SZAKIRODALOM ÖSSZEFOGLALÓ TANULMÁNY

A MESTERSÉGES INTELLIGENCIA FEJLESZTÉSE KVANTUMOSAN

Budapesti Műszaki és Gazdaságtudományi Egyetem

Villamosmérnöki és Informatikai Kar

Készítette:

Kemecsei Kornél

Témavezető:

Imre Sándor

Egyetemi tanár (BME)

Hálózati Rendszerek és Szolgáltatások Tanszék

A Kulturális és Innovációs Minisztérium ÚNKP-23-6-I-BME-455 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Tartalomjegyzék

Bevezetés

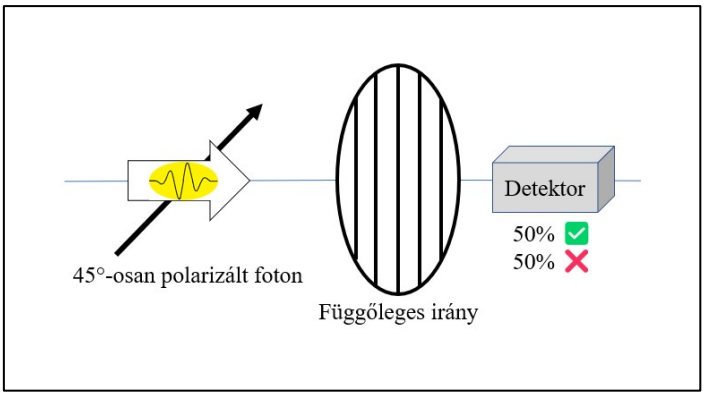
A kvantumszámítástechnika egy forradalmi technológia, amely a kvantummechanika alapelveire épül, és számos területen új távlatokat nyit. A 20. század elején felfedezett kvantummechanika napjainkban megkerülhetetlenné vált, az ipari és mérnöki életbe is leszivárogtak az atomi méretskálájú jelenségek. Gondoljunk csak például a gyógyszeriparra, az orvosi diagnosztikára, a nukleáris iparra és a félvezetőkre. A 20. század végén az egyedi kvantumrendszereken végzett kísérletek [1] [2] [3] [4] [5] ismét egy új fejezetet nyitottak, létrejött a kvantummechanika új alkalmazási területe, a kvantum-számítástechnika. Felmerült a kérdés, vajon képes-e az emberiség új alapokra helyezni a számítógépek működését, lehetséges-e a gyakorlati életben is jól használható kvantumszámítógép építése? Ennek motivációját az adta, hogy számos kvantummechanikai rendszer szimulálása klasszikus számítógéppel túlzottan bonyolultnak bizonyult. Feynman vetette fel elsőként, hogy kvantumrendszert szimuláljunk kvantumszámítógéppel [6]. Ezen tanulmány célja, hogy átfogó képet nyújtson a kvantumszámítógépek működéséről, szerkezetéről, valamint az előnyeiről és korlátairól a klasszikus számítógépekhez képest. Kiemelt figyelmet fordít a Grover algoritmusra és annak jelentőségére.

A kvantummechanika alapjai

A kvantuminformatika megértéséhez szükség van némi kvantumfizikai ismeretekre. Ehhez a [7] és az abban hivatkozott források segítenek. Ez volt tanulmányaim első lépése. Először maga a *foton*, mint elemi fénykvantum megismerése volt a feladatom. A fotonok felfedezését Einstein nevéhez kötjük, aki a fotoeffektus jelenségével kísérleti úton bizonyította létezésüket. Számításai szerint a fény nem egyenletes eloszlásban, hanem adagokban szállítja az energiát. Ezért a felfedezéséért 1921-ben fizikai Nobel-díjat kapott [8].

Folytatásképp megismerkedtem a fotonok egyedi eseményeinél fellépő *valószínűséggel*. A mikrovilágban az állapot ismerete mellett is elkerülhetetlen a valószínűség használata és ezt kísérletileg is igazolták. „Az Úristen tényleg kockajátékos", ezért járt 2022-ben a fizikai Nobel-díj [9].

Ezt követően a kvantummechanika matematikai alapjait ismertem meg. Először egy szakkör keretében elsajátítottam egy fotonpolarizációra épülő tananyagot, melyet röviden az alábbi cikk mutat be [10]. A későbbiek során felhasznált ismereteim egy konkrét példával demonstrálom, melyet az 1. ábra A 45°-osan polarizált foton 50% eséllyel áthalad a polarizátorlemezen, ekkor polarizációja függőleges lesz és a detektor érzékeli. Továbbá 50% valószínűséggel nyelődik el a foton, melyet elképzelhetünk úgyis, mintha a foton a vízszintes polarizációba esne bele, amely az elnyelődésnek felel meg. [7] 1.ábra mutat be. Essen egy függőleges irányú polarizátorlemezre egy 45°-osan polarizált foton. Mivel a foton és a lemez által bezárt szög 45°, ezért az áthaladás, vagy elnyelődés valószínűsége 50-50%. Ezt követően a foton állapota megváltozik. Az áthaladásnak függőleges, az elnyelődésnek pedig a vízszintes polarizáció felel meg.



1. ábra A 45°-osan polarizált foton 50% eséllyel áthalad a polarizátorlemezen, ekkor polarizációja függőleges lesz és a detektor érzékeli. Továbbá 50% valószínűséggel nyelődik el a foton, melyet elképzelhetünk úgyis, mintha a foton a vízszintes polarizációba esne bele, amely az elnyelődésnek felel meg [7].

