Quantum Computation and Cryptography
Day 8

Alexandru Gheorghiu

The University of Edinburgh

Part II
Where are the quantum computers?

Physical implementations

Physical implementations

- Electrons $\rightarrow$ Stern-Gerlach apparatus, quantum dots

Physical implementations

- Electrons $\rightarrow$ Stern-Gerlach apparatus, quantum dots
- Photons $\rightarrow$ linear and non-linear optics

Physical implementations

- Electrons $\rightarrow$ Stern-Gerlach apparatus, quantum dots
- Photons $\rightarrow$ linear and non-linear optics
- Atoms and molecules $\rightarrow$ NMR, ion traps

Physical implementations

- Electrons $\rightarrow$ Stern-Gerlach apparatus, quantum dots
- Photons $\rightarrow$ linear and non-linear optics
- Atoms and molecules $\rightarrow$ NMR, ion traps
- Superconductors $\rightarrow$ Josephson junctions, SQUIDS

Physical implementations

- Electrons $\rightarrow$ Stern-Gerlach apparatus, quantum dots
- Photons $\rightarrow$ linear and non-linear optics
- Atoms and molecules $\rightarrow$ NMR, ion traps
- Superconductors $\rightarrow$ Josephson junctions, SQUIDS
- And others

Physical implementations

- Electrons $\rightarrow$ Stern-Gerlach apparatus, quantum dots
- Photons $\rightarrow$ linear and non-linear optics
- Atoms and molecules $\rightarrow$ NMR, ion traps
- Superconductors $\rightarrow$ Josephson junctions, SQUIDS
- And others

So what's the problem? Why can't we scale these implementations?

The problem

The problem

Everything else

The problem

Everything else ... i.e. **the environment**

The problem

Everything else ... i.e. **the environment**

Quantum mechanics describes everything:
the quantum computer + the environment

The problem

Everything else ... i.e. **the environment**

Quantum mechanics describes everything:
the quantum computer + the environment

And since the computer is in the environment, it interacts with it!

The problem

Everything else ... i.e. **the environment**

Quantum mechanics describes everything:
the quantum computer + the environment

And since the computer is in the environment, it interacts with it!

The interaction is hard to control and can affect the computation

The problem

Everything else ... i.e. **the environment**

Quantum mechanics describes everything:
the quantum computer + the environment

And since the computer is in the environment, it interacts with it!

The interaction is hard to control and can affect the computation

How?

Decoherence

Decoherence

Say we have $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Decoherence

Say we have $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Say the environment is in a state $|E\rangle$

Decoherence

Say we have $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Say the environment is in a state $|E\rangle$

So our whole system (computer + environment) is:
$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |E\rangle$

Decoherence

Say we have $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Say the environment is in a state $|E\rangle$

So our whole system (computer + environment) is:
$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |E\rangle$

After a short time the environment interacts with the qubit

Decoherence

Say we have $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Say the environment is in a state $|E\rangle$

So our whole system (computer + environment) is:
$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |E\rangle$

After a short time the environment interacts with the qubit

I.e. it becomes correlated with the qubit, or entangled

Decoherence

Say we have $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Say the environment is in a state $|E\rangle$

So our whole system (computer + environment) is:
$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |E\rangle$

After a short time the environment interacts with the qubit

I.e. it becomes correlated with the qubit, or entangled

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |E\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle |E_1\rangle + |1\rangle |E_2\rangle)$$

Decoherence

Say we have $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Say the environment is in a state $|E\rangle$

So our whole system (computer + environment) is:
$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |E\rangle$

After a short time the environment interacts with the qubit

I.e. it becomes correlated with the qubit, or entangled

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |E\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle |E_1\rangle + |1\rangle |E_2\rangle)$$

Measuring initial qubit in $(|+\rangle, |-\rangle)$ basis always yielded $|+\rangle$

Decoherence

Say we have $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Say the environment is in a state $|E\rangle$

So our whole system (computer + environment) is:
$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |E\rangle$

After a short time the environment interacts with the qubit

I.e. it becomes correlated with the qubit, or entangled

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |E\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle |E_1\rangle + |1\rangle |E_2\rangle)$$

Measuring initial qubit in $(|+\rangle, |-\rangle)$ basis always yielded $|+\rangle$

Now, there is some chance that outcome will be $|-\rangle$!

