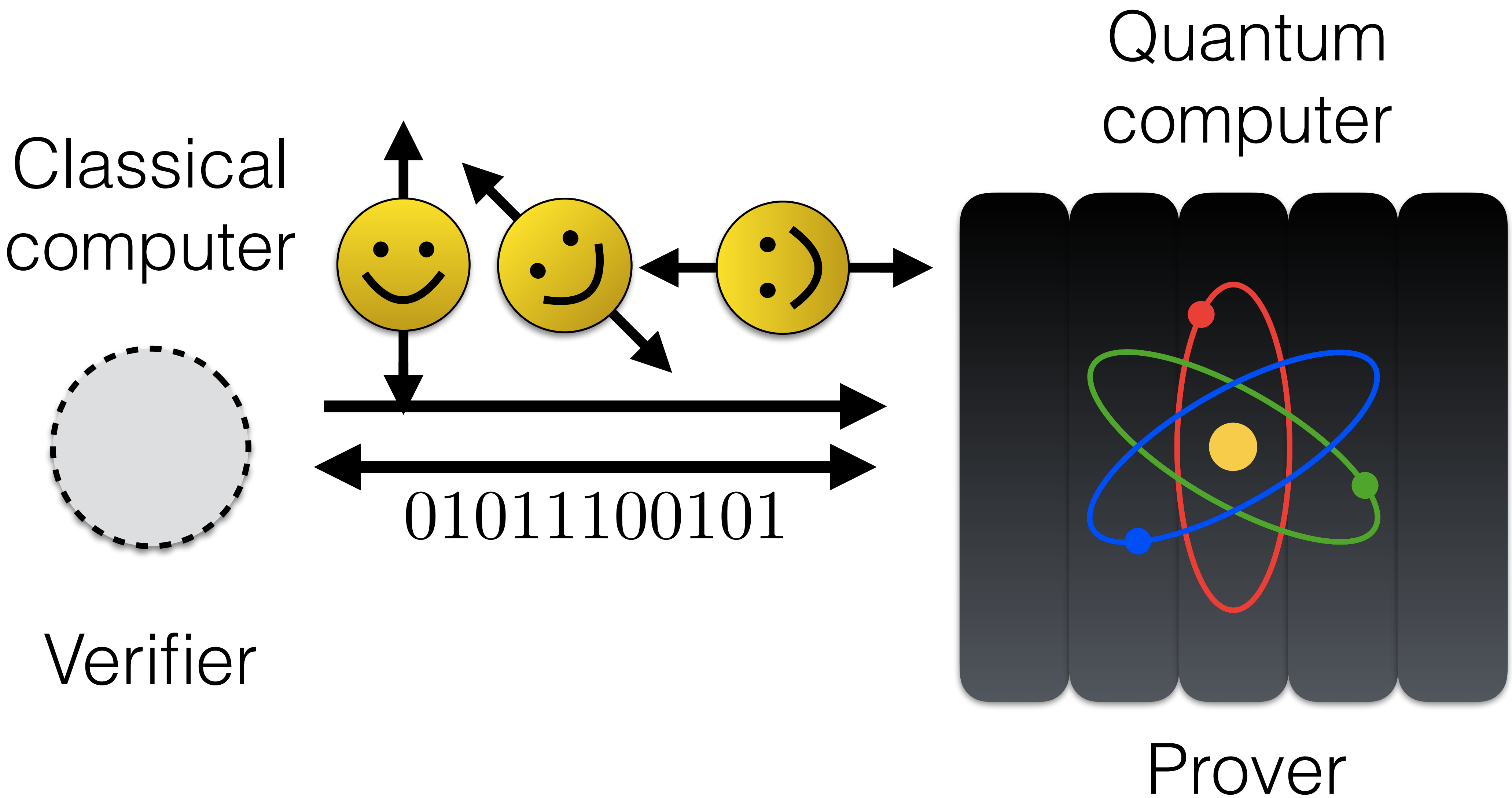


Efficiently computable on quantum computer

Efficiently verifiable solutions

Verification of quantum computation

How do we verify the correctness of quantum computations?



