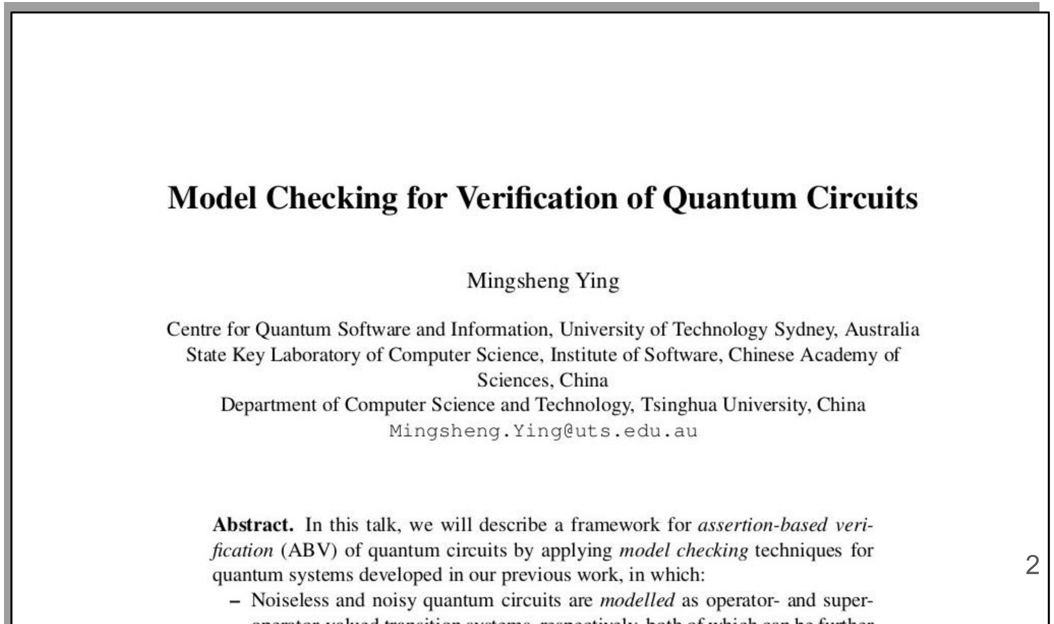
Model Checking Quantum Circuits

Approach

- Based on the paper by Ying

- A **pragmatic approach**

- We will give some context and reason about choices



Model Checking for Verification of Quantum Circuits

Mingsheng Ying

Centre for Quantum Software and Information, University of Technology Sydney, Australia
State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, China
Department of Computer Science and Technology, Tsinghua University, China
Mingsheng.Ying@uts.edu.au

Abstract. In this talk, we will describe a framework for *assertion-based verification* (ABV) of quantum circuits by applying *model checking* techniques for quantum systems developed in our previous work, in which:

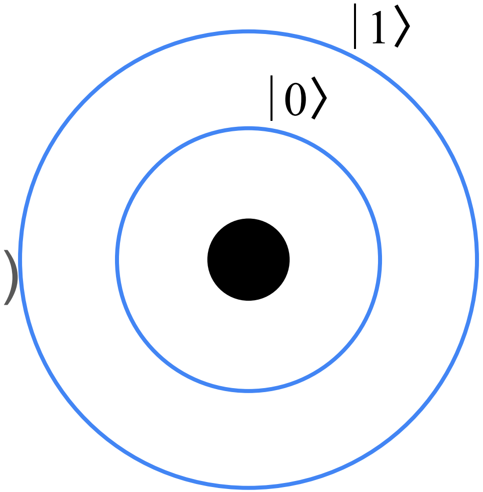
– Noiseless and noisy quantum circuits are *modelled* as operator- and super-

Content

- Brief **Introduction** to Quantum Circuits
- **Modeling** Quantum Circuits as Transition Systems
- A **Logic** for Temporal Properties on Quantum Systems
- Reduction to CTL **model checking**
- Dealing with **Mixed States**
- **Optimization** via Tensor Networks

Quantum Circuits

Qubits



- Two **classic states** $|0\rangle$ and $|1\rangle$
- Pure states (**superposition** of classic states)

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

$$a, b \in \mathbb{C} \quad |a|^2 + |b|^2 = 1$$

- **probability** of each classic state
- **wave** phase (interference)

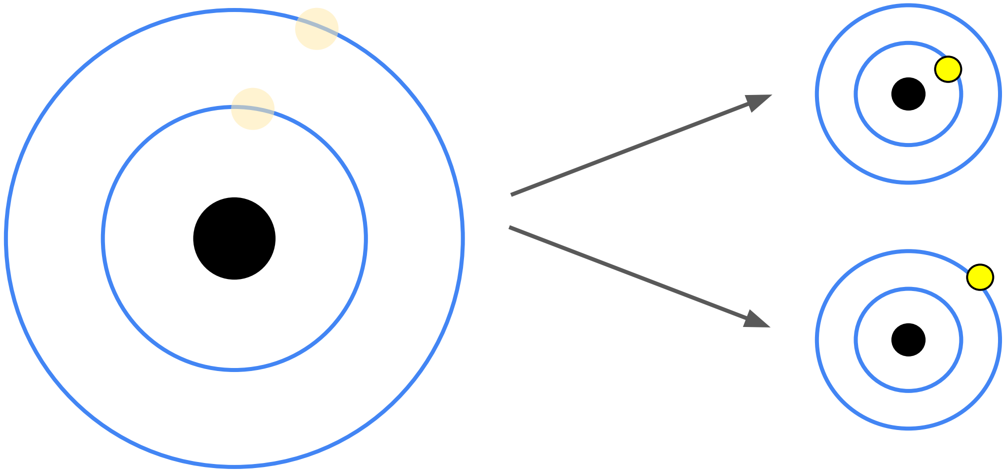
$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Measurements

Outcome on $|\varphi\rangle = a|0\rangle + b|1\rangle$

- $|0\rangle$ with probability $|a|^2$
- $|1\rangle$ with probability $|b|^2$

The system **decays** in the observed classical state



$$|\varphi'\rangle = 1|0\rangle + 0|1\rangle$$

$$|\varphi''\rangle = 0|0\rangle + 1|1\rangle$$

Dynamics of an (isolated) quantum system

$|\varphi\rangle \rightarrow |\varphi'\rangle$ with $|\varphi'\rangle = U\,|\varphi\rangle$

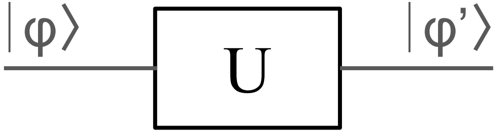
U is a transformation

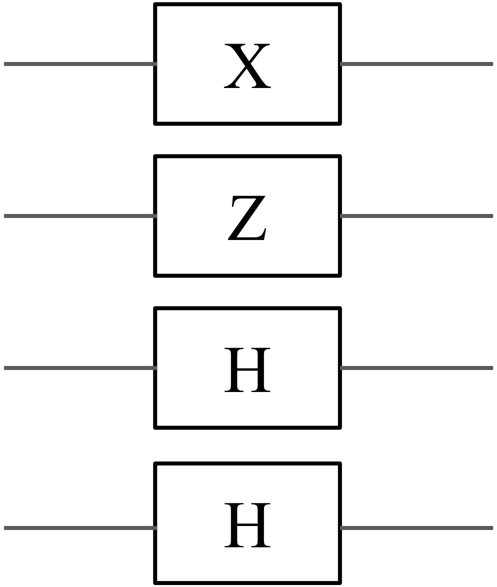
- **Linear**: $U(a|0\rangle + b|1\rangle) = a\,U|0\rangle + b\,U|1\rangle$
- **Unitary**: $U^\dagger U = U\,U^\dagger = I$

Single Qubit Transformations (Gates)

$|\varphi\rangle \longrightarrow |\varphi'\rangle$ with $|\varphi'\rangle = U\,|\varphi\rangle$

where $|\varphi\rangle = a|0\rangle + b|1\rangle$





$a|0\rangle + b|1\rangle$ — X — $b|0\rangle + a|1\rangle$

$a|0\rangle + b|1\rangle$ — Z — $a|0\rangle - b|1\rangle$

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

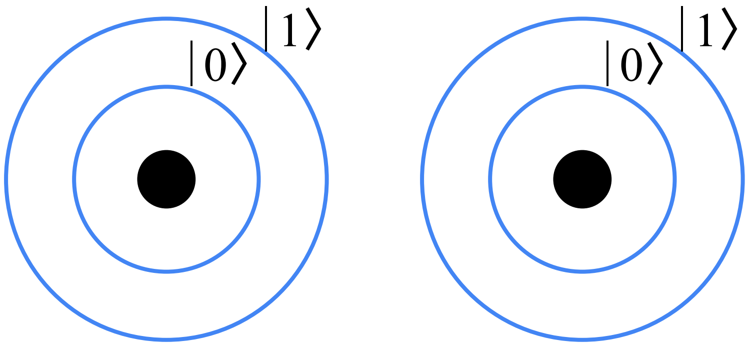
$|1\rangle$ — H — $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Multiple Qubits Systems

