

MS!C

Síla kvantového počítání

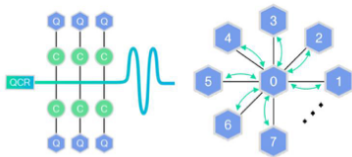
prof. RNDr. Marek Lampart, Ph.D.

(Vedoucí laboratoře kvantových výpočtů)

VŠB – Technická Univerzita Ostrava
marek.lampart@vsb.cz

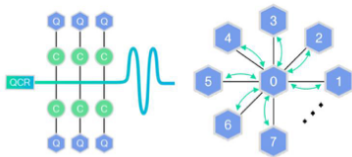
1. října, 2024

MS!C



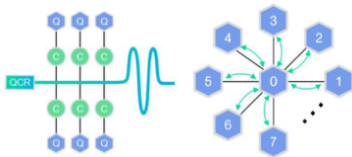
- Hvězdicová qubitová topologie, jednotné qubitové připojení,
- Výrazné snížení počtu operací SWAP
- Možné vysoce komplexní kvantové algoritmy
- Obrovský pokrok ve srovnání s čímkoli, co je v současné době k dispozici
- Zvýšený výkon





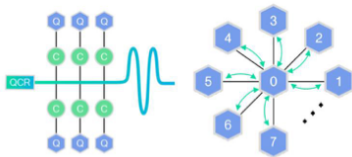
- Hvězdicová qubitová topologie, jednotné qubitové připojení,
- Výrazné snížení počtu operací SWAP
- Možné vysoce komplexní kvantové algoritmy
- Obrovský pokrok ve srovnání s čímkoli, co je v současné době k dispozici
- Zvýšený výkon





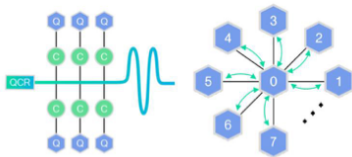
- Hvězdicová qubitová topologie, jednotné qubitové připojení,
- Výrazné snížení počtu operací SWAP
- Možné vysoce komplexní kvantové algoritmy
- Obrovský pokrok ve srovnání s čímkoli, co je v současné době k dispozici
- Zvýšený výkon





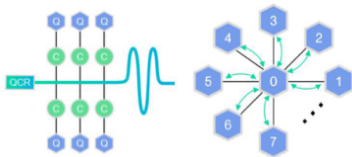
- Hvězdicová qubitová topologie, jednotné qubitové připojení,
- Výrazné snížení počtu operací SWAP
- Možné vysoce komplexní kvantové algoritmy
- Obrovský pokrok ve srovnání s čímkoli, co je v současné době k dispozici
- Zvýšený výkon





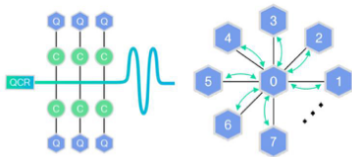
- Hvězdicová qubitová topologie, jednotné qubitové připojení,
- Výrazné snížení počtu operací SWAP
- Možné vysoce komplexní kvantové algoritmy
- Obrovský pokrok ve srovnání s čímkoli, co je v současné době k dispozici
- Zvýšený výkon





- Hvězdicová qubitová topologie, jednotné qubitové připojení,
- Výrazné snížení počtu operací SWAP
- Možné vysoce komplexní kvantové algoritmy
- Obrovský pokrok ve srovnání s čímkoli, co je v současné době k dispozici
- Zvýšený výkon





- Hvězdicová qubitová topologie, jednotné qubitové připojení,
- Výrazné snížení počtu operací SWAP
- Možné vysoce komplexní kvantové algoritmy
- Obrovský pokrok ve srovnání s čímkoli, co je v současné době k dispozici
- Zvýšený výkon



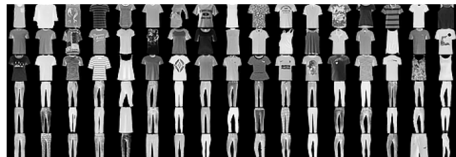


CUDA QUANTUM

■ NVIDIA CUDA Quantum

- Platforma pro hybridní kvantově-klasické výpočty
- Schopnost přepínat mezi běhy na CPU a QPU
- Příklad hybridní QNN s datasetem MNIST, rozpoznávání mezi ručně psanými číslicemi 0 a 1
- Příklad hybridní QNN rozlišující mezi různými obrázky oblečení
- Příklad na VQE: molekula H_2 , energie v rovnovážné poloze

- Použití CuTENSOR pro simulace na GPU pomocí Qiskitu.
 - Vytvořený modul na Karolině, který obsahuje jak Qiskit, tak CUDA a CuTENSOR (možné okamžité spuštění)
 - Minimální funkční příklad – měření kvantového obvodu (2 qubity)
 - Příklad na QNN bude přidán (kód v Qiskit, simulace s použitím backendu CuTENSOR)

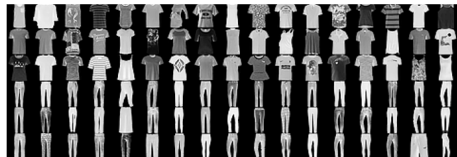




CUDA QUANTUM

- NVIDIA CUDA Quantum
 - Platforma pro hybridní kvantově-klasické výpočty
 - Schopnost přepínat mezi běhy na CPU a QPU
 - Příklad hybridní QNN s datasetem MNIST, rozpoznávání mezi ručně psanými číslicemi 0 a 1
 - Příklad hybridní QNN rozlišující mezi různými obrázky oblečení
 - Příklad na VQE: molekula H_2 , energie v rovnovážné poloze

- Použití CuTENSOR pro simulace na GPU pomocí Qiskitu.
 - Vytvořený modul na Karolině, který obsahuje jak Qiskit, tak CUDA a CuTENSOR (možné okamžité spuštění)
 - Minimální funkční příklad – měření kvantového obvodu (2 qubity)
 - Příklad na QNN bude přidán (kód v Qiskit, simulace s použitím backendu CuTENSOR)





- 2018 Quantum Technologies Flagship** desetiletá iniciativa s cílem využít evropské vědecké excelence v kvantových technologiích a přiblížit výsledky výzkumu k průmyslovému využití a aplikacím v reálném životě. <https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship>
- 2019 EuroQCI** na výstavbu a nasazení bezpečné kvantové komunikační infrastruktury, včetně komunikace satelitní, pokrývající celou EU.
<https://digital-strategy.ec.europa.eu/cs/policies/european-quantum-communication-infrastructure-euroqci>
- 2021 Nařízení Rady o zřízení Společného podniku Evropského vysoce výkonnou výpočetní techniku (HPC)** potřebu rozvíjet špičkové ekosystémy v HPC a kvantových výpočtech a jejich aplikacích po celé Evropě.
<https://eur-lex.europa.eu/CS/legal-content/summary/european-high-performance-computing-joint-undertaking.html>
- 2024 Evropská kvantové deklarace** – Česká republika přistoupila v únoru 2024, signatářské země deklarují podporu rozvoji kvantových technologií.
<https://digital-strategy.ec.europa.eu/cs/news/eu-member-states-commit-cooperating-world-class-quantum-technologies>
- 2023 Národní úřad pro kybernetickou a informační bezpečnost** – „Minimální požadavky na kryptografické algoritmy“ https://nukib.gov.cz/download/uredni_deska/Minimalni%20pozadavky%20na%20kryptograficke%20algoritmy.pdf
- ???? Národní kvantová strategie České republiky** – v přípravě Petr Kavalír
<https://digitalnicesko.gov.cz/aktuality/jednani-ceskeho-digitalniho-tymu-o-narodni-kvantov/>

- 2018 Quantum Technologies Flagship** desetiletá iniciativa s cílem využít evropské vědecké excelence v kvantových technologiích a přiblížit výsledky výzkumu k průmyslovému využití a aplikacím v reálném životě. <https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship>
- 2019 EuroQCI** na výstavbu a nasazení bezpečné kvantové komunikační infrastruktury, včetně komunikace satelitní, pokrývající celou EU.
<https://digital-strategy.ec.europa.eu/cs/policies/european-quantum-communication-infrastructure-euroqci>
- 2021 Nařízení Rady o zřízení Společného podniku Evropského vysoce výkonnou výpočetní techniku (HPC)** potřebu rozvíjet špičkové ekosystémy v HPC a kvantových výpočtech a jejich aplikacích po celé Evropě.
<https://eur-lex.europa.eu/CS/legal-content/summary/european-high-performance-computing-joint-undertaking.html>
- 2024 Evropská kvantové deklarace** – Česká republika přistoupila v únoru 2024, signatářské země deklarují podporu rozvoji kvantových technologií.
<https://digital-strategy.ec.europa.eu/cs/news/eu-member-states-commit-cooperating-world-class-quantum-technologies>
- 2023 Národní úřad pro kybernetickou a informační bezpečnost** – „Minimální požadavky na kryptografické algoritmy“ https://nukib.gov.cz/download/uredni_deska/Minimalni%20požadavky%20na%20kryptograficke%20algoritmy.pdf
- ???? Národní kvantová strategie České republiky** – v přípravě Petr Kavalír
<https://digitalnicesko.gov.cz/aktuality/jednani-ceskeho-digitalniho-tymu-o-narodni-quantum/>

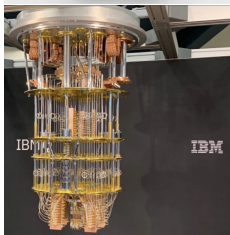
- 2018 Quantum Technologies Flagship** desetiletá iniciativa s cílem využít evropské vědecké excelence v kvantových technologiích a přiblížit výsledky výzkumu k průmyslovému využití a aplikacím v reálném životě. <https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship>
- 2019 EuroQCI** na výstavbu a nasazení bezpečné kvantové komunikační infrastruktury, včetně komunikace satelitní, pokrývající celou EU.
<https://digital-strategy.ec.europa.eu/cs/policies/european-quantum-communication-infrastructure-euroqci>
- 2021 Nařízení Rady o zřízení Společného podniku Evropského vysoce výkonnou výpočetní techniku (HPC)** potřebu rozvíjet špičkové ekosystémy v HPC a kvantových výpočtech a jejich aplikacích po celé Evropě.
<https://eur-lex.europa.eu/CS/legal-content/summary/european-high-performance-computing-joint-undertaking.html>
- 2024 Evropská kvantové deklarace** – Česká republika přistoupila v únoru 2024, signatářské země deklarují podporu rozvoji kvantových technologií.
<https://digital-strategy.ec.europa.eu/cs/news/eu-member-states-commit-cooperating-world-class-quantum-technologies>
- 2023 Národní úřad pro kybernetickou a informační bezpečnost** – „Minimální požadavky na kryptografické algoritmy“ https://nukib.gov.cz/download/uredni_deska/Minimalni%20pozadavky%20na%20kryptograficke%20algoritmy.pdf
- ???? Národní kvantová strategie České republiky** – v přípravě Petr Kavalír
<https://digitalnicesko.gov.cz/aktuality/jednani-ceskeho-digitalniho-tymu-o-narodni-kvantov/>

- 2018 Quantum Technologies Flagship** desetiletá iniciativa s cílem využít evropské vědecké excelence v kvantových technologiích a přiblížit výsledky výzkumu k průmyslovému využití a aplikacím v reálném životě. <https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship>
- 2019 EuroQCI** na výstavbu a nasazení bezpečné kvantové komunikační infrastruktury, včetně komunikace satelitní, pokrývající celou EU.
<https://digital-strategy.ec.europa.eu/cs/policies/european-quantum-communication-infrastructure-euroqci>
- 2021 Nařízení Rady o zřízení Společného podniku Evropského vysoce výkonnou výpočetní techniku (HPC)** potřebu rozvíjet špičkové ekosystémy v HPC a kvantových výpočtech a jejich aplikacích po celé Evropě.
<https://eur-lex.europa.eu/CS/legal-content/summary/european-high-performance-computing-joint-undertaking.html>
- 2024 Evropská kvantové deklarace** – Česká republika přistoupila v únoru 2024, signatářské země deklarují podporu rozvoji kvantových technologií.
<https://digital-strategy.ec.europa.eu/cs/news/eu-member-states-commit-cooperating-world-class-quantum-technologies>
- 2023 Národní úřad pro kybernetickou a informační bezpečnost** – „Minimální požadavky na kryptografické algoritmy“ https://nukib.gov.cz/download/uredni_deska/Minimalni%20pozadavky%20na%20kryptograficke%20algoritmy.pdf
- ???? Národní kvantová strategie České republiky** – v přípravě Petr Kavalír
<https://digitalnicesko.gov.cz/aktuality/jednani-ceskeho-digitalniho-tymu-o-narodni-kvantov/>

- 2018 Quantum Technologies Flagship** desetiletá iniciativa s cílem využít evropské vědecké excelence v kvantových technologiích a přiblížit výsledky výzkumu k průmyslovému využití a aplikacím v reálném životě. <https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship>
- 2019 EuroQCI** na výstavbu a nasazení bezpečné kvantové komunikační infrastruktury, včetně komunikace satelitní, pokrývající celou EU.
<https://digital-strategy.ec.europa.eu/cs/policies/european-quantum-communication-infrastructure-euroqci>
- 2021 Nařízení Rady o zřízení Společného podniku Evropského vysoce výkonnou výpočetní techniku (HPC)** potřebu rozvíjet špičkové ekosystémy v HPC a kvantových výpočtech a jejich aplikacích po celé Evropě.
<https://eur-lex.europa.eu/CS/legal-content/summary/european-high-performance-computing-joint-undertaking.html>
- 2024 Evropská kvantové deklarace** – Česká republika přistoupila v únoru 2024, signatářské země deklarují podporu rozvoji kvantových technologií.
<https://digital-strategy.ec.europa.eu/cs/news/eu-member-states-commit-cooperating-world-class-quantum-technologies>
- 2023 Národní úřad pro kybernetickou a informační bezpečnost** – „Minimální požadavky na kryptografické algoritmy“ https://nukib.gov.cz/download/uredni_deska/Minimalni%20požadavky%20na%20kryptograficke%20algoritmy.pdf
- ???? Národní kvantová strategie České republiky** – v přípravě Petr Kavalír
<https://digitalnicesko.gov.cz/aktuality/jednani-ceskeho-digitalniho-tymu-o-narodni-kvantov/>

