Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Hálózati Rendszerek és Szolgáltatások Tanszék

Kvantumszámítógépes számítási modellek és architektúrák összehasonlítása

TDK dolgozat

Készítette:

Kirchhof Barna

Konzulens:

Dr.Bacsárdi László

2023

Tartalomjegyzék

Kivonat

Ahogy egyre több figyelmet kapnak a kvantumtechnológiák, úgy nő a kérdés súlya, hogy ki és hogyan lesz képes az első univerzális kvantumszámítógép megalkotására. Újabb és újabb megoldások és ötletek látnak napvilágot minden évben, illetve nagy a kutatás a lehetséges alkalmazások területén is. Egy kiforratlan területről beszélve, nem könnyű egy-egy megvalósítást jellemezni, és főleg nehéz feladat megmondani, hogy melyik a legjobb, vagy hogy melyik lesz a legeredményesebb. Éppen ezért fontos, hogy meg tudjuk állapítani két, különböző architektúráról, hogy milyen hasonlóságok/különbségek vannak közöttük, továbbá, hogy melyik, mely területeken bizonyul eredményesebbnek. Ebben a munkában ezt a kérdés igyekszünk néhány szempont alapján megközelíteni, mind elméleti mind a megvalósítás területén, különböző megvalósítások összehasonlításával (IBM Quantum Experience, Xanadu Borealis). Az IBM már régóta ismert arról, hogy sok kutatást végez ezen az új és izgalmas területen, így már születtek korábbi munkák[16] is amelyekben, különféle módszerek segítségével történt vizsgálat, amelynek az IBM-Q gépei is tárgyát képezték. A Borealis pedig egy 2022 nyarán publikált kvantumszámítógép, melyet a kanadai Xanadu cég fejleszt. Érdekes, hogy annak ellenére, hogy a két gép fizikai felépítése nagyban különbözik, mindkettőt elérhetővé tette az adott fejlesztő cég egy felhő alapú infrastruktúrán keresztül, így nem csak a labor keretein belül folyhatnak kísérletezések. A továbbiakban szó lesz először elméleti modellekről, majd az említett fizikai rendszerek kerülnek elemzés alá.

Abstract

The more attention quantum technologies get, the more serious becomes the question that who/how will be able to produce a universal and practically useful fault-tolerant quantum computer. Newer solutions and ideas are unfolding in each year, as well as various possible applications. However, in this developing area of research it is not easy to compare two different kinds of solutions, and it is even harder to tell which will turn out to be the more successful one in the long term. That is the reason why the ability to compare two model or architecture and find similarities/differences is quite important. In this work the previous question is addressed in the area of computational models as well as in the architectural level (IBM-Q, Xanadu Borealis). IBM is well known for their entrepreneur approach to quantum computing, so there has already been works to investigate some of the features of their architecture[16] previously. Borealis is a photonic based device, that was released in the summer of 2022 and was developed by the Canadian company Xanadu. It is quite exciting that despite the physical differences between the two, both devices were made open for public to access through the cloud, so that the experimenting is not limited to the research facilities inside where the devices are present. In the following we will focus on computational models first, then take a tour around the architectures of these machines.

1. fejezet

Számítási modellek

1.1. Bevezető

Kvantumszámítások során különféle kvantummechanikai tulajdonságokat használunk ki. Ekkor fontos a fizikai tulajdonságok ismerete, ugynakkor ezek elméleti, matematikai leírása is gyakran önállóan kerül elő. Továbbá érdekes lehet, hogy kvantum számítások esetében sokszor lehetséges az elméleti és fizikai szintek szétválasztása. Ezen a gondolatmeneten elindulva külön tárgyalhatjuk az elméleti modelleket, illetve a konkrét implementációkat. Ehhez hozzátartozik az is, hogy először egy absztrakt szinten felépíthetőek az egyes algoritmusok, amelyeket egy adott modellben magvalósítani akarunk, majd a fizikai implementáció során már a konkrét fizikai rétegben feleltethetjük meg az egyes részeket, illetve azok képességeit az egyes absztrakt szinten leírt műveleteknek. Így persze előfordulhat (és jelenleg jellemző is), hogy az elkészített elméleti számítási modellhez képest, fizikai megkötések miatt kompromisszumokat kell tennünk (jelenleg az elméleti modellek még jóval túlmutatnak a fizikai megvalósítások képességein).

A kvantummechanikában egy rendszer állapota leírható egy adott pillanatban, a rendszerhez tartozó hullámfüggvénnyel $|\psi(t_0)\rangle$. Ez egy komplex együtthatós függvény, amely valójában reprezentálható, egy Hilbert-tér (komplex vektor-tér skalárszorzattal, amely egy teljes metrikus tér) bázisvektorainak a lineáris kombinációjaként. A rendszer állapota felírható minden időpillanatban, a rendszerhez tartozó Schrödinger-egyenlet segítségével[1]:

$$i\hbar\frac{\partial|\psi(t)\rangle}{\partial t} = \hat{H}|\psi(t)\rangle \tag{1.1}$$

Ahol $\hat{H}$ a rendszer Hamilton-operátora, $\hat{H} = \frac{\hat{p}^2}{2m} + \hat{V}$.
Amennyiben a $\hat{H}$ operátor időfüggetlen egy szeparálható differenciálegyenletet kapunk, és tekinthetjük az időfüggetlen Schrödigner-egyenletet:

$$\hat{H}|\psi\rangle = E|\psi\rangle \tag{1.2}$$

Melynek a megoldásai lesznek a rendszerben az energia sajátértékek és sajátállapotok, melyek egy jó bázist adnak az általános megoldáshoz:

$$|\Psi\rangle = \sum_n c_n e^{-i\frac{E_n t}{\hbar}}|n\rangle \tag{1.3}$$

[1] Dirac-féle bra-ket jelölést alkalmazva

Mérés következtében a szuperpozíció összeomlik (beugrik a hullámfüggvény) valamely bázisállapotba[2]. Továbbá a mérés eredménye valamely sajátérték lesz, pontosabban azon érték amely ahhoz a sajátállapothoz tartozik, amelybe a hullámfüggvény beugrott. Annak a valószínűsége, hogy egy tetszőleges $|\psi\rangle$ kvantumállapotban n sajátértéket kapunk mérés következtében, meghatározható a Born-szabály segítségével:

- Diszkrét bázison nem degenerált esetben:

$$\mathbb{P}(|\psi\rangle \text{ mérése } n \text{ - t ad végeredményül}) = |\langle n|\psi\rangle|^2 \tag{1.4}$$

- Diszkrét bázison degenerált esetben:

$$\mathbb{P}(|\psi\rangle \text{ mérése } n \text{ - t ad végeredményül}) = \sum_k |\langle k|\psi\rangle|^2 \tag{1.5}$$

  ahol szummázunk minden olyan állapotra, amelyhez tartozó sajátérték n.

- Folytonos spektrum esetén[3]:

$$\mathbb{P}(|\psi\rangle \text{ mérése } n \pm dn \text{ - t ad végeredményül}) = |\langle n|\psi\rangle|^2 2dn \tag{1.6}$$

Illetve a mérés utáni állapotok:

- Diszkrét bázis, degeneráció nélkül:

$$|\psi\rangle \to \frac{\hat{M}_n|\psi\rangle}{\sqrt{\langle\psi|\hat{M}_n^\dagger \hat{M}_n|\psi\rangle}} \tag{1.7}$$

  ahol $\hat{M}_n$ egy mérési operátor az n értékhez és $|n\rangle$ állapothoz.

- Diszkrét bázis, degenerált esetben:

$$|\psi\rangle \to \frac{\sum_k \langle k|\psi\rangle |k\rangle}{\sqrt{\sum_k |\langle k|\psi\rangle|^2}} \tag{1.8}$$

- Folytonos esetben, definiálunk egy mérési operátort:

$$\hat{P}_n := \int_{n-dn}^{n+dn} dn' \left|n'\right\rangle \left\langle n'\right| \tag{1.9}$$

  a mérés utáni állapot:

$$|\psi\rangle \to \frac{\hat{P}_n|\psi\rangle}{\sqrt{|\langle n|\psi\rangle|^2 2dn}} \tag{1.10}$$

Továbbá a rendszer állapota jellemezhető, a rendszer $\hat{H}$-jával, amely magába foglalja a rendszer teljes energiáját, mind kinetikus, mind potenciális.

A $\hat{H}$ egy olyan hermitikus($\hat{H} = \hat{H}^\dagger$) operátor, amely leírja a rendszer időfejlődését, várható értéke pedig egy adott állapothoz tartozó energia (sajátértékei alkotják az energiaspektrumot):

$$E_{|\psi\rangle} = \langle\psi|\hat{H}|\psi\rangle \tag{1.11}$$

[2]Valamelyik azon bázisállapotba ugorhat amely bázison a mérést végezzük (ez a mérési operátortól függ).

[3]Nincsen éles mérés, egy "ablakban" mérünk.

Ezek alapján megmondható minden lehetséges állapothoz, hogy akkor milyen energiaszint tartozik a rendszerhez. Tehát ha manipulálni tudjuk a rendszerhez tartozó $\hat{H}$ - t, akkor amennyiben a rendszer energiáját mérjük, végezhetünk számításokat.

1.1.1. Dirac-féle bra-ket jelölés

Ez a jelölésrendszer a kvantummechanika általános leírására született, így lehetőséget nyújt kvantummechanikai rendszerek effektív leírására. A $|\psi\rangle$ "ket" pszí egy valamely kvantummechanikai rendszert leíró $\mathcal{H}$ Hilbert-térbeli állapot ($|\psi\rangle \in \mathcal{H}$). Vagyis a rendszer mindenkori állapota egy-egy $|\psi(t)\rangle$ állapottal reprezentálható. A $\langle\psi|$ "bra" az eredeti $\mathcal{H}$ Hilbert-tér duális terének egy eleme, amelyre $\langle\psi| = |\psi\rangle^\dagger$ teljesül, ahol a † a hermitikus adjungált műveletét jelzi.
A Hilbert-téren értelmezett skalárszorzatot $\langle\psi|\,\phi\rangle$ - ként jelöljük. Egy tetszőleges állapot felírható egy bázison, a $\mathcal{H}$ Hilbert-tér felett $|\psi\rangle = \sum_n c_n |n\rangle = \sum_n \langle n|\,\psi\rangle\,|n\rangle$ (például a kvantumos harmonikus oszcillátor bázisán így néz ki: $\sum_n^\infty \langle n|\,\psi\rangle\,|n\rangle$).

1.2. Kapu-alapú modell

A kapu-alapú modellben (vagy circuit-based model) a rendszer unitér időbeli fejlődését befolyásolva végzünk kvantumszámításokat. Az időfejlődés során a következő fázisokba lépünk. 1. inicializációs fázis, itt megfelelő mennyiségű kvantumbitet (angolul: *qubit*) felveszünk és alaphelyzetbe[4] állítjuk őket. 2. időfejlődés unitér operátorokon keresztül. 3. mérés, hibajavítás esetlegesen klasszikus információfeldolgozás[5]. Ezt a vázat annyival érdemes még kiegészíteni, hogy lehetséges, hogy vannak valamilyen bemeneti értékeink is (ezek lehetnek klasszikusak vagy kvantumosak is akár) és ezek módosíthatják az alaphelyzetet[6].
Ennek a modellnek meg van az az erőssége, hogy adható klasszikus analógia. Képzeljük el a klasszikus logikai kapukat, akkor ezekhez lehetne megfeleltetni a kvantumos esetben az egyes operátorokat. Ez a megfeleltetés nem szükségszerűen egy-az-egyhez történne, ugyanakkor teljesül, hogy mint klasszikus esetben egy-egy algoritmus megadható logikai kapuk szekvenciájaként, hasonlóan ebben a modellben is lehetséges az eljárások leírása egy megfelelő operátor sorozattal. Éppen emiatt ezt a megközelítést követve könnyebb a modell megértése a klasszikus képből is.

Ez a számítási modell megfelelő kapu készlettel univerzális számítási sémát kínál. Ilyen kapu készlet például, amely biztosít tetszőleges egy kvantumbit forgatást, továbbá műveletet kvantumbitek összefonódásának elérésére, általában $C\hat{N}OT$ (kontrollált not) kapu.

[4] Ez általában annyit jelen, hogy a $\{|0\rangle, |1\rangle\}$ számítási bázisban valamely bázisállapotba állítjuk a kvantumbiteket.

[5] Nem minden esetben egyszerű egy probléma megfogalmazása, olyan alakra, hogy könnyen kvantum algoritmussal legyen futtatható, továbbá az eredmények interpretálása sem triviális minden esetben, ezért lehet szükséges klasszikus információfeldolgozás, vagyis olyan műveletek amelyekhez már nem szükséges kvantumszámítás a feladat megoldásában nem elhanyagolható/praktikus lépések.

[6] Persze klasszikus bemenet esetében ezek megfeleltethetőek könnyen annak, hogy minden kvantumbitet $|0\rangle$ - ba vesszük fel és feltételesen végrehajtunk egy σ_x kaput azokon, amelyek esetében a bementen 1-es van.

A számításokat a $\{|0\rangle, |1\rangle\}$ bázison végezzük, a végeredményt ebben a bázisban mérjük. A számítások alapját képező kvantumbiteket ezen a bázison írjuk fel, bázisvektorok általános lineárkombinációjaként:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.12}$$

Ahol α és β komplex valószínűségi együtthatók, és $|\alpha|^2 + |\beta|^2 = 1$.

Tehát végső soron olyan kapu sorozatot kell felírni, amely implementálja $\hat{U}(t)$ unitér operátort. Valóban a számítások jellemezhetőek, mint egy nagy unitér operátor (általában több kvantumbitre ható), amely implementálja a keresett számítást. Ugyanakkor, összhangban az eddigi gondolatmenettel ennek az operátornak elemi operátorokra való bontása szükséges[7].

Sok kvantumkapu létezik, de belátható, hogy minden több kvantumbites (angolul: *multi-qubit*) kapu felbontható egy kvantumbites (angolul: *single-qubit*) kapuk és $C\hat{N}OT$ kapuk tenzorszorzatára. Továbbá az is megmutatható, hogy minden egyes kvantumkapu egzaktul felírható, mint $e^{i\phi}\hat{R}_z(\gamma)\hat{R}_x(\beta)\hat{R}_z(\alpha)$, ahol:

$$\hat{R}_z(\alpha) = \begin{bmatrix} e^{-i\frac{\alpha}{2}} & 0 \\ 0 & e^{i\frac{\alpha}{2}} \end{bmatrix}$$

$$\hat{R}_x(\phi) = \begin{bmatrix} \cos(\frac{\phi}{2}) & -i\sin(\frac{\phi}{2}) \\ -i\sin(\frac{\phi}{2}) & \cos(\frac{\phi}{2}) \end{bmatrix}$$

Vagyis mondható, hogy ezek a kapuk univerzális halmazt alkotnak. Ugyanakkor fontos még megemlíteni a Pauli kapukat, mert fontos szerepük van a mérések elvégzésekor:

$$\hat{\sigma}_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\hat{\sigma}_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$\hat{\sigma}_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Ezen kapuk által definiált bázisokra gyakran szükséges elvégezni projektív méréseket, amelyeknek nagy jelentősége van a számításokban, így fontosak, amikor egy kvantumszámítógépet szeretnénk jellemezni.

1.3. Mérés-alapú modell

Ebben a számítási modellben (angolul: Measurement-Based Quantum Computing: MBQC) a számítás nagyon más módon hajtódik végre, ha összehasonlítjuk a korábbi szakaszban leírt kapu-alapú modellel. Fontos, hogy míg a korábbiban lehetséges klasszikus analógia felállítása/említése, ebben az esetben nem fellelhető klasszikus számítási modell[8].

Egy eljárás/algoritmus implementálásának a menete a következő: 1. felveszünk egy *cluster* állapotot (ez lehet 2-dimenziós, vagy 3-dimenziós is hibajavítás céljából), 2. meghatározunk egy kvantumbit mérési sorozatot (itt definiálni kell az egyes bázisokat amelyekben a mérést végre szeretnénk hajtani). A végeredmény hasonlóan az utolsó mérésből

[7] Elemi operátorok alatt itt olyan "kvantumos" logikai kapukat értünk, amelyeket az adott rendszeren megvalósítani tudunk.

[8] Ez azt is jelenti, hogy egészen más gondolatmenettel kell megközelíteni a feladatokat.

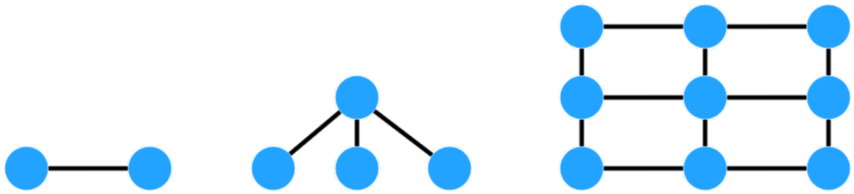
való kiolvasást jelenti majd, persze itt is lehetséges, hogy szükséges klasszikus utómunkálat, mint ahogyan arról korábban már volt szó. Továbbá erre a modellre is teljesül az univerzalitás[15], vagyis a kapu-alapú modellel ekvivalens abban az értelemben, hogy milyen feladatokat tudunk elvégezni (ezt legcélszerűbb úgy megmutatni, hogy belátjuk, hogy léteznek olyan eljárások a mérés-alapú modellben, amelyek megfeleltethetőek egy univerzális kapu halmaznak a kapu-alapú modellben).

