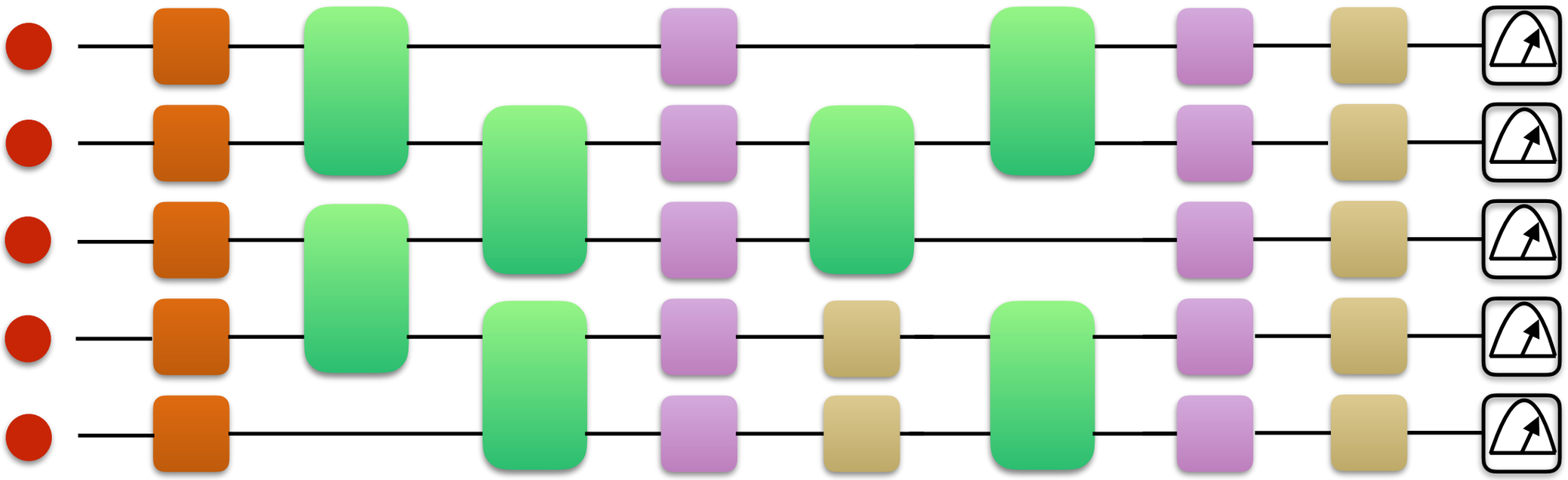
Quantum Computation & Cryptography
Day 2

How to make a physical theory 101

Andru Gheorghiu

Our goal today will be to understand this…



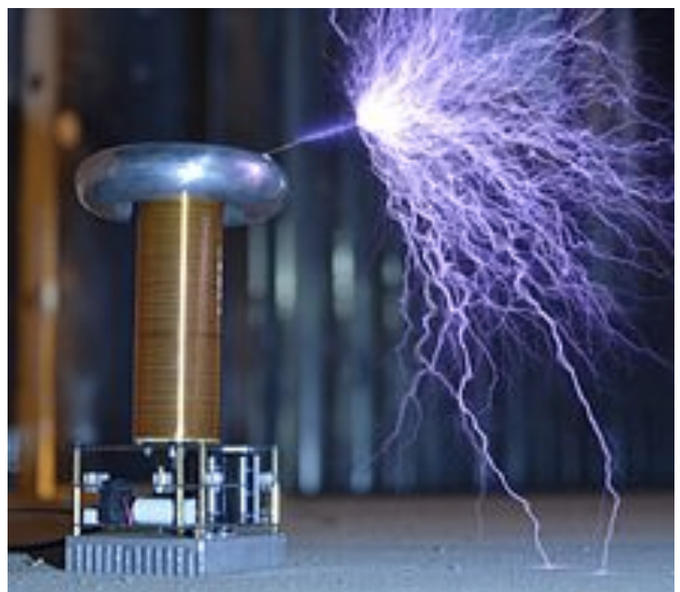
Physics

Observation

$$\nabla \cdot \mathbf{E} = \frac{\rho_V}{\varepsilon} \qquad \nabla \times \mathbf{E} = -\mu \frac{\partial \mathbf{H}}{\partial t}$$

$$\nabla \cdot \mathbf{H} = 0 \qquad \nabla \times \mathbf{H} = \varepsilon \frac{\partial \mathbf{E}}{\partial t} + \sigma \mathbf{E}$$

Mathematical modelling



Experiments

Characteristics of a physical theory

- Expressed in mathematics
- Ideally all aspects of theory are rigorously defined and consistent
- Can be used to make testable predictions

Newtonian (classical) mechanics

Quantum mechanics

Relativity theory

Electrodynamics

Thermodynamics

Quantum field theory

Quantum gravity?

A physicist's dream theory

States	Representing the state of the system	$\mathcal{S} \quad s \in \mathcal{S}$
Transformations	Changing states in time	$\mathcal{S} \to \mathcal{S}$
Composition	The state of multiple systems	$\mathcal{S}_{AB} = \mathcal{S}_A \otimes \mathcal{S}_B$
Observation (measurement)	Observing physical properties	$\mathcal{S} \to \mathbb{R}$ $\mathcal{S} \times \mathbb{R} \to [0, 1]$

A physicist's dream theory

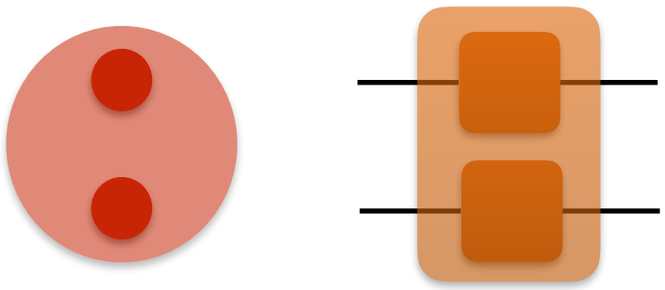
States

$\mathcal{S} \qquad s \in \mathcal{S}$

Transformations

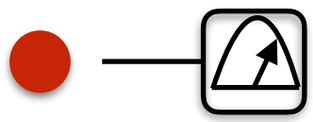
$\mathcal{S} \to \mathcal{S}$

Composition



$\mathcal{S}_{AB} = \mathcal{S}_A \otimes \mathcal{S}_B$

Observation (measurement)



$\mathcal{S} \to \mathbb{R}$

$\mathcal{S} \times \mathbb{R} \to [0, 1]$

Classical mechanics

States $\mathcal{S} = \mathbb{R}^{dN}$ $s = (\mathbf{q}_1, \mathbf{q}_2, ..., \mathbf{q}_N, \mathbf{p}_1, \mathbf{p}_2, ...\mathbf{p}_N)$

$\mathbf{q}_i = (q_i^1, q_i^2, ...q_i^d)$ $\mathbf{p}_i = (p_i^1, p_i^2, ...p_i^d)$

Transformations $H(\mathbf{q}_1, ...\mathbf{q}_N, \mathbf{p}_1, ...\mathbf{p}_N, t)$

$$\frac{dp_i^j}{dt} = -\frac{\partial H}{\partial q_i^j} \qquad \frac{dq_i^j}{dt} = \frac{\partial H}{\partial p_i^j}$$

Composition

Observation (measurement)

Classical mechanics

States $\mathcal{S} = \mathbb{R}^{dN}$ $s = (\mathbf{q}_1, \mathbf{q}_2, ..., \mathbf{q}_N, \mathbf{p}_1, \mathbf{p}_2, ...\mathbf{p}_N)$

$\mathbf{q}_i = (q_i^1, q_i^2, ...q_i^d)$ $\mathbf{p}_i = (p_i^1, p_i^2, ...p_i^d)$

Transformations $H(\mathbf{q}_1, ...\mathbf{q}_N, \mathbf{p}_1, ...\mathbf{p}_N, t)$

$$\frac{d\mathbf{p}}{dt} = -\frac{\partial H}{\partial \mathbf{q}} \qquad \frac{d\mathbf{q}}{dt} = \frac{\partial H}{\partial \mathbf{p}}$$

Composition

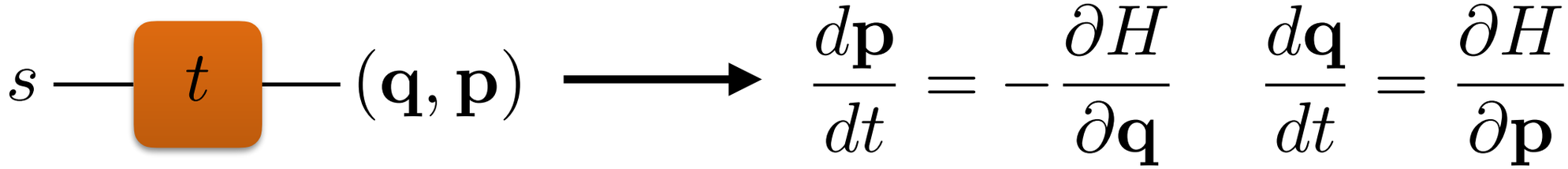
Observation (measurement)

Classical mechanics

States $\mathcal{S} = \mathbb{R}^{dN}$ $s = (\mathbf{q}_1, \mathbf{q}_2, ..., \mathbf{q}_N, \mathbf{p}_1, \mathbf{p}_2, ...\mathbf{p}_N)$

$\mathbf{q}_i = (q_i^1, q_i^2, ...q_i^d)$ $\mathbf{p}_i = (p_i^1, p_i^2, ...p_i^d)$

Transformations $H(\mathbf{q}_1, ...\mathbf{q}_N, \mathbf{p}_1, ...\mathbf{p}_N, t)$



