

Einführung in die Quanteninformation

Hans J. Briegel

Theoretical Physics, U Innsbruck
Department of Philosophy, U Konstanz*

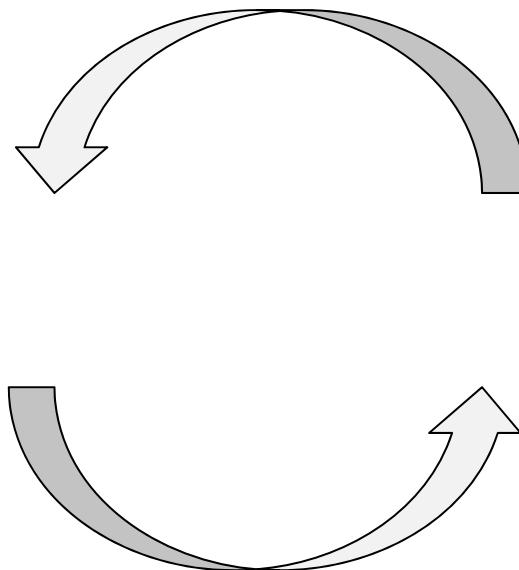
Quanteninformationsverarbeitung

- Untersuchung grundlegender Begriffe und Aussagen der Quantenmechanik (z.B. *Komplementarität, Indeterminismus, Verschränkung*) im Hinblick auf neuartige Anwendungen
 - Quantencomputer – Effizienz
 - Quantenkryptographie – Sicherheit
 - Quantensimulation – Reduktion
- „*Information is physical*“ → Prinzipielle Möglichkeiten und Grenzen von Computern und jeder Art von Informationsverarbeitung werden durch physikalische Gesetze bestimmt.
- Neuer Fokus: Maschinelles Lernen und künstliche Intelligenz

Dunjko & Briegel, *Machine learning and AI in the quantum domain*,
Rep. Progr. Phys. **81**, 074001 (2018); arXiv:1709.02779

Konzepte und Grundlagen
der Quantenmechanik

Anwendungen



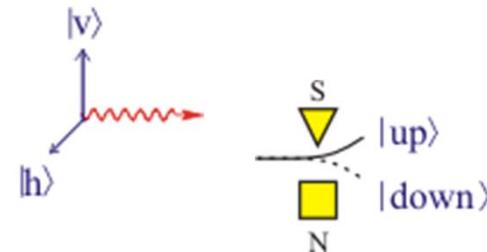
Basic concepts

Principle: Quantum information is represented by quantum states $|\psi\rangle \in H$ (Hilbert space) of a physical system.

Unit of information: 1 Qubit measures the information content that can be conveyed by communicating a quantum mechanical 2-state system.

Two-state system: Any system equivalent to spin $\frac{1}{2}$, such as

- Polarisation state of photon
- Magnetic moment of nucleus
- Selected subspace of atomic energy eigenstates
- ...



$$^{87}\text{Rb}: \begin{array}{c} \text{F=2} \\ \text{---} \end{array} \text{---} \bullet \text{---} \circ \text{---} \begin{array}{c} |\text{0}\rangle \\ |\text{1}\rangle \end{array}$$

Basis states: $|0\rangle$ and $|1\rangle$ (abstraction) generalize classical bit values 0 and 1.

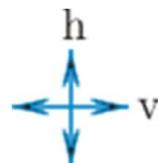
Different from classical binary information, any superposition

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

is allowed

Example photon: $|0\rangle = |h\rangle$

$$|1\rangle = |v\rangle$$



eigenstates
"mutually
"unbiased"

vs. $|0\rangle' = (|0\rangle + |1\rangle)/\sqrt{2} = |+45^\circ\rangle$
 $|1\rangle' = (|0\rangle - |1\rangle)/\sqrt{2} = |-45^\circ\rangle$



↑
Complementary
observables

→ Tafeleinschub: Notation

Tensor products such as $|0\rangle|0\rangle|0\rangle$, $|0\rangle|0\rangle|1\rangle$, $|0\rangle|1\rangle|0\rangle$, ... $\in H \otimes H \otimes H$ define a quantum register.

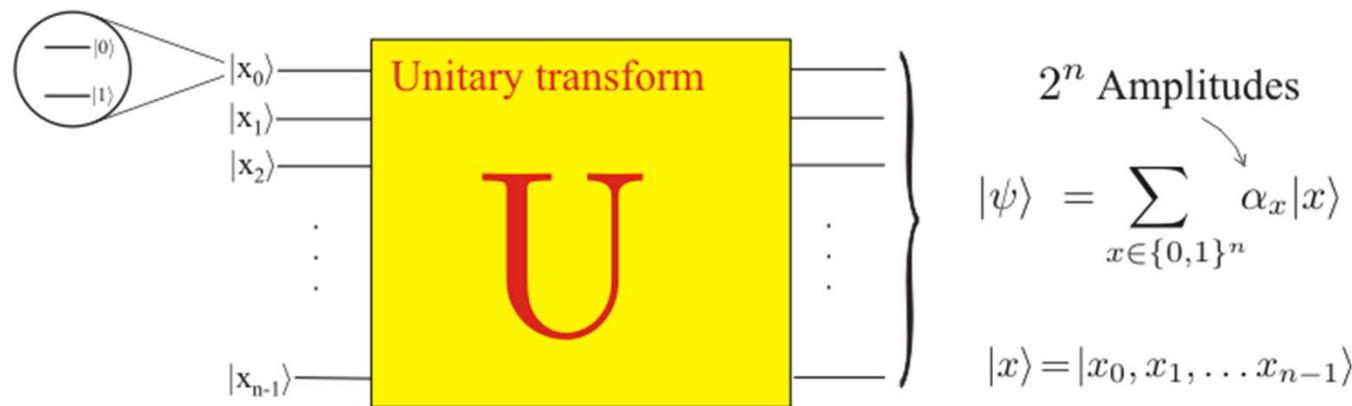


Linear superpositions $|\Psi\rangle = \alpha|0\rangle|1\rangle|0\rangle + \beta|1\rangle|0\rangle|1\rangle + \dots$ of register states are (typically) entangled states.