Egy szokásos szemléletes kép a modellre, hogy a cluster állapot úgy viselkedik, mint egy papírlap és a mérésekkel tudunk rá "írni", illetve "kivágni" belőle.

Egy cluster állapot egy speciális gráf állapot[19], adott egy $G = (V, E)$ gráf, akkor $|g\rangle$ állapot:

$$|g\rangle = \prod_{(i,j)\in E} \hat{CZ}_{i,j} \bigotimes_{n\in V} |+\rangle_n \tag{1.13}$$

ahol $\hat{CZ}_{i,j}$ egy kontrollált $\hat{\sigma}_z$ az i és j indexű kvantumbitek között. Tehát az állapot valójában sok $|+\rangle$ - ba definiált kvantumbitből áll, amelyekre kontrollált $\hat{\sigma}_z$ operátorok hatnak, vagyis az ilyen párok között összefonódás jelensége áll fent[9].
Amennyiben a kvantumbiteket kék körökként (mint egy gráf csúcsai) és a $\hat{CZ}_{i,j}$ operátorokat az i, j közötti szakasszal ábrázoljuk, valóban egy közel konvencionálisan ábrázolt gráfot kapunk [19].



1.1. ábra. Cluster állapotok ábrázolása gráfokként.

Valójában cluster állapotok megjelennek a korábban tárgyalt modellben is, ilyen például egy Bell-állapot is (a 1.1 képen az első gráf, 2 csúccsal és egy éllel).

A számítások ezek után az egyes kvantumbitek megfelelő bázisban való megmérésével zajlanak[10]. A kvantummechanika működésének megfelelően tudjuk azonban, hogy a mérés következtében összeomlik a hullámfüggvény, és egy, a mért bázisbeli állapotot kapjuk eredményül (a mért obszervábilis sajátértékét). A mérések ezzel megváltoztatják a teljes cluster - t, illetve direkt hatásuk van azokra a kvantumbitekre, amelyek össze voltak fonódva a megmérttel.

A számítás során kialakul egy hálózatszerű struktúra (amely hasonlóan képzelhető el a korábban tárgyalt gráf állapotokhoz), amelyben az információ "áramlik". Az egyes műveletek tehát alakítják a gráfot, viszont a különböző bázisban való méréseknek eltérő hatása van, így válik lehetségessé univerzális számítás. Persze a cluster állapot definíciójából következik, hogy kezdetben (még az összefonódás előtt) a clusterbeli minden egyes kvantumbit $|+\rangle$ állapotban van, tehát a $\hat{\sigma}_x$ operátor sajátállapotában vagyis, ha nem ebben a bázisban mérjük (hanem például a számítási bázisban), akkor semmiképpen nem remélhetünk biztos eredményt[11]. Így a kvantummechanikai mérések következtében fellép

[9] A $\hat{CZ}_{i,j}$ operátor esetében nem szükséges kikötni, hogy melyik a control illetve a cél/vezérelt kvantumbit (angolul: *target qubit*), mert az operátor indifferens ezek felcserélésére.

[10] Ezek sokszor az XY sík valamely bázisán történnek.

[11] Sőt a $\hat{CZ}$ műveleteket követően már a $\hat{\sigma}_x$ sajátbázisán való méréstől sem remélhetünk biztos eredményt.

egy bizonytalanság, ami változtathat kvantumállapotunkon, így ahhoz hogy a megfelelő mederben haladjon tovább a számítás, néha szükségesek lesznek korrekciók. Ezeket nevezzük *byproduct* - oknak. Ezeknek a feladata annyi, hogy feltételesen hattassanank egy operátort a fennmaradó állapotra[12].

Mint már korábban volt róla szó, a méréseknek csak lokálisan van hatása, amiből annyi következik, hogy a "kellően messze" elhelyezkedő kvantumbitekre nincsenek hatással[13]. Ez a tulajdonság azonban egy nagyon fontos következménnyel jár, amely főleg a modellt implementáló kvantumszámítógépek esetében nagyon fontos és előnyös is. Névlegesen arról van szó, hogy a kérdéses tulajdonság miatt nem szükséges, hogy a teljes cluster állapot már a számítás megkezdésekor rendelkezésre álljon. Ez annyit jelent, hogy ahhoz, hogy elkezdődjön a végrehajtás elegendő, ha az első mérésekhez áll rendelkezésre teljes egészében minden érintett kvantumbit és kapcsolat (hiszen a mérés a többi potenciálisan még nem is létező kvantumbiteket nem befolyásolja).

Még egy érdekes lehetőség a modellel kapcsolatban, hogy lehetővé teszi a számítások végrehajtását titkosítással, az úgynevezett *Blind Quantum Computation* - t lehet megvalósítani a modell felett[20][1]. Ennek a lényege, hogy a kvantumszámítás 2 különböző helyen megy végbe (Alice és Bob között), amelyek kommunikálnak egymással, annak érdekében, hogy az adott számítás meg legyen valósítva[1]. Alapvetően Alice a kezdeményező, aki egy adott algoritmust/számítást akar elvégezni. Ő képes kvantumbitek előállítására, amelyek a $\{\frac{1}{\sqrt{2}}(|0\rangle + e^{-\theta}|1\rangle)\}$ kerülnek ki, ahol $\theta = 0, \frac{\pi}{4}, ..., \frac{7\pi}{4}$. Bob pedig képes kvantumbitek összefonódtatására, illetve a $\hat{O}(\phi) = \cos(\phi)\hat{\sigma}_x + \sin(\phi)\hat{\sigma}_y$ obszervábilist megmérni (gyakorlatilag az XY-síkbeli bázison). A protokollban továbbá fontos szerepe van Alice és Bob közötti kommunikációnak, amelynek mérete Alice elvégezni kívánt áramkörével lineárisan skálázódik. Ez amiatt van így, mert az eljárásban fontos Bobnak közölni Alice-el a mért eredményeket, illetve Alicenak Bobbal a méréshez szükséges szöget. A protokoll absztrakt módon a következő lépésekből áll[1]:

1. Alice létrehozza a számításhoz szükséges kvantum biteket
2. Alice elküldi a létrehozott kvantumbiteket Bobnak
3. Bob létrehoz egy *brickwork* cluster állapotot a kapott kvantumbiteken[14]
4. Ezek után Alice és Bob üzenetváltásba kerülnek, amelyet Alice kezd azzal, hogy az első méréshez szükséges szöget kiszámítja, majd elküldi Bobnak
5. Bob elvégzi a mérést és az eredményt delegálja Alicenak
6. Alice kezdi a folyamatot újra, de a kapott eredményt beleveszi a számításába
7. A számítás végén elméletben a végeredmény, amelyet Alice szeretett volna elérni, lehet csupán egy klasszikus eredmény, vagy egy kvantumos. Mindkét esetben Bob elküldi az eredményt Alicenak, legyen az az utolsó mérési eredmény vagy néhány kvantum bit.

[12]Ezen korrekciók feloldása megtehető úgy is, hogy az eredetileg eltervezett mérési bázisoktól eltérünk és adoptáljuk a bázisokat annak megfelelően, hogy mik voltak a korábbi mérések eredményei.

[13]Itt a messzeség alatt azt értjük, hogy hány összefonódásra, vagyis mint gráfbeli távolság.

[14]Brickwork cluster állapot([1]): $\mathcal{G}_{n\times m}$ egy olyan cluster állapot, ahol $n \times m$ darab kvantumbitet veszünk fel a $|+\rangle$ állapotban, egy $n \times m$ méertű rácson. Minden sorban a szomszédos kvantumbitek között $\hat{CZ}$ kaput hajtunk végre. Majd minden $j \equiv 3 \pmod 8$ és páratlan sorra, az (i, j) és (i+1, j), illetve az (i, j+2) és (i+1, j+2) qubetek között $\hat{CZ}$ operátort hajtunk végre. Ugyanígy járunk el (i, j)és (i+1, j), illetve (i, j+2) és (i+1, j+2) kvantumbitek között, ahol $j \equiv 7 \pmod 8$ és i páros.

A valóságban az eljárás akkor lehet praktikus, amennyiben az egyes kvantumbitek előállítása nem annyira nehéz folyamat, viszont az összefonódott állapot és a mérések megvalósítása komolyabb infrastruktúrát igényel (például labori körülmények a hűtéshez). Ugyanakkor Alice által végzett számítás privát Bobra nézve, így Bob hasonló szerepet tölt be, mint egy központi szerver, Alice pedig egy távoli felhasználó, aki egy számítási problémát szeretne megoldani.

1.4. Folytonos változójú modell és GKP kódolás

Az eddigiekben olyan számítási modellekről volt szó, amelyek esetében a számítás alapegységét kvantumbitek képezték, illetve a számítás egy diszkrét Hilbert-tér felett ment végbe. Ugyanakkor nem ez az egyetlen lehetőség[3][14], arra hogy feladatokat oldjunk meg. Egy másik modell a folytonos változójú modell[10][6][7], melynek kvantumfotonikában van nagy jelentősége. Ebben az esetben a számítás alapegységét nem kvantumbitek, hanem *qumode*-ok (kvantum módusok) adják. Folytonosságról abban az értelemben beszélünk, hogy a modellt alkotó operátorok spektruma folytonos, ellentétben a korábban megismert diszkrét képpel. Itt érdemes ki is térni pár releváns operátorra, mint a kvadratúra operátorok $(\hat{x}, \hat{p})$ és a módus operátorok $(\hat{a}, \hat{a}^\dagger)$[15]. Vagyis egy qumode - ot felírhatunk valamely operátor bázisán, például a $\hat{x}$ operátor sajátállapotainak a lineárkombinációjaként:

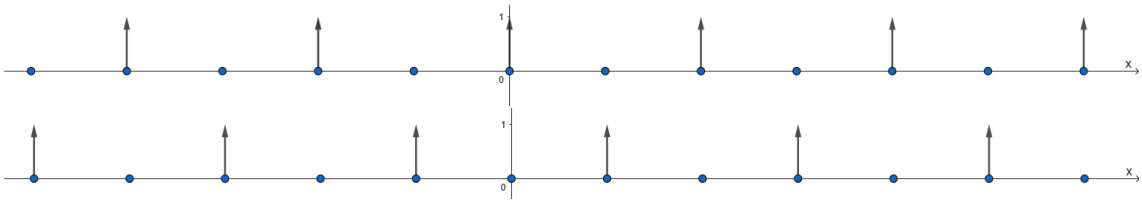
$$|\psi\rangle = \int dx\ \psi(x)\,|x\rangle \tag{1.14}$$

A modellben többféle mérésre is van lehetőség, homodyne, heterodyne és mérés a $\hat{n} = \hat{a}^\dagger\hat{a}$ sajátállapotainak a bázisán. A homodyne esetben a mérés az $\hat{x}$ operátor bázisa felett történik, vagyis a lehetséges értékek az $\hat{x}$ operátor sajátértékei, vagyis ezek egy kontinumot alkotnak és a méréssel az $\hat{x}$ valamely sajátállapotába ugrik be a hullámfüggvény. A heterodyne esetben egyszerre történik mérés az $\hat{x}$ és $\hat{p}$ operátorok bázisán, amely tekintve, hogy ezen operátorok kommutátora nem zérus, nem teljesülhet élesen. A harmadik mérési lehetőség lényegesen eltér a korábbiaktól, mert amíg eddig egy kontinuumból kaptunk értékeket, addig a $\hat{n}$ operátornak a spektruma diszkrét, pontosabban $\mathbb{N}$.

A számítási modell megfeleltethető a korábban tárgyalt diszkrét változós modelleknek, valójában több lehetőség is van arra, hogy egy végtelen dimenziós Hilbert-teret egy 2 dimenziósra képezzünk (abban az esetben ha egy kvantumbitet szeretnénk kódolni). Egy remek megoldást kínálhat a GKP kódolás, amely nem csak a leképezést, de hibajavítást is nyújthat. A GKP kódolás lényege, hogy folytonos változóba kódoljunk kvantumbiteket, pontosabban, hogy egy d dimenzionális logikai altéret kódoljunk n bozonikus módusba[16][4]. Tehát kódolhatunk egy $d = 2$ alteret egy módusba (ezzel megteremtve a lehetősget "bozonikus" kvantumbitek előállítására), lényegében egy darab kvantumbitet leíró logikai alteret kódolva egy módusba. A GKP kód definíciójához használhatjuk a stabilizátor operátor formalizmust. Legyen $\hat{S_X} = e^{-i2\sqrt{\pi}\hat{p}}$ és $\hat{S_Z} = e^{i2\sqrt{\pi}\hat{x}}$ stabilizátor operátorok, ekkor megállapítható, hogy annak ellenére, hogy $\hat{x}$ és $\hat{p}$ nem cserélnek fel, a definiált $\hat{S_Z}$ és $\hat{S_X}$ operátorok kommutálnak, illetve logikai Pauli operátorok $\hat{\sigma_z} = \sqrt{\hat{S_Z}}$ és $\hat{\sigma_x} = \sqrt{\hat{S_X}}$, ekkor úgy definiáljuk a logikai GKP kódteret, hogy közös altere legyen a stabilizátor operáto-

[15] Ezen operátorok teljesítik a kvantumos harmónikus oszcillátorbeli léptető operátorokra vonatkozó felcserélési relációt, illetve algebrát, vagyis az ott is használatos formalizmus ebben az esetben is hasznos lesz.

[16] Egy többrészecske rendszer bozonikus, ha a rendszert leíró $|\psi_N\rangle$ hullámfüggvényre teljesül, hogy $\hat{P}_{i,j}\,|\psi_N\rangle = |\psi_N\rangle$, ahol $\hat{P}_{i,j}$ az i és j részecske felcserélő operátor.



1.2. ábra. Ideális GKP állapotok. A felső állapot egy idális $|0_L\rangle$, az alsó pedig egy ideális $|1_L\rangle$ állapot. Az egyes Dirac-delták között $2\sqrt{\pi}$ távolság van.

roknak, méghozzá a +1 sajátértékhez tartozó állapotokból[5][4]:

$$|0_L\rangle = \sum_{j=-\infty}^{\infty} \left|2j\sqrt{\pi}\right\rangle \tag{1.15}$$

$$|1_L\rangle = \sum_{j=-\infty}^{\infty} \left|(2j+1)\sqrt{\pi}\right\rangle \tag{1.16}$$

Ahol a szummákban szereplő állapotok az $\hat{x}$ operátor sajátállapotai, illetve ezzel a választással a logikai $\tilde{\sigma_Z}$ operátornak a ± 1 - hez tartozó állapotokat kapjuk. Ehhez hasonlóan választhattuk volna úgy a logikai 2 szintes bázisállapotokat, hogy ugyenez teljesüljön a logikai $\tilde{\sigma_X}$ operátorra, azonban akkor a $\hat{p}$: operátor sajátállapotainak a lineár kombinációját kapjuk.
Megjegyzés: Könnyen megmutatható, hogy a fent említett tulajdonságok valóban teljesülnek, ehhez célszerű megvizsgálni a $\tilde{\sigma_z}|\phi\rangle = \phi|\phi\rangle$ sajátérték problémát, $|\phi\rangle = |k\sqrt{\pi}\rangle$ választással. Ha megnézzük, hogy az operátor hogyan hat az állapotra a következőt tapasztaljuk:

$$e^{i\sqrt{\pi}\hat{x}}\left|k\sqrt{\pi}\right\rangle = (1 + ik\pi - k^2\pi^2 - ik^3\pi^3 + k^4\pi^4 + ...)\left|k\sqrt{\pi}\right\rangle =$$

$$\sum_n \frac{(ik\pi)^n}{n!}\left|k\sqrt{\pi}\right\rangle = e^{ik\pi}\left|k\sqrt{\pi}\right\rangle$$

Most $k \in \mathbb{Z}$ esetet vizsgálva, ha k páros, akkor $e^{ik\pi} = 1$, és páratlan esetben $e^{ik\pi} = -1$ ezzel igazolva a fenti állítást.

Tehát mivel az $\hat{x}$ kvadratúra sajátfüggvényei Dirac-delta függvények[17], ezek az ideális GKP állapotok ezen Dirac-deltákból állnak. Vizuálisan ábrázolható a két állapot, az 1.2 ábrán látható.

Továbbá egy $|\psi\rangle = \int_{-\infty}^{\infty} \psi(x)dx$ általános állapot esetén információt a $\psi(x)$ hullámfüggvény hordoz, ugyanakkor $|\psi\rangle$ felírható a Fock-bázison is (ekkor az együtthatók hordozzák lényeges információt), $\sum_n c_n|n\rangle$. Valójában információt kódolunk egy kvantumos harmónikus oszcillátorba. A harmónikus oszcillátor léptető operátorai a szokásos módon $\hat{a} = \frac{\hbar}{\sqrt{2}}(\frac{\hat{x}}{x_0} + i\frac{\hat{p}}{p_0})$ és $\hat{a}^\dagger = \frac{\hbar}{\sqrt{2}}(\frac{\hat{x}}{x_0} - i\frac{\hat{p}}{p_0})$ (lefelé és felfelé léptető operátor), ahol $x_0 = \sqrt{\frac{\hbar}{m\omega}}$ és $p_0 = \sqrt{\hbar m\omega}$. A kvadratúra operátorok és a léptető operátorok közötti összefüggést átrendezve, azok is kifejezhetőek a léptető operátorok segítségével.

