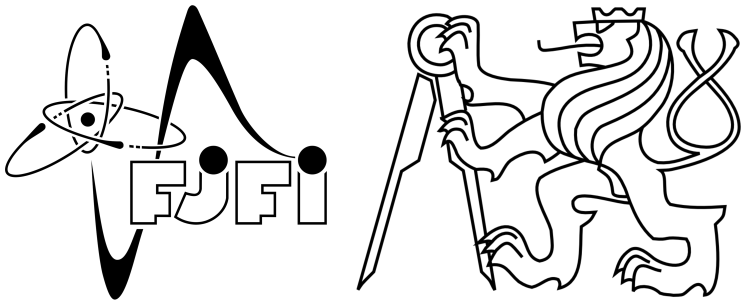
České Vysoké Učení Technické v Praze
Fakulta Jaderná a Fyzikálně Inženýrská

Katedra Fyziky



BAKALÁŘSKÁ PRÁCE

Kvantové počítače pro fyziku vysokých energií

Vedoucí práce: Ing. Bc. Michal Křelina, Ph.D.
Autor práce: Ondřej Brož

Praha 2024

FAKULTA JADERNÁ A FYZIKÁLNĚ INŽENÝRSKÁ

KATEDRA FYZIKY

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Akademický rok: 2022/2023

Student:	Ondřej Brož
Studijní program:	Jaderná a částicová fyzika
Název práce: (česky)	Kvantové počítače pro fyziku vysokých energií
Název práce: (anglicky)	Quantum computing for high energy physics
Jazyk práce:	Čeština

Pokyny pro vypracování:

1) Seznamte se se základními principy kvantových počítačů

2) Proveďte rešerši, kde se uvažuje o využití kvantových počítačů pro částicovou fyziku

3) Seznamte se se základními principy, proč by mohlo být výhodné použít kvantový počítač pro částicovou fyziku

4) Na jednoduchém příkladě demonstrujte výhodu kvantového počítače

Doporučená literatura:

1] M.A. Nielsen, I.L. Chuang, "Quantum computation and quantum information", (Cambridge University Press, Cambridge, 2000)

[2] Ian C. Cloët et al, "Opportunities for nuclear physics & quantum information science", arXiv:1903.05453 (2019)

[3] Christian W. Bauer et al, "Quantum simulation for high energy physics", arXiv:2204.03381 [quant-ph] (2022)

[4] Andrea Delgado et al, "Quantum computing for Data analysis in high-energy physics", arXiv:2203.08805 (2022)

[5] Yuri Alexeev, et al, "Quantum computer systems for scientific discovery", arXiv:1912.07577 (2020)

Jméno a pracoviště vedoucího bakalářské práce:

Ing. Bc. Michal Křelina, Ph.D.
Katedra fyziky, Fakulta jaderná a fyzikálně inženýrská ČVUT v Praze

Datum zadání bakalářské práce: 20.10.2022

Termín odevzdání bakalářské práce: 02.08.2023

Doba platnosti zadání je dva roky od data zadání.

.....
garant studijního programu

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE Fakulta jaderná a fyzikálně inženýrská -3-

.....
vedoucí katedry

.....
děkan

V Praze dne 20.10.2022

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta jaderná a fyzikálně inženýrská

Břehová 7
115 19 Praha 1

PROHLÁŠENÍ

Já, níže podepsaný(á)

Jméno a příjmení studenta:	Ondřej Brož
Osobní číslo:	502399
Studijní program:	Jaderná a částicová fyzika
Studijní obor:	
Specializace:	

prohlašuji, že jsem bakalářskou práci s názvem:

Kvantové počítače pro fyziku vysokých energií

vypracoval samostatně a uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Praze dne 8.1.2024

.....

podpis

Název práce:
Kvantové počítače pro fyziku vysokých energií

Autor:	Ondřej Brož
Studijní program:	Jaderná a částicová fyzika
Druh práce:	Bakalářská práce
Vedoucí práce:	Ing. Bc. Michal Křelina, Ph.D., Katedra fyziky, Fakulta jaderná a fyzikálně inženýrská ČVUT v Praze

Abstrakt: Tato bakalářská práce se zabývá využitím a fungováním kvantových počítačů. Cílem bylo demonstrovat jak a proč by jejich technologie mohla být prospěšná pro fyziku částicových srážek při vysokých energiích. Práce je rozdělena na teoretickou a demonstrační část. Teoretická část vysvětluje fungování kvantového počítače, popisuje jejich využití obecné a specifikuje pro konkrétní problémy v částicové fyzice. Demonstrační část implementuje kvantový algoritmus pro konkrétní problém – pozorování kvantové interference v toy modelu vyzařování skalárních bosonů fermionem s míchající se vůní – na idealizovaném simulovaném kvantovém počítači.

Klíčová slova: Qubit, kvantová brána, kvantový algoritmus

Title:
Quantum computing for high energy physics

Author: Ondřej Brož

Abstract: This bachelor's thesis deals with working and untillization of quantum computers. The goal was to demonstrate how and why their technology can be useful in the field of high energy physics. The thesis is divided into a theoretical and demonstrative part. Theoretical part explains the workings of a quantum computer, describes its general utilization and specifies for particular problems in particle physics. Demonstrative part implements a quantum algorithm for a specific problém – observation of quantum interference on a toy model of scalar boson emission by a fermion with mixing flavor – on an idealized simulated quantum computer.

Key words: Qubit, quantum gate, quantum algorithm

Obsah

1 Úvod **7**

2 Základní principy kvantového počítače **7**
2.1 Qubit . . . 7
2.2 Kvantový algoritmus . . . 7
2.3 Kvantový obvod . . . 8
2.4 Reprezentace brány a jednoqubitové brány . . . 8
2.5 C-brány a ostatní brány . . . 10

3 Obecné využití kvantových počítačů **13**
3.1 Kvantový simulátor . . . 13
3.2 Kvantové dešifrování . . . 14
3.3 Kvantová optimalizace . . . 15
3.4 Kvantové strojové učení . . . 15
3.5 Konkrétní algoritmy . . . 16

4 Problémy částicové fyziky řešitelné kvantovými algoritmy **18**
4.1 Řešení časového vývoje mnohačásticových systémů vysokých energií . . . 18
4.2 Kvantová realizace výpočtů na mřížce . . . 19
4.3 Extrakce vzácných signálů . . . 19
4.4 Kvantová rekonstrukce trajektorií . . . 20
4.5 Kvantová rekonstrukce jetů . . . 20
4.6 Kvantové generativní modely pro simulace . . . 21

5 Aktuální stav kvantových počítačů a jejich využití v částicové fyzice **21**
5.1 Typy qubitů . . . 21
5.1.1 Supravodivé qubity . . . 22
5.1.2 Fotonové qubity . . . 22
5.1.3 Spinové qubity . . . 23
5.1.4 Iontové qubity . . . 23
5.1.5 Qubity pomocí defektů na mřížce . . . 24
5.1.6 Neutrální atomy . . . 24
5.2 Kvantová nadvláda respektive výhoda a budoucnost kvantové informatiky . . . 24
5.3 Nejlepší aktuální kvantové počítače . . . 27

6 Interference v částicových sprškách pomocí kvantového algoritmu **27**
6.1 Problematika zvolená pro vlastní algoritmus . . . 28
6.2 Implementace kvantového algoritmu . . . 29
6.3 Výsledky na simulovaném kvantovém počítači . . . 31

7 Závěr **33**

1 Úvod

V této bakalářské práci se budeme zabývat kvantovými počítači a jejich využitím v problematice částicové fyziky.
Nejprve popíšeme základní principy kvantového počítače a kvantového počítání, základy fyzické realizace kvantového počítače a vlastnosti kvantového algoritmu. Dále představíme problémy fyziky vysokých energií, pro něž lze kvantové počítače a kvantovou informatiku využít, a vysvětlíme, jak konkrétně lze tyto technologie k řešení těchto problémů využít. Poté stručně zmíníme aktuální situaci v oboru kvantových počítačů a stav práce na jejich využití pro částicovou fyziku. Nakonec na toy modelu ukážeme jednoduchý praktický kvantový algoritmus.

2 Základní principy kvantového počítače

2.1 Qubit

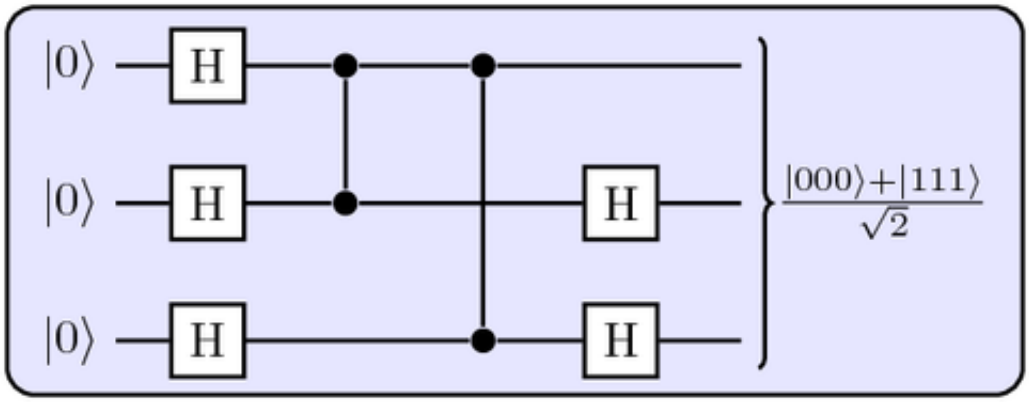
Základní princip a důvod, proč myšlenka kvantového počítače vůbec existuje, jsou qubity. Samotný název vychází z pojmu v klasické informatice - bitu - což je základní paměťová a operační jednotka klasické informatiky. Bit je v klasickém počítači reprezentován jako nabitý či vybitý rezistor tedy s hodnotou 1 či 0. [72]
Qubit je rozšíření této myšlenky za využití principu superpozice. Na nepozorovaném kvantovém systému využitém jako qubit interpretujeme určitou veličinu (například spin) jako hodnotu $|1\rangle$, $|0\rangle$ nebo jejich superpozici, tedy hodnotu mezi nimi. Qubit na konci kvantově informatického procesu je "změřen" a nabude tedy hodnotu $|1\rangle$ nebo $|0\rangle$, ale v samotném průběhu může být manipulován jako superponovaná mezihodnota a opakováním procesu získáme dostatečné množství hodnot $|1\rangle$ a $|0\rangle$, abychom interpretovali výslednou hodnotu jako cokoliv mezi $|0\rangle$ a $|1\rangle$.
Další výhodou qubitů je takzvané kvantové provázání, tedy přímé interakce 2 částic takovým způsobem, že jedna z nich nemůže být plně popsána bez druhé. V takovémto stavu částice vydrží, dokud jsou kvantově koherentní (tedy dokud nejsou změřeny, nebo samovolně neopustí kvantový stav) a to i na větší vzdálenost. Jsou-li 2 provázané částice využívány jako qubity, pak lze ovlivňovat oba dva operacemi pouze na jednom z nich.
Navíc díky realizaci informace jakožto vlastnosti částice je možné vytvořit i takzvané qutrity, qutetry atd., tedy informační jednotky s více než dvěma možnými stavy (3 pro qutrit, 4 pro qutetrit, obecně qudit pro d vlastních hodnot). Hodnota quditu je tedy superpozicí $|0\rangle+|1\rangle+|2\rangle+\cdots+|d-1\rangle$ stavů.

2.2 Kvantový algoritmus

Kvantovým algoritmem rozumíme soubor operací působící na jeden nebo (typicky) více qubitů. Operace jsou zprostředkovány takzvanými kvantovými branami (viz 2.4). Operace mění a provazují kvantové stavy jednotlivých qubitů, které na konci vyprodukují kvantový stav závislý na vstupních qubitech. Celý popsaný proces je ekvivalentní algoritmu z klasické informatiky, kde na diskrétní bity působí logické brány a vydává diskrétní hodnotu výstupu. Zásadní rozdíl je v možnosti superpozice výsledku kvantového algoritmu, kterou samozřejmě nemůžeme určit přímo, nicméně opakovaným průběhem algoritmu můžeme určit poměry mezi diskrétními stavy, z nich amplitudy stavů a z nich samotný stav výsledku. Pro příklady konkrétních algoritmů viz 3.5.

2.3 Kvantový obvod

Kvantový obvod je model, který reprezentuje kvantový algoritmus podobným způsobem jako u klasického elektrického obvodu. Vodorovná osa reprezentuje časový vývoj ve směru zleva doprava. Jednotlivé vodorovne čáry tedy reprezentují jednotlivé qubity (v případě zdvojených čar klasické bity vzniklé změřením qubitu). Na qubity v těchto diagramech působí takzvané kvantové logické brány, plnící obdobnou funkci jako AND, OR a NOT logické brány v klasickém počítači.
Pro popis kvantového obvodu se stanovují dvě rozměrové veličiny - hloubka a šířka daného obvodu. Hloubkou obvodu rozumíme maximální počet počet operací provedených na jednom qubitu ze všech využitých qubitů. Tato délka může být delší než kvantová koherence konkrétního qubitu (schopnost qubitu nebo obecně jakéhokoliv kvantového stavu zůstat v superpozici, popřípadě provázaný. Typicky se udává koherenční čas - doba, po kterou je stav koherentní, pro kvantový obvod také koherentní délka - kolika branami zvládne qubit projít než ztratí koherenci), v takovém případě obvod nemusí vydat takové výsledky, jak je předpokládáno. Šířkou kvantového obvodu rozumíme počet qubitů, se kterými obvod operuje. Ukázkový obvod na Obr. 1 má tedy hloubku 4 a šířku 3.



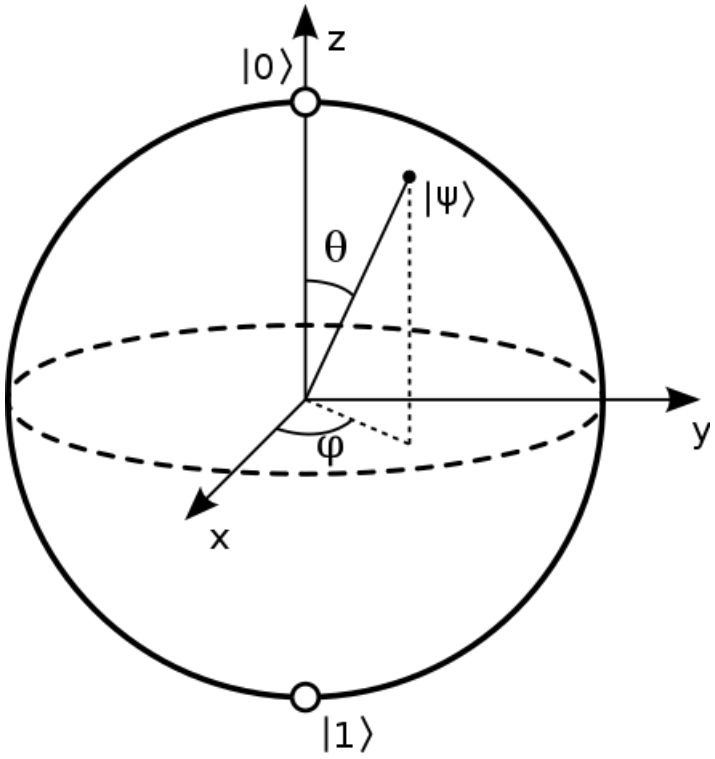
Obr. 1: Příklad jednoduchého kvantového obvodu s Hadamardovými bránami.

