Introduction to Quantum Computing

A Comprehensive Guide for Computer Scientists

Jin-Guo Liu

HKUST(GZ) - FUNH - Advanced Materials Thrust

2025-09-13

Outline

Mermin-Peres magic square

Quantum principle

Quantum computation, AI and more

Outline

Mermin-Peres magic square

Quantum principle

Quantum computation, AI and more

The magic square game

This is a **collaborative** game where two players work together to pass a test.

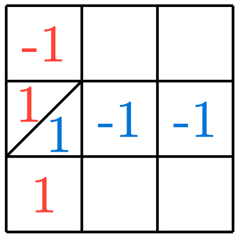
Players

- 👩 Rowena
- 👦 Colin

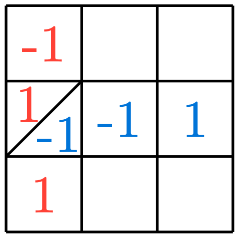
Board

Fill 1 or -1

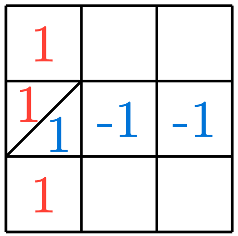
1. Game starts, the teacher tells Rowena and Colin a row/column number i/j.
   - 👩 Rowena gets $i(= 1, 2, 3)$
   - 👦 Colin gets j
2. Rowena and Colin fill the i-th row/j-th column with numbers (-1 or 1).
3. The teacher checks if the row/column product is 1/-1 and the numbers at the intersection are the same. If yes, Rowena and Colin pass the exam; otherwise, they fail.



win!



loss! inconsistency



loss! column product is 1

Winning strategy?

Rowena and Colin can agree on any kind of strategy **prior** to the game, but are not permitted to communicate during the game.

Question

Is there a 100% winning strategy for Rowena and Colin?

(5 min free discussion)

The optimal strategy for those who haven't studied quantum

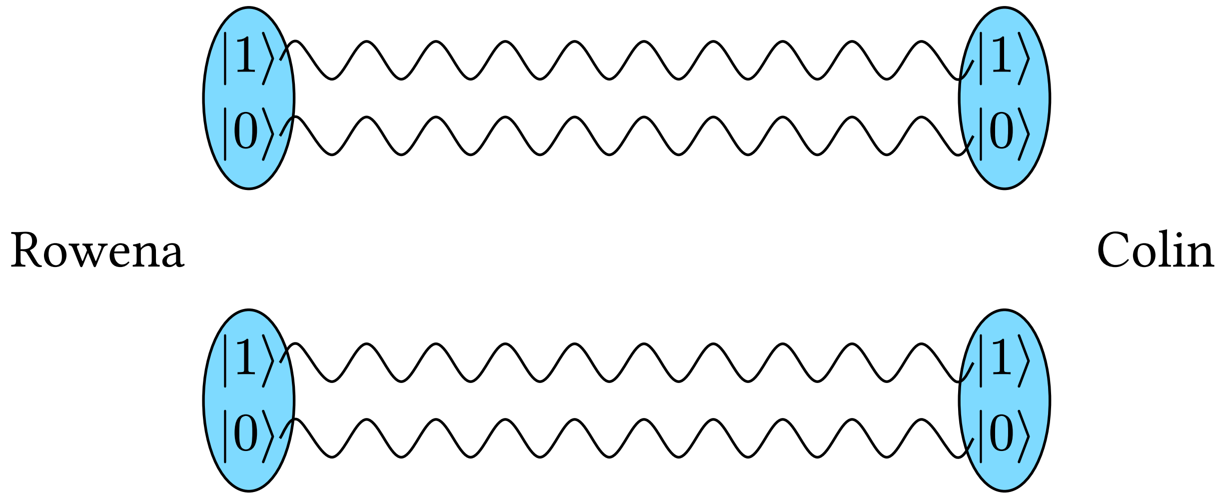
Sharing a predetermined table.