- **Classic states** $|00\rangle, |01\rangle, |10\rangle$ **and** $|11\rangle$
- **Pure states**

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

$$a, b, c, d \in \mathbb{C} \quad |a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$$



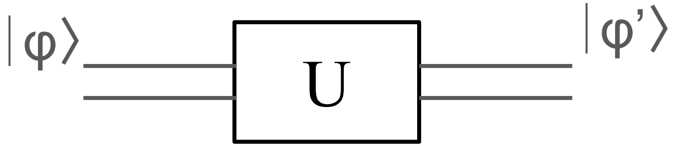
Entangled States

$$|\varphi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

- $|0\rangle$ or $|1\rangle$ with equal probability for both qubits
- BUT they **must be equal**
  - when one is measured, both of them decay

You **cannot decompose** the system in two components

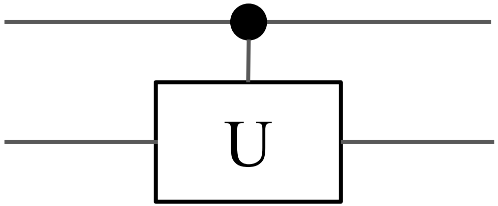
Two Qubits Transformations (Gates)



$|\varphi\rangle \longrightarrow |\varphi'\rangle$ with $|\varphi'\rangle = U\,|\varphi\rangle$
where $|\varphi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$

Only a specific case

- **control** qubit
- **target** qubit

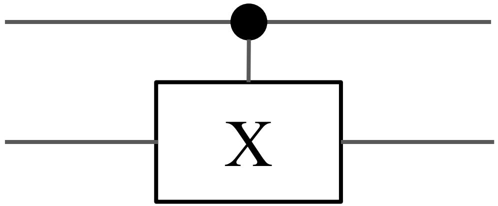


$|0,x\rangle \longrightarrow |0,x\rangle$

$|1,x\rangle \longrightarrow |1,Ux\rangle$

Controlled NOT

$|\varphi\rangle \longrightarrow |\varphi'\rangle$



$|0x\rangle \longrightarrow |0x\rangle$

$|10\rangle \longrightarrow |11\rangle$

$|11\rangle \longrightarrow |10\rangle$

CNOT can create entanglement

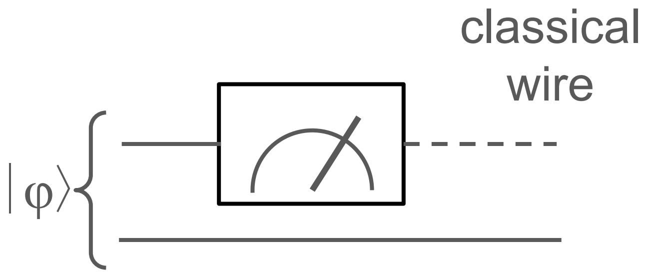
$|\varphi\rangle$ is non entangled $\quad \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$

$|\varphi'\rangle$ is entangled $\quad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Measurements (Again)

Outcome of measuring **the first** qubit of
$|\varphi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$

- $|0\rangle$ with probability $p(0) = |a|^2 + |b|^2$
- $|1\rangle$ with probability $p(1) = |c|^2 + |d|^2$

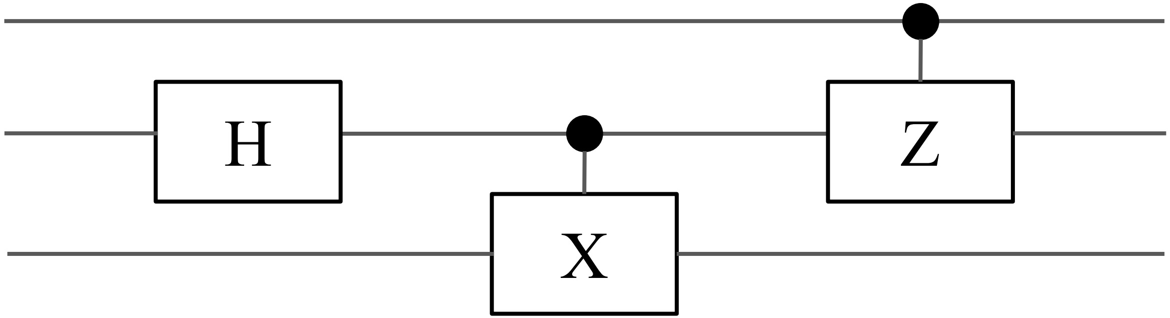


The system **decays** according to the observed classical state
Operators that applied to $|\varphi\rangle$ returns the new state:

- $M_{|0\rangle} / \sqrt{p(0)}$ where $M_{|0\rangle} = |0\rangle\langle 0|$ with $\langle 0| = (\ 1\ 0\ )$
- $M_{|1\rangle} / \sqrt{p(1)}$ where $M_{|1\rangle} = |1\rangle\langle 1|$ with $\langle 1| = (\ 0\ 1\ )$

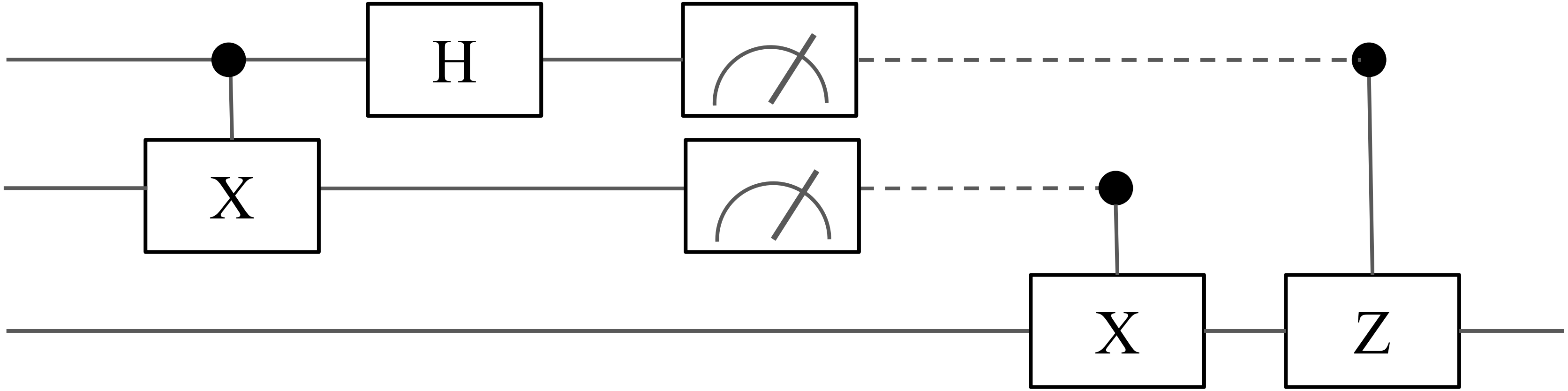
Combinatorial Quantum Circuits

Just a **composition** of gates on qubit wires
Measurements only at the end of computation



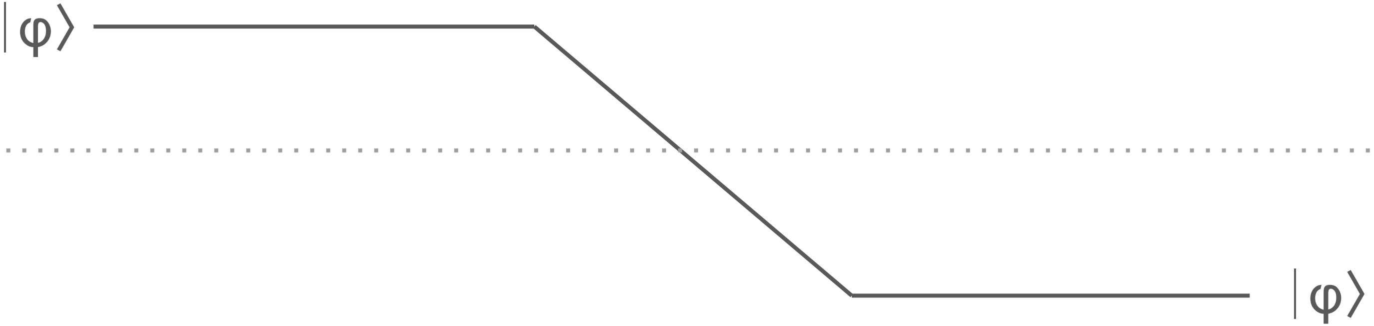
Dynamic Quantum Circuits

- **Quantum** bit wires
- **Classical** bit wires
- Quantum **Gates** (also controlled by classical bits)
- **Measurements** in arbitrary points of the computation