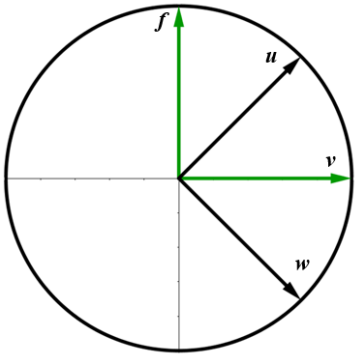
Reprezentáljuk egy foton polarizációs állapotát egy tetszőleges $\boldsymbol{u}$ kétdimenziós egységvektorral. Ez az egységvektor szemléletesen azt jelenti, hogy milyen irányban polarizáltak a fotonok. Ekkor az $\boldsymbol{u}$ egységvektor felírható a polarizátorlemez által kijelölt (lásd 1. *ábra*) függőleges ($\boldsymbol{f}$) és vízszintes ($\boldsymbol{v}$) egységvektorok lineáris kombinációjaként:

$$\boldsymbol{u} = \psi_1 \boldsymbol{v} + \psi_2 \boldsymbol{f}$$

ahol ψ_1 és ψ_2 a lineáris kombináció együtthatója. Tapasztalati tény, hogy egy foton nem csak a mérhető állapotokban (a fenti példában ez $\boldsymbol{v}$ és $\boldsymbol{f}$) lehet, hanem azok lineáris kombinációja is lehetséges állapot (ilyen a 45°-osan polarizációs állapot is). Ezt nevezzük a *szuperpozíció elvének.* A kvantummechanikában a valószínűségi leírás oka tehát a szuperpozíció elve. A

lineáris kombinációban az együtthatóknak, fizikai jelentése is van. A ψ_1^2 a ***v*** bázisállapot, ψ_2^2 az ***f*** bázisállapot mérési valószínűsége. A valószínűségi értelmezésből következik, hogy $\psi_1^2 + \psi_2^2 = 1$, azaz az állapotvektorok szükségképpen 1 hosszúak. Ez alapján felírható a példában szereplő 45°-os polarizációjú foton (***u***), az ***f*** és ***v*** állapotvektorokra vonatkoztatva:

$$\boldsymbol{u} = \frac{1}{\sqrt{2}}\mathbf{v} + \frac{1}{\sqrt{2}}\mathbf{f}.$$



2. ábra: A fotonok polarizációs állapotvektora ábrázolható egy egységkörön, melyet állapotkörnek nevezünk [11]. Az ábrán különböző polarizációk egységkörön való ábrázolása látható. A w állapot a -45°-os polarizációnak felel meg. Az azonos színnel jelölt vektorok egy lehetséges mérési bázist adnak, ezek merőlegesek egymásra [7].

A szuperpozíció szemléletesen azt jelenti, hogy egy részecske állapota kettős. Egy 45°-osan polarizált fotonra nem lehet azt mondani, hogy csak vízszintes, vagy csak függőleges polarizációjú, mindkettő mérési eredmény lehetősége keveredik benne

$$\boldsymbol{v} = \frac{1}{\sqrt{2}}\mathbf{u} + \frac{1}{\sqrt{2}}\mathbf{w}.$$

Kvantumszámítógépek Alapjai

Kvantuminformáció

A kvantuminformáció olyan speciális információs formát jelent, amelyet kvantumbitek, azaz qubitek hordoznak. A kvantumbitek kétállapotú kvantumrendszerek, amelyek a 0 és 1 klasszikus bitállapotok kvantum-megfelelői, de lehetőségük van egyszerre több állapotban is lenni a szuperpozíció elve alapján. Ez azt jelenti, hogy egy qubit állapota egyidejűleg lehet 0 és 1, egy megfelelő kvantumállapotban. A kvantuminformáció másik különleges tulajdonsága az összefonódás (entanglement). Az összefonódott qubitek között olyan kapcsolat áll fenn, hogy az egyik qubit állapotának megváltoztatása azonnal befolyásolja a másik qubit állapotát, függetlenül attól, milyen távol vannak egymástól. Ez az összefonódás lehetőséget biztosít kvantuminformációk gyors és biztonságos továbbítására, például kvantumteleportáció révén. A kvantumszámítások során használt kapuk, mint például a Hadamard-kapu, a CNOT-kapu vagy a kvantum Fourier-transzformáció, a klasszikus logikai kapuk kvantum-megfelelői. Ezekkel a kapukkal végzett műveletek lehetővé teszik a kvantumalgoritmusok végrehajtását, amelyek bizonyos feladatokat lényegesen gyorsabban tudnak megoldani, mint a klasszikus algoritmusok. Példa erre Shor algoritmusa [12], amely hatékonyan képes nagy számok prímtényezőkre bontására, ami komoly következményekkel jár a jelenlegi titkosítási rendszerek biztonságára nézve. A kvantum-számítástechnika egy másik fontos tulajdonsága a szimmetria és a visszafordíthatóság. A kvantumkapuk unitér transzformációk, amelyek megőrzik az állapotok normáját és lehetővé teszik a kvantumállapotok visszafordíthatóságát.

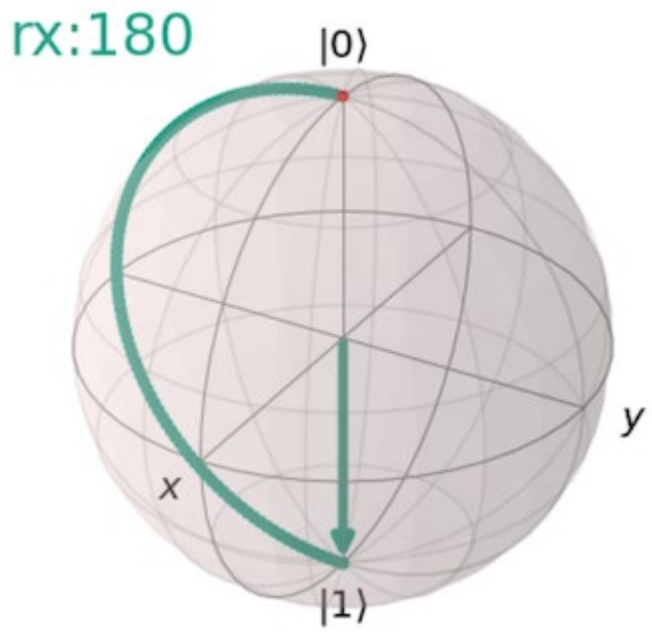
Ez azt jelenti, hogy minden kvantumalgoritmusban végrehajtott művelet megfordítható, ami különbözik a klasszikus számítástechnikában használt irreverzibilis műveletektől.