- 2018 Quantum Technologies Flagship** desetiletá iniciativa s cílem využít evropské vědecké excelence v kvantových technologiích a přiblížit výsledky výzkumu k průmyslovému využití a aplikacím v reálném životě. <https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship>
- 2019 EuroQCI** na výstavbu a nasazení bezpečné kvantové komunikační infrastruktury, včetně komunikace satelitní, pokrývající celou EU.
<https://digital-strategy.ec.europa.eu/cs/policies/european-quantum-communication-infrastructure-euroqci>
- 2021 Nařízení Rady o zřízení Společného podniku Evropského vysoce výkonnou výpočetní techniku (HPC)** potřebu rozvíjet špičkové ekosystémy v HPC a kvantových výpočtech a jejich aplikacích po celé Evropě.
<https://eur-lex.europa.eu/CS/legal-content/summary/european-high-performance-computing-joint-undertaking.html>
- 2024 Evropská kvantové deklarace** – Česká republika přistoupila v únoru 2024, signatářské země deklarují podporu rozvoji kvantových technologií.
<https://digital-strategy.ec.europa.eu/cs/news/eu-member-states-commit-cooperating-world-class-quantum-technologies>
- 2023 Národní úřad pro kybernetickou a informační bezpečnost** – „Minimální požadavky na kryptografické algoritmy“ https://nukib.gov.cz/download/uredni_deska/Minimalni%20pozadavky%20na%20kryptograficke%20algoritmy.pdf
- ???? Národní kvantová strategie České republiky** – v přípravě Petr Kavalír
<https://digitalnicesko.gov.cz/aktuality/jednani-ceskeho-digitalniho-tymu-o-narodni-kvantov/>

- 2018 Quantum Technologies Flagship** desetiletá iniciativa s cílem využít evropské vědecké excelence v kvantových technologiích a přiblížit výsledky výzkumu k průmyslovému využití a aplikacím v reálném životě. <https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship>
- 2019 EuroQCI** na výstavbu a nasazení bezpečné kvantové komunikační infrastruktury, včetně komunikace satelitní, pokrývající celou EU.
<https://digital-strategy.ec.europa.eu/cs/policies/european-quantum-communication-infrastructure-euroqci>
- 2021 Nařízení Rady o zřízení Společného podniku Evropského vysoce výkonnou výpočetní techniku (HPC)** potřebu rozvíjet špičkové ekosystémy v HPC a kvantových výpočtech a jejich aplikacích po celé Evropě.
<https://eur-lex.europa.eu/CS/legal-content/summary/european-high-performance-computing-joint-undertaking.html>
- 2024 Evropská kvantové deklarace** – Česká republika přistoupila v únoru 2024, signatářské země deklarují podporu rozvoji kvantových technologií.
<https://digital-strategy.ec.europa.eu/cs/news/eu-member-states-commit-cooperating-world-class-quantum-technologies>
- 2023 Národní úřad pro kybernetickou a informační bezpečnost** – „Minimální požadavky na kryptografické algoritmy“ https://nukib.gov.cz/download/uredni_deska/Minimalni%20pozadavky%20na%20kryptograficke%20algoritmy.pdf
- ???? Národní kvantová strategie České republiky** – v přípravě Petr Kavalír
<https://digitalnicesko.gov.cz/aktuality/jednani-ceskeho-digitalniho-tymu-o-narodni-kvantov/>



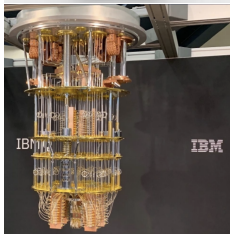
■ Kvantový počítač

- teoretický model zařízení vykonávající výpočty
- využívá fenomény kvantové mechaniky: **superpozice**, **interference**

■ Kvantové počítání

- v klasickém počítači data reprezentujeme **bity** (0, 1)
- v kvantovém počítači se používáme **qubity** (kvantové bity), které mohou být nula, jedna, nebo i kombinace obou





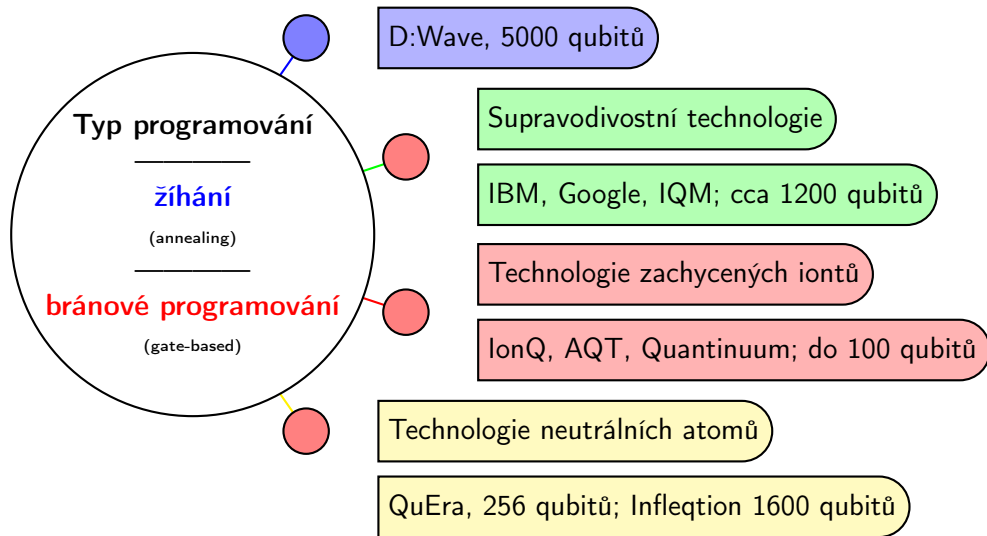
■ Kvantový počítač

- teoretický model zařízení vykonávající výpočty
- využívá fenomény kvantové mechaniky: **superpozice**, **interference**

■ Kvantové počítání

- v klasickém počítači data reprezentujeme **bity** (0, 1)
- v kvantovém počítači se používáme **qubity** (kvantové bity), které mohou být nula, jedna, nebo i kombinace obou





Žihání vs. programování bran

	annealing	bránové programování
kvantová výhoda	zatím nedokázáno	několik důkazů
zrychlení	polynomiální	exponenciální
příklady použití	optimalizační úlohy	všude

Dosahování propletenosti různých technologií

supravodivost	zachycené ionty	neutrální atomy
CNOT	MS	CNOT

Žíhání vs. programování bran

	annealing	bránové programování
kvantová výhoda	zatím nedokázáno	několik důkazů
zrychlení	polynomiální	exponenciální
příklady použití	optimalizační úlohy	všude

Dosahování propletenosti různých technologií

supravodivost	zachycené ionty	neutrální atomy
CNOT	MS	CNOT

Žíhání vs. programování bran

	annealing	bránové programování
kvantová výhoda	zatím nedokázáno	několik důkazů
zrychlení	polynomiální	exponenciální
příklady použití	optimalizační úlohy	všude

Dosahování propletenosti různých technologií

supravodivost	zachycené ionty	neutrální atomy
CNOT	MS	CNOT

Žíhání vs. programování bran

	annealing	bránové programování
kvantová výhoda	zatím nedokázáno	několik důkazů
zrychlení	polynomiální	exponenciální
příklady použití	optimalizační úlohy	všude

Dosahování propletenosti různých technologií

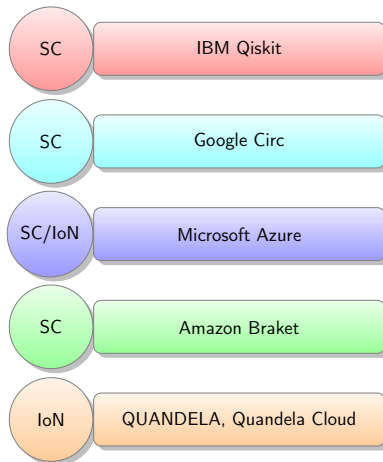
supravodivost	zachycené ionty	neutrální atomy
CNOT	MS	CNOT

Žíhání vs. programování bran

	annealing	bránové programování
kvantová výhoda	zatím nedokázáno	několik důkazů
zrychlení	polynomiální	exponenciální
příklady použití	optimalizační úlohy	všude

Dosahování propletenosti různých technologií

supravodivost	zachycené ionty	neutrální atomy
CNOT	MS	CNOT



"Quantum computers are here!"

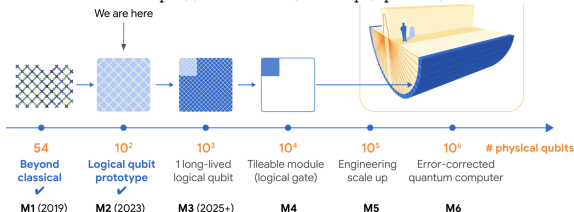
"... it's not question **when** but **who** ... nobody will share it with us"

J. I. Latorre, Univ. Barcelona, CYBER WEEK, Tel Aviv, 2019

<https://www.youtube.com/watch?v=400FnZTPqyc>

2023	2024	2025	2027	2029	2030+
Introduce parallelization of quantum computations. 2023 is all about pushing speed in quantum workflows by introducing parallelization in the Qiskit Primitives.	Expand the utility of quantum computing. We will improve the quality and speed of quantum circuits to allow running 5,000 gates with parametric circuits.	Demonstrate quantum-centric supercomputing. In 2025, we will enhance the quality of quantum circuits to allow running 7,500 gates and bring together modular processors, middleware, and quantum communication to demonstrate the first quantum-centric supercomputer.	Scale quantum computing. We will scale qubits, electronics, infrastructure, and software to reduce footprint, cost, and energy usage. The quality of quantum circuits will improve to allow running 10,000 gates.	Deliver a fully error-corrected system. We will bring users a quantum system with 200 qubits capable of running 100 million gates.	Deliver quantum-centric supercomputers with 1,000's of logical qubits. Beyond 2033, quantum-centric supercomputers will include thousands of qubits capable of running 1 billion gates, unlocking the full power of quantum computing.

<https://www.ibm.com/roadmaps/quantum/>



<https://quantumai.google/decmilestone>



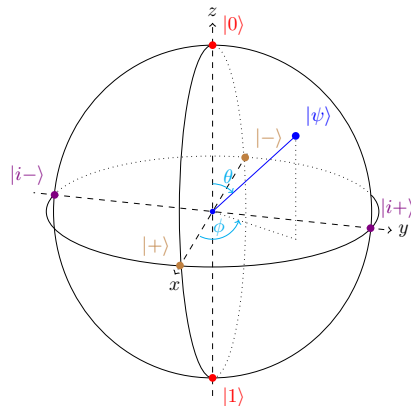
Kvantový bit (zkráceně *qubit*) je dvoudimenzionální kvantově mechanický systém, který je ve stavu

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

kde α i β jsou komplexní čísla, což jsou *amplitudy* kvantových stavů $|0\rangle$ resp. $|1\rangle$, platí $|\alpha|^2 + |\beta|^2 = 1$.

V této definici se užívá standardní *bra-ketová* notace, tedy označuje

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



Kvantový registr

- zahrnuje více qubitů najednou,
- kvantový registr je tedy analogie klasického procesorového registru a kvantové počítače provádějí výpočty pomocí manipulací qubitů v rámci daného registru,
- každý qubit $|\psi\rangle$ v registru je superpozicí $\alpha|0\rangle + \beta|1\rangle$ prvků výpočetní báze $|0\rangle$ a $|1\rangle$,
- registr s n qubity je superpozicí všech možných 2^n bitových řetězců, které mohou být reprezentovány n bity,
- stavový prostor n kvantového registru je lineární kombinací n báзовých vektorů délky 2^n

$$|\psi_n\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle \quad (1)$$

kde i je celé číslo v desítkové soustavě reprezentující číslo délky n ve dvojkové soustavě.

Kvantový registr

- zahrnuje více qubitů najednou,
- kvantový registr je tedy analogie klasického procesorového registru a kvantové počítače provádějí výpočty pomocí manipulací qubitů v rámci daného registru,
- každý qubit $|\psi\rangle$ v registru je superpozicí $\alpha|0\rangle + \beta|1\rangle$ prvků výpočetní báze $|0\rangle$ a $|1\rangle$,
- registr s n qubity je superpozicí všech možných 2^n bitových řetězců, které mohou být reprezentovány n bity,
- stavový prostor n kvantového registru je lineární kombinací n báзовých vektorů délky 2^n

$$|\psi_n\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle \quad (1)$$

kde i je celé číslo v desítkové soustavě reprezentující číslo délky n ve dvojkové soustavě.

Kvantový registr

- zahrnuje více qubitů najednou,
- kvantový registr je tedy analogie klasického procesorového registru a kvantové počítače provádějí výpočty pomocí manipulací qubitů v rámci daného registru,
- každý qubit $|\psi\rangle$ v registru je superpozicí $\alpha|0\rangle + \beta|1\rangle$ prvků výpočetní báze $|0\rangle$ a $|1\rangle$,
- registr s n qubity je superpozicí všech možných 2^n bitových řetězců, které mohou být reprezentovány n bity,
- stavový prostor n kvantového registru je lineární kombinací n báзовých vektorů délky 2^n

$$|\psi_n\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle \quad (1)$$

kde i je celé číslo v desítkové soustavě reprezentující číslo délky n ve dvojkové soustavě.