[17] Valójában disztribúciók.

A GKP kód hibajavító képességének tárgyalásához először definiáljuk a koherens eltolás (angolul: *displacement*) operátort[18]:

$$\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}$$

A számítás közben fellépő hiba következtében előfordulhat, hogy az állapotok eltolódnak, amelyeket szeretnénk detektálni. Erre a célra fogjuk használni a stabilizátor operátorokat, amelyek mivel nem tesznek különbséget a logikai $|0_L\rangle$ és $|1_L\rangle$ állapotok között, vagyis mérésükkor nem teszik tönkre a kvantumállapotot, használhatóak hibajavításra[2]. Mérésükkor valamely sajátértéküket kapjuk eredményül, amely $e^{i\theta}$ formájú lesz, illetve tudjuk, hogy a megfelelő bázisállapot esetében $e^{i2k\pi} = 1$ ($k \in \mathbb{Z}$) - nak kell teljesülni. Tehát amennyiben ez nem teljesül, akkor kapunk egy θ szöget, amelyet ki kell korrigálni az állapoton. Ez a korrekció megtehető mindaddig, amíg a $\theta < \sqrt{\pi}/2$, mert ekkor még a helyes állapothoz közelebb vagyunk. Vagyis a stabilizátor operátorok mérésével ezen hibák orvosolhatóak, hiszen θ ismeretében egy feltételes displacement operátor végrehajtása elegendő.

Néhány további lehetséges művelet példaként, folytonos változó felett [18]:

$$\hat{R}(\alpha) = e^{i\alpha\hat{a}^\dagger\hat{a}} \tag{1.17}$$

$$\hat{B}(r,\phi) = e^{\theta(e^{i\phi}\hat{a}_1\hat{a}_2^\dagger - e^{-i\phi}\hat{a}_1^\dagger\hat{a}_2)} \tag{1.18}$$

$$\hat{SUM}(g) = e^{-ig\hat{x}_1\otimes\hat{p}_2} \tag{1.19}$$

Ugyanakkor az ideális GKP állapotok nem normalizálhatóak, vagyis nem realizálhatóak. Persze ez azt is jelenti, hogy közelítőállapotokat használhatunk GKP kódolásra. Egy szokásos módszer GKP állapotok közelítésére, hogy véges szélességű Gauss-függvényekből rakjuk ki az állapotot, amelyekre egy burkoló Gauss-függvény fekszik, így már normalizálható állapotot kapva. Ez az állapot az ideális GKP állapotokkal ellentétben már realizálható, természetesen a modell szempontjából (éppen a véges szélesség miatt) nem lesz tökéletes, amit számítások elvégzésekor figyelembe kell venni[19].

[18] Az operátornak sok érdekes tulajdonsága van, amelyekről nem lesz részletesen szó, mint például, hogy lehetséges koherens állapotok generálására használni, ha a $|0\rangle$ vákuum állapotra hattatjuk egy harmónikus oszcillátor esetében: $\hat{D}(\alpha)|0\rangle = |\alpha\rangle$, ahol $|\alpha\rangle$ egy koherens állapot, amelyet az α paraméter jellemez.

[19] Egy-egy algoritmus többszöri lefuttatása például statisztikai alapú hibajavításhoz vezethet ebben az esetben, így kompenzálva a konstrukció tökéletlenségét.

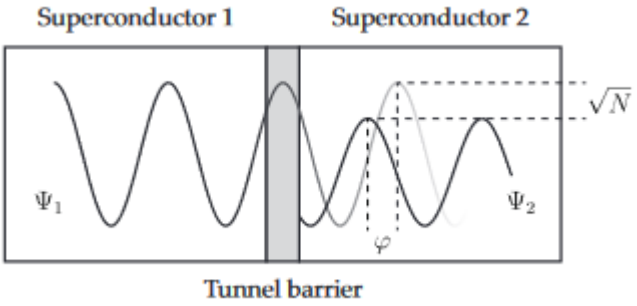
2. fejezet

Fizikai architektúrák

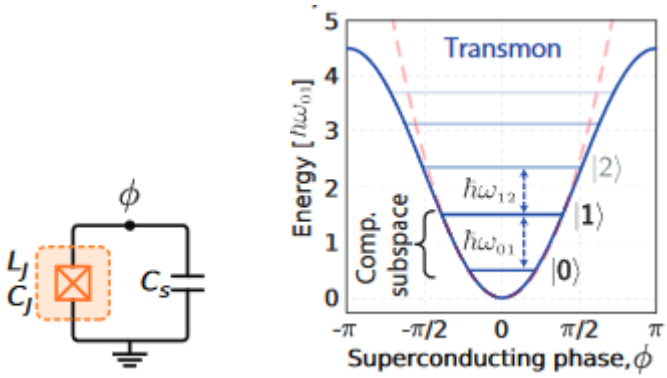
2.1. Szupravezető-alapú technológia

Kvantumszámítógépek fejlesztése esetében az egyik gyakran kutatott megoldás, a szupravezető technológiával készített áramkörök. Ilyen megoldással készültek az IBM kvantumszámítógépei is. Az eljárás során egy kvantumbitet egy mesterséges atom két legalsó sajátállapota (alapállapot és első gerjesztett állapot) reprezentál. Egy ilyen rendszernek sok elvárásnak kell megfelelni[9], mint például hosszú koherencia, szabályozhatóság, anharmonikus viselkedés (hogy jól definiált 2-szintes rendszerként lehessen használni). Ezen felül az áramkörnek nagyon alacsony hőmérsékletre van szüksége (mK nagyságrend), ennek érdekében a rendszert folyamatosan hűteni kell. Emiatt nehezen elképzelhető labori környezeten kívüli megvalósítása, ennek a módszernek.

Szupravezető áramkörök megvalósításához *Josephson junction*-t használnak[9], amelynek a sematikus ábrája a 2.1-es ábrán látható. Ugyanakkor ez az architektúra típus támogatja a diszkrét, kapu-alapú modell használatát[3]. Továbbá egy kvantumbit megvalósítható, egy változtatható külső mágneses térbe helyezve.



2.1. ábra. Josephson junction sematikus ábrája, a [9] munkából adoptálva.



2.2. ábra. Josephson kvantumbit sematikus ábrája, és a hozzá tartozó energia szintek ábrázolva, a [8] munkából adoptálva. Fontos megfigyelni, hogy az egyes szintek közötti átmenethez különböző frekvencia tartozik.

2.2. Foton-alapú megoldások

Az optikai megoldások nagyon elterjedtek lettek a kommunikáció területén, az elmúlt években. A folyamatosan növő igényeknek hála ez egyáltalán nem meglepő, hiszen az optikai hálózatokban nagyon magas sávszélesség érhető el. Kvantumkommunikáció területén is sok megoldás optikai alapú rendszerekben látott napvilágot. Ugyanakkor mint kvantumszámítógépes platform egy ideig nehez volt elképzelhető, hiszen az úgynevezett Di Vincenzo kritériumok közül a skálázhatóságra vonatkozó feltétel teljesülése erősen kérdéses volt.

Ugyanakkor az optikai rendszereknek nagy előnye, hogy a legtöbb részében nem szükséges közel 0 Kelvin hőmérséklet felállítása (esetleg mérésekhez lehet szükséges a mérő berendezés hűtése, alacsony hőmérsékleten tartása).

2020-ban azonban a hefei-i University of Science kutatói sikeresen demonstráltak kvantumfölényt (angolul: *quantum supremacy*)-t, vagyis egy feladatot gyorsabban megoldani, mint bármely klasszikus számítógép képes lenne, amivel bemutatták, a megoldásban rejlő potenciált, és persze nehézségeket is.

Továbbá a kanadai Xanadu cég foglalkozik optikai kvantumszámítógépek kutatásával és fejlesztésével. Több termékvonaluk is ismert, mint az X-széria, illetve a 2020 nyarán bemutatott Borealis, amellyel sikeresen demonstráltak kvantum előnyt (a kínai géphez hasolóan szintén gaussi bozon-mintavételezési problémában).

3. fejezet

Algoritmusok, protokollok implementálása és összehasonlítása különböző modellekben

3.1. Általános alapelvek

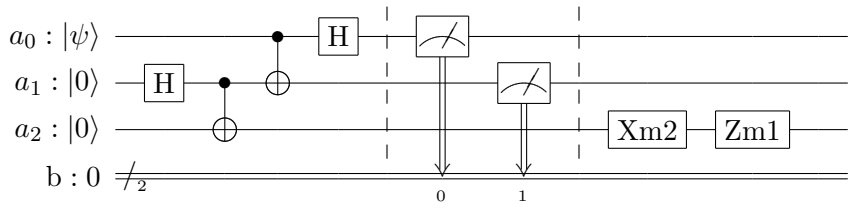
Ebben a részben az előző szakaszban megvizsgált számítási modellek felett mutatok megvalósítást különböző algoritmusokra/eljárásokra, és ezeken keresztül teszek kísérletet az egyes modellek összehasonlítására. Kiindulópontként a kapu-alapú modell fogom választani, vagyis elsőként ebben a modellben írom le az egyes algoritmusok megoldását, majd a további modellekbeli megoldás fog következni, illetve, hogy az egyes modellek esetében mi okoz nehézséget, vagy éppen milyen részek az erősségeik. Elöljáróban annyit érdemes megemlíteni, hogy a kapu-alapú modell választása valóban praktikus, hiszen általánosságban ez a legelterjedtebb, továbbá klasszikus analógia miatt ennek a megértése általában könnyebb feladat.

3.2. Teleportáció

Az algotitmus lényege, hogy egy tetszőleges kvantumállapotot kvantumbitek között teleportáljunk, anélkül, hogy az adott állapotot "ismernénk"[1].

[1] Pontosabban ismernénk abban az értelemben, hogy tudnánk preparálni.

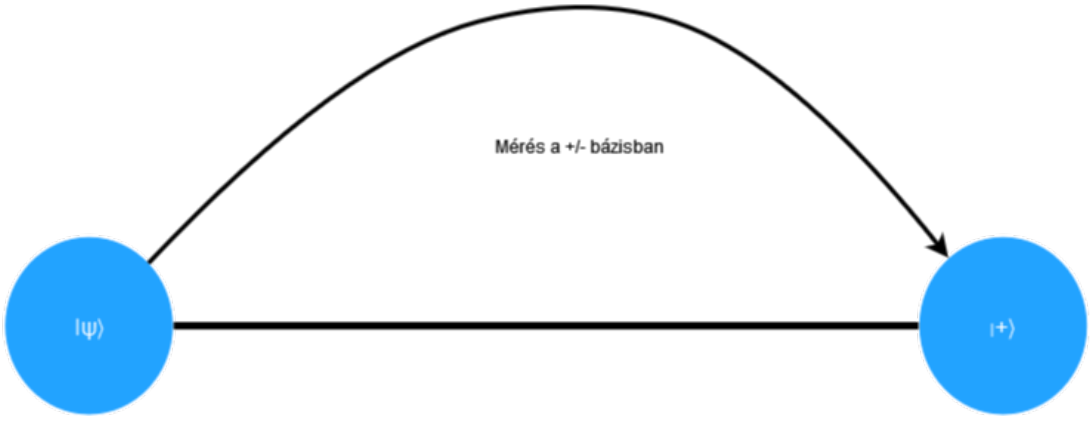
3.2.1. Kapu-alapú modell



3.1. ábra. Teleportáció implementációm kapu-alapú modellbeli áramköre. Az egyes kapuk a következőket jelentik: 'H' = Hadamard kapu, 'Xm2' = Pauli-X kapu az alsó mérés feltételében, 'Zm1' = Pauli-Z kapu a felső mérés feltételében. Illetve a kapcsolás elején az első művelet egy vezérelt Pauli-X kapu ($C\hat{N}OT$).

A felső vezetéken található a bemenet, egy $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ ($|\alpha|^2 + |\beta|^2 = 1$) teljesen tetszőleges kvantum állapot. Továbbá az algoritmus előállít egy Bell-állapotot ($\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ jelen esetben), amelyet az algoritmus folyamán felhasznál. Az eljárás végére az alsó vezetéken megjelenik a teleportálni kívánt állapot.

3.2.2. Mérés-alapú modell



3.2. ábra. Mérés-alapú környezetbeli teleportáció megvalósításom sematikus ábrája.

Ezen modell esetében kiderül, hogy a teleportációnak elég fontos szerepe van a teljes modell működése kapcsán. Pontosabban használata szinte minden eljárásban szükséges, mert ennek segítségével tehető lehetővé az információ propagálása.
Működésének demonstrálására egy 2 összefonódott kvantumbitből álló gráf állapotból indulok ki. Vagyis a

$$|g\rangle = \hat{CZ}_{1,2}\,|\psi\rangle \otimes |+\rangle\,, \text{ ahol } |\psi\rangle \text{ tetszőleges kvantum állapot.} \tag{3.1}$$

A korábbiaknak megfelelően $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ normalizált állapot, illetve $|+\rangle = \frac{|0\rangle+|2\rangle}{\sqrt{2}}$ a szokásos módon a $\hat{\sigma}_x$ operátor sajátállapota. Az állapotot a standard bázisban kifejtve:

$$|g\rangle = \frac{\hat{CZ}_{1,2}}{\sqrt{2}}(\alpha|00\rangle + \alpha|01\rangle + \beta|10\rangle + \beta|11\rangle) \tag{3.2}$$

Illetve a vezértelt Pauli-Z csak a $|11\rangle$ állapotnak hoz be egy -1 - es szorzót, tehát:

$$|g\rangle = \frac{1}{\sqrt{2}}(\alpha|00\rangle + \alpha|01\rangle + \beta|10\rangle - \beta|11\rangle) = \alpha|0\rangle \otimes |+\rangle + \beta|1\rangle \otimes |-\rangle \tag{3.3}$$

Az algoritmus végrehajtásához arra van szükség, hogy az első kvantumbitet megmérjük a σ_x bázisban. Ehhez praktikus lehet minden kvantumbit felírása ebben a bázisban:

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}} \text{ és } |1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}} \tag{3.4}$$

Innen a teljes állapot:

$$|g\rangle = \frac{\alpha}{\sqrt{2}}(|++\rangle + |-+\rangle) + \frac{\beta}{\sqrt{2}}(|+-\rangle - |--\rangle) \tag{3.5}$$

Most ebben az állapotban könnyebben vizsgálhatjuk, hogy mi történik, ha mérés eredménye $m = 0$ ($|+\rangle$ esetén), és $m = 1$ ($|-\rangle$ esetén), eltekintve a valódi sajátértékektől. A szóban forgó állapotok normalizálva:

$$\begin{aligned} m = 0 &\rightarrow \alpha|+\rangle + \beta|-\rangle \\ m = 1 &\rightarrow \alpha|+\rangle - \beta|-\rangle \end{aligned} \tag{3.6}$$

Ahonnan már látszik, hogy az első esetben megkaptuk $|\psi\rangle$ állapotot csak a Pauli-X bázisban, a második esetben is hasonlóan, leszámítva egy Pauli-korrekciót[2]. Pontosabban $m = 0$ esetében $\hat{H}|\psi\rangle$ és $m = 1$ esetében a $\hat{H}\hat{\sigma}_z|\psi\rangle$ állapotot kapjuk, amely kompaktabb módon írható $\hat{H}\hat{\sigma}_z^m|\psi\rangle$, amelyet írhatunk $\hat{\sigma}_x^m\hat{H}|\psi\rangle$ alakban is. Vagyis sikeresen teleportáltunk egy tetszőleges 1 kvantumbites kvantumállapotot, amelyet esetlegesen másik bázisban de megkapunk.
Valójában felfogható az eljárás mint egy eszköz a gráf állapotban, mint hálózatban egy állapot mozgatására. Továbbá mivel az állapotaink információt tárolnak, a protokollt felhasználhatjuk az információ hálózaton belüli propagálására. Ez fontos hiszen ebben a modellben a műveleteinket mérésekkel szeretnénk megvalósítani, így ha egy kvantum bit nem megfelelő "helyen" van a hálózaton belül egy művelet végrehajtásához, akkor azt valahogyan el kell juttatni, ahhoz a kvantumbithez, amelyen a megfelelő mérést/műveletet végre akarjuk hajtani anélkül, hogy az állapotot megváltoztatnánk[3].

[2] A mérés-alapú sémában gyakran jelennek meg ilyen Pauli-korekciók. Sokszor feltételes operátorokat kell hattatnunk egy-egy eredmény-állapotra a korábbi méréseknek a függvényében. Ezen operátorokat szokás *byproduct* - oknak nevezni.

[3] Persze jelen esetben mondhatnánk, hogy de az állapot változik, de valójában a változás az vagy egy újabb propagálásnál eltűnik (mivel a Hadamard operátor hermitikus), vagy számításba kell vennünk korrekciós operátort.