1	1	1
-1	1	-1
1	-1	?

success rate = $8/9 \approx 0.889$

Quantum solution to the Magic square game

superposition - both 0 and 1

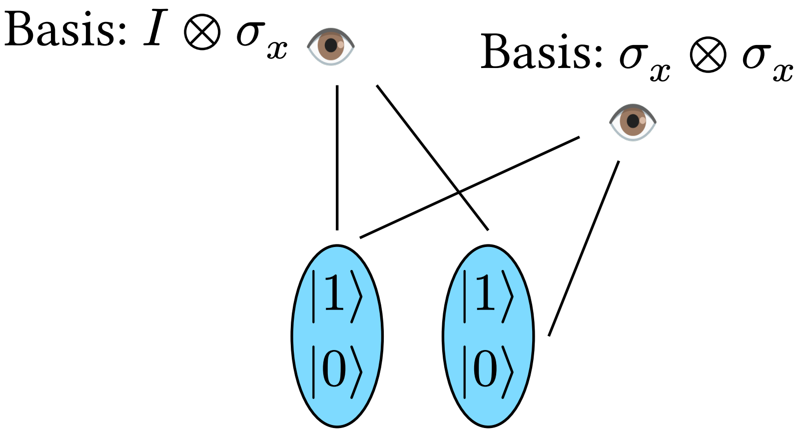


- Step 1: Share two **entangled** pairs of **qubits** (or **Bell pairs**) (Mermin, 1990). Each qubit can be in any **superposition** of $|0\rangle$ and $|1\rangle$ (this is the **Dirac notation**).
- Step 2: **Measure** the qubits, and send the outcome to the teacher.

Quantum solution to the Magic square game

Measure on different **bases**!

$$\begin{pmatrix} I\otimes\sigma_z & \sigma_z\otimes I & \sigma_z\otimes\sigma_z \\ \sigma_x\otimes I & I\otimes\sigma_x & \sigma_x\otimes\sigma_x \\ -\sigma_x\otimes\sigma_z & -\sigma_z\otimes\sigma_x & \sigma_y\otimes\sigma_y \end{pmatrix}$$



Finally verified by experiments (Xu et al., 2022).

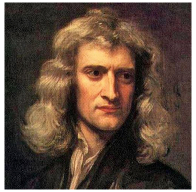
Outline

Mermin-Peres magic square

Quantum principle

Quantum computation, AI and more

Classical view of the world: probability is due to lack of knowledge



Newton's law: $f = ma$

- Our world is a deterministic machine, and the future is predictable.

How to understand probability?

Boltzmann distribution: $p(E) = e^{-\frac{E}{kT}}$

- Probability is due to a lack of knowledge about underlying **hidden variables**.

Probabilistic view of state

Probabilistic **state** is a real vector

$$\vec{p} = \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix}, \text{ s.t. } \sum_i p_i = 1$$

where n is the number of possible outcomes.

- bit: $x = 0$ or 1
- p-bit (Chowdhury et al., 2023): $p(x) = \binom{p}{1-p}$

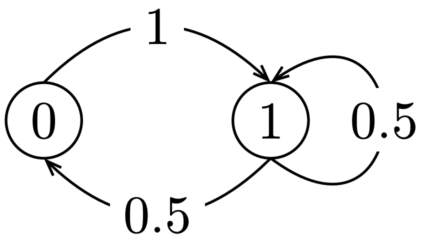
Probabilistic view of operations

Probabilistic **operation** is a transition matrix $\hat{T} = (t_{ij})$

$$\vec{p}' = \hat{T}\vec{p} \quad \text{s.t.} \quad t_{ij} \geq 0 \quad \text{and} \quad \sum_i t_{ij} = 1 \text{ by conservation of probability}$$

Example: $t_{10} = 1, t_{01} = 0.5, t_{11} = 0.5$

State Machine:



$$\hat{T} = \begin{pmatrix} 0 & 0.5 \\ 1 & 0.5 \end{pmatrix}$$

Example: Probabilistic NOT gate

- NOT gate (classical):

$$y = \neg x = \begin{cases} 1 & \text{if} \quad x = 0 \\ 0 & \text{if} \quad x = 1 \end{cases}$$

- NOT gate on a probabilistic bit:

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

- Probabilistic NOT gate on a bit:

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

state = 1

↓ (flip with probability 0.3)

$p(1) = 0.7$

$p(0) = 0.3$

Probabilistic gates are a **superset** of deterministic gates.

Probabilistic view of measurement

Probabilistic **measurement** is a sampling

$x \sim \vec{p}(x)$, after measurement, $\vec{p} \to \delta(x)$

$$\delta(x) = \begin{pmatrix} \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix}$$

$p(1) = 0.7$

$p(0) = 0.3$

$(p = 0.7) \swarrow$ 👁 $\searrow (p = 0.3)$

State = 1

State = 0

Note: The state is changed by measurement!