Composition

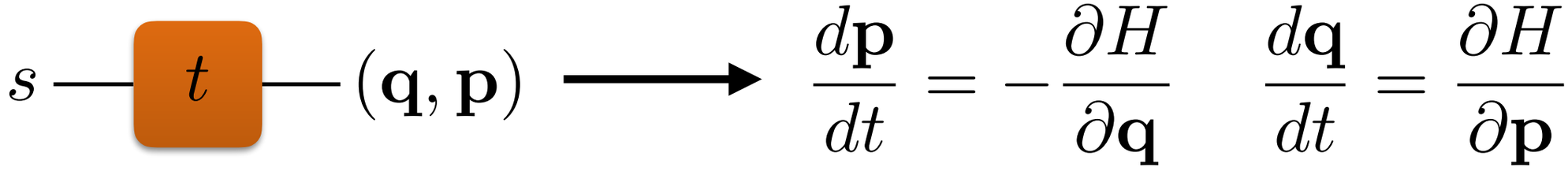
Observation (measurement)

Classical mechanics

States $\mathcal{S} = \mathbb{R}^{dN}$ $s = (\mathbf{q}_1, \mathbf{q}_2, ..., \mathbf{q}_N, \mathbf{p}_1, \mathbf{p}_2, ...\mathbf{p}_N)$

$\mathbf{q}_i = (q_i^1, q_i^2, ...q_i^d)$ $\mathbf{p}_i = (p_i^1, p_i^2, ...p_i^d)$

Transformations $H(\mathbf{q}_1, ...\mathbf{q}_N, \mathbf{p}_1, ...\mathbf{p}_N, t)$



Composition $\mathcal{S}_{AB} = \mathcal{S}_A \times \mathcal{S}_B$ $s_{AB} = s_A \cdot s_B$

Observation (measurement)

Pretty much any “well-behaved” function of the form:

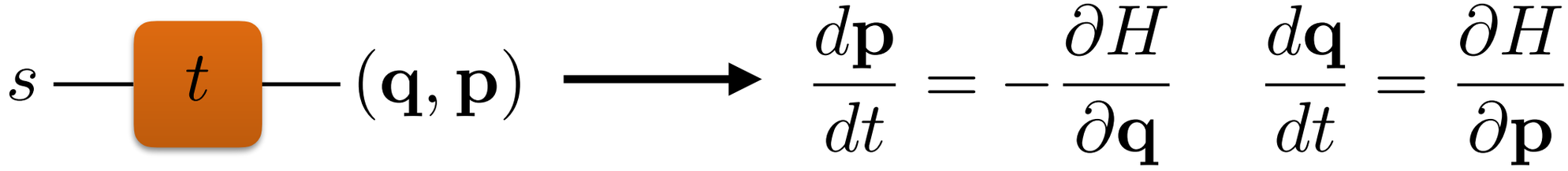
$f : \mathcal{S} \to \mathbb{R}$

Classical mechanics

States $\mathcal{S} = \mathbb{R}^{dN}$ $s = (\mathbf{q}_1, \mathbf{q}_2, ..., \mathbf{q}_N, \mathbf{p}_1, \mathbf{p}_2, ...\mathbf{p}_N)$

$\mathbf{q}_i = (q_i^1, q_i^2, ...q_i^d)$ $\mathbf{p}_i = (p_i^1, p_i^2, ...p_i^d)$

Transformations $H(\mathbf{q}_1, ...\mathbf{q}_N, \mathbf{p}_1, ...\mathbf{p}_N, t)$



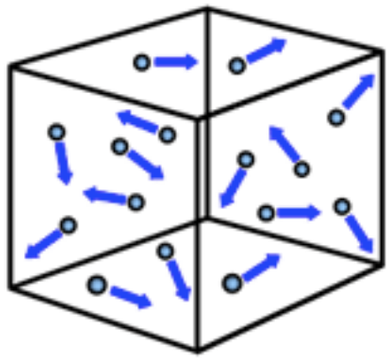
Composition $\mathcal{S}_{AB} = \mathcal{S}_A \times \mathcal{S}_B$ $s_{AB} = s_A \cdot s_B$

Observation (measurement)

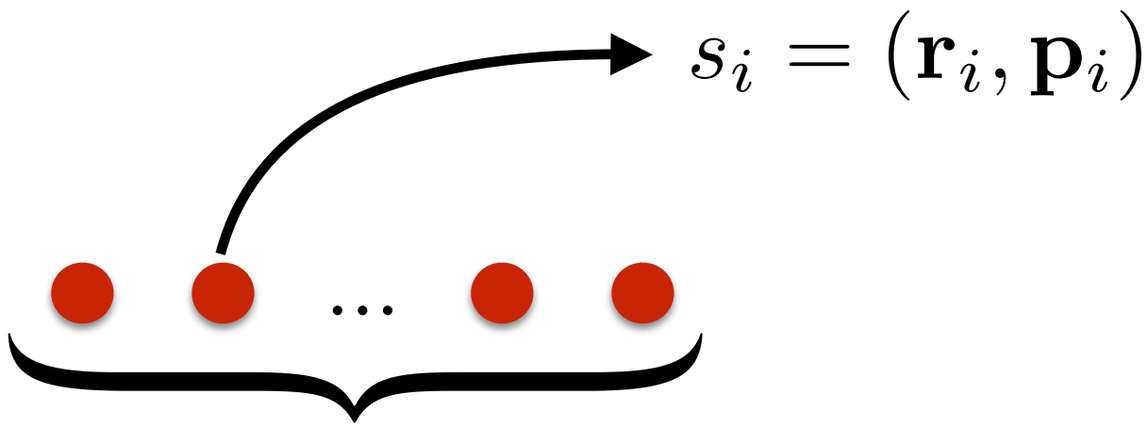
E.g.