3.2.3. Folytonos változójú modell

Ebben az esetben a nehézséget az okozhatja, hogy kilépünk az eddig megszokott 2-dimenziós Hilbert-térből egy végtelen-dimenziós Hilbert-térbe. Mint azt a modell alapvető tárgyalásakor említettem, használhatunk beágyazásokat (kódolásokat), annak érdekében, hogy egy logikai Hilbert-teret állítsunk elő, amin az algoritmust futtatni tudjuk. Persze ekkor, még mindig fent áll az a probléma, hogy az egyes műveletek az eredeti Hilbert-téren vannak értelmezve, vagyis egy megfelelő paraméterezés szükséges, amely segítségével a beágyazott térre úgy hatunk, ahogyan az algoritmusnak megfelelő.

A folytonos modellben praktikus használni a léptető operátoros formalizmust, az egyes műveletek leírására[4]. Ezzel továbbá a kódolást egy harmónikus oszcillátorral végezzük (így használható a Fock-bázis is).

Jelen esetben követhetjük a kapu-alapú modell esetében megismert eljárást, az algoritmus implementálásához. Ehhez szükséges az egyes műveleteket megfelelő paraméterekkel végrehajtani. Szükséges operátorokról összefoglaló táblázat:

$\hat{U}$	Művelet	Megnevezés
$\hat{\sigma_x}$	$\hat{D}(\sqrt{\pi/2})$	$\hat{x}$ *displacement*
$\hat{\sigma_z}$	$\hat{D}(i\sqrt{\pi/2})$	$\hat{p}$ *displacement*
$\hat{H}$	$\hat{R}(\frac{\pi}{2}) = e^{i\frac{\pi}{2}\hat{a}^\dagger\hat{a}}$	Hadamard kapu
$\hat{CNOT}$	$\hat{CX} = e^{-i\hat{x}_1\otimes\hat{p}_2}$	Kontrollált Pauli-X
$\hat{CZ}$	$e^{i\alpha\hat{x}_1\hat{x}_2}$	Kontrollált Pauli-Z

3.1. táblázat. Összefoglaló táblázat az egyes műveletekhez [18]-alapján.

A $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ Bell-állapot előállításához is elegendőek ezek a műveletek így az algoritmus folytonos változóba ágyazva is megoldható. Vegyünk fel 3 GKP kódolt kvantumbitet: $|0_L0_L0_L\rangle$ állapotot elérve, majd az algoritmus:

$$\hat{\sigma}_{z3}^{m_1}\hat{\sigma}_{x3}^{m_2}\hat{M}_{1,2}\hat{H}_1\hat{CNOT}_{1,2}\hat{CNOT}_{2,3}\hat{H}_2\,|0_L0_L0_L\rangle \tag{3.7}$$

ahol az alsó indexek jelenti, hogy az egyes operátorok melyik GKP kvantumbitre hatnak. Továbbá az m_1 illetve m_2 értékek a megfelelő mérések eredményei, melyek felvehetnek értéket a $\{0,1\}$ halmazból.

3.2.4. Összegzés

Eltekintve az algoritmus felhasználási lehetősgeitől és csupán az egyes modellekben való implementációra koncentrálva a következőket lehet megállapítani. Megfelelő paraméterezéssel a folytonos változójú modellben a kapu-alapú modellbeli megvalósítás működik, mert képesek vagyunk létrehozni egy beágyazást a folytonos változóba. Ennek nagyobb jelentősége inkább a fizikai rétegben keresendő, hiszen mivel 2 különböző modell egymásnak megfeleltetésének segítségével lehetőség nyílik az egyik kezelhetőségét és a másik megvalósíthatóságát egyszerre kihasználni. A helyzet egy kissé érdekesebb a mérés-alapú modell

[4]Továbbá a fizikai rétegben is fontos szerepet játszanak, az olyan megvalósításokban, ahol ezt a modellt használják.

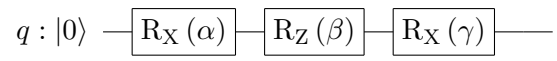
esetében, hiszen annak ellenére, hogy az applikációktól erre a szakaszra elvonatkoztattam, itt meg kell jegyezni, hogy az algoritmusnak a modellben fontos betöltött szerepe van, az információ áramlásában a hálózatszerű struktúrában. Vagyis összehasonlítás eredményeként elmondható, hogy a mérés-alapú modellben sokkal természetesebben jelenik meg az eljárás, szinte már mint egy "elemi műveletként" is lehet rá tekinteni.

3.3. Általános egy-kvantumbit kapu

Algoritmusokban/eljárásokban szükséges, hogy képesek legyünk arra, hogy az adott kvantumbitjeinken (legyenek azok akármelyik modellben értelmezve valahogyan) tetszőleges egy-kvantumbit műveleteket végezzünk el[5]. Ez annyit jelent, hogy ha vesszük egy kvantumbit ábrázolására a Bloch-gömböt, akkor ennek a gömbnek a felületén szeretnénk bármelyik pontot elérni bármelyik másik pontból. Ez megvalósítható forgatások segítségével, pontosabban elegendőek csupán az X és Z tengely körüli forgatások. Továbbá mint ahogy említettem a 1.2 szakaszban, belátható, hogy egy tetszőleges $\hat{U}$ unitér operátor $\hat{U} = e^{i\theta}\hat{R}_x(\gamma)\hat{R}_z(\beta)\hat{R}_x(\alpha)$ - ként realizálható, ahol $\hat{R}_i(\phi)$ az i tengely körüli ϕ szöggel való forgatást jelenti. Továbbá az $e^{i\theta}$ csak egy globális fázist ad az állapotnak, amelyre hat, amelynek jelen esetben nincs jelentősége, ezért most elhagyható.

3.3.1. Kapu-alapú modell

Mivel ebben a modellben a lehetséges operátoraink tetszőleges unitér operátorok, ezért a fenti összefüggés alapján könnyen realizálható bármilyen unitér operátor, forgatás operátorok használatával.



3.3. ábra. Tetszőleges egy-kvantumbit művelet, a kapu-alapú modellben implementáló áramköröm. Az egyes kapuk a következőket jelentik: $R_i(\phi)$ az i tengely körüli ϕ szöggel való forgatás.

3.3.2. Mérés-alapú modell

Itt az előző szakaszban látott teleportációt fogom használni, egy kis mértékben átalakítani, annak érdekében, hogy utána használható legyen jelen esetben is. Először vegyük a korábban megismert mérés előtti cluster állapotot (azaz $\hat{CZ}_{1,2}\,|\psi+\rangle$ állapot). Ezek után végezzünk mérést az XY síkon ϕ szöggel jellemezhető bázison, ahol az $\hat{O}(\phi) = \cos(\phi)\hat{\sigma}_x + \sin(\phi)\hat{\sigma}_y$ obszervábilis szerint mérünk. Az operátor sajátbázis rendszere legyen $\{|b_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}\,|1\rangle), |b_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle - e^{i\phi}\,|1\rangle)\}$, ekkor felírhatjuk a cluster állapot első

[5]Ezért annak ellenére, hogy külön önmagában meglepő lehet tárgyalni, mint algoritmust, fontos szerepe van tetszőleges algoritmusok kialakításában, ezért praktikus a tárgyalása.

kvantum bitjét ebben a bázisban, hogy könnyebben kezelhető legyen a mérés:

$$\begin{aligned} |\psi\rangle &= \alpha\,|0\rangle\,|+\rangle + \beta\,|1\rangle\,|-\rangle \\ |\psi\rangle &= |b_1\rangle \otimes (\frac{\alpha}{\sqrt{2}}\,|+\rangle + \frac{\beta e^{-i\phi}}{\sqrt{2}}\,|-\rangle) + |b_2\rangle \otimes (\frac{\alpha}{\sqrt{2}}\,|+\rangle + \frac{\beta e^{-i\phi}}{\sqrt{2}}\,|-\rangle) \end{aligned} \tag{3.8}$$

Innen hasonlóan a teleportációnál tárgyalt módon a mérés eredménye lehet 0 vagy 1 (amelyekhez $|b_1\rangle$ illetve $|b_2\rangle$ tartoznak).

$$\begin{aligned} m = 0 &\rightarrow \alpha\,|+\rangle + \beta e^{-i\phi}\,|-\rangle \\ m = 1 &\rightarrow \alpha\,|+\rangle - \beta e^{-i\phi}\,|-\rangle \end{aligned} \tag{3.9}$$

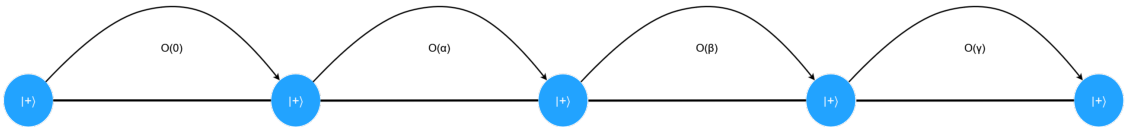
Vagyis a mérés után $\left|\psi'\right\rangle = \hat{H}e^{i\frac{\phi}{2}\hat{\sigma}_z}\hat{\sigma}_z^m\,|\psi\rangle = \hat{\sigma}_x^m\hat{H}e^{i\frac{\phi}{2}\hat{\sigma}_z}\,|\psi\rangle$.

Ezzel általános esetét kaptuk a teleportációs algoritmusnak, pontosabban az eljárás lehetővé tette, hogy egy Z tengely körüli forgatást is elvégezzünk ($e^{i\frac{\phi}{2}\hat{\sigma}_z}$). Ez azért érdekes, mert ahogyan a korábban tárgyalt kapu-alapú modellben volt róla szó, egy álatlános unitér művelet megvalósítható forgatásokkal, és ez egy ilyen szükséges forgatás.

Ezek után már össze lehet rakni a teljes eljárást, amely megvalósítja a kívánt tetszőleges unitér operátort egy kvantumbiten. Ehhez egy nagyobb cluster állapotra lesz szükség, mint korábban, a kiindulási állapot:

$$\hat{CZ}_{1,2}\hat{CZ}_{2,3}\hat{CZ}_{3,4}\hat{CZ}_{4,5}\,|\psi\rangle \otimes \bigotimes_{n=2}^{4} |+\rangle_n \tag{3.10}$$

Ezek után használjuk először a bemeneti kvantumbiten a teleportációs protokollt, majd az általános eljárást a mérésre 3-szor, α, β, γ szögekkel, ahol az egyes szögek megfeleltethetőek az Euler-szögeknek, ezzel egy általános forgatást definiálva[19]. Pontosabban a szögekhez tartozik egy-egy feltételes előjel, amely a korábbi mérések eredményétől függ. Az egyes szögek megfelelő sorrendben $(-1)^{m_1}$, $(-1)^{m_2}$, $(-1)^{m_1+m_3}$ előjelet kapnak, ahol m_i az i.-dik mérés eredménye. Valójában annyi történik, hogy a bemeneti kvantumbitet teleportáljuk, majd 3 forgatást hajtunk végre, mindet tetszőleges szöggel. Ha eltekintünk a lehetséges korrekcióktól, akkor alapvetően a $\hat{H}e^{i\frac{\gamma}{2}\hat{\sigma}_z}\hat{H}e^{i\frac{\beta}{2}\hat{\sigma}_z}\hat{H}e^{i\frac{\alpha}{2}\hat{\sigma}_z}\hat{H}\,|\psi\rangle$ állapotot kapunk, amelyet átírhatunk, $e^{i\frac{\gamma}{2}\hat{\sigma}_x}e^{i\frac{\beta}{2}\hat{\sigma}_z}e^{i\frac{\alpha}{2}\hat{\sigma}_x}\,|\psi\rangle$ állapotra[6], amelyek pontosan az egyes tengelyek körüli forgatásnak felelnek meg.



3.4. ábra. A mérés-alapú modellben tetszőleges unitér operátor megvalósítását reprezentáló ábrám. Az O(ϕ) jelölés annyit jelent, hogy a korábban definiált $\hat{O}(\phi)$ obszervábilist mérjük.

3.3.3. Folytonos változójú modell

Ahogyan a korábbi szakaszban most is alkalmazható az eljárás, hogy a lehetséges műveleteket használjuk olyan paraméterekkel, hogy a kapu-alapú modellben definiált eljárást kapjuk.

[6]Részletesebb levezetés az átalakításhoz a Grover algoritmust tárgyaló szakaszban.

3.3.4. Összegzés

Függetlenül, hogy milyen modellt használunk egy számításhoz, tetszőleges kvantum kapuk megvalósítása egy kvantumbiten szükséges feladat. A vizsgált modellek esetében erre adható megfelelő megoldás (szükséges is, ahhoz hogy az univerzalitásuk teljesüljön), ugyanakkor eltérő módon.
A kapu-alapú modell esetében könnyen követhető az eljárás, és a Bloch-gömbnek köszönhetően remekül illusztrálható/szemléltethető a folyamat. A geometriai megfelelő miatt intuitívebb a művelet.
A mérés-alapú modellben kissé nagyobb mértékben szükséges a számításokra hagyatkozni. Mint a klasszikus analógiával is a helyzet, ezen eljárás szemléletes ábrázolása nehéz feladat. Ez visszavezethető arra, hogy a mérések leírásához rendelkezésre álló eszközök limitáltak, illetve magából a mérésből is adódik egy fajta bizonytalanság, és mivel a modell lényege, hogy a műveleteket mérések sorozatával végezzük el, így nem meglepő, ha minden eljárás esetében előkerül ez a gondolat.

3.4. Deutsch-Jozsa algoritmus

A következő 2 szakaszban egy-egy híres algoritmust vizsgálok meg[7]. A Deutsch-Jozsa algoritmus története nagyon régre nyúlik vissza (1992, David Deutsch és Richard Jozsa), az első algoritmusok között volt, amely azt volt hivatott prezentálni, hogy bizonyos problémák esetében kvantumalgoritmusok szignifikáns gyorsítást érhetnek el. Ugyanakkor azt érdemes megemlíteni, hogy a feladat amelyre az algoritmus megoldást kínál, olyan módon van megformálva, hogy könnyen szemléltethető legyen a gyorsulás, azonban nem egy praktikus értelemben vett hasznos problémára kínál megoldást. Ettől függetlenül egy önmagában is nagyon érdekes eljárás, amely meghatározó szerepet játszik a kvantumalgoritmusok történetében.

Jelen eset pedig egy érdekes példaként szolgálhat az egyes modellek közötti összehasonlításban, illetve a korábban látott eljárásokhoz képest komplexebb eljárásként egy érdekes vizsgálati tárgy.

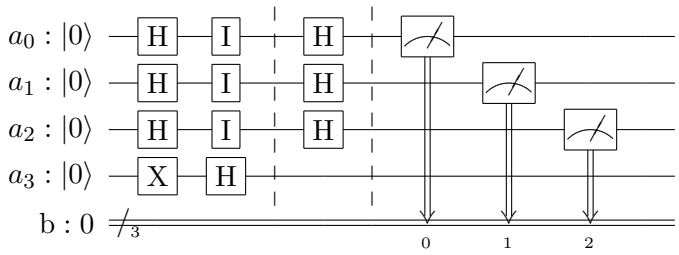
A Deutsch-Jozsa algoritmus a következő problémára keresi a választ: Adott egy $f : \{x_0, x_1, x_2, ..., x_n\} \to \{0, 1\}$ függvény, ahol minden x_i egy bináris változó, tehát a bemenet egy n hosszú bit string, és a hozzárendelési szabály alapvetően kétféle lehet (vagyis kétféle függvény valósítható meg). Vagy konstans (vagyis minden lehetséges bemeneti karaktersorozathoz 0-át vagy 1-et rendel hozzá), vagy kiegyensúlyozott (vagyis a bemeneti string-ek pontosan felére 0-át a másikra pedig 1-et kapunk). Belátható, hogy n hosszú bit stringre éppen 2^n féle lehetséges bemeneti karaktersorozat létezik. A feladat, hogy olyan megoldást adjunk amely képes 100% biztossággal megadni, egy adott f-re, hogy az éppen milyen hozzárendelési szabállyal rendelkezik, konstans vagy kiegyensúlyozott a függvény.

A feladat megoldása klasszikus esetben, hogy sorra kiértékeljük az egyes bemeneti karaktersorozatokat, addig amíg nem kapunk kétféle kimenetet (vagyis 0-át és 1-et is), vagy kiértékeltünk elegendő bemenetet ($\frac{N}{2} + 1$ darabot, ahol N a lehetséges bemeneti string-ek száma). Vagyis legjobb esetben 2 kiértékelés után készen leszünk, azonban legrosszabb esetben (illetve amikor a függvény konstans akkor mindig) ki kell számolni $\frac{N}{2}+1$ értéket. Mivel $N = 2^n$, ezért N mérete a bemenet hosszában exponenciálisan nő.

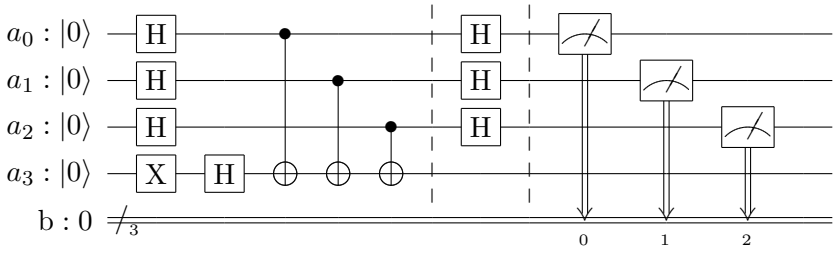
Ezzel szemben kvantumos esetben elegendő lesz egyetlen kiértékelés, a függvényt egyetlen uniform szuperpozíción elvégezve, majd megfelelő méréssel kiolvasható a válaszhoz szükséges információ.