Decoherence

Say we have $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Say the environment is in a state $|E\rangle$

So our whole system (computer + environment) is:
$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |E\rangle$

After a short time the environment interacts with the qubit

I.e. it becomes correlated with the qubit, or entangled

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |E\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle |E_1\rangle + |1\rangle |E_2\rangle)$$

Measuring initial qubit in $(|+\rangle, |-\rangle)$ basis always yielded $|+\rangle$

Now, there is some chance that outcome will be $|-\rangle$!

We say that the qubit has lost coherence, or decohered

Decoherence

Decoherence

Decoherence $\rightarrow$ no interference

Decoherence

Decoherence $\rightarrow$ no interference

No interference $\rightarrow$ everything becomes classical
(from the observer's point of view)

Decoherence

Decoherence $\rightarrow$ no interference

No interference $\rightarrow$ everything becomes classical
(from the observer's point of view)

Isn't the joint state $\frac{1}{\sqrt{2}}(|0\rangle |E_1\rangle + |1\rangle |E_2\rangle)$ still coherent?
Can't we do a joint measurement?

Decoherence

Decoherence $\rightarrow$ no interference

No interference $\rightarrow$ everything becomes classical
(from the observer's point of view)

Isn't the joint state $\frac{1}{\sqrt{2}}(|0\rangle |E_1\rangle + |1\rangle |E_2\rangle)$ still coherent?
Can't we do a joint measurement?

Environment is huge (on order of 10^{23} particles)

Decoherence

Decoherence $\rightarrow$ no interference

No interference $\rightarrow$ everything becomes classical
(from the observer's point of view)

Isn't the joint state $\frac{1}{\sqrt{2}}(|0\rangle |E_1\rangle + |1\rangle |E_2\rangle)$ still coherent?
Can't we do a joint measurement?

Environment is huge (on order of 10^{23} particles)
Environment can contain photons which leave at the speed of light

Decoherence

Decoherence $\rightarrow$ no interference

No interference $\rightarrow$ everything becomes classical
(from the observer's point of view)

Isn't the joint state $\frac{1}{\sqrt{2}}(|0\rangle |E_1\rangle + |1\rangle |E_2\rangle)$ still coherent?
Can't we do a joint measurement?

Environment is huge (on order of 10^{23} particles)
Environment can contain photons which leave at the speed of light
Irreversible change

Decoherence

Decoherence $\rightarrow$ no interference

No interference $\rightarrow$ everything becomes classical
(from the observer's point of view)

Isn't the joint state $\frac{1}{\sqrt{2}}(|0\rangle |E_1\rangle + |1\rangle |E_2\rangle)$ still coherent?
Can't we do a joint measurement?

Environment is huge (on order of 10^{23} particles)
Environment can contain photons which leave at the speed of light
Irreversible change

Does this sound familiar?

Decoherence

Decoherence $\rightarrow$ no interference

No interference $\rightarrow$ everything becomes classical
(from the observer's point of view)

Isn't the joint state $\frac{1}{\sqrt{2}}(|0\rangle |E_1\rangle + |1\rangle |E_2\rangle)$ still coherent?
Can't we do a joint measurement?

Environment is huge (on order of 10^{23} particles)
Environment can contain photons which leave at the speed of light
Irreversible change

Does this sound familiar?
Decoherence is a manifestation of
the second law of thermodynamics!

Decoherence

Decoherence $\rightarrow$ no interference

No interference $\rightarrow$ everything becomes classical
(from the observer's point of view)

Isn't the joint state $\frac{1}{\sqrt{2}}(|0\rangle |E_1\rangle + |1\rangle |E_2\rangle)$ still coherent?
Can't we do a joint measurement?

Environment is huge (on order of 10^{23} particles)
Environment can contain photons which leave at the speed of light
Irreversible change

Does this sound familiar?
Decoherence is a manifestation of
the second law of thermodynamics!