2.4 Reprezentace brány a jednoqubitové brány

Kvantová brána obecně působí nějakým jí odpovídajícím operátorem na jeden nebo více qubitů, které skrz ni prochází. Jeden qubit lze reprezentovat buďto jako vektor:

$$|a\rangle = v_0 |0\rangle + v_1 |1\rangle \rightarrow \begin{bmatrix} v_0 \\ v_1 \end{bmatrix}, \tag{1}$$

kde v_0 a v_1 jsou komplexní amplitudy pravděpodobnosti - dohromady normované k 1 (tedy $|v_0|^2 + |v_1|^2 = 1$) - toho zda je qubit $|0\rangle$ či $|1\rangle$, nebo na Blochově sféře.
Blochova sféra (viz Obr. 2) je geometrická interpretace výše zmíněného vektoru za pomocí úhlů θ a φ následovně: $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$, kde tedy θ a φ jsou unikátní pro každý ket $|\psi\rangle$ a udávají polohu na povrchu koule: $\overrightarrow{a} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\varphi)$ (viz Obr. 2).



Obr. 2: Reprezentace hodnoty qubitu na Blochově sféře

Působení brány tedy můžeme buďto vyjádřit jako posun na této kouli, nebo v maticové formě, kde vektor qubitu prošlého touto bránou odpovídá součinu vektoru zmíněného qubitu před bránou a jistou maticí.
Nejjednodušší příklady kvantových bran jsou Pauliho brány. Ty působí pouze na jeden qubit, jsou trojího druhu - $\hat{X}$, $\hat{Y}$ a $\hat{Z}$ - a odpovídají rotaci o π kolem odpovídajících os na Blochově sféře.
V maticové formě je lze vyjádřit jako:

$$\hat{X} = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \hat{Y} = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \hat{Z} = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

X-brána odpovídá NOT operaci v klasické informatice, kde převede $\hat{X}\,|0\rangle = |1\rangle$ a naopak. Y-brána působí obdobně, ovšem v komplexní složce, zatímce Z-brána působí spíše jako fázový posun, jelikož nepůsobí na $|0\rangle$ ($\hat{Z}\,|0\rangle = |0\rangle$), ale $|1\rangle$ převádí na $\hat{Z}\,|1\rangle = -\,|1\rangle$.
Dalším příkladem jednoduché a zásadní jednoqubitové brány je takzvaná Hadamardova brána, která převádí qubit do superpozice obou stavů jedna ku jedné. Tyto stavy jsou známé jako qubitové stavy

$$|+\rangle = \hat{H}\,|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{2}$$

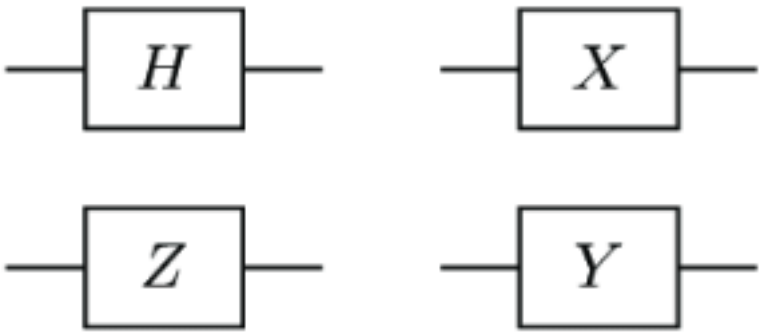
a

$$|-\rangle = \hat{H}\,|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{3}$$

V maticové formě tedy:

$$\hat{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Jednoqubitové brány graficky v kvantovém obvodu značíme stejným písmenem jako jeho operátor, v obyčejné čtvercové buňce, tedy následovně:



Obr. 3: Značení jednoqubitových kvantových bran v kvantovém obvodu (Hadamardova brána vlevo nahoře, Pauliho X brána vpravo nahoře, Pauliho Y brána vlevo dole a Pauliho Z brána vpravo dole

2.5 C-brány a ostatní brány

Druhou nejjednodušší branou působící na více - dva - qubity a mající ze všech bran nejblíže ke klasické informatické bráně, konkrétně k NOT bráně, je CNOT brána. Pokud je první qubit $|0\rangle$ tak nechá oba qubity nepozměněné a pokud je $|1\rangle$, tak prohodí jejich hodnoty. V rovnicovém zápisu tedy:

$$\hat{\text{CNOT}}\,|a,b\rangle = |a,(a+b)\text{mod}2\rangle$$

respektive maticově

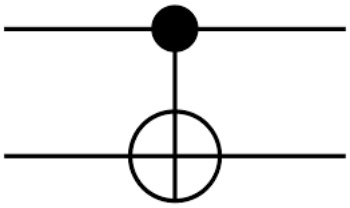
$$\hat{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Název C-NOT vychází ze značení takzvaných kontrolních bran (anglicky control, tedy C), kde jeden qubit řídí, jestli operace má být provedena - v případě C-NOT brány stav prvního qubitu - a s druhým je operováno. C-NOT je ve skutečnosti jen kontrolní verzí Pauliho X brány, u níž jsme zmiňovali, že se jedná o ekvivalentu negace z klasické informatiky. Na stejném principu poté existují i C-Y a C-Z brány (tedy brány, které na druhý qubit působí jako Y, respektive Z brána, je-li první qubit ve stavu $|1\rangle$). Jakožto přímou kvantovou ekvivalentu klasické logické brány je možné ji zapsat jako logickou tabulku:

VSTUP		VÝSTUP	
řídící qubit	operovaný qubit	řídící qubit	operovaný qubit
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Tab. 1: Logická tabulka reprezentující chování C-NOT brány na čistých $|0\rangle$ a $|1\rangle$ stavech

V kvantovém obvodu ji značíme jako propojení dvou qubitů s kruhy na uzlech, kde kruh na kontrolním qubitu je vyplněný a kruh na operovaném qubitu je prázdný (viz Obr. 4).



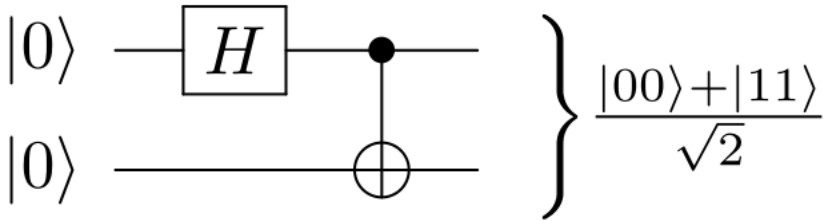
Obr. 4: Značení CNOT brány v kvantovém obvodu

CNOT brána a obdobné kontrolované brány mimo jiné zajišťují provázání qubitů. Zároveň umožňují vytvoření takzvaných Bellových stavů, tedy nejprovázanějších možných stavů. Ty existují celkem 4 [87]:

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad |\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \quad |\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \quad |\Psi^+\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{4}$$

K jejich realizaci je potřeba kombinace Hadamardovy brány a CNOT brány (viz realizace $|\Phi^+\rangle$ Obr. 5) a k dosažení ostatních Bellových stavů stačí stejný obvod s jiným počátečním stavem. Označíme-li obvod z Obr. 5 jako $B\hat{E}LL$, pak platí:

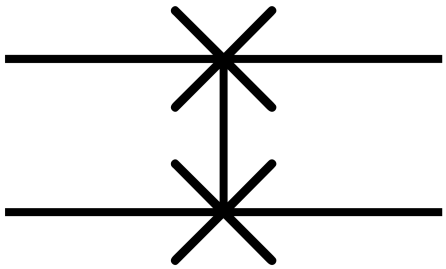
$$B\hat{E}LL\,|00\rangle = |\Phi^+\rangle \quad B\hat{E}LL\,|01\rangle = |\Phi^-\rangle \quad B\hat{E}LL\,|10\rangle = |\Psi+\rangle \quad B\hat{E}LL\,|11\rangle = |\Psi^-\rangle\,. \tag{5}$$



Obr. 5: Realizace Bellova stavu $|\Phi^+\rangle$ pomocí Hadamardovy brány a CNOT brány

Kvantových bran existuje velmi mnoho, ovšem všechny mohou být vytvořeny kombinací výše zmíněných bran, ekvivalentně jako všechny komplexní logické brány klasické informatiky jsou jen kombinacemi NOT, OR a ANDových bran. Mezi nejznámější příklady patří:

- **Swap brána** - navzájem prohodí stavy dvou qubitů.
  V rovnicovém zápisu:
  $$\hat{\text{SWAP}}\,|a,b\rangle = |b,a\rangle\,,$$
  respektivě v maticovém zápisu:
  $$\hat{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$
  a v kvantovém obvodu značíme propojením dvou qubitů a křížky na uzlech (viz Obr. 6).



Obr. 6: Značení swap brány v kvantovém obvodu

- **Toffoliho brána** - někdy také nazývána CCNOT brána - pracuje se 3 qubity, ale operuje jen s posledním, pokud jsou první 2 ve stavu $|1\rangle$.
  V rovnicovém zápisu tedy:

$$\hat{\text{TOFF}}\,|a,b,c\rangle = |a,b,(c+ab)\text{mod}2\rangle\,,$$

  respektive v maticovém zápisu:

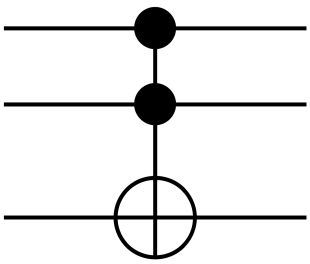
$$\hat{TOFF} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

  a jakožto kvantový ekvivalent klasické logické brány ji lze zapsat i logickou tabulkou:

VSTUP			VÝSTUP		
1. řídící qubit	2. řídící qubit	operovaný qubit	1. řídící qubit	2. řídící qubit	operovaný qubit
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Tab. 2: Logická tabulka reprezentující chování Toffoliho brány na čistých $|0\rangle$ a $|1\rangle$ stavech

  Značíme ji jako CNOT bránu se dvěma kontrolními uzly (viz Obr. 7).



Obr. 7: Značení Toffoliho brány v kvantovém obvodu

- **Obecná brána** - posune hodnotu na Blochově sféře o jakoukoliv hodnotu v jakémkoliv směru.

  Označíme-li posunovanou hodotu jako: $\overrightarrow{\delta} = (\delta_x, \delta_y, \delta_z)$, tak rovnicový zápis odpovídá:

$$\hat{U}(a\,|0\rangle + b\,|1\rangle) = a\cos\left(\frac{\delta_z}{2}\right)|0\rangle + be^{i\delta_x - \delta_y}\,|1\rangle$$

  respektive v maticovém zápisu:

$$\begin{pmatrix} 0 & 1 \\ e^{-i\delta_x} & 0 \end{pmatrix} \times \begin{pmatrix} 0 & -i \\ ie^{-i\delta_y} & 0 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta_z} \end{pmatrix}$$

  a v kvantovém obvodu značíme čtvercovou buňkou s T (viz Obr. 8).

Obr. 8: Značení obecné kvantové brány v kvantovém obvodu

3 Obecné využití kvantových počítačů

Dříve než se bude moct věnovat využitím kvantových počítačů a jejich technologií v částicové fyzice, uvedeme menší vhled do jejich obecného využití ve vědeckých i komerčních sférách a zhruba popíšeme fungování jednotlivých cest jejich využití. Ještě předtím je ovšem nutné zmínit, že žádné z využití kvantových počítačů nevytváří nic nového, čeho by nebylo možné dosáhnout numerickou či jinou metodou počítačem klasickým, jsou ovšem zásadně rychlejší, kompaktnější nebo méně zdrojově náročné než jejich klasické alternativy.

3.1 Kvantový simulátor

Kvantový simulátor je laicky asi nejzřejmější využití kvantového počítače, tedy řešení propabilistických problémů propabilistickým (kvantovým) počítačem. Jinak řečeno problém, který z důvodu zadání nebo jeho podstaty nelze řešit přímo a konkrétně a jen jako pravděpodobnost různých výsledků, je nejvhodnější řešit počítačem, který vyhodnocuje výsledek jako pravděpodobnost stavů. Nejde o první druh pravděpodobnostního počítače, statistické či

analogické pravděpodovnostní počítače existují již pár desítek let. Realizace pravděpodobnostního počítače pomocí kvantové informace je ale výrazně zdrojově výhodnější pro určité typy úloh a může využít superponovaných stavů pro nižší algebraickou komplexitu výpočtu.
Tato myšlenka sahá nejméně do osmdesátých let dvacátého století k Richardu Feynmanovi a jeho simulaci oblaku částic [35], kde demonstroval, že přímá simulace vede k exponenciálnímu nárůstu komplexnosti programu, ale i velikosti simulujícího počítače kvůli paměti nutné k samotnému provedení a jako řešení navrhuje právě počítač operující s pravděpodobnostmi stavů částic - kvantový počítač. Hlavní princip kvantového simulátoru je algoritmus nějakým způsobem ekvivalentní procesu, který se snažíme simulovat - tedy aby veličina využívaná jako qubit odpovídala vlastnosti, hodnotě či pozorovatelné, jejíž chování se snažíme nasimulovat. Toho lze dosáhnout pomocí algoritmu s kvantovými branami [3] (tedy stále jako kvantový ekvivalent digitálního počítače) nebo také systémem nepozorovaných částic udržovaných ve stabilním prostředí s Hamiltoniánem zvoleným tak, aby odpovídal procesu, který simulujeme, čímž se celý hamiltonián chová jako jedna velká brána komplexně působící na všechny qubity, tedy analogového kvantového počítače.
Kvantový simulátor je zřejmě užitečný nástroj pro různé oblasti fyziky včetně té částicové (o tom viz níže), ale také pro fyziku velmi nízkých teplot [78] nebo klasické mechaniky s mnohatělesovými systémy [20], zároveň také pro různé oblasti chemie [43], ale i pro nevědecké oblasti, jako je predikce chování obchodních trhů a jiných ekonomických struktur [28]. V neposlední řadě kvantové simulátory s Hamiltoniánem působícím na všechny qubity byly použity k simulaci časových krystalů, a tedy mohou sloužit k jejich zkoumání [45]. Časový krystal je struktura hmoty v základním kvantovém stavu, jejíž stav se v čase opakuje, podobně jako se rozestavení molekul opakuje v klasickém krystalu [91].

3.2 Kvantové dešifrování

Kvantové dešifrování je asi nejznámější a dnes nejvíce rozebírané využití kvantových počítačů. Působí totiž jako reálná hrozba internetového a obecně informačního zabezpečení v blízké budoucnosti a potenciálně již dnes.
Nejrozšířenější způsob asymetrického šifrování informací (RSA) funguje na principu klíče získaného součinem velkých prvočísel (v řádech $10^{\sim 100}$) [5]. Informace je zakódována pomocí tohoto součinu, ale může být rozkódována pouze pomocí samotných prvočísel [51]. To bylo poměrně dlouho považováno za bezpečné, jelikož rozkódování, když cíl zná daná prvočísla, je komplexnostně triviální, ale určení těchto prvočísel pomocí nejlepších známých hledacích algoritmů na dnešních nejvýkonnějších superpočítačích by zabralo absurdně velké množství let.
Problém nastává s kvantovými počítači a Shorovým algoritmem [83] vynalezeným Peterem Shorem v roce 1994, který využívá schopnosti kvantového počítače pomocí superpozice zkoumat více stavů zároveň, a exponenciálně tak urychluje nejzdlouhavější část hledacích algoritmů. Rozdíl u velkých prvočísel je tak velký, že hledací času mnoha a mnoha let zkracuje na otázku hodin, ne-li minut.
S dostatečně výkonným kvantovým počítačem by bylo tedy možné rozluštit jakoukoliv internetovou komunikaci se současnými šiframi, což je důvod pro znepokojení jak běžných občanů, tak hlavně velkých firem a vlád. Tak výkonný počítač dnes naštěstí ještě neexistuje (viz kapitola 5), ale jeho existenci lze v blízké budoucnosti očekávat (opět viz kapitola 5), což vede některé dnešní vlády a společnosti ke shromažďování citlivých přenosů informací, které budou moci, až bude dostatečně výkonný kvantový počítač vyvinut, dešifrovat a potenciálně zneužít (takzvaný harvest now, decrypt later útok).