[7] A korábbi szakaszokból a teleportáció is egyike a "szokásos" híres algoritmusoknak, azonban annak a korábbra vétele/korábban tárgyalása, a mérés-alapú modellben betöltött alapvető szerepe miatt volt praktikus.

3.4.1. Kapu-alapú modell



3.5. ábra. Deutsch-Jozsa algoritmus (3-bites) megvalósításomnak áramköre kapu-alapú modellben, amikor a kérdéses f függvény konstans.



3.6. ábra. Deutsch-Jozsa algoritmus (3-bites) megvalósításomnak áramköre kapu-alapú modellben, amikor a kérdéses f függvény kiegyensúlyozott.

Az algoritmus implementálásához szükség van $n+1$ kvantumbitre, illetve n klasszikus bitre, annak érdekében hogy a kimenetet el lehessen tárolni. Továbbá egy orákulumra, amely implementálja a függvényt. Azt feltételezzük, hogy egy ilyen orákulum rendelkezésre áll (ebből 2 lehetséges van, egy amely a konstans (ábra 3.5), egy pedig amelyik a kiegyensúlyozott (ábra 3.6) függvényt valósítja meg). Az algoritmus többi részét pedig ennek felhasználásával kell megvalósítani.

A kezdeti állapot $\bigotimes_{i=1}^{n} |0\rangle \otimes |1\rangle$, majd az orákulum bemenetére érkező állapot (Hadamad kapuval az alsó kvantumbitet $|-\rangle$-ba transzformálva):

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{3.11}$$

Az ezt követő állapotban már benne lesz a keresett függvény (minden bemenetre adott válaszával):

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes \frac{|f(x)\rangle - |f(x) \oplus 1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{3.12}$$

Majd a végállapot:

$$|\Phi\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} (-1)^{xy} (-1)^{f(x)} |y\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{3.13}$$

Amely esetében a $\bigotimes_{i=1}^{n} |0\rangle$ állapot valószínűsége[8] $\bigotimes_{i=1}^{n} \langle 0 |\Phi\rangle = 1$, ha a függvény konstans, és 0, ha kiegyensúlyozott. Vagyis méréskor, ha $\bigotimes_{i=1}^{n} |0\rangle$-t mérünk, akkor f konstans, különben kiegyensúlyozott.

3.4.2. Mérés-alapú modell

Ebben a modellben az implementáció először egy $n = 3$ bit hosszú bemenet esetén működő példán keresztül lesz megvizsgálva (csak azért éppen $n = 3$, hogy szemléletes legyen a korábbi kapu-alapú modell mellett, ahol szintén az volt a példa), majd az eljárásnak az általánosabb verziójáról is esik szó. A konstrukció alap ötletét a [17] munka képezi, ugyanakkor a megvalósítás során számításba vettem, hogy lehetőleg minél kisebb legyen a cluster állapot, ennek érdekében nem egy teljes cluster-ből indulok ki[9].

Kezdetben, az alapállapot 7 darab $|+\rangle$ és egy $|-\rangle$ állapotból áll[10]. Majd $\hat{CZ}$ műveletek alkalmazásával alakítsuk ki a következő gráf állapotot (illusztráció az 3.7 ábrán):

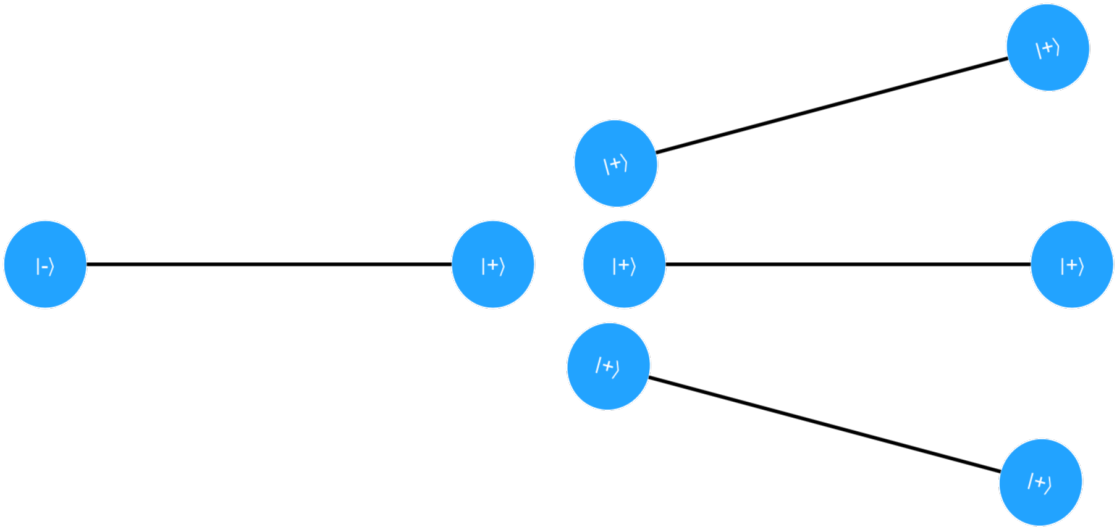
$$\frac{|+\rangle |1\rangle + |-\rangle |0\rangle}{\sqrt{2}} \otimes \frac{1}{\sqrt{2^3}} \bigotimes_{i=1}^{3} (|+\rangle |0\rangle + |-\rangle |1\rangle)_i \tag{3.14}$$

Vagyis 4 különálló párt hoztunk létre (ahol valójában elsőre egyetlen párra van szükség, így a többi kvantumbitet akár később is inicializálhattunk volna).

[8] A legalsó kvantumbit mérése nem érdekes, mert a függvényről szükséges információk a felső regiszterben vannak.

[9] Annak ellenére, hogy a legelső MBQC séma egy elegendően nagy cluster-ből indul ki. Itt a gondolatmenet mögött az ötlet, hogy szem előtt tartsa a megvalósítás lehetőségét, amely esetében nem szerencsés/-lehetséges (például dekoherencia miatt) egy-egy kvantum állapot sokáig megőrzése, ezért célszerű mindet a lehető legkésőbbi időpillanatban létrehozni.

[10] Amikor a cluster állapotok definíciójáról volt szó, akkor minden állapot $|+\rangle$-ként szerepelt. Ez valójában annyit jelent, hogy a modellben feltesszük, hogy képesek vagyunk ilyen állapotok preparálására. Továbbá a modellben a $\hat{CZ}$ kezelésénél használt σ_z Pauli-Z operátor használatával a preparációt követően elérhetjük, hogy némely kezdeti állapotunk $|-\rangle$ legyen $|+\rangle$ helyett. (Persze elképzelhető, hogy a korrekciók miatt a Pauli operátorok támogatva legyenek alapból.)



3.7. ábra. A kiindulási állapotom a Deutsch-Jozsa algoritmus implementálásához, a mérés-alapú modellben.

Következő lépésként az első kvantumbitet mérjük meg a $\hat{\sigma}_x$ bázisán, vagyis alkalmazzuk a korábbi szakaszban tárgyalt teleportációs protokollt[11], és állítsuk elő a 2-es kvantumbiten a $\hat{H}\hat{\sigma}_z^m |-\rangle$ állapotot. Ez valójában annyit jelent, hogy $m = 0$ esetén $|1\rangle$-et, $m = 1$ esetén, pedig $\hat{H}\hat{\sigma}_z |-\rangle = |0\rangle$-t kapunk. A továbbiakban a $|1\rangle$-es állapotra koncentrálhatunk, amennyiben nem ez a helyzet, akkor csak megismételhetjük az eljárást, amíg azt nem kapjuk[12] (erre felállítható egy geometriai eloszlású valószínűségi váltózó, és a várható érték 2 lesz, illetve $\mathbb{P}$(10-nél több)=1-$\sum_{n=1}^{10} = (\frac{1}{2})^{10}$, amely már elég kicsi).

Eddig a pontig nem volt szó arról, hogy mi a helyzet az orákulummal. A kapu-alapú modellben láttuk, hogy az egy-egy fajta orákulumhoz más-más áramkör tartozott, persze mindkét esetben az algoritmust végrehajtóként úgy kell erre tekinteni, mint egy "fekete doboz"-ra. Ettől függetlenül érdemes beszélni az orákulumok megvalósításról. A mérés-alapú modell esetében az orákulumok implementálhatóak kontrollált Pauli-Z műveletekkel illetve azok hiányával. Elképzelhető úgy, hogy előállítjuk az állapotot, amiről eddig volt szó, majd valakinek odaadjuk a kvantumbiteket aki végrehajtja az orákulumot, majd befejezzük az algoritmust és megmondjuk, hogy milyen az f függvény.

A konstans esetben ezen a ponton már csak méréseket végzünk (persze nem megfeledkezve mérések utáni korrekciókról). A $|1\rangle$ állapottal már nincs dolgunk, az összefonódott párokon egy teleportációt végrehajtva (vagyis a $|\pm\rangle$ bázisban megmérve az első kvantumbitet) megkapjuk, hogy a maradék kvantumbitek mind a $\hat{H}\hat{\sigma}_z^{m_i} |+\rangle$ állapotban vannak, ahol m_i az i.-dik pár első kvantum bit mérésének az eredménye. Ekkor a szükséges korrekciók után, a számítási bázisban mérve $|0\rangle |0\rangle |0\rangle$ állapotot kapjuk.

A kiegyensúlyozott esetben érdemes feljegyezni, hogy a $\hat{CZ} |0\rangle |\pm\rangle = |0\rangle |\pm\rangle$ és $\hat{CZ} |1\rangle |\pm\rangle = |1\rangle |\mp\rangle$, amiből az utóbbi lesz most érdekes. Úgy folytatódik az eljárás, hogy sorra vesszük (vagy egyszerre ha ilyet enged az aktuális architektúra) az eddig nem használt összefonódott párokat, és mindre végrehajtunk egy $\hat{CZ}$-t ahol az egyik operandus a $|1\rangle$ állapot, így használjuk a fent említett összefüggést. Ezek után a $|1\rangle$-re már nem lesz szükség többet, itt ez hasonló szerepet töltött be, mint a kapu-alapú modell esetében a

[11] Ahogy arról ott is volt szó, ennek a protokollnak ebben a modellben nagy szerepe van.

[12] Persze amennyiben $|1\rangle$ állapot preparálható, a probléma nem lép fel, továbbá egy Pauli-X korrekció is használható.

legalsó kvantumbit, az eredmény állapot:

$$\frac{1}{\sqrt{2^3}} \bigotimes_{i=1}^{3} (|-\rangle |0\rangle + |+\rangle |1\rangle)_i \tag{3.15}$$

Ezt követően ismét mérjük meg páronként az első kvantumbitet a $|\pm\rangle$ bázisban, $m_i = 0$ esetében $|1\rangle$-es állapot marad és $m_i = 1$ esetében egy $\hat{\sigma}_z$ Pauli-Z byproduct megjelenik, így $|0\rangle$ jelenik meg amit megfelelően korrigálni kell. Mivel itt ismét a teleportációs protokollt használtunk a kimeneti állapot minden esetben $\hat{H}\hat{\sigma}_z^{m_i} |-\rangle$, vagyis ezek után a számítási bázisban mérve kiolvasható a kimenet. Minden kvantumbit a $|1\rangle$-es állapotban van (itt figyelembe véve a lehetséges byproductokat). Tehát összehasonlítva a konstans esettel egyértelműen eldönthető az algoritmus egyszeri lefuttatásával, hogy milyen típusú a függvény.

Könnyen látszik, hogy az algoritmus tetszőleges n-re működni fog, csak természetesen több kvantumbit-párra lesz szükség.

3.4.3. Folytonos változójú modell

Folytonos változó esetén, mint már korábban is, a már megszokott módon lehetséges egy diszkrét rendszer folytonosba való ágyazása, ily formán megoldva a feladatot. Azonban probléma (így az algoritmus is) megfogalmazható oly módon, hogy működjön "natívan" folytonos változó esetében is. További érdekessége, hogy folytonossága miatt legrosszabb esetben a klasszikus algoritmushoz képest *végtelenszeres* gyorsítást eredményez.

Hasonlóan a [12]-ben ismertetett problémával közelítem meg a kérdést, ugyanakkor konkrétan megfogalmazva az alaphelyzetet és lehetséges függvényeket definiálva.

Legyen a kérdés megfogalmazva folytonos változóra a következő. Keresünk egy $f(x) \to \{0, 1\}$ bináris értékű függvényt, amelynek értelmezési tartománya $x \in]-1; 1]$, és mint diszkrét esetben is tudjuk, hogy $f(x)$ vagy mindig ugyanazt az értéket veszi fel, ekkor ugye *konstans*-ként hivatkozunk rá, vagy a bemenetek felére 0 a másik felére pedig 1 az értéke, ekkor *kiegyensúlyozott* lesz. Itt érdemes visszacsatolni a korábbi megállapításhoz miszerint a legrosszabb esetben a klasszikus algoritmus végtelen értére számolja $f(x)$-et (vagyis nem terminálódik), hiszen x most egy kontinuum része így az értékek "fele" is végtelen sokat jelent. Ezzel szemben a kvantumos megoldást ugyancsak egyszer kell lefuttatni.

Az alapállapot 2 $\hat{x}$ sajátértékből áll, $|\psi_0\rangle = |x_0\rangle \otimes \left|\frac{\pi}{2}\right\rangle$. Ezek után alkalmazunk egy-egy $\hat{H}$ kaput az állapotokon (irodalmakban [12][18] $\hat{\mathcal{F}}$: Fourier-kapunak is nevezik, melyet a diszkrét esetben is adoptálhatnánk, hiszen egy Hadamard transzformáció éppen úgy viselkedik, mint egy egy-bites QFT, kvantum Fourier-transzformáció)[12]:

$$|\psi_1\rangle = \hat{H} |x_0\rangle \hat{H} \left|\frac{\pi}{2}\right\rangle = \frac{1}{\pi} \int\int dy dx e^{2ix_0 x + i\pi y} |x\rangle |y\rangle \tag{3.16}$$

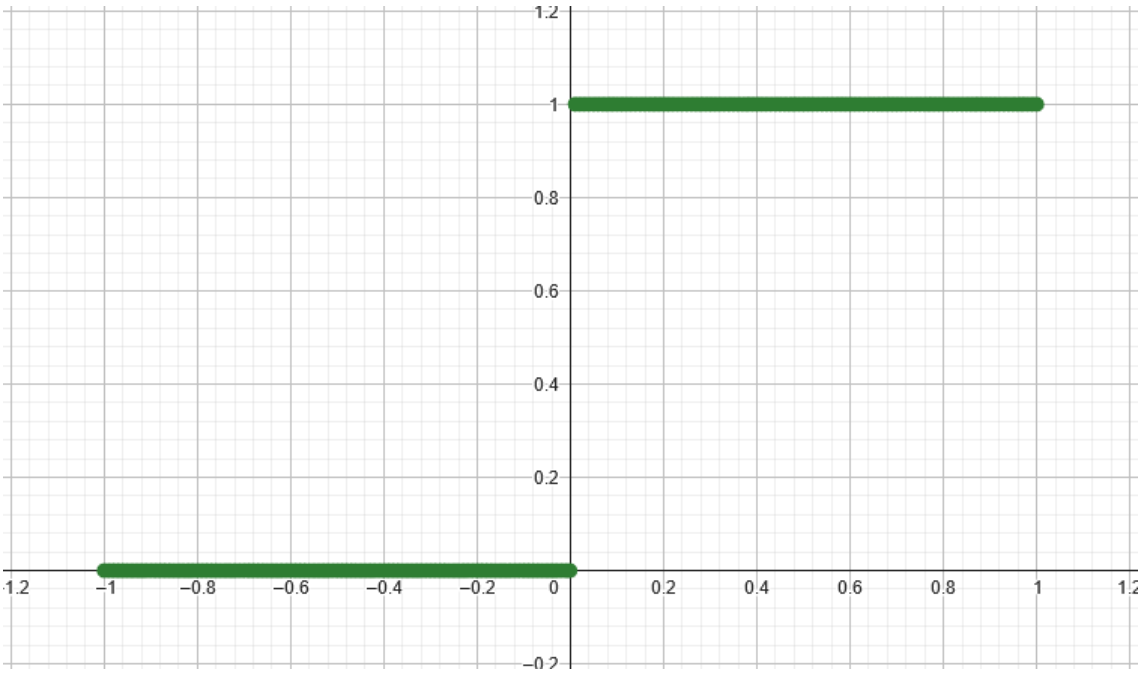
Továbbá az orákulumtól folytonos esetben hasonló működést várunk el, mint a diszkrét esetben $\hat{U}_f |x\rangle |y\rangle = |x\rangle |y + f(x)\rangle$. Illetve használva hogy $\hat{U}_f |x\rangle \hat{\mathcal{F}} \left|\frac{\pi}{2}\right\rangle = (-1)^{f(x)} |x\rangle \hat{\mathcal{F}} \left|\frac{\pi}{2}\right\rangle$[12], az állapot:

$$|\psi_2\rangle = \frac{1}{\pi} \int\int dx dy e^{2ix(x_0 - y)} (-1)^{f(x)} |y\rangle \hat{\mathcal{F}} \left|\frac{\pi}{2}\right\rangle \tag{3.17}$$

Végül pedig a méréseknél tárgyalt projektor definícióját használva folytonos esetben, mérünk egy $|x_0\rangle$-ra projektáló operátor segítségével az első állapoton. Kiderül, hogy csak akkor lehet a kimenetel $|x_0\rangle$, ha $f(x)$ konstans, és ha nem az, akkor viszont $|x_0\rangle$-tól különbözőt mérünk.