While decoherence is damaging to computation, it explains why we don't see quantum weirdness around us

Decoherence

Decoherence

"Not only are we trying to keep errors from leaking into our computer, we're trying to keep the computer from leaking into the rest of the world" - **Scott Aaronson**

Decoherence

"*Not only are we trying to keep errors from leaking into our computer, we're trying to keep the computer from leaking into the rest of the world*" - **Scott Aaronson**

How can we solve this problem?

Decoherence

"*Not only are we trying to keep errors from leaking into our computer, we're trying to keep the computer from leaking into the rest of the world*" - **Scott Aaronson**

How can we solve this problem?

Let's look at a different question first

Question

Question

Is a quantum computer an analog computer?

Question

Is a quantum computer an analog computer?

NO!

Question

Is a quantum computer an analog computer?

NO!

Analog computers are sensitive to small changes in input or operation

Question

Is a quantum computer an analog computer?

NO!

Analog computers are sensitive to small changes in input or operation

Quantum threshold theorem

Question

Is a quantum computer an analog computer?

NO!

Analog computers are sensitive to small changes in input or operation

Quantum threshold theorem

If the error rate (decoherence rate) per qubit, per gate operation is below a constant threshold $\rightarrow$ errors can be corrected faster than they occur!

Question

Is a quantum computer an analog computer?

NO!

Analog computers are sensitive to small changes in input or operation

Quantum threshold theorem

If the error rate (decoherence rate) per qubit, per gate operation is below a constant threshold $\rightarrow$ errors can be corrected faster than they occur!

This leads to our solution...

Fault tolerance

Fault tolerance

- Encode qubits and gates in an error correcting code (QECC)

Fault tolerance

- Encode qubits and gates in an error correcting code (QECC)
- Code should be able to detect and correct for errors

Fault tolerance

- Encode qubits and gates in an error correcting code (QECC)
- Code should be able to detect and correct for errors
- Threshold theorem guarantees that it works

Fault tolerance

- Encode qubits and gates in an error correcting code (QECC)
- Code should be able to detect and correct for errors
- Threshold theorem guarantees that it works
- QECC use redundancy

Fault tolerance

- Encode qubits and gates in an error correcting code (QECC)
- Code should be able to detect and correct for errors
- Threshold theorem guarantees that it works
- QECC use redundancy
- I.e. one qubit is encoded in several qubits

Fault tolerance

- Encode qubits and gates in an error correcting code (QECC)
- Code should be able to detect and correct for errors
- Threshold theorem guarantees that it works
- QECC use redundancy
- I.e. one qubit is encoded in several qubits
- Computation is run with the encoded qubits

Fault tolerance
Example

Fault tolerance
Example

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

Fault tolerance
Example

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

We will encode $|\psi\rangle$ using 3 qubits

Fault tolerance
Example

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

We will encode $|\psi\rangle$ using 3 qubits

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

Fault tolerance
Example

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

We will encode $|\psi\rangle$ using 3 qubits

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

$|\psi\rangle_L$ is called a **logical qubit**

Fault tolerance
Example

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

We will encode $|\psi\rangle$ using 3 qubits

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

$|\psi\rangle_L$ is called a **logical qubit**
The 3 encoding qubits are called **physical qubits**

Fault tolerance
Example

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

We will encode $|\psi\rangle$ using 3 qubits

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

$|\psi\rangle_L$ is called a **logical qubit**
The 3 encoding qubits are called **physical qubits**

With this encoding we can detect and correct flip (X) errors

Fault tolerance
Example

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

We will encode $|\psi\rangle$ using 3 qubits

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

$|\psi\rangle_L$ is called a **logical qubit**
The 3 encoding qubits are called **physical qubits**

With this encoding we can detect and correct flip (X) errors

E.g. if there is a flip on the first physical qubit
$|\psi\rangle_L \to a\,|100\rangle + b\,|011\rangle$

Fault tolerance
Example

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

We will encode $|\psi\rangle$ using 3 qubits

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

$|\psi\rangle_L$ is called a **logical qubit**
The 3 encoding qubits are called **physical qubits**

With this encoding we can detect and correct flip (X) errors

E.g. if there is a flip on the first physical qubit
$|\psi\rangle_L \rightarrow a\,|100\rangle + b\,|011\rangle$

This can be detected and corrected

Fault tolerance
Example

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

We will encode $|\psi\rangle$ using 3 qubits

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

$|\psi\rangle_L$ is called a **logical qubit**
The 3 encoding qubits are called **physical qubits**

With this encoding we can detect and correct flip (X) errors

E.g. if there is a flip on the first physical qubit
$|\psi\rangle_L \to a\,|100\rangle + b\,|011\rangle$

This can be detected and corrected

How?