Kvantový registr

- zahrnuje více qubitů najednou,
- kvantový registr je tedy analogie klasického procesorového registru a kvantové počítače provádějí výpočty pomocí manipulací qubitů v rámci daného registru,
- každý qubit $|\psi\rangle$ v registru je superpozicí $\alpha|0\rangle + \beta|1\rangle$ prvků výpočetní báze $|0\rangle$ a $|1\rangle$,
- registr s n qubity je superpozicí všech možných 2^n bitových řetězců, které mohou být reprezentovány n bity,
- stavový prostor n kvantového registru je lineární kombinací n báзовých vektorů délky 2^n

$$|\psi_n\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle \quad (1)$$

kde i je celé číslo v desítkové soustavě reprezentující číslo délky n ve dvojkové soustavě.

Kvantový registr

- zahrnuje více qubitů najednou,
- kvantový registr je tedy analogie klasického procesorového registru a kvantové počítače provádějí výpočty pomocí manipulací qubitů v rámci daného registru,
- každý qubit $|\psi\rangle$ v registru je superpozicí $\alpha|0\rangle + \beta|1\rangle$ prvků výpočetní báze $|0\rangle$ a $|1\rangle$,
- registr s n qubity je superpozicí všech možných 2^n bitových řetězců, které mohou být reprezentovány n bity,
- stavový prostor n kvantového registru je lineární kombinací n báзовých vektorů délky 2^n

$$|\psi_n\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle \quad (1)$$

kde i je celé číslo v desítkové soustavě reprezentující číslo délky n ve dvojkové soustavě.

Kvantový registr

- zahrnuje více qubitů najednou,
- kvantový registr je tedy analogie klasického procesorového registru a kvantové počítače provádějí výpočty pomocí manipulací qubitů v rámci daného registru,
- každý qubit $|\psi\rangle$ v registru je superpozicí $\alpha|0\rangle + \beta|1\rangle$ prvků výpočetní báze $|0\rangle$ a $|1\rangle$,
- registr s n qubity je superpozicí všech možných 2^n bitových řetězců, které mohou být reprezentovány n bity,
- stavový prostor n kvantového registru je lineární kombinací n báзовých vektorů délky 2^n

$$|\psi_n\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle \quad (1)$$

kde i je celé číslo v desítkové soustavě reprezentující číslo délky n ve dvojkové soustavě.

- Pro (1) platí normalizační podmínka pro jednotlivé amplitudy pravděpodobností:

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1. \quad (2)$$

- Logicky, součet pravděpodobností všech možných stavů musí být 1, protože žádný jiný stav nastat nemůže a zároveň se jednotlivé stavy navzájem vylučují.
- Kvantové registry jsou přímým rozšířením qubitů.

- Pro (1) platí normalizační podmínka pro jednotlivé amplitudy pravděpodobností:

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1. \quad (2)$$

- Logicky, součet pravděpodobností všech možných stavů musí být 1, protože žádný jiný stav nastat nemůže a zároveň se jednotlivé stavy navzájem vylučují.
- Kvantové registry jsou přímým rozšířením qubitů.

- Pro (1) platí normalizační podmínka pro jednotlivé amplitudy pravděpodobností:

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1. \quad (2)$$

- Logicky, součet pravděpodobností všech možných stavů musí být 1, protože žádný jiný stav nastat nemůže a zároveň se jednotlivé stavy navzájem vylučují.
- Kvantové registry jsou přímým rozšířením qubitů.

- Každá bitová konfigurace v kvantové superpozici je označena jako tenzorový součin jednotlivých qubitů.
- Například $|010\rangle$, která reprezentuje v bitovém řetězci číslo 2, má tvar:

$$|010\rangle = |0\rangle \otimes |1\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = (00100000)^T.$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

- Každá bitová konfigurace v kvantové superpozici je označena jako tenzorový součin jednotlivých qubitů.
- Například $|010\rangle$, která reprezentuje v bitovém řetězci číslo 2, má tvar:

$$|010\rangle = |0\rangle \otimes |1\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = (00100000)^T.$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

- Každá bitová konfigurace v kvantové superpozici je označena jako tenzorový součin jednotlivých qubitů.
- Například $|010\rangle$, která reprezentuje v bitovém řetězci číslo 2, má tvar:

$$|010\rangle = |0\rangle \otimes |1\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = (00100000)^T.$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

- Každá bitová konfigurace v kvantové superpozici je označena jako tenzorový součin jednotlivých qubitů.
- Například $|010\rangle$, která reprezentuje v bitovém řetězci číslo 2, má tvar:

$$|010\rangle = |0\rangle \otimes |1\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = (00100000)^T.$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

Například tří qubitový registr má tvar

$$\begin{aligned} |\psi_3\rangle &= \alpha_0 |000\rangle + \alpha_1 |001\rangle + \alpha_2 |010\rangle + \alpha_3 |011\rangle + \alpha_4 |100\rangle + \alpha_5 |101\rangle + \alpha_6 |110\rangle + \alpha_7 |111\rangle \\ &= \sum_{i=0}^7 \alpha_i |i\rangle. \end{aligned}$$

- Klasické logické brány jsou matematicky popsány pomocí Booleovské algebry. Kvantové logické brány fungují na podobném principu.
- Kvantové logické brány aplikované na kvantové registry zobrazují kvantovou superpozici na jinou a společně umožňují vývoj systému do nějakého požadovaného konečného stavu, správné odpovědi.
- Kvantové logické brány jsou matematicky reprezentovány pomocí transformací matic (lineárních operací) aplikovaných na kvantový registr tenzorováním transformačních matic maticí reprezentující daný registr.
- Všechny matice odpovídající kvantové logické bráně jsou *unitární*¹.
- Unitární transformace prováděné na jednom qubitu mohou být efektivně vizualizovány na Blochově sféře.
- Tak jako v případě klasických logických bran je i v případě kvantových logických bran zavedena standardní množina používaných bran.

¹Komplexní matice U je *unitární* právě tehdy, když $U^{-1} = U^\dagger$, kde $U^\dagger$ je matice konjugovaná k matici U ($U^\dagger = \overline{U}^T$). Navíc platí $UU^\dagger = U^\dagger U = I$.

- Klasické logické brány jsou matematicky popsány pomocí Booleovské algebry. Kvantové logické brány fungují na podobném principu.
- Kvantové logické brány aplikované na kvantové registry zobrazují kvantovou superpozici na jinou a společně umožňují vývoj systému do nějakého požadovaného konečného stavu, správné odpovědi.
- Kvantové logické brány jsou matematicky reprezentovány pomocí transformací matic (lineárních operací) aplikovaných na kvantový registr tenzorováním transformačních matic maticí reprezentující daný registr.
- Všechny matice odpovídající kvantové logické bráně jsou *unitární*¹.
- Unitární transformace prováděné na jednom qbitu mohou být efektivně vizualizovány na Blochově sféře.
- Tak jako v případě klasických logických bran je i v případě kvantových logických bran zavedena standardní množina používaných bran.

¹Komplexní matice U je *unitární* právě tehdy, když $U^{-1} = U^\dagger$, kde $U^\dagger$ je matice konjugovaná k matici U ($U^\dagger = \overline{U}^T$). Navíc platí $UU^\dagger = U^\dagger U = I$.

- Klasické logické brány jsou matematicky popsány pomocí Booleovské algebry. Kvantové logické brány fungují na podobném principu.
- Kvantové logické brány aplikované na kvantové registry zobrazují kvantovou superpozici na jinou a společně umožňují vývoj systému do nějakého požadovaného konečného stavu, správné odpovědi.
- Kvantové logické brány jsou matematicky reprezentovány pomocí transformací matic (lineárních operací) aplikovaných na kvantový registr tenzorováním transformačních matic maticí reprezentující daný registr.
- Všechny matice odpovídající kvantové logické bráně jsou *unitární*¹.
- Unitární transformace prováděné na jednom qbitu mohou být efektivně vizualizovány na Blochově sféře.
- Tak jako v případě klasických logických bran je i v případě kvantových logických bran zavedena standardní množina používaných bran.

¹Komplexní matice U je *unitární* právě tehdy, když $U^{-1} = U^\dagger$, kde $U^\dagger$ je matice konjugovaná k matici U ($U^\dagger = \overline{U}^T$). Navíc platí $UU^\dagger = U^\dagger U = I$.

- Klasické logické brány jsou matematicky popsány pomocí Booleovské algebry. Kvantové logické brány fungují na podobném principu.
- Kvantové logické brány aplikované na kvantové registry zobrazují kvantovou superpozici na jinou a společně umožňují vývoj systému do nějakého požadovaného konečného stavu, správné odpovědi.
- Kvantové logické brány jsou matematicky reprezentovány pomocí transformací matic (lineárních operací) aplikovaných na kvantový registr tenzorováním transformačních matic maticí reprezentující daný registr.
- Všechny matice odpovídající kvantové logické bráně jsou *unitární*¹.
- Unitární transformace prováděné na jednom qbitu mohou být efektivně vizualizovány na Blochově sféře.
- Tak jako v případě klasických logických bran je i v případě kvantových logických bran zavedena standardní množina používaných bran.

¹Komplexní matice U je *unitární* právě tehdy, když $U^{-1} = U^\dagger$, kde $U^\dagger$ je matice konjugovaná k matici U ($U^\dagger = \overline{U}^T$). Navíc platí $UU^\dagger = U^\dagger U = I$.

- Klasické logické brány jsou matematicky popsány pomocí Booleovské algebry. Kvantové logické brány fungují na podobném principu.
- Kvantové logické brány aplikované na kvantové registry zobrazují kvantovou superpozici na jinou a společně umožňují vývoj systému do nějakého požadovaného konečného stavu, správné odpovědi.
- Kvantové logické brány jsou matematicky reprezentovány pomocí transformací matic (lineárních operací) aplikovaných na kvantový registr tenzorováním transformačních matic maticí reprezentující daný registr.
- Všechny matice odpovídající kvantové logické bráně jsou *unitární*¹.
- Unitární transformace prováděné na jednom qbitu mohou být efektivně vizualizovány na Blochově sféře.
- Tak jako v případě klasických logických bran je i v případě kvantových logických bran zavedena standardní množina používaných bran.

¹Komplexní matice U je *unitární* právě tehdy, když $U^{-1} = U^\dagger$, kde $U^\dagger$ je matice konjugovaná k matici U ($U^\dagger = \overline{U}^T$). Navíc platí $UU^\dagger = U^\dagger U = I$.

- Klasické logické brány jsou matematicky popsány pomocí Booleovské algebry. Kvantové logické brány fungují na podobném principu.
- Kvantové logické brány aplikované na kvantové registry zobrazují kvantovou superpozici na jinou a společně umožňují vývoj systému do nějakého požadovaného konečného stavu, správné odpovědi.
- Kvantové logické brány jsou matematicky reprezentovány pomocí transformací matic (lineárních operací) aplikovaných na kvantový registr tenzorováním transformačních matic maticí reprezentující daný registr.
- Všechny matice odpovídající kvantové logické bráně jsou *unitární*¹.
- Unitární transformace prováděné na jednom qbitu mohou být efektivně vizualizovány na Blochově sféře.
- Tak jako v případě klasických logických bran je i v případě kvantových logických bran zavedena standardní množina používaných bran.

¹Komplexní matice U je *unitární* právě tehdy, když $U^{-1} = U^\dagger$, kde $U^\dagger$ je matice konjugovaná k matici U ($U^\dagger = \overline{U}^T$). Navíc platí $UU^\dagger = U^\dagger U = I$.