A kérdéses függvények megvalósításával kapcsolatban igazából (mint a korábbi modellek esetében is) a kiegyensúlyozott esetre érdemes kitérni. Itt a feladat kezdeti megfogalmazásának megfelelő függvény:

$$f(x) = \begin{cases} \frac{sign(x)+1}{2} & \text{ha } x \neq 0 \\ 0 & \text{ha } x = 0 \end{cases} \tag{3.18}$$



3.8. ábra. $f(x)$ függvényem a kiegyensúlyozott esetben.

3.4.4. Összegzés

Annak ellenére, hogy a Deutsch-Jozsa algoritmus nem tartamaz praktikus problémára megoldást, modellek összehasonlítására teljesen alkalmas. Az egyes implementációk során szembetűnőek az alapvető megközelítési különbségek, mint például a kapu-alapú modellben az orákulum megvalósítása unitér operátorokkal történik, míg a mérés-alapú esetében mérések végrehajtásával tehetjük meg ugyanezt.

Érdekes, hogy az egyszerűbb megözelítés érdekében valóban célszerű a kapu-alapú modellel kezdeni, illetve aztán a későbbieket ahhoz hasonlítani, vagy azt megvalósítani megfelelő hozzárendelések segítségével (például folytonos változóba ágyazással).

Másik fontos észrevétel, hogy a mérés-alapú modellben a nagy kihívás a megfelelő cluster struktúra felírása, amely ha az algoritmus elegendően komplex, akkor valóban nem egyszerű feladat. Ugyanakkor az orákulumok implementálása ezek után már kevesebb művelettel megoldható, mint más modellek esetében.

A folytonos modell esetében a feladat átfogalmazása működőképes volt, amely a korábban vizsgált eljárásokhoz lépest, egy kifelyezetten érdekes tapasztalat. Ennek persze meg van az a szépség hibája, hogy az orákulum megalkotása nehéz feladat, és emiatt érdemes volt elvonatkoztatni attól a résztől. Illetve még mindig fent áll, hogy a folytonos esetben idealizált(nem normálható) állapotokkal dolgoztunk. Ennek megfelelően a *végtelenszeres* gyorsítás csak az ideális esetben megfigyelhető, amikor tudunk a $|x_0\rangle$ állapotra pontosan mérni.

3.5. Grover algoritmus

Hasonlóan az előző algoritmushoz, a Grover algoritmus (néha kvantumos keresési algoritmusnak is hivatkoznak rá) is egyike a legkorábban formalizált kvantumalgoritmusoknak, és nagyban hozzájárult a kvantumalgoritmusok népszerűségének növeléséhez.

Az algoritmus ismét egy szignifikáns gyorsítást eredményez a legjobb klasszikus megoldással szemben. Az eljárás gyakorlatilag egy keresési feladatra ír le megoldást, rendezetlen adatbázisban. Klasszikus esetben a megoldáshoz csak lináris keresés alkalmazható, hiszen a rendezettség hiányában nem használhatóak jobb eljárások, mint például bináris keresés. Könnyen belátható, hogy emiatt egy keresett elemet átlagosan $O(\frac{N}{2}) = O(N)$ (komplexitását vizsgálva) időben találunk meg, vagyis az elemek számában lineárisan. Ugyanakkor a kvantumalgoritmus lehetővé teszi a feladat elvégzését csupán $O(\sqrt{N})$ időkomplexitással, ezzel egy gyorsabb megoldást adva.

Fontos, hogy Grover algoritmusa is egy orákulum alapú eljárás. Ez praktikusan annyit jelent, hogy létezik egy olyan operátorunk, amelynek a képessége, hogy $|i\rangle \to (-1)^{f(x_i)} |i\rangle$, ahol x_i az i indexen található érték. Vagyis az operátor megjelelöli a keresett elemet. Persze felmerülhet a kérdés, hogy akkor ez nem azt jelenti, hogy már eredetileg ismerjük, amit keresünk? Ennek megválaszolásához vegyük az NP-beli problémákat példának, ugyanis ott is valami hasonló a helyzet. A megoldás megtalálása nem egyeszerű, azonban ha már van egy megoldás jelöltem, akkor "könnyen" ellenőrizhetem annak helyességét.

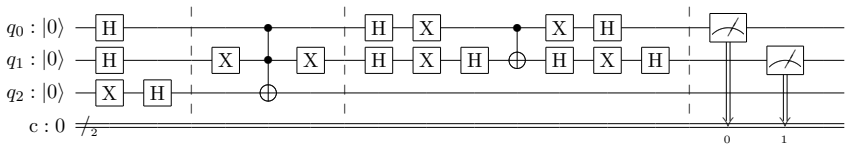
Az algoritmus felbontható 2 lépésre, először a keresett elem megjelölése (ez a lépés történik egy orákulum segítségével), majd amplitúdó erősítés, ezt végzi a *Grover diffuser* operátor:

$$\hat{OP}_{diff} = 2 |s\rangle \langle s| - \mathbb{I} \text{ , ahol } |s\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \tag{3.19}$$

Az egész eljárás alapvetően olyan "receptet" ír le, amely más kvanutmalgoritmus esetében is hasznos lehet. A keresett elemet (amelyet mérést követően megtalálni szeretnénk) az orákulum megjelöli, méghozzá úgy, hogy a hozzátartozó valószínűségi amplitúdónak az előjelét negatívra állítja, míg a nem kívánatos elemeknek a valószínűségi amplitúdója pozitív lesz, ez alapvetően egy tükrözésként képzelhető el, a keresett elem esetében. Ezután a diffuser operátor egy másik tükrözést hajt végre, amely megnöveli a keresett elemhez tartozó amplitúdót a többi elem kárára. Ez azt jelenti, hogy ezen lépés után, ha elvégeznénk egy mérést, akkor nagyobb valószínűséggel kapnánk meg a keresett eredményt, mint a műveletek előtt, illetve kisebb valószínúséggel kapnánk valamelyik nem kívánt tagot.

3.5.1. Kapu-alapú modell

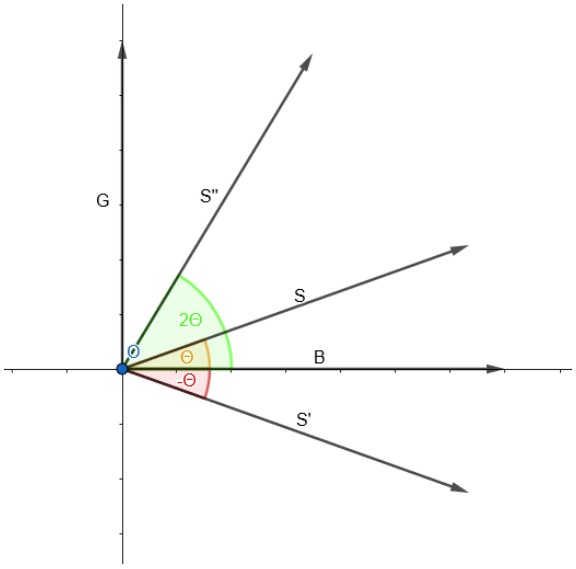
Orákulummal működő algoritmusról van szó ismét, ezért az a Deutsch-Jozsa-hoz hasonlóan definiálnunk kell az algoritmus vázát, és az orákulum külön kezelendő. Mint abban a szakaszban is ugyanakkor, itt is megtehetjük, hogy mutatunk lehetőséget az orákulum implementációjára, de fontos megjegyezni, hogy ez csak tesztelési célból érdekes. Az algoritmus 3-bites implementációja a 3.9-es ábrán látható. Amennyiben mondjuk a $|x_0\rangle$ állapothoz tartozó amplitúdót szeretnénk növelni, akkor az $\mathbb{I} - 2 |x_0\rangle \langle x_0|$ orákulum megfelelő választás.



3.9. ábra. 2-bites Grover algoritmus implementációm (egy lehetséges orákulummal), a kapu-alapú modellben. A harmadik kvantumbit a teszt orákulum implementációjához szükséges, valójában emiatt nem hajtok végre mérést rajta.

Az algoritmusnak létezik, egy szemléletes geometriai interpretációja, méghozzá, hogy a 2 tükrözésen keresztül növeljük meg a keresett elemhez tartozó valószínűségi amplitúdót. Ezt szemlélteti a 3.10-s ábra.

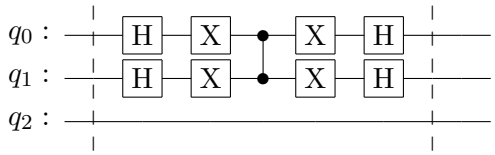
Ebben a modellben ismét elegendő az algoritmus egyes lépéseit végrehajtani, ahogy azok formulálva vannak, kezdőállapotok preparálása, orákulum és Grover operátor végrehajtása megfelelő lépésszer, majd mérés.



3.10. ábra. A Grover algoritmus geometriai interpretációját szemléltető ábra. Először a kezdeti állapotot ”S” tükrözzük a rossz állapotokra ”B”, majd az így kapott ”S’”-őt az eredeti ”S’”-re, megkapva ”S””-őt, amely a kívánt ”G” jó állapothoz közel van. (Jó és rossz abban az értelemben vesszük, hogy a helyes eredményt kapnák-e méréskor, ha az adott állapotba ugrana be a hullámfüggvény.)

3.5.2. Mérés-alapú modell

A mérés-alapú modell tárgyalásához először alakítsunk az algoritmus leírásán (a kapu-alapú modellbeli leírást alkalmazva, annak érdekében, hogy könnyebb legyen az algoritmus átfogalmazása). Ehhez először érdemes a Grover operátort felírni olyan formában amely könnyeben implementálható a mérés-alapú modell keretein belül. Az operátorban



3.11. ábra. 2-bites Grover operátor implementációm, a kapu-alapú modellben, az előző szakaszhoz képest átfogalmazva annak érdekében, hogy könnyebben össze lehessen vetni a mérés-alapú párjával.

megjelenő $C\hat{N}OT$ kapu esetében a target kvantumbitnél az operátor "szendvicselve" van 2 Hadamard-kapuval, és mivel $\hat{H}^\dagger = \hat{H}$, ezért ez éppen egy unitér evolúciónak felel meg, vagyis $\hat{H}^\dagger \hat{\sigma}_x \hat{H} = \hat{\sigma}_Z$. Ez azért szerencsés, hiszen, így a $C\hat{N}OT$ helyett használható kontrollált Pauli-Z. A kapott operátort mutatja be a 3.11 ábra.

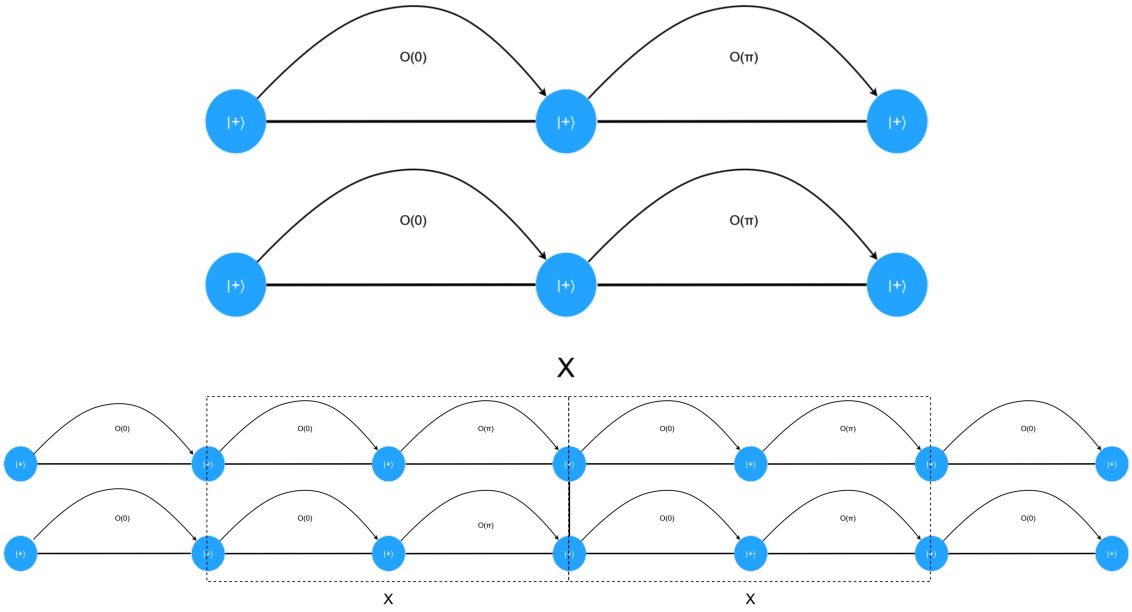
Ez a művelet azért szerencsés, mert az így kapott Grover operátorban már csak olyan komponensek szerepelnek, amelyeket megtalálhatunk a mérés-alapú modellben, így könnyebben implementálva az operátort. Konkrétabban a Hadamard-kapuk megvalósításához elegendő egy mérés (és lehetséges Pauli-korrekció) a $|\pm\rangle$ bázisban, egy bemeneti $|\psi\rangle$ állapoton. Az $\hat{\sigma}_x$ kapu megvalósítása érdekében 2 mérésre lesz szükségünk. Az első mérés megint a $|\pm\rangle$ bázisban, ezzel egy Hadamard-transzformációt végrehajtva az állapoton. A második méréshez a $\hat{O}(\phi) = \cos(\phi)\hat{\sigma}_x + \sin(\phi)\hat{\sigma}_y$ obszervábilis szerint hajtjuk végre a mérést, és ahogy az az általános operátorral foglalkozó szakaszban látható volt, ekkor az állapot $\hat{H}e^{i\frac{\phi}{2}\hat{\sigma}_z}|\psi\rangle$-re módosul, a feltételes korrekciót egyszerűség kedvéért most elhagyva. A két mérés után vizsgálhajtuk a teljes műveletet:

$$\hat{H}e^{i\frac{\phi}{2}\hat{\sigma}_z}\hat{H} = \hat{H}(\cos(\frac{\phi}{2})\mathbb{I} + i\sin(\frac{\phi}{2})\hat{\sigma}_z)\hat{H} = (\cos(\frac{\phi}{2})\mathbb{I} + i\sin(\frac{\phi}{2})\hat{\sigma}_x) = e^{i\frac{\phi}{2}\hat{\sigma}_x} \tag{3.20}$$

Ahol kihasználtam, hogy $e^{i\frac{\phi}{2}\hat{\sigma}_z}$ unitér, illetve, hogy $\hat{H}\hat{\sigma}_z\hat{H} = \hat{\sigma}_x$ teljesül. Ekkor könnyen látható, hogy így az X tengely körüli forgatáshoz jutottunk, $\phi = \pi$ választással az operátor éppen $\hat{\sigma}_x$-et hajt végre. Továbbá a $\hat{CZ}$ műveletet is támogatja a mérés-alapú modell, tehát a teljes Grover diffuser operátor megvalósítható, a következő mérési sorozattal és $\hat{CZ}$-vel:

$$\hat{O}_i(0)\hat{O}_i(\pi)\hat{O}_i(0)\hat{CZ}_{1,2}\hat{O}_i(\pi)\hat{O}_i(0)\hat{O}_i(0) \text{ ahol } i \in \{1,2\} \tag{3.21}$$

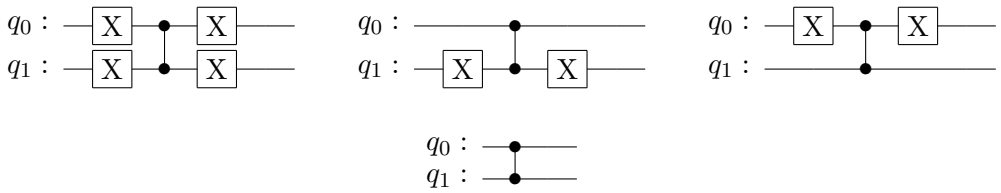
Ahol a $\hat{O}(\phi)_i$ az adott obszervábilis szerinti mérést jelöli, az i-dik kvantumbiten. Az operátor felépítését a 3.12 ábra szemlélteti.



3.12. ábra. Első kép az $\hat{\sigma}_x$ operátor megvalósítása, amelyet az átláthatóság kedvéért a második képben 'X' felirattal jelöltem a logikailag egy műveletet megvalósító részeket. A második ábrámon a teljes 2-bites Grover diffuser operátor implementációm látható, a mérés-alapú környezetben.

Innen a teljes algoritmus implementációja a 3.13 ábrán látható.

3.13. ábra. Grover algoritmus mérés-alapú környezetbeli implementációját szemléltető ábrám. Mivel a struktúra már viszonylag kis (2-bites) esetben is elég hosszú, ezért azzal az absztrakcióval éltem, hogy a logikailag egybe tartozó részeket egy darab egységes elemként ábrázoltam. A Grover diffuser operátort a korábban ismertetett ábra szemlélteti, illetve a továbbiakban az orákulumról is lesz szó.



