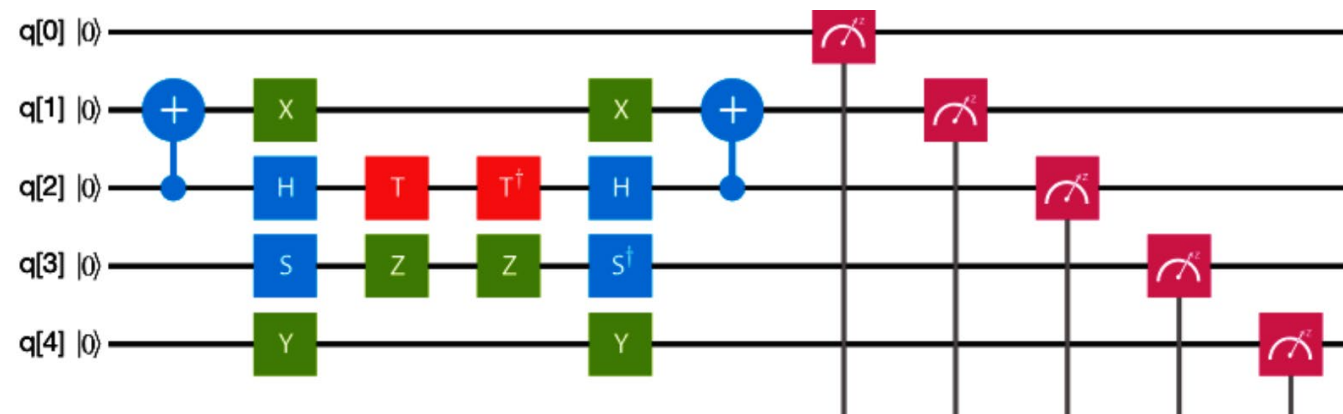


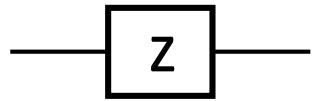
# 17. Quantum circuits



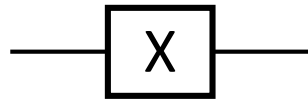
# Recap: Elementary gates

In the previous lecture we met several quantum gates:

## 1 qubit gates



$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

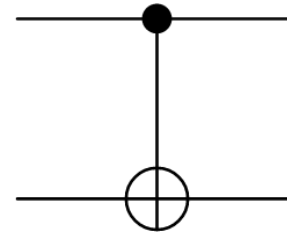


$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$



$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

## 2 qubit gate



$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

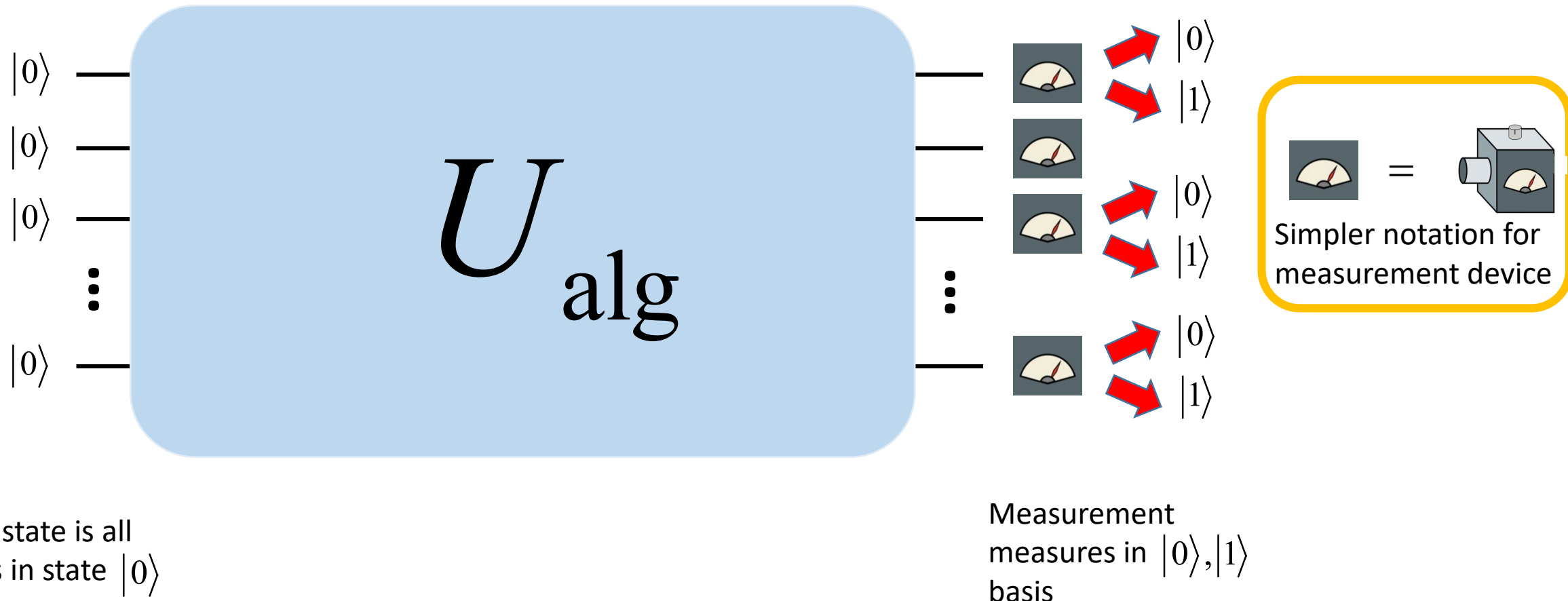
The key aspect here is that the quantum gates all needed to be unitary such that they are compatible with the Schrodinger equation.

$$U^\dagger U = I$$

Universality: By combining an arbitrary 1 qubit unitary with a CNOT we can make a completely arbitrary unitary evolution (i.e. quantum algorithm) for an arbitrary number of qubits.