$Pos_i^j(s) = q_i^j$ $Mom_i^j(s) = p_i^j$

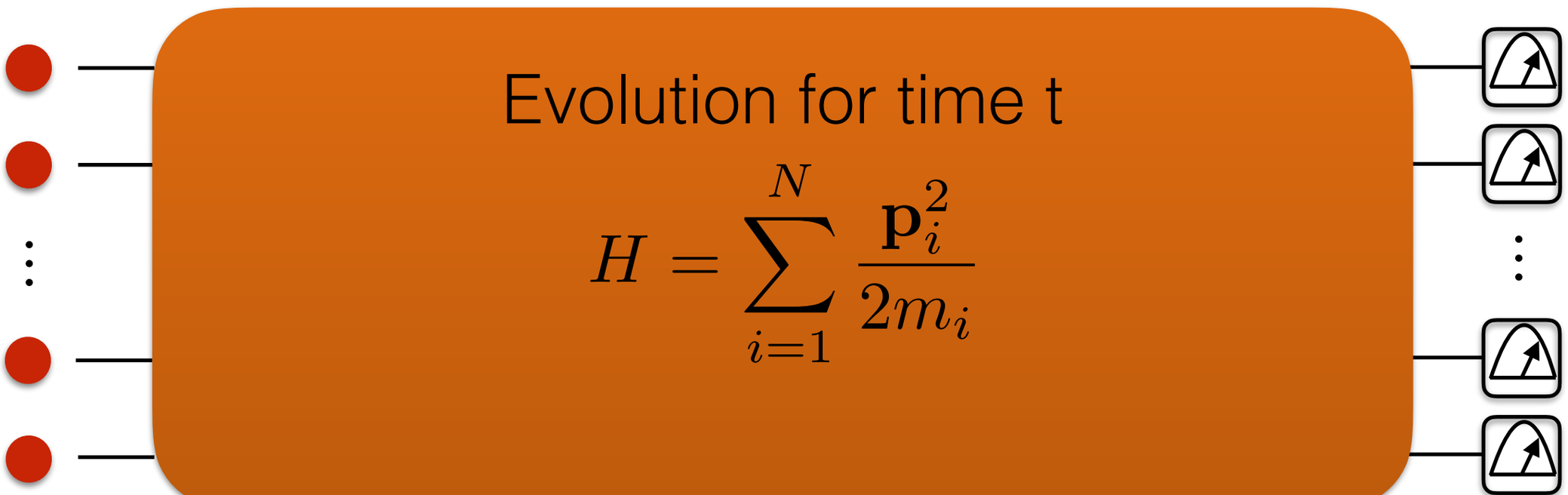
Example



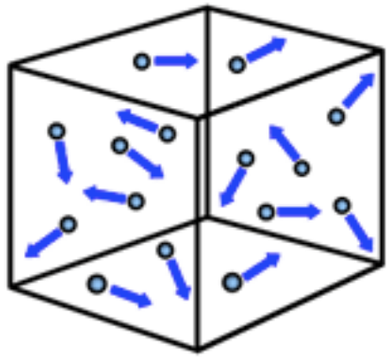
N particles
non-interacting



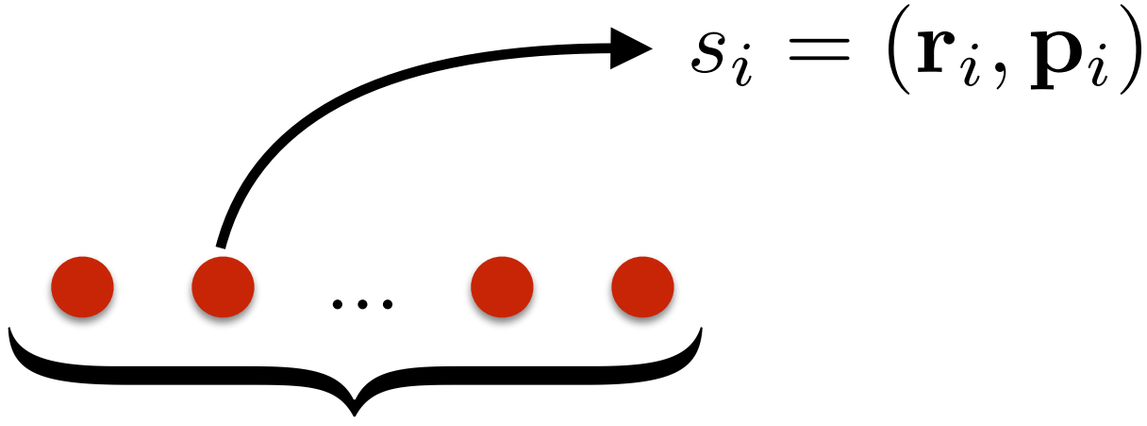
N states



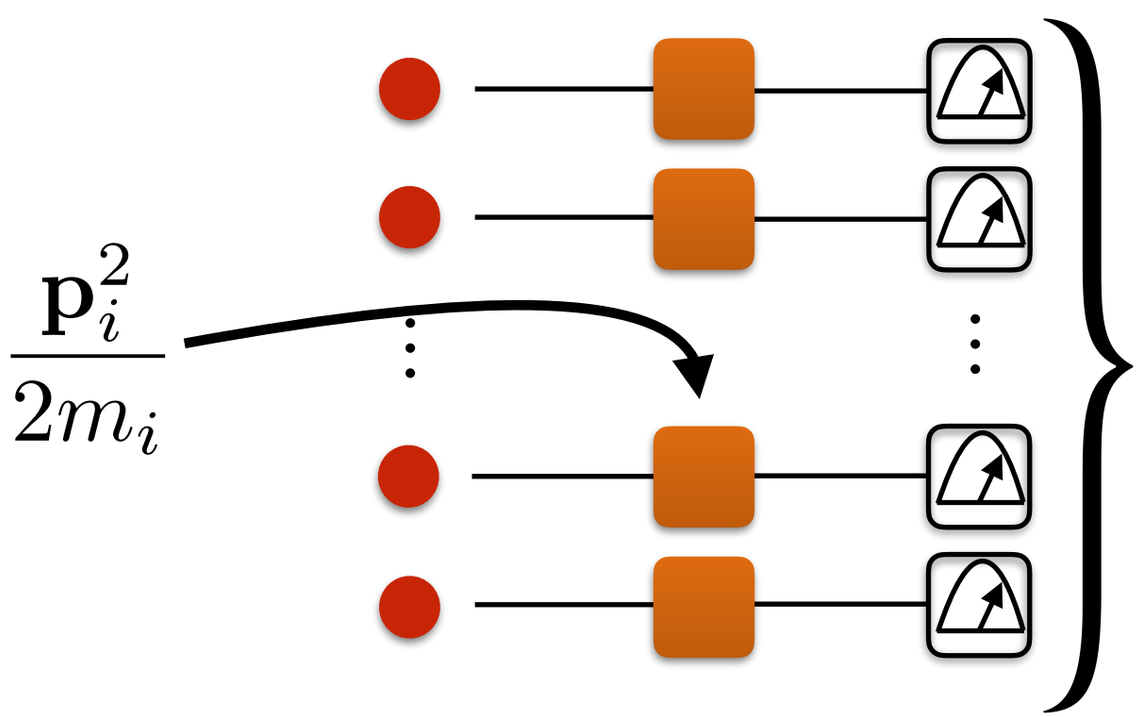
Example



N particles
non-interacting

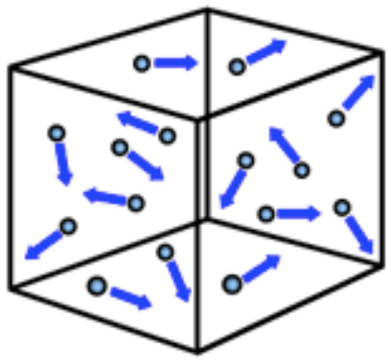


N states

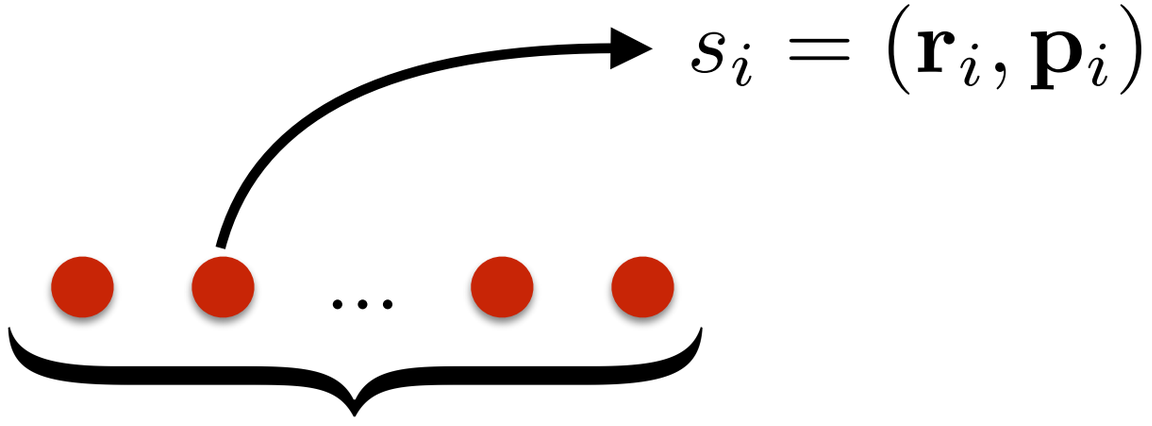


Can also be one