- *Pauliho brány* X , Y a Z odpovídají rotaci o úhel π kolem osy x , y či z respektive.
- Pauliho brána X přehodí amplitudy $|0\rangle$ a $|1\rangle$

$$\boxed{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

- *Pauliho brány* X , Y a Z odpovídají rotaci o úhel π kolem osy x , y či z respektive.
- Pauliho brána X přehodí amplitudy $|0\rangle$ a $|1\rangle$

$$\boxed{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

- *Pauliho brány* X , Y a Z odpovídají rotaci o úhel π kolem osy x , y či z respektive.
- Pauliho brána X přehodí amplitudy $|0\rangle$ a $|1\rangle$

$$\boxed{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

- *Pauliho brány* X , Y a Z odpovídají rotaci o úhel π kolem osy x , y či z respektive.
- Pauliho brána X přehodí amplitudy $|0\rangle$ a $|1\rangle$

$$\boxed{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

- Nejdůležitější a taky nejpoužívanější binární kvantovou branou je CNOT



$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} |11\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle$$

- Nejdůležitější a taky nejpoužívanější binární kvantovou branou je CNOT

$$\begin{array}{c} \text{---} \bullet \text{---} \\ | \\ \text{---} \oplus \text{---} \end{array} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} |11\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle$$

- Nejdůležitější a taky nejpoužívanější binární kvantovou branou je CNOT

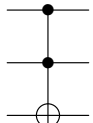
$$\begin{array}{c} \text{---} \bullet \text{---} \\ | \\ \text{---} \oplus \text{---} \end{array} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} |11\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle$$

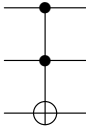
Nejdůležitější a taky nejpoužívanější ternární kvantovou branou je **Toffoliho brána** (CCNOT)


$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Nejdůležitější a taky nejpoužívanější ternární kvantovou branou je **Toffoliho brána** (CCNOT)

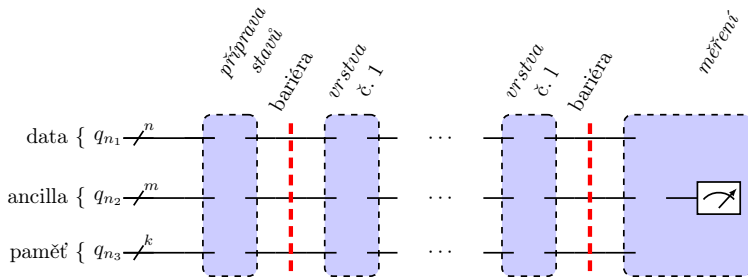

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Brána	značení	vstup	výstup
Pauli-X		$ 0\rangle$	$ 1\rangle$
		$ 1\rangle$	$ 0\rangle$
CNOT		$ 00\rangle$	$ 00\rangle$
		$ 01\rangle$	$ 01\rangle$
		$ 10\rangle$	$ 11\rangle$
		$ 11\rangle$	$ 10\rangle$

Brána	značení	vstup	výstup
Toffoli		$ 000\rangle$	$ 000\rangle$
		$ 001\rangle$	$ 001\rangle$
		$ 010\rangle$	$ 010\rangle$
		$ 100\rangle$	$ 100\rangle$
		$ 011\rangle$	$ 011\rangle$
		$ 101\rangle$	$ 101\rangle$
		$ 110\rangle$	$ 111\rangle$
		$ 111\rangle$	$ 110\rangle$

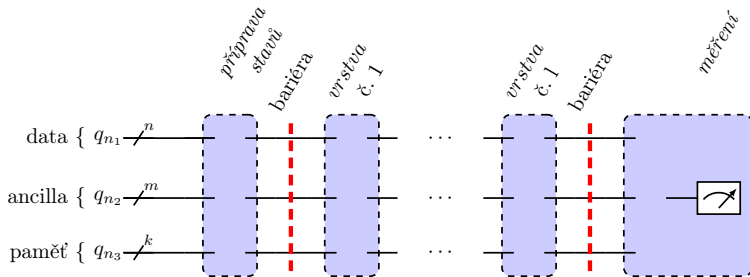
Tři základní vrstvy:

1. kódování dat, která mohou být klasická nebo kvantová, do stavu sady vstupních qubitů,
2. posloupnost kvantových bran aplikovaných na tuto sadu vstupních qubitů,
3. měření jednoho nebo více qubitů na konci pro získání klasicky interpretovatelného výsledku.



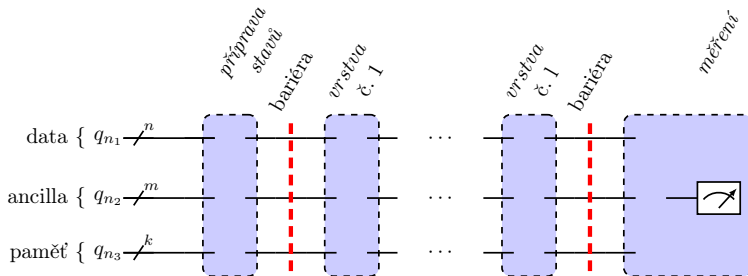
Tři základní vrstvy:

1. kódování dat, která mohou být klasická nebo kvantová, do stavu sady vstupních qubitů,
2. posloupnost kvantových bran aplikovaných na tuto sadu vstupních qubitů,
3. měření jednoho nebo více qubitů na konci pro získání klasicky interpretovatelného výsledku.



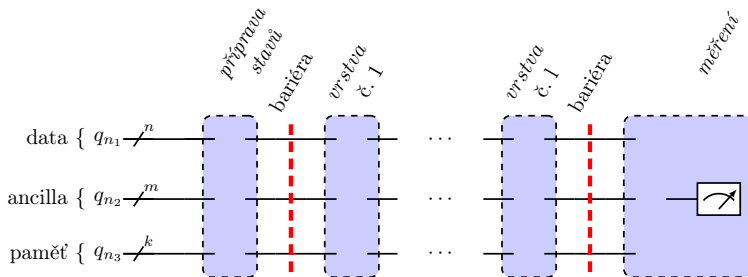
Tři základní vrstvy:

1. kódování dat, která mohou být klasická nebo kvantová, do stavu sady vstupních qubitů,
2. posloupnost kvantových bran aplikovaných na tuto sadu vstupních qubitů,
3. měření jednoho nebo více qubitů na konci pro získání klasicky interpretovatelného výsledku.



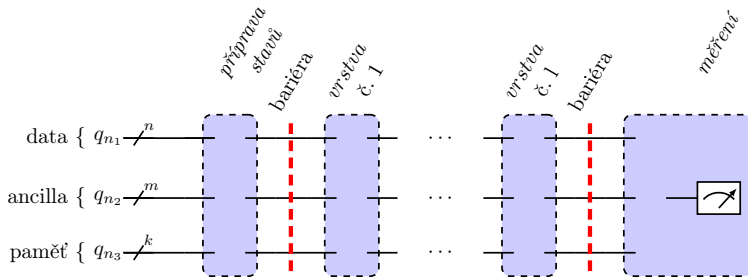
Tři základní vrstvy:

1. kódování dat, která mohou být klasická nebo kvantová, do stavu sady vstupních qubitů,
2. posloupnost kvantových bran aplikovaných na tuto sadu vstupních qubitů,
3. měření jednoho nebo více qubitů na konci pro získání klasicky interpretovatelného výsledku.



Tři základní vrstvy:

1. kódování dat, která mohou být klasická nebo kvantová, do stavu sady vstupních qubitů,
2. posloupnost kvantových bran aplikovaných na tuto sadu vstupních qubitů,
3. měření jednoho nebo více qubitů na konci pro získání klasicky interpretovatelného výsledku.



- 1 jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
- 2 proces měření provádí hardware s digitálním displejem, tzv. n -qubitová měřicí brána,
- 3 n -qubitová měřicí brána je schematicky znázorněna symbolem



- 4 na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
- 5 akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
- 6 měření je **nevratné**,
- 7 měření není v žádném smyslu lineární,
- 8 říkáme, že stav před měřením se v důsledku měření **redukuje/kolabuje** na stav po měření,
- 9 stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

- 1 jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
- 2 proces měření provádí hardware s digitálním displejem, tzv. n -qubitová měřicí brána,
- 3 n -qubitová měřicí brána je schematicky znázorněna symbolem



- 4 na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
- 5 akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
- 6 měření je **nevratné**,
- 7 měření není v žádném smyslu lineární,
- 8 říkáme, že stav před měřením se v důsledku měření **redukuje/kolabuje** na stav po měření,
- 9 stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

- 1 jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
- 2 proces měření provádí hardware s digitálním displejem, tzv. n -qubitová měřicí brána,
- 3 n -qubitová měřicí brána je schematicky znázorněna symbolem



- 4 na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
- 5 akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
- 6 měření je **nevratné**,
- 7 měření není v žádném smyslu lineární,
- 8 říkáme, že stav před měřením se v důsledku měření **redukuje/kolabuje** na stav po měření,
- 9 stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

- 1 jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
- 2 proces měření provádí hardware s digitálním displejem, tzv. n -qubitová měřicí brána,
- 3 n -qubitová měřicí brána je schematicky znázorněna symbolem



- 4 na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
- 5 akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
- 6 měření je **nevratné**,
- 7 měření není v žádném smyslu lineární,
- 8 říkáme, že stav před měřením se v důsledku měření **redukuje/kolabuje** na stav po měření,
- 9 stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

- 1 jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
- 2 proces měření provádí hardware s digitálním displejem, tzv. n -qubitová měřicí brána,
- 3 n -qubitová měřicí brána je schematicky znázorněna symbolem



- 4 na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
- 5 akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
- 6 měření je **nevratné**,
- 7 měření není v žádném smyslu lineární,
- 8 říkáme, že stav před měřením se v důsledku měření **redukuje/kolabuje** na stav po měření,
- 9 stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

- 1 jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
- 2 proces měření provádí hardware s digitálním displejem, tzv. n -qubitová měřicí brána,
- 3 n -qubitová měřicí brána je schematicky znázorněna symbolem



- 4 na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
- 5 akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
- 6 měření je **nevratné**,
- 7 měření není v žádném smyslu lineární,
- 8 říkáme, že stav před měřením se v důsledku měření **redukuje/kolabuje** na stav po měření,
- 9 stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

- 1 jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
- 2 proces měření provádí hardware s digitálním displejem, tzv. n -qubitová měřicí brána,
- 3 n -qubitová měřicí brána je schematicky znázorněna symbolem



- 4 na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
- 5 akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
- 6 měření je **nevratné**,
- 7 měření není v žádném smyslu lineární,
- 8 říkáme, že stav před měřením se v důsledku měření **redukuje/kolabuje** na stav po měření,
- 9 stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

- 1 jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
- 2 proces měření provádí hardware s digitálním displejem, tzv. n -qubitová měřicí brána,
- 3 n -qubitová měřicí brána je schematicky znázorněna symbolem



- 4 na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
- 5 akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
- 6 měření je **nevratné**,
- 7 měření není v žádném smyslu lineární,
- 8 říkáme, že stav před měřením se v důsledku měření **redukuje/kolabuje** na stav po měření,
- 9 stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

- 1 jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
- 2 proces měření provádí hardware s digitálním displejem, tzv. n -qubitová měřicí brána,
- 3 n -qubitová měřicí brána je schematicky znázorněna symbolem



- 4 na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
- 5 akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
- 6 měření je **nevratné**,
- 7 měření není v žádném smyslu lineární,
- 8 říkáme, že stav před měřením se v důsledku měření **redukuje/kolabuje** na stav po měření,
- 9 stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

- 1 jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
- 2 proces měření provádí hardware s digitálním displejem, tzv. n -qubitová měřicí brána,
- 3 n -qubitová měřicí brána je schematicky znázorněna symbolem



- 4 na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
- 5 akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
- 6 měření je **nevratné**,
- 7 měření není v žádném smyslu lineární,
- 8 říkáme, že stav před měřením se v důsledku měření **redukuje/kolabuje** na stav po měření,
- 9 stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

Kvantová superpozice stavů

- základní princip kvantové mechaniky
- každé dva (a více) kvantové stavy lze kombinovat (superponovat)
- vzniká nový kvantový stav

Brána	značení	vstup	výstup
Hadamard		$ 0\rangle$	$\frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$
		$ 1\rangle$	$\frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$

50% pravděpodobnost, že na výstupu bude naměřena hodnota $|0\rangle$

50% pravděpodobnost, že na výstupu bude naměřena hodnota $|1\rangle$

Kvantová superpozice stavů

- základní princip kvantové mechaniky
- každé dva (a více) kvantové stavy lze kombinovat (superponovat)
- vzniká nový kvantový stav

Brána	značení	vstup	výstup
Hadamard	$\boxed{H}$	$ 0\rangle$	$\frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$
		$ 1\rangle$	$\frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$

50% pravděpodobnost, že na výstupu bude naměřena hodnota $|0\rangle$

50% pravděpodobnost, že na výstupu bude naměřena hodnota $|1\rangle$

Kvantová superpozice stavů

- základní princip kvantové mechaniky
- každé dva (a více) kvantové stavy lze kombinovat (superponovat)
- vzniká nový kvantový stav

Brána	značení	vstup	výstup
Hadamard	$\text{---} \boxed{H} \text{---}$	$ 0\rangle$	$\frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$
		$ 1\rangle$	$\frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$

50% pravděpodobnost, že na výstupu bude naměřena hodnota $|0\rangle$

50% pravděpodobnost, že na výstupu bude naměřena hodnota $|1\rangle$

Kvantová superpozice stavů

- základní princip kvantové mechaniky
- každé dva (a více) kvantové stavy lze kombinovat (superponovat)
- vzniká nový kvantový stav

Brána	značení	vstup	výstup
Hadamard	$\boxed{H}$	$ 0\rangle$	$\frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$
		$ 1\rangle$	$\frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$

50% pravděpodobnost, že na výstupu bude naměřena hodnota $|0\rangle$

50% pravděpodobnost, že na výstupu bude naměřena hodnota $|1\rangle$

Kvantová superpozice stavů

- základní princip kvantové mechaniky
- každé dva (a více) kvantové stavy lze kombinovat (superponovat)
- vzniká nový kvantový stav

Brána	značení	vstup	výstup
Hadamard	$\boxed{H}$	$ 0\rangle$	$\frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$
		$ 1\rangle$	$\frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$

50% pravděpodobnost, že na výstupu bude naměřena hodnota $|0\rangle$

50% pravděpodobnost, že na výstupu bude naměřena hodnota $|1\rangle$

Kvantová superpozice stavů

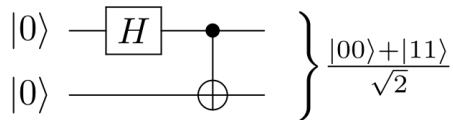
- základní princip kvantové mechaniky
- každé dva (a více) kvantové stavy lze kombinovat (superponovat)
- vzniká nový kvantový stav

Brána	značení	vstup	výstup
Hadamard		$ 0\rangle$	$\frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$
		$ 1\rangle$	$\frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$

50% pravděpodobnost, že na výstupu bude naměřena hodnota $|0\rangle$

50% pravděpodobnost, že na výstupu bude naměřena hodnota $|1\rangle$

Jednoduchý kvantový obvod, který vytváří *provázanost* dvou qubitů



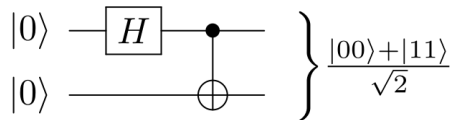
výstup tohoto obvodu nelze rozdělit na jednotlivé základní stavy $|0\rangle$ a $|1\rangle$

Stavový prostor jednoho qubitů $H_1 = \text{span}\{|0\rangle, |1\rangle\}$.