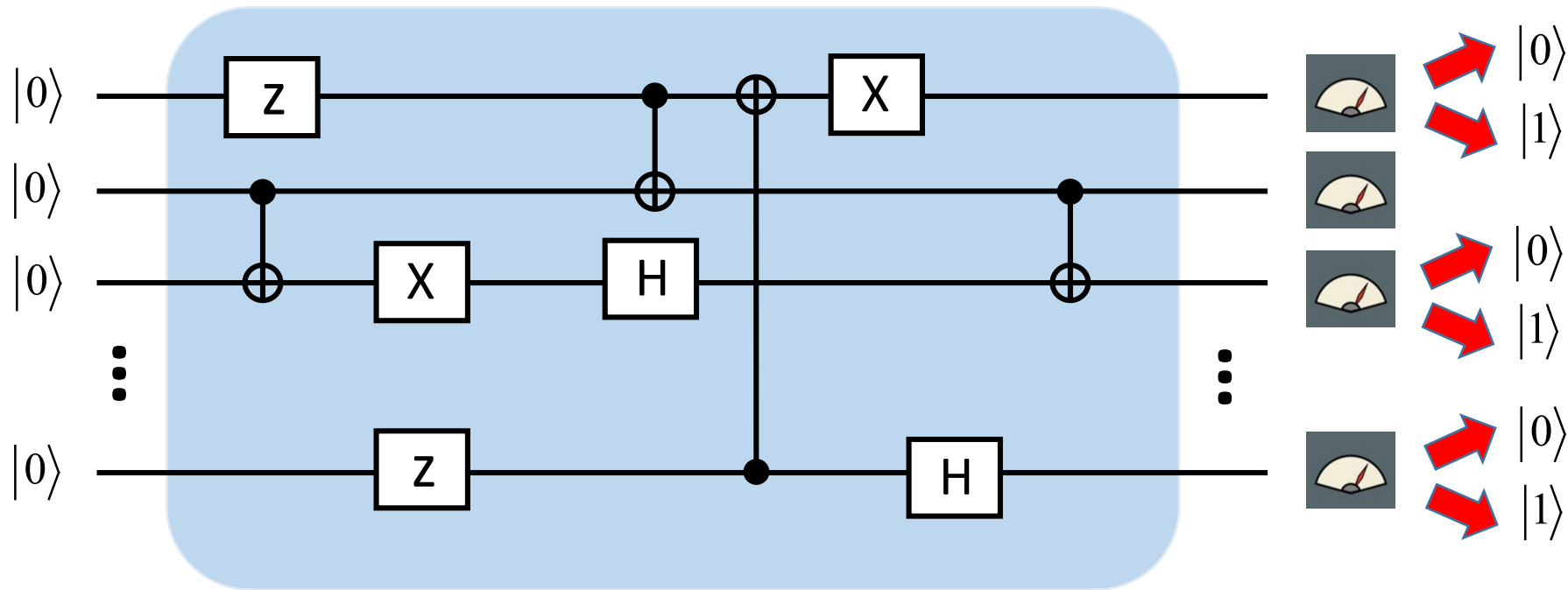
# General structure of a quantum algorithm

Quantum circuits (without feed-forward) can be always written in “standard form”



# General structure of a quantum algorithm

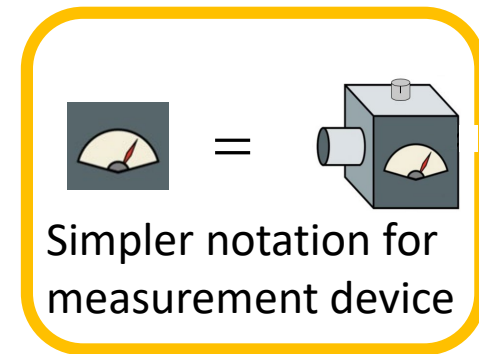
Typically a quantum circuit always looks like



Initial state is all qubits in state  $|0\rangle$

Consists of 1 and 2 qubit gates. Any unitary can be made by a combination of these.

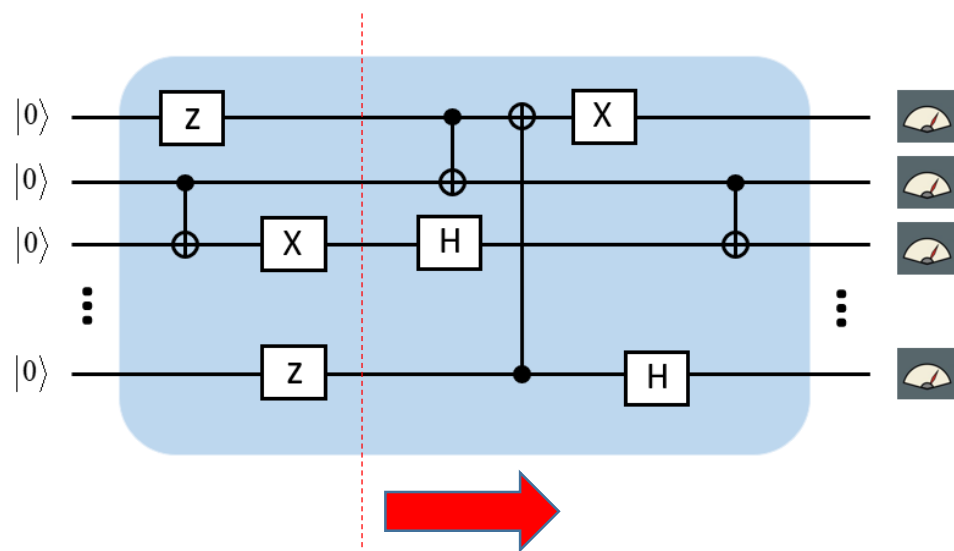
Measurement measures in  $|0\rangle, |1\rangle$  basis



# Quantum circuit rules

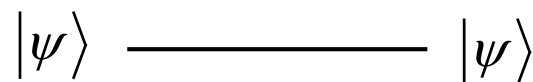
Not all quantum circuits are valid quantum circuits. Some rules about quantum circuits:

1) Gates are applied sequentially from left to right.

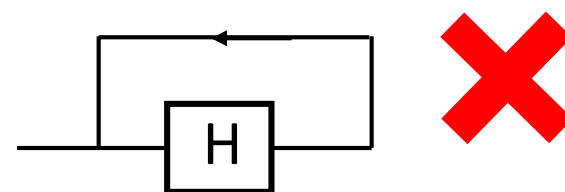


At each point the quantum computer is in a particular state.