Probabilistic state space

Q: How many numbers are needed to represent an n-bit probability distribution:

$$p(x_1, x_2, ..., x_n)$$

Is PTM more powerful than Turing machine?

Answer: 2^n

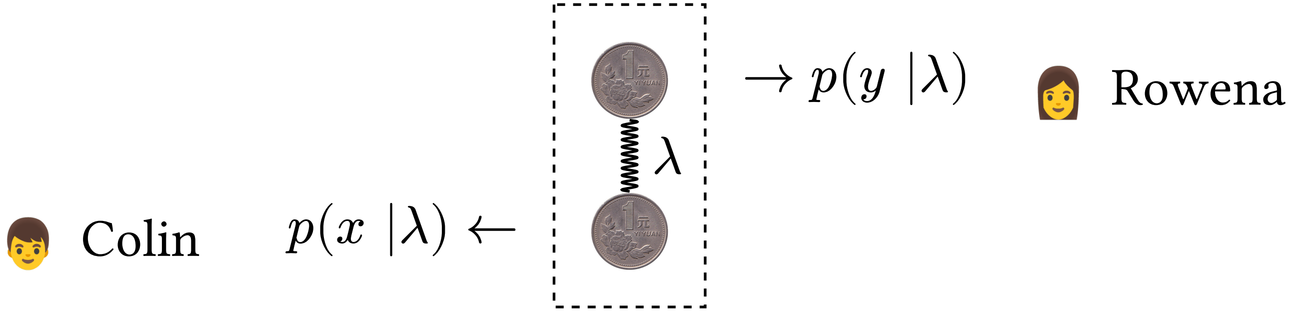
$$\boxed{\text{Probabilistic Turing machine (PTM)} = \text{Turing machine} + \text{Coin} \stackrel{?}{=} \text{Turing machine}}$$

PTM is probably not more powerful than a Turing machine, e.g., linear congruential generators can simulate random numbers.

$$X_{n+1} = (aX_n + c) \bmod m$$

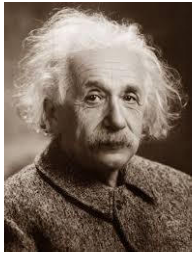
Hidden variable models

Let x and y be the bits that Colin and Rowena share.

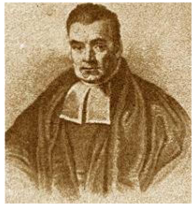


Q: If Colin and Rowena share coins with probability distribution $p(x, y|\lambda)$, can they have a higher success rate than 8/9?

Hidden variable models cannot explain our world



God does not play dice.



Classical statistics cannot help. 😔

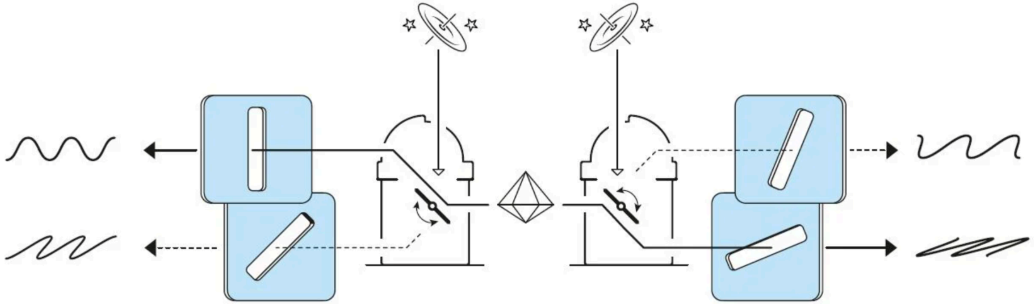


Figure 1: Bell's inequality experiment, Nobel prize in physics, 2022.

Probabilistic model with hidden variable λ:

$$\text{left} \sim \quad p(A) = p(A|\lambda)$$
$$\text{right} \sim \quad p(B) = p(B|\lambda)$$

Even with an infinite number of hidden variables, it is still impossible to explain the outcome!