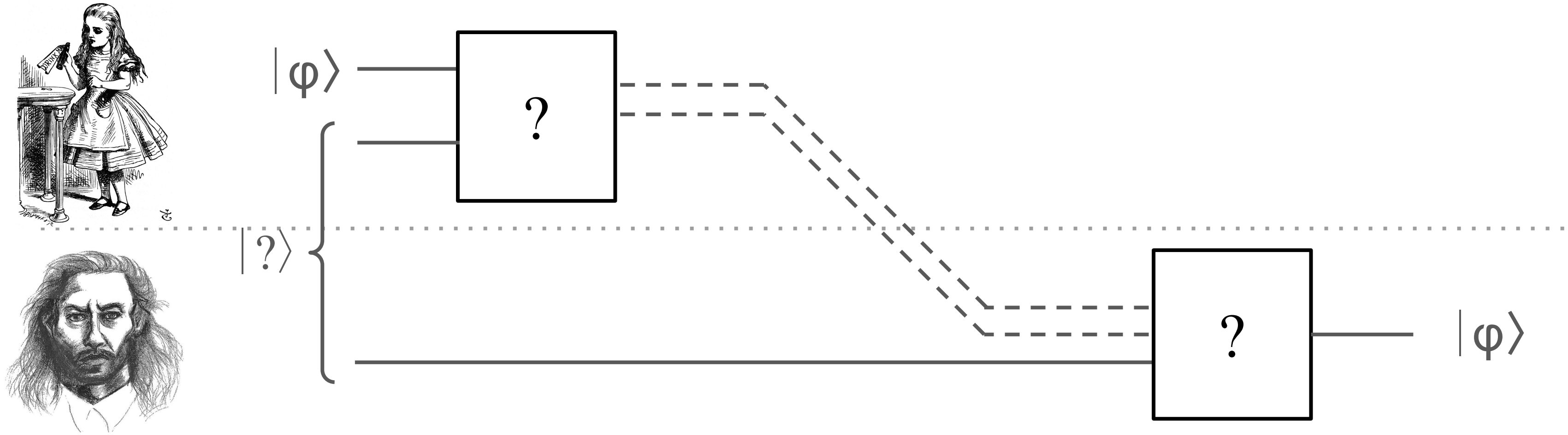
Quantum Teleportation

- Alice send $|\varphi\rangle$ to Bob using **classical communication**
- They can start with **entangled qubits**



Quantum Teleportation

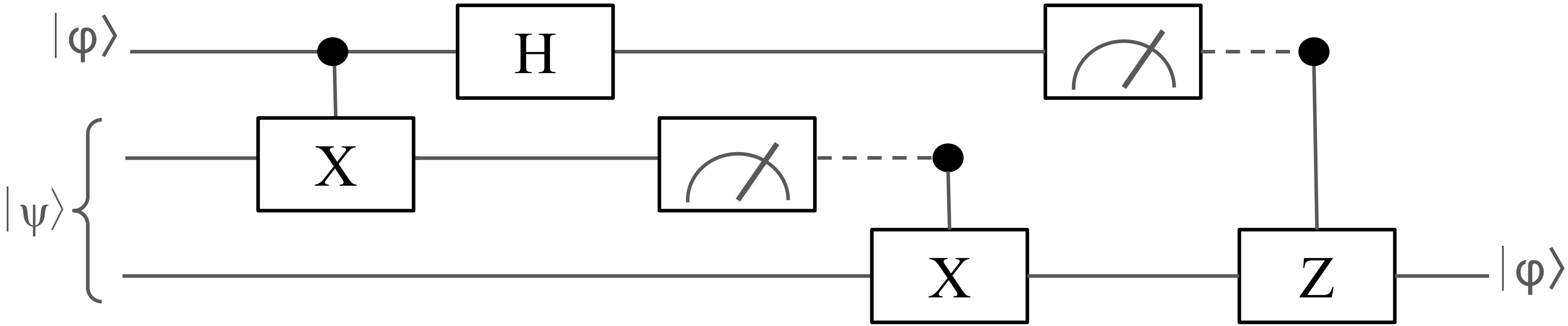
- Alice send $|\varphi\rangle$ to Bob using **classical communication**
- They can start with **entangled qubits**



Quantum Teleportation

The solution

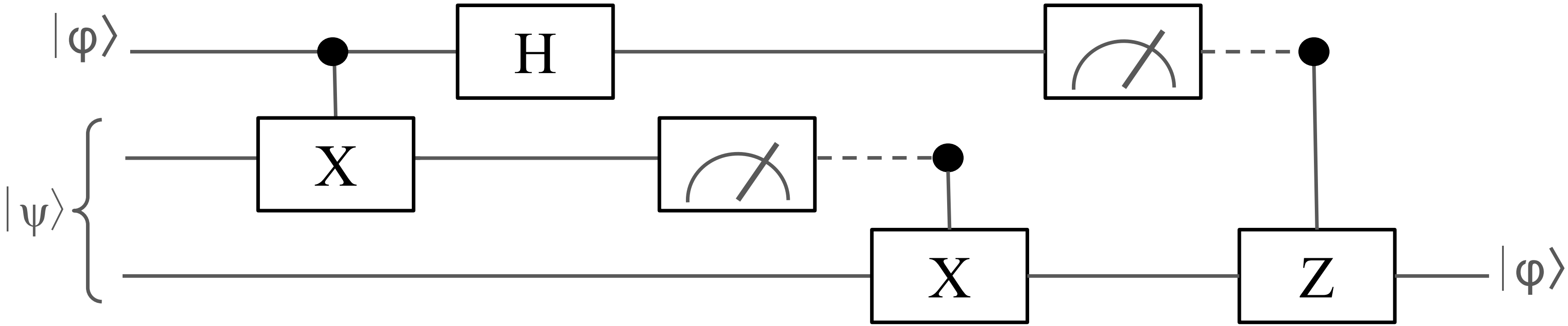
$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$



Quantum Teleportation - Explanation

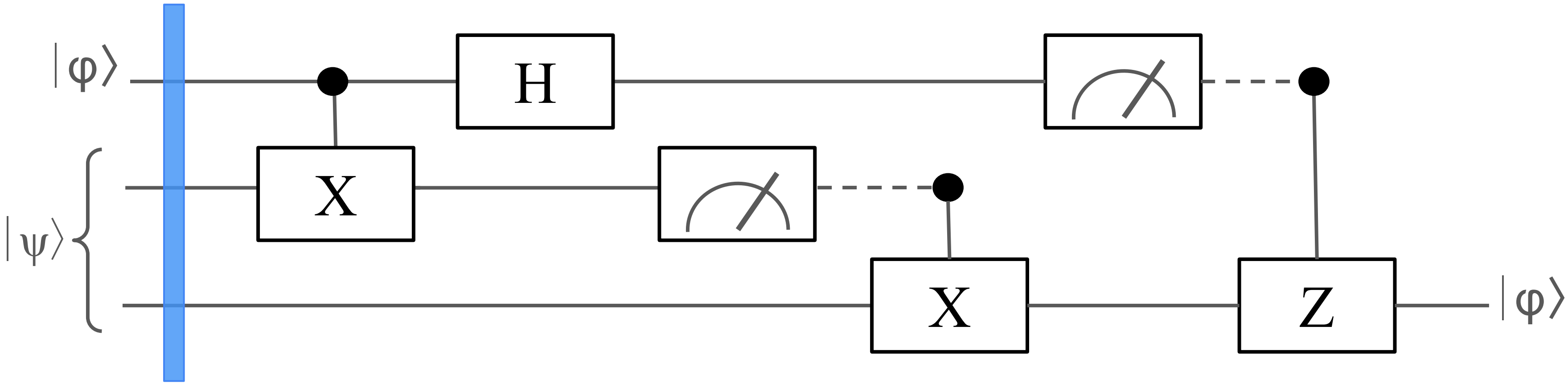
$$|\varphi\rangle = a|0\rangle + b|1\rangle$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$



Quantum Teleportation - Explanation

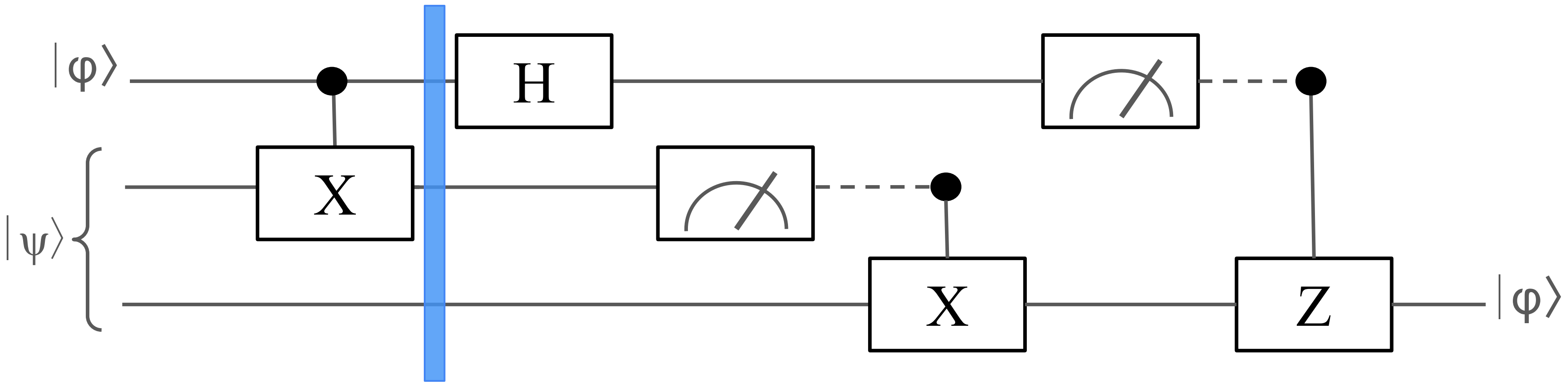
$$\frac{1}{\sqrt{2}}\left(a\,|0\rangle(\,|00\rangle + |11\rangle) + b\,|1\rangle(\,|00\rangle + |11\rangle)\right)$$