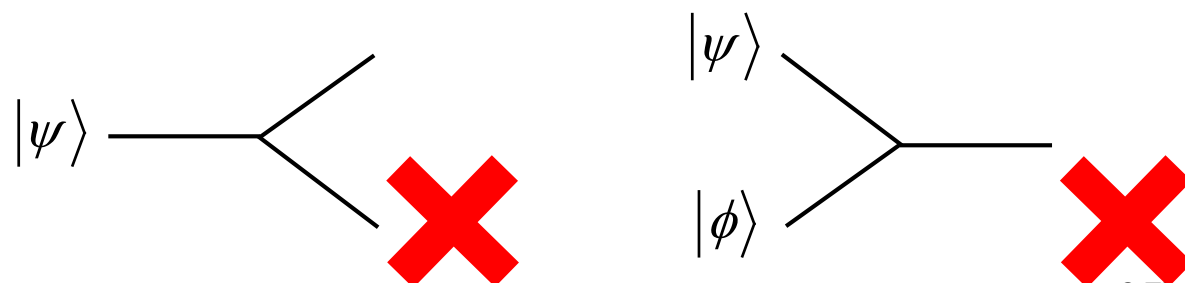
2) Wires represent the identity matrix (“do nothing”)



3) There are no loops

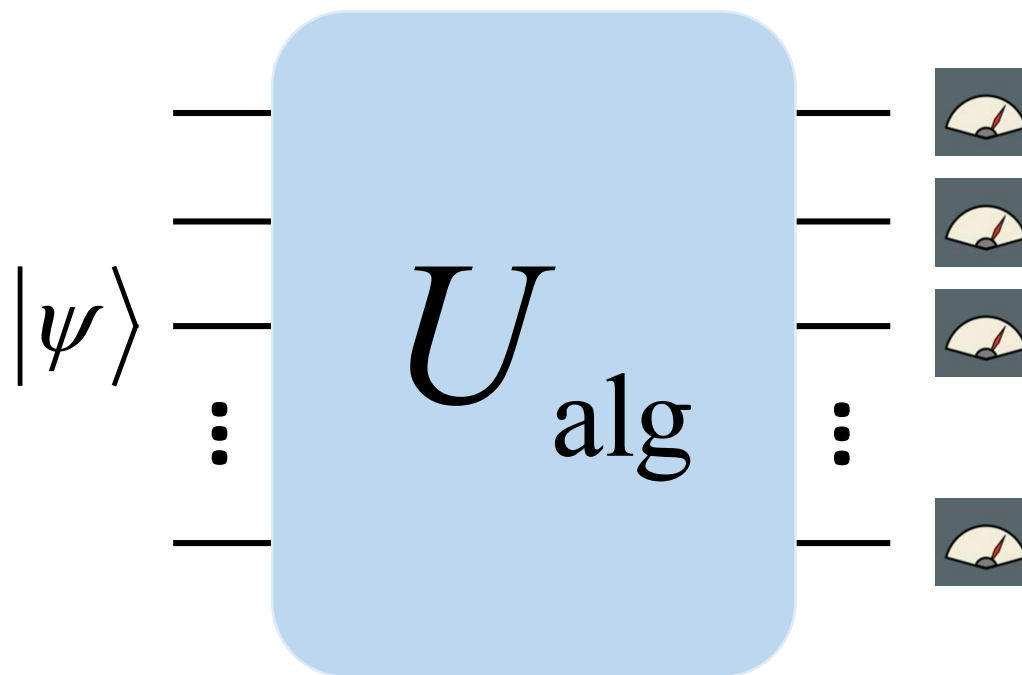


4) Number of qubits is preserved



# Initial state

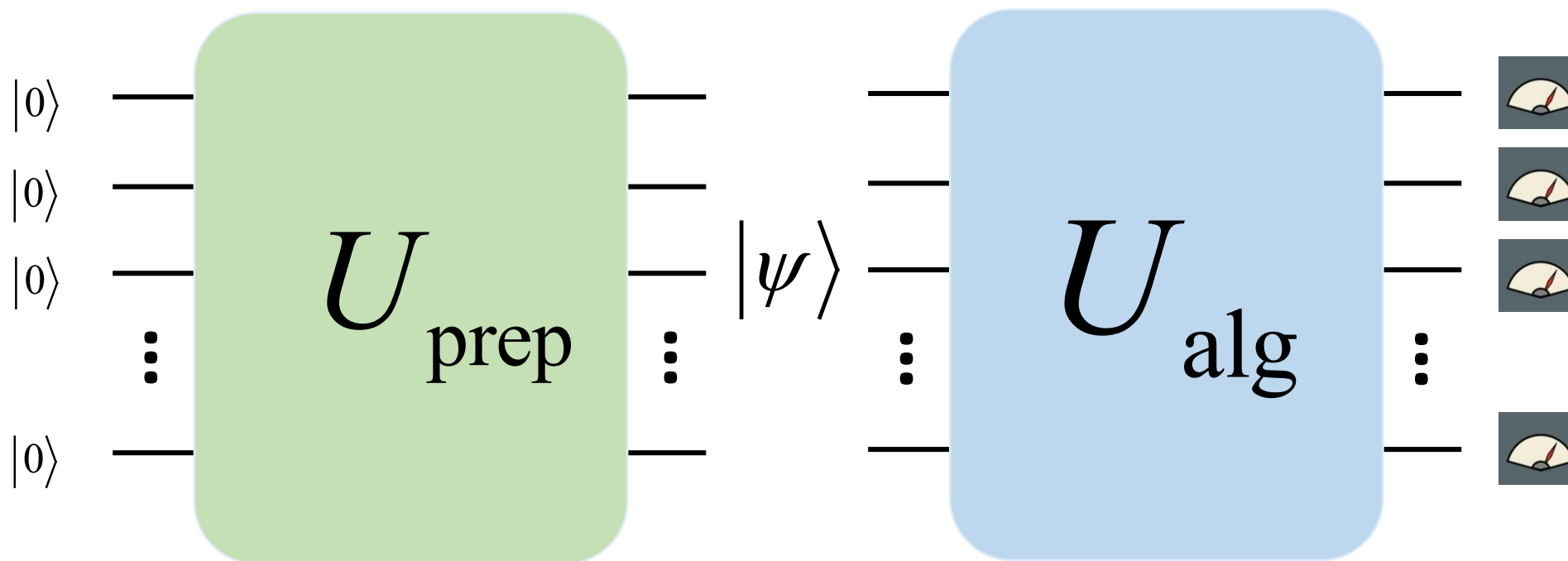
The initial state is set to all  $|0\rangle$ . This seems like an unnecessary restriction.  
Why can't we have a more general initial state?



# Initial state

The initial state is set to all  $|0\rangle$ . This seems like an unnecessary restriction.  
Why can't we have a more general initial state?