Quantum view of state

A quantum state is the square root of a probability distribution:

$$|\psi\rangle = \sqrt{\vec{p}} \text{ (hand-waving)}$$

Quantum **state** is a vector of complex numbers

$$\text{Ket: } |\psi\rangle = \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix} = \begin{pmatrix} \sqrt{p_1} e^{i\varphi_1} \\ \sqrt{p_2} e^{i\varphi_2} \\ \vdots \\ \sqrt{p_n} e^{i\varphi_n} \end{pmatrix} \text{ s.t. } \langle\psi|\psi\rangle = 1$$

$$\text{Hermitian conjugate (bra): } \langle\psi| = \begin{pmatrix} \psi_1^* & \psi_2^* & \ldots & \psi_n^* \end{pmatrix}$$

Normalization of probability

$$\langle\psi|\psi\rangle = \begin{pmatrix}\psi_1^* & \psi_2^* & \ldots & \psi_n^*\end{pmatrix}\begin{pmatrix}\psi_1 \\ \psi_2 \\ \vdots \\ \psi_n\end{pmatrix} = \sum_i \psi_i^* \psi_i = \sum_i p_i = 1$$

For complex numbers, $\psi_i^* = \sqrt{p_i} e^{-i\varphi_i}$ and $\psi_i^* \psi_i = p_i$.

To access probability, we use basis vectors:

$$|i\rangle = \begin{pmatrix}\vdots \\ 0 \\ 1 \\ 0 \\ \vdots\end{pmatrix}, p_i = |\langle i|\psi\rangle|^2$$

Quantum view of operations

$$\text{Probabilistic operation: } \hat{T}\vec{p} = \vec{p'}, \text{ s.t. } \sum_i t_{ij} = 1$$

Quantum **operation** is a unitary operator.

$$\hat{U}|\psi\rangle = |\psi'\rangle \text{ s.t. } \hat{U}\hat{U}^\dagger = \hat{I} \text{ conservation of probability}$$

The normalization condition requires $\left(\langle\psi|U^\dagger\right)\left(U\ |\psi\rangle\right) = 1$ for any state $|\psi\rangle$. Hence, a quantum operation must be a **unitary operator**, i.e. $\hat{U}\hat{U}^\dagger = \hat{I}$.

Quantum computation, from classical gates to quantum gates

- Probabilistic NOT gate:

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

- Quantum NOT (or X) gate:

$$y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \sqrt{p} \\ \sqrt{1-p}e^{i\varphi} \end{pmatrix} = \begin{pmatrix} \sqrt{1-p}e^{i\varphi} \\ \sqrt{p} \end{pmatrix}$$

$$|0\rangle \; - \boxed{X} - \; |1\rangle$$

- Hadamard gate:

$$y = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

$$|0\rangle \; - \boxed{H} -$$

Unitary matrix vs. transition matrix

- *Remark*: Unitary matrices are reversible.
- *Remark*: Bennett showed (Bennett, 1982) that RTM = TM.
- *Remark*: Landauer's principle showed (Reeb & Wolf, 2014) that erasing information requires thermal dissipation.

- *Remark*: Two qubit quantum gates are universal (Dawson & Nielsen, 2005). Stronger: almost any single arbitrary two qubit gate is universal (Deutsch et al., 1995). Spectral gap theory shows any gate can be approximated exponentially fast (Bourgain & Gamburd, 2011).
- *Remark*: QTM $\geq$ PTM. Unitary circuits cannot be simulated classically in polynomial time

Quantum Measurement

Probabilistic measurement:

$$x \sim \vec{p}(x) = \delta(x)^T \vec{p}, \text{after measurement}, \quad \vec{p} \to \delta(x)$$

Quantum **measurement** follows the Born's rule:

$$x \sim |\langle x|\psi\rangle|^2, \text{after measurement}, \quad |\psi\rangle \to |x\rangle$$

Example: Quantum measurement

$$|\psi\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$\langle 0|\psi\rangle = \frac{1}{\sqrt{2}}, p(0) = |\langle 0|\psi\rangle|^2 = \frac{1}{2}$$
$$\langle 1|\psi\rangle = \frac{1}{\sqrt{2}}, p(1) = |\langle 1|\psi\rangle|^2 = \frac{1}{2}$$

With 50% probability, we get 0, and the state collapses to $|0\rangle$;

With 50% probability, we get 1, and the state collapses to $|1\rangle$.

Example: Quantum measurement

$$|\psi\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

$$\langle 0|\psi\rangle = \frac{1}{\sqrt{2}}, p(0) = |\langle 0|\psi\rangle|^2 = \frac{1}{2}$$

$$\langle 1|\psi\rangle = -\frac{1}{\sqrt{2}}, p(1) = |\langle 1|\psi\rangle|^2 = \frac{1}{2}$$

With 50% probability, we get 0, and the state collapses to $|0\rangle$;

With 50% probability, we get 1, and the state collapses to $|1\rangle$.