Quantum Teleportation - Explanation

$$\frac{1}{\sqrt{2}} (a\,|0\rangle\ (\ |00\rangle + |11\rangle\ ) + b\,|1\rangle\ (\ |00\rangle + |11\rangle\ ))$$

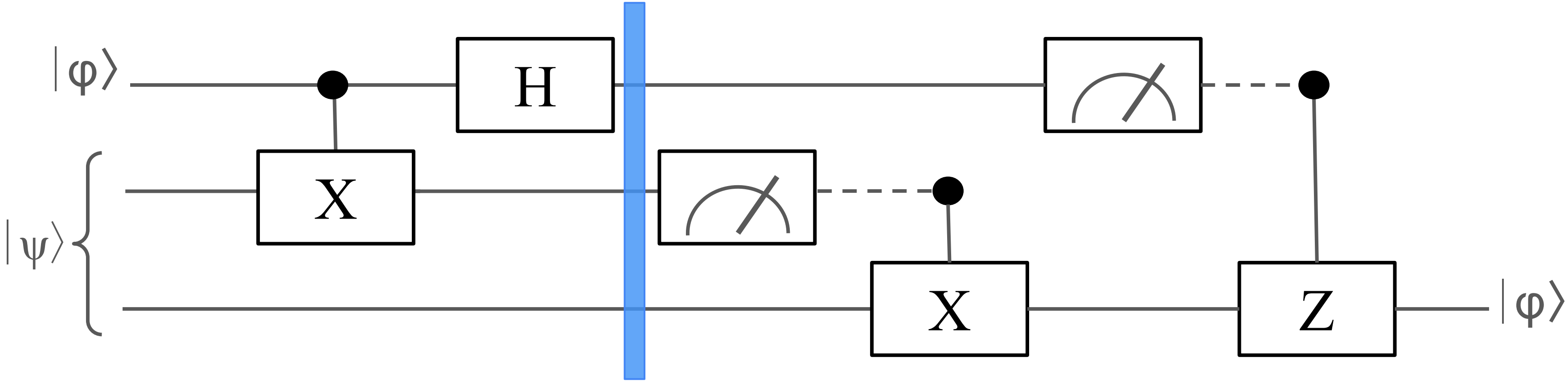
$$\frac{1}{\sqrt{2}} (a\,|0\rangle\ (\ |00\rangle + |11\rangle\ ) + b\,|1\rangle\ (\ |10\rangle + |01\rangle\ ))$$



Quantum Teleportation - Explanation

$$\frac{1}{\sqrt{2}}\left(a\boxed{|0\rangle}\left(|00\rangle+|11\rangle\right)+b\boxed{|1\rangle}\left(|10\rangle+|01\rangle\right)\right)$$

$$\frac{1}{2}\left(a\left(|0\rangle+|1\rangle\right)\left(|00\rangle+|11\rangle\right)+b\left(|0\rangle-|1\rangle\right)\left(|10\rangle+|01\rangle\right)\right)$$

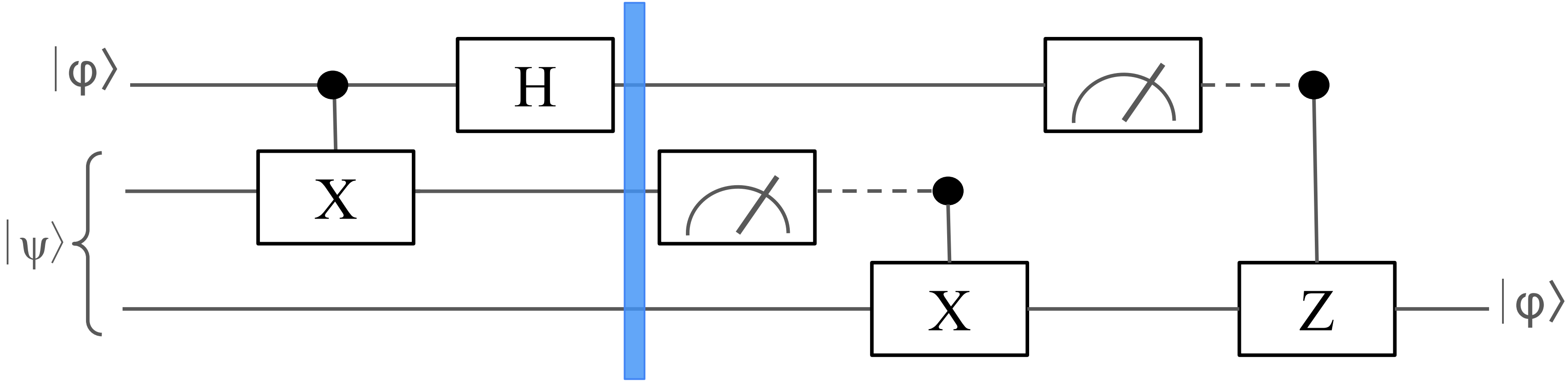


Quantum Teleportation - Explanation

$$\frac{1}{2}\,(a\,(|0\rangle + |1\rangle)\,(|00\rangle + |11\rangle) + b\,(|0\rangle - |1\rangle)(|10\rangle + |01\rangle))$$

$$\left.\frac{1}{2}\begin{array}{l}(\quad a\,(|000\rangle + |100\rangle + |011\rangle + |111\rangle) \\ \;+\, b\,(|010\rangle + |001\rangle - |110\rangle - |101\rangle))\end{array}\right\}$$

~ a single qubit



Quantum Teleportation - Explanation

$$\frac{1}{2}\Big(\, a\,(|000\rangle + |100\rangle + |011\rangle + |111\rangle)$$
$$+\, b\,(|010\rangle + |001\rangle - |110\rangle - |101\rangle)\Big)$$

Measurement of the first two qubit

$0\ \ 0 \rightarrow a|0\rangle + b|1\rangle$

$0\ \ \boxed{1} \rightarrow a|1\rangle + b|0\rangle$

$\boxed{1}\ \ 0 \rightarrow a|0\rangle - b|1\rangle$

$\boxed{1}\ \ \boxed{1} \rightarrow a|1\rangle - b|0\rangle$

X is needed

Z is needed

Models and Properties

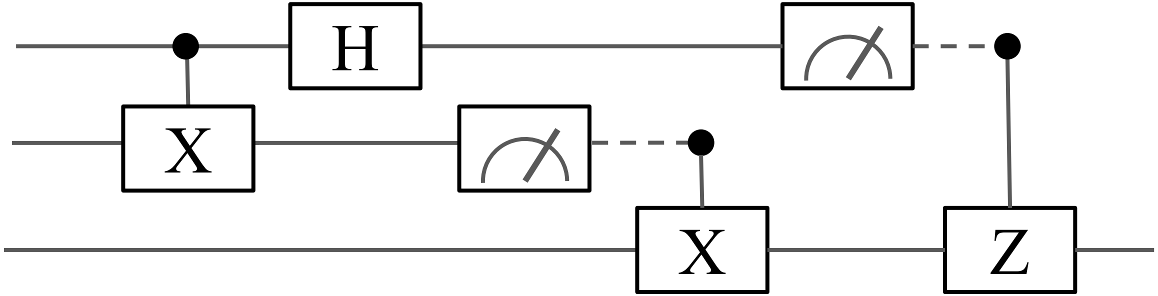
Quantum Transition System

- H - Hilbert space (**state** space for the quantum system)
- L - set of **locations** $l, l', l'', \ldots, l_0$
- l_0 - **initial** location
- T - **transitions** (l, l', U) or (l, l', M_m)

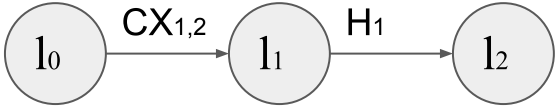
When representing Quantum Circuits

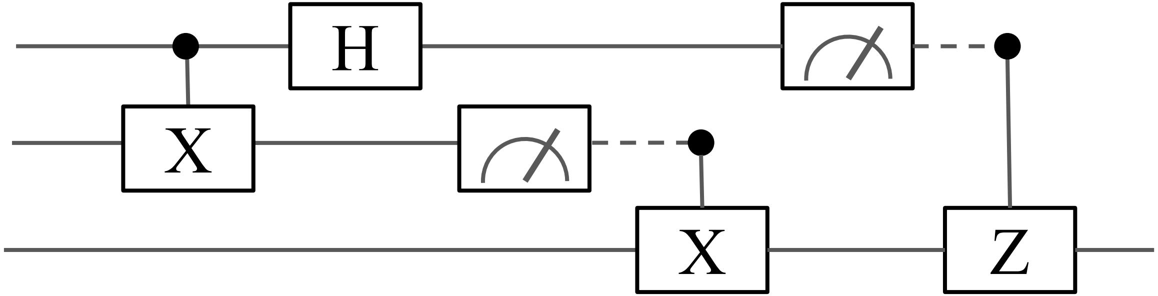
- **Transformation** gates cause **deterministic** transitions
- **Measurements** cause **nondeterministic** transitions
  - create one branch for each possible result