big measurement

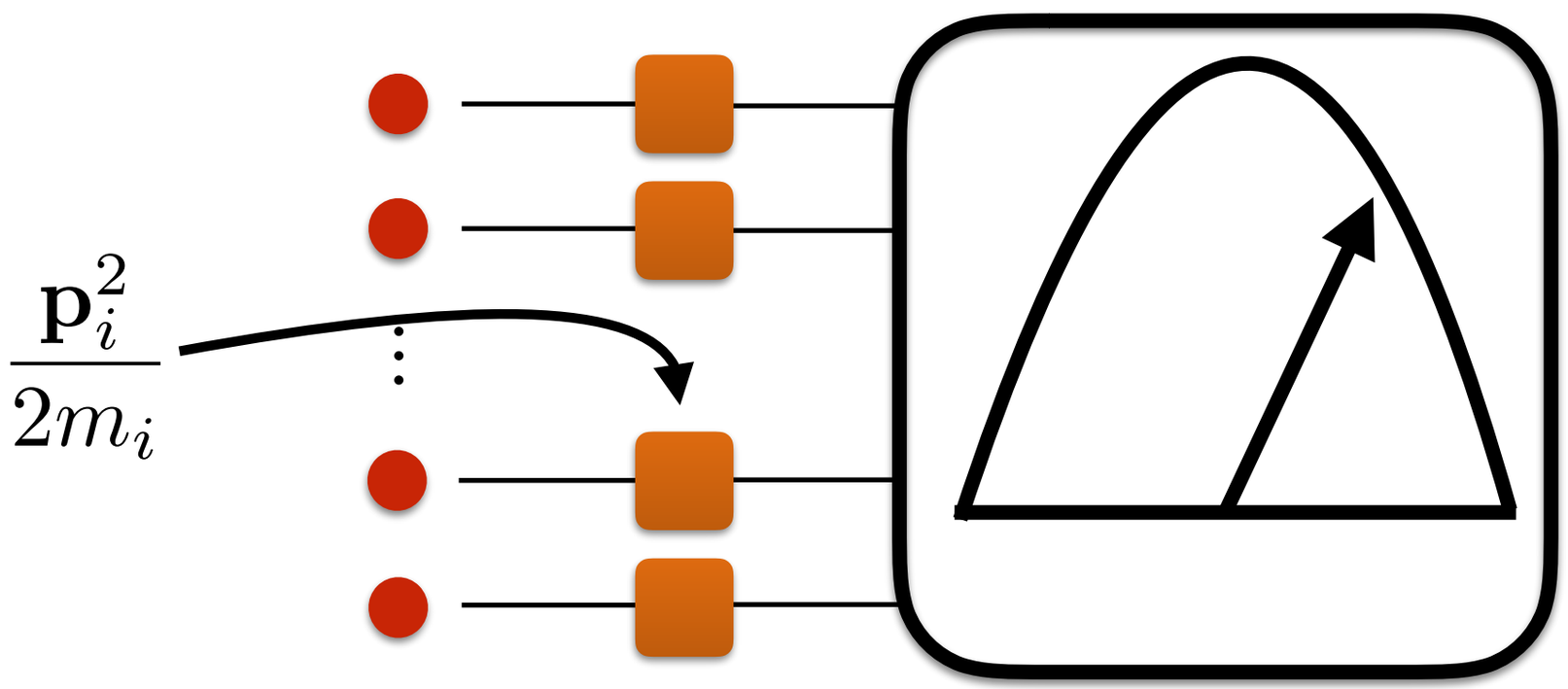
Example



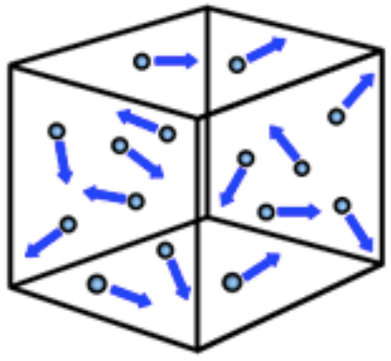
N particles
non-interacting



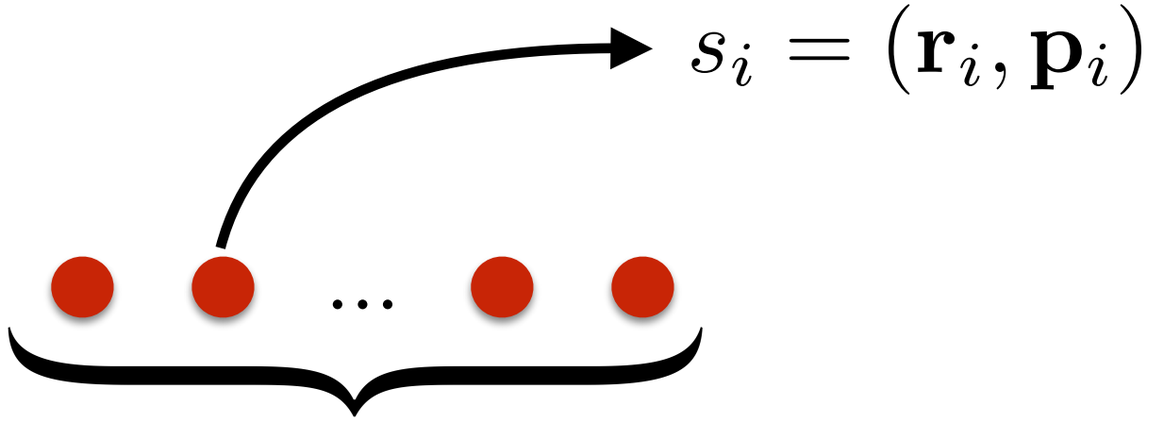
N states



Example

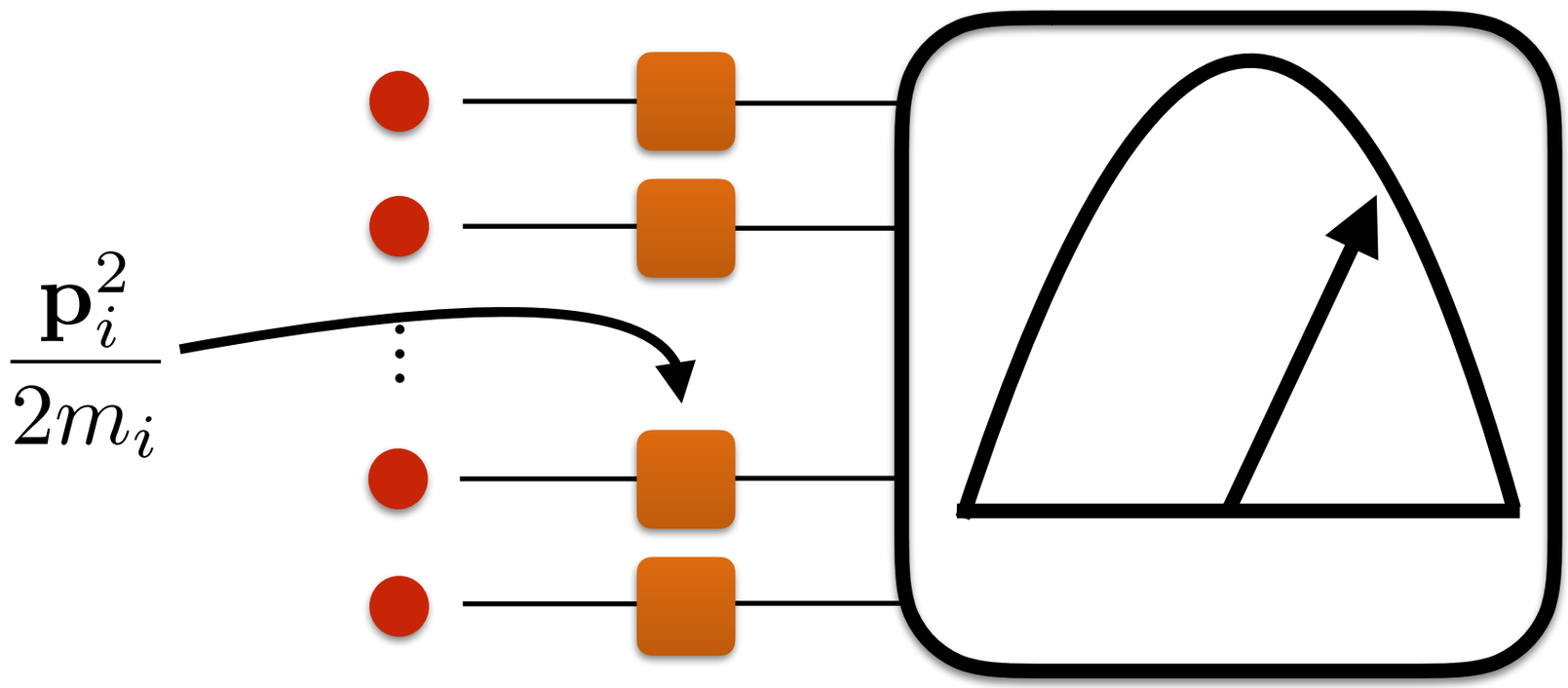


N particles
non-interacting

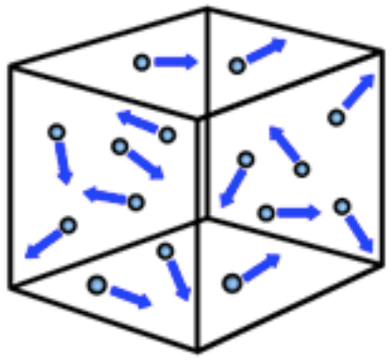


N states

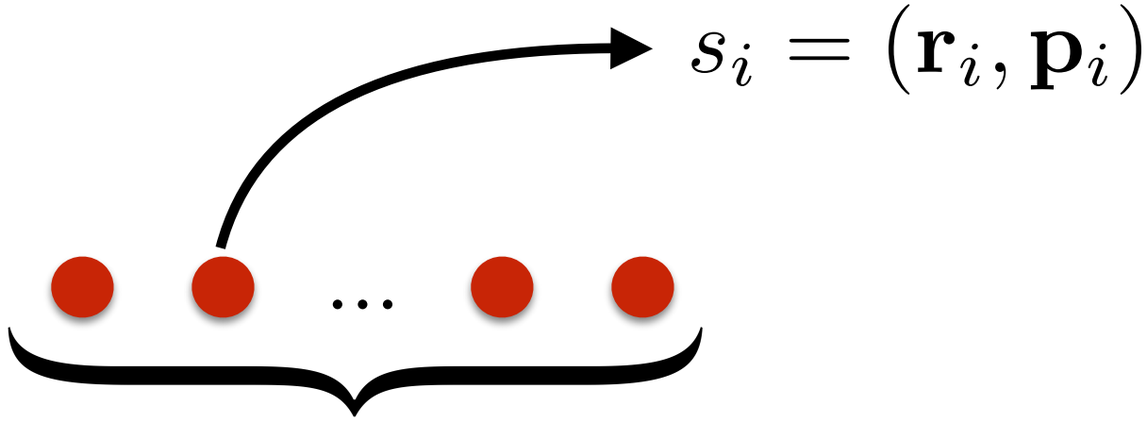
What if the particles interact?