3.3 Kvantová optimalizace

Kvantová optimalizace je (mimo kvantové dešifrování zmíněné v předchozí podkapitole) asi nejzkoumanější obor kvantové informatiky. Jde o hledání (optimálních) řešení algebraicky náročných problémů pomocí schopnosti qubitů pracovat na několika stavech zároveň díky superpozici. Tato řešení pro určité problémy přináší teoreticky az polynomiální zrychlení, které pro masivní problémy může být klíčové.
Typickým příkladem jsou kombinatorické optimalizační problémy jako Problém obchodního cestujícího (hledání nejkratší spojnice v ohodnoceném úplném grafu - derivované z klasické úlohy o nejkratší trase cestujícího obchodníka) či Problém batohu (hledání nejefektivnějšího naplnění omezeného obsahu objekty s nejvyšší hodnotou - derivované z klasické úlohy z naplnění batohu s maximální nosností předměty se známými vahami), které jsou v jádru většiny logistických problémů a v klasické informatice jsou exponenciálně náročné na řešení. [73] Obdobně pro více akademické účely - fitování náročných funkcí na velkém množství dat může být drasticky zrychleno kvantovým fitováním namísto toho klasického.
V neposlední řadě jsou kvantové algoritmy vhodné pro řešení soustav lineárních rovnic, kde nabízí opět exponenciální zrychlení (z $O(N)$ na $O(\log N)$ [92], což může být zásadní pro soustavy o tisících rovnicích s tisíci proměnnými, které se nachází například v neuronových sítích (viz následující podkapitola) nebo v hledacích algoritmech, kde nabízí sice jen polynomiální zrychlení, nicméně pro neuspořádané seznamy o stovkách milionech prvků ve vyhledávačích jako Google mohou mít mimořádné využití. Realizování tohoto procesu, kromě problémů vyvstávajících v realizaci jakéhokoliv kvantového algoritmu, naráží také na problém převedení velkých matic do kvantového formátu. [1]

3.4 Kvantové strojové učení

Strojové učení je další aktuálně se rychle rozvíjející technologické odvětví slibující mnoho využití a zlepšení v nejrůznějších odvětvích vědy i soukromého sektoru. Strojové učení právě teď zažívá velké rozšíření mezi veřejností díky představení aplikací jako DALL-E a ChatGPT [25], ale samo o sobě může být využito i k akademičtějším účelům [66] od generování simulovaných částicových srážek až po hledání vhodných proteinů při designování nejrůznějších léků.
Strojové učení (také známé jako umělá inteligence) obecně funguje jako program hledající vzory a opakující se prvky v zadaném programu, aby nalezl řešení. Tento proces teoreticky funguje jako propojování prvků a vlastností a přiřazování jim váhy (důležitosti) a z komplexního opakování tohoto procesu ve finále interpretování výsledku. Jak program určí váhy k jednotlivým prvkům a jak rozpoznává jednotlivé prvky, není jasné ani tvůrci samotného programu, a jde tedy o takzvanou "černou skříňku" [7]. Programu je tedy představeno velké množství příkladů problémů, které má řešit, entit, které má generovat, nebo objektů, které má rozpoznávat, podobné množství příkladů, které nesplňují požadavky, a program se poté snaží zadání replikovat.
Kvantové strojové učení se rozděluje do 4 druhů (viz Obr. 9), podle metody kterou je uskutečňováno (klasický/kvantový algoritmus), a podle problematiky, kterou řeší (klasická data/kvantová data): [9]

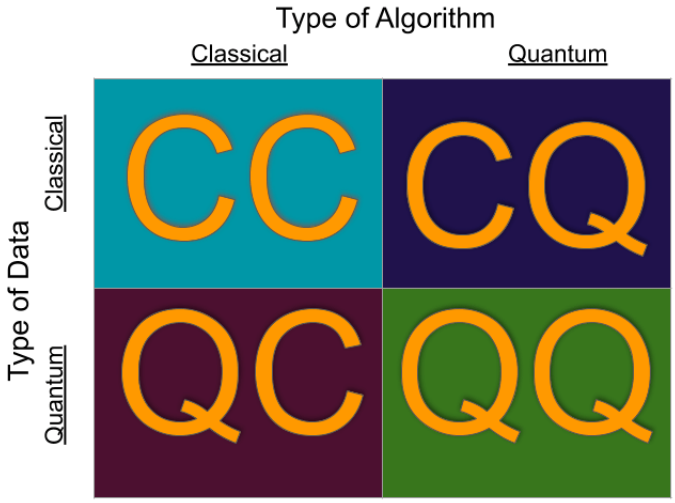
- **CC - klasický algoritmus na klasických datech**
  Nejde ve skutečnosti o kvantové strojové učení, ale jen o klasické strojové učení, jako je například Chat-GPT.

- **CQ - kvantový algoritmus na klasických datech**
  Aktuálně silně zkoumaný kvadrant kvantového strojového učení. Naráží na problém

převedení obrovských matic nutných pro strojové učení do kvantového zápisu a na dosažení dostatečně vysokého koherenčního času a nízké chybovosti, aby algoritmus opravdu proběhl. Jedna z navrhovaných implementací navrhuje úpravu klasických neuronových sítí s realizací samotných jednotlivých neuronů kvantově a zanechání jejich propojení klasicky. Celá tato technologie si slibuje polynomiální a vyšší zrychlení stávajících umělých inteligencí.

- **QC - klasický algoritmus na kvantových problémech**
  S výjimkou CC aktuálně nejvyužívanější a nejvíce se rozvíjející kvadrant. Využívá klasických cílených umělých inteligencí k řešení problémů při realizaci a práci s kvantovými algoritmy (optimalizace konkrétního algoritmu, řešení chybovosti, simulace qubitové realizace atd. ...).

- **QQ - kvantový algoritmus na kvantových datech**
  Zatím nejméně zkoumaný kvadrant. Jeho realizace bude možná, až když chybovost klesne a škálovatelnost spolu s koherentními časy vzroste na úroveň běžného využití kvantových počítačů. V budoucnosti by mohl reprezentovat skutečně kvantové strojové učení.



Obr. 9: 4 druhy kvantového strojového učení. Na vodovné ose: typ algoritmu(metody) a na svislé ose typ dat(problematiky) [11]

3.5 Konkrétní algoritmy

Již dnes existuje mnoho kvantových algoritmů pro řešení konkrétních problémů. Většina z nich předchází existenci kvantového počítače schopného je spustit, některé dokonce existenci samotných funkčních kvantových počítačů či realizace jednoho qubitu. V této podkapitole si zběžně představíme nejznámější z nich, k čemu slouží a jejich srovnání s klasickými algoritmy:

- **Shorův algoritmus**
  Shorův algortimus je algorimus provádějící kvantovou verzi Fourierovy transformace. Nejznámější příklad využití této transformace je hledání opakujícího se vzorce v dlouhé řadě, typicky při rozkladu čísla na velká provčísla (stovky cifer), například při dešifrování online komunikací šifrovaných právě takovýmto klíčem (viz 3.2). To z něj dělá jeden z dnes nejvíce zájmových kvantových algoritmů [86] a byl již několikrát zrealizovaný (například na čísle 15 v Institutu experimentální fyziky v Innsbrucku [67]). Shorův algoritmus nabízí exponenciální

zrychlení oproti jeho klasickým alternativám, jelikož dosahuje časové náročnosti $O(\log(N)^2 \log\log(N))$ [83], zatímco nejlepší klasické algoritmy dosahují $O(e^{\log(N)^{\frac{1}{3}} \log\log(N)^{\frac{2}{3}}})$. [60]

- **Groverův algoritmus**
  Groverův algoritmus [48] je kvantový hledací algoritmus využívající superpozice qubitu ke zkoumání několika členů zároveň. Dosahuje časové náročnosti $O(\sqrt{N})$ a tudíž má velké využití pro hledání v neuspořádaných seznamech, kde nejlepší klasické hledací algoritmy dosahují $O(N)$, jelikož musejí jednotlivě projít alespoň polovinu členů. To je ovšem jen polynomiální zrychlení a nemá tak lákavé využití jako dříve zmíněný Shorův algoritmus, tudíž zájem o jeho brzkou realizaci není tak velký. Aktuálně probíhá několik pokusů a jeho realizaci přes spinové qubity na iontech [30] či pomocí optických metod [74].

- **VQE algoritmus**
  VQE algoritmus (Variational quantum eigensolver) není čistě kvantový algoritmus, ale hybrid mezi kvantovým a klasickým algoritmem, který slouží k nalezení vlastních čísel a vlastních vektorů (eigenvalues and eigenvectors) kvantového operátoru (typicky hamiltoniánu) pomocí hledání jeho základního stavu ze známého ansatzu [85]. Jeho hlavní výhoda není zrychlení (jelikož proces, který řeší, není nijak výrazně časově náročný), nýbrž jeho přesnost, která je až kvadraticky lepší než u alternativních řešení, a odolnost vůči chybovosti kvantového hardwaru [34]. Hlavní využití nalézá v kvantové chemii, kde hledání základních stavů komplikovaných systémů, jako jsou velké molekuly, může být poměrně náročné. Místy se již testuje jeho využití a hlavní práce nyní probíhá na jeho škálování [80] a snižování jeho chybovosti [50].

- **Kvantový aproximační optimalizační algoritmus**
  Kvantový aproximační optimalizační algoritmus (nebo zkráceně QAOA) je opět hybrid mezi klasickým a kvantovým algoritmem, sloužící k nalezení řešení kombinatorických optimalizačních problémů [33]. QAOA oproti klasickým algoritmům poskytuje polynomiální zrychlení, jelikož klasické řešení kombinatorických optimalizačních problémů dosahuje typicky časových náročností kolem $O(2^N)$, QAOA dosahuje polynomiálních výsledků [95]. Tento druh problémů zahrnuje víceméně celý obor logistiky od plánování procesů, datových struktur, skladování, až po cestování a mnoha dalšího a zájem o jejich efektivnější řešení je tedy samozřejmě značný. Postup na realizaci těchto algoritmů je zatím bohužel ještě v počátcích a nedošel dál než do povrchových vrstev [84]. Zároveň se zdá, že ke zkonstruování funkčního algoritmu, který by opravdu efektivně zrychlil řešení těchto problémů, je nutný výkon kvantového počítače, který je zatím v nedohlednu [38].

- **Deutsch-Jozsův algoritmus**
  Deutsch-Jozsův algoritmus je řešení Deutsch-Jozsova problému a spíše než pro praktické využití sloužil jako jeden z prvních důkazů exponenciálního zrychlení kvantového počítače oproti klasickému [18]. Deutsch-Jozsův algoritmus spočívá ve zkoumání "černé skříňky", což je program, který pro n vstupů generuje výstupy 0 nebo 1 a to buďto konstantně (0 pro všechny vstupy, nebo 1 pro všechny vstupy), nebo balancovaně (0 pro přesně polovinu vstupů a 1 pro přesně polovinu vstupů). Cílem problému je určit, jestli "černá skříňka" odpovídá konstantně, nebo balancovaně. Pro kvantový počítač je tento problém triviální a odpověď určí po jediném pokusu. Pro klasický počítač je tato úloha v nejhorším prípadě exponenciálně náročná (musí provést $2^{n-1}+1$ srovnání a je tedy $O(2^n)$). To bylo již demonstrováno na skutečném kvantovém počítači v IBM výzkumném zařízení v San Jose v roce 1998 [17]. Tento algoritmus slouží hlavně jako teoretická demonstrace, ale probíhají i práce na jeho praktickém

využití jakožto šifrovacím způsobu pro online zabezpečení, kde by "černá skříňka" generovala pro velmi velké množství vstupů a určení funkce by bylo pro klasický počítač obdobně náročné jako rozklad na velká prvočísla [70].

- **Harrow-Hassidim-Lloydův algoritmus**
  Harrow-Hassidim-Lloydův algoritmus (nebo krátce HHL) je kvantový algoritmus určený k řešení soustav lineárních rovnic. Jejich běžné řešení (například Gaussovou eliminací) dosahuje časové náročnosti až $O(N^3)$ a nejlepší řešení klasickým počítačem lze snížit až na $O(N)$. HHL je soustavu schopný řešit s $O(\log N)$ a nabízí tedy exponenciální zrychlení [68]. Jelikož řešení soustav lineárních rovnic je jeden z nejčastějších informaticky řešených problémů, je zřejmé, že toto zrychlení by nalezlo využití prakticky v každém oboru. Díky tomu zájmu a zároveň poměrné jednoduchosti pro konstrukci na malých škálách jde o jeden z nejčastěji konstruovaných kvantových algoritmů [94]. Řešení soustav lineárních rovnic je navíc hlavní princip strojového učení, což z HHL dělá hlavní součást produkce kvantového strojového učení [2].

4 Problémy částicové fyziky řešitelné kvantovými algoritmy

V této kapitole konečně představíme 6 využití technologií kvantových počítačů pro částicovou fyziku. V každé podkapitole představíme konkrétní problém, jeho aktuální snahy o řešení a jak by tyto snahy mohly být zlepšeny kvantovou informatikou. [27]

4.1 Řešení časového vývoje mnohačásticových systémů vysokých energií

Experimentální výsledky při pokusech srážek vysokých energií (jako například LHC) jsou určované z produktů generovaných v těchto srážkách. Tyto částice jsou ale produkované až v pozdějších částech studované interakce a veškeré predikce založené čistě na těchto informacích jsou tedy poněkud limitované. Analytické řešení je typicky řešené poruchovou teorií ve formě Feynmannových diagramů, nicméně víme, že kvantová chromodynamika je v některých svých oblastech silně neporuchový systém, a proto jej v realitě studujeme spíše pomocí modelu - které však mohou obsahovat část poruchového počtu. Alternativním neanalytickým řešením je mřížková kalibrační invariance (více o ní v následující podkapitole). [58]
Řešení, které v tomto směru nabízí kvantová informatika, je přistupování k těmto problémům jako k mnohočásticovému systému, kterým opravdu jsou. Ty není možné analyticky vyjádřit, ale je dost dobře možné je reprezentovat jako hamiltonián na kvantovém simulátoru a přiřazením jednotlivých pozorovatelných na simulátoru k časově nezávislým proměnným srážky by umožňovalo simulovat části srážky způsobem bližším analytickému než mřížková kalibrační invariance (byť stále také neanalytická). [27]. Alternativně k vývoji pozorovatelné na kvantovém simulátoru D-teorie, tedy neporuchový přístup ke kvantové teorii pole, kde d-rozměrná pole uvažujeme jako d+1-rozměrná, což vede k několika extra symetriím a umožňuje počítání
s částicemi bez uvažování jejich hmotnosti, [14] propagovaná soukromou firmou D-Wave System navrhuje (a pro jiné komerční a jednodušší akademické problémy i demonstruje) hledání těchto řešení pomocí kvantového žíhání (v angličtině quantum annealing). Kvantový žíhač je specifický neuniverzální typ kvantového počítače, určený k hledání základního stavu hamiltoniánu, na kterém byl spuštěn, pomocí kvantového počtu s adiabatickými sumami. Jeho neuniverzálnost vyvažuje výkonnostní objem aktuálně převyšující jakýkoliv aktuální univerzální kvantový počítač (viz kapitola 5 sekce Nejlepší aktuální kvantové počítače). [59]