3.14. ábra. A 2-bites Grover algoritmushoz használható orákulum implmentációim, a kapu-alapú modellben szemléltetve.

Érdemes az (teszt)-orákulumról is egy pár szóban említést tenni, ehhez egy pillanatra visszatérek a kapu-alapú modell formalizmusához. Minden megjelölés (orákulum fajta) megvalósítható 2 kvantumbiten is, az ezekhez tartozó megoldások a 3.14-os ábrán láthatóak. Most amennyiben ugyanazt szeretnénk megvalósítani, amelyet az előző szakaszban a kapu-alapú modell esetében, akkor az q_1-es kvantumbiten kell végrehajtani $\hat{\sigma}_x$ műveleteket kizárólag (a 3.14-os ábrán a jobb felső képen látható). Vagyis a teljes megoldáshoz preparálni kell clustert (mint korábban ez történhet több szakaszban/az algoritmus folyamatában), végre kell hajtani az orákulumot, majd folytatódik a diffuser operátorral a végrehajtás, majd a végeredmény kiolvasása. *Megjegyzés: Ebben a modellben kezdetben* $|+\rangle$ *állapotokat hozunk létre, emiatt jelen esetben nincsen szükség számításokra az orákulum előtt, a számítás kezdődhet annak végrehajtásával.*

3.5.3. Folytonos változójú modell

Folytonos esetben ismét több lehetőség is van az algoritmus megvalósítására. Egyik lehetőség, hogy a folytonos változóba kódolunk diszkrét változót (mint például GKP kódolás) és az 3.1 táblázat alapján végrehajtuk az algoritmust. Ezzel szemben lehetséges megoldás a Deutsch-Jozsa algoritmusnál használt módszer, hogy az algoritmust átfogalmazzuk és folytonos változójú problémaként kezeljük. Erre a megközelítésre is találhatunk példát [13].

3.5.4. Összegzés

A Grover algoritmus egy fontos tagja az eddig ismert algoritmusok halmazának, továbbá praktikus értelemben is hasznos. Ennek megfelelően több részből tevődik össze, így komplexebb, mint az eddig tárgyalt eljárások.

Amit az eljárás küldönböző implementálásaihoz érdekes kiemelni, hogy a kapu-alapú modell megfelelő átfogalmazásával az algoritmus átírható volt abból a megoldásból, a mérés-alapú modellbeli implementációba, hasonlóan mint a korábban is említett folytonos változós megoldások esetén. Továbbá az átírásban kölcsönös megfeleltetések írhatók fel, amelyek segítségével automatizálható a feladat. Ez olyan következménnyel járhat, hogy lehetőséget nyújt, a kapu-alapú modellbeli tervezésre, majd egy fordítási eljárás segítségével a mérés-alapú modellben felírjuk a megoldást. Ugyanakkor meg kell jegyezni, hogy a számítások során nem foglalkoztunk a lehetséges szükséges korrekciókkal, amelyek természetesen módosíthatnak a végrehajtás menetén.

Továbbá szeretném nyomatékosítani, hogy az algoritmus működését, leírását többször a mérés-alapú modellbeli tárgyalás során is a kapu-alapú modellbeli ábrázolással tettem meg. Természetesen ez a döntés praktikus volt, hiszen így könnyebben lehetett követni az egyes állapotok megváltozását, ugyanakkor ezen megoldás használatával eltekintettem például attól a ténytől, hogy az egyes operátorokat valójában mérésekkel lehet megvalósítani,

és a végeredmény ugyan meg kell, hogy egyezzen, valójában nem ugyanazt a kvantumbitet használom az eljárás végén, mint amelyikkel kezdtem a feladat megoldását, hiszen azt már megmértem korábban. Tehát ebben az értelemben ezt a megoldást tekinthetjük egyfajta absztrakciós lépésnek, hiszen azzal, hogy néhol nem a mérés-alapú modellbeli ábrázolást használtam egyszerűbb volt leírni az algoritmust.

4. fejezet

Kommunikáció kvantumszámítógépek között, mérés-alapú teleportációval

4.1. Elméleti felépítés

A számítási modellek tanulmányozásával, és azok tulajdonságainak a figyelembevételével lehetséges a következő (elosztott kvantumszámítások elvégzésére is alkalmas) kommunikációs architektúra, amelyben az egyes kvantumszámítógépek (csomópontok) képesek teleportációs protokollal kommunikálni egymással.

Az eljárás lényege, hogy képes legyen egy tetszőleges (akár ismeretlen) kvantum állapotot, két fél között eljuttatni, a teleportációs algoritmus segítségével, azonban a mérés-alapú környezetben, úgy hogy az a kommunikáció előtt és után használható legyen, mint kvantum bit számításokhoz. A két kommunikáló fél legyen Alice és Bob, és tegyük fel, hogy mind a ketten el akarnak végezni egy kvantumszámítást, úgy, hogy Bob bemenetként Alice eredményét akarja használni, azonban kvantumos bemenetre van szüksége (például gondolhatnánk egy elosztott rendszerre). Ehhez a mérés-alapú számítási modellt használnák, mind a kommunikációhoz, mind a számításokhoz. Példaként, vehető egy bites kimenet, illetve bemenetre. Kezdetben Alice és Bob megosztozik egy 2 kvantumbites cluster állapoton:

$$|\phi\rangle = \hat{CZ}\,|+\rangle_1\,|+\rangle_2 = \frac{|0\rangle_1\,|+\rangle_2 + |1\rangle_1\,|-\rangle_2}{\sqrt{2}}$$

Ezek után Alice elvégzi a megfelelő számítást, amelyet megvalósítani szeretett volna, és legyen a kimeneti állapota valamilyen tetszőleges $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ állapot, eltárolva egy kvantumbitben. Ekkor Alice ezt az állapotot először az általa birtokolt összefonódott kvantumbitre fogja teleportálni. Először ezt a kvantumbitet hozzá kell fonódtatnia a cluster-höz egy $\hat{CZ}$ kapuval:

$$\hat{CZ}_{\psi,\phi_1}\,|\psi\rangle\,|\phi\rangle = \hat{CZ}_{\psi,\phi_1}\frac{\alpha\,|0\rangle\,|0\rangle_1\,|+\rangle_2 + \alpha\,|0\rangle\,|1\rangle_1\,|-\rangle_2 + \beta\,|1\rangle\,|0\rangle_1\,|+\rangle_2 + \beta\,|1\rangle\,|1\rangle_1\,|-\rangle_2}{\sqrt{2}} =$$

$$\frac{\alpha\,|0\rangle\,|0\rangle_1\,|+\rangle_2 + \alpha\,|0\rangle\,|1\rangle_1\,|-\rangle_2 + \beta\,|1\rangle\,|0\rangle_1\,|+\rangle_2 - \beta\,|1\rangle\,|1\rangle_1\,|-\rangle_2}{\sqrt{2}}$$

Majd Alice megméri a kimeneti kvantumbitet a $|\pm\rangle$ bázisban, aminek az eredménye praktikusan elemezhető, ha a szóbanforgó kvantum bitet először ebben a bázisban írjuk fel a $|0\rangle = \frac{|+\rangle+|-\rangle}{\sqrt{2}}$ és $|1\rangle = \frac{|+\rangle-|-\rangle}{\sqrt{2}}$ összefüggések felhasználásával:

$$\frac{|+\rangle}{\sqrt{2}}\frac{\alpha\,|0\rangle_1\,|+\rangle_2 + \alpha\,|1\rangle_1\,|-\rangle_2 + \beta\,|0\rangle_1\,|+\rangle_2 - \beta\,|1\rangle_1\,|-\rangle_2}{\sqrt{2}} +$$

$$\frac{|-\rangle}{\sqrt{2}}\frac{\alpha\,|0\rangle_1\,|+\rangle_2 + \alpha\,|1\rangle_1\,|-\rangle_2 - \beta\,|0\rangle_1\,|+\rangle_2 + \beta\,|1\rangle_1\,|-\rangle_2}{\sqrt{2}}$$

Most a mérés eredménye legyen $m_1 = 0$ $|+\rangle$ esetén és $m_1 = 1$ $|-\rangle$ esetén, ekkor az egyes lehetőségek normálást követően, a mérési eredmény függvényében:

- $m_1 = 0$ esetén:

$$\frac{\alpha\,|0\rangle_1\,|+\rangle_2 + \alpha\,|1\rangle_1\,|-\rangle_2 + \beta\,|0\rangle_1\,|+\rangle_2 - \beta\,|1\rangle_1\,|-\rangle_2}{\sqrt{2}}$$

- $m_1 = 1$ esetén:

$$\frac{\alpha\,|0\rangle_1\,|+\rangle_2 + \alpha\,|1\rangle_1\,|-\rangle_2 - \beta\,|0\rangle_1\,|+\rangle_2 + \beta\,|1\rangle_1\,|-\rangle_2}{\sqrt{2}}$$

Alicenak ekkor már csak annyi feladata maradt, hogy az állapotot elteleportálja Bobnak (a lehetséges korrekciókat is elküldve), ehhez egy újabb mérést végez, ismét a $|\pm\rangle$ bázisban, amelynek tárgyalásához írjuk át megint a megmérendő kvantumbitet ebbe a bázisba (illetve a másikat a számítási bázisba, amely későbbi diszkusszióban praktikus lesz):

- $m_1 = 0$ esetén:

$$|+\rangle\,\frac{\alpha\,|0\rangle + \beta\,|1\rangle}{\sqrt{2}} + |-\rangle\,\frac{\alpha\,|1\rangle + \beta\,|0\rangle}{\sqrt{2}}$$

- $m_1 = 1$ esetén:

$$|+\rangle\,\frac{\alpha\,|0\rangle - \beta\,|1\rangle}{\sqrt{2}} + |-\rangle\,\frac{\alpha\,|1\rangle - \beta\,|0\rangle}{\sqrt{2}}$$

A mérés utáni normalizált állapotok pedig írhatóak:

- $m_1 = 0$; $m_2 = 0$ esetén:

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

- $m_1 = 0$; $m_2 = 1$ esetén:

$$\alpha\,|1\rangle + \beta\,|0\rangle = \hat{\sigma}_x\,|\psi\rangle$$

- $m_1 = 1$; $m_2 = 0$ esetén:

$$\alpha\,|0\rangle - \beta\,|1\rangle = \hat{\sigma}_z\,|\psi\rangle$$

- $m_1 = 1$; $m_2 = 1$ esetén:

$$\alpha\,|1\rangle - \beta\,|0\rangle = \hat{\sigma}_x\hat{\sigma}_z\,|\psi\rangle$$

Illetve a végállapotokat kompakt módon is írhatjuk, mert amikor a $|\pm\rangle$ bázisban mérünk, akkor $m = 0, 1$ eredmény mellett a mérés előtti állapot jelenik meg a megmaradt összefonódott páron, egy $\hat{H}\hat{\sigma}_z^m$ operátorral:

$$\hat{H}\hat{\sigma}_z^{m_2}\hat{H}\hat{\sigma}_z^{m_1}\,|\psi\rangle$$

Egy kicsit jobban megvizsgálva, látszik, hogy ez az eredmény konzisztens a korábbi mérési erdemény és állapot párosokkal. Alicenak még szükséges lesz a mérési eredményeket Bobnak továbbítani, ehhez viszont csak egy klasszikus csatornára lesz szüksége. Ezek után Bob már elvégezhet tetszőleges kvantum algoritmust, az Alicetól kapott bemenettel.

Az eljárásnak van néhány fontos tulajdonsága, amelyeket érdemes megemlíteni:

- A számítás során Alice és Bob nem ismerik a másik által implementált algoritmust, vagyis ebben az értelemben egymástól függetlenül dolgoznak.
- Kvantumos információ átadásról beszélünk, hiszen Bob kvantum állapotokat kap Alicetól, a klasszikus csatorna csak ezek kezeléséhez kell, de amelyeket használ azokra gondolhat mint $\hat{H}\hat{\sigma}_z^{m_i} |\psi\rangle_j$, ahol j az j-dik kvantumbit és m_i az i-dik mérési eredmény.
- Mivel Alice és Bob közötti kommunikácó kvantumos része teleportációval történik, ezért ők lehetnek tetszőlegesen messze egymástól, és használhatják a protokollt, mert nem szükséges a kvantum állpotok továbbítása valamilyen közvetítő médiumon keresztül, így az érzékeny kvantum állapotokon az esetleges csillapítással kapcsolatos problémák nem lépnek fel, és a dekoherencia sem játszik közbe.
- Mivel a mérés-alapú modell univerzális modell, ezért, ha Alice és Bob ezt használják az algoritmusaik megvalósításához, akkor így a kommunikációjukhoz is azt használva egységesen valósul meg a számítás és kommunikáció.
- Az eljárás használható elosztott kvantumszámítási rendszerek megvalósításához, hiszen ha 2 félről többre kiterjesztjük az eljárást, akkor csak annyi változik hogy lesznek akik betöltik Alice és Bob szerepét is.
- Ugyanakkor az eljárás hátránya, hogy vagy kvantummemória szükséges hozzá, hiszen a megosztott, összefonódott párokat Alicenak és Bobnak is el kell tárolnia addig, amíg nem végeznek vele műveleteket, vagy folyamatosan generálnunk kell friss összefonódott párokat, és meg kell szervezni Alice és Bob szinkronitását.

4.2. Megvalósítási lehetőségek

Kommunikácós rendszerekben foton alapú megoldásokkal gyakran lehet találkozni, ennek az infrastruktúrája már az elmúlt években kialakult. Továbbá, optikai kvantumszámítógépek esetében a mérés-alapú modell használata jó választás, ezen rendszerek alkalmasak ennek a számítási modellnek a megvalósítására. Vagyis teljesen optikai megoldással létrehozható lehet, egy olyan rendszer, amelyben lehetséges kvantumszámítások elvégzése, az egyes kvantumszámítógépek közötti kommunikáció (akár a számítást elosztva végezve).

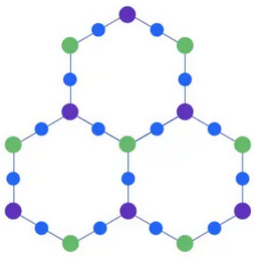
Az eljárásban van lehetőség kisebb módosításokra, annak érdekében, hogy az aktuális megvalósítás könnyebb legyen. Ilyen megoldás lehet például, ha összefonódott fotonokat generálunk folyamatosan, és bizonyos időközönként eldobjuk a fel nem használtakat. Ez a művelet azért lehet szükséges, mert az egyes fotonokat nem lehet sokáig megtartani, így azok hosszó ideig nem képesek erőforrásként szolgálni, időközönként cserélni kell őket. Ez úgy nézne ki, hogy amíg Alice és Bob között kapcsolat van, addig egy forrás összefonódott párokat oszt meg, amik egy (előre meghatározott) ideig Alice és Bob rendszerében maradnak. Ha Alice ez idő alatt végez a feladatával, akkor elvégzi a teleportációt, és a byproductokhoz szükséges biteket elküldi Bobnak, aki elkezdi a saját számítását a megkapott inputtal. Amennyiben Alice nem végez a feladattal, eldobja a lejárt összefonódott párját, nem küld Bobnak semmit a klasszikus csatornán, amiből Bob is tudja, hogy nem történt mérés amikor lejár az idő, és ő is eldobja a saját párját. Ezzel a megoldással még egy dologra kell figyelni, hogy mekkora a klasszikus információ áramlásának a sebessége

Alice és Bob között, mert ha Alice későn küldi az eredményt, akkor Bob már lehet eldobja a saját kvantumbitjét. Emiatt Alice választ a csatorna paramétereinek megfelelő határt amelyet egy összefonódott pár lejártának vége előtt megtart, és amennyiben nem lenne elég ideje megérkezni az eredményeknek majd csak a következő párral küldi.

5. fejezet

Példák fizikai megvalósításokra

5.1. IBM kvantumszámítógépei



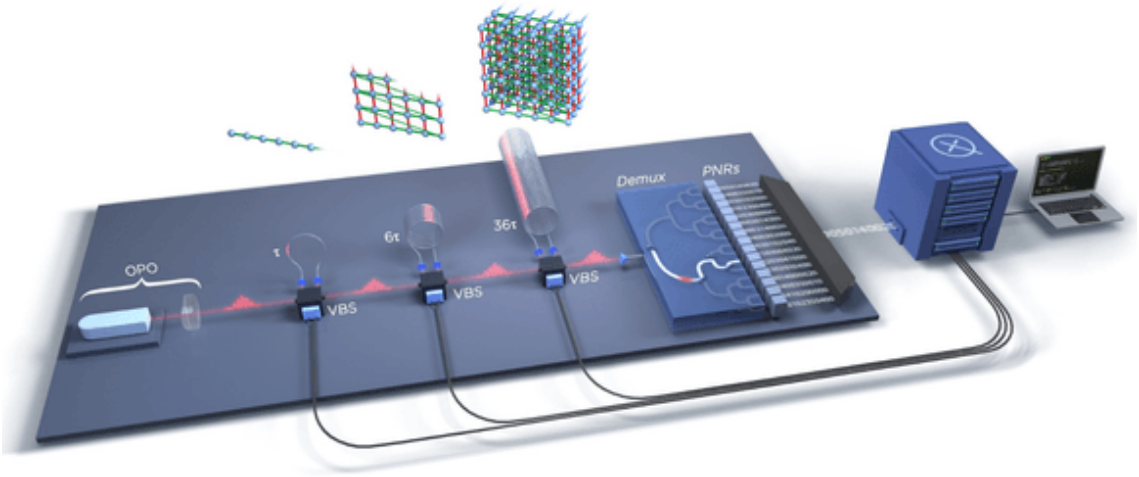
5.1. ábra. IBM szupravezető kvantumszámítógépeinek topológiáját szemléltető ábra, a gyártó blog-jából.