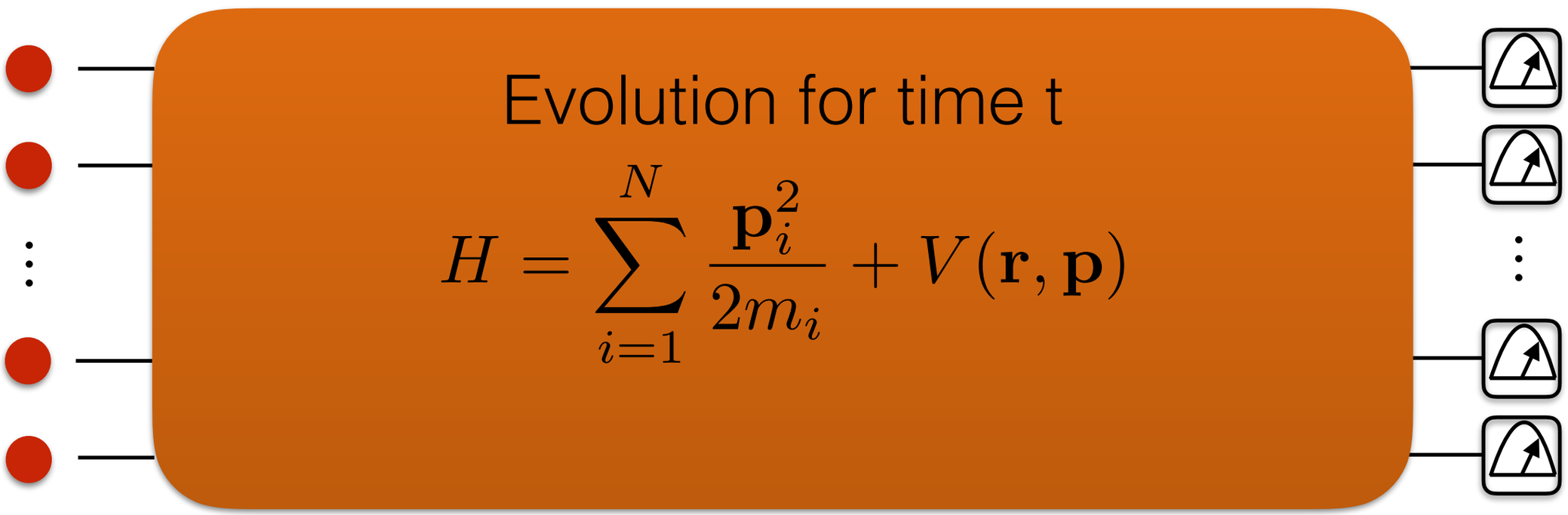
Example



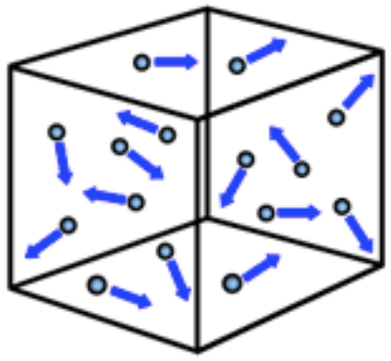
N **interacting** particles



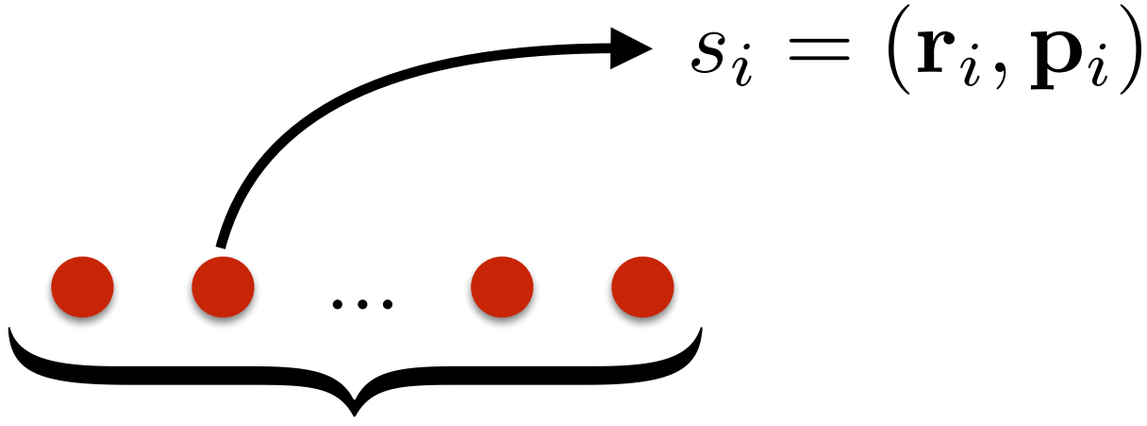
N states



Example

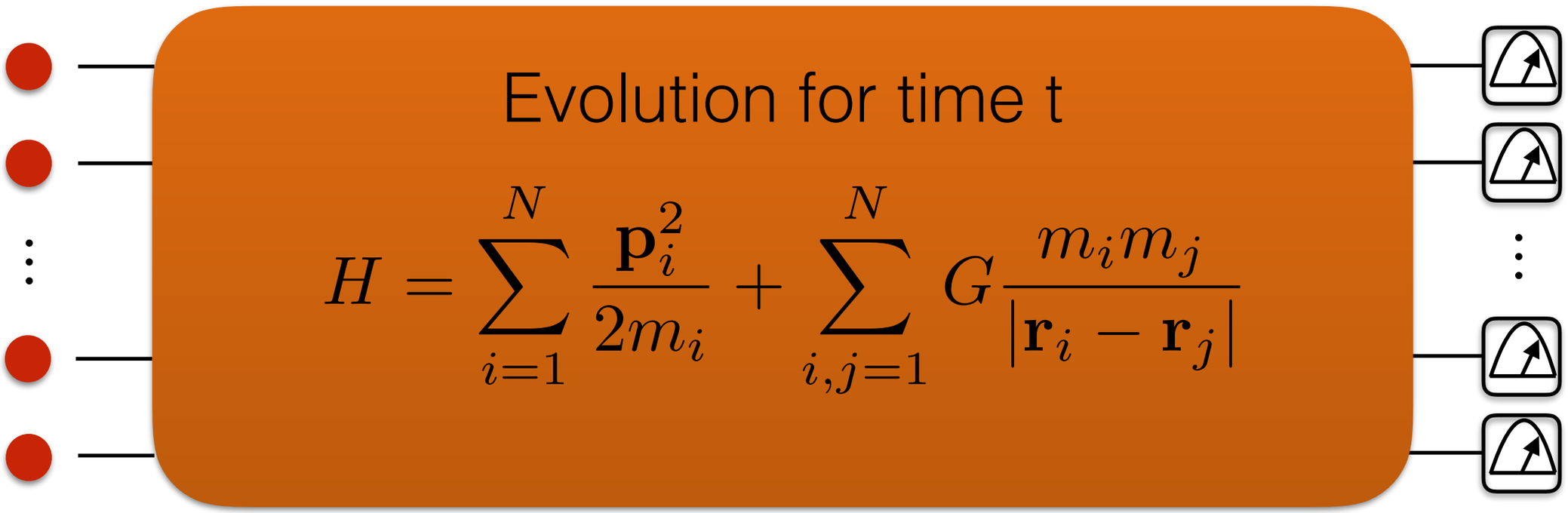


N **interacting** particles

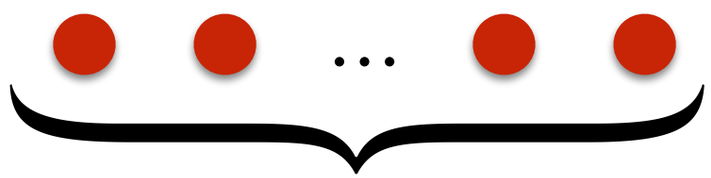


N states

Gravitational interaction



Example



N states

Hamiltonian can have local terms and interaction terms

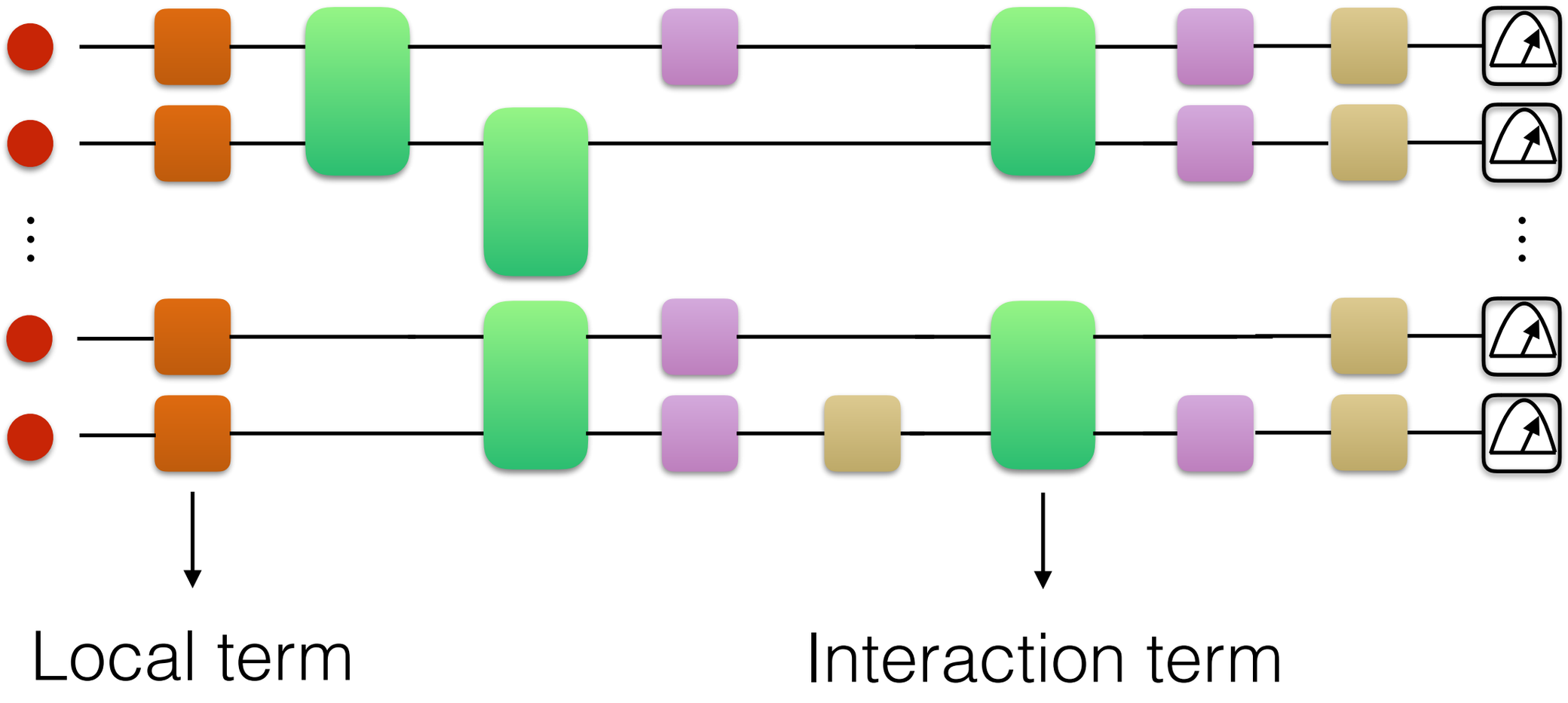
$\frac{\mathbf{p}_i^2}{2m_i}$ acts only on state i

$G\frac{m_i m_j}{|\mathbf{r}_i - \mathbf{r}_j|}$ acts on states i and j together

Imagine we can turn on/off the interaction terms *whenever* we wanted to

Example

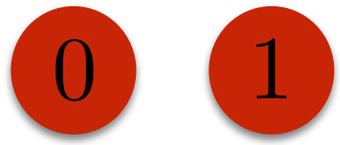
N states



Computation

States

Binary strings $\mathcal{S} = \{0,1\}^*$



Transformations

Boolean logic gates

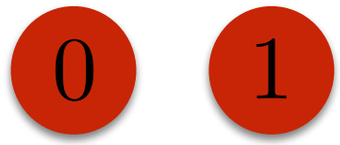
Composition

Observation (measurement)

Computation

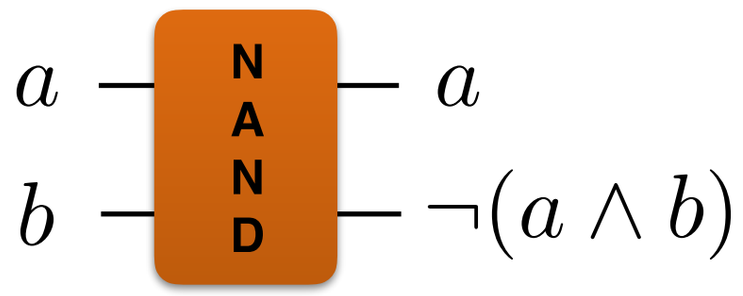
States

Binary strings $\mathcal{S} = \{0,1\}^*$



Transformations

Boolean logic gates



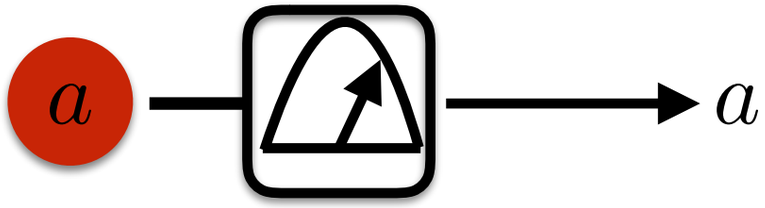
Composition

Cartesian product

$\mathcal{S}_A = \{0,1\}$ $\mathcal{S}_{AB} = \mathcal{S}_A \times \mathcal{S}_B$

$\mathcal{S}_B = \{0,1\}$ $\mathcal{S}_{AB} = \{00, 01, 10, 11\}$

Observation (measurement)