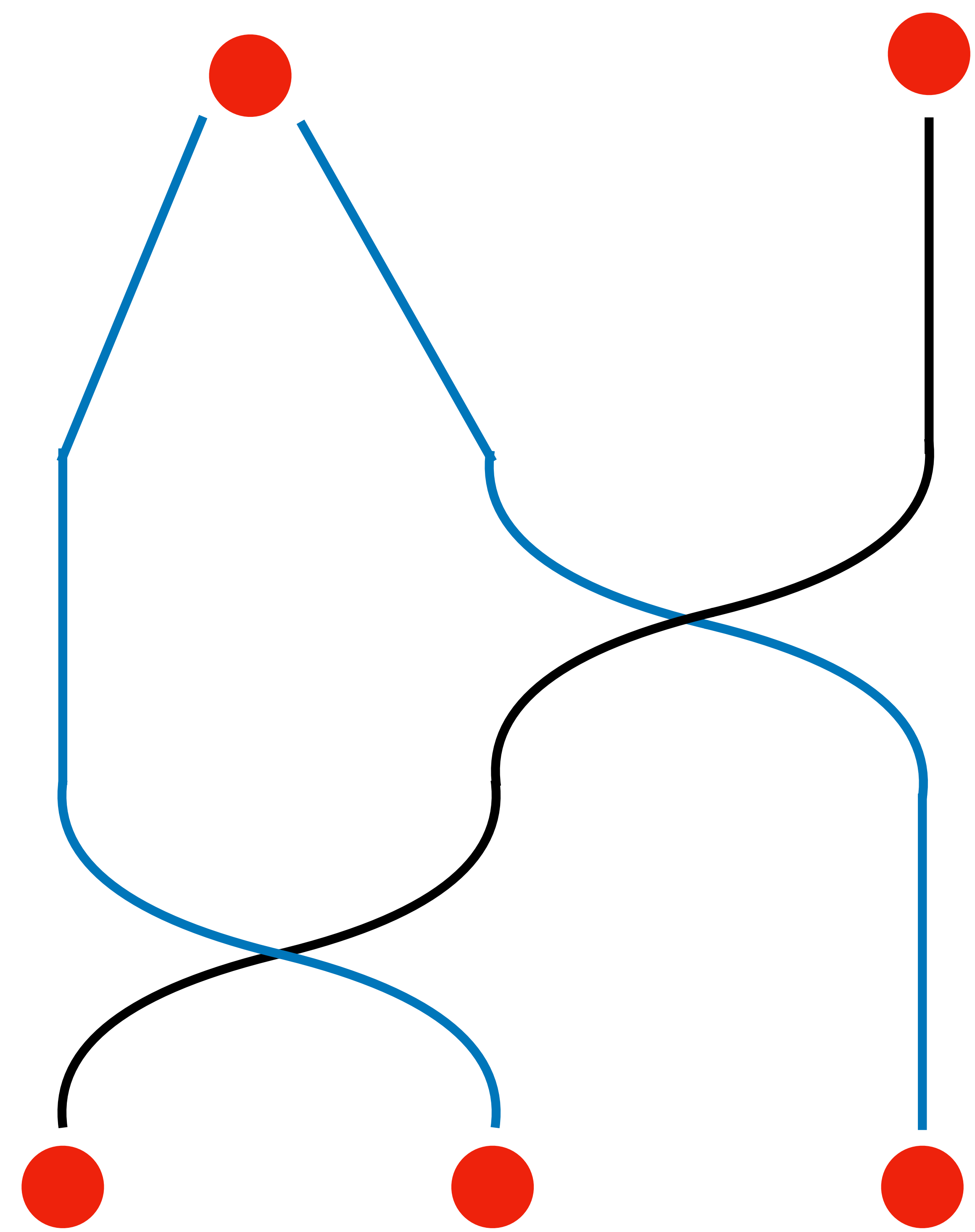
https://arxiv.org/abs/1709.06984

Topological