4.2 Kvantová realizace výpočtů na mřížce

Jedním z aktuálně využívaných klasických řešení problému, zmíněného o podkapitolu výše, je mřížková kalibrační invariance, také známá jen jako výpočty na mřížce (v angličtině Lattice gauge theory), která rozděluje časoprostor na "mřížku" diskrétních úseků času a prostoru, ve kterých již lokalizované analytické řešení najít lze a jejich sloučením lze dosáhnout poměrně realistických výsledků. Lagrangiány v jednotlivých dílcích této mřížky mají snadno nalezitelné (někdy až analyticky) lokální minimum/maximum a rozdíly mezi jednotlivými dílky odpovídají kvantové povaze takto řešených problémů. [56]
Dimenzionalita těchto mřížek se typicky zapisuje jako N+1D, kde N značí počet prostorových dimenzí a 1 je nezbytná časová dimenze. Nejzřejmější, ale i výkonnostně nejnáročnější příklad je 3+1D mřížka, která nemá žádná další omezení, oproti ostatním příkladům mřížek, nicméně její časová i paměťová náročnost je exponenciálně vyšší. Výrazně častěji používaná je 2+1D mřížka, která zjednodušuje například děje při neperiferních srážkách v příčné rovině, kde vzniklá "palačinka" může být aproximována do roviny. Nakonec 1+1D mřížka nebývá využívána pro výpočet konkrétních dějů, ale spíše jako toy model procesů s nízkou asymptotickou volností, výměnou za to je ale časově i paměťově nejvýhodnější. [57]
Tyto metody jsou v klasickém přístupu typicky realizovatelné pomocí Markov Chain Monte Carlo modelů (dále jen MCMC), tedy statistického rozložení s náhodnými vstupy, kde jednotlivé kroky závisí na těch předchozích. [13] Ty ale tíhnou ke spojité limitě, která z kvantové povahy problému nedodává výsledky shodující se s experimentálními daty. Navíc dráhové integrály využívané těmito MCMC modely trpí "znaménkovým problémem", tedy exponenciálním nárůstem v náročnosti pro výpočty s nenulovými fermionovými hustotami, což pro MCMC modely kvantové chromodynamiky brání zkoumání fázového modelu mimo nulovou baryonovou hustotu, tedy oblasti zásadní pro problémy motivující tento výzkum (pochopení raných fází vesmíru, neutronových hvězd, fázových přechodů kvark-gluonového plazmatu atd.). [27] Realizace těchto modelů pomocí kvantového počítače by se pomaleji blížily spojité limitě, jelikož výsledky tohoto počítače jsou samy, ze své kvantové povahy, diskrétní, tak navíc pomocí algebraického zrychlení mohou vyrušit zpomalení způsobené "znaménkovým problémem". Nicméně efektivní realizace takovýchto simulací by vyžadovaly kvantový software v řádu alespoň tisíců qubitů, což v nejbližší budoucnosti nebude možné (viz kapitola 5). [63]

4.3 Extrakce vzácných signálů

Extrakce vzácných signálů je jeden z nejzásadnějších analytických procesů při hledání nové fyziky ve zkoumání srážek vysokých energií. Problém leží hlavně v ohromném množství dat a ve skrytí signálu pozadím. [27] Klasické řešení spoléhá na metody klasifikačních problémů, kde jsou určitá kritéria při výběru zkoumaných instancí pod-, či pře- hodnocována, což by mělo vést ke snazšímu odhalení neobvyklých jevů. Tyto metody jsou ale časově i zdrojově náročné [71]. Aktuálně rozvíjený a slibný způsob řešení tohoto problému jsou různé variace strojového učení jako neomezovaný vyhledávací model či posílený klasifikační strom. [12]
Výhoda řešení těchto problémů kvantovými metodami není zatím matematicky rigorózně dokázána, nicméně je silně očekávána ať už jako posílení aktuálně úspěšných řešení strojových učení (viz podkapitola 3.4), tak jako využití algebraického zrychlení ke zpracování větších objemů dat při klasických klasifikačních řešeních. Unikátně kvantové řešení také slibují geometricky orientované strojové učení (v angličtině geometrically oriented machine learning či GOQML) a kvantově posílené pomocně vektorové stroje (v angličitně quantum-enhanced support vector machine či Q-SVM)[42] , které využívá známých symetrií a vzorů v dříve zkoumaných problematikách a hledá neobvyklosti

v nich.

4.4 Kvantová rekonstrukce trajektorií

Mnoho analytických kroků při rekonstrukci události (v angličtině event reconstruction) jsou jen specifické případy rozpoznávání vzorů ve větších objemech dat. Jedním z nich je rekonstrukce trajektorií nabitých částic po srážce. Kandidáti na tyto trajektorie jsou určované prostorovými body v citlivých částech detektorů, kde byla zanechána část energie prolétající částice, a jsou vybíráni tak, aby korespondovali ke stejnému místu srážky a dalším proměnným (energie, hybnost, náboj, atd.) očekávatelným v dané události. Ty jsou poté využívány k analýze a rekonstrukci dalších pozorovatelných proměnných a fyzikálních procesů probíhajících při srážce. Tento problém má ve fyzice vysokých energií velmi vysokou dimenzionalitu kvůli granulárním strukturám detektorů využívaných ke změření těchto dat. [27]
Rekonstrukce trajektorií klasickým způsobem je, kvůli výše zmíněné vysoké dimenzionalitě a možnosti duplicity signálu na jednom zrnu detektoru při průchodu více částic najednou, výkonově nejnáročnější částí rekonstrukce srážkových událostí. [24] Nově se k tomuto zpracování začíná využívat i grafické neurální sítě (Graphical Neural Networks v angličtině), které vykazují lineární zrychlení. To není sice zatím rigorózně dokázané, ale vykazuje empirické výsledky. [49] To by tedy stejně jako v předchozí podkapitole mohlo při posílení strojového učení kvantovým algebraickým zrychlením proces urychlit až o vyšší polynomiální stupeň.
Alternativně lze tento proces převést na problém kvantové neomezené binární optimalizace (Quantum Unconstrained Binary Optimalization dále jen QUBO) [8], kde dvojice či trojice zásahů po sobě umístěných detektorů odpovídají jednotlivým složkám kandidátů trajektorií, což lze vyjádřit jako relativně jednoduchý hamiltonián a být řešené QAOA algoritmem (viz podkapitola 3.5).

4.5 Kvantová rekonstrukce jetů

Rekonstrukce jetů je obdobně jako v předchozí podkapitole výkonnostně náročný problém na rozpoznávání vzorů. Jetem rozumíme spršku stabilních částic vylétávajících v kuželovitém regionu. Ty vznikají hadronizací kvarků a gluonů vznikajících ve vysoko-energetických srážkách, která produkuje barevně neutrální částice, měřitelné detektory. Samotnou rekonstrukcí jetu rozumíme odhad kinematiky a složení částic(e) produkující samotný jet. Rekonstrukce a analýza jetů jsou elementární složkou moderního zkoumání srážkových fenomenů a například vedly k důkazu existence gluonů (při detekci 3 jetů v e^+e^- srážkách). [27]
Jety jsou klasicky rozpoznávané a rekonstruované kónickým či sekvenčním rekombinačním způsobem. Kónický způsob rozpoznávají jety pomocí hledání intenzivních energetických proudů a do jetu jsou sdružovány pomocí definitivního geometrického kuželu. Sekvenční způsob rozpoznává jety pomocí vzdálenostních metrik v různých fázích detekce a závisí více na logických souvislostech než na geometrickém předpokladu. [24] Tyto procesy mohou být zjednodušeny opět převedením na QUBO problém (viz podkapitola 4.4) [8], kde je kombinovaná kónická i sekvenční metoda. Zároveň je navržený alternativní systém rozpoznávání jetů pomocí 2 subrutin, kde první porovnává Minkowského vzdálenosti mezi částicemi a druhá maximální vzdálenou distribuci, jejichž kombinace by měla být schopná rozpoznávat jety s polynomiálním zrychlením [23] ve srovnání s klasickými metodami, nicméně tato metoda vyžaduje aktuálně nedohledné QRAM architektury (tedy kvantovou ekvivalentu RAM=rapid access memory, tedy extra úložiště využívané hlavně k vyhledávání v úložišti hlavním s rychlým přístupem), které při aktuálním stavu šumových qubitů nebudou ani v blízké budoucnosti realizovatelné.

4.6 Kvantové generativní modely pro simulace

Mimo teoretických modelování a zpracovávání experimentálních dat, fyzika vysokých energií také silně využívá simulaci samotných dat. Simulují se jak surová data naměřená z detektorů v urychlovači, tak již zpracovaná vyšší data užívaná k analýze. Aktuální odhady tvrdí, že více než 50% výpočetního výkonu v LHC je využíváno k simulaci dat. [44] Tyto simulace nám dávají náhled do možných očekávaných výsledků, což umožňuje lépe určovat, které experimenty realizovat a jak rozpoznat anomálie či chyby ve skutečných datech.
Dlouhodobě byla tato data simulována pomocí různých typů Monte Carlo modelů (v angličtině MC event generators). Nově jsou zkoumány i možnosti využití strojového učení ke generování specifičtějších simulací. Kvantové (či hybridní kvantově-klasické) generativní modely jako Kvantová generativní protichůdná síť (Quantum generative adversarial network v angličtině či QAE) [39] slibují nejen algebraické zrychlení, které jsme již probírali u ostatních problémů využívajících velká data, tak ale i přesnější výsledky díky zahrnutí komplexních složek kvantových dějů probíhajících při srážkových událostech (více v kapitole 6). [27] Alternativně Bornův stroj na kvantovém obvodě (Quantum circuit Born machine v angličtině) využívá generování událostí ne pomocí metody s klasickou ekvivalentou, ale pomocí Bornova rozhodovacího pravidla (Bornovým strojem rozumíme druh architektury umělé inteligence, která je kompatibilní s kvantovými obvody). [21]

5 Aktuální stav kvantových počítačů a jejich využití v částicové fyzice

Nyní, když vidíme možná využití technologií kvantových počítačů pro potřeby částicové fyziky, nastává zásadní otázka: Je to skutečně dosažitelné, za jak dlouho můžeme využití těchto technologií očekávat a jaká je situace dnes?
V této kapitole si povíme právě o tom. Nejprve popíšeme různé způsoby realizace qubitů, jejich výhody, nevýhody a vlastnosti. Poté prozkoumáme stav takzvané kvantové nadvlády a co můžeme od budoucnosti očekávat. Nakonec představíme aktuálně největší, nejrychlejší a nejkomplexnější fungující kvantové počítače, jejich parametry, schopnosti a plány do budoucna.

5.1 Typy qubitů

Každý kvantový systém se dvěma možnými kvantovymi stavy lze využít jako qubit (v případě více stavů qudit). Některé z nich jsou ale jednodušší na využití než jiné. Každá realizace qubitu/quditu by měla být schopná [29]:

(a) **robustně reprezentovat kvantovou informaci** - tedy jednoduše nabývat obou možných stavů, být schopná udržet superponovaný stav a neztrácet informaci kvůli interferenci s vlivy zvenčí.

(b) **provádět universální rodinu unitárních operací** - tedy musí na ní být možno provádět operace, jimiž generovaný prostor pokrývá všechny možné dosažitelné stavy - ať už pomocí universální sady kvantových bran či pomocí jednoho komplexního operátoru.

(c) **provádět dvou-qubitové operace** - tedy jde o více než o velice malou samostatnou paměťovou jednotku.

(d) **připravit koherentní počáteční stav, vynulovat ho a restartovat ho** - nelze-li definitivně určit počáteční stav, na který kvantový algoritmus působí, pak jeho měření nemá smysl, a nelze-li ho poté přepsat, aby bylo možné algortimus zopakovat, pak také nemá smysl.

(e) **jednoznačně změřit finální stav** - chceme-li z naměřených stavů určit distribuci popisující finální kvantový stav, tak si musíme být jistí jednoznačností naměřených jednotlivých stavů.

Podívejme se tedy na aktuálně zkoumané a vyráběné druhy qubitů:

5.1.1 Supravodivé qubity

Supravodivé qubity využívají jako qubit elektrony, ovšem nevyužívají elektrony jednotlivé, ale jejich takzvané Cooperovy páry (viz dále) a jakožto jednotku informace měří jejich energii [26].
Cooperovy páry jsou dvojice vázaných elektronů vznikající v supravodivých materiálech s celkovou energií nižší než Fermiho energie (nejnižší možná energetická hladina, které může volný elektron v materiálu dosáhnout). Tyto páry mohou vznikat pouze v supravodivém prostředí, jelikož energie této vazby je velmi nízká (10^{-3}eV) a termální efekty v normálním vodiči by ji snadno rozbily [90].
Dva různé stavy jsou rozlišeny pomocí Josephsonovy spojky (Josephson junction), tedy tenké nesupravodivé vrstvy materiálu mezi dvěma supravodivými celky. Cooperovy páry se mohou skrz Josephsonovu spojku protunelovat, pokud mají dostatečně velkou energii. Stavy $|0\rangle$ a $|1\rangle$ Cooperových párů tedy jsou, zda se pár jednoznačně vyskytuje v jednom, či druhém supravodivém celku. Jejich energie a jejich měření jsou realizovány pomocí mikrovlnné manipulace a resonance [61].
Supravodivé qubity jsou aktuálně nejdominantnější typ qubitu díky jejich ekvivalenci s klasickými obvody a hlavně díky tomu, že narozdíl od ostatních (dále zmíněných) typů qubitů nevyužívají samotný kvantový objekt, ale vlastně typ kvantového oscilátoru, což vede k dobré škálovatelnosti a potenciálně komplexnějším informatickým strukturám, jaké známe u klasických počítačů [53].

5.1.2 Fotonové qubity

Fotony jsou jedny z nejstarších zrealizovaných způsobů implementování skutečných qubitů [55]. Díky jejich povaze je možné je využít hned několik způsoby [36]:
Fotony jakožto nehmotná částice se spinem 1 má dvě možné polarizace, ty lze tedy využít jako dva různé stavy.
Zároveň jakožto propagátor prostorového šíření elektromagnetického pole v prostoru má foton také orbitální moment hybnosti jakožto složku své celkové hybnosti. Ta sice může nabývat "libovolných" hodnot, ovšem pouze ve dvou směrech - pravotočivém a levotočivém, což lze využít jako dva požadované stavy pro qubit.
Asi nejjednodušší způsob, jak využít fotonu jako qubitu je jeho samotná přítomnost, tedy nechat nepozorovaný foton se lámat na rozcestích a změřit až na jejich konci, zda dorazil, či ne.
Na podobném principu funguje i poslední způsob, takzvaný interferometrický kvantový fotonický počítač, kde namísto toho, zda foton dorazil, zjišťujeme, kdy dorazil. Měříme tedy na stejném místě, ale různé cesty, kterými se foton může vydat, jsou různě dlouhé a foton tedy podle toho dorazí v různou dobu. Různé časy tedy tvoří naše různé stavy - ne nutně jen dva, tedy možnost konstrukce quditů. Jako logický qubit se v tomto případě nepoužívá samotný foton, ale provázané stavy více fotonů dohromady.
Hlavní výhodou fotonových qubitů je jejich odolnost vůči dekoherenci [65]. Fotony mezi sebou totiž příliš neinteragují, nestojí-li jim v cestě hmotná překážka. Díky této nízké poruchovosti je také překvapivě jednoduché (ve srovnání s ostatními metodami) škálovat na nich postavený kvantový

počítač do vyšších paměťových rozměrů. Zásadní problém je ale rychlost, s níž jejich kvantové algoritmy operují (doslova rychlost světla) a je tedy náročné produkovat přesné současné počáteční stavy pro vyšší počty qubitů, přesné měření finální stavů v opakujících se běžích algoritmu. Nejzásadnější nevýhodou je ale skladování kvantové informace z fotonových qubitů (není snadné nepozorovaný foton někde dlouhodobě udržet), ale na řešení těchto problémů se aktuálně pracuje [97]. Dalším problémem je zavedení dvou a více qubitových operací mezi fotony, jelikož samotné fotony mezi sebou neinteragují.