The difference!

Unlike classical probability, $|x\rangle$ can be any state! (not just the computational basis $|i\rangle$)

Basis is a **key** to access the information in the quantum state. Any set of **normalized, orthogonal states** can be a basis.

	z-basis	x-basis
Outcome: $\lambda = +1$	$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$|x;+\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$
Outcome: $\lambda = -1$	$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$|x;-\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$
Orthogonality	$\langle 0|1\rangle = 0$	$\langle x;+|x;-\rangle = 0$
Normalization	$\langle 0|0\rangle = 1$	$\langle x;+|x;+\rangle = 1$

Phase matters

$$\text{State:}\quad |\psi\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}}e^{i\varphi} \end{pmatrix}$$

$$\begin{aligned}
\text{Expectation value:}\quad \mathbb{E}(\sigma_z) &= \sum_i p_i \lambda_i \\
&= 1|\langle 0|\psi\rangle|^2 - 1|\langle 1|\psi\rangle|^2 \\
&= \left|\begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}}e^{i\varphi} \end{pmatrix}\right|^2 - \left|\begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}}e^{i\varphi} \end{pmatrix}\right|^2 \\
&= \frac{1}{2} - \frac{1}{2} = 0
\end{aligned}$$

Phase matters

$$
\begin{aligned}
\text{Expectation value } (\sigma_x):\ \ \mathbb{E}(\sigma_x) &= 1|\langle x; +|\psi\rangle|^2 - 1|\langle x; -|\psi\rangle|^2 \\
&= \left|\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} e^{i\varphi} \end{pmatrix}\right|^2 - \left|\begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} e^{-i\varphi} \end{pmatrix}\right|^2 \\
&= \cos(\varphi)
\end{aligned}
$$

That's all about quantum mechanics

Congratulations! You have learned all about quantum mechanics!

1. Quantum states are complex vectors.
2. Quantum operations are unitary operators.
3. Quantum measurement is described by the Born's rule.

Quantum observables

Quantum **observables** can be represented by Hermitian operators.

$$\langle\psi|\hat{A}|\psi\rangle \text{ s.t. } \quad \hat{A} = \hat{A}^\dagger$$

Measurement bases correspond to unitary operators

$$\begin{array}{cc} z\text{-basis} & x\text{-basis} \\ (|0\rangle, |1\rangle) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & (|x;+\rangle, |x;-\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ = I & = H \end{array}$$

Question: These bases are unitary—is this an accident?

Observable represented by Hermitian operator

Let $A^\dagger = A$ be a Hermitian operator. Then we have

$$U \Lambda_A U^\dagger = A,$$

where Λ_A is a **real** diagonal matrix of eigenvalues and U is a unitary matrix.

- U is a unitary operator representing the measurement basis.
- Λ_A contains the real values for labeling the outcomes of the measurement.

Why bother? Convenient for calculating expectation values

$$\langle\psi|A|\psi\rangle = \langle\psi|U\Lambda_A U^\dagger|\psi\rangle = \sum_i \lambda_i \, |\langle\psi|i\rangle|^2,$$

where

- λ_i is the value for the ith eigenvalue of A, representing the measurement outcome.
- $|i\rangle$ is the ith eigenvector of A, representing the measurement basis.

Popular observables: Pauli matrices

Pauli matrices are both Hermitian and unitary.

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The x, y, and z bases are on "equal footing"

$$\langle x; \pm |\ y; \pm \rangle = \langle x; \pm |\ z; \pm \rangle = \langle y; \pm |\ z; \pm \rangle = \frac{1}{2}$$

Q: Is there a fourth basis satisfying the same properties?