quantum computing

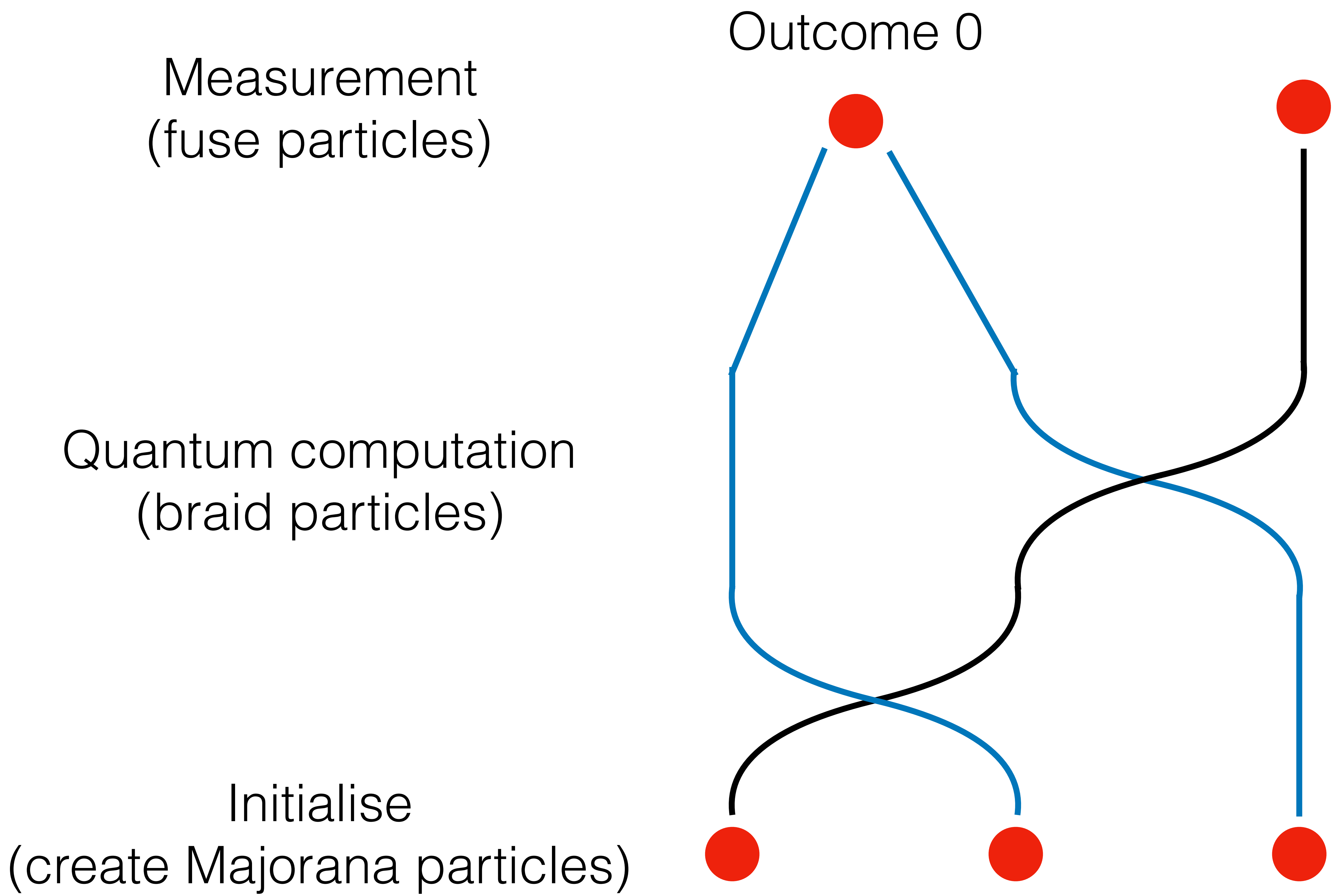
Measurement
(fuse particles)