Entanglement leads to correlations in the data, some of which may be algorithmically interesting (such as period of a function).

Quantum information processing: Sequence of unitary operations (or CP maps) on quantum register, which may be interrupted and steered by measurements (or POVMs).

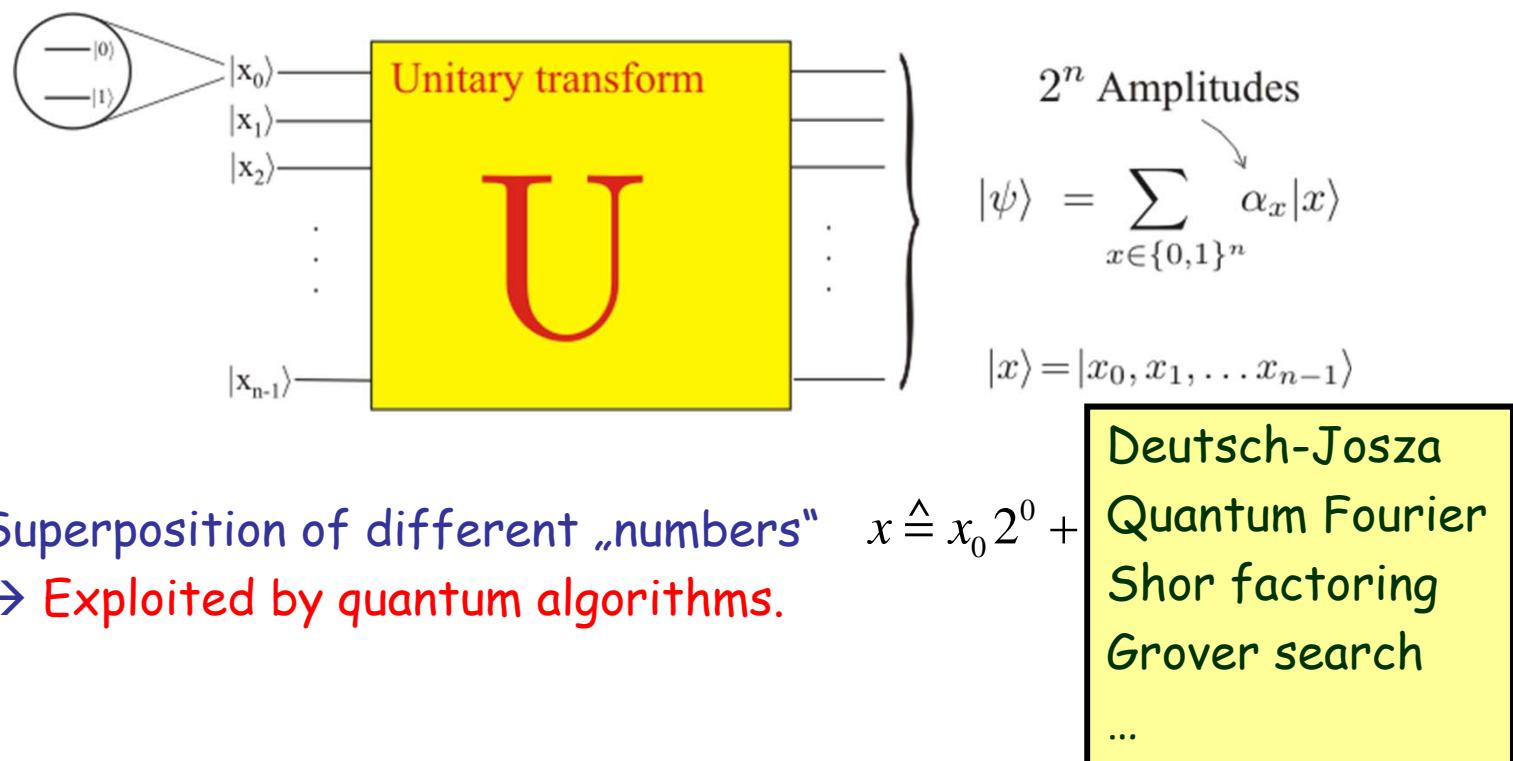
Universal quantum computer: Device that can be programmed to execute any unitary transformation U with arbitrary precision.



Superposition of different „numbers” $x \triangleq x_0 2^0 + x_1 2^1 + \dots + x_{n-1} 2^{n-1}$
 → Exploited by quantum algorithms.

Quantum information processing: Sequence of unitary operations (or CP maps) on quantum register, which may be interrupted and steered by measurements (or POVMs).

Universal quantum computer: Device that can be programmed to execute any unitary transformation U with arbitrary precision.