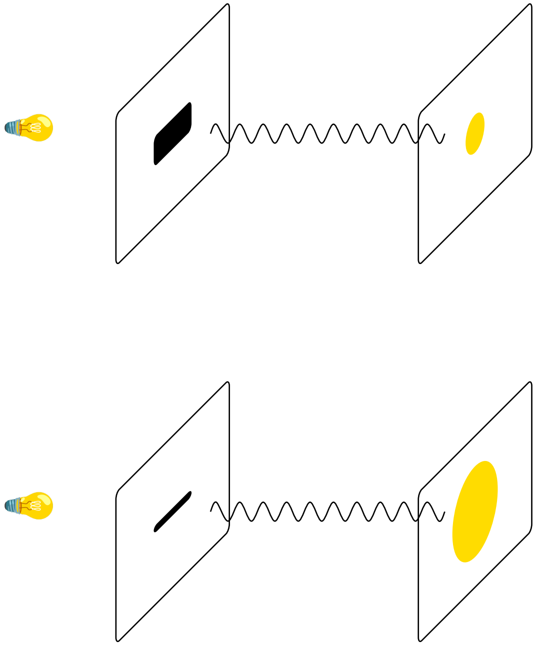
Key facts about quantum mechanics

- **Ubiquitous**: Quantum mechanics explains all phenomena in the microscopic world, e.g., superconductivity. The only missing piece in this course is the quantum dynamics.
- **Computational advantage**: Quantum many-body systems are intractable for classical computers(Arute et al., 2019), (Pan et al., 2022).
- **Delicate**: Quantum probabilities always reduce to classical probabilities at the macroscopic limit(Zhang et al., 2024).

Uncertainty principle

Information contained in different bases (e.g., σ_x and σ_z) cannot be simultaneously known precisely. (**Uncertainty principle**)

Uncertainty principle - position and momentum



The less we know about the position,
the more we know about the momentum.

Returning to the magic square game

Qubits are measured in different **bases**.

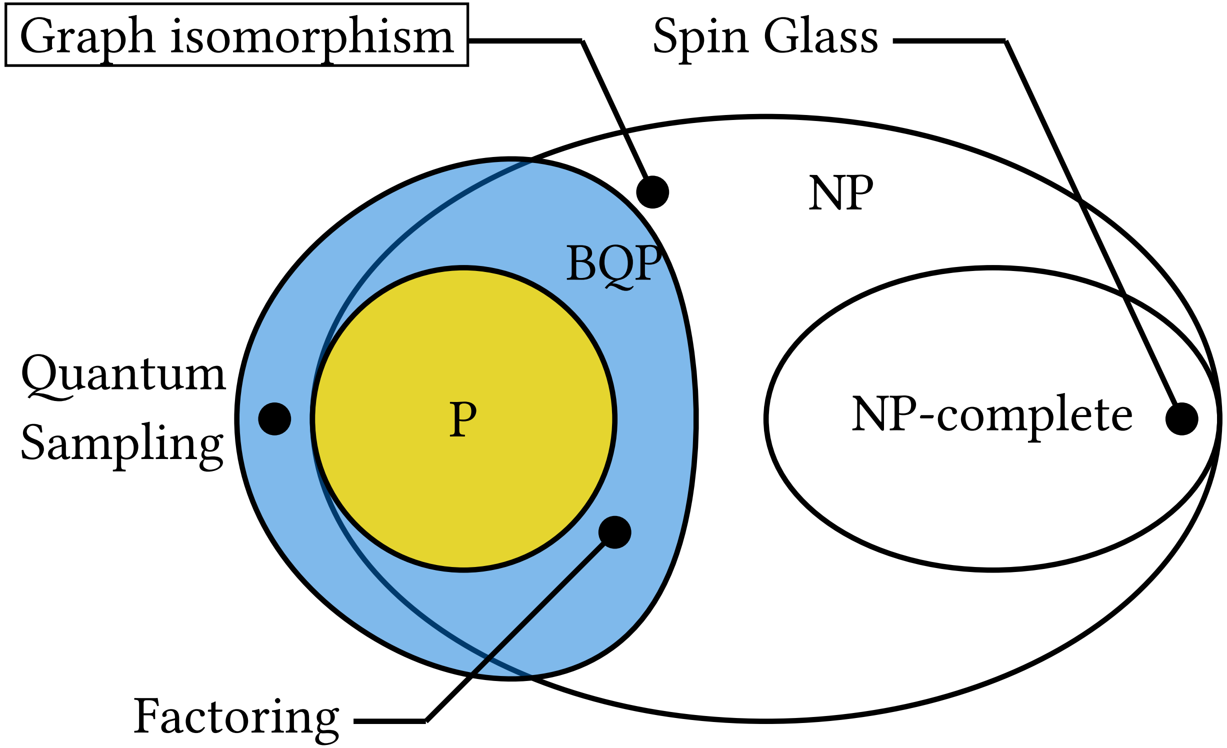
$$\begin{pmatrix} I \otimes \sigma_z & \sigma_z \otimes I & \sigma_z \otimes \sigma_z \\ \sigma_x \otimes I & I \otimes \sigma_x & \sigma_x \otimes \sigma_x \\ -\sigma_x \otimes \sigma_z & -\sigma_z \otimes \sigma_x & \sigma_y \otimes \sigma_y \end{pmatrix}$$