Fault tolerance
Example

Fault tolerance
Example

We'll define a 3 qubit measurement by the following projectors:

Fault tolerance
Example

We'll define a 3 qubit measurement by the following projectors:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

Fault tolerance
Example

We'll define a 3 qubit measurement by the following projectors:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

What is the action of P_0 on $|\psi\rangle_L$?

Fault tolerance
Example

We'll define a 3 qubit measurement by the following projectors:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

What is the action of P_0 on $|\psi\rangle_L$?

$$P_0 |\psi\rangle_L = P_0(a|000\rangle + b|111\rangle) = aP_0|000\rangle + bP_0|111\rangle$$

Fault tolerance
Example

We'll define a 3 qubit measurement by the following projectors:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

What is the action of P_0 on $|\psi\rangle_L$?

$$P_0 |\psi\rangle_L = P_0(a|000\rangle + b|111\rangle) = aP_0|000\rangle + bP_0|111\rangle$$

$$P_0|000\rangle = (|000\rangle\langle 000| + |111\rangle\langle 111|)|000\rangle =$$

Fault tolerance
Example

We'll define a 3 qubit measurement by the following projectors:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

What is the action of P_0 on $|\psi\rangle_L$?

$$P_0 |\psi\rangle_L = P_0(a|000\rangle + b|111\rangle) = aP_0|000\rangle + bP_0|111\rangle$$

$$P_0|000\rangle = (|000\rangle\langle 000| + |111\rangle\langle 111|)|000\rangle =$$
$$= |000\rangle\langle 000|000\rangle + |111\rangle\langle 111|000\rangle =$$

Fault tolerance
Example

We'll define a 3 qubit measurement by the following projectors:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

What is the action of P_0 on $|\psi\rangle_L$?

$$P_0 |\psi\rangle_L = P_0(a|000\rangle + b|111\rangle) = aP_0|000\rangle + bP_0|111\rangle$$

$$P_0|000\rangle = (|000\rangle\langle 000| + |111\rangle\langle 111|)|000\rangle =$$
$$= |000\rangle\langle 000|000\rangle + |111\rangle\langle 111|000\rangle =$$
$$= |000\rangle + 0|111\rangle = |000\rangle$$

Fault tolerance
Example

We'll define a 3 qubit measurement by the following projectors:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

What is the action of P_0 on $|\psi\rangle_L$?

$$P_0 |\psi\rangle_L = P_0(a|000\rangle + b|111\rangle) = aP_0|000\rangle + bP_0|111\rangle$$

$$P_0|000\rangle = (|000\rangle\langle 000| + |111\rangle\langle 111|)|000\rangle =$$
$$= |000\rangle\langle 000|000\rangle + |111\rangle\langle 111|000\rangle =$$
$$= |000\rangle + 0|111\rangle = |000\rangle$$

$$P_0|111\rangle = |111\rangle$$

Fault tolerance
Example

We'll define a 3 qubit measurement by the following projectors:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

What is the action of P_0 on $|\psi\rangle_L$?

$$P_0|\psi\rangle_L = P_0(a|000\rangle + b|111\rangle) = aP_0|000\rangle + bP_0|111\rangle$$

$$P_0|000\rangle = (|000\rangle\langle 000| + |111\rangle\langle 111|)|000\rangle =$$
$$= |000\rangle\langle 000|000\rangle + |111\rangle\langle 111|000\rangle =$$
$$= |000\rangle + 0|111\rangle = |000\rangle$$

$$P_0|111\rangle = |111\rangle$$

$$P_0|\psi\rangle_L = a|000\rangle + b|111\rangle = |\psi\rangle_L$$

Fault tolerance
Example

We'll define a 3 qubit measurement by the following projectors:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