Quantum computation
(braid particles)

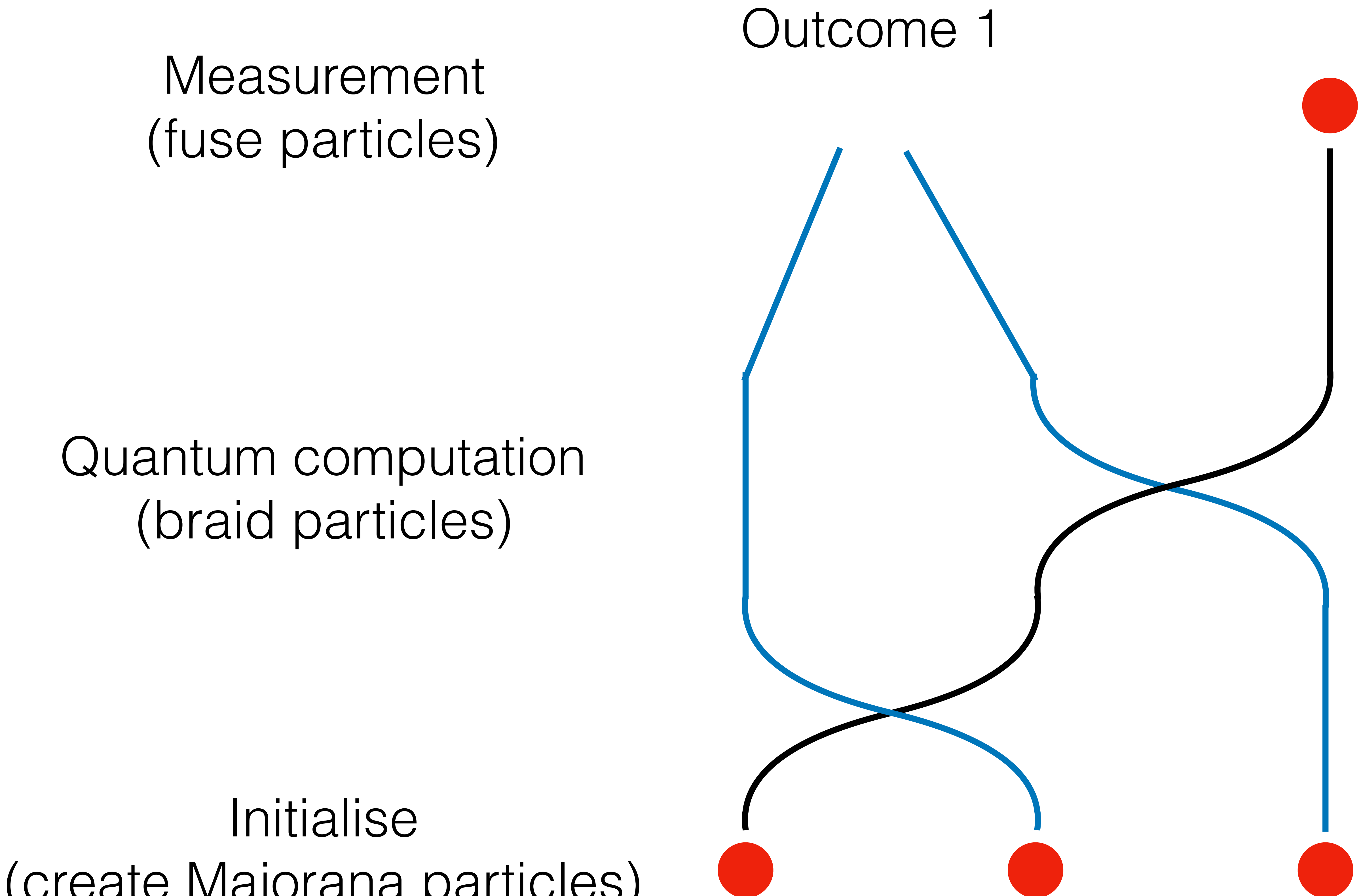
Initialise
(create Majorana particles)