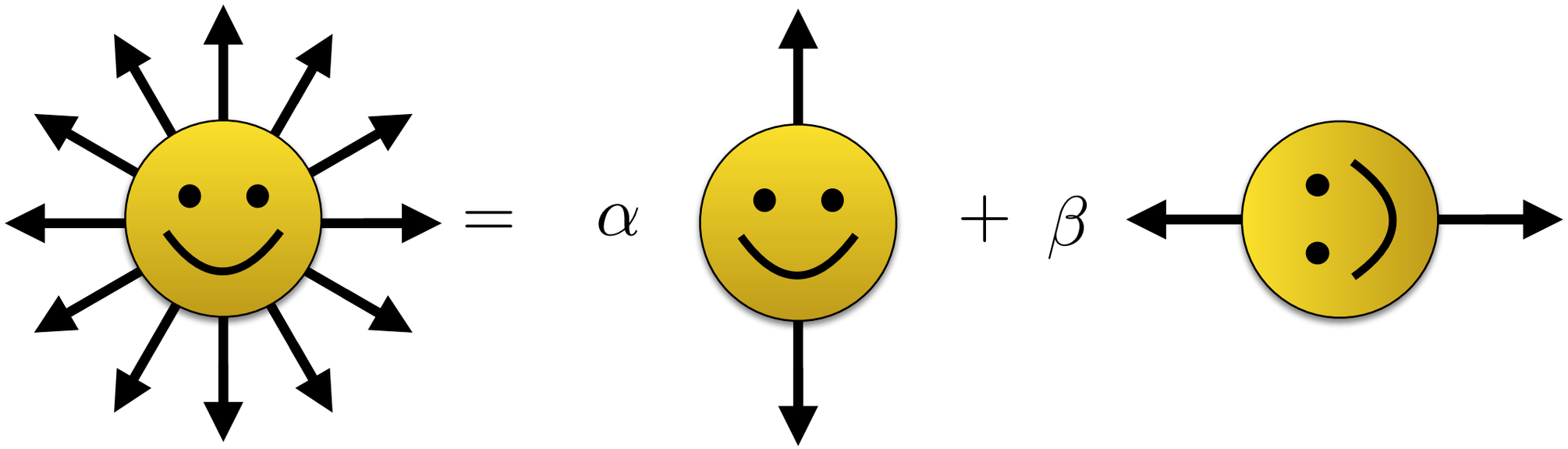


Quantum mechanics

States	Unit vectors in a complex vector space	$\|\psi\rangle \in \mathcal{H}$ $\|\|\psi\rangle\|^2 = 1$
Transformations	Schrödinger's equation	$H\|\psi\rangle = i\hbar\frac{d\|\psi\rangle}{dt}$
Composition	Tensor product	$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$
Observation (measurement)	Hermitian operators	$O = O^\dagger$

Quantum states

One qubit $dim(\mathcal{H}) = 2$



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

$$|\alpha|^2 + |\beta|^2 = 1$$

$$|\psi\rangle \equiv e^{i\phi}|\psi\rangle$$

Quantum states

One qutrit $dim(\mathcal{H}) = 3$

Three level quantum systems

Can't really represent them with polarisation

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$$

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$$

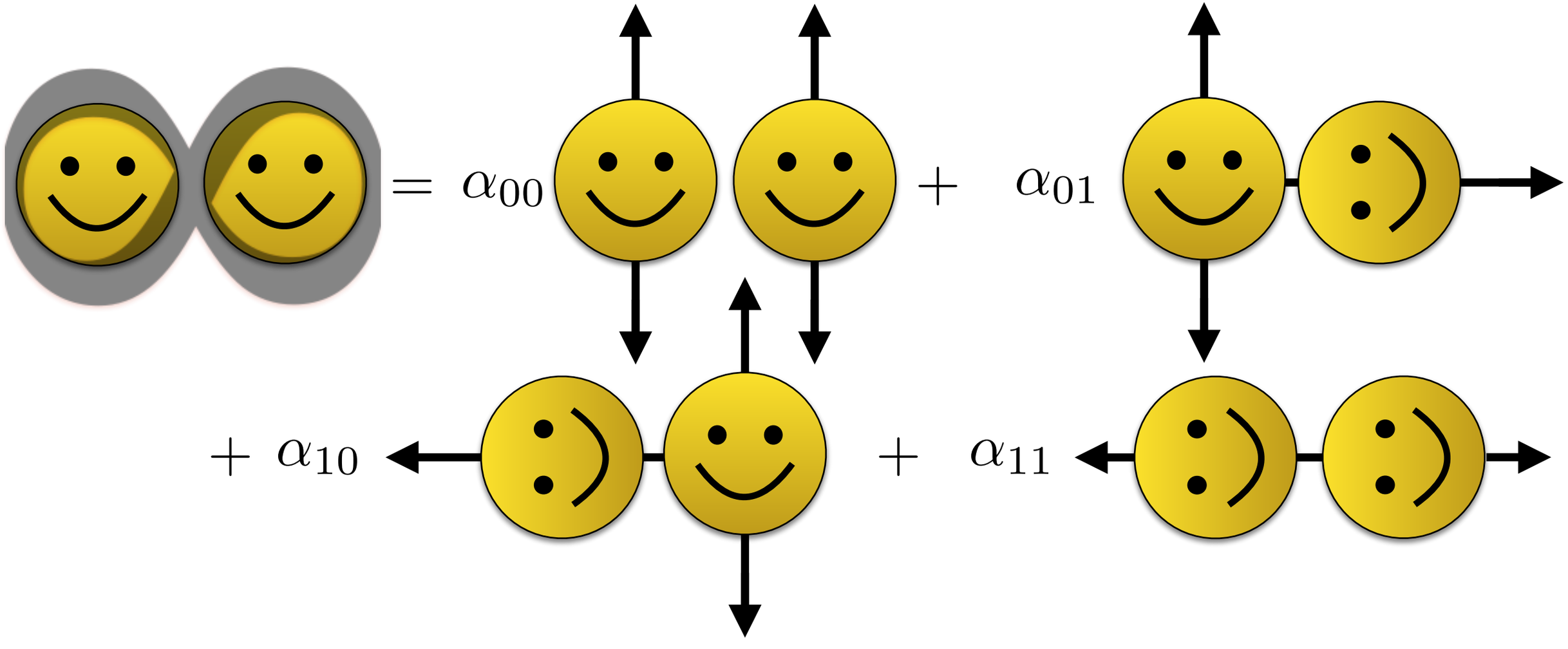
We almost never talk about qutrits :(

Quantum states

Two qubits $dim(\mathcal{H}) = 4$

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

$$\sum_{i,j\in\{0,1\}} |\alpha_{ij}|^2 = 1$$



Quantum states

N qubits $dim(\mathcal{H}) = 2^N$

$$|\psi\rangle = \alpha_0|00...0\rangle + \alpha_1|00...1\rangle + ... + \alpha_{2^N-1}|11...1\rangle$$

$$\sum_{i=0}^{2^N-1} |\alpha_i|^2 = 1$$

$$|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{2^N-1} \end{pmatrix} \quad \langle\psi| = \begin{pmatrix} \alpha_0^* & \alpha_1^* & \cdots & \alpha_{2^N-1}^* \end{pmatrix}$$

$$\langle\psi|\psi\rangle = 1$$

Inner products

All bases we consider should be **orthonormal**

$$|\psi\rangle = \sum_i \alpha_i |i\rangle$$

It is the case that

$$\forall i, j \text{ s.t. } \; i \neq j, \; \langle i|j\rangle = \langle j|i\rangle = 0$$

$$\forall i, \; \langle i|i\rangle = 1$$

Note that:

$$\langle i|\psi\rangle = \alpha_i$$

$$\langle \psi|\phi\rangle = \langle \phi|\psi\rangle^*$$

Composition

$$\mathcal{H}_A \quad dim(\mathcal{H}_A) = m$$

$$|\psi\rangle_A = \alpha_0|0\rangle_A + \alpha_1|1\rangle_A + ... + \alpha_{m-1}|m-1\rangle_A$$

$$\mathcal{H}_B \quad dim(\mathcal{H}_B) = n$$

$$|\psi\rangle_B = \beta_0|0\rangle_B + \beta_1|1\rangle_B + ... + \beta_{n-1}|n-1\rangle_B$$

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$$

$$dim(\mathcal{H}_{AB}) = m \cdot n$$

$$|\psi\rangle_{AB} = \gamma_{00}|0\rangle_A|0\rangle_B + \gamma_{01}|0\rangle_A|1\rangle_B + ...$$

$$... + \gamma_{m-1,n-1}|m-1\rangle_A|n-1\rangle_B$$

Composition

$$|\psi\rangle_A = \alpha_0|0\rangle_A + \alpha_1|1\rangle_A + ... + \alpha_{m-1}|m-1\rangle_A$$
$$|\psi\rangle_B = \beta_0|0\rangle_B + \beta_1|1\rangle_B + ... + \beta_{n-1}|n-1\rangle_B$$

What if we put these states together?

$$|\psi\rangle_A|\psi\rangle_B = |\psi\rangle_A \otimes |\psi\rangle_B$$
$$= \alpha_0\beta_0|0\rangle_A|0\rangle_B + ... + \alpha_i\beta_j|i\rangle_A|j\rangle_B + ...$$
$$... + \alpha_{m-1}\beta_{n-1}|m-1\rangle_A|n-1\rangle_B$$

If $|\psi\rangle_{AB} = |\psi\rangle_A|\psi\rangle_B$

$$\gamma_{i,j} = \alpha_i\beta_j$$

In general this might not be the case!

Entanglement

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}|0\rangle_A|0\rangle_B + \frac{1}{\sqrt{2}}|1\rangle_A|1\rangle_B$$

Suppose $|\psi\rangle_{AB} = |\psi\rangle_A|\psi\rangle_B$

$$|\psi\rangle_A = \alpha_0|0\rangle_A + \alpha_1|1\rangle_A$$

$$|\psi\rangle_B = \beta_0|0\rangle_B + \beta_1|1\rangle_B$$

$$|\psi\rangle_A|\psi\rangle_B = \alpha_0\beta_0|0\rangle_A|0\rangle_B + \alpha_0\beta_1|0\rangle_A|1\rangle_B +$$
$$+\alpha_1\beta_0|1\rangle_A|0\rangle_B + \alpha_1\beta_1|1\rangle_A|1\rangle_B$$

$$\alpha_0\beta_0 = \alpha_1\beta_1 = 1 \qquad \alpha_0\beta_1 = \alpha_0\beta_1 = 0$$

Contradiction!