Elementary protocols using entanglement

Bell states

$$|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)$$

Tafeleinschub: EPR

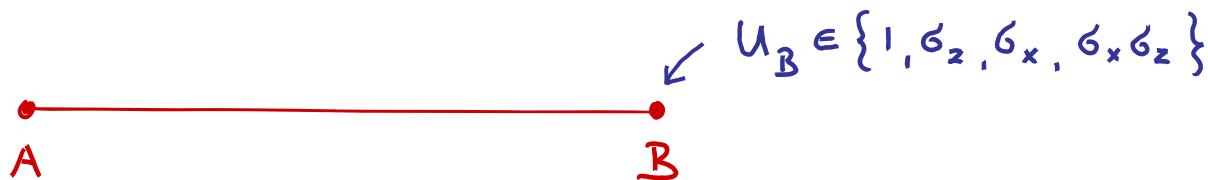
$$|\phi^-\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B - |1\rangle_A |1\rangle_B) = \sigma_z^B |\phi^+\rangle_{AB}$$

$$|\psi^+\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B) = \sigma_x^B |\phi^+\rangle_{AB}$$

$$|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B) = \sigma_x^B \sigma_z^B |\phi^+\rangle_{AB}$$

basis of maximally entangled two-qubit states

They can be transformed into each other by local unitary transformations



Dense coding (Bennett & Wiesner '92)

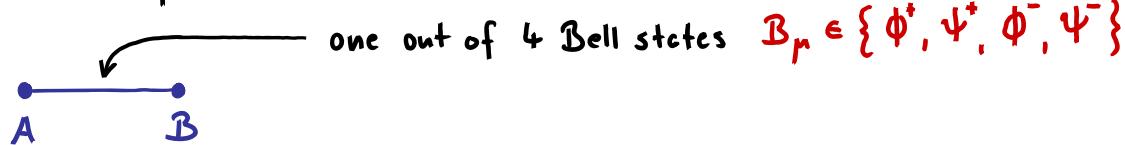
(0) Alice prepares Bell state $|\Phi^+\rangle_{AB}$ and sends particle B to Bob:



(1) Bob applies one of 4 unitary operations to particle B.



(2) Bob sends particle B back to Alice



(3) Alice measures state, using a "Bell state analyzer"

4 possible results!

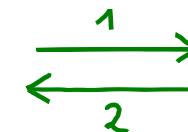
Bob can convey 2 bits of classical information
by sending a single q.m. two-state particle

BUT: Holevo's Theorem !?

*Roughly: Using one q.m. two-state system, you can encode max. 1 bit of classical information

Remark: „No contradiction to Holevo's theorem*“: ☺

If you count also step (0), there are in total
2 qubits exchanged between Alice and Bob“



More precisely: Bob does not encode his message in a single, isolated particle, but in a (non-locally) entangled two-particle system.

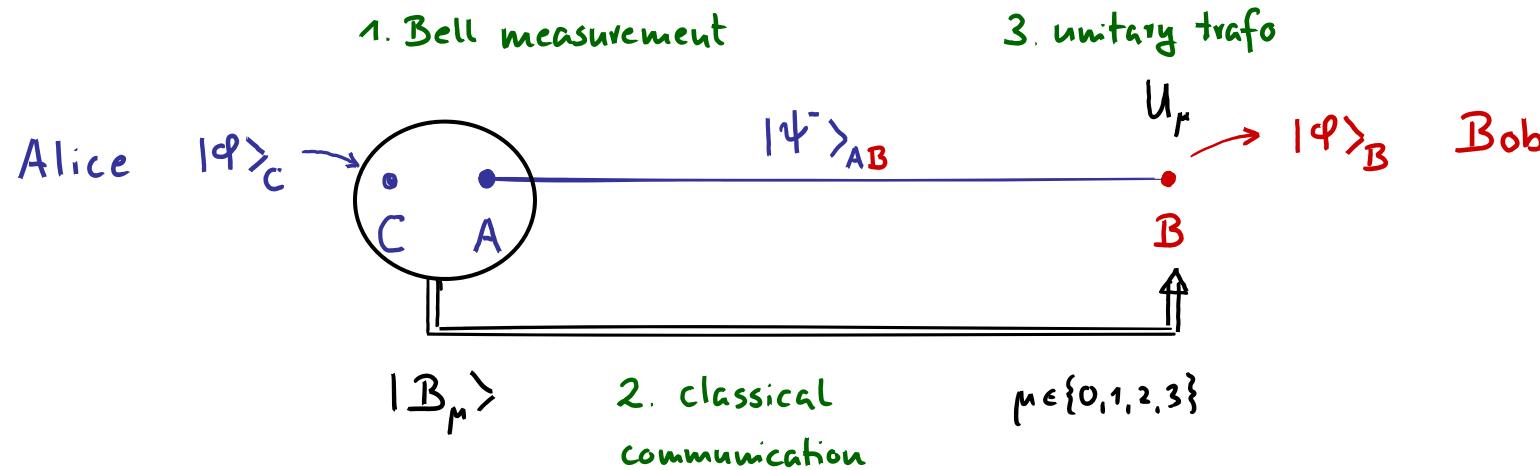


Not separable into two isolated particles!

Bob has access to a 4-dimensional Hilbert space!

N.B.: Interesting mainly from a conceptual perspective.

Teleportation (Bennett et al. 1993)



3-step protocol: Note necessity of 2nd step!

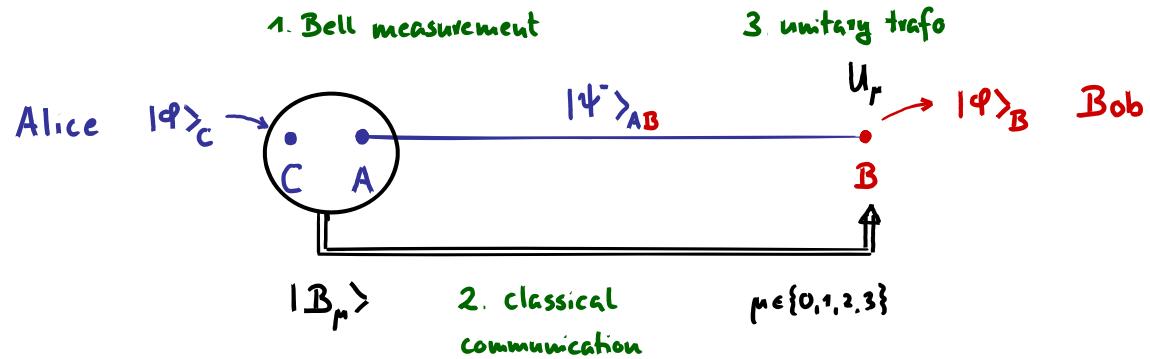
After:



Remarks:

1. Q-information $|\varphi\rangle$ never copied.
2. Because of step 2, no possibility of superluminal communication.

Teleportation (details):



3 - Qubit initial state :

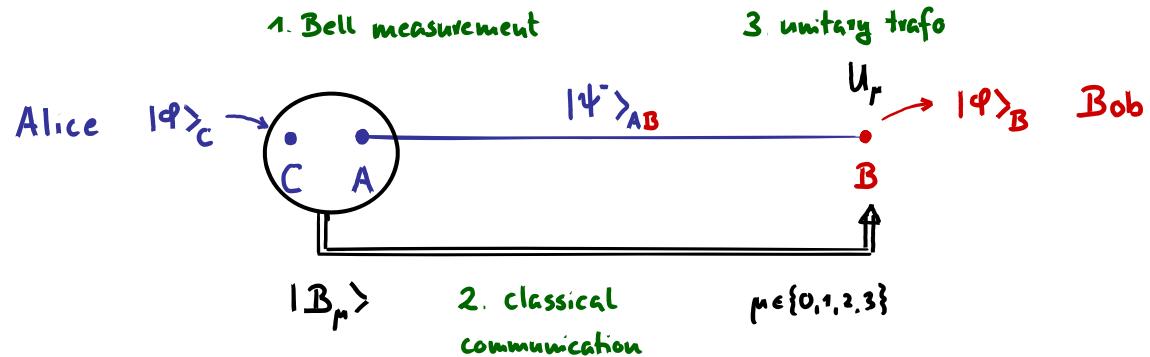
$$(\alpha|0\rangle_C + \beta|1\rangle_C) \otimes \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_C - |1\rangle_A|0\rangle_C)$$

$$\begin{aligned}
 &= -\frac{1}{2} |\Psi^-\rangle_{CA} \otimes (\alpha|0\rangle_B + \beta|1\rangle_B) &\rightarrow U_B = \text{id} \\
 &- \frac{1}{2} |\Psi^+\rangle_{CA} \otimes (\alpha|0\rangle_B - \beta|1\rangle_B) &U_B = \sigma_z \\
 &+ \frac{1}{2} |\phi^+\rangle_{CA} \otimes (\alpha|1\rangle_B + \beta|0\rangle_B) &U_B = \sigma_x \\
 &+ \frac{1}{2} |\phi^-\rangle_{CA} \otimes (\alpha|1\rangle_B - \beta|0\rangle_B) &U_B = \sigma_z \sigma_x
 \end{aligned}$$

Alice's measurement result

Bob's unitary transformation

Teleportation (details):



3 - Qubit initial state :

$$(\alpha|0\rangle_C + \beta|1\rangle_C) \otimes \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$$

Teleportation is a fundamental protocol of QIT

- Applications both in quantum communication (noisy channels) and in quantum computation (gate teleportation model).
- Inspiring conceptual role (e.g. q.m. non-locality)

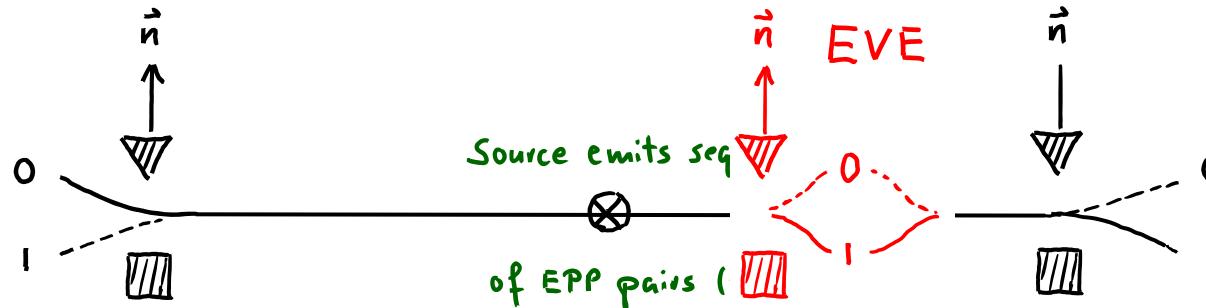
$$+ \frac{1}{2} |\Phi^-\rangle_{CA} \otimes (\alpha|1\rangle_B - \beta|0\rangle_B)$$

$$U_B = \sigma_z \sigma_x$$

Alice's measurement result

Bob's unitary transformation

Entanglement-based quantum key distribution (Ekert 91)



Alice measures: 01011010100...

random

Bob measures: 10100101011...

random

strictly correlated

Candidate for a cryptographic key:

secret, identical sequence of random numbers
(but, need choice of different directions...)