Quantum Teleportation as Transition System

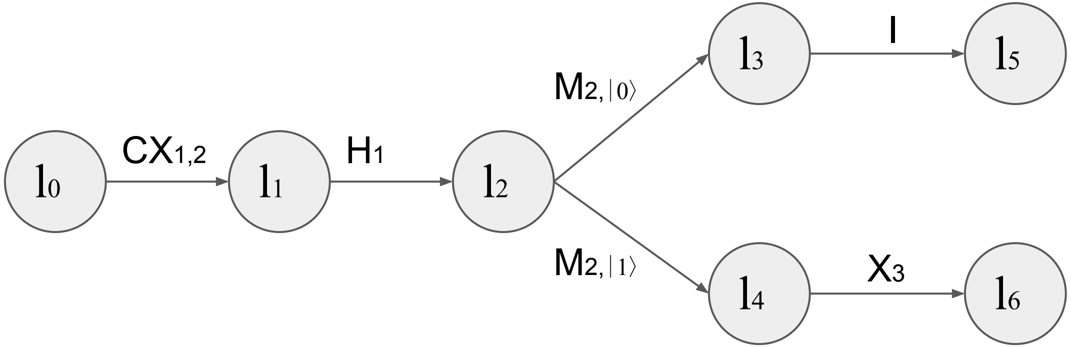


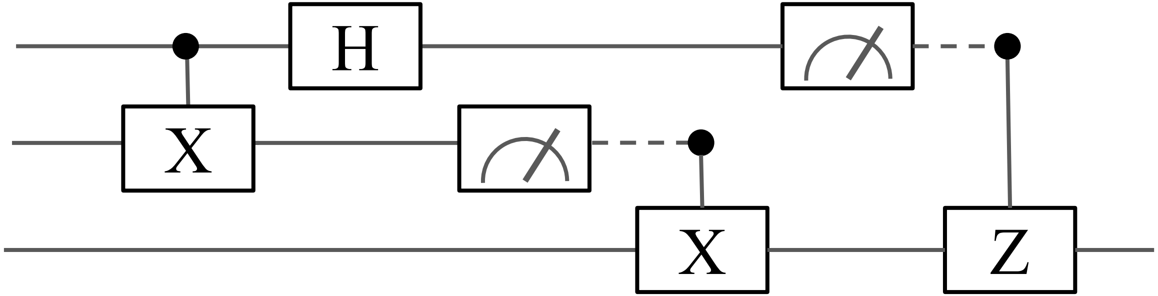
Quantum Teleportation as Transition System



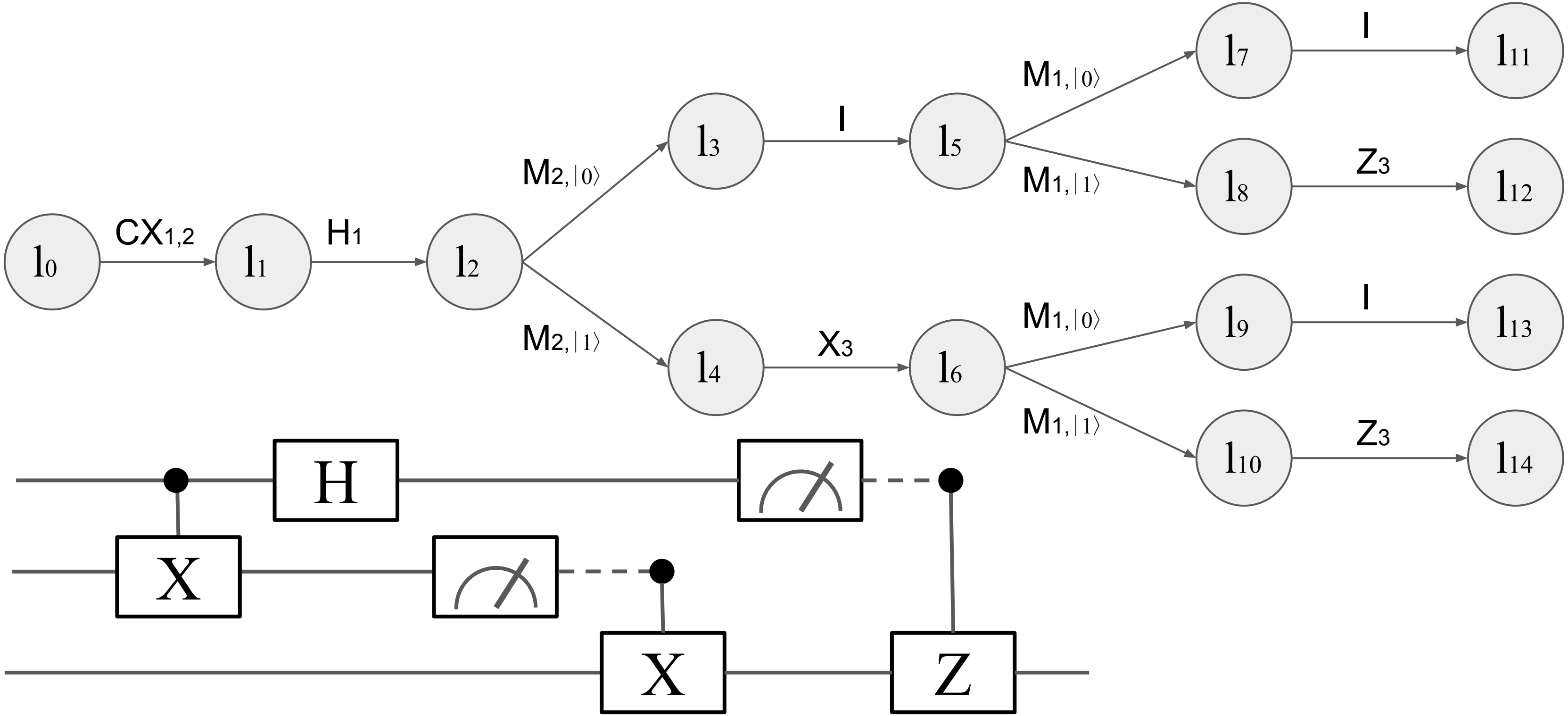


Quantum Teleportation as Transition System





Quantum Teleportation as Transition System



Birkhoff-von Neumann logic

H - state space of the quantum system (*Hilbert space*)

Atomic propositions χ - **closed subspaces** of H

e.g.

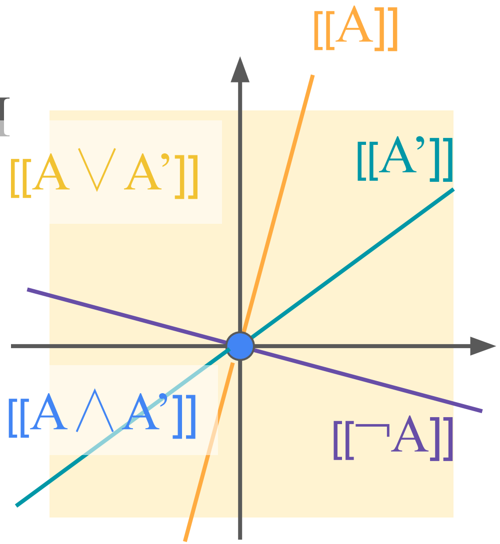
- the quantum particle has x position in the interval $[a, b]$
- the first qubit of the system is $|\varphi'\rangle$ or $-1\ |\varphi'\rangle$

$$A ::= \chi \mid \neg A \mid A \wedge A \mid A \vee A$$

Birkhoff-von Neumann logic

The semantics of a proposition A is a subset of H

$$|\varphi\rangle \vDash A \quad \text{iff} \quad |\varphi\rangle \in [[A]]$$



$$[[\chi]] = \chi$$

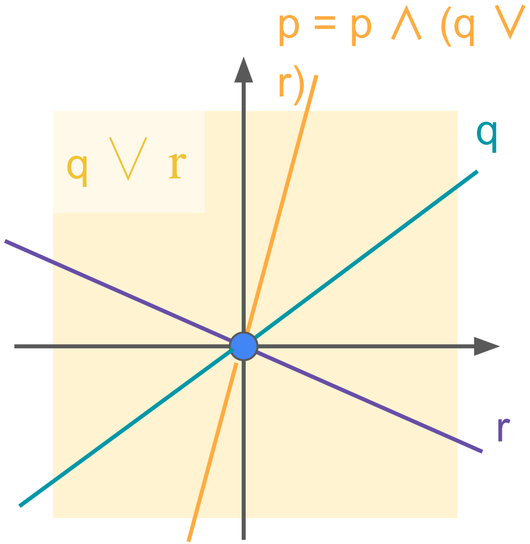
$$[[\neg A]] = \{\, |\varphi\rangle | \langle \psi | \varphi \rangle = 0,\ \psi \in [[A]] \,\}$$