Kvantum Algoritmusok

A kvantum algoritmusok jelentős előnyt nyújtanak a klasszikus algoritmusokhoz képest, akár exponenciális gyorsulást is elérve bizonyos problémák megoldásában. Például az RSA titkosítás klasszikus algoritmusokkal nem oldható meg polinomiális idő alatt, míg kvantum algoritmusokkal igen. [13] A hatékony kvantum algoritmusok megvalósításához szükség van a DiVincenzo kritériumainak betartására, amelyek előírják a kvantumregiszterek megfelelő állapotba állítását és az adatok kinyerését a számítások után. A DiVincenzo-kritérium hét feltételből áll, amelyeknek egy kísérleti összeállításnak meg kell felelnie a kvantumalgoritmusok sikeres megvalósításához, mint például a Grover-féle keresési algoritmus vagy a Shor-faktorizáció.

Bloch-gömb

A Bloch-gömb egy szemléletes eszköz, amelyet a kvantumbitek (qubitek) állapotának ábrázolására használunk. Ez nem más, mint a korábban megismert egységkör, egységgömbbé való kiterjesztése. A gömb felületén minden pont egy qubit állapotot jelölhet, ahol a pólusok a klasszikus 0 és 1 állapotokat, míg a köztes pontok a szuperpozíciós állapotokat reprezentálják. A qubit állapotát egy vektor határozza meg, amely a gömb középpontjából indul és a gömb felületének valamely pontjára mutat. A Bloch-gömb segítségével szemléltethető a kvantumkapuk hatása is, amelyek a vektort forgatásokkal módosítják a gömbön. Ez az ábrázolási mód különösen hasznos a kvantumalgoritmusok vizualizálásában és megértésében. Az állapot szuperpozícióját és fázisát is intuitív módon lehet érzékeltetni a Bloch-gömbön keresztül. A gömb geometriai jellege révén könnyen ábrázolhatóak a különböző kvantumkapuk által végzett unitér transzformációk.



2. ábra Bloch gömb

Bell-egyenlőtlenség

A Bell-egyenlőtlenségek a kvantummechanika és a klasszikus fizika közötti különbségeket emelik ki, különösen az összefonódás jelenségén keresztül. John Bell 1964-ben bizonyította [2], hogy bizonyos kvantumállapotok korrelációi nem magyarázhatók a klasszikus valószínűségi elméletekkel. Az egyenlőtlenségek megsértése kísérletileg bizonyítja a kvantummechanika érvényességét és az összefonódott állapotok különleges természetét. Eredményei alapján olyan kísérleteket terveztek, amelyekben fotonpárok vagy más részecskék összefonódott állapotát vizsgálták. Az ilyen kísérletek, például az Alain Aspect által végzett kísérletek [4], megerősítették a kvantummechanika jóslatait. A Bell-egyenlőtlenségek megsértése az egyik legerősebb érv a rejtett változók elméleteinek kizárására, amelyek a klasszikus fizika keretein belül próbálják magyarázni a kvantumjelenségeket. Ez a koncepció kulcsfontosságú szerepet játszik a kvantuminformációs tudományok fejlődésében.

No-cloning theorem

A no-cloning theorem, vagyis a nem-klónozási tétel, a kvantuminformáció egyik alapvető elve, amely kimondja, hogy egy ismeretlen kvantumállapot tökéletesen nem másolható. Ez a tétel 1982-ben Wootters és Zurek, valamint Dieks függetlenül dolgozták ki [14], és központi szerepet játszik a kvantummechanika alapvető természetében. A tétel következménye, hogy kvantumállapotok nem másolhatók ugyanúgy, mint a klasszikus információk. Ez jelentős hatással van a kvantumkriptográfiára, mivel garantálja, hogy egy kvantumkulcs biztonságosan továbbítható. Ha egy lehallgató megpróbálja másolni a kvantuminformációt, az állapot elkerülhetetlenül megváltozik, észrevehető hibát okozva. Egy ilyen titkosítással, itt [7] már foglalkoztam korábban. A no-cloning theorem továbbá korlátozza a kvantuminformáció másolására és terjesztésére vonatkozó lehetőségeket, biztosítva, hogy az összefonódott állapotok és a kvantumtitkosítás biztonsága megmaradjon. Ennek a tételnek a megértése elengedhetetlen a kvantumszámítástechnika és a kvantuminformációs rendszerek tervezésében.

Kvantumszámítógépek Felépítése

Kapuk

A kvantumkapuk, mint például a NOT és CNOT kapuk, univerzális kvantum számításra használhatók, és csak a lényeges kimenetet tartják meg. A fizikai megvalósítás során különféle technológiákat alkalmaznak, például ioncsapdákat, szupravezetőket, lineáris optikai eszközöket, gyémántokat, kvantumpontokat, donor-alapú rendszereket vagy topológiai kvantumszámítási elemeket. A hibaszűrés és -korrekció továbbra is jelentős kihívást jelent ezen a területen, ezért szükség van ezeknek az előfordulásának vizsgálatára és szimulálására. Napjainkban rengeteg új eredményt érnek el ezen a területen [15].

Memória

A kvantummemóriák létfontosságú szerepet játszanak a kvantumáramkörök számításaiban, tárolva a kvantumállapotokat az információfeldolgozáshoz. Különféle megközelítések léteznek, mint például a topológiai kvantummemória, amely összefonódott kvantumrendszereket használ. A memória élettartamának meghosszabbítása terén bár történt némi előrelépés, például a szobahőmérsékletű kvantumbit memória elérése, továbbra is jelentős kihívások állnak fenn. A Quantum Random Access Memória (qRAM) qubiteket használ a memóriacellák címezésére, és csökkenti az energiaigényt kvantumoptikai megvalósítást használva. A neurális hálózatok optimalizálják a dinamikus szétválasztást a kvantummemóriák

hibajavítása érdekében. A kvantum-memrisztorok és a qubit-alapú mem-kondenzátorok/meminduktorok potenciális alkalmazásokat kínálnak a kvantumszámítástechnikában [16].

CPU

A kvantum CPU-k kvantumbuszokat alkalmaznak a funkcionális elemek közötti kommunikációhoz. A kvantumösszeadók a kvantumszámítások kulcsfontosságú összetevői. A kvantumáramkörök párhuzamosítása két hálózati modellt tartalmaz: a távolsági és a helyi kommunikációt, melyek hasonló összeadó teljesítményűek.

Qubitek, kapuk

A kvantummechanika axiómái

1. Kvantumállapotok: egy zárt fizikai rendszer leírható állapotvektorokkal mely komplex számokból és egységvektorokból állnak a Hilbert térben.