5.1.3 Spinové qubity

Využití elektronu jakožto qubitu je poměrně intuitivní. Jakožto částice se spinem 1/2 má přesně dva stavy, se kterými lze poměrně dobře manipulovat pomocí elektromagnetického pole. Zároveň je výrazně snazší je uchovávat než dříve zmíněné fotony [96]. Zásadní problém ovšem je škálování již jen na více než jeden elektron. Při interakci elektronů v dvou- a více-qubitových branách snadno dochází k dekoherenci a pohybující se elektrony generují elektromagnetické pole, které může působit na ostatní elektrony a narušovat tak průběh algoritmu [77]. Samotné elektrony tedy nejsou využívány jako základ kompletních kvantových počítačů, jsou ale někdy využívány jako přenosné qubity pro přenos informace mezi vzdálenými qubity jiné povahy [81].
Povýšení tohoto konceptu je využití kvantových teček jakožto qubitů, což je výrazně více využívaná metoda realizace. Kvantová tečka je výraz pro polovodičový nanokrystal. Tato technologie je podobně stará jako myšlenka kvantových počítačů a dnes se využívá v inženýrství pevných materiálů, v některých druzích scintilačních detektorů, nebo dokonce i v medicíně (kde se využívají ke zdravotně nezávadnému zabarvování rakovinných buněk). V principu funguje jako klasický polovodič - excitovatelný materiál, kde elektrony mohou přejít z valenční vrstvy do vodivé vrstvy, čímž změní energetickou hladinu i vodivé vlastnosti. Zásadní vlastnost kvantové tečky je ale ta, že díky její velikosti dochází k přechodu pouze jednoho elektronu (vzniku jen jednoho elektron-dírového páru) [10]. Kvantové tečky mají zároveň až překvapivě koherentní kvantové stavy a dobře pracují v provázání s dalšími tečkami, což z nich dělá výborné kandidáty pro qubitovou realizaci [54]. Jejich využití je atraktivní nejen díky jednoduchosti s pracováním s nimi, jakožto krystaly, ale díky podobnosti s využitím polovodičů v klasické informatice [22], [88].

5.1.4 Iontové qubity

Využití atomových jader (tedy iontů) jakožto informačních nosičů pomocí jejich spinu naráží na stejné překážky jako elektronové qubity ovšem se dvěma zásadními rozdíly. Zaprvé atomové jádro může dosahovat více než jen dvou spinových stavů (spin jádra může a bývá vyšší než 1/2, pro licho-lichá jádra až 8, některá jádra mohou tedy dosahovat až $2 \cdot 8 + 1 = 17$ různých spinových stavů) a jejich manipulace elektromagnetickým polem je výrazně náročnější než u elektronu. Jako alternativa se proto využívá namísto elektromagnetického pole manipulace laserovým pulsy, které je schopné excitovat jádra do různých spinových stavů s lepší přesností než magnetická manipulace jednoduchých spinových qubitů [79]. To sice komplikuje konstrukci kvantových bran pro iontové qubity, ale snižuje to chybovost díky vzájemným nevyžádaným interakcím [47]. Udržování elektronů zbavených jader je na druhou stranu výrazně komplikovanější než samotných elektronů [76]. Jde tedy o technické zlepšení elektronových qubitů, ale náklady na škálování jsou stále nepřiměřené získanému výkonu [46], a nevyužívá se tedy tolik jako následující metoda.
Výrazně využívanější metodou jsou ultrastudené iontové pasti, kde se jako informační jednotka využívá energetická hladina zachycených iontů s jedním valenčním elektronem (tedy alkalinové, nebo alkalinům podobné ionty) [16]. Využívají se díky své jednoduché stavbě, kde jsou obě možné

hladiny dobře manipulovatelné (pomocí mikrovlnných a optických efektů či vzájemné interakce mezi ionty [52] - jsou stejně nabité a není tedy nutné bát se ztráty elektronu a s ním kvantové informace) a změřitelné. Ignorujeme-li náročnost udržení ultrastudeného prostředí (což je trochu jináý druh problematiky, než který trápí realizaci qubitů) [15], tak je i poměrně jednoduché skladovat takto informaci a připravit jednoznačný počáteční stav. Mnohé dnešní kvantové počítače fungují právě na tomto principu a z klasických qubitových realizací se tato těší největšímu úspěchu.

5.1.5 Qubity pomocí defektů na mřížce

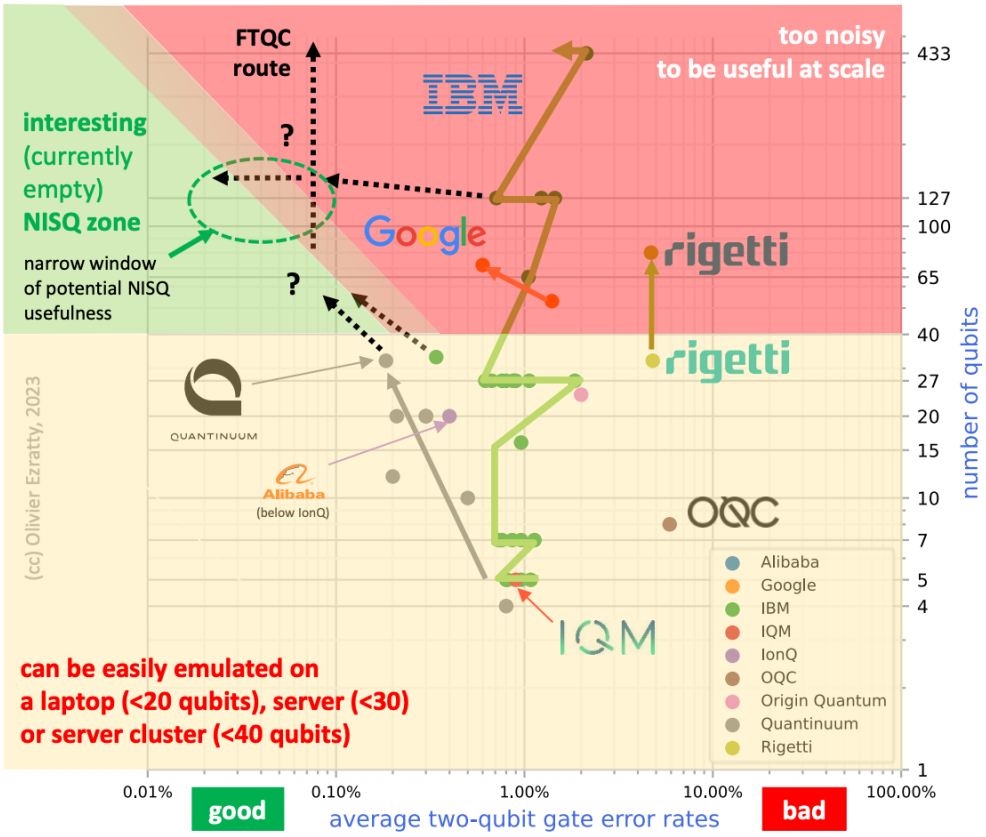
Qubity realizované pomocí defektů na mřížce jsou další specifickou variací využití elektronového spinu jako qubitu. Do jisté stabilní pevné krystalické mřížky jsou umístěny "kazové" atomy, které mají o 1 valenční elektron více, či méně (v případě méně elektronů se zachází s elektronovou dírou namísto elektronu samotného). Tyto elektrony jsou poté samotnou strukturou udržovány v neměřeném stabilním stavu a je možné s nimi manipulovat pomocí silných magnetických polí [37]. Alternativně je-li mřížka světelně propustná, pak mohou být elektrony/elektronové díry manipulovány i optickými metodami [40]. Nejpoužívanějším příkladem této realizace jsou NV-centra (Nitrogen-vacancy centres) v diamantu. Ty jsou výhodné, protože splňují výše zmíněné podmínky pro vhodnou mřížku (velmi pevná, stabilní a světlo propouštějící struktura), ale navíc narozdíl od supravodivých qubitů mohou pracovat i při pokojových teplotách (ke zvýšení koherentních časů, a tedy vyšší komplexitu kvantových obvodů je vhodnější také pracovat při ultranízkých teplotách, ale možnost fungování za běžných podmínek je slibná pro budoucí využití) [62].

5.1.6 Neutrální atomy

Qubity realizované pomocí neutrálních atomů využívají nábojově neutrální stabilní atomy s možným metastabilním excitovaným stavem, kde základní stav reprezentuje $|0\rangle$ a čistý excitovaný stav reprezentuje $|1\rangle$ [82]. Kvantové brány na nich jsou realizovany pomocí laserových pulsů či mikrovlnného záření podobně jako supravodivé qubity. Jedna z jejich hlavních výhod je velký koherentní čas (až v řádu desítek milisekund) [75]. Také mají poměrně slibnou škálovatelnost, jelikož je lze napojovat pomocí optických pastí.

5.2 Kvantová nadvláda respektive výhoda a budoucnost kvantové informatiky

Kvantové počítače v posledních 10 letech zažívají nejrychlejší růst od vzniku jejich samotného konceptu v 80. letech hlavně díky zájmu ze strany komerčních subjektů (Google, IBM, IQM, Rigetti a další). Kvantově počítačový průmysl zvolna přesouvá své priority z vynalézání nových způsobů realizace qubitů, logických bran a psaní hypotetických algoritmů, čekajících na to, až je hardwarové divize doženou, k realizaci skutečných kvantových počítačů s desítkami, či dokonce stovkami qubitů (viz Obr. 10), úspěšným demonstracím existujících kvantových algoritmů na malých škálách (viz 3.5), prodlužování kvantových koherencí existujících qubitových typů a hlavně snižování chybovosti.



Obr. 10: Diagram vývoje kvantových počítačů a jednotlivých "zón" v nichž se nacházejí převzatý z [31]. Na vodorovné ose průměrná chybovost dvouqubitových bran v daném počítači a na svislé ose počet qubitů, se kterými počítač operuje.

Na již výše zmíněném Obr. 10 vidíme 3 "zóny" do nichž se aktuálně realizované kvantové počítače dělí: [31]

- **Žlutá "slabá" zóna**
  Kvantové počítače ve žluté zóně se pohybují v nízkých počtech qubitů a jsou nahraditelné emulací na klasickém počítači/servru/klastru servrů. Kromě prototypních kroků pro výkonnější počítače slouží také k demonstraci již formulovaných kvantových algoritmů na nízké škále (například rozkladu čísla 15 na prvočísla pomocí Shorova algoritmu).

- **Červená "chybová" zóna**
  V červené zóně se nacházejí kvantové počítače s takovým množstvím qubitů, že jejich procesy nelze emulovat na aktuálně existujících klasických počítačích. Jejich průměrná chybovost je ale příliš vysoká pro praktické využití, a jimi produkované výsledky jsou tedy přinejmenším neprůkazné. Vliv chybovosti jednotlivé dvouqubitové operace na celkový výsledek s počtem qubitů totiž přirozeně roste exponenciálně (proto se tato zóna s postupem svislé osy ve vodorovném směru rozšiřuje).

- **Zelená "ideální" zóna**
  Zelená, také ideální zóna se pohybuje ve stejných řádech qubitového objemu jako zóna červená, ale s chybovostí dostatečně nízkou pro praktické využití. Do této zóny se při psaní této bakalářské práce žádný kvantový počítač zatím nedostal. Tento přesun je ale hlavním

cílem všech vývojových skupin (akademických či soukromých) zabývajících se kvantovými počítači.

- **Šedá (nezobrazená) zóna**
  Existují systémy pracující s mnoha stovkami, či dokonce tisíci qubity. Ty ovšem v diagramu, jelikož se v praxi nejedná a celistvé fungující kvantové počítače, nejsou. Vzdálenosti a koherenční časy takovýchto systémů vedou k nemožnosti propojení či operace qubitů z opačných částí systému. Z pragmatického pohledu se tedy jedná spíše o několik menších kvantových počítačů poskládaných dohromady do jednoho kusu hardwaru. (Tyto jednotlivé kusy se obvykle pohybují ve žluté, v lepším případě v červené zóně).

Cílem je tedy přesunout se ze žluté a červené zóny do té zelené, kde bude možné využít výhod kvantové informatiky zmíněných v této bakalářské práci.
Mnoho ze zmíněných komerčních firem tvrdí, že toto vede k takzvané kvantové nadvládě. Než budeme diskutovat, zda to je možné, nebo ne, zadefinujme, co kvantová nadvláda, respektive výhoda znamená: [41]

- **Totální kvantová nadvláda**
  Totální kvantová nadvláda spočívá zaprvé v praktické ukázce toho, že řešení jakéhokoliv informatického problému pomocí kvantového počítání je super-polynomiálně (rychleji než polynomicky například exponenciálně) rychlejší, než klasické řešení, a zadruhé v matematickém důkazu univerzálnosti tohoto tvrzení.

- **Slabá kvantová nadvláda**
  Slabá kvantová nadvláda spočívá v demonstraci, že jakýkoliv informatický problém lze lépe řešit pomocí kvantového počítače než pomocí klasického digitálního, kde lépe je poměrně široký pojem, zahrnující mimo jiné rychlejší, levnější, paměťově méně náročné nebo efektivnější.

- **Kvantová výhoda**
  Kvantová výhoda spočívá v řešení hodnotných problémů kvantovým počítačem lépe (pro definici lépe viz Slabá kvantová nadvláda) než pomocí klasického počítače, kde výhodným problémem rozumíme problém, který řeší problém s praktickým využitím. Jde tedy spíše o komerční pojem.

- **Silná kvantová výhoda**
  Silná kvantová výhoda je rozdílná od běžné kvantové výhody pouze důkazem super-polynomiálního zrychlení kvantového řešení hodnotných problémů (obdobně jako při srovnání totální a slabé kvantové nadvládě).

Hodnotný problém je tedy jak zmíněno spíše komerční pojem, ale lze ho vnímat jako lepší řešení problémů, které lze lépe řešit, což je poněkud definice kruhem, ale umožňuje nám zahrnout využití zmíněná v této bakalářské práci a stále rozděluje nadvláda a výhodu jako univerzální a specifické zlepšení. Důkazy zmmíněné v totální nadvládě a silné výhodě totiž existují pouze pro některé specifické problémy a to ani ne všechny, pro které se výhoda předpokládá. Celkově aktuálně přijímaná teorie a hypotézy poukazují na slabou, popřípadě silnou kvantovou výhodu v momentu dosažení zelené zóny a kvantová nadvláda je spíše kvalitním reklamním tahem než realitou blízké budoucnosti. [32]

5.3 Nejlepší aktuální kvantové počítače

Jak bylo zmíněno výše, určení nejlepšího akutálního kvantového počítače není problematické jen kvůli rychlému vývoji v tomto typu technologií, ale hlavně proto, že lze těžko kvalifikovat jejich kvalitu (kombinace chybovosti, qubitového objemu a kvantové koherence). V této podkapitole zmíníme nejlepší kvantové počítače v jednotlivých kritériích a pár příkladů s lepšími kombinacemi několika z nich:

- **Barium-137 fidelity SPAM**
  Jak zmíněno v předchozí podkapitole chybovost kvantových počítačů doposud nebyla hlavní priorita při konstrukci kvantových počítačů. Nejméně chybovým kvantově informatickým systémem tedy nepřekvapivě není kompletní počítač, ale systém přípravy a čtení kvantového systému (v angličtině state preparation and measurement - tedy SPAM) zkonstruovaný Fangzhao Alex Anem a jeho týmem v roce 2022, kde dosáhli chybovosti 99.9904% . [4]

- **D-wave kvantový žíhač**
  Kvantový počítač s nejvyšším počtem qubitů není univerzální kvantový počítač, ale kvantový žíhač od firmy D-wave s 5000 qubity. Mimo to, že se nejedná o univerzální počítač (o kvantovém žíhání níže), tak se jedná o počítač z výše zmíněné šedé zóny, tedy má sice tisíce qubitů, ale ty nejsou schopné mezi sebou komunikovat každý s každým a dal by se spíše klasifikovat jako shluk několika kvantových počítačů dohromady na jednom hardwaru. Kvantový žíhač (v angličtině quantum annealer) je počítač určující základní (energeticky nejnižší) stav hamiltoniánu, tedy konkrétně běžícího algoritmu (viz podkapitola 4.1). [93]

- **Koherenční čas bosonového experimentu**
  Obdobně jako u chybovosti kvantový systém s nejdelším koherenčním časem není kompletní kvantový počítač. Čínský tým vedený profesorem Kihwan Kimem zkonstruoval dvojici Ytterbiových qubitů s koherenčním časem přes 10 minut (o řád vyšší než pro běžné kvantové počítače). [89]

- **IBM Osprey machine**
  Aktuálně asi nejlepší kvantový počítač co se týče všech 3 kritérií je Osprey machine od firmy IBM. Aktuálně pracuje s 433 supravodivými qubity. Jeho chybovost nelze snadno ohodnotit, jelikož je stále zlepšována, ale akutálně se pohybuje kolem 99%. [6] Startupová firmy Atom computing tvrdí, že jejich nejnovější kvantový počítač překoná IBM Osprey machine a dokonce přesáhne hranici 1000 qubitů. Zatím se ale jedná jen o startup a ne kompletní kvantový počítač. [19]

6 Interference v částicových sprškách pomocí kvantového algoritmu

V této kapitole představíme konkrétní ukázku problému fyziky srážek při vysokých energiích řešitelnou kvantovým algoritmem a to kvantovou interferenci v částicových sprškách. Kvantovou interferencí rozumíme destruktivní, respektive konstruktivní skládání amplitud pravděpodobností výsledných pozorovatelných. Dochází k ní, pokud v systému (ať už fyzikálním procesu nebo kvantovém algoritmu) existuje více průběžných mezistavů, vedoucích na stejný výsledek měřené pozorovatelné. Tyto efekty nejsou pozorovatelné v klasických MCMC simulacích, které provádějí jen samostatné pseudonáhodné kroky, ve kterých k interakci pravděpodobností nedochází, a ani docházet nemůže.