- Operators in the same row/column are **commuting** (can be measured simultaneously with certainty).
- The operators in the same row/column multiply to $+1/-1$, e.g.

$$\langle\psi|(\sigma_x \otimes I)(I \otimes \sigma_x)(\sigma_x \otimes \sigma_x)|\psi\rangle = 1$$
$$\langle\psi|(\sigma_z \otimes I)(I \otimes \sigma_x)(-\sigma_z \otimes \sigma_x)|\psi\rangle = -1$$

- The bell states, when measured, always give the same result.

Quantum complexity classes



P: Polynomial time solvable

NP: Polynomial time verifiable

NP-complete: The hardest problems in NP

BQP: Polynomial time solvable on a quantum computer

Outline

Mermin-Peres magic square

Quantum principle

Quantum computation, AI and more

Modeling probabilistic distributions with quantum circuits

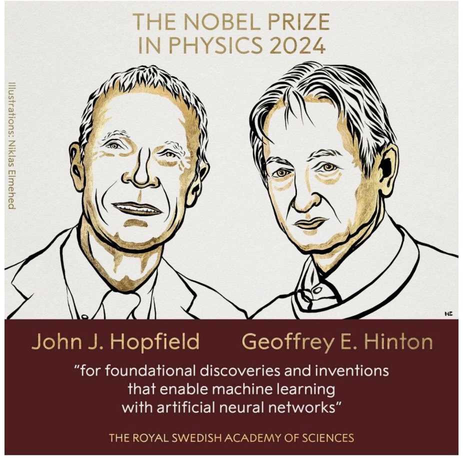
Born machine (Liu & Wang, 2018)

Contextual recurrent neural network(Anschuetz et al., 2023)

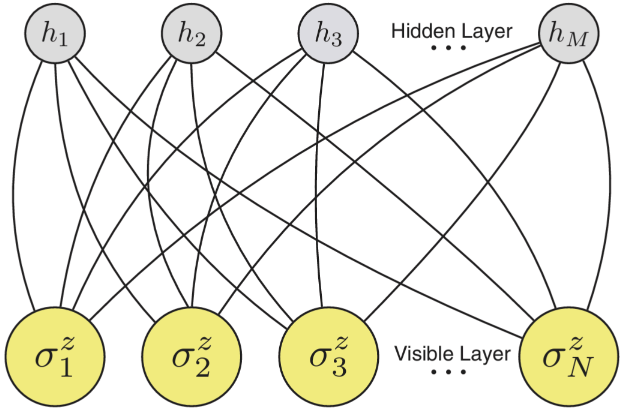
Input	"Debemos limpiar la cocina."
Truth	"We must clean up the kitchen."
CRNN	"We must clean the kitchen."
GRU	"We have to turn the right address."

What can AI do for quantum physics?

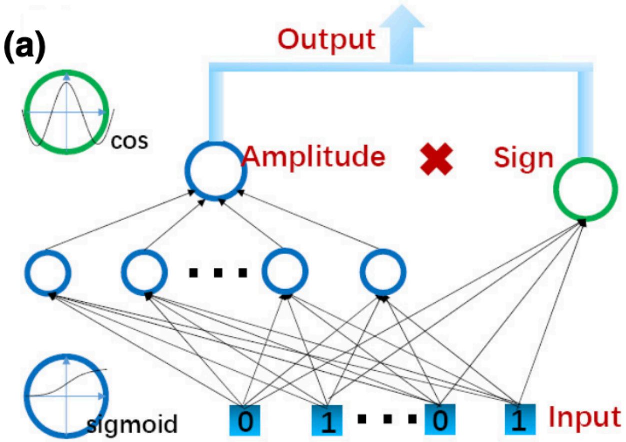
Restricted Boltzmann Machine (RBM) for quantum states.