2. Evolution/Állapotfejlődés: minden zárt fizikai rendszer karakterizálható olyan transzformációkkal, amik a szuperpozíció összetételét nem változtatják.

3. A kvantum mérés leírható unitér mérő operátorokkal.

4. kompozíció: Két vagy több kvantumrendszer egyesített állapotát a Hilbert-terek tenzorszorzataként reprezentáljuk. Ha két rendszer állapota $|\psi\rangle$ és $|\phi\rangle$, akkor a kombinált rendszer állapota $|\psi\rangle \otimes |\phi\rangle$

QBitek, QRegiszterek

Qbit: két bázisvektor $|0$ és $|1\rangle$ (megfeleltethetően 0 és 1 klasszikus biteknek), $|\varphi\rangle$ pedig ezek lineáris kombinációja $a|0\rangle + b|1\rangle$. Ez továbbá megadja a mérés valószínűségét is: $|a|^2$ a valószínűsége a $|0\rangle$ mérésének és $|b|^2$ az $|1\rangle$ mérésének.

Kvantum Kapuk

A kvantumkapuk a kvantum-számítástechnika alapvető építőelemei, amelyekkel kvantumbiteken (qubiteken) műveleteket végezhetünk. A klasszikus logikai kapukkal ellentétben, amelyek bitenként 0 és 1 értékekkel dolgoznak, a kvantumkapuk a qubit állapotát módosítják, amely lehet szuperpozícióban és összefonódásban [17].

1. Hadamard-kapu (H)

A Hadamard-kapu egy kvantumkapu, amely egy qubitet egyenlő valószínűséggel két állapot szuperpozíciójába helyez. Matematikailag a Hadamard-kapu az alábbi unitér mátrixszal írható le:

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

Ez a kapu a $|0\rangle$ és $|1\rangle$ állapotokat a következőképpen alakítja át:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

2. CNOT-kapu (vezérelt-NOT)

A CNOT-kapu két qubiten működik: egy vezérlő (control) qubit és egy célszál (target) qubit. A kapu csak akkor változtatja meg a célszál állapotát, ha a vezérlő qubit állapota 1. Matematikai leírása a következő:

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

A CNOT-kapu az alábbi módon hat a qubit állapotokra:

$$\text{CNOT}|00\rangle = |00$$

$$\text{CNOT}|01\rangle = |01$$

$$\text{CNOT}|10\rangle = |11$$

$$\text{CNOT}|11\rangle = |10$$

3. SWAP-kapu

A SWAP-kapu két qubit állapotát cseréli meg. Matematikailag a SWAP-kapu mátrixa:

$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Az állapotok cseréje a következőképpen történik:

$$\text{SWAP}|01\rangle = |10\rangle$$

$$\text{SWAP}|10\rangle = |01\rangle$$

4. Pauli-X kapu

A Pauli-X kapu egy qubit klasszikus NOT kapunak felel meg, amely a qubit állapotát 0-ról 1-re vagy 1-ről 0-ra váltja. Matematikailag az alábbi mátrixszal írható le:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

A Pauli-X kapu hatása a következő:

$$X|0\rangle = |1\rangle$$

$$X|1\rangle = |0\rangle$$

5. Pauli-Y kapu

A Pauli-Y kapu a qubit állapotát forgatja a Bloch-gömbön az Y-tengely körül 180 fokkal. Matematikai leírása:

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

A Pauli-Y kapu hatása:

$$Y|0\rangle = i|1\rangle$$

$$Y|1\rangle = -i|0\rangle$$

6. Pauli-Z kapu

A Pauli-Z kapu egy fázisfordítást végez a qubit állapotán, ami a Z-tengely körüli forgatásnak felel meg 180 fokkal. Mátrixa:

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

A Pauli-Z kapu hatása:

$$[Z|0\rangle = |0\rangle$$

$$Z|1\rangle = -|1\rangle$$

7. Rx kapu

Az Rx kapu a qubit állapotát az X-tengely körül forgatja (θ) szöggel. Mátrixa:

$$R_x(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

8. Ry kapu

Az Ry kapu a qubit állapotát az Y-tengely körül forgatja (θ) szöggel. Mátrixa:

$$R_y(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

9. Rz kapu

Az Rz kapu a qubit állapotát a Z-tengely körül forgatja (θ) szöggel. Mátrixa:

$$R_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$$

Mérések a Kvantummechanikában

A kvantummechanikában a mérések különleges szerepet játszanak, mivel az állapotok és a mérési eredmények közötti kapcsolat jelentősen eltér a klasszikus fizikától. Ebben a fejezetben a kvantumrendszerek mérésének elméleti alapjait és a mérési operátorok használatát vizsgáljuk, különös tekintettel a valószínűségi eloszlásokra és a rendszer állapotára a mérés után.

Valószínűség

Ha egy kvantumrendszer állapota ($|\varphi\rangle$), és mérést végzünk rajta, a mérési eredmény (m) detektálásának valószínűsége a következőképpen adható meg:

$$P(m \mid \varphi) = \left|\left\langle \varphi \middle| M_m^\dagger M_m \middle| \varphi \right\rangle\right|^2 = \langle \varphi | P_m | \varphi \rangle$$

Itt (M_m) a mérési operátor, amely a mérési folyamatot reprezentálja, és ($P_m = M_m^\dagger M_m$) egy projektor, amely a mérés során a rendszer állapotára hat. Ez a formula a Born-szabály egy speciális esete, amely a kvantummechanikai mérések valószínűségi természetét írja le.

Mérési operátor

Egy kvantumállapot ($|\varphi_m\rangle$) esetén a hozzá tartozó mérési operátor (M_m) a következő formában írható fel:

$$M_m = \langle \varphi_m || \varphi_m \rangle$$

Ez az operátor a rendszert a ($|\varphi_m\rangle$) állapotba projiciálja, és biztosítja, hogy a mérés eredményeképpen a rendszer ebbe az állapotba kerüljön.