Stabilizer description of Bell- and similar states

- Consider again Bell state, say $|\phi^+\rangle_{ab} = \frac{1}{\sqrt{2}}(|0\rangle_a|0\rangle_b + |1\rangle_a|1\rangle_b)$
- It satisfies two eigenvalue equations: $X_a X_b |\phi^+\rangle = |\phi^+\rangle$ $Z_a Z_b |\phi^+\rangle = |\phi^+\rangle$ \iff $\langle X_a X_b \rangle = +1$
 $Z_a Z_b |\phi^+\rangle = |\phi^+\rangle$ $\langle Z_a Z_b \rangle = +1$
- Furthermore: $\langle Y_a Y_b \rangle = +1$ etc.
 $\langle X_a \rangle = \langle Y_a \rangle = \langle Z_a \rangle = 0$ random
- The observables $\begin{cases} K_x \equiv X_a X_b \\ K_z \equiv Z_a Z_b \end{cases}$ are called **stabilizer operators** of state $|\phi^+\rangle$
we can write $|\phi^+\rangle = |1,1\rangle = |K'_x, K'_z\rangle$

In standard Q.M. terminology: C.S.C.O. Compare e.g. Hydrogen atom $\{H, L^2, L_z\}$

eigenstates: $|n, l, m\rangle$ etc.

Equivalent:

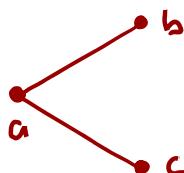
$$x_a z_b |\phi\rangle = |\phi\rangle \quad \Rightarrow \quad |\phi\rangle = \frac{1}{\sqrt{2}} (|0\rangle_z |0\rangle_x + |1\rangle_z |1\rangle_x)$$

$$z_a x_b |\phi\rangle = |\phi\rangle$$



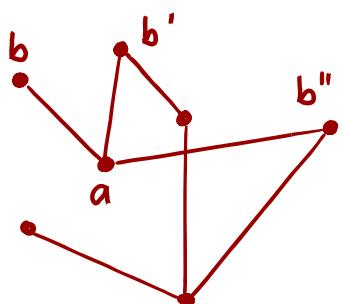
Bell state ; (rotated basis)

Generalisations:



$$\left. \begin{array}{l} x_a z_b z_c |\phi\rangle = |\phi\rangle \\ z_a x_b z_c |\phi\rangle = |\phi\rangle \\ z_a z_b x_c |\phi\rangle = |\phi\rangle \end{array} \right\} \Rightarrow |\phi\rangle = \frac{1}{\sqrt{2}} (|0\rangle_z |0\rangle_x |0\rangle_x + |1\rangle_z |1\rangle_x |1\rangle_x)$$

GHZ state



$$\left. \begin{array}{l} x_a \prod_{(a,b) \in E} z_b |\phi\rangle = |\phi\rangle \\ \text{for all vertices } a \in V \end{array} \right\} \Rightarrow |\phi\rangle = |k_1, k_2, \dots, k_M\rangle$$

Graph state

Graph $G = (V, E)$

N.B.: N qubits $\rightarrow 2^{\binom{N}{2}}$ different graphs

Equivalent :

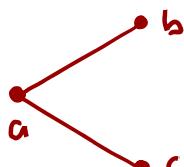
$$x_a z_b |\phi\rangle = |\phi\rangle \quad \Rightarrow \quad |\phi\rangle = \frac{1}{\sqrt{2}} (|0\rangle_z |0\rangle_x + |1\rangle_z |1\rangle_x)$$

$$z_a x_b |\phi\rangle = |\phi\rangle$$



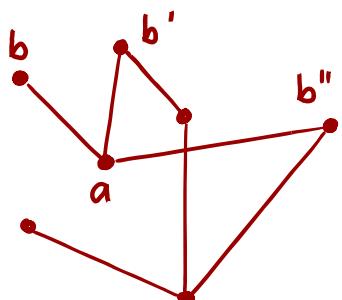
Bell state ; (rotated basis)

Generalisations:



Graph states are natural multi-particle generalisations of the Bell state.

They form useful entanglement resources for applications in quantum information processing



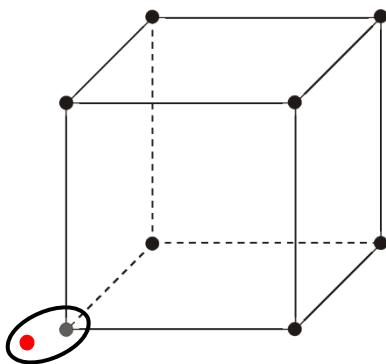
Graph $G = (V, E)$

$$\left. \begin{aligned} x_a \prod_{(a,b) \in E} z_b |\phi\rangle &= |\phi\rangle \\ \text{for all vertices } a \in V \end{aligned} \right\} \Rightarrow |\phi\rangle = |k_1, k_2, \dots, k_m\rangle$$

Graph state

N.B.: N qubits $\rightarrow 2^{\binom{N}{2}}$ different graphs

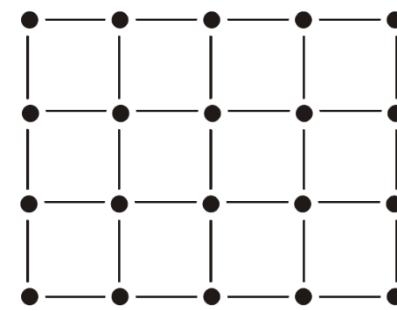
More examples of graph states:



Graph code



Resource for **encoding a qubit**
into the CSS [7,1,3] code

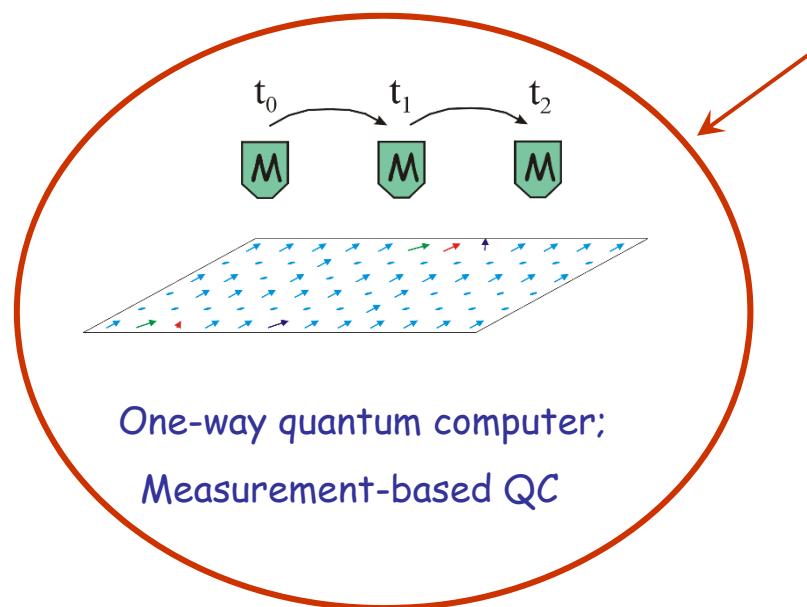
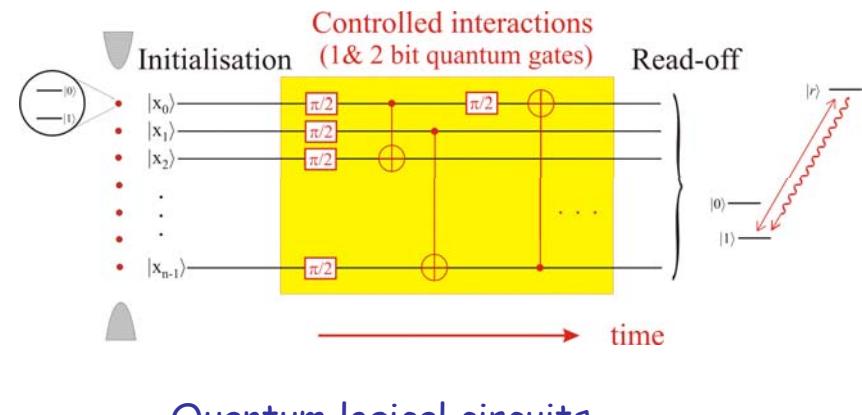
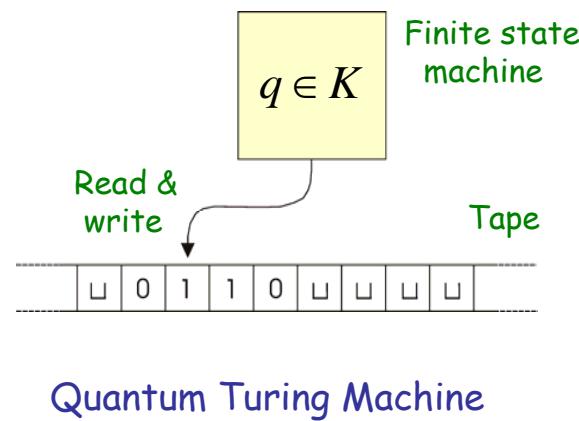


2D Cluster state

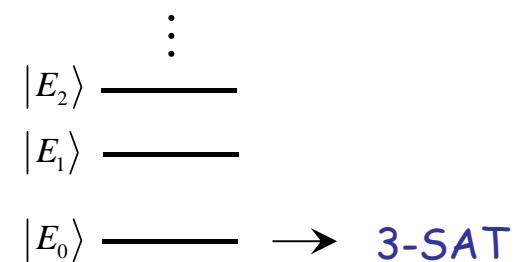


Resource for **universal**
quantum computation

Models for quantum computation



Role of entanglement explicit

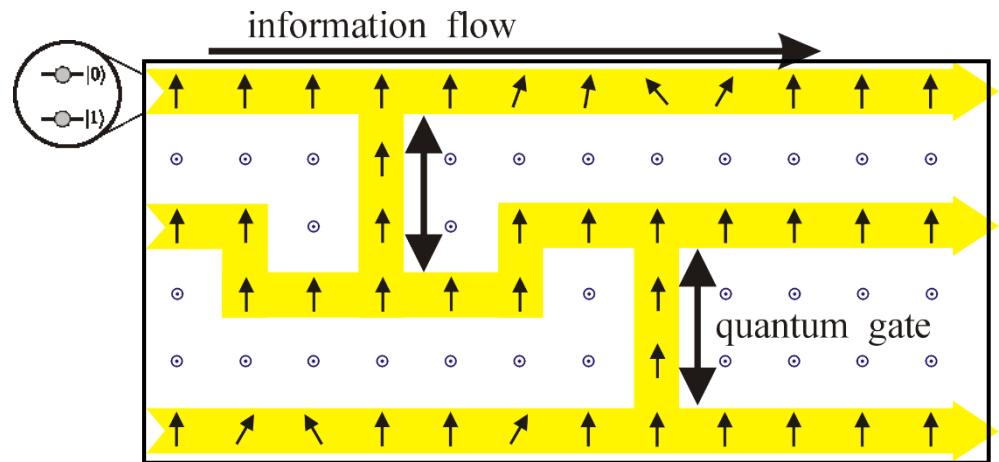


One-way quantum computer

1. Create entangled cluster state of qubits (e.g. via Ising interaction)

$$K^{(a)} |\phi\rangle_C = |\phi\rangle_C$$

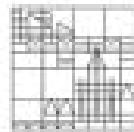
2. Measure individual qubits in certain order



measurements:

- in Z direction
- ↑ in X direction
- ↖ in X-Y plane

Quantum algorithm → Measurement pattern

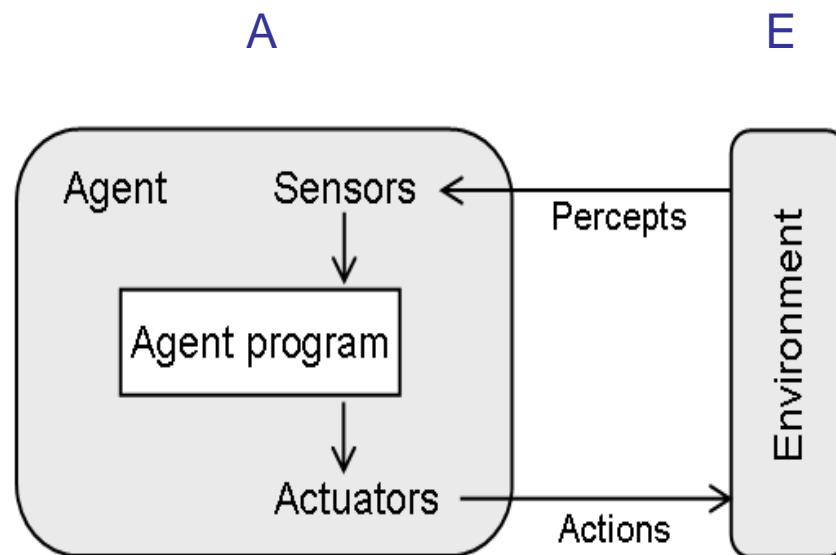


Learning and artificial intelligence in the quantum domain

Hans J. Briegel

Theoretical Physics, U Innsbruck
Department of Philosophy, U Konstanz

Artificial agents

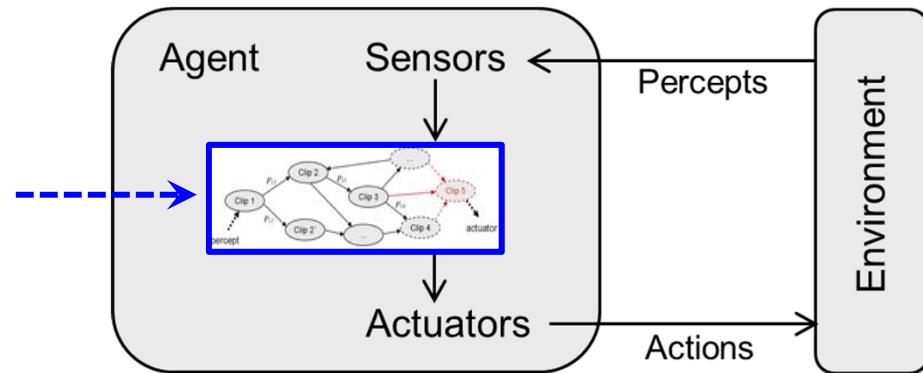


- Modern platform to discuss concepts of artificial intelligence
→ Computers vs. agents; robotics; *embodied artificial intelligence*
- Existing schemes in QIP can be described as (simple) agents
→ A-E framework for *quantum machine learning* and A.I.

Dunjko *et al.*, *PRL* **117**, 130501 (2016)

*from Russel & Norvig, *Artificial Intelligence, A modern approach*, Prentice Hall, 2010.

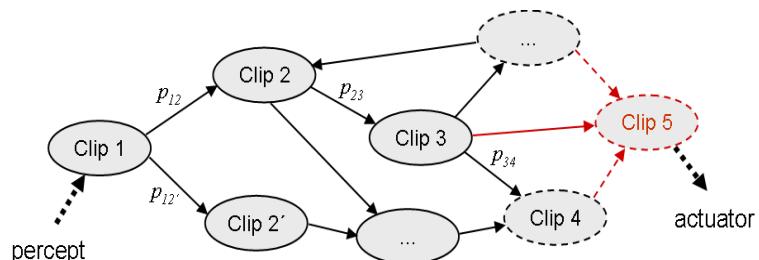
Quantum artificial agents



Four different classes: CC, CQ, QC, QQ (agent, environment)