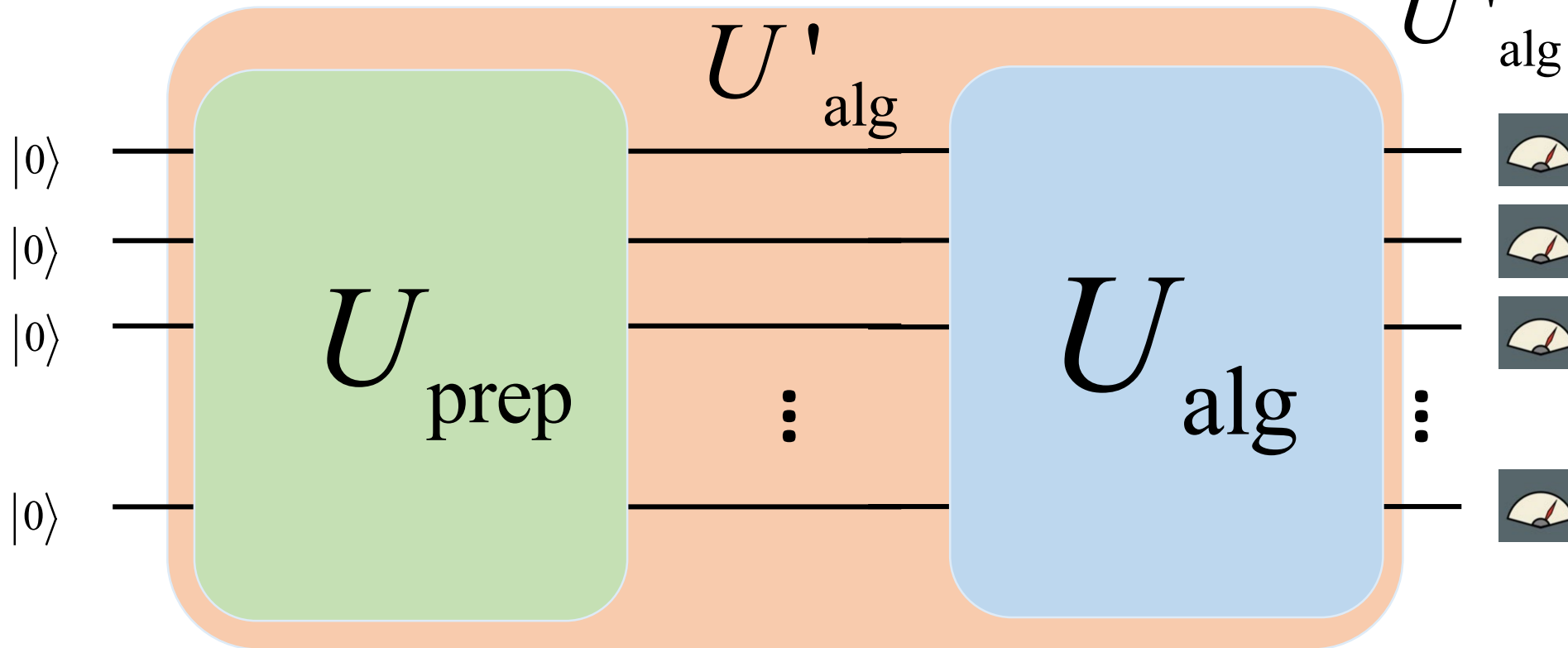
ANSWER: We can, but we could add a state preparation circuit which prepares the desired state.



# Initial state

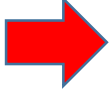
The initial state is set to all  $|0\rangle$ . This seems like an unnecessary restriction. Why can't we have a more general initial state?

ANSWER: We can, but we could add a state preparation circuit which prepares the desired state.



The total circuit is then

$$U'_{\text{alg}} = U_{\text{alg}} U_{\text{prep}}$$



Reduces to  
standard form

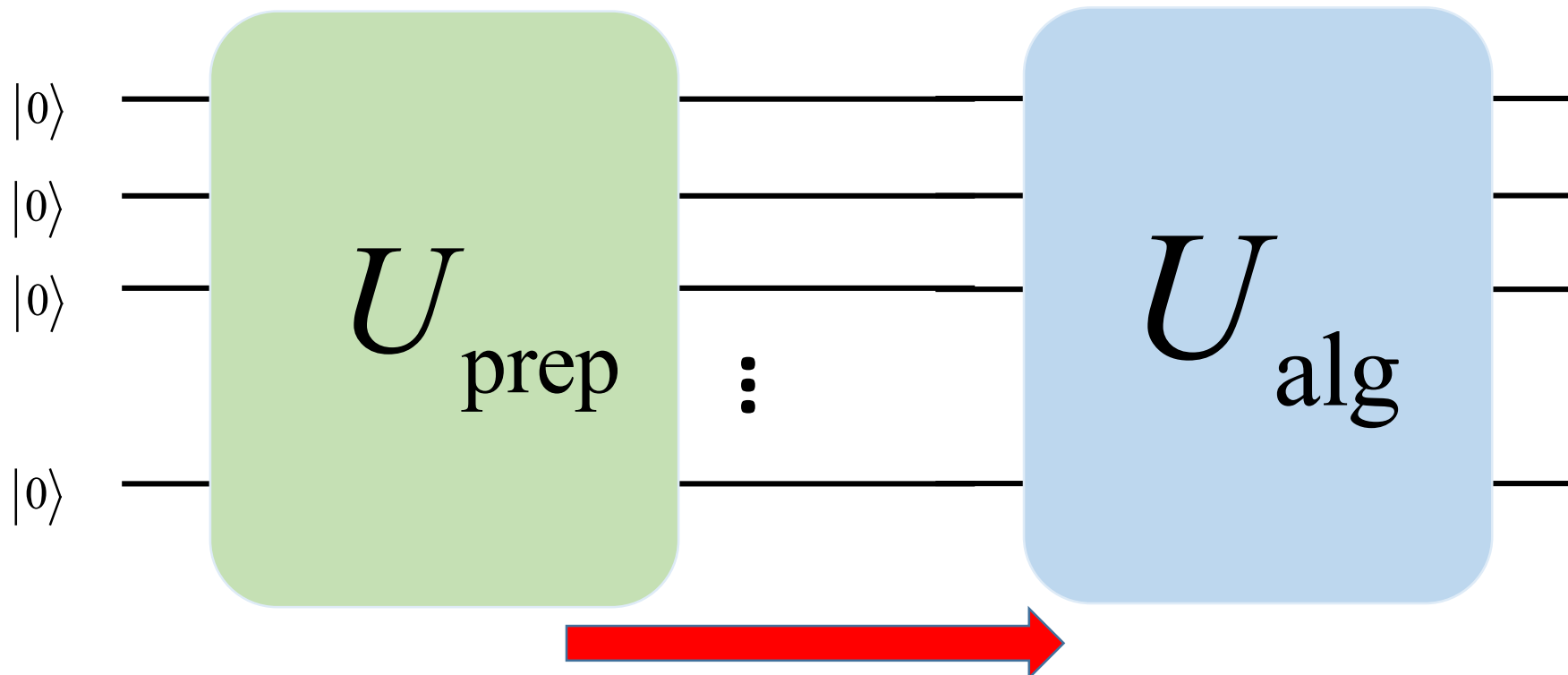


# Caution: quantum circuit notation vs math notation

Note that the mathematical notation for the whole circuit was written

$$U_{\text{alg}} U_{\text{prep}} |0\rangle |0\rangle \cdots |0\rangle$$

While the quantum circuit ordering was the reverse order.