(Hinton & Salakhutdinov, 2006)



(Carleo & Troyer, 2017)



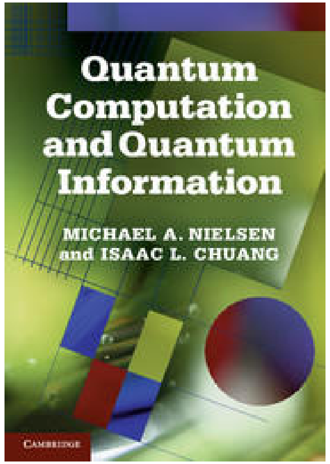
(Cai & Liu, 2018)

Hardware

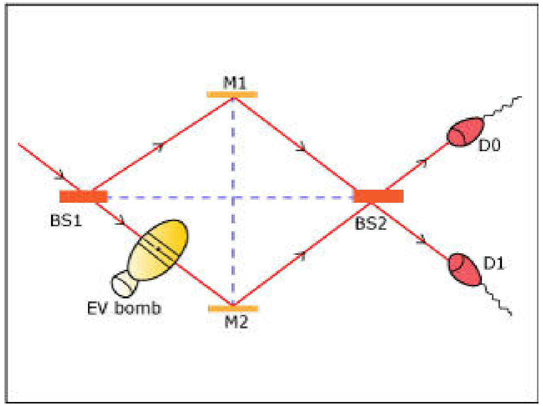
Nuclear magnetic resonance (NMR) qubits (3 qubits)
Location: W3-6F, Modern Matter Lab

Learning resources

Book: Nielsen & Chuang: Quantum Computation and Quantum Information



MIT Open Course: Quantum Physics I, II, III



References

[1] N. D. Mermin, “Simple unified form for the major no-hidden-variables theorems,” *Physical review letters*, vol. 65, no. 27, p. 3373, 1990.

[2] J.-M. Xu *et al.*, “Experimental demonstration of quantum pseudotelepathy,” *Physical Review Letters*, vol. 129, no. 5, p. 50402, 2022.

[3] S. Chowdhury *et al.*, “A full-stack view of probabilistic computing with p-bits: devices, architectures, and algorithms,” *IEEE Journal on Exploratory Solid-State Computational Devices and Circuits*, vol. 9, no. 1, pp. 1–11, 2023.

[4] C. H. Bennett, “The Thermodynamics of Computation–a Review,” vol. 21, no. 12, pp. 905–940, 1982.

[5] D. Reeb and M. M. Wolf, “An Improved Landauer Principle with Finite-Size Corrections,” *New Journal of Physics*, vol. 16, pp. 1–34, 2014, doi: 10.1088/1367-2630/16/10/103011.

References

[6] C. M. Dawson and M. A. Nielsen, "The Solovay-Kitaev Algorithm," no. arXiv:quant-ph/0505030. arXiv, Aug. 2005. doi: 10.48550/arXiv.quant-ph/0505030.

[7] D. Deutsch, A. Barenco, and A. Ekert, "Universality in Quantum Computation," *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, vol. 449, no. 1937, pp. 669–677, Jun. 1995, doi: 10.1098/rspa.1995.0065.

[8] J. Bourgain and A. Gamburd, "A Spectral Gap Theorem in \$SU(d)\$," no. arXiv:1108.6264. arXiv, Aug. 2011. doi: 10.48550/arXiv.1108.6264.

[9] F. Arute *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.

[10] F. Pan, K. Chen, and P. Zhang, "Solving the sampling problem of the sycamore quantum circuits," *Physical Review Letters*, vol. 129, no. 9, p. 90502, 2022.

THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY (GUANGZHOU) 香港科技大學(廣州)

References

[11] T. Zhang *et al.*, "Quantification of Entanglement and Coherence with Purity Detection," *npj Quantum Information*, vol. 10, no. 1, p. 60, Jun. 2024, doi: 10.1038/s41534-024-00857-2.

[12] J.-G. Liu and L. Wang, "Differentiable learning of quantum circuit born machines," *Physical Review A*, vol. 98, no. 6, p. 62324, 2018.

[13] E. R. Anschuetz, H.-Y. Hu, J.-L. Huang, and X. Gao, "Interpretable quantum advantage in neural sequence learning," *PRX Quantum*, vol. 4, no. 2, p. 20338, 2023.

[14] G. E. Hinton and R. R. Salakhutdinov, "Reducing the dimensionality of data with neural networks," *science*, vol. 313, no. 5786, pp. 504–507, 2006.

[15] G. Carleo and M. Troyer, "Solving the quantum many-body problem with artificial neural networks," *Science*, vol. 355, no. 6325, pp. 602–606, 2017.

References

[16] Z. Cai and J. Liu, "Approximating Quantum Many-Body Wave Functions Using Artificial Neural Networks," *Physical Review B*, vol. 97, no. 3, p. 35116, Jan. 2018, doi: 10.1103/PhysRevB.97.035116.