What is the action of P_0 on $|\psi\rangle_L$?

$$P_0|\psi\rangle_L = P_0(a|000\rangle + b|111\rangle) = aP_0|000\rangle + bP_0|111\rangle$$

$$P_0|000\rangle = (|000\rangle\langle 000| + |111\rangle\langle 111|)|000\rangle =$$
$$= |000\rangle\langle 000|000\rangle + |111\rangle\langle 111|000\rangle =$$
$$= |000\rangle + 0|111\rangle = |000\rangle$$

$$P_0|111\rangle = |111\rangle$$

$$P_0|\psi\rangle_L = a|000\rangle + b|111\rangle = |\psi\rangle_L$$

So $p(0) = \langle\psi|_L P_0|\psi\rangle_L = 1$ and $p(1) = p(2) = p(3) = 0$

Fault tolerance
Example

We'll define a 3 qubit measurement by the following projectors:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

What is the action of P_1 on $|\phi\rangle_L = a|100\rangle + b|011\rangle$?
(i.e. $(X \otimes I \otimes I)|\psi\rangle_L$)

Fault tolerance
Example

We'll define a 3 qubit measurement by the following projectors:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

What is the action of P_1 on $|\phi\rangle_L = a|100\rangle + b|011\rangle$?

(i.e. $(X \otimes I \otimes I)|\psi\rangle_L$)

$$P_1|\phi\rangle_L = P_1(a|100\rangle + b|011\rangle) = aP_1|100\rangle + bP_1|011\rangle$$

Fault tolerance
Example

We'll define a 3 qubit measurement by the following projectors:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

What is the action of P_1 on $|\phi\rangle_L = a|100\rangle + b|011\rangle$?
(i.e. $(X \otimes I \otimes I)|\psi\rangle_L$)

$$P_1|\phi\rangle_L = P_1(a|100\rangle + b|011\rangle) = aP_1|100\rangle + bP_1|011\rangle$$

$$P_1|100\rangle = |100\rangle$$
$$P_1|011\rangle = |011\rangle$$

Fault tolerance
Example

We'll define a 3 qubit measurement by the following projectors:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

What is the action of P_1 on $|\phi\rangle_L = a|100\rangle + b|011\rangle$?
(i.e. $(X \otimes I \otimes I)|\psi\rangle_L$)

$$P_1|\phi\rangle_L = P_1(a|100\rangle + b|011\rangle) = aP_1|100\rangle + bP_1|011\rangle$$

$$P_1|100\rangle = |100\rangle$$
$$P_1|011\rangle = |011\rangle$$

$$P_1|\phi\rangle_L = a|100\rangle + b|011\rangle = |\phi\rangle_L$$

Fault tolerance
Example

We'll define a 3 qubit measurement by the following projectors:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

What is the action of P_1 on $|\phi\rangle_L = a|100\rangle + b|011\rangle$?
(i.e. $(X \otimes I \otimes I)|\psi\rangle_L$)

$$P_1|\phi\rangle_L = P_1(a|100\rangle + b|011\rangle) = aP_1|100\rangle + bP_1|011\rangle$$

$$P_1|100\rangle = |100\rangle$$
$$P_1|011\rangle = |011\rangle$$

$$P_1|\phi\rangle_L = a|100\rangle + b|011\rangle = |\phi\rangle_L$$

So $p(1) = 1$ and $p(0) = p(2) = p(3) = 0$

Fault tolerance
Example

Fault tolerance
Example

So the previous measurement leaves the state unchanged
(if only one X flip occurred)

Fault tolerance
Example

So the previous measurement leaves the state unchanged
(if only one X flip occurred)

The outcome of the measurement tells us where the flip occurred!
(if it did)

Fault tolerance
Example

So the previous measurement leaves the state unchanged
(if only one X flip occurred)

The outcome of the measurement tells us where the flip occurred!
(if it did)

This is called **syndrome measurement**
(or Quantum Non-Destructive measurement, QND)

Fault tolerance
Example

So the previous measurement leaves the state unchanged
(if only one X flip occurred)