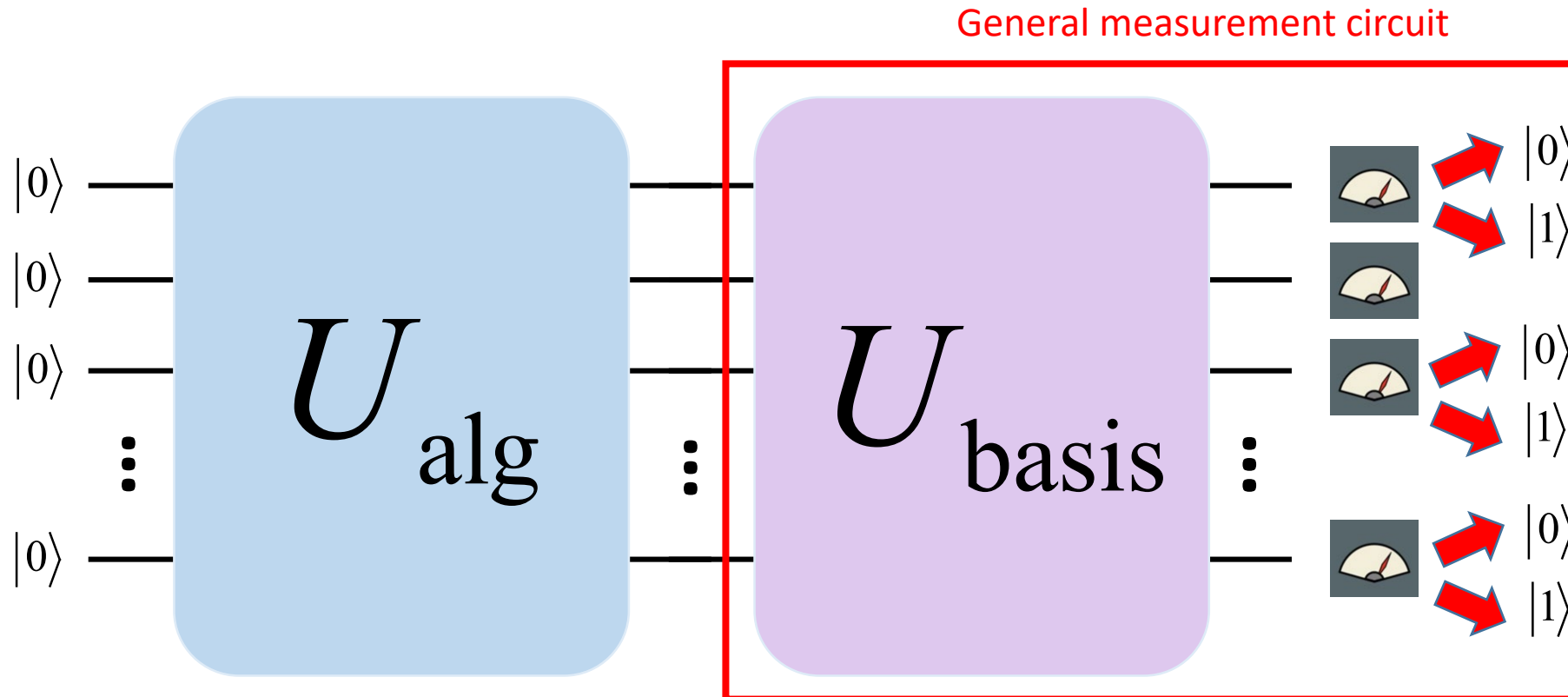


The ordering of gates on the quantum circuit is always the reverse of the math notation.

# Measurement basis

Similarly, why is the measurement basis fixed to  $|0\rangle, |1\rangle$ ? Isn't this a restriction?