Entanglement

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}|0\rangle_A|0\rangle_B + \frac{1}{\sqrt{2}}|1\rangle_A|1\rangle_B$$

This is called a **Bell state**
(more on Day 4)

Entanglement is a sort of *holism* of quantum states

Whole cannot be expressed in terms of its parts

This generalises to multiple systems

Transformations

$$H|\psi\rangle = i\hbar\frac{d|\psi\rangle}{dt}$$

If you solve the equation…

$$|\psi(t)\rangle = e^{-iHt/\hbar}|\psi(0)\rangle$$

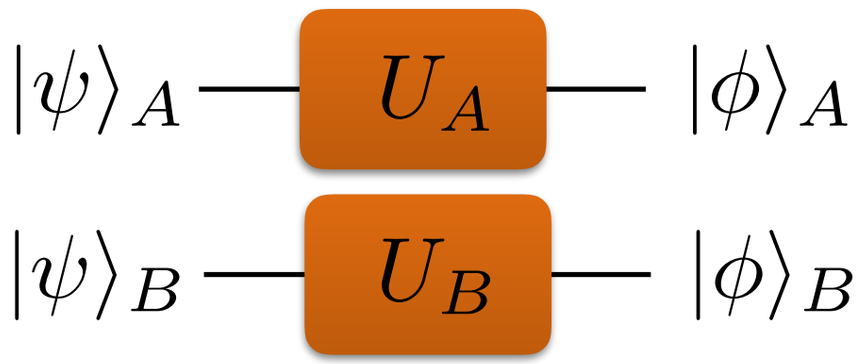
$e^{-iHt/\hbar}$ is a **unitary** matrix

$$UU^\dagger = U^\dagger U = I$$

† means transpose & complex conjugate

Transformations

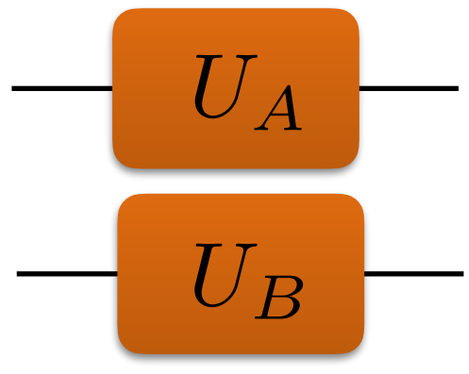
$$U|\psi\rangle = |\phi\rangle$$



$$(U_A|\psi\rangle_A) \otimes (U_B|\psi\rangle_B) = |\phi\rangle_A|\phi\rangle_B$$

$$(U_A \otimes U_B)|\psi\rangle_A|\psi\rangle_B = |\phi\rangle_A|\phi\rangle_B$$

$$U_A \otimes U_B =$$



Transformations

But what is $U_A \otimes U_B$?

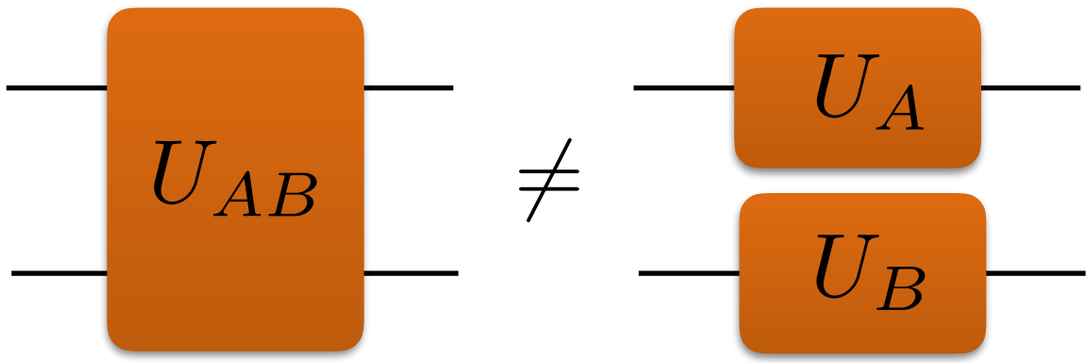
$$U_A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \qquad U_B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$$

$$U_A \otimes U_B = \begin{pmatrix} a_1b_1 & a_1b_2 & a_2b_1 & a_2b_2 \\ a_1b_3 & a_1b_4 & a_2b_3 & a_2b_4 \\ a_3b_1 & a_3b_2 & a_4b_1 & a_4b_2 \\ a_3b_3 & a_3b_4 & a_4b_3 & a_4b_4 \end{pmatrix}$$

This generalises for different dimensions and multiple tensor products

Transformations

Note that we might have…



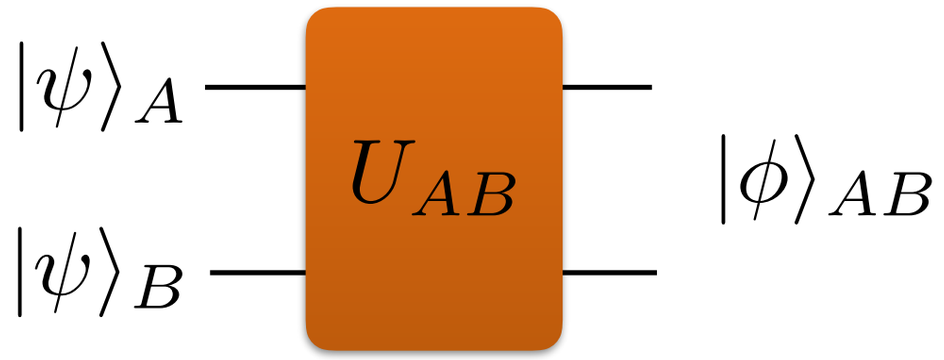
Just like entangled states, these are **entangling gates**/operations

Can be written as…

$$U_{AB} = U_A^1 \otimes U_B^1 + ... + U_A^m \otimes U_B^n$$

We'll see an example later

Transformations

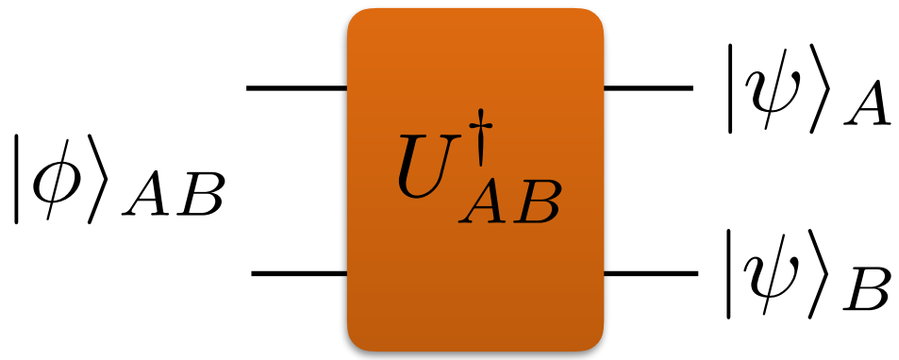


$$|\phi\rangle_{AB} = U_{AB}|\psi\rangle_A|\psi\rangle_B$$

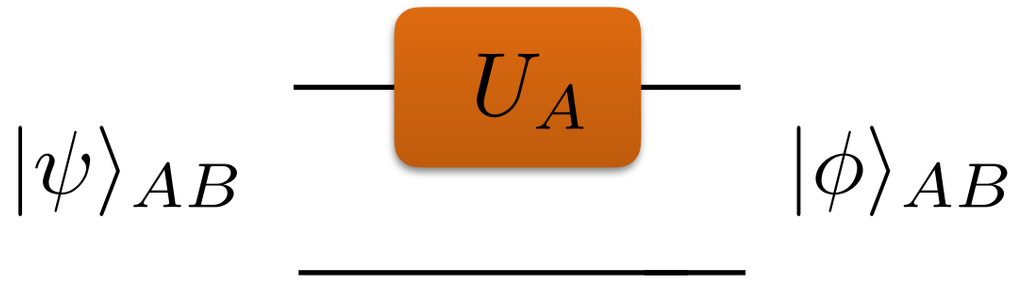
$|\phi\rangle_{AB}$ is entangled $\quad |\phi\rangle_{AB} \neq |\phi\rangle_A|\phi\rangle_B$

Note that unitaries are invertible, so…

$$U_{AB}^\dagger|\phi\rangle_{AB} = |\psi\rangle_A|\psi\rangle_B$$



Transformations



$$U_{AB}|\psi\rangle_{AB} = |\phi\rangle_{AB}$$

What is U_{AB} ?

$$U_{AB} = U_A \otimes I$$

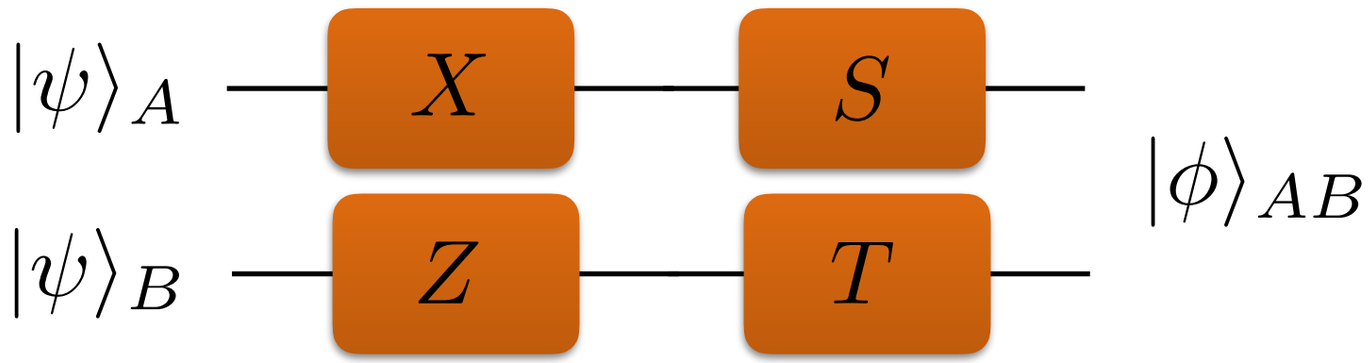
Not the same as…

$$I \otimes U_A$$

What is $U^\dagger_{AB}$?

$$U^\dagger_{AB} = U^\dagger_A \otimes I$$

Transformations



$$|\phi\rangle_{AB} = (S \otimes T)(X \otimes Z)|\psi\rangle_A|\psi\rangle_B$$

$$|\phi\rangle_{AB} = (SX) \otimes (TZ)|\psi\rangle_A|\psi\rangle_B$$

$$|\phi\rangle_{AB} = SX|\psi\rangle_A \otimes TZ|\psi\rangle_B$$

Always keep track of which operation acts on which system!