The outcome of the measurement tells us where the flip occurred!
(if it did)

This is called **syndrome measurement**
(or Quantum Non-Destructive measurement, QND)

Syndrome measurement $\approx$ measurement which gives us some information about the (logical) state without disturbing it

Fault tolerance
Example

So the previous measurement leaves the state unchanged
(if only one X flip occurred)

The outcome of the measurement tells us where the flip occurred!
(if it did)

This is called **syndrome measurement**
(or Quantum Non-Destructive measurement, QND)

Syndrome measurement $\approx$ measurement which gives us some information about the (logical) state without disturbing it

When we know where the error occurred, just correct for it!

Fault tolerance
Example

So the previous measurement leaves the state unchanged
(if only one X flip occurred)

The outcome of the measurement tells us where the flip occurred!
(if it did)

This is called **syndrome measurement**
(or Quantum Non-Destructive measurement, QND)

Syndrome measurement $\approx$ measurement which gives us some information about the (logical) state without disturbing it

When we know where the error occurred, just correct for it!

I.e. if outcome is 1 (first qubit flipped), just apply X to first qubit

Fault tolerance
Example

So the previous measurement leaves the state unchanged
(if only one X flip occurred)

The outcome of the measurement tells us where the flip occurred!
(if it did)

This is called **syndrome measurement**
(or Quantum Non-Destructive measurement, QND)

Syndrome measurement $\approx$ measurement which gives us some information about the (logical) state without disturbing it

When we know where the error occurred, just correct for it!

I.e. if outcome is 1 (first qubit flipped), just apply X to first qubit

This can be generalized to detect any kind of error
(on a single physical qubit), with 9 physical qubits!

Error models

Error models

Wait, but we're making the circuit larger right?

Error models

Wait, but we're making the circuit larger right?

Doesn't that make it more likely for an error to occur?

Error models

Wait, but we're making the circuit larger right?

Doesn't that make it more likely for an error to occur?

Not necessarily (it depends on the code and the error models)

Error models

Wait, but we're making the circuit larger right?

Doesn't that make it more likely for an error to occur?

Not necessarily (it depends on the code and the error models)

Assume we discretize time in intervals Δt

Error models

Wait, but we're making the circuit larger right?

Doesn't that make it more likely for an error to occur?

Not necessarily (it depends on the code and the error models)

Assume we discretize time in intervals Δt

Each "quantum instruction" is executed in one such interval

Error models

Wait, but we're making the circuit larger right?

Doesn't that make it more likely for an error to occur?

Not necessarily (it depends on the code and the error models)

Assume we discretize time in intervals Δt

Each "quantum instruction" is executed in one such interval

Examples of assumptions regarding errors (per interval):

- Environment independently corrupts a qubit with probability p_1
- Single qubit gates fail with some probability p_2
- Two-qubit gates fail with some probability p_3 (correlated error)

Concatenation codes

Concatenation codes

So say the chance of having an error in a circuit C is p (based on the error model)

Concatenation codes

So say the chance of having an error in a circuit C is p (based on the error model)

It is possible to construct an encoded circuit $E(C)$ with probability of error $O(p^2)$

Concatenation codes

So say the chance of having an error in a circuit C is p (based on the error model)

It is possible to construct an encoded circuit $E(C)$ with probability of error $O(p^2)$

Then $E(E(C))$ will have error probability $O(p^4)$

Concatenation codes

So say the chance of having an error in a circuit C is p (based on the error model)

It is possible to construct an encoded circuit $E(C)$ with probability of error $O(p^2)$

Then $E(E(C))$ will have error probability $O(p^4)$

Codes which can be composed in this way are called **concatenation codes**

Concatenation codes

So say the chance of having an error in a circuit C is p (based on the error model)

It is possible to construct an encoded circuit $E(C)$ with probability of error $O(p^2)$

Then $E(E(C))$ will have error probability $O(p^4)$

Codes which can be composed in this way are called **concatenation codes**

They can make the error rate arbitrarily small

Concatenation codes

So say the chance of having an error in a circuit C is p (based on the error model)

It is possible to construct an encoded circuit $E(C)$ with probability of error $O(p^2)$