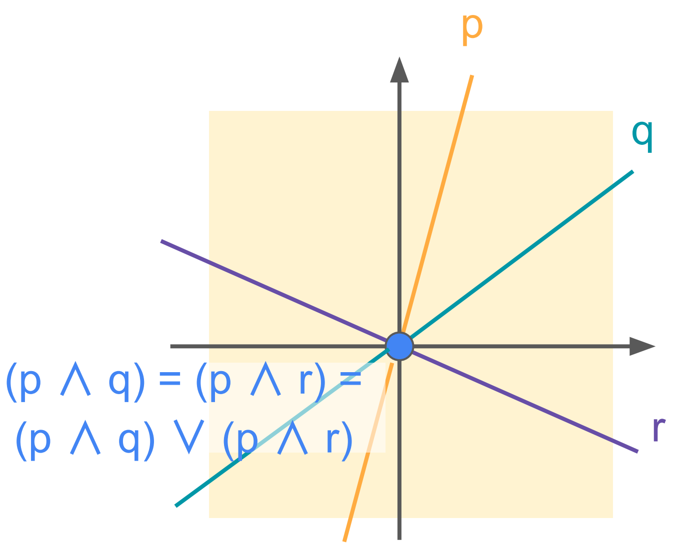
$$[[A \wedge A']] = [[A]] \cap [[A']]$$

$$[[A \vee A']] = \{\, a|\varphi\rangle + b|\psi\rangle | \ |\varphi\rangle \in [[A]],\ |\psi\rangle \in [[A']] \,\}$$

Birkhoff-von Neumann logic

$$p \wedge (q \vee r) \neq (p \wedge q) \vee (p \wedge r)$$





Temporal Extension

You can take any temporal logic with Birkhoff-von Neumann propositions instead of the classical propositions.

Computation Tree Quantum Logic

State formulas $\Phi ::= A \mid \exists\ P \mid \forall\ P \mid \neg\Phi \mid \Phi \wedge \Phi$

Path formulas $P ::= O\Phi \mid \Phi U \Phi$

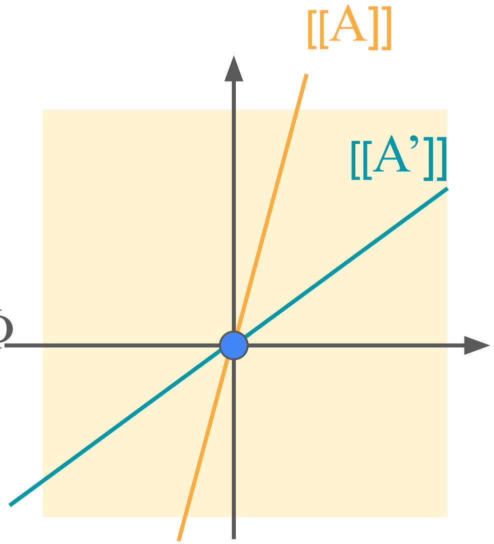
Temporal Extension

You can take any temporal logic with Birkhoff-von Neumann propositions instead of the classical propositions.

Computation Tree Quantum Logic

State formulas $\Phi ::= A \mid \exists\ P \mid \forall\ P \mid \neg\Phi \mid \Phi \wedge \Phi$

Path formulas $P ::= O\Phi \mid \Phi U \Phi$



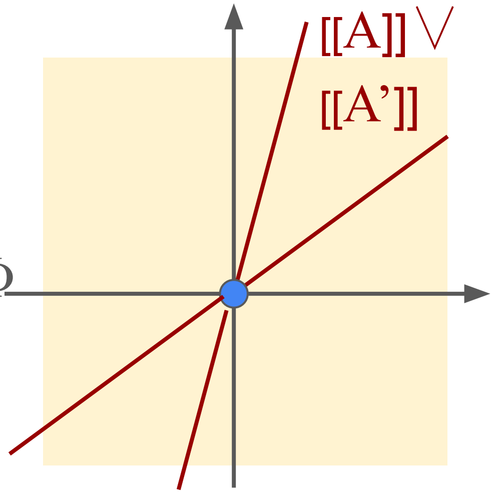
Temporal Extension

You can take any temporal logic with Birkhoff-von Neumann propositions instead of the classical propositions.

Computation Tree Quantum Logic

State formulas $\Phi ::= A \mid \exists P \mid \forall P \mid \neg\Phi \mid \Phi \wedge \Phi$

Path formulas $P ::= O\Phi \mid \Phi U \Phi$



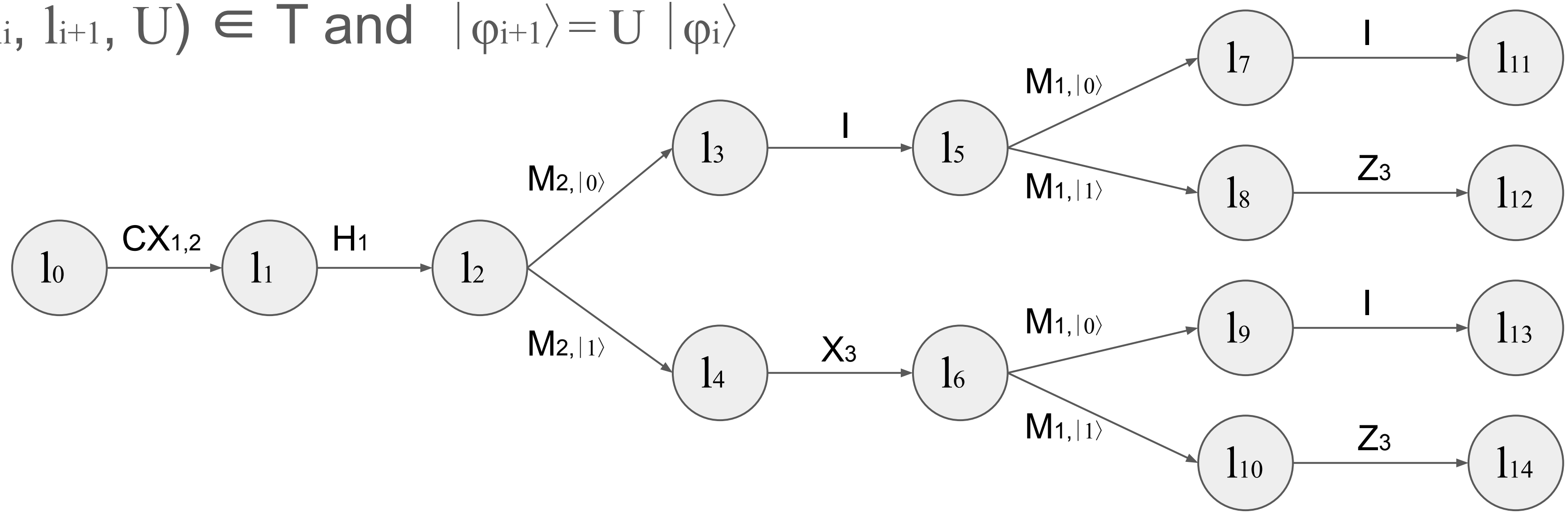
Traces of a Quantum Transition System (L, l_0, T)

Traces π are **sequences of pairs** $(l, |\varphi\rangle)$

$$(l_0, |\varphi_0\rangle)\,(l_1, |\varphi_1\rangle) \ldots (l_i, |\varphi_i\rangle) \ldots$$

s.t. for each consecutive pair $(l_i, |\varphi_i\rangle)\,(l_{i+1}, |\varphi_{i+1}\rangle)$

$(l_i, l_{i+1}, U) \in T$ and $|\varphi_{i+1}\rangle = U\,|\varphi_i\rangle$



Semantics of CTQL

$(l, |\varphi\rangle) \models A$ iff $|\varphi\rangle \in [[A]]$

$(l, |\varphi\rangle) \models \exists P$ iff $\pi \models P$ for some π starting from $(l, |\varphi\rangle)$

$(l, |\varphi\rangle) \models \forall P$ iff $\pi \models P$ for all π starting from $(l, |\varphi\rangle)$

$(l, |\varphi\rangle) \models \neg\Phi$ iff $(l, |\varphi\rangle) \not\models \Phi$

$(l, |\varphi\rangle) \models \Phi \wedge \Phi'$ iff $(l, |\varphi\rangle) \models \Phi$ and $(l, |\varphi\rangle) \models \Phi'$

$\pi \models O\Phi$ iff $\pi[1] \models O\Phi$

$\pi \models \Phi U \Phi'$ iff $\exists i.\ \pi[i] \models \Phi'$ and $\forall j < i.\ \pi[j] \models \Phi'$