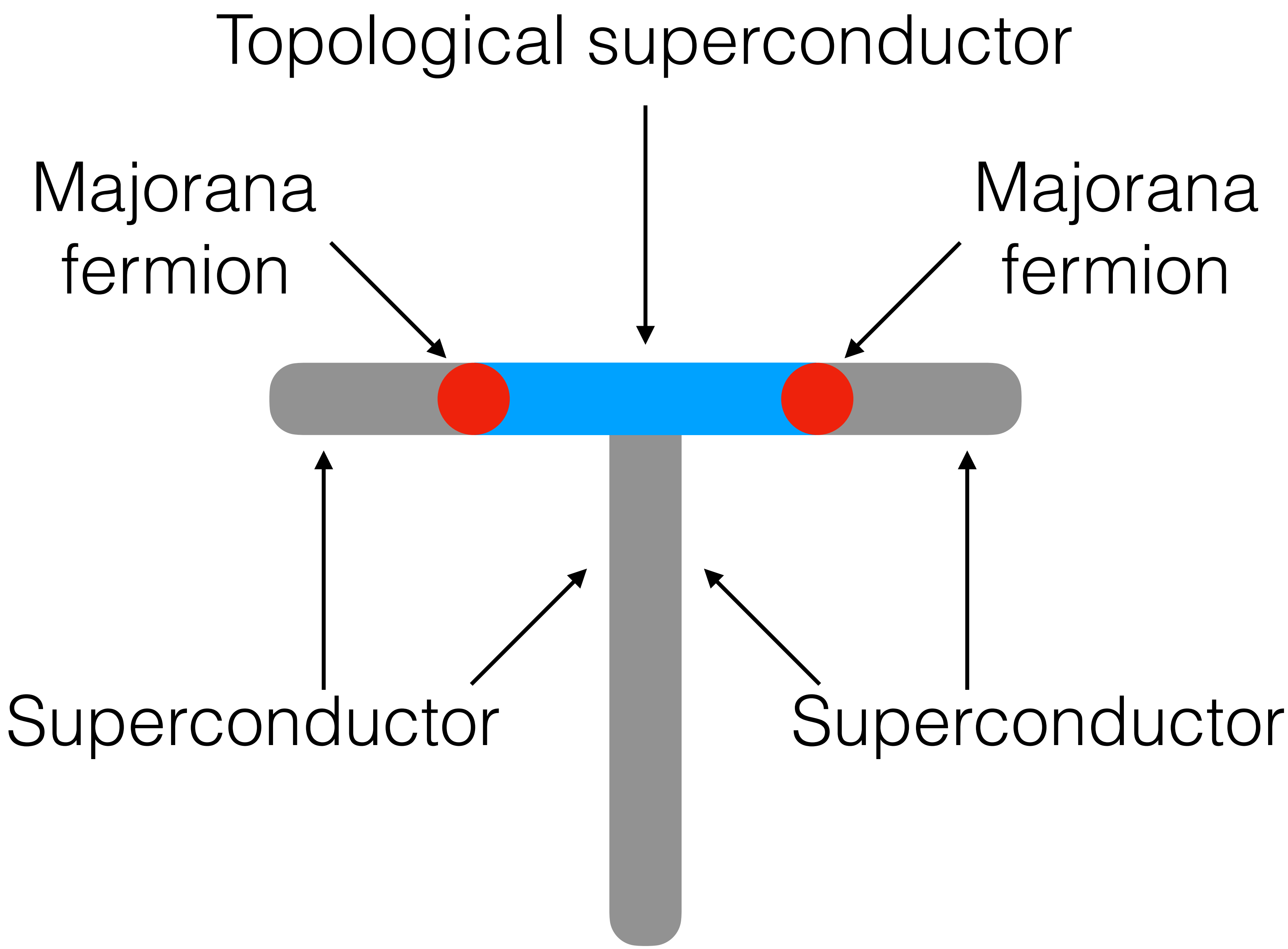
Topological quantum computing



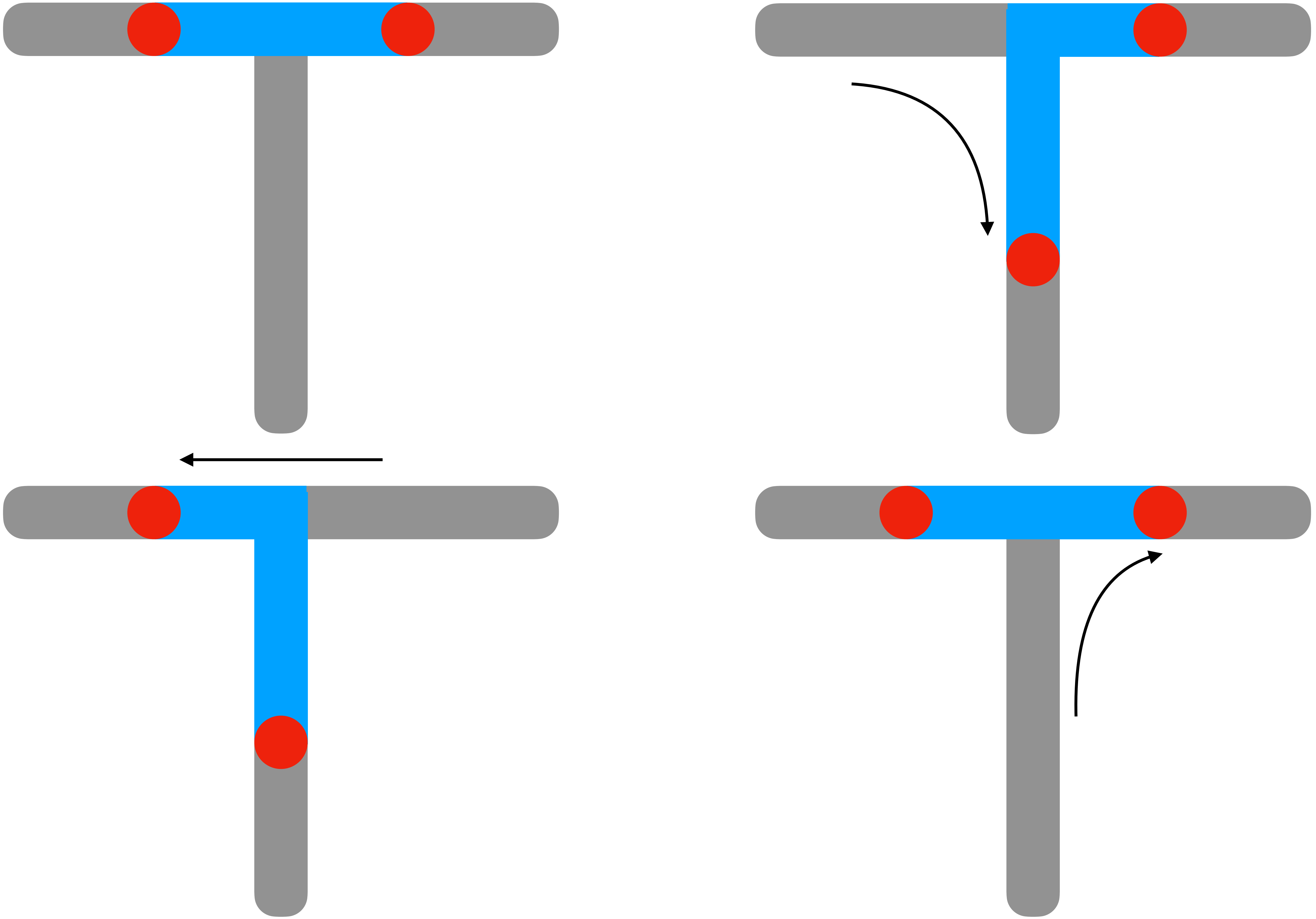
Topological quantum computing



Topological quantum computing



Topological quantum computing



What if quantum computing doesn't pan out?

The theory of QC is still relevant

Theoretical physics

GR **QM**

Quantum information ⇣ Quantum error-correcting codes

Quantum Gravity

Recommender systems

Efficient quantum algorithm

↓ *De-quantising*

Efficient classical algorithm

My own thoughts and predictions

I think there will be large scale quantum computers
in my lifetime

But I'm a theorist, so to me it's interesting either way :)

Quantum computational supremacy
My prediction: 2-3 years

Large scale QC (factoring 512-bit numbers)
My prediction: 25-30 years

Likely many interesting developments along the way

References and resources

Fault-tolerant quantum computation

http://www.theory.caltech.edu/people/preskill/ph229/notes/chap7.pdf