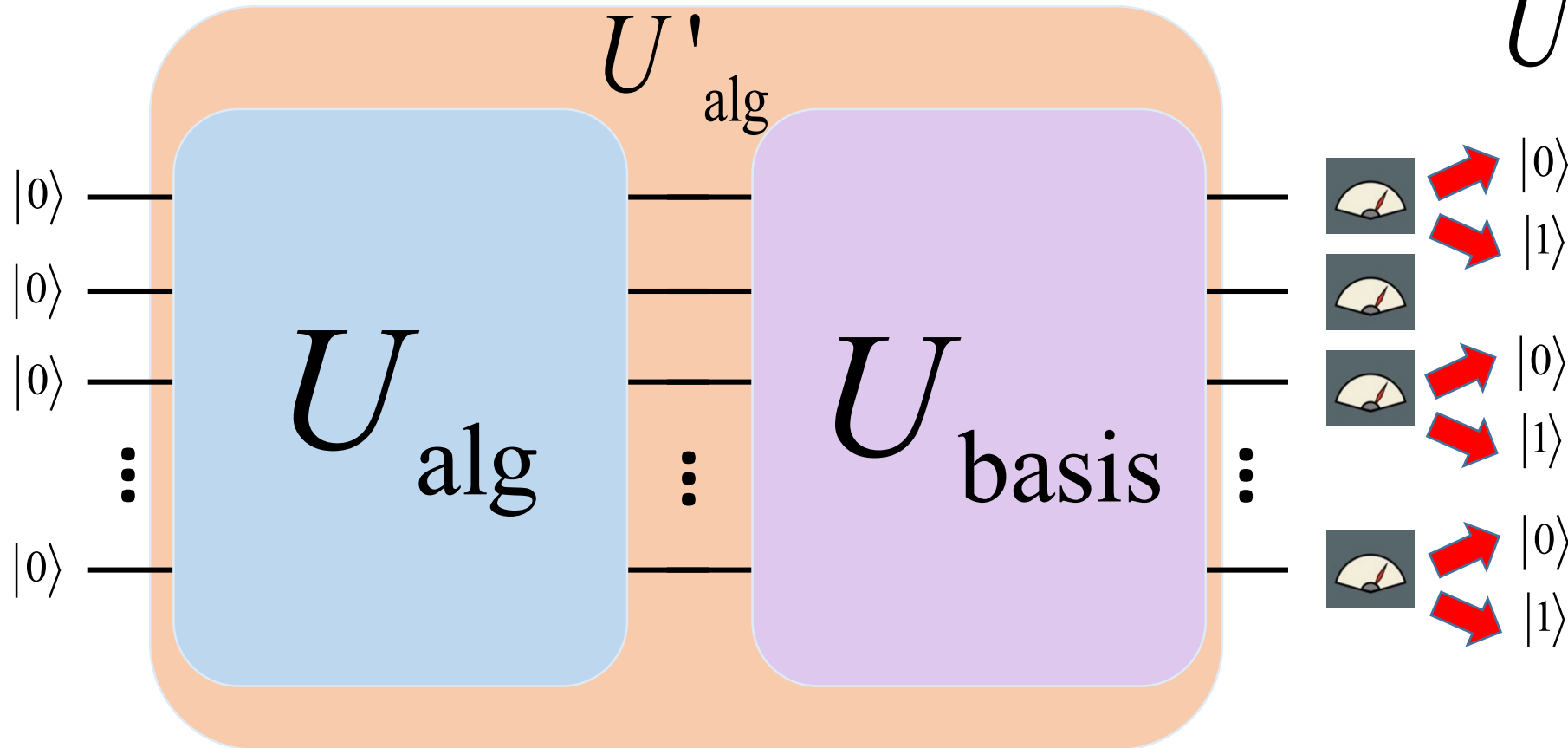
ANSWER: No, since we can always add a basis rotation circuit before the measurement



# Measurement basis

Similarly, why is the measurement basis fixed to  $|0\rangle, |1\rangle$ ? Is this a restriction?

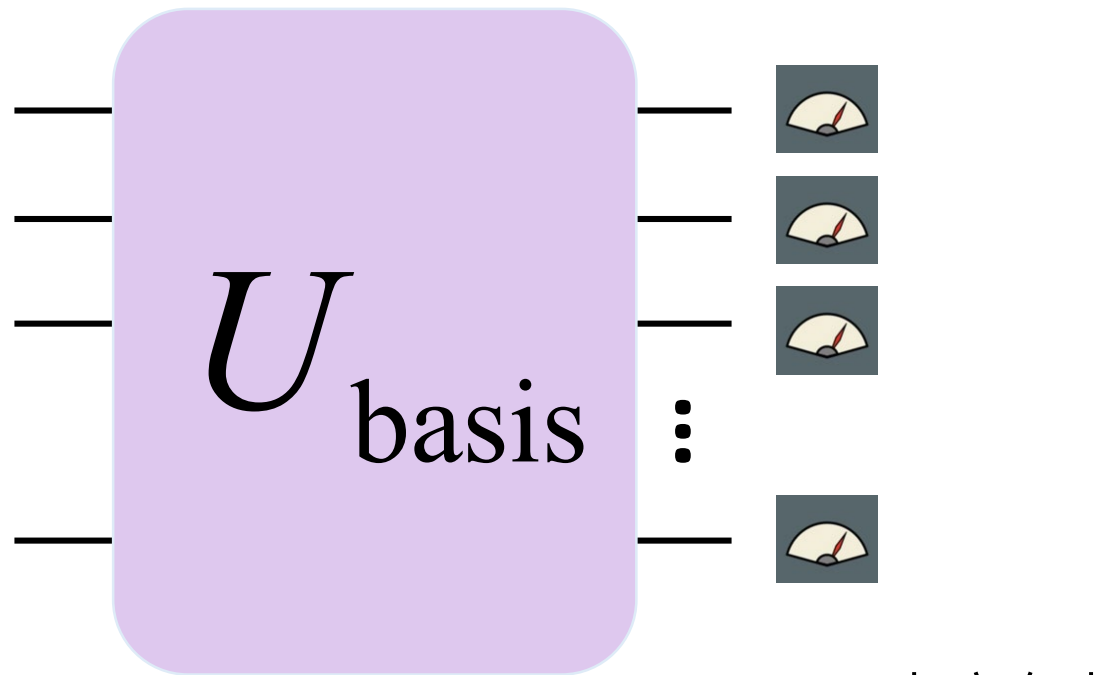
ANSWER: No, since we can always add a basis rotation circuit before the measurement



$$U'_{\text{alg}} = U_{\text{basis}} U_{\text{alg}}$$

# General measurement

The combination of the  $U_{\text{basis}}$  and the measurement in the  $|0\rangle, |1\rangle$  basis can achieve a general measurement.



$$M_n = |n\rangle\langle n|$$

e.g.  $|n\rangle = |0010\rangle$

The combination can be written

$$M_n^{\text{gen}} = M_n U_{\text{basis}}$$

But since

$$U_{\text{basis}} = \sum_{mm'} u_{mm'} |m\rangle\langle m'| = \sum_m |m\rangle\langle b_m|$$

Where a general measurement basis element is

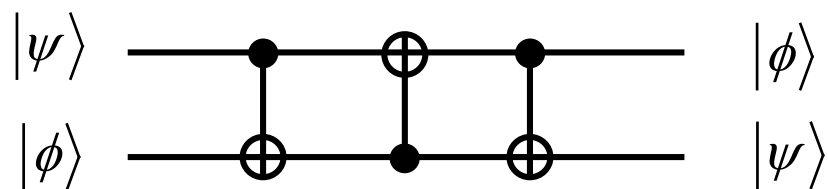
$$|b_m\rangle = \sum_{m'} u_{mm'}^* |m'\rangle$$

Then

$$M_n^{\text{gen}} = |n\rangle\langle b_n|$$

# A simple quantum circuit: SWAP

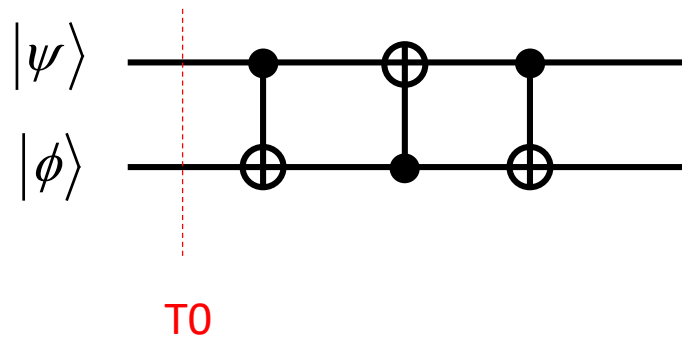
The aim of the SWAP circuit is to swap the state between two qubits.