Ortogonalitás

Két vektor ortogonális, ha skalárszorzatuk nulla, például merőlegesen polarizált fotonok esetében. Az ortogonális vektorokhoz tartozó projektorok a következőképpen írhatók fel:

$$P_1|\varphi_1\rangle = |\varphi_1\rangle\langle\varphi_1|$$

Ezek a projektorok kielégítik az alábbi feltételt is:

$$P_1 + P_2 = I$$

ahol (I) az identitásoperátor. Ez biztosítja, hogy a két állapot együtt a teljes állapottér egy ortogonális bázisát alkotja. Ha a rendszer egy ortogonális állapotban van, akkor a megfelelő projektor hatása a következőképpen adható meg:

$$P(m|\varphi\rangle) = 1$$

Ez azt jelenti, hogy a mérési eredmény biztosan az adott állapot lesz, ha a rendszer abban az állapotban van.

Normáltság

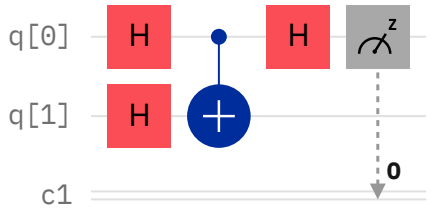
A kvantummechanikai rendszerek állapotainak normáltsága alapvető követelmény, amely biztosítja, hogy az állapotok valószínűségi eloszlásai megfelelően viselkedjenek. Az állapot normáltsága az alábbi módon van kifejezve:

$$\langle\psi|\psi\rangle = 1$$

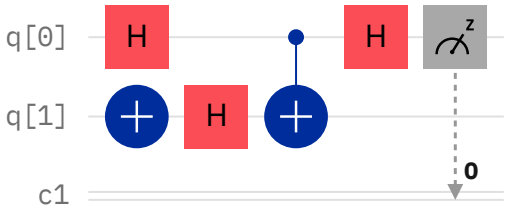
Ez a kifejezés azt jelenti, hogy az állapot vektorának hosszúsága (normája) egy, ami a valószínűségi értelmezés miatt szükséges. Ez a normáltság feltétel biztosítja, hogy a rendszer állapotát megfelelően lehessen leírni és kezelni a kvantummechanika matematikai keretén belül.

Egyszerű kvantumos algoritmusok

Deutsch-Jozsa



3. ábra függvény melyről megállapítja az algoritmus, hogy konstans



***4**. ábra kiegyensúlyozott függvény*

A Deutsch-Jozsa algoritmus kvantummechanikai interferencia segítségével hatékonyan dönti el egy függvényről, hogy konstans vagy kiegyensúlyozott, mindössze egyetlen oracle hívással. Ez jelentős előnyt jelent a klasszikus algoritmusokkal szemben, amelyek esetében az összes bemenet felének ellenőrzésére van szükség a biztos eredmény eléréséhez.

Shor

A Shor-féle prímfaktorizációs algoritmusban a kvantumátviteli hullámosító összeadó különféle forgatókönyvekben kiváló, és nagy számok gyors faktorizálását kínálja a klasszikus algoritmusokhoz képest. Az algoritmus működésének lényege, hogy egy A és B kvantum

regisztert használnak, ahol az A regisztert szuperpozícióba helyezik a Hadamard-kapuval, majd egy unitárius műveletet végeznek el a perióduskereséshez. B-t megmérik, majd A-n az inverz kvantum Fourier transzformációt alkalmazzák, és újra megmérik.

Quantum Fourier Transformáció és Fázisbecslés

A kvantumszámítás egyik legfontosabb és legmélyrehatóbb eredménye a Quantum Fourier Transformáció (QFT) és az ebből származó fázisbecslés (Quantum Phase Estimation, QPE) algoritmusok. Ezek az eszközök alapvető szerepet játszanak számos kvantumalgoritmusban, beleértve Shor faktorizáló algoritmusát és az általános kvantum szimulációkat. Ebben a fejezetben áttekintjük a QFT és a QPE alapelveit, működését és alkalmazásait.

Quantum Fourier Transformáció (QFT)

A Quantum Fourier Transformáció a klasszikus Fourier Transformáció kvantum megfelelője. Míg a klasszikus Fourier Transformáció az idő vagy térbeli tartományból átalakít egy jelet a frekvenciatartományba, a QFT egy kvantumbitet vagy kvantumbit sorozatot alakít át a kvantum szuperpozíció állapotaiba.

Definíció és Matematika

A QFT egy n-qubit rendszerre a következőképpen definiálható:

Legyen ($|x\rangle$) egy n-qubit állapot, ahol (x) egy bináris szám ($x_0x_1 \dots x_{n-1}$). A QFT ennek az állapotnak az amplitúdóit alakítja át:

$$|x\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i x k/2^n} |k\rangle$$

Ez a transzformáció unitér, azaz megőrzi a kvantumállapot normáját.

Algoritmus

A QFT algoritmusa n qubitre a következő lépéseket tartalmazza:

1. **Hadamard transzformáció**: Az első qubitre alkalmazunk egy Hadamard kaput, amely egyenletes szuperpozícióba hozza.

2. **Kontrollált fáziseltolások**: Minden további qubitre kontrollált fáziseltolásokat alkalmazunk, amelyek a kvantum állapotok közötti fázisokat változtatják meg.

3. **Iteráció**: Az 1. és 2. lépéseket ismételjük minden qubitre, egyre kisebb mértékű fáziseltolásokkal.

4. **Quibitek cseréje**: A végső lépésben a qubitek sorrendjét megfordítjuk, hogy a megfelelő Fourier képhez jussunk.

A QFT időkomplexitása $(O(n^2))$, ami jelentős javulás a klasszikus Fourier Transzformáció $(O(n2^n))$ komplexitásához képest.

Fázisbecslés (Quantum Phase Estimation, QPE)

A Quantum Phase Estimation algoritmus a QFT-re épül, és célja, hogy egy unitér operátor sajátértékének fázisát pontosan meghatározza. Ez az algoritmus kulcsfontosságú szerepet játszik többek között a Shor algoritmusban és annak a problémának az eldöntésében, hogy egy keresési kérésre, hány jó megoldás van.

Alapelvek

A QPE algoritmus két kvantum regisztert használ:

1. **Vezérlő regiszter**: n qubitből áll, amelyeken a QFT-t alkalmazzuk.

2. **Munkaregiszter**: Mely az unitér operátor sajátállapotában van.