https://cs.uwaterloo.ca/~watrous/LectureNotes/CPSC519.Winter2006/16.pdf

https://arxiv.org/pdf/quant-ph/9712048.pdf

https://arxiv.org/pdf/0904.2557.pdf

http://www.theory.caltech.edu/~preskill/talks/preskill-QISWorkshop2009.pdf

Section 10 of Nielsen & Chuang

Quantum threshold theorem

https://arxiv.org/pdf/quant-ph/9906129.pdf

https://arxiv.org/pdf/quant-ph/9705052.pdf

References and resources

Road towards fault tolerant QC

https://www.nature.com/articles/nature23460

https://www.nqit.ox.ac.uk/sites/www.nqit.ox.ac.uk/files/2016-11/NQIT%20Technical%20Roadmap.pdf

Surface codes

https://arxiv.org/pdf/1208.0928.pdf

https://arxiv.org/pdf/1708.08474.pdf

Quantum computational supremacy and random circuit sampling

https://arxiv.org/pdf/1011.3245.pdf

https://www.nature.com/articles/nature23458

https://www.scottaaronson.com/papers/quantumsupre.pdf

https://arxiv.org/pdf/1803.04402.pdf

References and resources

Images on slides 34, 35, 37

https://i.imgur.com/U0F0vK4.jpg

https://northstar.church/wp-content/uploads/2017/11/The-Future-Is-Bright.jpg

https://www.nextbigfuture.com/wp-content/uploads/2018/04/edfa031bcd997a0f9299d58b4054a49e.png

https://www.youtube.com/watch?v=nycwc-wXuuw&feature=youtu.be

Verification of quantum computation

https://arxiv.org/pdf/1709.06984.pdf

http://swarm.cs.pub.ro/~agheorghiu/thesis/thesis.pdf

https://arxiv.org/pdf/1804.01082.pdf

https://www.youtube.com/watch?v=RQGW4KcLMIQ

References and resources

Topological QC and inspiration for slides 42,43,44

https://www.youtube.com/watch?v=igPXzKjqrNg
https://arxiv.org/pdf/1705.04103.pdf
http://www.theory.caltech.edu/~preskill/ph219/topological.pdf
https://arxiv.org/pdf/0904.2771.pdf
https://arxiv.org/pdf/quant-ph/0101025.pdf

Quantum gravity and quantum information

https://www.perimeterinstitute.ca/it-qubit-summer-school/it-qubit-summer-school-resources

De-quantising recommender systems

https://www.scottaaronson.com/blog/?p=3880