Then $E(E(C))$ will have error probability $O(p^4)$

Codes which can be composed in this way are called **concatenation codes**

They can make the error rate arbitrarily small

There are additional details to this which are omitted

Concatenation codes

So say the chance of having an error in a circuit C is p
(based on the error model)

It is possible to construct an encoded circuit $E(C)$
with probability of error $O(p^2)$

Then $E(E(C))$ will have error probability $O(p^4)$

Codes which can be composed in this way are called
concatenation codes

They can make the error rate arbitrarily small

There are additional details to this which are omitted

E.g. to have small error rate per interval, make circuit such that at most one gate acts per qubit (in an interval)

Fault tolerant quantum computer

Fault tolerant quantum computer

1. Encode all qubits and gates in fault tolerant code

Fault tolerant quantum computer

1. Encode all qubits and gates in fault tolerant code

2. Do some computation in short time (small decoherence)

Fault tolerant quantum computer

1. Encode all qubits and gates in fault tolerant code
2. Do some computation in short time (small decoherence)
3. Make syndrome measurements to detect errors

Fault tolerant quantum computer

1. Encode all qubits and gates in fault tolerant code
2. Do some computation in short time (small decoherence)
3. Make syndrome measurements to detect errors
4. Apply correction procedures

Fault tolerant quantum computer

1. Encode all qubits and gates in fault tolerant code
2. Do some computation in short time (small decoherence)
3. Make syndrome measurements to detect errors
4. Apply correction procedures
5. Repeat until computation is finished!

Fault tolerant quantum computer

1. Encode all qubits and gates in fault tolerant code
2. Do some computation in short time (small decoherence)
3. Make syndrome measurements to detect errors
4. Apply correction procedures
5. Repeat until computation is finished!

Quantum memories would also have to do this!

In the real world

In the real world

- Having many qubits is useless without fault tolerance!

In the real world

- Having many qubits is useless without fault tolerance!
- Fault tolerant quantum computation is heavily researched

In the real world

- Having many qubits is useless without fault tolerance!
- Fault tolerant quantum computation is heavily researched
- NQIT, Google, IBM are all working towards fault tolerant quantum computers

In the real world

- Having many qubits is useless without fault tolerance!
- Fault tolerant quantum computation is heavily researched
- NQIT, Google, IBM are all working towards fault tolerant quantum computers
- They are also trying to make it scalable