To show how this circuit works, look at the quantum state step by step.

# A simple circuit: SWAP

The aim of the SWAP circuit is to swap the state between two qubits.



Time  $T0$ : The initial state is

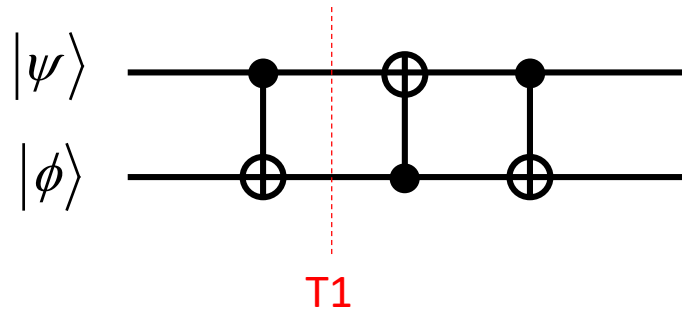
$$\begin{aligned}|T0\rangle &= |\psi\rangle|\phi\rangle = (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \lambda|1\rangle) \\ &= \alpha\gamma|00\rangle + \alpha\lambda|01\rangle + \beta\gamma|10\rangle + \beta\lambda|11\rangle\end{aligned}$$

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

$$|\phi\rangle = \gamma|0\rangle + \lambda|1\rangle$$

# A simple circuit: SWAP

The aim of the SWAP circuit is to swap the state between two qubits.

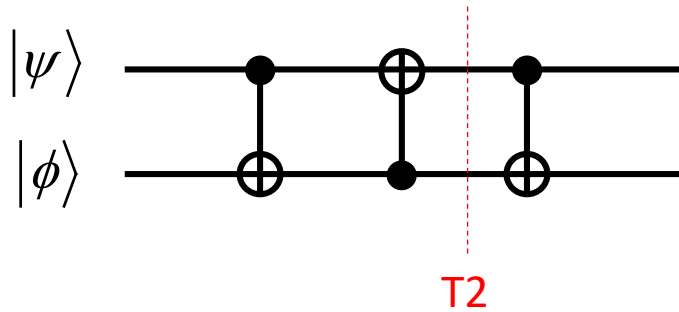


Time T1: Apply CNOT between qubits (control qubit is 1)

$$\begin{aligned} |T1\rangle &= U_{\text{CNOT}}^{(\text{ctrl}=q1)} |T0\rangle = U_{\text{CNOT}}^{(\text{ctrl}=q1)} (\alpha\gamma|00\rangle + \alpha\lambda|01\rangle + \beta\gamma|10\rangle + \beta\lambda|11\rangle) \\ &= \alpha\gamma|00\rangle + \alpha\lambda|01\rangle + \beta\gamma|11\rangle + \beta\lambda|10\rangle \end{aligned}$$

# A simple circuit: SWAP

The aim of the SWAP circuit is to swap the state between two qubits.



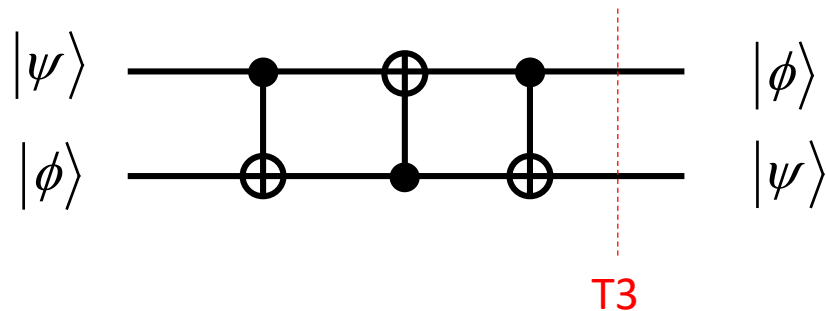
Time T2: Apply CNOT between qubits (control qubit is 2)

$$\begin{aligned} |T2\rangle &= U_{\text{CNOT}}^{(\text{ctrl}=q2)} |T1\rangle = U_{\text{CNOT}}^{(\text{ctrl}=q2)} (\alpha\gamma|00\rangle + \alpha\lambda|01\rangle + \beta\gamma|11\rangle + \beta\lambda|10\rangle) \\ &= \alpha\gamma|00\rangle + \alpha\lambda|11\rangle + \beta\gamma|01\rangle + \beta\lambda|10\rangle \end{aligned}$$



# A simple circuit: SWAP

The aim of the SWAP circuit is to swap the state between two qubits.

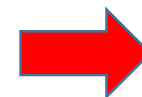


Time T3: Apply CNOT between qubits (control qubit is 1)

$$\begin{aligned}
 |T3\rangle &= U_{\text{CNOT}}^{(\text{ctrl}=q1)} |T2\rangle = U_{\text{CNOT}}^{(\text{ctrl}=q1)} (\alpha\gamma|00\rangle + \alpha\lambda|11\rangle + \beta\gamma|01\rangle + \beta\lambda|10\rangle) \\
 &= \alpha\gamma|00\rangle + \alpha\lambda|10\rangle + \beta\gamma|01\rangle + \beta\lambda|11\rangle \\
 &= \alpha(\gamma|0\rangle + \lambda|1\rangle)|0\rangle + \beta(\gamma|0\rangle + \lambda|1\rangle)|1\rangle \\
 &= (\gamma|0\rangle + \lambda|1\rangle)(\alpha|0\rangle + \beta|1\rangle)
 \end{aligned}$$