Stavový prostor dvou qubitů H_2 :

kanonická báze	Bellova báze
$ 00\rangle$	$ \Phi^+\rangle = \frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$
$ 01\rangle$	$ \Phi^-\rangle = \frac{1}{\sqrt{2}}(00\rangle - 11\rangle)$
$ 10\rangle$	$ \Psi^+\rangle = \frac{1}{\sqrt{2}}(01\rangle + 10\rangle)$
$ 11\rangle$	$ \Psi^-\rangle = \frac{1}{\sqrt{2}}(01\rangle - 10\rangle)$

Jednoduchý kvantový obvod, který vytváří *provázanost* dvou qubitů



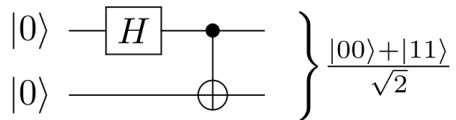
výstup tohoto obvodu nelze rozdělit na jednotlivé základní stavy $|0\rangle$ a $|1\rangle$

Stavový prostor jednoho qubitů $H_1 = \text{span}\{|0\rangle, |1\rangle\}$.

Stavový prostor dvou qubitů H_2 :

kanonická báze	Bellova báze
$ 00\rangle$	$ \Phi^+\rangle = \frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$
$ 01\rangle$	$ \Phi^-\rangle = \frac{1}{\sqrt{2}}(00\rangle - 11\rangle)$
$ 10\rangle$	$ \Psi^+\rangle = \frac{1}{\sqrt{2}}(01\rangle + 10\rangle)$
$ 11\rangle$	$ \Psi^-\rangle = \frac{1}{\sqrt{2}}(01\rangle - 10\rangle)$

Jednoduchý kvantový obvod, který vytváří *provázanost* dvou qubitů



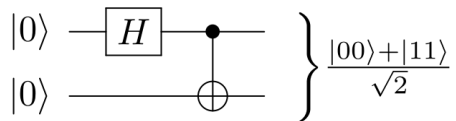
výstup tohoto obvodu nelze rozdělit na jednotlivé základní stavy $|0\rangle$ a $|1\rangle$

Stavový prostor jednoho qubitů $H_1 = \text{span}\{|0\rangle, |1\rangle\}$.

Stavový prostor dvou qubitů H_2 :

kanonická báze	Bellova báze
$ 00\rangle$	$ \Phi^+\rangle = \frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$
$ 01\rangle$	$ \Phi^-\rangle = \frac{1}{\sqrt{2}}(00\rangle - 11\rangle)$
$ 10\rangle$	$ \Psi^+\rangle = \frac{1}{\sqrt{2}}(01\rangle + 10\rangle)$
$ 11\rangle$	$ \Psi^-\rangle = \frac{1}{\sqrt{2}}(01\rangle - 10\rangle)$

Jednoduchý kvantový obvod, který vytváří *provázanost* dvou qubitů



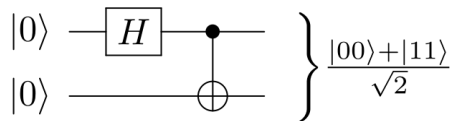
výstup tohoto obvodu nelze rozdělit na jednotlivé základní stavy $|0\rangle$ a $|1\rangle$

Stavový prostor jednoho qubitů $H_1 = \text{span}\{|0\rangle, |1\rangle\}$.

Stavový prostor dvou qubitů H_2 :

kanonická báze	Bellova báze
$ 00\rangle$	$ \Phi^+\rangle = \frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$
$ 01\rangle$	$ \Phi^-\rangle = \frac{1}{\sqrt{2}}(00\rangle - 11\rangle)$
$ 10\rangle$	$ \Psi^+\rangle = \frac{1}{\sqrt{2}}(01\rangle + 10\rangle)$
$ 11\rangle$	$ \Psi^-\rangle = \frac{1}{\sqrt{2}}(01\rangle - 10\rangle)$

Jednoduchý kvantový obvod, který vytváří *provázanost* dvou qubitů



výstup tohoto obvodu nelze rozdělit na jednotlivé základní stavy $|0\rangle$ a $|1\rangle$

Stavový prostor jednoho qubitů $H_1 = \text{span}\{|0\rangle, |1\rangle\}$.

Stavový prostor dvou qubitů H_2 :

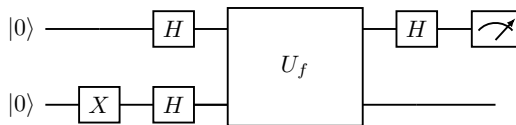
kanonická báze	Bellova báze
$ 00\rangle$	$ \Phi^+\rangle = \frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$
$ 01\rangle$	$ \Phi^-\rangle = \frac{1}{\sqrt{2}}(00\rangle - 11\rangle)$
$ 10\rangle$	$ \Psi^+\rangle = \frac{1}{\sqrt{2}}(01\rangle + 10\rangle)$
$ 11\rangle$	$ \Psi^-\rangle = \frac{1}{\sqrt{2}}(01\rangle - 10\rangle)$

Předpoklad: $f : \{0, 1\} \longrightarrow \{0, 1\}$

$$\begin{array}{llll} f_1 : 0 \mapsto 0 & f_2 : 0 \mapsto 1 & f_3 : 0 \mapsto 0 & f_4 : 0 \mapsto 1 \\ & 1 \mapsto 0 & 1 \mapsto 1 & 1 \mapsto 0 \end{array}$$

f_1 a f_2 jsou konstantní f_3 a f_4 jsou vyvážené

Úkol: zjistit zda je f konstantní nebo vyvážená.



$$U_f : |xy\rangle \mapsto |x, y \oplus f(x)\rangle$$

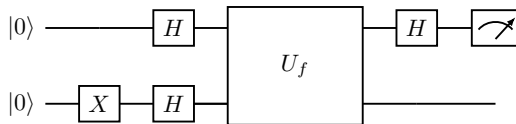
$$(H \otimes I) U_f (H \otimes H) (I \otimes X) |0\rangle \otimes |0\rangle$$

Předpoklad: $f : \{0, 1\} \longrightarrow \{0, 1\}$

$$\begin{array}{llll} f_1 : 0 \mapsto 0 & f_2 : 0 \mapsto 1 & f_3 : 0 \mapsto 0 & f_4 : 0 \mapsto 1 \\ 1 \mapsto 0 & 1 \mapsto 1 & 1 \mapsto 1 & 1 \mapsto 0 \end{array}$$

f_1 a f_2 jsou konstantní f_3 a f_4 jsou vyvážené

Úkol: zjistit zda je f konstantní nebo vyvážená.



$$U_f : |xy\rangle \mapsto |x, y \oplus f(x)\rangle$$

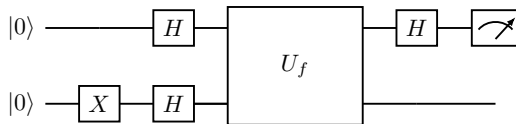
$$(H \otimes I) U_f (H \otimes H) (I \otimes X) |0\rangle \otimes |0\rangle$$

Předpoklad: $f : \{0, 1\} \longrightarrow \{0, 1\}$

$$\begin{array}{llll} f_1 : 0 \mapsto 0 & f_2 : 0 \mapsto 1 & f_3 : 0 \mapsto 0 & f_4 : 0 \mapsto 1 \\ & 1 \mapsto 0 & 1 \mapsto 1 & 1 \mapsto 0 \end{array}$$

f_1 a f_2 jsou konstantní f_3 a f_4 jsou vyvážené

Úkol: zjistit zda je f konstantní nebo vyvážená.



$$U_f : |xy\rangle \mapsto |x, y \oplus f(x)\rangle$$

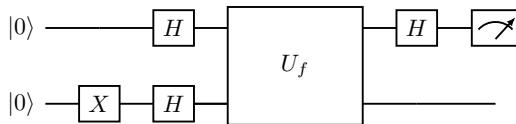
$$(H \otimes I) U_f (H \otimes H) (I \otimes X) |0\rangle \otimes |0\rangle$$

Předpoklad: $f : \{0, 1\} \longrightarrow \{0, 1\}$

$$\begin{array}{llll} f_1 : 0 \mapsto 0 & f_2 : 0 \mapsto 1 & f_3 : 0 \mapsto 0 & f_4 : 0 \mapsto 1 \\ & 1 \mapsto 0 & 1 \mapsto 1 & 1 \mapsto 0 \end{array}$$

f_1 a f_2 jsou konstantní f_3 a f_4 jsou vyvážené

Úkol: zjistit zda je f konstantní nebo vyvážená.



$$U_f : |xy\rangle \mapsto |x, y \oplus f(x)\rangle$$

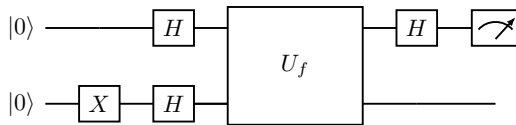
$$(H \otimes I) U_f (H \otimes H) (I \otimes X) |0\rangle \otimes |0\rangle$$

Předpoklad: $f : \{0, 1\} \longrightarrow \{0, 1\}$

$$\begin{array}{cccc} f_1 : 0 \mapsto 0 & f_2 : 0 \mapsto 1 & f_3 : 0 \mapsto 0 & f_4 : 0 \mapsto 1 \\ 1 \mapsto 0 & 1 \mapsto 1 & 1 \mapsto 1 & 1 \mapsto 0 \end{array}$$

f_1 a f_2 jsou konstantní f_3 a f_4 jsou vyvážené

Úkol: zjistit zda je f konstantní nebo vyvážená.



$$U_f : |xy\rangle \mapsto |x, y \oplus f(x)\rangle$$

$$(H \otimes I) U_f (H \otimes H) (I \otimes X) |0\rangle \otimes |0\rangle$$

$$\begin{aligned}
& (H \otimes I) U_f (H \otimes H) (I \otimes X) |0\rangle \otimes |0\rangle = \\
& (H \otimes I) U_f (H \otimes H) |0\rangle \otimes |1\rangle = \\
& (H \otimes I) U_f \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \\
& (H \otimes I) U_f \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \\
& (H \otimes I) \frac{1}{2} (|0, f(0)\rangle - |0, \neg f(0)\rangle + |1, f(1)\rangle - |1, \neg f(1)\rangle) = \\
& \frac{1}{2\sqrt{2}} \left((|0\rangle + |1\rangle)(|f(0)\rangle - |\neg f(0)\rangle) + (|0\rangle - |1\rangle)(|f(1)\rangle - |\neg f(1)\rangle) \right)
\end{aligned}$$

pokud je f konstantní $\Rightarrow |f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |0\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

pokud je f vyvážená $\Rightarrow |\neg f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |1\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

$$\begin{aligned}
& (H \otimes I) U_f (H \otimes H) (I \otimes X) |0\rangle \otimes |0\rangle = \\
& (H \otimes I) U_f (H \otimes H) |0\rangle \otimes |1\rangle = \\
& (H \otimes I) U_f \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \\
& (H \otimes I) U_f \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \\
& (H \otimes I) \frac{1}{2} (|0, f(0)\rangle - |0, \neg f(0)\rangle + |1, f(1)\rangle - |1, \neg f(1)\rangle) = \\
& \frac{1}{2\sqrt{2}} \left((|0\rangle + |1\rangle)(|f(0)\rangle - |\neg f(0)\rangle) + (|0\rangle - |1\rangle)(|f(1)\rangle - |\neg f(1)\rangle) \right)
\end{aligned}$$

pokud je f konstantní $\Rightarrow |f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |0\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

pokud je f vyvážená $\Rightarrow |\neg f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |1\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

$$\begin{aligned}
& (H \otimes I) U_f (H \otimes H) (I \otimes X) |0\rangle \otimes |0\rangle = \\
& (H \otimes I) U_f (H \otimes H) |0\rangle \otimes |1\rangle = \\
& (H \otimes I) U_f \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \\
& (H \otimes I) U_f \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \\
& (H \otimes I) \frac{1}{2} (|0, f(0)\rangle - |0, \neg f(0)\rangle + |1, f(1)\rangle - |1, \neg f(1)\rangle) = \\
& \frac{1}{2\sqrt{2}} \left((|0\rangle + |1\rangle)(|f(0)\rangle - |\neg f(0)\rangle) + (|0\rangle - |1\rangle)(|f(1)\rangle - |\neg f(1)\rangle) \right)
\end{aligned}$$

pokud je f konstantní $\Rightarrow |f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |0\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

pokud je f vyvážená $\Rightarrow |\neg f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |1\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

$$\begin{aligned}
& (H \otimes I) U_f (H \otimes H) (I \otimes X) |0\rangle \otimes |0\rangle = \\
& (H \otimes I) U_f (H \otimes H) |0\rangle \otimes |1\rangle = \\
& (H \otimes I) U_f \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \\
& (H \otimes I) U_f \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \\
& (H \otimes I) \frac{1}{2} (|0, f(0)\rangle - |0, \neg f(0)\rangle + |1, f(1)\rangle - |1, \neg f(1)\rangle) = \\
& \frac{1}{2\sqrt{2}} \left((|0\rangle + |1\rangle)(|f(0)\rangle - |\neg f(0)\rangle) + (|0\rangle - |1\rangle)(|f(1)\rangle - |\neg f(1)\rangle) \right)
\end{aligned}$$