Működés

A QPE algoritmus lépései a következők:

1. **Előkészítés**: A vezérlő regisztereket egyenletes szuperpozícióba hozzuk Hadamard kapukkal.

2. **Unitér operátor alkalmazása**: A munkaregiszteren alkalmazzuk az (U) operátort, melynek sajátértékét meg akarjuk becsülni, és a vezérlő regiszter minden qubitjén az $\left(U^{2^j}\right)$ operátort alkalmazzuk (ahol (j) az adott qubit pozíciója).

3. **QFT alkalmazása**: A vezérlő regiszteren elvégezzük a QFT-t.

4. **Mérés**: A vezérlő regiszterek qubitjeit megmérjük, és az eredmény alapján a sajátérték fázisát meghatározzuk.

Pontosság és Használat

A QPE pontossága az alkalmazott qubitek számától és az algoritmus lépéseinek számától függ. Minél több qubitet és lépést használunk, annál pontosabban tudjuk meghatározni a fázist. Ez az algoritmus nélkülözhetetlen a kvantum számítási feladatok széles körében.

A Quantum Fourier Transformáció és a fázisbecslés kvantuminformatikai alkalmazásai jelentős áttörést hoztak a számítástechnika, kriptográfia és kvantumfizika területein, lehetővé téve a klasszikus számítási módszerek által megoldhatatlan problémák hatékony kezelését.

Grover

A kvantumszámítógépek megjelenése, különösen Grover algoritmus segítségével, forradalmasítja a keresés hatékonyságát, drasztikusan csökkentve a számítások bonyolultságát O(N) helyett O(√N) -re, jelentős előrelépést jelentve az hatékony keresési módszerek felé tett úton [18].

Grover Algoritmus

Probléma: Egy N elemű adatbázisban (pl. gyümölcs nevek), az x_0 indexet keressük, ahol $DB[x_0]$=alma.

A probléma megoldásához az eddig megismert eszközöket használjuk.

Kvantum paralelizmus segítségével az összes lehetséges választ betöltjük egyenlő valószínűségekkel. Ezután az U_f operátorral feldolgozzuk az adatot. Ehhez szükségünk lesz egy alsó segéd qregiszterre, majd a Hadamard vagy IQFT kaput használjuk a kvantum interferencia létrehozásához a felső qregisztereken. Végül pedig megmérjük a qregiszrtereinket.

Initialization - Parralelizmus

Az felső regiszter n db q-bittel rendelkezik a $N = 2^n$ adatbázis méretéhez, $|0\rangle$ kezdeti állapottal inicializáljuk. Egy n-dimenziós Hadamard kaput használunk a felső regiszteren. Az alsó q-regiszter egy ismeretlen T kapuhoz kapcsolódik.

G első szakasza - Oracle

A második szakaszban egy Oracle-t használunk, akárcsak a Deutsch-Jozsa algoritmusban (3. 4. ábra). Itt az oraclet a megjelölt és nem megjelölt állapotok megkülönböztetésére használjuk. Az Oracle megszorozza az igényelt elem valószínűségi amplitúdóját -1-gyel, és bármely más amplitúdót változatlanul hagy.

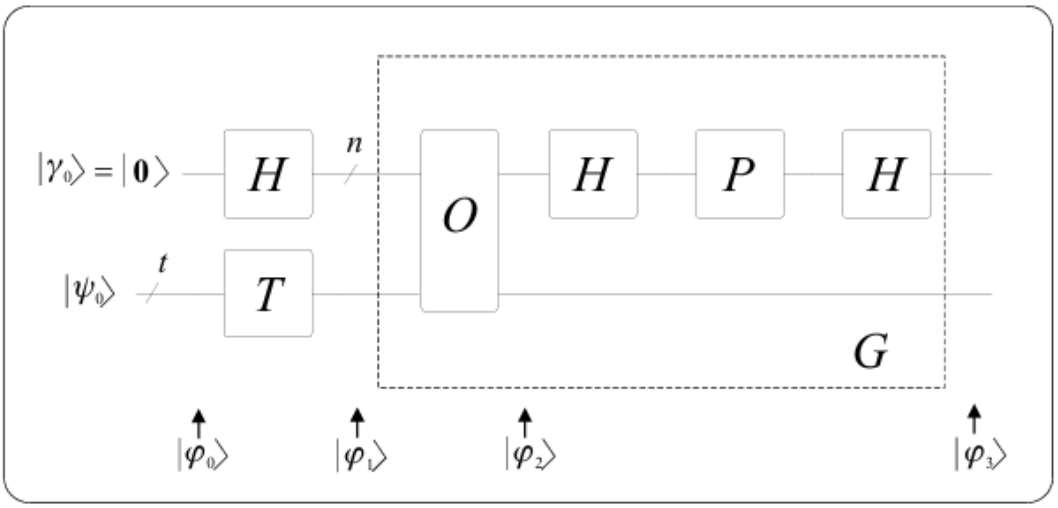
$$|x\rangle|y\rangle \rightarrow (-1)^{f(x)}|x\rangle|y\rangle$$

$$O\colon |x\rangle|y\rangle \rightarrow |x\rangle|y\rangle \oplus f(x)$$

(Általánosságban feltételeztük, hogy N egy 2 hatványa. Ha ez nem így van, akkor kiegészítjük N-t a legközelebbi 2^n-re a $f(x) = 0$-val.)

Megvalósítás

Az oracle megvalósításához a Deutsch-Jozsa-ból tanultakat használjuk. t=1 qbit $|1\rangle$-re initializálva az alsó regiszteren és T egy H kapu. Ezt az állapotot az oracle nem változtatja a felső regiszteren pedig ez lesz a control bitünk.