Následně prakticky ukážeme implementaci algoritmu, který tento problém řeší a nasimulujeme na "ideálním" kvantovém počítači (tedy simulací qubitů na klasickém zařízení bez uvažování chybovosti systému). Simulaci srovnáme pro případy s povolenou, nepovolenou a potlačenou kvantovou interferencí.
Podobné toy modely jsou užitečné k budování komplexnějších a komplexnějších modelů. S postupným přidáváním interakcí a konkretizování členů v modelu (například specifikováním bosonu jakožto gluonu a umožněním interakcí mezi nimi) se zaprvé zvyšuje efekt interference, kterou může kvantový počítač spouštějící takovýto model určit, tak zadruhé prudce narůstá komplexita, kterou je snazší (pomalejší vzrůst nároků jak časových, tak paměťových) realizovat na kvantovém počítači než na klasickém.

6.1 Problematika zvolená pro vlastní algoritmus

Námi zvolený problém, který jsme zopakovali podle [69] a dále poupravili, se zabývá toy modelem emisí bosonů fermionem se dvěma možnými vůněmi. To je fyzikálně zajímavé, jelikož při dosazení gluonu jako konkrétního bosonu, se pak jedná o zjednodušený model procesu z kvantové chromodynamiky. Pro jednoduchost kvantově datového ukládání uvažujeme pouze skalární boson, ne vektorový. Celý systém je popsán lagrangiánem:

$$\mathcal{L} = \overline{f_1}(i\not{\partial} + m_1)f_1 + \overline{f_2}(i\not{\partial} + m_2)f_2 + (\partial_\mu\phi)^2 + g_1\overline{f_1}f_1\phi + g_2\overline{f_2}f_2\phi + g_{12}[\overline{f_1}f_2 + \overline{f_2}f_1]\phi, \quad (6)$$

kde první 3 členy popisují kinematické složky pro náš toy model téměř irelevantní, členy $g_i\overline{f_i}f_i\phi$ popisují emisi bosonu fermionem pro i-tou vůni a rozpad bosonu na fermionový-antifermionový pár a poslední člen popisuje proces, při kterém je také vyzářen boson a navíc fermion změní vůni. Tento model jsme zvolili, jelikož pro nenulovou vazbovou konstantu g_{12} může obsahovat kvantové interferenční jevy způsobené superpozicí různých výsledných stavů. Výsledným stavem rozumíme počet bosonů na konci algoritmu. Těch lze dosáhnout přes různé mezičástice a kombinace těchto stavů produkuje požadovanou itnerfenci. To je pro nás zajímavé, jelikož tato interference může být simulována pomocí kvantového počítače, který se superpozicí různých stavů operuje vždy, zatímco na klasickém počítači by nebyla pozorována vůbec, nebo by ji bylo potřeba uměle domodelovat.
Pro formulaci jednotlivých interakcí využijeme rozdělovacích funkcí $P_{i\to i\phi}(\theta) = g_i^2\hat{P}_f$, kde θ je úhel(získaný z kinematiky), při kterém rozdělení probíhá, a $\hat{P}_f(\theta)$ je kvantový operátor popisující energetickou závislost rozdělení (pro účely této demonstrace si vystačíme s $\hat{P}_f(\theta) = \log(\theta)$). Pro fermiony máme v našem modelu 6 možnosti: $P_{i\to i\phi}(\theta)$ $i \in \{1;2\}$, které určují výše popsané interakce, a $P_{\phi\to ii}$, která by určovala chování pro rozpad bosonu na 2 fermiony. Tu ale pro zjednodušení implementace kvantového obvodu nebudeme v této bakalářské práci uvažovat.
Nakonec je potřeba vzít v úvahu i případy, kdy k rozdělení nedojde (vzhledem k tomu, že všechny popisované děje jsou pravděpodobnostní). Pravděpodobnost nerozdělení lze vyjádřit pomocí takzvaného Sudakova faktoru následovně:

$$\Delta_{i,k}(\theta_1,\theta_2) = \exp\left[-g_i^2\int_{\theta_1}^{\theta_2}\mathrm{d}\theta'\hat{P}_k(\theta')\right], \quad (7)$$

kde $i \in \{1;2\}$ je vůně fermionu a $k \in \{f,\phi\}$ určuje typ interakce. Vyjadřuje nám tedy pravděpodobnost nerozdělení fermionu i interakcí k mezi úhly θ_1 a θ_2. Aby byla zachována unitární podmínka kvantového operátoru, tak musí Sudakův faktor a rozdělovací funkce splňovat rovnici

$$\Delta_{i,k}(\theta_1,\theta_2) + g_i^2\int_{\theta_1}^{\theta_2}\mathrm{d}\theta\hat{P}_k(\theta)\,\Delta_{i,k}(\theta_1,\theta) = 1. \quad (8)$$

6.2 Implementace kvantového algoritmu

Nyní popíšeme, jak byl implementován algoritmus na řešení tohoto toy modelu.
Využijeme k tomu 2 kvantové registry. Jeden bosonový, s N qubity kde N se rovná počtu kroků, do kterého budeme toy model simulovat (v našem případě 16) a fermionový, ve kterém nám při neuvažování dělení se bosonů stačí 1 qubit. Pro implementaci na obvodu je vhodnější rozdělovací operátor

$$P_{i\to j\phi}(\theta) = G_{ij}\hat{P}(\theta) = \begin{pmatrix} g_1 & g_{12} \\ g_{12} & g_2 \end{pmatrix} \hat{P}(\theta) \tag{9}$$

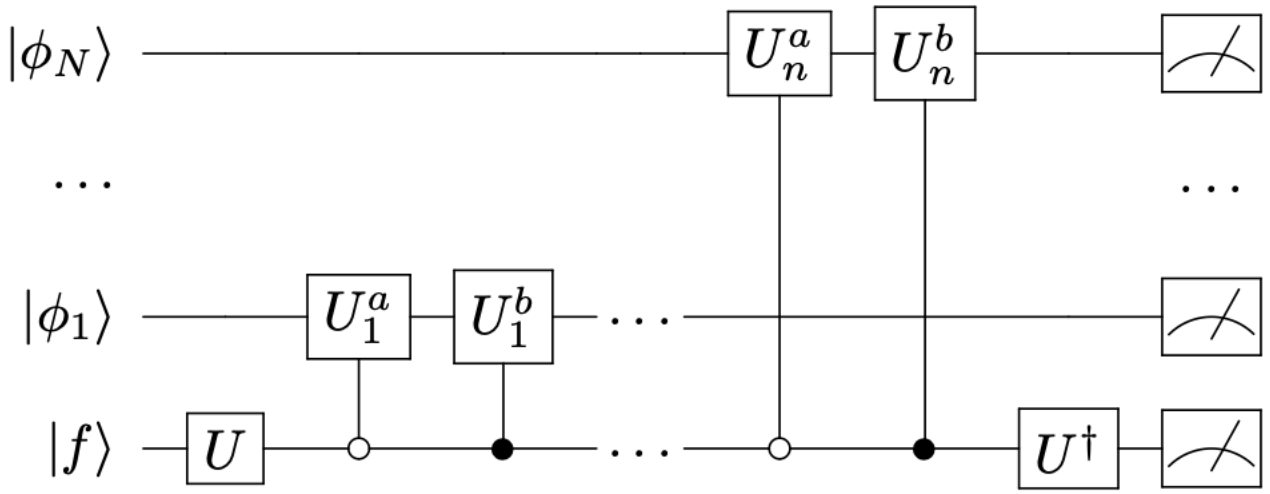
přeznačit do báze v níž je diagonalizovatelný, kterou označíme jako a a b, tedy

$$g_a = \frac{g_1 + g_2 - g'}{2} \qquad\qquad g_b = \frac{g_1 + g_2 + g'}{2}, \tag{10}$$

kde

$$g' = \mathrm{sign}(g_2 - g_1)\sqrt{(g_1 - g_2)^2 + 4g_{12}^2}. \tag{11}$$

V ní jsou všechny námi uvažované interakce složené do 2 složek operátoru a vůní 1 či 2 budeme rozumět superpozice čistých stavů a a b, které v našem algoritmu odpovídají $|0\rangle$ a $|1\rangle$. Samotný obvod je zobrazen na Obr. 11 a dále popíšeme jeho jednotlivé složky a jejich funkci.



Obr. 11: Schéma použitého kvantového algoritmu pro N kroků pomocí univerzálních rotačních bran U. Jednoqubitovou bránu U nazveme inicializační a bránu s operátorem k ní inverzním nazveme finalizační. Každý krok simulace je proveden pomocí 2 kontrolovaných bran U_k^a a U_k^b (dále jen $U_k^{a/b}$), kde k značí, o který krok se jedná, a a/b, o kterou superpozici interakcí se jedná. Nakonec změříme. Převzato z [69]

Inicializační bránu jsme realizovali pomocí maticí definované rotační jednoqubitové brány s maticí

$$\hat{U} = \begin{pmatrix} \sqrt{1-u^2} & u \\ -u & \sqrt{1-u^2} \end{pmatrix}, \tag{12}$$

kde

$$u = \sqrt{\frac{g_1 - g_2 + g'}{2g'}} \tag{13}$$

(g' stejné jako u definice g_a a g_b) a bránu finalizační identicky pouze s invertovanou maticí.
Brána inicializační nám fermionový qubit uvede buďto do superpozice odpovídající fermionové vůni 1, ze stavu $|0\rangle$ (ve kterém celý obvod začíná), je-li interference vypnuta (tedy g_{12} je zvoleno jako 0), nebo do superpozice obou vůní, je-li interference zapnuta (tedy g_{12} zvoleno nenulově), a brána finalizační, jakožto jeho inverze, fermionový qubit do stavu $|0\rangle$ opět vrátí.
Dvojici bran $U_k^{a/b}$ je také možno popsat pomocí matice:

$$U_k^{a/b} = \begin{pmatrix} \sqrt{\Delta_{a/b}(\theta_k)} & \sqrt{1-\Delta_{a/b}(\theta_k)} \\ \sqrt{1-\Delta_{a/b}(\theta_k)} & \sqrt{\Delta_{a/b}(\theta_k)} \end{pmatrix} \tag{14}$$

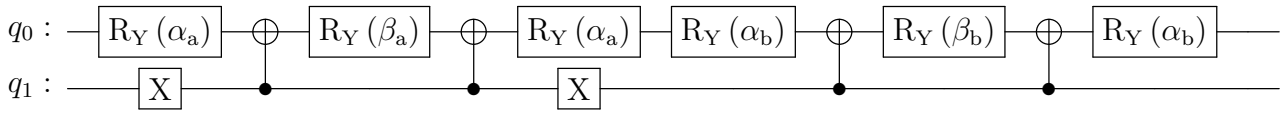
(kde $\Delta_{a/b}(\theta_k)$ je stejná jako ve výrazu (19)), ale implementovat ji budeme pomocí elementárních bran, jelikož se jedná jen o rotaci $\Delta_{a/b}(\theta_k)$ a obecnou kontrolovanou rotační bránu lze vyjádřit jakožto:

$$U = \exp(i\psi)AXBXC \qquad\qquad ABC = I, \tag{15}$$

kde jako A, B, C rozumíme

$$A = R_Y(\alpha) \qquad\qquad B = R_Y(\beta) \qquad\qquad C = R_Y(\alpha), \tag{16}$$

X značí CNOT bránu a $\exp(i\psi)$ je obecný operátor modifikující komplexní složku, který pro naše účely stačí zvolit jako $\psi = 0$. Rozdílem mezi U_k^a a U_k^b mimo změnu ve využitých úhlech bude navíc i dvojice X bran u U_k^a, která slouží k rozlišení g_a a g_b interakcí (jelikož jedna působí v případě čistých stavů na $|0\rangle$ a druhá na $|1\rangle$). Dostáváme tedy Obr. 12 jakožto opakovaný podobvod.



Obr. 12: Implementace dvojice bran $U_k^{a/b}$ pomocí elementárních bran. Úhly $\alpha_a, \alpha_b, \beta_a$ a β_b závisí na k (viz dále).

Zbývá určit, co znamenají a jakou hodnotu mají úhly $\alpha_{a/b}$ a $\beta_{a/b}$. Ty jsou určeny z druhé podmínky (15) jakožto následující násobky úhlu $\theta_{a/b}$

$$\alpha_{a/b} = \frac{\theta_{a/b}}{4} \qquad\qquad \beta_{a/b} = -\frac{\theta_{a/b}}{2}, \tag{17}$$

kde $\theta_{a/b}$ nám do definic obecné rotace přináší zpět toy model, jelikož odpovídá simplifikovanému Sudakovu faktoru:

$$\theta_{a/b} = 2 \cdot \arccos\left(\sqrt{\Delta_{a/b}(\theta_k)}\right) \tag{18}$$

$$\Delta_{a/b}(\theta_k) = \exp\left[-\Delta\theta P_{a/b}(\theta_k)\right], \tag{19}$$

kde

$$P_{a/b}(\theta_k) = P_{a/b\to a/b\phi}(\theta_k) = g_{a/b}^2 \hat{P}_f(\theta_k) \tag{20}$$

a

$$\Delta\theta = \theta_k - \theta_{k+1}. \tag{21}$$

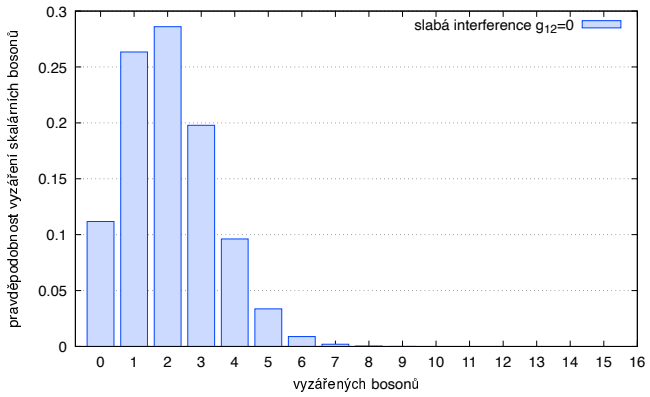
To nám díky podmínce (8) a unitárnosti kvantových bran plně popisuje využívané interakce.
K rozdělení jednotlivých stavů (tedy aby například q_7 a q_12 nepopisovaly stejný boson) je potřeba zvolit fyzikální škálu, která je mezi sebou rozliší. V našem případě využijeme úhel vyzáření bosonu θ_k, o kterých z kinematiky víme, že musí splňovat:

$$\theta_0 \gg \theta_1 \gg \cdots \gg \theta_n \qquad \wedge \qquad \forall i \in n \quad \theta_i > 0. \tag{22}$$

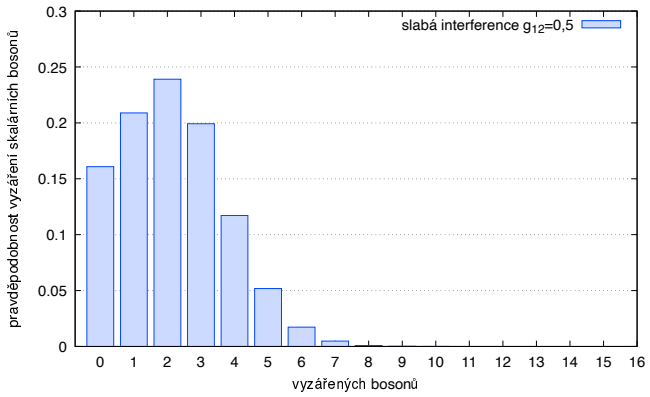
Konkrétně zvolíme rovnoměrné rozdělení na logaritmické škále od $\ln(\theta_0)$=0 po $\ln(\theta_{15})$ = -7. Konec této škály ($\theta_{15} = e^{-7}$) je zvolen podle kolineární hranice $e = 0,001$ (převzato z [69]), pod níž již nelze jednotlivé emise rozlišit.