Note that the satisfaction depends on the initial state $|\varphi\rangle$

Simulation-based semantics

When we check the state of the system to know if it verifies a property, **the state is not disturbed**

This means that our analysis runs on a **simulation** of the quantum circuit

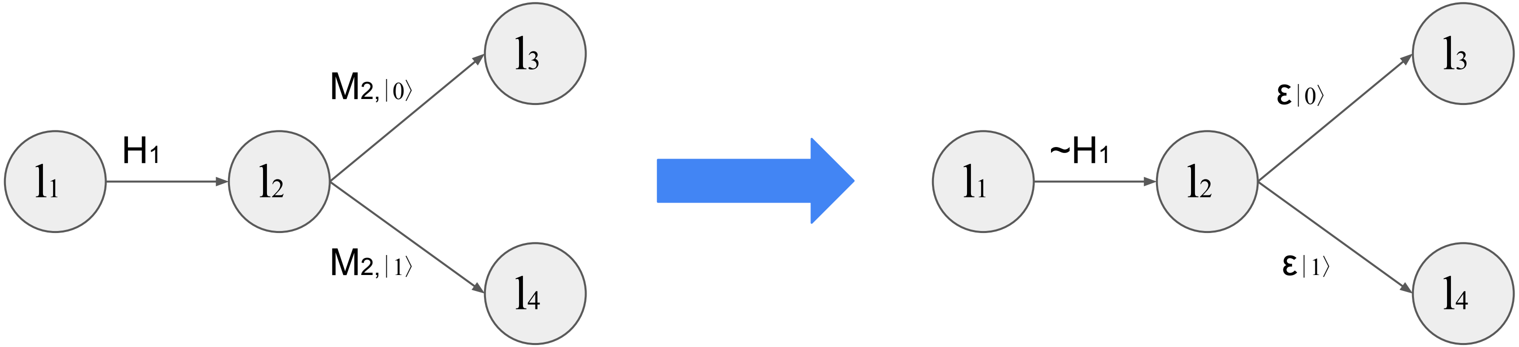
In the **measurement-based semantics**, when we check a property the system decays

Quantitative Extension of CTQL

in **Probabilistic Temporal Logic** you have $P_{[a,b]}[P]$
i.e. P is true with probability between a and b

We need to change the model

Arrows encode both transformations and (quantum) **probabilities**



Quantitative Extension of CTQL

Generalization of the classical probability measure

- **classically** we give probability $\in [0, 1]$ to an infinite path based on the probability of the finite extensions of its finite prefixes
- we can proceed **similarly** in quantum with $M \in [0, I]$

State formulas $\Phi ::= A \mid Q_{\sim M}[P] \mid \neg\Phi \mid \Phi \wedge \Phi$

Path formulas $P ::= O\Phi \mid \Phi U \Phi$

- $\sim \in \{ \sqsubseteq, \sqsupseteq, = \}$
- $M \in [0, I]$

CTQL Model Checking

CTQL Model Checking

Problem: given

- QTS $S = (H, L, l_0, T)$
- Initial state $|\varphi\rangle$
- CTQL state formula Φ

check $(S, |\varphi\rangle) \models \Phi$ [i.e. $(l_0, |\varphi\rangle) \models \Phi$]

We build a **classical** Transition System $S'_{|\varphi\rangle}$ s.t.

$(S, |\varphi\rangle) \models \Phi$ iff $S'_{|\varphi\rangle} \models \Phi$

CTQL reduced to CTL

$S'_{|\varphi\rangle} = (L', (l_0, |\varphi\rangle), T', Ap, Lab)$

where:

- $L' = L \times H$
- $((l_i, |\varphi_i\rangle), (l_j, |\varphi_j\rangle)) \in T'$ iff $(l_i, l_j, U) \in T$ and $|\varphi_j\rangle = U|\varphi_i\rangle$
- Ap is the set of Birkhoff-von Neumann propositions
- $A \in Lab(l_i, |\varphi_i\rangle)$ iff $|\varphi_i\rangle \vDash A$

Theorem

$(S, |\varphi\rangle) \vDash \Phi$ iff $S'_{|\varphi\rangle} \vDash \Phi$

CTQL reduced to CTL

$S'_{|\varphi\rangle} = (L', (l_0, |\varphi\rangle), T', Ap, Lab)$

where:

- $L' = L \times H$ (Actually just the reachable configurations)
- $((l_i, |\varphi_i\rangle), (l_j, |\varphi_j\rangle)) \in T'$ iff $(l_i, l_j, U) \in T$ and $|\varphi_j\rangle = U|\varphi_i\rangle$
- Ap is the set of Birkhoff-von Neumann propositions
- $A \in Lab(l_i, |\varphi_i\rangle)$ iff $|\varphi_i\rangle \models A$

Theorem

$(S, |\varphi\rangle) \models \Phi$ iff $S'_{|\varphi\rangle} \models \Phi$

Reachability Analysis of Quantum Circuits

A simpler case:

the system evolves as described by ε (Quantum Markov Chain)

The image of a subspace X under ε is

$$\varepsilon(X) = \mathrm{span}\left(\bigcup_{|\varphi\rangle \in X} \mathrm{supp}(\varepsilon(|\varphi\rangle\langle\varphi|))\right)$$

We actually need the states reachable with $\varepsilon^0, \varepsilon^1, \varepsilon^2, \varepsilon^3 \ldots$

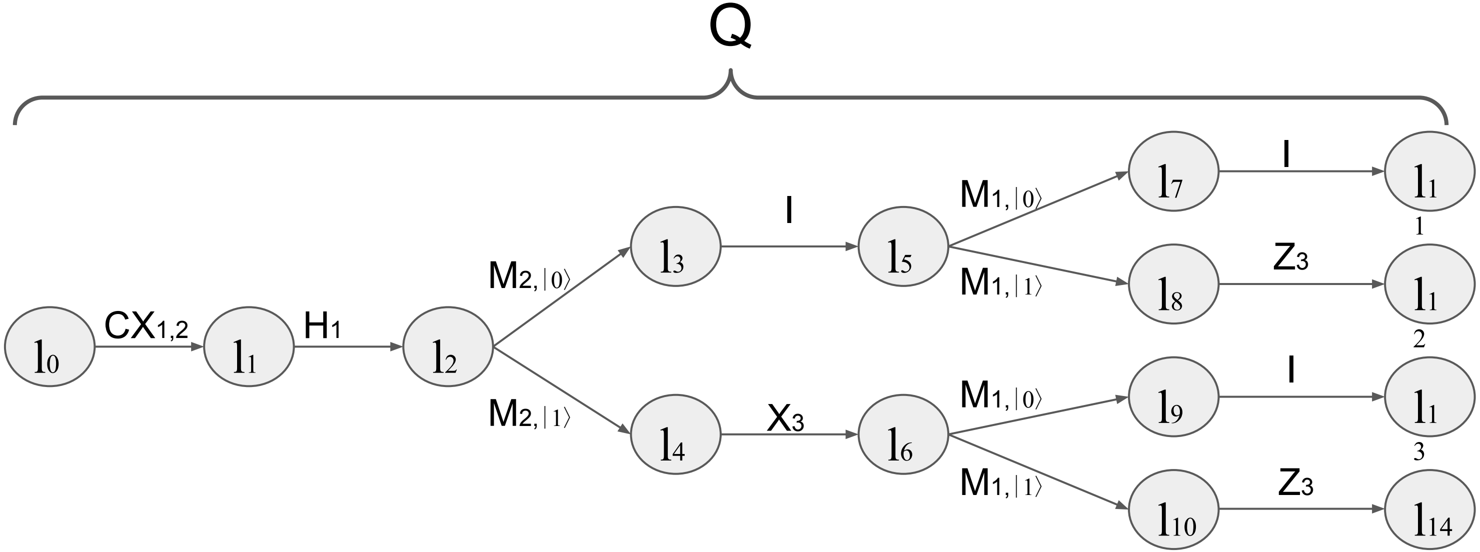
Theorem

$$\mathrm{span}\left(\bigcup_{i=0\ldots d} \mathrm{supp}(\varepsilon^i(\{|\varphi\rangle\}))\right) = \mathrm{supp}\left(\sum_{i=0\ldots d} \varepsilon^i(\{|\varphi\rangle\})\right)$$

Reachability Analysis of Quantum Circuits

L’ = configurations reachable from (l_0, $|\varphi\rangle$)

Compute the reachable subspace w.r.t. Q ∋ (l, l’, ε)



Something More

Dealing with Mixed States

- **Pure states** (superposition of classic states)

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

  $a, b \in \mathbb{C} \quad |a|^2 + |b|^2 = 1$
- **Mixed states** are **classical mixture** of pure quantum states

  $\{ (|\varphi_i\rangle, \ p_i) \}$ s.t. $\forall$i. $p_i \geq 1$ and $\sum_i \ p_i = 1$
  - The system is in state $|\varphi_i\rangle$ with probability p_i

Represent missing information and not isolated states
e.g. one qubit of an entangled pair