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

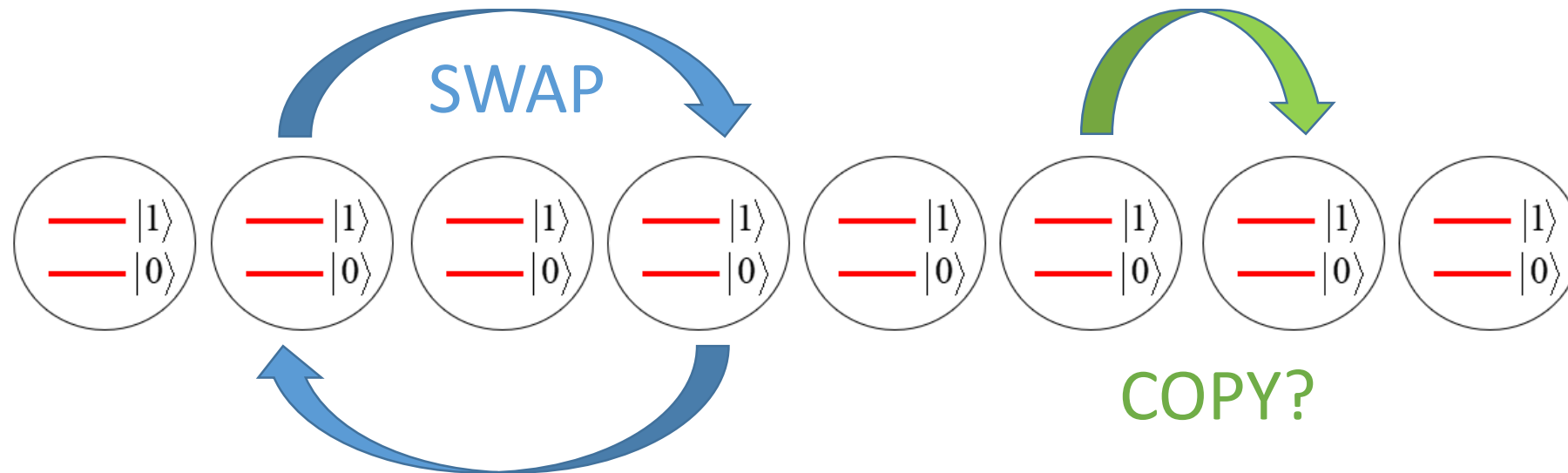
$$|\phi\rangle = \gamma|0\rangle + \lambda|1\rangle$$



Output qubits are swapped as desired

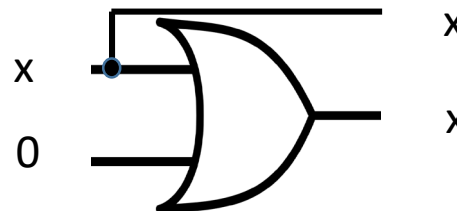
# The COPY circuit?

The SWAP is an elementary circuit that might be used in larger algorithms.



The next reasonable (and useful) algorithm would be a COPY circuit.

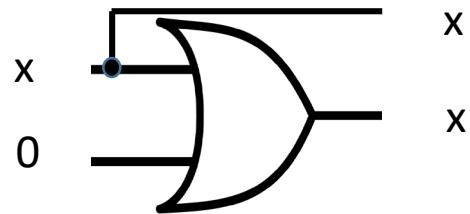
Classically, this can be done with the OR gate:



in 1 (x)	in 2 (=0)	in 1 (x)	out
0	0	0	0
1	0	1	1

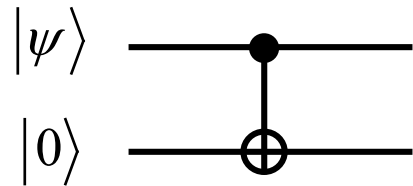
# The COPY circuit?

What is the quantum version of the COPY circuit?



in 1 (x)	in 2 (=0)	in 1 (x)	out
0	0	0	0
1	0	1	1

Let's try our plain and simple CNOT gate:



For the equivalent classical states

$$|\psi\rangle = |0\rangle \text{ case:}$$

$$|\text{output}\rangle = U_{\text{CNOT}}^{(\text{ctrl}=q1)} |0\rangle|0\rangle = |0\rangle|0\rangle$$

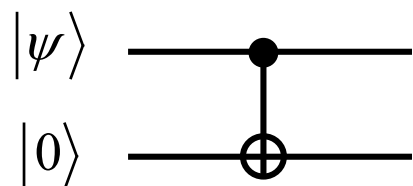
So far so good!

$$|\psi\rangle = |1\rangle \text{ case:}$$

$$|\text{output}\rangle = U_{\text{CNOT}}^{(\text{ctrl}=q1)} |1\rangle|0\rangle = |1\rangle|1\rangle$$

Does the same thing as the classical circuit.

# The COPY circuit?



For a more general input state

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

$$|\text{output}\rangle = U_{\text{CNOT}}^{(\text{ctrl}=q1)} (\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha|00\rangle + \beta|11\rangle$$

But what we actually wanted was

$$\begin{aligned} |\text{output}\rangle &= |\psi\rangle|\psi\rangle = (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle \end{aligned}$$

Clearly this is different!

# The No Cloning theorem

Actually it is **impossible** to make a circuit that copies a qubit!

Proof:

By contradiction. Suppose there is a circuit such that

$$U_{COPY} |\phi\rangle |0\rangle = e^{i\omega} |\phi\rangle |\phi\rangle$$

Now consider two instances of states to be copied  $|\phi\rangle, |\phi'\rangle$

Then

$$\langle\phi|\phi'\rangle = \langle\phi|\phi'\rangle\langle 0|0\rangle = (\langle\phi|\langle 0|)(|\phi'\rangle|0\rangle) = \langle\phi|\langle 0|U_{COPY}^\dagger U_{COPY}|\phi'\rangle|0\rangle = e^{i(\omega'-\omega)} (\langle\phi|\phi'\rangle)^2$$

We can remove the phase by taking the modulus squared

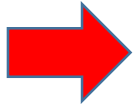
$$|\langle\phi|\phi'\rangle|^2 = |\langle\phi|\phi'\rangle|^4 \quad \text{This is only true if} \quad |\langle\phi|\phi'\rangle|^2 = 0, 1$$

# The No Cloning theorem

The cases that worked with the CNOT gate are exactly these cases:

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

$$|\langle\phi|\phi'\rangle|^2 = 0, 1$$



It is impossible to make a quantum circuit that copies a qubit in an arbitrary state. “No cloning theorem”

This was only discovered for the first time in 1970 by Park and rediscovered by Wootters, Zurek, Dieks in 1982.

Wootters & Zurek Nature 299, 802 (1982)

This gives a hint why it is quite difficult to make quantum circuits in general. The laws of quantum mechanics imposes some restrictions on what operations are allowed.

But it does include all classical algorithms, so the question is how the extra quantum “power” can be utilized.