pokud je f konstantní $\Rightarrow |f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |0\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

pokud je f vyvážená $\Rightarrow |\neg f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |1\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

$$\begin{aligned}
& (H \otimes I) U_f (H \otimes H) (I \otimes X) |0\rangle \otimes |0\rangle = \\
& (H \otimes I) U_f (H \otimes H) |0\rangle \otimes |1\rangle = \\
& (H \otimes I) U_f \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \\
& (H \otimes I) U_f \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \\
& (H \otimes I) \frac{1}{2} (|0, f(0)\rangle - |0, \neg f(0)\rangle + |1, f(1)\rangle - |1, \neg f(1)\rangle) = \\
& \frac{1}{2\sqrt{2}} \left((|0\rangle + |1\rangle)(|f(0)\rangle - |\neg f(0)\rangle) + (|0\rangle - |1\rangle)(|f(1)\rangle - |\neg f(1)\rangle) \right)
\end{aligned}$$

pokud je f konstantní $\Rightarrow |f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |0\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

pokud je f vyvážená $\Rightarrow |\neg f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |1\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

$$\begin{aligned}
& (H \otimes I) U_f (H \otimes H) (I \otimes X) |0\rangle \otimes |0\rangle = \\
& (H \otimes I) U_f (H \otimes H) |0\rangle \otimes |1\rangle = \\
& (H \otimes I) U_f \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \\
& (H \otimes I) U_f \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \\
& (H \otimes I) \frac{1}{2} (|0, f(0)\rangle - |0, \neg f(0)\rangle + |1, f(1)\rangle - |1, \neg f(1)\rangle) = \\
& \frac{1}{2\sqrt{2}} \left((|0\rangle + |1\rangle)(|f(0)\rangle - |\neg f(0)\rangle) + (|0\rangle - |1\rangle)(|f(1)\rangle - |\neg f(1)\rangle) \right)
\end{aligned}$$

pokud je f konstantní $\Rightarrow |f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |0\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

pokud je f vyvážená $\Rightarrow |\neg f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |1\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

$$\begin{aligned}
& (H \otimes I) U_f (H \otimes H) (I \otimes X) |0\rangle \otimes |0\rangle = \\
& (H \otimes I) U_f (H \otimes H) |0\rangle \otimes |1\rangle = \\
& (H \otimes I) U_f \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \\
& (H \otimes I) U_f \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \\
& (H \otimes I) \frac{1}{2} (|0, f(0)\rangle - |0, \neg f(0)\rangle + |1, f(1)\rangle - |1, \neg f(1)\rangle) = \\
& \frac{1}{2\sqrt{2}} \left((|0\rangle + |1\rangle)(|f(0)\rangle - |\neg f(0)\rangle) + (|0\rangle - |1\rangle)(|f(1)\rangle - |\neg f(1)\rangle) \right)
\end{aligned}$$

pokud je f konstantní $\Rightarrow |f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |0\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

pokud je f vyvážená $\Rightarrow |\neg f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |1\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

$$\begin{aligned}
& (H \otimes I) U_f (H \otimes H) (I \otimes X) |0\rangle \otimes |0\rangle = \\
& (H \otimes I) U_f (H \otimes H) |0\rangle \otimes |1\rangle = \\
& (H \otimes I) U_f \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \\
& (H \otimes I) U_f \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \\
& (H \otimes I) \frac{1}{2} (|0, f(0)\rangle - |0, \neg f(0)\rangle + |1, f(1)\rangle - |1, \neg f(1)\rangle) = \\
& \frac{1}{2\sqrt{2}} \left((|0\rangle + |1\rangle)(|f(0)\rangle - |\neg f(0)\rangle) + (|0\rangle - |1\rangle)(|f(1)\rangle - |\neg f(1)\rangle) \right)
\end{aligned}$$

pokud je f konstantní $\Rightarrow |f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |0\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

pokud je f vyvážená $\Rightarrow |\neg f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |1\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

$$\begin{aligned}
& (H \otimes I) U_f (H \otimes H) (I \otimes X) |0\rangle \otimes |0\rangle = \\
& (H \otimes I) U_f (H \otimes H) |0\rangle \otimes |1\rangle = \\
& (H \otimes I) U_f \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \\
& (H \otimes I) U_f \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \\
& (H \otimes I) \frac{1}{2} (|0, f(0)\rangle - |0, \neg f(0)\rangle + |1, f(1)\rangle - |1, \neg f(1)\rangle) = \\
& \frac{1}{2\sqrt{2}} \left((|0\rangle + |1\rangle)(|f(0)\rangle - |\neg f(0)\rangle) + (|0\rangle - |1\rangle)(|f(1)\rangle - |\neg f(1)\rangle) \right)
\end{aligned}$$

pokud je f konstantní $\Rightarrow |f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |0\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

pokud je f vyvážená $\Rightarrow |\neg f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |1\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

$$\begin{aligned}
& (H \otimes I) U_f (H \otimes H) (I \otimes X) |0\rangle \otimes |0\rangle = \\
& (H \otimes I) U_f (H \otimes H) |0\rangle \otimes |1\rangle = \\
& (H \otimes I) U_f \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \\
& (H \otimes I) U_f \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \\
& (H \otimes I) \frac{1}{2} (|0, f(0)\rangle - |0, \neg f(0)\rangle + |1, f(1)\rangle - |1, \neg f(1)\rangle) = \\
& \frac{1}{2\sqrt{2}} \left((|0\rangle + |1\rangle)(|f(0)\rangle - |\neg f(0)\rangle) + (|0\rangle - |1\rangle)(|f(1)\rangle - |\neg f(1)\rangle) \right)
\end{aligned}$$

pokud je f konstantní $\Rightarrow |f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |0\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

pokud je f vyvážená $\Rightarrow |\neg f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |1\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

$$\begin{aligned}
& (H \otimes I) U_f (H \otimes H) (I \otimes X) |0\rangle \otimes |0\rangle = \\
& (H \otimes I) U_f (H \otimes H) |0\rangle \otimes |1\rangle = \\
& (H \otimes I) U_f \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \\
& (H \otimes I) U_f \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \\
& (H \otimes I) \frac{1}{2} (|0, f(0)\rangle - |0, \neg f(0)\rangle + |1, f(1)\rangle - |1, \neg f(1)\rangle) = \\
& \frac{1}{2\sqrt{2}} \left((|0\rangle + |1\rangle)(|f(0)\rangle - |\neg f(0)\rangle) + (|0\rangle - |1\rangle)(|f(1)\rangle - |\neg f(1)\rangle) \right)
\end{aligned}$$

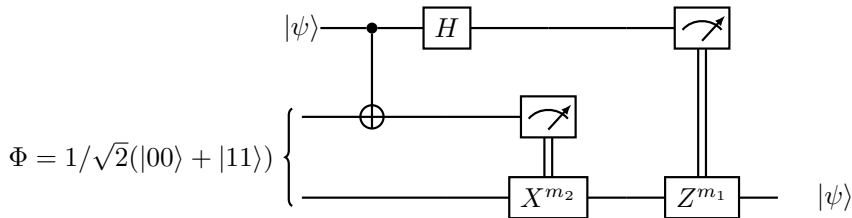
pokud je f konstantní $\Rightarrow |f(0)\rangle = |f(1)\rangle \Rightarrow$

$$\frac{1}{\sqrt{2}} |0\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

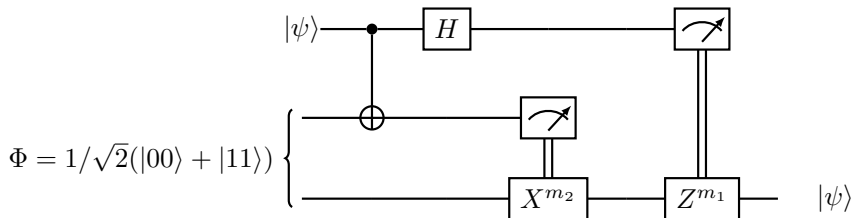
pokud je f vyvážená $\Rightarrow |\neg f(0)\rangle = |f(1)\rangle \Rightarrow$

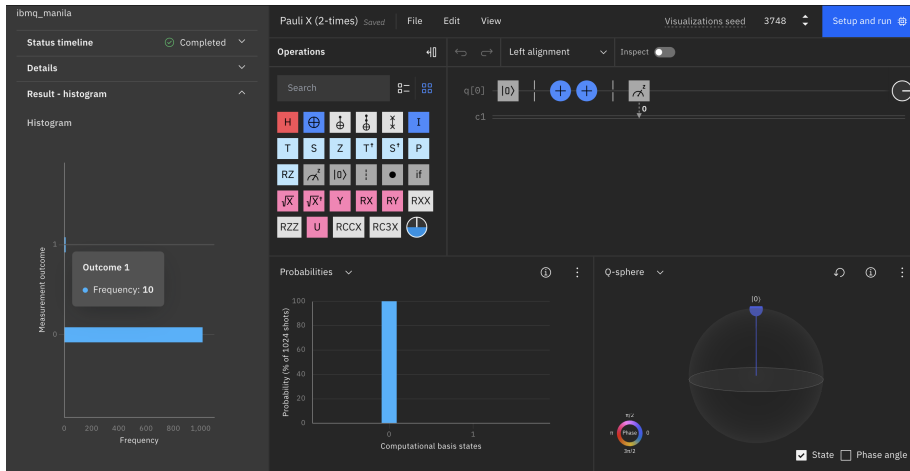
$$\frac{1}{\sqrt{2}} |1\rangle (|f(0)\rangle - |\neg f(0)\rangle)$$

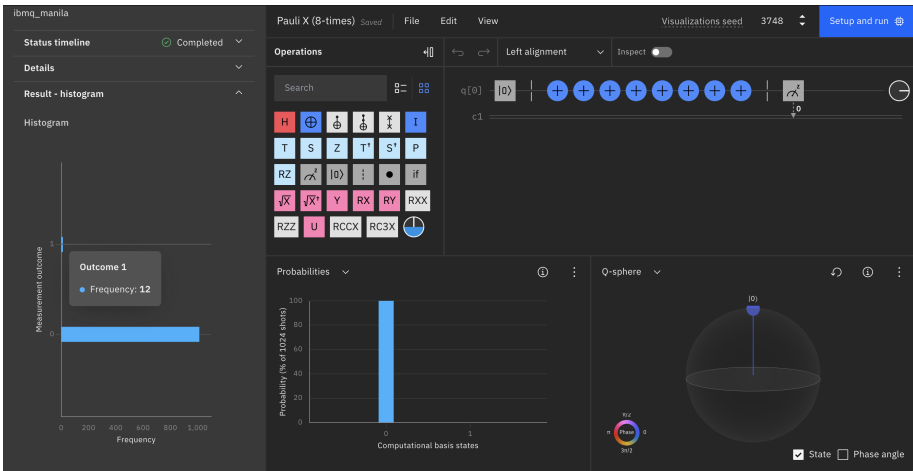
Kvantový obvod reprezentující teleportaci kvantového stavu

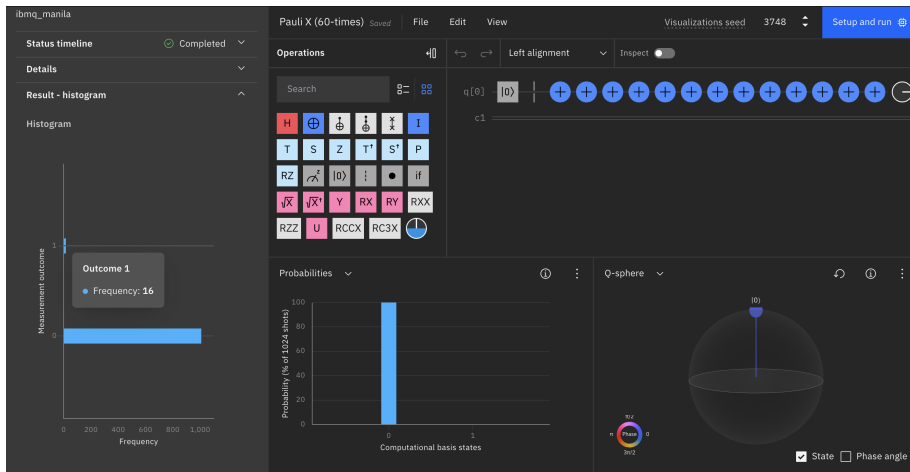


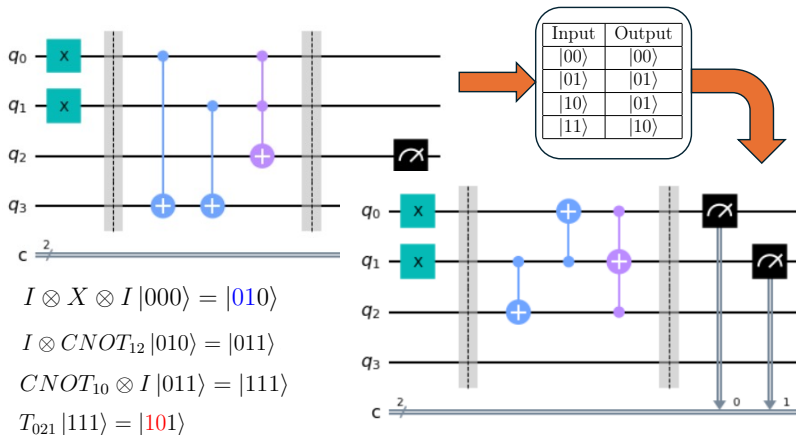
Kvantový obvod reprezentující teleportaci kvantového stavu



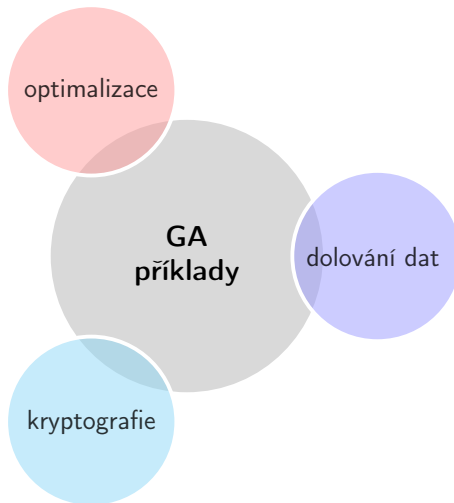








Groverův algoritmus příklady použití



Předpoklad: $f : \{0, 1, \dots, N - 1\} \longrightarrow \{0, 1\}$

Úkol:

- V analogii „nestrukturované databáze“ představuje definiční obor f indexy pro databázi a $f(x) = 1$ právě tehdy, když data, na která x ukazuje, splňují kritérium vyhledávání.
- Dále předpokládáme, že pouze jeden index splňuje $f(x) = 1$ a tento index značíme ω .
- Cílem je identifikovat ω .