Observables

Let O be an $m \times m$ matrix such that $O = O^\dagger$

This condition is equivalent to:

O has only **real** eigenvalues

If O has eigenvectors

$$|v_1\rangle, |v_2\rangle, ...|v_m\rangle$$

Then it is the case that

$$\forall i, j \text{ s.t. } i \neq j, \ \langle v_i | v_j \rangle = 0$$

We can also normalise the vectors, so that

$$\forall i, \langle v_i | v_i \rangle = 1$$

Observables

Let O be an $m \times m$ matrix such that $O = O^\dagger$

This condition is equivalent to:

O has only **real** eigenvalues

The eigenvectors of O form an orthogonal basis (that can be made orthonormal)

Any state on an m-dimensional space can be written as

$$|\psi\rangle = \sum_i \alpha_i |v_i\rangle$$

What does all this have to do with measurement?

Observables

If you measure the state $|\psi\rangle$ with observable O

having eigenvalues…

$$\lambda_1, \lambda_2, ...\lambda_m$$

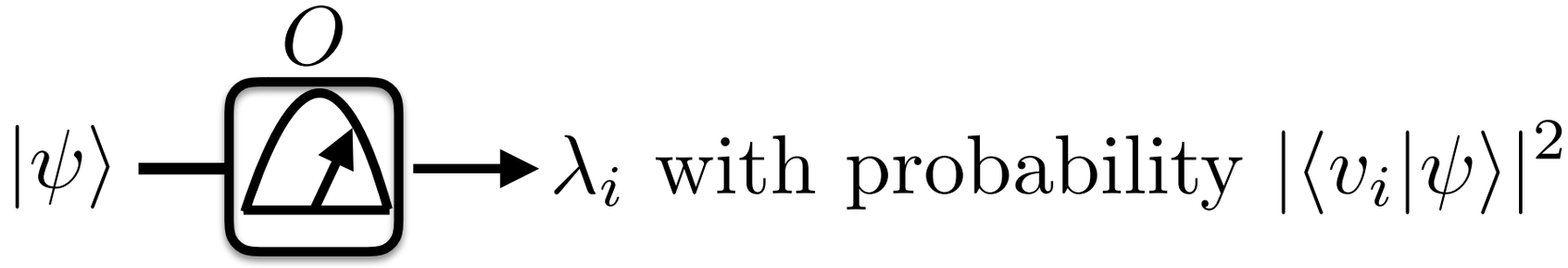
and eigenvectors…

$$|v_1\rangle, |v_2\rangle, ...|v_m\rangle$$

You will observe λ_i with probability $|\langle v_i|\psi\rangle|^2$

and the state becomes (**collapses to**) $|v_i\rangle$

Observables



What if we have degeneracy?

$$\lambda_i = \lambda_j \ (i \neq j)$$

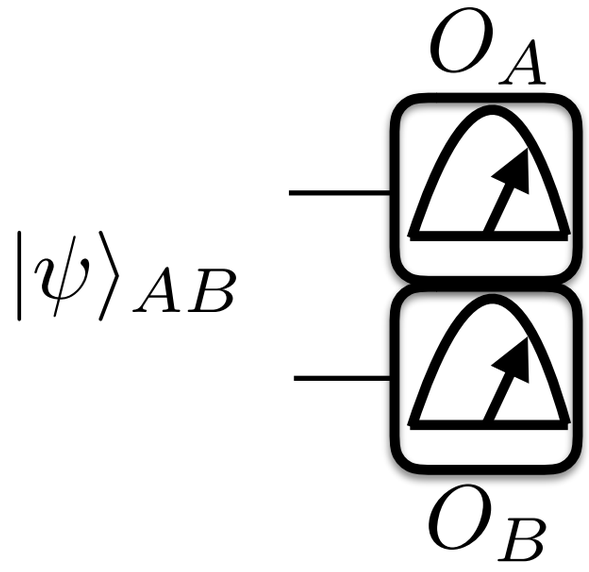
We get outcome $\lambda_i = \lambda_j$ with probability $|\langle v_i|\psi\rangle|^2 + |\langle v_j|\psi\rangle|^2$

State collapses to

$$\frac{\langle v_i|\psi\rangle \ |v_i\rangle + \langle v_j|\psi\rangle \ |v_j\rangle}{\sqrt{|\langle v_i|\psi\rangle|^2 + |\langle v_i|\psi\rangle|^2}}$$

Observables

What about this…



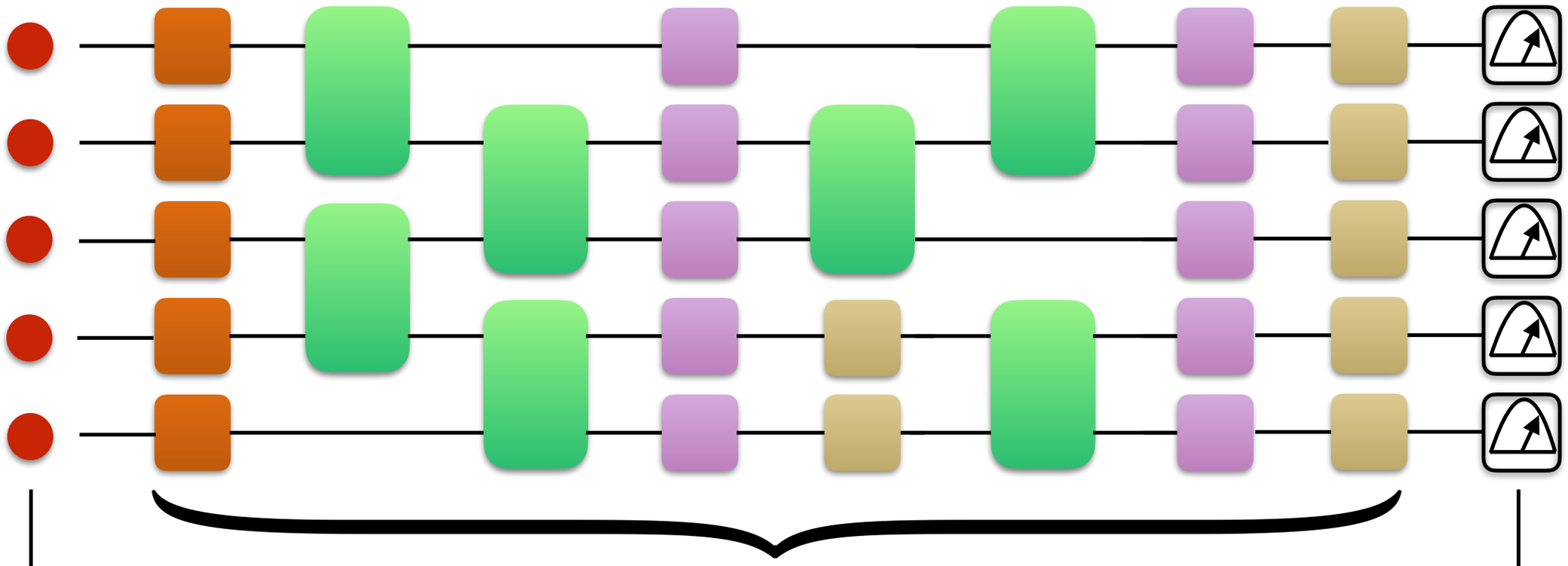
$$O_{AB} = O_A \otimes O_B$$

Has eigenvalues $\lambda_A^1 \lambda_B^1, \lambda_A^1 \lambda_B^2, ...$

And eigenvectors $|v_1\rangle_A |w_1\rangle_B, |v_1\rangle_A |w_2\rangle_B, ...$

Where λ_A^i and $|v_i\rangle_A$ are the eigenvalues, eigenvectors of O_A
Where λ_B^i and $|w_i\rangle_B$ are the eigenvalues, eigenvectors of O_B

Putting it all together



Qubits

Quantum gates

Measurement

$$\begin{pmatrix} \psi_0 \\ \psi_1 \\ \vdots \\ \psi_{2^N-1} \end{pmatrix} \quad \begin{pmatrix} \mathcal{C}_{0,0} & \cdots & \mathcal{C}_{0,2^N-1} \\ \mathcal{C}_{1,0} & \cdots & \mathcal{C}_{1,2^N-1} \\ \vdots & & \vdots \\ \mathcal{C}_{2^N-1,0} & \cdots & \mathcal{C}_{2^N-1,2^N-1} \end{pmatrix} \quad \begin{matrix} |\phi_0|^2 \rightarrow 00...0 \\ |\phi_1|^2 \rightarrow 00...1 \\ \vdots \\ |\phi_{2^N-1}|^2 \rightarrow 11...1 \end{matrix}$$

$$|\psi\rangle \qquad |\phi\rangle = \mathcal{C}|\psi\rangle \qquad |\phi\rangle \rightarrow b_1 b_2 ... b_N$$

References and resources

An awesome course that views things operationally (categorical quantum mechanics)

http://www.inf.ed.ac.uk/teaching/courses/cqi/

Operational theories

https://www.cs.ox.ac.uk/people/sean.tull/OpTheoriesAsCats.pdf

https://arxiv.org/pdf/quant-ph/0508211.pdf

https://foundations.ethz.ch/wp-content/uploads/2017/06/reconstructions.pdf

Quantum mechanics from operational principles

https://arxiv.org/abs/1303.1538