5. ábra Grover Algoritmus tervrajza kapukkal

(P = phase kapu)

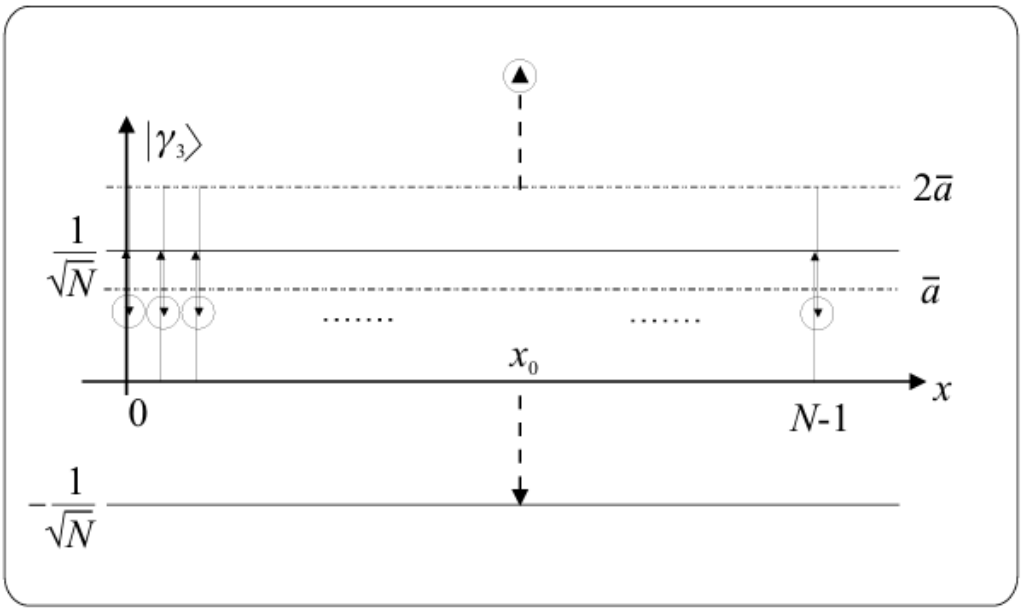
A P kapu transzformációs szabálya: az összes valószínűségi amplitúdót változatlanul hagyja, kivéve a |0⟩-ét, aminek a jelét megfordítja.

G második szakasza - invertálás átlagnál - amplitude amplification

Olyan unitárius transzformációt keresünk (U_γ) ami felerősíti az amplitúdóját a mérni kívánt értéknek (azaz x_0 −nak) Ezt az átlagnál való invertálással érjük el, ami egy számból kivonja mindegyik input értékét. Azaz x_0 értéke nő (mert +valami - (-1), többi +valami - (+1)) a többi állapot értéke csökken. (Ez a transzformáció megtartja a vektor hosszát és visszafordítható tehát unitér.)

$$\mathbf{U}_\gamma = \begin{bmatrix} \frac{1}{\sqrt{N}} \\ \frac{1}{\sqrt{N}} \\ \vdots \\ \frac{1}{\sqrt{N}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{N}} & \frac{1}{\sqrt{N}} & \cdots & \frac{1}{\sqrt{N}} \end{bmatrix} - I = \begin{bmatrix} \frac{1}{N} & \frac{1}{N} & \cdots & \frac{1}{N} \\ \frac{1}{N} & \frac{1}{N} & \cdots & \frac{1}{N} \\ \vdots & & \ddots & \vdots \\ \frac{1}{N} & \cdots & \cdots & \frac{1}{N} \end{bmatrix} - I = \begin{bmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \cdots & \frac{2}{N} \\ \vdots & & \ddots & \vdots \\ \frac{2}{N} & \cdots & \frac{2}{N} & \frac{2}{N} - 1 \end{bmatrix}. \quad (7.13)$$

6. ábra Invertáló kapu mátrixa



7. ábra Adatbázis elemeit reprezentáló elemek állapota a forgatás és erősítés után

Ennek birtokában már megkaphatjuk a Grover operátort:

$$G = HPHO = (2H|0\rangle\langle 0|\, H - I)O = |2\gamma_1\rangle\langle 1| - I)(I - |2x_0\rangle\langle x_0|)$$

Az amplitúdó felerősítése arra törekszik, hogy az értékét minél közelebb vigye az 1-hez, ezáltal az egyéb valószínűségi amplitúdókat nullához csökkenti. Egyetlen G művelettel csak nagyon különleges esetekben lehet elérni ezt a célt, ha a keresett elem indexe 4-szerese az adatbázis mérete. Szerencsére a segéd q-bit állapota nem változik az input és output között, így többször is alkalmazhatjuk egymás után a G-t. Ha több megoldás is van az adatbázisban akkor több amplitúdót is erősítünk, így előfordulhat több azonos méretű "tüske" is az eredmény leolvasásakor, ez az algoritmuson nem változtat. A fő különbség és újdonság az edigi algoritmusokhoz képest, hogy egyetlen Hadamard vagy IQFT kapu helyett amplitude amplificationt használlunk, így magát az algoritmust tekinthetjük a Grover operátor ismételt alkalmazásának.

Szükséges iterációk mennyisége

Hányszor kell elvégeznünk a keresést (hány G kapu kell) az optimális kimenet érdekében? Az optimális iterációk száma meghatározható a kezdeti szög és a forgási lépés közötti aránynak megfelelően. Az optimális érték függ a kezdeti szög és közvetve az adatbázis mérete és a keresett bejegyzések száma (M) közötti aránytól.

$$\frac{\Omega_\gamma}{2} \sim \sqrt{\frac{M}{N}} L_{opt} = \frac{\frac{\pi}{2} - \frac{\Omega_\gamma}{2}}{\Omega_\gamma} = \frac{\pi}{4}\sqrt{\frac{N}{M}}$$

Ebből következik, hogy $L_{opt} = O\left(\sqrt{\frac{N}{M}}\right)$ ami lényegesen kevesebb szükséges lépés, mint klasszikus esetben $O(N)$, nem rendezett adatbázisban)

Hibaanalízis

Ha l_{opt} nem egész akkor a hiba valószínűsége:

$$P_\epsilon = |\langle \alpha G^{L_{opt}} \rangle \gamma_1|^2 = \cos^2\left(\frac{(2L_{opt}+1)\Omega_\gamma}{2}\right)$$

Ebből következik, hogy az algoritmus sikeres alkalmazásának valószínűsége: $1 - P_\epsilon$

Generikus Grover Algoritmus

Eddig csak H $|0\rangle$ állapotú inputtal foglalkoztunk. Most egy generikusabb bemenetre is meg kéne oldani az algoritmus működését.