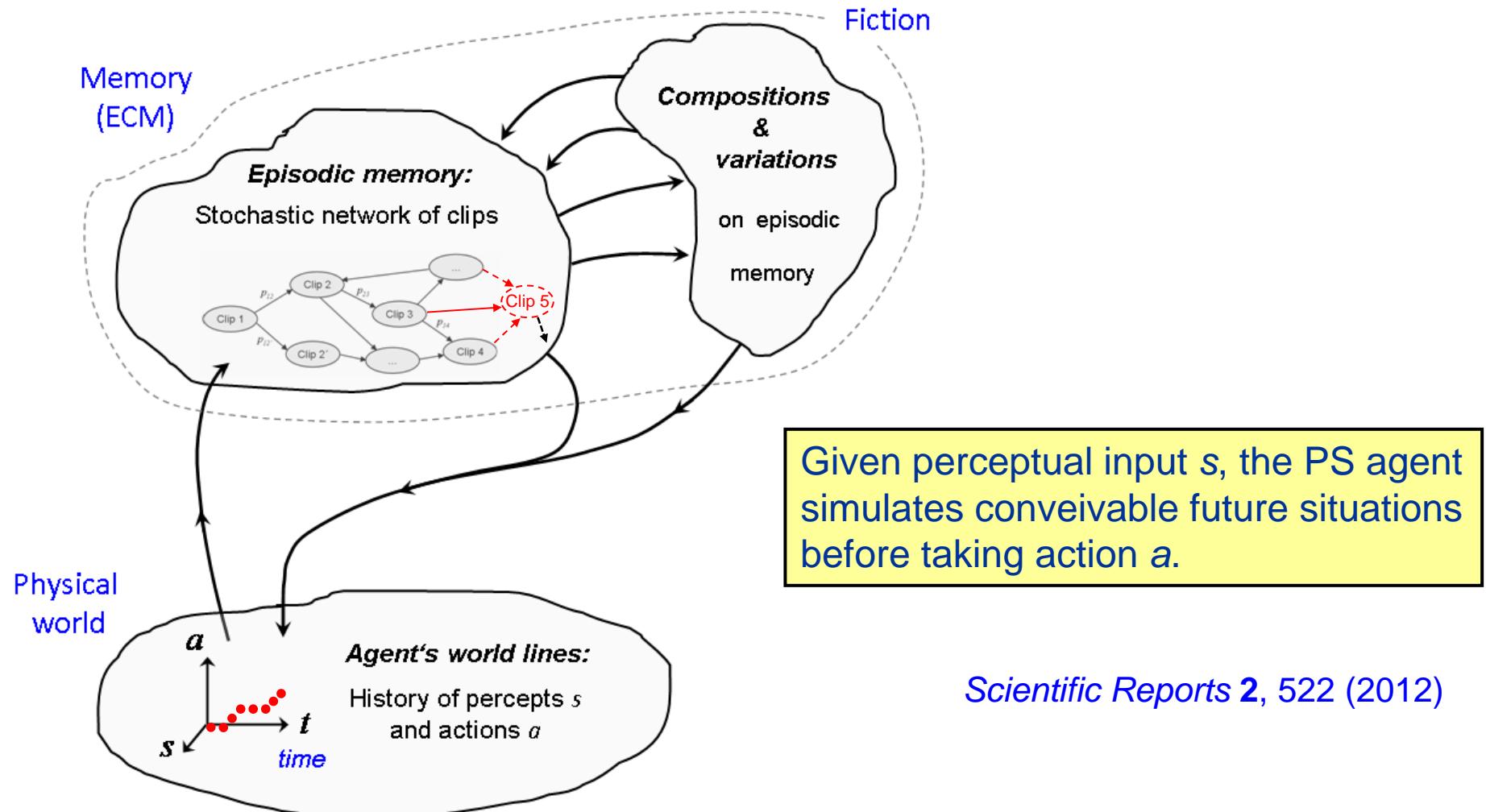
General framework: Dunjko & Briegel, *Machine learning and AI in the quantum domain*, Rep. Prog. Phys. **81**, 074001 (2018)

Projective simulation (PS): Agent model for deliberation and learning, based on episodic & compositional memory



Sci. Rep. **2**, 400 (2012)

Projective simulation learning agents

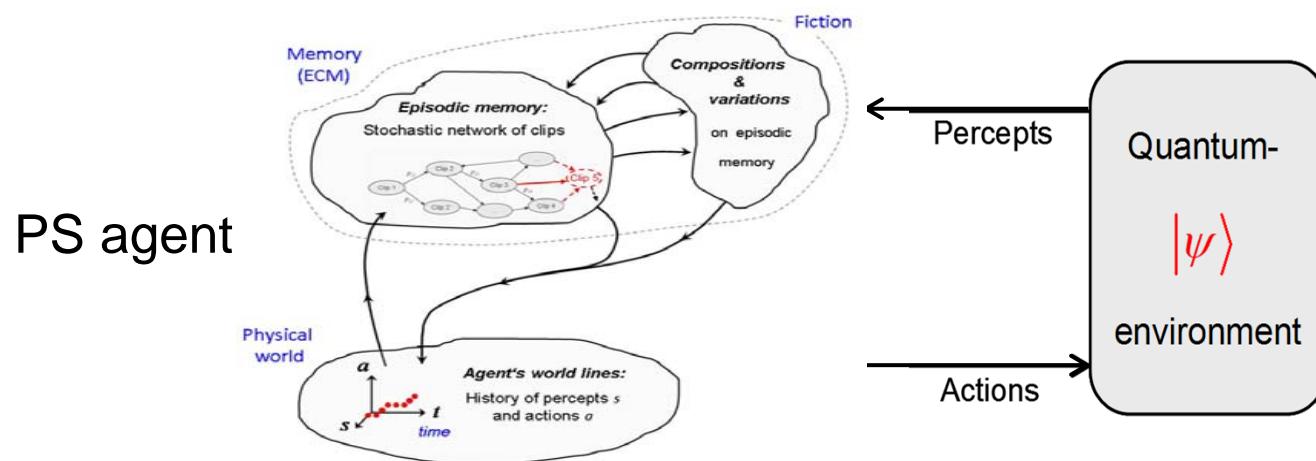


Experimental artificial agency

Which role will A.I. play in future basic research?

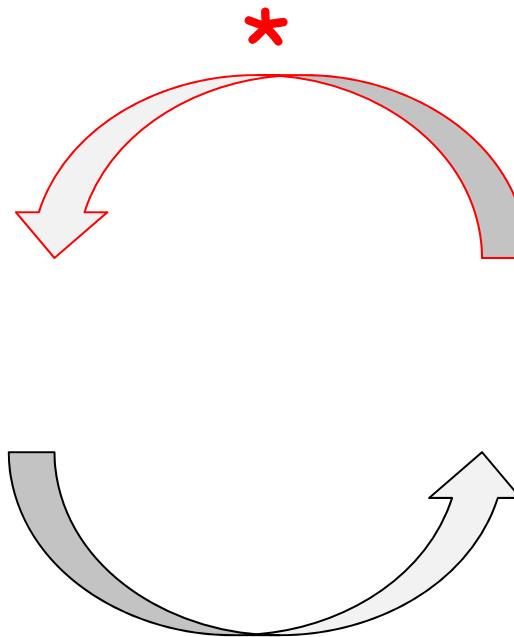
Learning agents can be used for the design of novel quantum experiments.

Melnikov *et al.*, PNAS 115, 1221 (2018)



Konzepte und Grundlagen
der Quantenmechanik

Anwendungen



----- APPENDIX -----