6.3 Výsledky na simulovaném kvantovém počítači

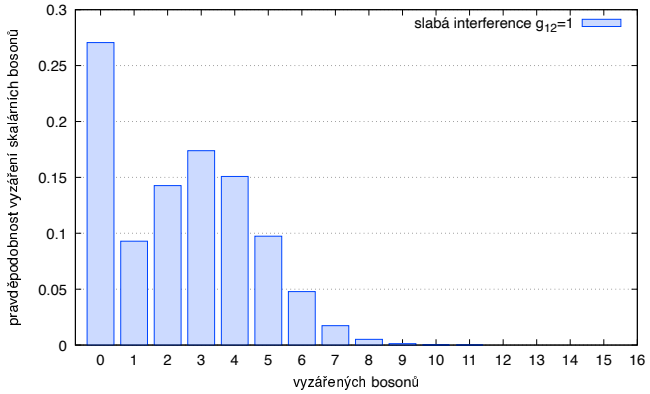
Algoritmus popsaný v předchozí podkapitole jsme implementovali a spustili v Pythonovém prostředí Qiskit [64], které na klasickém zařízení simuluje kvantový systém. Implementovali jsme ho pro 16 qubitů ve 3 verzích ve všech s volbou parametrů $g_1 = 2$ a $g_2 = 1$, které se od sebe lišily volbou parametru g_{12}, jelikož právě ten za pomoci míchání vůní vnáší do toy modelu interferenci.
V první verzi byla tedy interference plně povolena ($g_{12} = 1$), v druhé plně zakázána ($g_{12} = 0$) a v třetí byla interference povolena, ale oslabena ($g_{12} = 0,5$). Třetí hodnota g_{12} byla zvolena, aby se výsledek co nejvíce lišil od plně povolené i plně zakázané verze. Všechny 3 byly spuštěny se 100000 opakováními a jejich výsledky jsou zobrazeny na Obr. 13.



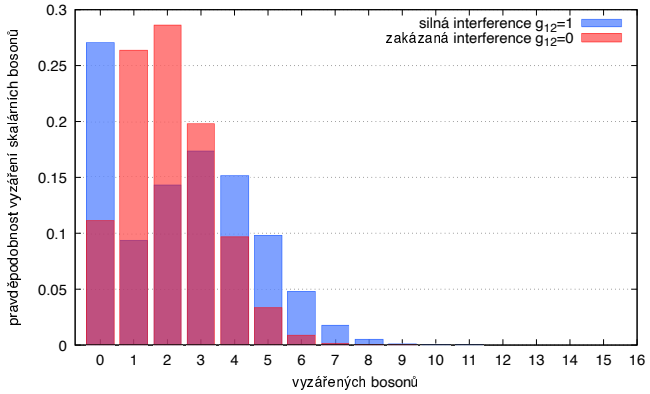
(a) Interference zakázána



(b) Interference povolena slabší



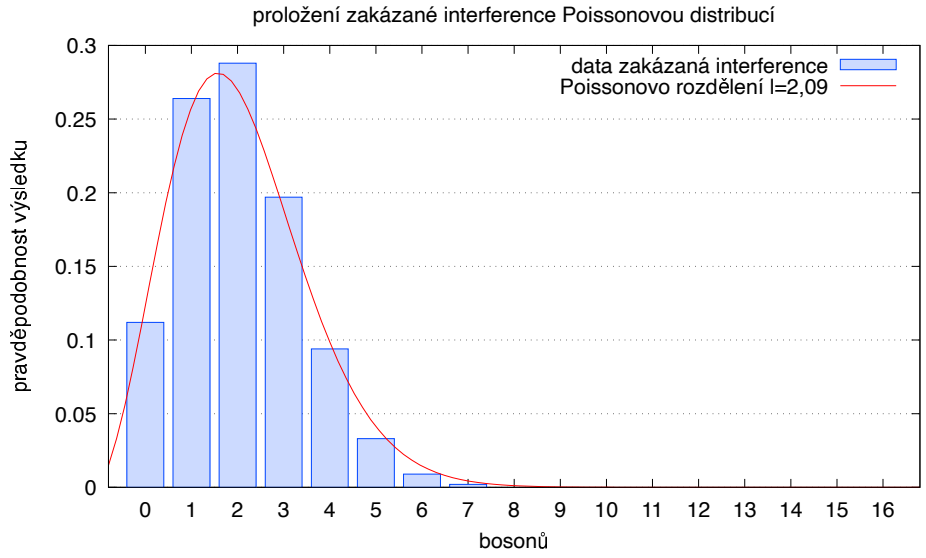
(c) Interference povolena silnější



(d) Srovnání s a bez interference

Obr. 13: Histogramy simulace průběhu algoritmu na ideálním kvantovém počítači pro 16 qubitů se 100000 opakováními pro 3 různé případy. Ve všech 3 případech byly zvoleny $g_1 = 2$ a $g_2 = 1$. g_{12} jakožto zdroj interference byla zvolena (a) nulová, (b) rovna 0,5 a (c) 1. Nakonec na (d) jsou silná a nulová interference vykresleny ve stejném histogramu, kde modrá je silná interakce, červená je nulová interakce a fialový je překryv mezi nimi.

V případě 13a nedochází k míchání vůní, jde jen o skládání stejné pravděpodobnosti samu na sebe a dle očekávání tedy odpovídá Poissonovou rozdělení (viz Obr 14) s l blízkým g_1.
V případě 13c pozorujeme těžké posílení případu, kdy není vyzářen žádný boson, zatímco vrchol navazujícího rozdělení se zvýšil o jeden vyzářený boson. Oba tyto jevy mohou být vysvětleny právě jako projevy hledané interference, kde se pravděpodobnosti vyzáření bosonů v různých větvích dle vzájemné fáze skládají (a posouvají tak vrchol), či naopak vyruší (a posilují tak nulový výsledek). Nakonec v případě 13b je viditelný mezikrok, mezi předchozími dvěma stavy. Na něm je již patrná destruktivní interference, jelikož typicky vede na nulový výsledek, zatímco posunutí vrcholu rozdělení ještě není zřejmě pozorovatelné, jelikož konstruktivní interference dělí svůj vliv mezi mnoho výsledků.



Obr. 14: Proložení výsledku se zakázanou interferencí Poissonovou distribucí

Mimo rozložení stavů je z výsledků možné vyčíst ještě i jednu pozorovatelnou a to střední hodnotu vyzářených bosonů. Ta odpovídá 2,559 pro 13c, 2,050 pro 13a a 2,157 pro 13b. Interference tedy zcela jistě pro tento toy model zvyšuje množství vyzářených bosonů i přes posílení pravděpodobnosti, že nebude vyzářen ani jeden, a to i pro interferenci oslabenou.

7 Závěr

Vysvětlili jsme tedy, že kvantové počítače jsou informaticky využité kvantové systémy, které využívají neobvyklých kvalit kvantového stavu jako je superpozice a kvantové provázání k pravděpodobnostním výpočtům. Nabízí teoreticky algebraické zrychlení pro mnoho problémů komerčních i akademických, alternativní způsob řešení komplexních problémů pomocí kvantových simulátorů a kvantových žíhačů a posílení jiných čerstvě se rozvíjejících se technologií, jako je strojové učení.
Ukázali jsme, že konkrétně pro fyziku srážek při vysokých energiích představují způsob, jak zlehčit a urychlit některé ze zdrojově nejnáročnějších úkonů prováděných v tomto oboru, od teoretického zkoumání kvantových systémů pomocí modelování na kvantovém systému, vyhledávání anomálií v datasetech, které mohou buďto upozornit na chybu v systému či měření, nebo na nový naměřený fyzikální fenomén, snazší konstrukci pozorovatelných ze surových dat, až po přesnější simulování dějů vybíraných k budoucímu výzkumu.
Nakonec jsme na simulovaném ideálním kvantovém počítači implementovali konkrétní algoritmus pro toy model vyzařování skalárních bosonů fermionem s měnící se vůní v kvantové chromodynamice, na kterém jsme demonstrovali pozorování kvantové interference umožněné skládáním pravděpodobností různých stavů v superpozici na pravděpodobnostním počítači, jako je kvantový počítač.

Literatura

[1] Steve Abel, Andrew Blance, and Michael Spannowsky. Quantum optimization of complex systems with a quantum annealer. *Physical Review A*, 106(4):042607, 2022.

[2] Sonia Lopez Alarcon, Cory Merkel, Martin Hoffnagle, Sabrina Ly, and Alejandro Pozas-Kerstjens. Accelerating the training of single layer binary neural networks using the hhl quantum algorithm. In *2022 IEEE 40th International Conference on Computer Design (ICCD)*, pages 427–433. IEEE, 2022.

[3] Ehud Altman, Kenneth R. Brown, Giuseppe Carleo, Lincoln D. Carr, Eugene Demler, Cheng Chin, Brian DeMarco, Sophia E. Economou, Mark A. Eriksson, Kai-Mei C. Fu, Markus Greiner, Kaden R.A. Hazzard, Randall G. Hulet, Alicia J. Kollár, Benjamin L. Lev, Mikhail D. Lukin, Ruichao Ma, Xiao Mi, Shashank Misra, Christopher Monroe, Kater Murch, Zaira Nazario, Kang-Kuen Ni, Andrew C. Potter, Pedram Roushan, Mark Saffman, Monika Schleier-Smith, Irfan Siddiqi, Raymond Simmonds, Meenakshi Singh, I.B. Spielman, Kristan Temme, David S. Weiss, Jelena Vučković, Vladan Vuletić, Jun Ye, and Martin Zwierlein. Quantum simulators: Architectures and opportunities. *PRX Quantum*, 2(1), February 2021.

[4] Fangzhao Alex An, Anthony Ransford, Andrew Schaffer, Lucas R Sletten, John Gaebler, James Hostetter, and Grahame Vittorini. High fidelity state preparation and measurement of ion hyperfine qubits with i> 1 2. *Physical Review Letters*, 129(13):130501, 2022.

[5] Kazumaro Aoki, Yuji Kida, Takeshi Shimoyama, and Hiroki Ueda. Gnfs factoring statistics of rsa-100, 110,..., 150. *Cryptology ePrint Archive*, 2004.

[6] Anjum Ashraaf, Hasham Sarwar, and Ghulam Murtaza. Efficient quantum full adder using ibm quantum experience.

[7] Taiwo Oladipupo Ayodele. Machine learning overview. *New Advances in Machine Learning*, 2:9–18, 2010.

[8] Frédéric Bapst, Wahid Bhimji, Paolo Calafiura, Heather Gray, Wim Lavrijsen, Lucy Linder, and Alex Smith. A pattern recognition algorithm for quantum annealers. *Computing and Software for Big Science*, 4:1–7, 2020.

[9] Jacob Biamonte, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe, and Seth Lloyd. Quantum machine learning. *Nature*, 549(7671):195–202, 2017.

[10] Dieter Bimberg, Marius Grundmann, and Nikolai N Ledentsov. *Quantum dot heterostructures*. John Wiley & Sons, 1999.

[11] Mausam Bindhani, Bikash Behera, and Prasanta Panigrahi. Hand written digit recognition using quantum support vector machine. 05 2020.

[12] Markward Britsch, Nikolai Gagunashvili, and Michael Schmelling. Classifying extremely imbalanced data sets. *arXiv preprint arXiv:1011.6224*, 2010.

[13] Stephen Brooks. Markov chain monte carlo method and its application. *Journal of the royal statistical society: series D (the Statistician)*, 47(1):69–100, 1998.

[14] R Brower, S Chandrasekharan, S Riederer, and U-J Wiese. D-theory: field quantization by dimensional reduction of discrete variables. *Nuclear physics B*, 693(1-3):149–175, 2004.

[15] Kenneth R Brown, John Chiaverini, Jeremy M Sage, and Hartmut Häffner. Materials challenges for trapped-ion quantum computers. *Nature Reviews Materials*, 6(10):892–905, 2021.

[16] Colin D Bruzewicz, John Chiaverini, Robert McConnell, and Jeremy M Sage. Trapped-ion quantum computing: Progress and challenges. *Applied Physics Reviews*, 6(2), 2019.

[17] Isaac L Chuang, Lieven MK Vandersypen, Xinlan Zhou, Debbie W Leung, and Seth Lloyd. Experimental realization of a quantum algorithm. *Nature*, 393(6681):143–146, 1998.

[18] David Collins, K. W. Kim, and W. C. Holton. Deutsch-jozsa algorithm as a test of quantum computation. *Phys. Rev. A*, 58:R1633–R1636, Sep 1998.

[19] Atom computing. Quantum startup atom computing first to exceed 1,000 qubits, Oct 2023.

[20] Murilo G Coutinho. *Dynamic simulations of multibody systems*. Springer Science & Business Media, 2001.

[21] Brian Coyle, Daniel Mills, Vincent Danos, and Elham Kashefi. The born supremacy: quantum advantage and training of an ising born machine. *npj Quantum Information*, 6(1):60, 2020.

[22] Dimitrie Culcer, Łukasz Cywiński, Qiuzi Li, Xuedong Hu, and S. Das Sarma. Quantum dot spin qubits in silicon: Multivalley physics. *Phys. Rev. B*, 82:155312, Oct 2010.

[23] Jorge J Martínez de Lejarza, Leandro Cieri, and Germán Rodrigo. Quantum clustering and jet reconstruction at the lhc. *Physical Review D*, 106(3):036021, 2022.

[24] Andrea Delgado, Kathleen E Hamilton, Jean-Roch Vlimant, Duarte Magano, Yasser Omar, Pedrame Bargassa, Anthony Francis, Alessio Gianelle, Lorenzo Sestini, Donatella Lucchesi, et al. Quantum computing for data analysis in high energy physics. *arXiv preprint arXiv:2203.08805*, 2022.

[25] Jianyang Deng and Yijia Lin. The benefits and challenges of chatgpt: An overview. *Frontiers in Computing and Intelligent Systems*, 2(2):81–83, Jan. 2023.

[26] Michel H Devoret, Andreas Wallraff, and John M Martinis. Superconducting qubits: A short review. *arXiv preprint cond-mat/0411174*, 2004.