Dynamics of Mixed States

- Mixed states are represented by **density matrices** ρ

  $\{ (|\varphi_i\rangle, \ p_i) \}$

  $\rho = \sum_i \ p_i \ |\varphi_i\rangle\langle\varphi_i|$
- Isolated System Evolution $\rho \rightarrow \rho'$
  - Unitary transformation $\rho' = U \rho U^\dagger$
  - Measurement $\rho' = M_m \rho M_m^\dagger / tr (M_m^\dagger M_m \rho)$
- Open System Evolution $\rho' = \varepsilon (\rho)$
  - ε is a Linear Transformation (super-operator) s.t. …

Super-operators

- Can represent Unitary Operators U

  $$\varepsilon(\rho) = U \rho U^\dagger$$

- Can represent the decay for a measurement with result m

  $$\varepsilon_m(\rho) = M_m \rho M_m^\dagger$$

- Can represent the decay for a measurement

  $$\varepsilon(\rho) = \sum_m M_m \rho M_m^\dagger$$

- **Can represent quantum noises and noisy gates**

Open Systems

- Given a composite system $S + E$ in state $\rho_{S+E} \in H_{S+E}$
- The state of the **subsystem** S is defined as

$$\rho_S = tr_E (\rho_{S+E})$$

- And its evolution is according a super-operator ε

Open Systems

Closed Composite System

Open Subsystem

$$
\begin{tikzcd}[column sep=huge, row sep=huge]
\rho_{S+E}(t_0) \arrow[r, shift left, "\varepsilon_U"] \arrow[d, "\mathrm{tr}_E"'] & \rho_{S+E}(t_1) \arrow[l, shift left, "\varepsilon_U^{-1}"] \arrow[d, "\mathrm{tr}_E"'] \\
\rho_S(t_0) \arrow[r, "\varepsilon"] & \rho_S(t_1)
\end{tikzcd}
$$

Crossing the line causes a lost of information:you cannot go back

Model Checking with Mixed States

- Everything seen so far **works with mixed states** ρ
  - In quantum transition systems:
    arrows are labeled with super-operators ε
  - In Quantum Logic: $\rho \models A \quad \text{iff} \quad \text{supp}(\rho) \subseteq [[A]]$
  - In CTQL: $(l, \rho) \models A \quad \text{iff} \quad \text{supp}(\rho) \subseteq [[A]]$

- **We can model check noisy circuits!**

Optimization via Tensor Networks

A Tensor is a **multidimensional matrix with named indexes**.

Formally:

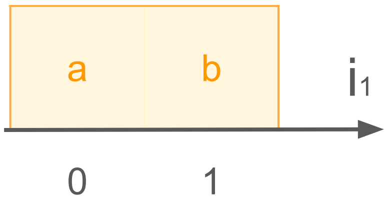
Given a set of indexes $\bar{I} = (i_1, \ldots i_n)$,

a Tensor is a mapping

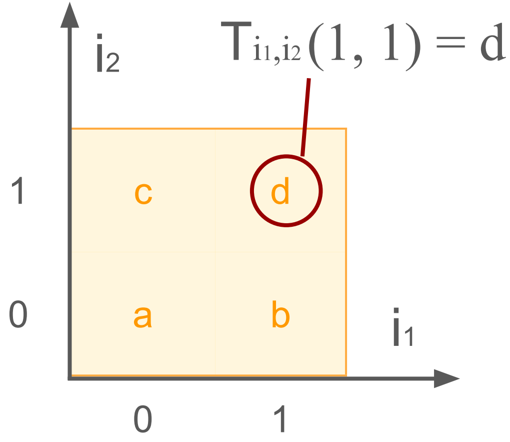
$$T : \{0, 1\}^{\bar{I}} \longrightarrow \mathbb{C}$$

Tensor Representation of Quantum States

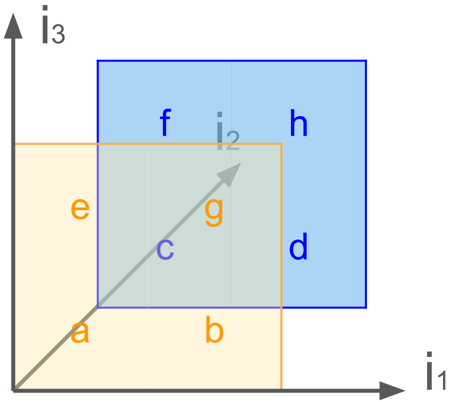
- Single qubit
  $|\varphi\rangle = a|0\rangle + b|1\rangle$



- Pair of qubits
  $|\varphi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$



- Triplet of qubits
  $|\varphi\rangle = a|000\rangle + b|001\rangle + c|010\rangle + d|011\rangle$
  $+ \ e|100\rangle + f|101\rangle + g|110\rangle + h|111\rangle$



Tensor Representation of Gates

Gates on n qubits can be represented as tensors with indices $(\underbrace{i_1, \ldots i_n}_{\text{inputs}}, \underbrace{i_1', \ldots i_n'}_{\text{outputs}})$

Tensor Network is a hyper-graph with

- Tensors as nodes
- hyper-edges are the **shared indexes**

Tensor Contraction

A generalization of Matrix product

- T_1 on indices $\bar{I}_1\bar{I}_c$
- T_2 on indices $\bar{I}_2\bar{I}_c$

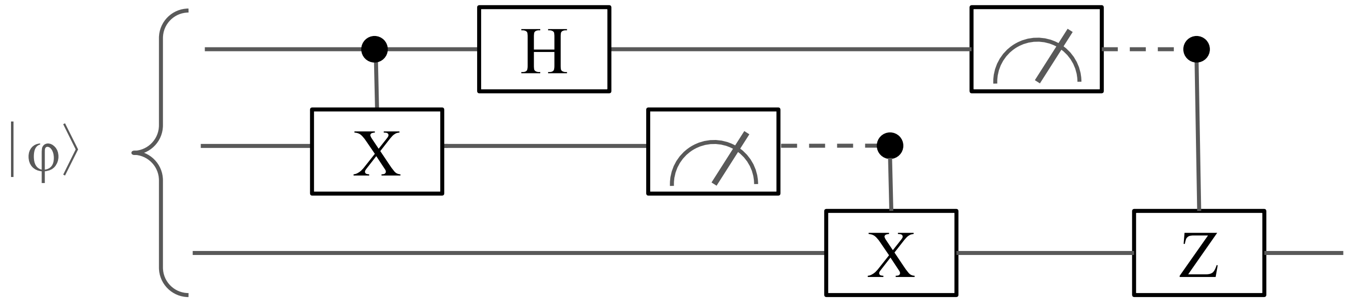
Contraction returns a Tensor T' on indices $\bar{I}_1\bar{I}_2$

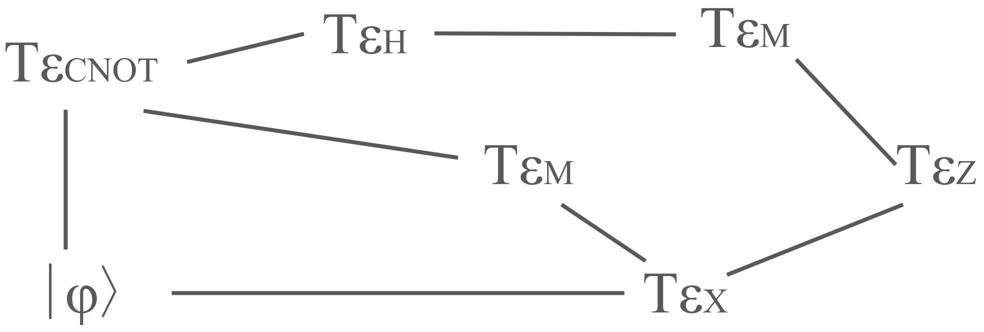
$$T'_{\bar{I}_1\bar{I}_2}(\bar{a},\bar{e}) = \sum_{\bar{o}\in\{0,1\}^{\bar{I}_c}} T_{\bar{I}_1\bar{I}_c}(\bar{a},\bar{o}) \cdot T_{\bar{I}_2\bar{I}_c}(\bar{e},\bar{o})$$

- **Composing** transformations
- **Applying** transformation to qubits

In any order

Tensor Contraction





Why Tensor Networks

- Contraction cost depends on the **actual information** stored in the system (linked to entanglement)
- You can choose **any order**
- Thus you can **exploit regularity and locality** in the quantum circuit

Conclusions

Conclusions

- We have seen
  - Quantum Transition Systems
  - CTQL
  - Reduction to CTL model checking
  - Works with Open Systems and noisy gates
  - Optimization via Tensor Networks
- With a small comparison w.r.t.
  - More expressive modeling and logics

Bibliography

- ***Model Checking for Verification of Quantum Circuits***, by Mingsheng Ying. arXive 2021

- ***Model Checking Quantum Systems, Principles and Algorithms***, by Mingsheng Ying and Yuan Feng. Cambridge University Press 2021

- ***Quantum logic, A brief outline***, by Karl Svozi. arXive 2005