1. H kapu helyett bármilyen unitér U kapu használható

2. Az Oracle szögét (φ) módosítjuk, amely a megjelölt elem valószínűségi amplitúdóit forgatja az index regiszterben.

3. A kontrollált fáziskaput (P) is módosítjuk, hogy tetszőleges kiinduló állapotot lehessen használni.

4. Az index regiszter kezdeti állapota egy általánosított formára cserélődik $H|0\rangle$, helyett.

Kitekintés

Kutatásom során, ezen ismeretek elsajátítása után a Grover algoritmus szimulálásával foglalkoztam és annak vizsgálatával zajos környezetben. Az ismertetett algoritmusokról szintén készültek (ugyan egyszerűbb, de szemléletes) szimulációk Qiskitben. A megismert anyagok könnyebb megértéséhez továbbá közzé tettem a saját jegyzeteimet is a szimulációkkal és minden egyéb anyaggal. [19]

Összefoglalás

A kvantumszámítástechnika ígéretes jövőt kínál a számítástechnika terén, számos kihívással és lehetőséggel. Az előnyök, mint a gyorsabb számítási sebesség és a klasszikus számítógépeknél hatékonyabb algoritmusok, mellett számos megoldandó technikai kérdés is van, például a hibajavítás és a kvantummemóriák élettartamának növelése. A technológia fejlődése lehetővé teszi, hogy a jövőben egyre szélesebb körben alkalmazzuk a kvantumszámítógéperangle, ám jelenleg még főként laboratóriumi környezetben léteznek. A kutatások és fejlesztések folyamatosak, és a legfrissebb eredmények és aktuális problémák figyelemmel kísérése kulcsfontosságú a terület előrehaladásához.

Irodalomjegyzék

[1] A. Einstein, . B. Podolsky és N. Rosen, „Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? Physical Review 47, 777," 1935. [Online]. Available: https://doi.org/10.1103/PhysRev.47.777.

[2] J. Bell, „On the Einstein–Poldolsky–Rosen paradox. Physics 1 3, 195–200," 1964. [Online]. Available: https://cds.cern.ch/record/111654/files/vol1p195-200_001.pdf .

[3] J. F. Clauser, M. A. Horne, A. Shimony és R. A. , „Proposed Experiment to Test Local Hidden-Variable Theories. Physical Review Letters. 23 880," 1970. [Online]. Available: https://doi.org/10.1103/PhysRevLett.23.880.

[4] G. Roger, P. Grangier és A. Aspect, „Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities. Physical Review Letter 49 (2) 91," 1982. [Online]. Available: https://doi.org/10.1103/PhysRevLett.49.91.

[5] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter és A. Zeilinger, „Experimental quantum teleportation. Nature 390, 575-579," 1997. [Online]. Available: https://doi.org/10.1038/37539 .

[6] R. P. Feynman, „Simulating Physics with Computers. International Journal of Theoretical Physics. 21 (6–7). 467–488.," 1982. [Online]. Available: https://doi.org/10.1007/BF02650179 .

[7] K. Kemecsei és M. Csaplár, „A B92 KVANTUMOS KULCSELOSZTÁSI PROTOKOLL VIZSGÁLATA ZAJOS KÖRNYEZETBEN," 2022. [Online]. Available: https://github.com/Harcipan/B92_Protocol/blob/main/A%20B92%20KVANTUMOS%20KULCSELOSZT%C3%81SI%20PROTOKOLL%20VIZSG%C3%81LATA%20ZAJOS%20K%C3%96RNYEZETBEN.pdf.

[8] A. Einstein, „Nobel Prize Physics," 1921. [Online]. Available: https://www.nobelprize.org/prizes/physics/1921/summary/.

[9] „The Nobel Prize in Physics," 19 10 2022. [Online]. Available: https://www.nobelprize.org/prizes/physics/2022/summary/.

[10] K. Tóth, Modell kvantummechanika középiskolában. Fizikai Szemle. 209-214. 71(6), 2021.

[11] C. Bernhardt, „Quantum Computing for Everyone," The MIT Press, Cambridge, 2019.

[12] P. W. Shor, „Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science. 124-134,” 1994. [Online]. Available: doi: 10.1109/SFCS.1994.365700.

[13] C. H. Bennett és G. Bassard, Quantum cryptography: Public key distribution and coin tossing. Proceedings of the International Conference on Computers, Systems & Signal 175-179, Bangalore, India: Processing,, 1984.

[14] W. K. Wootters és W. H. Zurek , „A single quantum cannot be cloned,” 1982. [Online]. Available: https://www.nature.com/articles/299802a0.

[15] I. Spectrum, „QUANTUM ERROR CORRECTION: TIME TO MAKE IT WORK,” [Online]. Available: https://spectrum.ieee.org/quantum-error-correction.

[16] G. László és S. Imre, A Survey on Quantum Computing Technology, COMPUTER SCIENCE REVIEW (1574-0137 1876-7745): 31 pp 51-71, 2019.

[17] S. Imre és F. Balázs, Quantum Computing and Communications – An Engineering Approach, Chichester, John Wiley & Sons, 283 p., 2005.

[18] S. Imre, Quantum Existence Testing and its Application for Finding Extreme Values in Unsorted Databases, IEEE TRANSACTIONS ON COMPUTERS (0018-9340 1557-9956): 56 5 pp 706-710, 2007.

[19] K. Kornél, „Grover Szimulátor,” [Online]. Available: https://github.com/Harcipan/QAI_GroverSim.

[20] G. S. El és S. Imre, Constrained Quantum Optimization for Resource Distribution Management, INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS (2158-107X 2156-5570): 12 8 pp 42-51 (2021).

[21] G. S. El és S. Imre, Implementation of a constrained quantum optimisation method in resource distribution management with considering queueing scenarios, NTERNATIONAL JOURNAL OF COMMUNICATION NETWORKS AND DISTRIBUTED SYSTEMS (1754-3916 1754-3924): 28 2 pp 126-146, 2022.

[22] „High-threshold and low-overhead fault-tolerant quantum memory,” Nature volume 627, pages778–782, 2024. [Online]. Available: https://www.nature.com/articles/s41586-024-07107-7.

[23] „Build noise models,” Qiskit, [Online]. Available: https://docs.quantum.ibm.com/verify/building_noise_models.

[24] A. Rockenbauer, A kvantummechanikán innen és túl, Scolar, 2017.