Az IBM kvantumszámítógépei szupravezető technológiát alkalmazva működnek, vagyis a korábban tárgyaltaknak megfelelően, az eszközöknek a működéshez nagyon alacsony hőmérséklet szükséges. Ez megnehezíti laboron kívüli használatukat.

Ezen típusú kvantumszámítógépek, támogatját a kapu-alapú modellt, diszkrét változóval, hiszen a két legalsó energia szint használható, mint kitüntetett állapotok, és nem ekvikvantált energia szintek miatt, lehetséges, hogy egy-egy rendszer ne kerüljön magasabb gerjesztett állapotokba. Természetesen itt is felléphetnek hibák, amelyek ezt neagtívan befolyásolják. Ugyanakkor a topológia kialakításakor fontos szerepet játszott, hogy lehetőség legyen hibajavításra, így használhatóak különböző stabilizátor kódolások.

Az IBM kvantumszámítógépei programozhatóak a kapu-alapú modellt használva, így ennek a modellnek az ismerete elegendő, ezen eszközökre való fejlesztéshez. Ez előny, hiszen így ezeken a kvantumszámítógépeken leírt algoritmusok könnyen elemezhetők, vagy akár remek kiindulási pontot biztosítanak, egy másik platformra való fejlesztés során is. Továbbá a konkrét megvalósítás el van rejtve a programozó elől (úgy értve, hogy nem szükséges ismernie, hogy milyen topológiájú az adott eszköz, vagy hogy milyen energia különbség van az alapállapot és az első gerjesztett állapot között.).

5.2. Borealis



5.2. ábra. Képen a Borealis ábrázolása, a gyártó blog-jából.

A Borealis fényforrásként egy 1550nm-es lézert használ, amely 3ns széles négyszögletes jeleket küld, 6 MHz frekvenciával [11]. Az impulzusok gyakorlatilag egy hálózaton haladnak végig, amelyben található 3, különböző értékű késleltető hurok, majd a rendszer végén fotonoszámlálók segítségével lehetséges mérés elvégzése a Fock-bázisban.

A fényforrásból érkező fény először egy összenyomó (angolul: *Squeezing*) kapun megy keresztül, amellyel előkészítjük a kvantum állapotot. Majd következik a fent említett 3 hurok. Minden hurok lehetővé teszi, hogy egymást követő kvantumbitek interakcióba lépjenek egymással, egy nyalábosztó (angolul: *Beam splitter*) segítségével, illetve előtte egy forgatásra is van lehetőség. Annyi a különbség a hurkok között, hogy más-más időbeli (fényforrástól vett kibocsátástól számítva) távolsággal rendelkező kvantumbitek léphetnek interakcióba (1, 6, és 36 egység). Ha fel akarjuk rajzolni a keletkezett kvantumbit elrendezést, akkor egy 3 dimenziós rácsot kapnánk, egy *3D cluster state*-et.

A kvantumeszköz mérés-alapú modellt használ, folytonos változóval, a lehetséges műveleteket a 5.1 táblázat foglalja össze. A folytonos változós megoldás elég természetesen adja magát foton-alapú rendszerek esetében, hiszen a megfelelő operátorok, a megfelelő felcserélési relációkkal adottak. Például a kvadratúra operátorok (korábban $\hat{x}, \hat{p}$) megfeleltethetőek elektromos mező kvadratúráinak (vagy akár amplitúdó és fázis), ezzel lehetővé téve, hogy a már létező formalizmust használja.

A használt számítási modelleknek megfelelően az univerzalitáshoz szükség lenne, arra hogy az egyes kvantumbiteken (most úgy értve hogy ezeket a folytonos változóba kódoljuk, például GKP kódolás) létre lehessen hajtani méréseket bizonyos bázisokban. Mivel a Borealis-on mérésre csak a fotonszám bázisban van lehetőség, ezért univerzális számítások elvégzése nem lehetséges.

Jelölés	Definíció	Megnevezés
$\hat{Sgate}(\mathrm{z})$	$e^{\frac{1}{2}(z^*\hat{a}^2 - z\hat{a}^{\dagger 2})}$	Összenyomó kapu
$\hat{R}(\phi)$	$e^{i\phi\hat{a}^\dagger\hat{a}}$	Forgató kapu
$\hat{BS}(\theta,\phi)$	$e^{\theta(e^{i\phi}\hat{a}_1\hat{a}_2^\dagger - e^{-i\phi}\hat{a}_1^\dagger\hat{a}_2)}$	Nyalábosztó

5.1. táblázat. Összefoglaló táblázat a Borealis-on lehetséges műveletekről.

Egy másik probléma, amire érdemes figyleni, hogy folytonos változó esetében megismert GKP kódolás nem normálható idealizált állapotokat használ, amelyeket fizikailag preparálni nem lehet. Éppen ezért a rendszerben eredetileg jelen lesz egy ebből származó pontatlanság/zaj.

6. fejezet

Összefoglalás, értékelés

Összegzésként először érdemes áttekinteni, hogy milyen témák kerültek szóba, voltak megvizsgálva. Elméleti, számítási modellek elemzése és összehasonlítása algoritmusokon kersztül, illetve 2 fizikai implementáció alapvető jellemzőinek megemlítése.

A számítási modellek esetében fontos szempont azon kívül, hogy lehetséges-e univerzális kvantumszámítás elvégzése az adott modellben (ennek a tulajdonságnak minden modell ebben a munkában megfelelt), az egyes modellek értelmezhetősége, átláthatósága. Ebben az értelemben, részben a felállítható klasszikus analógia miatt, a kapu-alapú modell bizonyul a legcélszerűbb megoldásnak. Ennek következtében elterjedtebb is, mint a másik kettő, illetve kompakt leírást ad az egyes eljárások leírására. Továbbá remekül használható más modellek jellemzésére, illetve arra, hogy megmutatható legyen más modellek univerzalitása. Vagyis algoritmusok magasabb szintű leírására a kapu-alapú modell használata célszerű.

A felhasznált erőforrások számának vizsgálata is érdekes szempont. Ebből a szempontból amire érdemes kitérni az a felhasznált kvantumbitek száma, összefonódáshoz szükséges operátor, illetve összefonódások száma. Mivel a folytonos változós modell általában nem egyedül áll, hanem valamely másik modell van beleágyazva emiatt az érdekesebb összehasonlításra a kapu-alapú és mérés-alapú modellek között van lehetőség[1].

Modell	Operátor összefonódáshoz
Kapu-alapú	$C\hat{NOT}$
Mérés-alapú	$\hat{CZ}$
Folytonos változó	$\hat{SUM}(g) = e^{-ig\hat{x}_1 \otimes \hat{p}_2}$

6.1. táblázat. Összefonódáshoz használt operátorok az egyes modellekben.

[1] Ugyanakkor kapu-alapú modellben más operátorral is megoldható, illetve használható, de általában a $C\hat{NOT}$ szolgál erre a célra, illetve az algoritmusok definiálásakor is gyakori megoldás.

Algoritmus	Műveletek száma		Mérések száma	
	Kapu-alapú	Mérés-alapú	Kapu-alapú	Mérés-alapú
Ált. 1-kvantumbit operátor	3	12	0	4
Teleportáció	6	3	2	1
Deutsch-Jozsa(n)	3n+2	4n+3/3n+3	n	n+1
Grover(2-bit)	20	38	2	19

6.2. táblázat. Összefoglaló táblázat a vizsgált algoritmusokhoz felhasznált műveletek és mérések számáról, az egyes számítási modellekben.

Algoritmus	Kvantumbitek száma		Összefonódások száma	
	Kapu-alapú	Mérés-alapú	Kapu-alapú	Mérés-alapú
Ált. 1-kvantumbit operátor	1	5	0	4
Teleportáció	3	2	2	1
Deutsch-Jozsa(n)	n+1	2n+2	0/n	n+1/2n+1
Grover(2-bit)	3	19	2	19

6.3. táblázat. Összefoglaló táblázat a vizsgált algoritmusokhoz felhasznált kvantumbitek és összefonódások számáról, az egyes számítási modellekben.

Az összefoglaló táblázatok (6.2, 6.3) vizsgálatával megjegyezhető, hogy általában a mérés-alapú modell esetében több erőforrásra van szükség, ugyanazon eljárás megvalósításához. Ettől kivétel azonban a teleportációs protokoll, amelyet a modell szinte, mint elemi műveletet alkalmaz[2]. Továbbá a műveletek jelentős része valójában a cluster állapot felépítése, illetve mérések végrehajtása, amely nem meglepő, hiszen alapvetően ezek szükségesek az egyes műveletek implementáláshoz. Ezen felül a kapu-alapú modell esetében pedig gyakran arról van szó, hogy összetettebb műveleteket is elemi módon kezel. Ebből az okból kifolyólag is tekinthető alkalmasabbnak algoritmusok tömör, kompakt leírására.

Másik fontos szempont az implementálhatóság. Ebben a kategóriában a mérés-alapú, és a folytonos változós modelleket szeretném kiemelni. A folytonos változó esetében nem meglepő, hiszen a valóság gyakran folytonos függvényekkel írható le pontosan, így egy rendszer modellezéséhez is elengedhetetlenek ilyen modellek. A mérés-alapú modellről azért érdemes beszélni implementálhatóság támogatásának szempontjából, mert alapvetően maga

[2]Ez a megállapítás nincs messze a valóságtól, hiszen elemi műveletként a mérésekre gondolhatunk, és mivel maga a protokoll elvégezhető egy méréssel, ezért gyakorlatilag elemi operáció.

a ”mérés” fogalma közel áll a megvalósításhoz (másképpen, fizikai értelemben van jelentősége). Továbbá egészen természetesen támogatja a foton-alapú megvalósításokat, ahol egy folyamatosan épülő cluster-ből lehetséges kvantumbitek kimérése, amelyekhez elér a számítás.

Mint ahogyan klasszikus tervezés esetén sem a leggyakoribb céleszköz például az Assembly, hanem magasabb szintű nyelvek, így kvantumos esetben is praktikus ily módon tenni. Ebből kifolyólag lenne célszerű egy olyan fejlesztési megoldás alkalmazása, amely a klasszikus programozáshoz hasonlít. A folyamat a gyakran alkalmazott szintes architektúrát követné. A legfelső szinten lenne egy programozási nyelv/eljárás, amelyben egy algoritmus megadása kapu-alapú modellben lenne lehetséges. A következő szint lenne a *compiler*, amely képes lenne az adott kódot fordítani, változatos architektúrákra. Ezek alatt helyezkedne el egy *driver* szint, amelynek a feladata, hogy a compiler felé kínált függvények mögé megfelelő paraméterezés mellett képes legyen a hardver felé megfelelő vezérlő jelek kiküldésére. Majd ez alatt, a legalsó szinten, maga a hardver állna.

Lehetséges jövőbeli munkaként tudom elképzelni egy működő fordító program megtervezését, amely képes egy kapu-alapú modellben implementált eljárás fordítására, mind kapu-alapú modellt követő, mind mérés-alapú modellt követő platformra.

A kutatás a Kulturális és Innovációs Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával, a 2022-2.1.1-NL-2022-00004 számú projekt finanszírozásában valósult meg.

Irodalomjegyzék

[1] Anne Broadbent – Joseph Fitzsimons – Elham Kashefi: Universal blind quantum computation. In *Proceedings of the 2009 50th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '09 konferenciasorozat. USA, 2009, IEEE Computer Society, 517–526. p. ISBN 9780769538501.
URL https://doi.org/10.1109/FOCS.2009.36. 10 p.

[2] P. Campagne-Ibarcq – A. Eickbusch – S. Touzard – E. Zalys-Geller – N. E. Frattini – V. V. Sivak – P. Reinhold – S. Puri – S. Shankar – R. J. Schoelkopf – L. Frunzio – M. Mirrahimi – M. H. Devoret: Quantum error correction of a qubit encoded in grid states of an oscillator. *Nature*, 584. évf. (2020. aug) 7821. sz., 368–372. p. URL https://doi.org/10.1038%2Fs41586-020-2603-3.

[3] Sophie Choe: Quantum computing overview: discrete vs. continuous variable models, 2022.

[4] Arne L. Grimsmo – Shruti Puri: Quantum error correction with the gottesman-kitaev-preskill code. *PRX Quantum*, 2. évf. (2021. jun) 2. sz.
URL https://doi.org/10.1103%2Fprxquantum.2.020101.

[5] Arne L. Grimsmo – Shruti Puri: Quantum error correction with the gottesman-kitaev-preskill code. *PRX Quantum*, 2. évf. (2021. Jun), 020101. p.
URL https://link.aps.org/doi/10.1103/PRXQuantum.2.020101. 20 p.

[6] Introduction to quantum photonics. https://strawberryfields.ai/photonics/concepts/photonics.html. [Hozzáférés dátuma: 2023.október.21.].

[7] D. Kienzler – H.-Y. Lo – V. Negnevitsky – C. Flühmann – M. Marinelli – J. P. Home: Quantum harmonic oscillator state control in a squeezed fock basis. *Physical Review Letters*, 119. évf. (2017. jul) 3. sz.
URL https://doi.org/10.1103%2Fphysrevlett.119.033602.

[8] P. Krantz – M. Kjaergaard – F. Yan – T. P. Orlando – S. Gustavsson – W. D. Oliver: A quantum engineer's guide to superconducting qubits. *Applied Physics Reviews*, 6. évf. (2019. jun) 2. sz. URL https://doi.org/10.1063%2F1.5089550.

[9] Sangil Kwon – Akiyoshi Tomonaga – Gopika Lakshmi Bhai – Simon J. Devitt – Jaw-Shen Tsai: Gate-based superconducting quantum computing. *Journal of Applied Physics*, 129. évf. (2021. jan) 4. sz. URL https://doi.org/10.1063%2F5.0029735.

[10] Seth Lloyd – Samuel L. Braunstein: Quantum computation over continuous variables. *Physical Review Letters*, 82. évf. (1999. feb) 8. sz., 1784–1787. p.
URL https://doi.org/10.1103%2Fphysrevlett.82.1784.

[11] Lars S. Madsen – Fabian Laudenbach – Mohsen Falamarzi. Askarani – Fabien Rortais – Trevor Vincent – Jacob F. F. Bulmer – Filippo M. Miatto – Leonhard Neuhaus – Lukas G. Helt – Matthew J. Collins – Adriana E. Lita – Thomas Gerrits – Sae Woo Nam – Varun D. Vaidya – Matteo Menotti – Ish Dhand – Zachary Vernon – Nicolás Quesada – Jonathan Lavoie: Quantum computational advantage with a programmable photonic processor. *Nature*, 606. évf. (2022. Jun) 7912. sz., 75–81. p. ISSN 1476-4687. URL `https://doi.org/10.1038/s41586-022-04725-x`.

[12] Arun K. Pati – Samuel L. Braunstein: *Deutsch-Jozsa Algorithm for Continuous Variables*. Dordrecht, 2003, Springer Netherlands, 31–36. p. ISBN 978-94-015-1258-9. URL `https://doi.org/10.1007/978-94-015-1258-9_4`.

[13] Arun K. Pati – Samuel L. Braunstein – Seth Lloyd: Quantum searching with continuous variables, 2000.

[14] Olivier Pfister: Continuous-variable quantum computing in the quantum optical frequency comb. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 53. évf. (2019. nov) 1. sz., 012001. p.
URL `https://dx.doi.org/10.1088/1361-6455/ab526f`.

[15] Swapnil Nitin Shah: Realizations of measurement based quantum computing, 2021.

[16] Adrien Suau – Jon Nelson – Marc Vuffray – Andrey Y. Lokhov – Lukasz Cincio – Carleton Coffrin: Single-qubit cross platform comparison of quantum computing hardware, 2021.

[17] M. S. Tame – M. S. Kim: Scalable method for demonstrating the deutsch-jozsa and bernstein-vazirani algorithms using cluster states. *Phys. Rev. A*, 82. évf. (2010. Sep), 030305. p. URL `https://link.aps.org/doi/10.1103/PhysRevA.82.030305`. 4 p.

[18] Ilan Tzitrin – J. Eli Bourassa – Nicolas C. Menicucci – Krishna Kumar Sabapathy: Progress towards practical qubit computation using approximate gottesman-kitaev-preskill codes. *Physical Review A*, 101. évf. (2020. mar) 3. sz.
URL `https://doi.org/10.1103%2Fphysreva.101.032315`.

[19] Tzu-Chieh Wei: Measurement-based quantum computation, 2021. 03.
URL `https://oxfordre.com/physics/view/10.1093/acrefore/9780190871994.001.0001/acrefore-9780190871994-e-31`.

[20] Hai-Ru Xu – Bang-Hai Wang: Universal single-server blind quantum computation for classical clients. *Laser Physics Letters*, 19. évf. (2021. nov) 1. sz., 015202. p. URL `https://dx.doi.org/10.1088/1612-202X/ac3a0d`.