Předpoklad: $f : \{0, 1, \dots, N - 1\} \longrightarrow \{0, 1\}$

Úkol:

- V analogii „nestrukturované databáze“ představuje definiční obor f indexy pro databázi a $f(x) = 1$ právě tehdy, když data, na která x ukazuje, splňují kritérium vyhledávání.
- Dále předpokládáme, že pouze jeden index splňuje $f(x) = 1$ a tento index značíme ω .
- Cílem je identifikovat ω .

Předpoklad: $f : \{0, 1, \dots, N - 1\} \longrightarrow \{0, 1\}$

Úkol:

- V analogii „nestrukturované databáze“ představuje definiční obor f indexy pro databázi a $f(x) = 1$ právě tehdy, když data, na která x ukazuje, splňují kritérium vyhledávání.
- Dále předpokládáme, že pouze jeden index splňuje $f(x) = 1$ a tento index značíme ω .
- Cílem je identifikovat ω .

Předpoklad: $f : \{0, 1, \dots, N - 1\} \longrightarrow \{0, 1\}$

Úkol:

- V analogii „nestrukturované databáze“ představuje definiční obor f indexy pro databázi a $f(x) = 1$ právě tehdy, když data, na která x ukazuje, splňují kritérium vyhledávání.
- Dále předpokládáme, že pouze jeden index splňuje $f(x) = 1$ a tento index značíme ω .
- Cílem je identifikovat ω .

Předpoklad: $f : \{0, 1, \dots, N - 1\} \longrightarrow \{0, 1\}$

Úkol:

- V analogii „nestrukturované databáze“ představuje definiční obor f indexy pro databázi a $f(x) = 1$ právě tehdy, když data, na která x ukazuje, splňují kritérium vyhledávání.
- Dále předpokládáme, že pouze jeden index splňuje $f(x) = 1$ a tento index značíme ω .
- Cílem je identifikovat ω .

- K f můžeme přistupovat pomocí podprogramu (někdy nazývaného *orákulum*) ve formě unitárního operátoru U_ω , který funguje následovně:

$$\begin{cases} U_\omega|x\rangle = -|x\rangle & \text{pro } x = \omega, \text{ což odpovídá situaci, } f(x) = 1, \\ U_\omega|x\rangle = |x\rangle & \text{pro } x \neq \omega, \text{ což odpovídá situaci, } f(x) = 0. \end{cases}$$

- Operátor se píše jednoduchou formou

$$U_\omega|x\rangle = (-1)^{f(x)}|x\rangle.$$

- Zde je N -dimenzionální stavový prostor $\mathcal{H}$, který odpovídá registru s $n = \lceil \log_2 N \rceil$ qubitů.
- Výstupem Groverova algoritmu je ω s pravděpodobností alespoň $1/2$ s pomocí $O(\sqrt{N})$ aplikací U_ω .
- Tato pravděpodobnost může růst s iteračním opakováním Groverova algoritmu.
- Groverův algoritmus naide ω pomocí $O(\sqrt{N})$ operací, klasicky je zapotřebí operací $O(N)$

- K f můžeme přistupovat pomocí podprogramu (někdy nazývaného *orákulum*) ve formě unitárního operátoru U_ω , který funguje následovně:

$$\begin{cases} U_\omega|x\rangle = -|x\rangle & \text{pro } x = \omega, \text{ což odpovídá situaci, } f(x) = 1, \\ U_\omega|x\rangle = |x\rangle & \text{pro } x \neq \omega, \text{ což odpovídá situaci, } f(x) = 0. \end{cases}$$

- Operátor se píše jednoduchou formou

$$U_\omega|x\rangle = (-1)^{f(x)}|x\rangle.$$

- Zde je N -dimenzionální stavový prostor $\mathcal{H}$, který odpovídá registru s $n = \lceil \log_2 N \rceil$ qubitů.
- Výstupem Groverova algoritmu je ω s pravděpodobností alespoň $1/2$ s pomocí $O(\sqrt{N})$ aplikací U_ω .
- Tato pravděpodobnost může růst s iteračním opakováním Groverova algoritmu.
- Groverův algoritmus naide ω pomocí $O(\sqrt{N})$ operací, klasicky je zapotřebí operací $O(N)$

- K f můžeme přistupovat pomocí podprogramu (někdy nazývaného *orákulum*) ve formě unitárního operátoru U_ω , který funguje následovně:

$$\begin{cases} U_\omega|x\rangle = -|x\rangle & \text{pro } x = \omega, \text{ což odpovídá situaci, } f(x) = 1, \\ U_\omega|x\rangle = |x\rangle & \text{pro } x \neq \omega, \text{ což odpovídá situaci, } f(x) = 0. \end{cases}$$

- Operátor se píše jednoduchou formou

$$U_\omega|x\rangle = (-1)^{f(x)}|x\rangle.$$

- Zde je N -dimenzionální stavový prostor $\mathcal{H}$, který odpovídá registru s $n = \lceil \log_2 N \rceil$ qubitů.
- Výstupem Groverova algoritmu je ω s pravděpodobností alespoň $1/2$ s pomocí $O(\sqrt{N})$ aplikací U_ω .
- Tato pravděpodobnost může růst s iteračním opakováním Groverova algoritmu.
- Groverův algoritmus naide ω pomocí $O(\sqrt{N})$ operací, klasicky je zapotřebí operací $O(N)$.

- K f můžeme přistupovat pomocí podprogramu (někdy nazývaného *orákulum*) ve formě unitárního operátoru U_ω , který funguje následovně:

$$\begin{cases} U_\omega|x\rangle = -|x\rangle & \text{pro } x = \omega, \text{ což odpovídá situaci, } f(x) = 1, \\ U_\omega|x\rangle = |x\rangle & \text{pro } x \neq \omega, \text{ což odpovídá situaci, } f(x) = 0. \end{cases}$$

- Operátor se píše jednoduchou formou

$$U_\omega|x\rangle = (-1)^{f(x)}|x\rangle.$$

- Zde je N -dimenzionální stavový prostor $\mathcal{H}$, který odpovídá registru s $n = \lceil \log_2 N \rceil$ qubitů.
- Výstupem Groverova algoritmu je ω s pravděpodobností alespoň $1/2$ s pomocí $O(\sqrt{N})$ aplikací U_ω .
- Tato pravděpodobnost může růst s iteračním opakováním Groverova algoritmu.
- Groverův algoritmus naide ω pomocí $O(\sqrt{N})$ operací, klasicky je zapotřebí operací $O(N)$.

- K f můžeme přistupovat pomocí podprogramu (někdy nazývaného *orákulum*) ve formě unitárního operátoru U_ω , který funguje následovně:

$$\begin{cases} U_\omega|x\rangle = -|x\rangle & \text{pro } x = \omega, \text{ což odpovídá situaci, } f(x) = 1, \\ U_\omega|x\rangle = |x\rangle & \text{pro } x \neq \omega, \text{ což odpovídá situaci, } f(x) = 0. \end{cases}$$

- Operátor se píše jednoduchou formou

$$U_\omega|x\rangle = (-1)^{f(x)}|x\rangle.$$

- Zde je N -dimenzionální stavový prostor $\mathcal{H}$, který odpovídá registru s $n = \lceil \log_2 N \rceil$ qubitů.
- Výstupem Groverova algoritmu je ω s pravděpodobností alespoň $1/2$ s pomocí $O(\sqrt{N})$ aplikací U_ω .
- Tato pravděpodobnost může růst s iteračním opakováním Groverova algoritmu.

■ Groverův algoritmus naide ω pomocí $O(\sqrt{N})$ operací, klasicky je zapotřebí operací $O(N)$

- K f můžeme přistupovat pomocí podprogramu (někdy nazývaného *orákulum*) ve formě unitárního operátoru U_ω , který funguje následovně:

$$\begin{cases} U_\omega|x\rangle = -|x\rangle & \text{pro } x = \omega, \text{ což odpovídá situaci, } f(x) = 1, \\ U_\omega|x\rangle = |x\rangle & \text{pro } x \neq \omega, \text{ což odpovídá situaci, } f(x) = 0. \end{cases}$$

- Operátor se píše jednoduchou formou

$$U_\omega|x\rangle = (-1)^{f(x)}|x\rangle.$$

- Zde je N -dimenzionální stavový prostor $\mathcal{H}$, který odpovídá registru s $n = \lceil \log_2 N \rceil$ qubitů.
- Výstupem Groverova algoritmu je ω s pravděpodobností alespoň $1/2$ s pomocí $O(\sqrt{N})$ aplikací U_ω .
- Tato pravděpodobnost může růst s iteračním opakováním Groverova algoritmu.
- Groverův algoritmus najde ω pomocí $O(\sqrt{N})$ operací, klasicky je zapotřebí operací $O(N)$

- 1 Inicializace systému: uniformní superpozice všech vstupních stavů

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

- 2 Exekuce *Groverovy iterace* $r(N)$ krát:

- 1 Aplikace operátoru U_ω
 - 2 Aplikace Groverova difuzního operátoru $U_s = 2|s\rangle\langle s| - I$
- 3 Provést měření výsledného stavu ve výpočetní bázi

- 1 Inicializace systému: uniformní superpozice všech vstupních stavů

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

- 2 Exekuce *Groverovy iterace* $r(N)$ krát:

- 1 Aplikace operátoru U_ω

- 2 Aplikace Groverova difuzního operátoru $U_s = 2|s\rangle\langle s| - I$

- 3 Provést měření výsledného stavu ve výpočetní bázi

- 1 Inicializace systému: uniformní superpozice všech vstupních stavů

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

- 2 Exekuce *Groverovy iterace* $r(N)$ krát:

- 1 Aplikace operátoru U_ω
- 2 Aplikace Groverova difuzního operátoru $U_s = 2|s\rangle\langle s| - I$
- 3 Provést měření výsledného stavu ve výpočetní bázi

- 1 Inicializace systému: uniformní superpozice všech vstupních stavů

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

- 2 Exekuce *Groverovy iterace* $r(N)$ krát:

- 1 Aplikace operátoru U_ω
- 2 Aplikace Groverova difuzního operátoru $U_s = 2|s\rangle\langle s| - I$
- 3 Provést měření výsledného stavu ve výpočetní bázi

- 1 Inicializace systému: uniformní superpozice všech vstupních stavů

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

- 2 Exekuce *Groverovy iterace* $r(N)$ krát:

- 1 Aplikace operátoru U_ω

- 2 Aplikace Groverova difuzního operátoru $U_s = 2|s\rangle\langle s| - I$

- 3 Provést měření výsledného stavu ve výpočetní bázi

- 1 Inicializace systému: uniformní superpozice všech vstupních stavů

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

- 2 Exekuce *Groverovy iterace* $r(N)$ krát:

- 1 Aplikace operátoru U_ω

- 2 Aplikace Groverova difuzního operátoru $U_s = 2|s\rangle\langle s| - I$

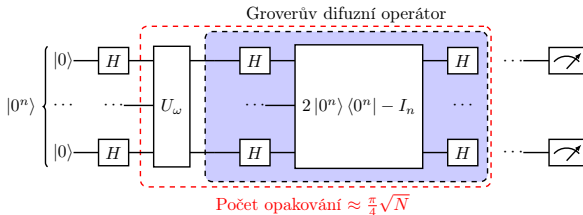
- 3 Provést měření výsledného stavu ve výpočetní bázi

- 1 Inicializace systému: uniformní superpozice všech vstupních stavů

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

- 2 Exekuce *Groverovy iterace* $r(N)$ krát:

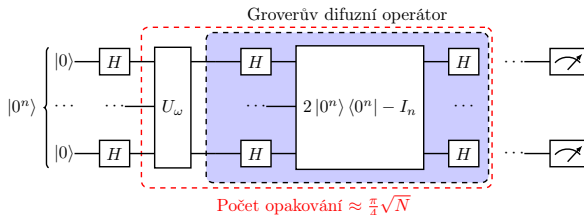
- 1 Aplikace operátoru U_ω
 - 2 Aplikace Groverova difuzního operátoru $U_s = 2|s\rangle\langle s| - I$
- 3 Provést měření výsledného stavu ve výpočetní bázi