[27] Alberto Di Meglio, Karl Jansen, Ivano Tavernelli, Constantia Alexandrou, Srinivasan Arunachalam, Christian W Bauer, Kerstin Borras, Stefano Carrazza, Arianna Crippa, Vincent Croft, et al. Quantum computing for high-energy physics: state of the art and challenges. summary of the qc4hep working group. *arXiv preprint arXiv:2307.03236*, 2023.

[28] Yongcheng Ding, Javier Gonzalez-Conde, Lucas Lamata, José D. Martín-Guerrero, Enrique Lizaso, Samuel Mugel, Xi Chen, Román Orús, Enrique Solano, and Mikel Sanz. Toward prediction of financial crashes with a d-wave quantum annealer. *Entropy*, 25(2):323, February 2023.

[29] B Douçot and LB Ioffe. Physical implementation of protected qubits. *Reports on Progress in Physics*, 75(7):072001, 2012.

[30] Vladimir L. Ermakov and B. M. Fung. Experimental realization of a continuous version of the grover algorithm. *Phys. Rev. A*, 66:042310, Oct 2002.

[31] Olivier Ezratty. Where are we heading with nisq? *arXiv preprint arXiv:2305.09518*, 2023.

[32] Olivier Ezratty. Where are we heading with nisq? *arXiv preprint arXiv:2305.09518*, 2023.

[33] Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. A quantum approximate optimization algorithm. *arXiv preprint arXiv:1411.4028*, 2014.

[34] Dmitry A Fedorov, Bo Peng, Niranjan Govind, and Yuri Alexeev. Vqe method: a short survey and recent developments. *Materials Theory*, 6(1):1–21, 2022.

[35] Richard P Feynman. Simulating physics with computers. *International journal of theoretical physics*, 21(6/7):467–488, 1982.

[36] Fulvio Flamini, Nicolo Spagnolo, and Fabio Sciarrino. Photonic quantum information processing: a review. *Reports on Progress in Physics*, 82(1):016001, 2018.

[37] Bernhard Grotz, Moritz V Hauf, Markus Dankerl, Boris Naydenov, Sébastien Pezzagna, Jan Meijer, Fedor Jelezko, Jörg Wrachtrup, Martin Stutzmann, Friedemann Reinhard, et al. Charge state manipulation of qubits in diamond. *Nature communications*, 3(1):729, 2012.

[38] Gian Giacomo Guerreschi and Anne Y Matsuura. Qaoa for max-cut requires hundreds of qubits for quantum speed-up. *Scientific reports*, 9(1):6903, 2019.

[39] Zhao-Yu Han, Jun Wang, Heng Fan, Lei Wang, and Pan Zhang. Unsupervised generative modeling using matrix product states. *Physical Review X*, 8(3):031012, 2018.

[40] Joanne Harrison, MJ Sellars, and NB Manson. Optical spin polarisation of the nv centre in diamond. *Journal of luminescence*, 107(1-4):245–248, 2004.

[41] Aram W Harrow and Ashley Montanaro. Quantum computational supremacy. *Nature*, 549(7671):203–209, 2017.

[42] Vojtěch Havlíček, Antonio D Córcoles, Kristan Temme, Aram W Harrow, Abhinav Kandala, Jerry M Chow, and Jay M Gambetta. Supervised learning with quantum-enhanced feature spaces. *Nature*, 567(7747):209–212, 2019.

[43] Cornelius Hempel, Christine Maier, Jonathan Romero, Jarrod McClean, Thomas Monz, Heng Shen, Petar Jurcevic, Ben P. Lanyon, Peter Love, Ryan Babbush, Alán Aspuru-Guzik, Rainer Blatt, and Christian F. Roos. Quantum chemistry calculations on a trapped-ion quantum simulator. *Phys. Rev. X*, 8:031022, Jul 2018.

[44] HEP Software Foundation hsf-editorial-secretariat@ googlegroups. com, Johannes Albrecht, Antonio Augusto Alves, Guilherme Amadio, Giuseppe Andronico, Nguyen Anh-Ky, Laurent Aphecetche, John Apostolakis, Makoto Asai, Luca Atzori, et al. A roadmap for hep software and computing r&d for the 2020s. *Computing and software for big science*, 3:1–49, 2019.

[45] Matteo Ippoliti, Kostyantyn Kechedzhi, Roderich Moessner, S.L. Sondhi, and Vedika Khemani. Many-body physics in the nisq era: Quantum programming a discrete time crystal. *PRX Quantum*, 2:030346, Sep 2021.

[46] Alec Jenkins, Joanna W Lis, Aruku Senoo, William F McGrew, and Adam M Kaufman. Ytterbium nuclear-spin qubits in an optical tweezer array. *Physical Review X*, 12(2):021027, 2022.

[47] Liang Jiang, MV Gurudev Dutt, Emre Togan, Lily Childress, Paola Cappellaro, Jacob Mason Taylor, and Mikhail D Lukin. Coherence of an optically illuminated single nuclear spin qubit. *Physical Review Letters*, 100(7):073001, 2008.

[48] Richard Jozsa. Searching in grover's algorithm. *arXiv preprint quant-ph/9901021*, 1999.

[49] Xiangyang Ju, Daniel Murnane, Paolo Calafiura, Nicholas Choma, Sean Conlon, Steven Farrell, Yaoyuan Xu, Maria Spiropulu, Jean-Roch Vlimant, Adam Aurisano, et al. Performance of a geometric deep learning pipeline for hl-lhc particle tracking. *The European Physical Journal C*, 81:1–14, 2021.

[50] Abhinav Kandala, Antonio Mezzacapo, Kristan Temme, Maika Takita, Markus Brink, Jerry M Chow, and Jay M Gambetta. Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets. *nature*, 549(7671):242–246, 2017.

[51] V Kapoor. Data encryption and decryption using modified rsa cryptography based on multiple public keys and 'n'prime number. *International Journal of Scientific Research in network security and communication*, 1(2):35–38, 2013.

[52] V Kaushal, Bjoern Lekitsch, A Stahl, J Hilder, Daniel Pijn, C Schmiegelow, Alejandro Bermudez, M Müller, Ferdinand Schmidt-Kaler, and U Poschinger. Shuttling-based trapped-ion quantum information processing. *AVS Quantum Science*, 2(1), 2020.

[53] Morten Kjaergaard, Mollie E Schwartz, Jochen Braumüller, Philip Krantz, Joel I-J Wang, Simon Gustavsson, and William D Oliver. Superconducting qubits: Current state of play. *Annual Review of Condensed Matter Physics*, 11:369–395, 2020.

[54] Christoph Kloeffel and Daniel Loss. Prospects for spin-based quantum computing in quantum dots. *Annu. Rev. Condens. Matter Phys.*, 4(1):51–81, 2013.

[55] Emanuel Knill, Raymond Laflamme, and Gerald J Milburn. A scheme for efficient quantum computation with linear optics. *nature*, 409(6816):46–52, 2001.

[56] John Kogut and Leonard Susskind. Hamiltonian formulation of wilson's lattice gauge theories. *Physical Review D*, 11(2):395, 1975.

[57] John B Kogut. An introduction to lattice gauge theory and spin systems. *Reviews of Modern Physics*, 51(4):659, 1979.

[58] Jonas Köhler, Leon Klein, and Frank Noé. Equivariant flows: sampling configurations for multi-body systems with symmetric energies. *arXiv preprint arXiv:1910.00753*, 2019.

[59] Yaroslav Koshka and Mark A Novotny. Comparison of d-wave quantum annealing and classical simulated annealing for local minima determination. *IEEE Journal on Selected Areas in Information Theory*, 1(2):515–525, 2020.

[60] Arjen K Lenstra, Hendrik W Lenstra Jr, Mark S Manasse, and John M Pollard. The number field sieve. In *Proceedings of the twenty-second annual ACM symposium on Theory of computing*, pages 564–572, 1990.

[61] M Levi, Frank C Hoppensteadt, and WL Miranker. Dynamics of the josephson junction. *Quarterly of Applied Mathematics*, 36(2):167–198, 1978.

[62] Tobias Lühmann, Roger John, Ralf Wunderlich, Jan Meijer, and Sébastien Pezzagna. Coulomb-driven single defect engineering for scalable qubits and spin sensors in diamond. *Nature communications*, 10(1):4956, 2019.

[63] Esteban A Martinez, Christine A Muschik, Philipp Schindler, Daniel Nigg, Alexander Erhard, Markus Heyl, Philipp Hauke, Marcello Dalmonte, Thomas Monz, Peter Zoller, et al. Real-time dynamics of lattice gauge theories with a few-qubit quantum computer. *Nature*, 534(7608):516–519, 2016.

[64] David C McKay, Thomas Alexander, Luciano Bello, Michael J Biercuk, Lev Bishop, Jiayin Chen, Jerry M Chow, Antonio D Córcoles, Daniel Egger, Stefan Filipp, et al. Qiskit backend specifications for openqasm and openpulse experiments. *arXiv preprint arXiv:1809.03452*, 2018.

[65] GJ Milburn. Photons as qubits. *Physica Scripta*, 2009(T137):014003, 2009.

[66] Eric Mjolsness and Dennis DeCoste. Machine learning for science: state of the art and future prospects. *science*, 293(5537):2051–2055, 2001.

[67] Thomas Monz, Daniel Nigg, Esteban A Martinez, Matthias F Brandl, Philipp Schindler, Richard Rines, Shannon X Wang, Isaac L Chuang, and Rainer Blatt. Realization of a scalable shor algorithm. *Science*, 351(6277):1068–1070, 2016.

[68] Hector Jose Morrell Jr, Anika Zaman, and Hiu Yung Wong. Step-by-step hhl algorithm walkthrough to enhance the understanding of critical quantum computing concepts. *arXiv preprint arXiv:2108.09004*, 2021.

[69] Benjamin Nachman, Davide Provasoli, Wibe A De Jong, and Christian W Bauer. Quantum algorithm for high energy physics simulations. *Physical review letters*, 126(6):062001, 2021.

[70] Koji Nagata, Tadao Nakamura, and Ahmed Farouk. Quantum cryptography based on the deutsch-jozsa algorithm. *International Journal of Theoretical Physics*, 56:2887–2897, 2017.

[71] Hien M Nguyen, Eric W Cooper, and Katsuari Kamei. Borderline over-sampling for imbalanced data classification. *International Journal of Knowledge Engineering and Soft Data Paradigms*, 3(1):4–21, 2011.

[72] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[73] Román Orús, Samuel Mugel, and Enrique Lizaso. Quantum computing for finance: Overview and prospects. *Reviews in Physics*, 4:100028, 2019.

[74] Benjamin Perez-Garcia, Raul I Hernandez-Aranda, Andrew Forbes, and Thomas Konrad. The first iteration of grover's algorithm using classical light with orbital angular momentum. *Journal of Modern Optics*, 65(16):1942–1948, 2018.

[75] CJ Picken, R Legaie, K McDonnell, and JD Pritchard. Entanglement of neutral-atom qubits with long ground-rydberg coherence times. *Quantum Science and Technology*, 4(1):015011, 2018.

[76] Jarryd J Pla, Fahd A Mohiyaddin, Kuan Y Tan, Juan P Dehollain, Rajib Rahman, Gerhard Klimeck, David N Jamieson, Andrew S Dzurak, and Andrea Morello. Coherent control of a single si 29 nuclear spin qubit. *Physical review letters*, 113(24):246801, 2014.

[77] Jarryd J Pla, Kuan Y Tan, Juan P Dehollain, Wee H Lim, John JL Morton, David N Jamieson, Andrew S Dzurak, and Andrea Morello. A single-atom electron spin qubit in silicon. *Nature*, 489(7417):541–545, 2012.

[78] F. Robicheaux and K. Niffenegger. Quantum simulations of a freely rotating ring of ultracold and identical bosonic ions. *Phys. Rev. A*, 91:063618, Jun 2015.

[79] Christian F Roos. Ion trap quantum gates with amplitude-modulated laser beams. *New Journal of Physics*, 10(1):013002, 2008.

[80] Eliott Rosenberg, Paul Ginsparg, and Peter L McMahon. Experimental error mitigation using linear rescaling for variational quantum eigensolving with up to 20 qubits. *Quantum Science and Technology*, 7(1):015024, 2022.

[81] Maximilian Russ and Guido Burkard. Three-electron spin qubits. *Journal of Physics: Condensed Matter*, 29(39):393001, 2017.

[82] Dominik Schrader, I Dotsenko, M Khudaverdyan, Y Miroshnychenko, A Rauschenbeutel, and D Meschede. Neutral atom quantum register. *Physical Review Letters*, 93(15):150501, 2004.

[83] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE Comput. Soc. Press, 1994.

[84] Reuben Tate, Majid Farhadi, Creston Herold, Greg Mohler, and Swati Gupta. Bridging classical and quantum with sdp initialized warm-starts for qaoa. *ACM Transactions on Quantum Computing*, 4(2):1–39, 2023.

[85] Jules Tilly, Hongxiang Chen, Shuxiang Cao, Dario Picozzi, Kanav Setia, Ying Li, Edward Grant, Leonard Wossnig, Ivan Rungger, George H. Booth, and Jonathan Tennyson. The variational quantum eigensolver: A review of methods and best practices. *Physics Reports*, 986:1–128, 2022. The Variational Quantum Eigensolver: a review of methods and best practices.

[86] Lieven MK Vandersypen, Matthias Steffen, Gregory Breyta, Costantino S Yannoni, Mark H Sherwood, and Isaac L Chuang. Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414(6866):883–887, 2001.

[87] Philip Walther and Anton Zeilinger. Experimental realization of a photonic bell-state analyzer. *Physical Review A*, 72(1):010302, 2005.

[88] Ke Wang, Hai-Ou Li, Ming Xiao, Gang Cao, and Guo-Ping Guo. Spin manipulation in semiconductor quantum dots qubit. *Chinese Physics B*, 27(9):090308, 2018.

[89] Ye Wang, Mark Um, Junhua Zhang, Shuoming An, Ming Lyu, Jing-Ning Zhang, L-M Duan, Dahyun Yum, and Kihwan Kim. Single-qubit quantum memory exceeding ten-minute coherence time. *Nature Photonics*, 11(10):646–650, 2017.

[90] Victor F Weisskopf. The formation of cooper pairs and the nature of superconducting currents. *Contemporary Physics*, 22(4):375–395, 1981.

[91] Frank Wilczek. Quantum time crystals. *Physical Review Letters*, 109(16), October 2012.

[92] Romina Yalovetzky, Pierre Minssen, Dylan Herman, and Marco Pistoia. Nisq-hhl: Portfolio optimization for near-term quantum hardware. *arXiv preprint arXiv:2110.15958*, 2021.

[93] Tristan Zaborniak and Rogério de Sousa. Benchmarking hamiltonian noise in the d-wave quantum annealer. *IEEE Transactions on Quantum Engineering*, 2:1–6, 2021.

[94] Meng Zhang, Lihua Dong, Yong Zeng, and Ning Cao. Improved circuit implementation of the hhl algorithm and its simulations on qiskit. *Scientific Reports*, 12(1):13287, 2022.

[95] Leo Zhou, Sheng-Tao Wang, Soonwon Choi, Hannes Pichler, and Mikhail D Lukin. Quantum approximate optimization algorithm: Performance, mechanism, and implementation on near-term devices. *Physical Review X*, 10(2):021067, 2020.

[96] Xianjing Zhou, Gerwin Koolstra, Xufeng Zhang, Ge Yang, Xu Han, Brennan Dizdar, Xinhao Li, Ralu Divan, Wei Guo, Kater W Murch, et al. Single electrons on solid neon as a solid-state qubit platform. *Nature*, 605(7908):46–50, 2022.

[97] Zong-Quan Zhou, Wei-Bin Lin, Ming Yang, Chuan-Feng Li, and Guang-Can Guo. Realization of reliable solid-state quantum memory for photonic polarization qubit. *Phys. Rev. Lett.*, 108:190505, May 2012.