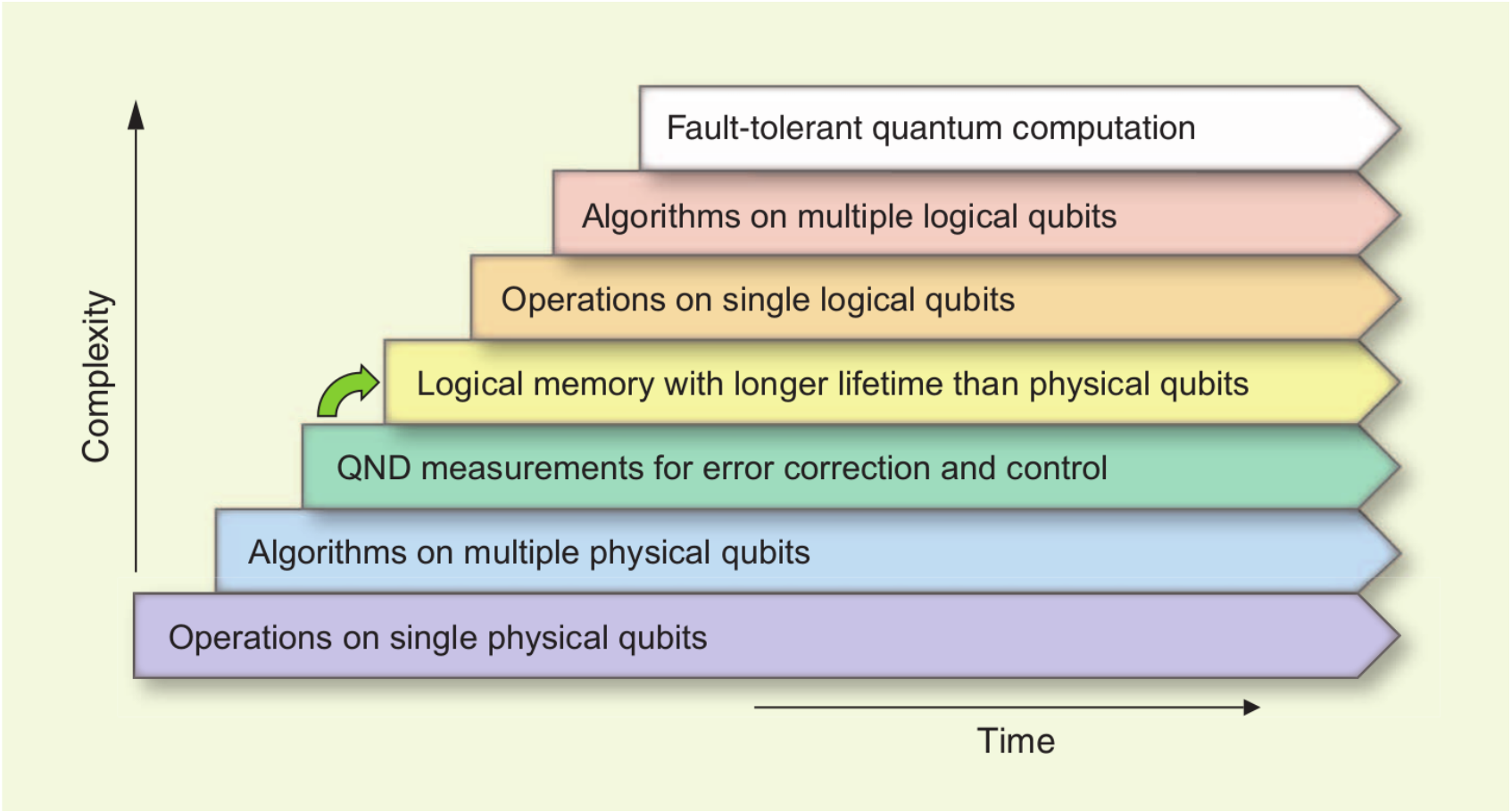
In the real world

- Having many qubits is useless without fault tolerance!
- Fault tolerant quantum computation is heavily researched
- NQIT, Google, IBM are all working towards fault tolerant quantum computers
- They are also trying to make it scalable
- Only a technological challenge, not a physical one!

In the real world

- Having many qubits is useless without fault tolerance!
- Fault tolerant quantum computation is heavily researched
- NQIT, Google, IBM are all working towards fault tolerant quantum computers
- They are also trying to make it scalable
- Only a technological challenge, not a physical one!
- D-Wave machines are not universal, nor fault tolerant

The current picture



Useful resources

- **The physical implementation of quantum computing** - http://www-users.cs.york.ac.uk/schmuel/book/quantum.pdf
- **NQIT and Q20:20** - http://nqit.ox.ac.uk/
- **Linear Optics Quantum Computation: an Overview** - http://arxiv.org/pdf/quant-ph/0512104v1.pdf
- **Superconducting Circuits for Quantum Information: An Outlook** (also image on slide 18) - http://www.sciencemag.org/content/339/6124/1169.full
- **Against the scepticism of quantum computing** - http://www.scottaaronson.com/democritus/lec14.html
- **Decoherence and hidden variables** - http://www.scottaaronson.com/democritus/lec11.html
- **Decoherence explained mathematically** - Section 11 in http://arxiv.org/pdf/quant-ph/0011013.pdf
- **The role of decoherence in quantum mechanics** - http://plato.stanford.edu/entries/qm-decoherence/

Useful resources

- **Quantum Error Correction for Beginners** - http://arxiv.org/pdf/0905.2794v4.pdf
- **An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation** - http://arxiv.org/abs/0904.2557
- **Stabilizer codes and Quantum Error Correction** - http://arxiv.org/pdf/quant-ph/9705052v1.pdf
- **Magic states** - http://www.iqst.ca/events/csqic05/talks/nathan%20b.pdf