- Pro správně zvolené r bude výstup $|\omega\rangle$ s pravděpodobností blízké 1, pro $N \gg 1$.
- Hodnotu $r(N)$ lze odhadnout

$$r(N) \leq \left\lceil \frac{\pi}{4} \sqrt{N} \right\rceil.$$

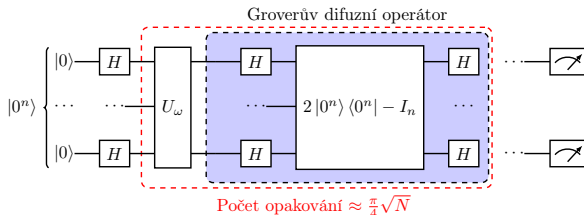
- Implementaci kroků tohoto algoritmu lze provést pomocí řady bran jejichž počet je lineárních k počtu qubitů.
- Složitost algoritmu je tedy $O(\log(N)r(N))$ vzhledem k počtu bran, nebo $O(\log(N))$ na iteraci



- Pro správně zvolené r bude výstup $|\omega\rangle$ s pravděpodobností blízké 1, pro $N \gg 1$.
- Hodnotu $r(N)$ lze odhadnout

$$r(N) \leq \left\lceil \frac{\pi}{4} \sqrt{N} \right\rceil.$$

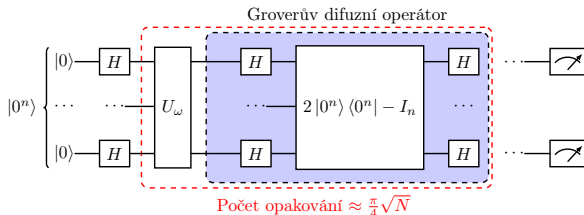
- Implementaci kroků tohoto algoritmu lze provést pomocí řady bran jejichž počet je lineárních k počtu qubitů.
- Složitost algoritmu je tedy $O(\log(N)r(N))$ vzhledem k počtu bran, nebo $O(\log(N))$ na iteraci



- Pro správně zvolené r bude výstup $|\omega\rangle$ s pravděpodobností blízké 1, pro $N \gg 1$.
- Hodnotu $r(N)$ lze odhadnout

$$r(N) \leq \left\lceil \frac{\pi}{4} \sqrt{N} \right\rceil.$$

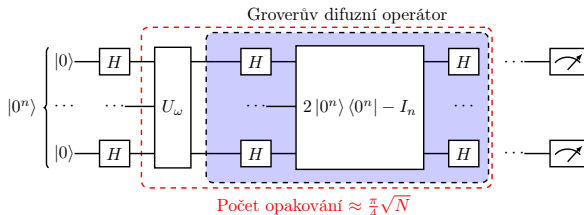
- Implementaci kroků tohoto algoritmu lze provést pomocí řady bran jejichž počet je lineárních k počtu qubitů.
- Složitost algoritmu je tedy $O(\log(N)r(N))$ vzhledem k počtu bran, nebo $O(\log(N))$ na iteraci.



- Pro správně zvolené r bude výstup $|\omega\rangle$ s pravděpodobností blízké 1, pro $N \gg 1$.
- Hodnotu $r(N)$ lze odhadnout

$$r(N) \leq \left\lceil \frac{\pi}{4} \sqrt{N} \right\rceil.$$

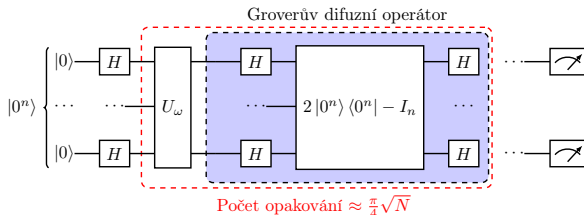
- Implementaci kroků tohoto algoritmu lze provést pomocí řady bran jejichž počet je lineárních k počtu qubitů.
- Složitost algoritmu je tedy $O(\log(N)r(N))$ vzhledem k počtu bran, nebo $O(\log(N))$ na iteraci



- Pro správně zvolené r bude výstup $|\omega\rangle$ s pravděpodobností blízké 1, pro $N \gg 1$.
- Hodnotu $r(N)$ lze odhadnout

$$r(N) \leq \left\lceil \frac{\pi}{4} \sqrt{N} \right\rceil.$$

- Implementaci kroků tohoto algoritmu lze provést pomocí řady bran jejichž počet je lineárních k počtu qubitů.
- Složitost algoritmu je tedy $O(\log(N)r(N))$ vzhledem k počtu bran, nebo $O(\log(N))$ na iteraci



- Pro správně zvolené r bude výstup $|\omega\rangle$ s pravděpodobností blízké 1, pro $N \gg 1$.
- Hodnotu $r(N)$ lze odhadnout

$$r(N) \leq \left\lceil \frac{\pi}{4} \sqrt{N} \right\rceil.$$

- Implementaci kroků tohoto algoritmu lze provést pomocí řady bran jejichž počet je lineárních k počtu qubitů.
- Složitost algoritmu je tedy $O(\log(N)r(N))$ vzhledem k počtu bran, nebo $O(\log(N))$ na iteraci

- **Kvadratické zrychlení:** GA poskytuje kvadratické zrychlení ve srovnání s klasickými algoritmy, což znamená, že může poskytnout významné zrychlení pouze u některých problémů, které mají velký vyhledávací prostor.
- **Omezeno hardwarem:** GA vyžaduje použití velkého počtu qubitů k dosažení výrazného zrychlení, což je v současné době mimo možnosti většiny kvantového hardwaru.
- **Omezeno na nestrukturované vyhledávání:** GA je navržen pro problémy s nestrukturovaným vyhledáváním, což znamená, že nemusí být použitelný na jiné typy problémů, jako je optimalizace nebo simulace.
- **Náchylnost k chybám:** GA, stejně jako všechny kvantové algoritmy, je náchylný k chybám v důsledku šumu a dekoherence. Tyto chyby mohou ovlivnit přesnost a spolehlivost.
- **Omezená použitelnost v kryptografii:** GA lze použít k prolomení určitých kryptografických algoritmů, nelze jej použít pro všechny typy šifrování. Například šifrování veřejným klíčem není zranitelné GA

- **Kvadratické zrychlení:** GA poskytuje kvadratické zrychlení ve srovnání s klasickými algoritmy, což znamená, že může poskytnout významné zrychlení pouze u některých problémů, které mají velký vyhledávací prostor.
- **Omezeno hardwarem:** GA vyžaduje použití velkého počtu qubitů k dosažení výrazného zrychlení, což je v současné době mimo možnosti většiny kvantového hardwaru.
- **Omezeno na nestrukturované vyhledávání:** GA je navržen pro problémy s nestrukturovaným vyhledáváním, což znamená, že nemusí být použitelný na jiné typy problémů, jako je optimalizace nebo simulace.
- **Náchylnost k chybám:** GA, stejně jako všechny kvantové algoritmy, je náchylný k chybám v důsledku šumu a dekoherence. Tyto chyby mohou ovlivnit přesnost a spolehlivost.
- **Omezená použitelnost v kryptografii:** GA lze použít k prolomení určitých kryptografických algoritmů, nelze jej použít pro všechny typy šifrování. Například šifrování veřejným klíčem není zranitelné GA

- **Kvadratické zrychlení:** GA poskytuje kvadratické zrychlení ve srovnání s klasickými algoritmy, což znamená, že může poskytnout významné zrychlení pouze u některých problémů, které mají velký vyhledávací prostor.
- **Omezeno hardwarem:** GA vyžaduje použití velkého počtu qubitů k dosažení výrazného zrychlení, což je v současné době mimo možnosti většiny kvantového hardwaru.
- **Omezeno na nestrukturované vyhledávání:** GA je navržen pro problémy s nestrukturovaným vyhledáváním, což znamená, že nemusí být použitelný na jiné typy problémů, jako je optimalizace nebo simulace.
- **Náchylnost k chybám:** GA, stejně jako všechny kvantové algoritmy, je náchylný k chybám v důsledku šumu a dekoherence. Tyto chyby mohou ovlivnit přesnost a spolehlivost.
- **Omezená použitelnost v kryptografii:** GA lze použít k prolomení určitých kryptografických algoritmů, nelze jej použít pro všechny typy šifrování. Například šifrování veřejným klíčem není zranitelné GA

- **Kvadratické zrychlení:** GA poskytuje kvadratické zrychlení ve srovnání s klasickými algoritmy, což znamená, že může poskytnout významné zrychlení pouze u některých problémů, které mají velký vyhledávací prostor.
- **Omezeno hardwarem:** GA vyžaduje použití velkého počtu qubitů k dosažení výrazného zrychlení, což je v současné době mimo možnosti většiny kvantového hardwaru.
- **Omezeno na nestrukturované vyhledávání:** GA je navržen pro problémy s nestrukturovaným vyhledáváním, což znamená, že nemusí být použitelný na jiné typy problémů, jako je optimalizace nebo simulace.
- **Náchylnost k chybám:** GA, stejně jako všechny kvantové algoritmy, je náchylný k chybám v důsledku šumu a dekoherence. Tyto chyby mohou ovlivnit přesnost a spolehlivost.
- **Omezená použitelnost v kryptografii:** GA lze použít k prolomení určitých kryptografických algoritmů, nelze jej použít pro všechny typy šifrování. Například šifrování veřejným klíčem není zranitelné GA

- **Kvadratické zrychlení:** GA poskytuje kvadratické zrychlení ve srovnání s klasickými algoritmy, což znamená, že může poskytnout významné zrychlení pouze u některých problémů, které mají velký vyhledávací prostor.
- **Omezeno hardwarem:** GA vyžaduje použití velkého počtu qubitů k dosažení výrazného zrychlení, což je v současné době mimo možnosti většiny kvantového hardwaru.
- **Omezeno na nestrukturované vyhledávání:** GA je navržen pro problémy s nestrukturovaným vyhledáváním, což znamená, že nemusí být použitelný na jiné typy problémů, jako je optimalizace nebo simulace.
- **Náchylnost k chybám:** GA, stejně jako všechny kvantové algoritmy, je náchylný k chybám v důsledku šumu a dekoherence. Tyto chyby mohou ovlivnit přesnost a spolehlivost.
- **Omezená použitelnost v kryptografii:** GA lze použít k prolomení určitých kryptografických algoritmů, nelze jej použít pro všechny typy šifrování. Například šifrování veřejným klíčem není zranitelné GA

- **Kvadratické zrychlení:** GA poskytuje kvadratické zrychlení ve srovnání s klasickými algoritmy, což znamená, že může poskytnout významné zrychlení pouze u některých problémů, které mají velký vyhledávací prostor.
- **Omezeno hardwarem:** GA vyžaduje použití velkého počtu qubitů k dosažení výrazného zrychlení, což je v současné době mimo možnosti většiny kvantového hardwaru.
- **Omezeno na nestrukturované vyhledávání:** GA je navržen pro problémy s nestrukturovaným vyhledáváním, což znamená, že nemusí být použitelný na jiné typy problémů, jako je optimalizace nebo simulace.
- **Náchylnost k chybám:** GA, stejně jako všechny kvantové algoritmy, je náchylný k chybám v důsledku šumu a dekoherence. Tyto chyby mohou ovlivnit přesnost a spolehlivost.
- **Omezená použitelnost v kryptografii:** GA lze použít k prolomení určitých kryptografických algoritmů, nelze jej použít pro všechny typy šifrování. Například šifrování veřejným klíčem není zranitelné GA

- **Kvadratické zrychlení:** GA poskytuje kvadratické zrychlení ve srovnání s klasickými algoritmy, což znamená, že může poskytnout významné zrychlení pouze u některých problémů, které mají velký vyhledávací prostor.
- **Omezeno hardwarem:** GA vyžaduje použití velkého počtu qubitů k dosažení výrazného zrychlení, což je v současné době mimo možnosti většiny kvantového hardwaru.
- **Omezeno na nestrukturované vyhledávání:** GA je navržen pro problémy s nestrukturovaným vyhledáváním, což znamená, že nemusí být použitelný na jiné typy problémů, jako je optimalizace nebo simulace.
- **Náchylnost k chybám:** GA, stejně jako všechny kvantové algoritmy, je náchylný k chybám v důsledku šumu a dekoherence. Tyto chyby mohou ovlivnit přesnost a spolehlivost.
- **Omezená použitelnost v kryptografii:** GA lze použít k prolomení určitých kryptografických algoritmů, nelze jej použít pro všechny typy šifrování. Například šifrování veřejným klíčem není zranitelné GA

■ Knihy

■ "Bible" kvantových výpočtů

Michael A. Nielsen , Isaac L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition Anniversary Edition*, 2011, ISSN-10:9781107002173

■ s akcentem na matematický formalizmus:

Nakahara, Mikio and Rahimi, Robabeh and SaiToh, Akira, *Mathematical Aspects of Quantum Computing 2007*, WORLD SCIENTIFIC, 2008, doi = 10.1142/6851

■ s akcentem na informatiku

N. David Mermin, *Quantum Computer Science An Introduction*, Cornell University, New York, Cambridge University Press , 2012, ISBN: 9780511813870

■ Pomocné materiály

■ An Introduction to Quantum Algorithms, Emma Strubell, COS498 – Chawathe Spring 2011

http://cq.us.tempcloudsite.com/archivos/quantum_tutorial.pdf

■ Quantum Algorithm Implementations for Beginners, kolektiv autorů

<https://arxiv.org/abs/1804.03719>

■ Online-přednáška

■ Prof. Dr. Michael J. Hartmann, Quantum Computing, Friedrich-Alexander-Universität Erlangen-Nürnberg, Deutschland

<https://www.fau.tv/clip/id/11992>

Děkuji za pozornost

prof. RNDr. Marek Lampart, Ph.D.

(Vedoucí laboratoře kvantových výpočtů)

VŠB – Technická Univerzita Ostrava
marek.lampart@vsb.cz

1. října, 2024

MS!C