Milyen kérdéseket vet fel az oktatás területén a kvantumszámítógépek megjelenése?

Biró Csaba[1,2], Koczka Ferenc[1,3], Prantner Csilla[1]

{biro.csaba, koczka.ferenc, prantner.csilla}@uni-eszterhazy.hu
[1] Eszterházy Károly Katolikus Egyetem
[2] Eötvös Loránd Tudományegyetem
[3] Nemzeti Közszolgálati Egyetem

Absztrakt. A kvantumszámítógépek megjelenése várhatóan jelentős változásokat indukál az informatika területén. A teljesen újszerű elveken működő számítógépek korábban nem megoldható problémákra hozhatnak hatékony megoldást. Az Európai uniós és magyar törvénykezésben megjelentek már azok a rendeletek, amelyek ráerősítenek arra, hogy egyre közelebb vagyunk a kvantumszámítógépek időszakához. Úgy gondoljuk, hogy az oktatásnak és a tanároknak lépést kell tartaniuk a technológiai fejlődéssel, hogy ne érje váratlanul az informatika szektorban jövőben elhelyezkedő diákokat, legyen szó informatika tanárok, fizikusok vagy programozók képzéséről. Tanulmányunkban néhány külföldi példát mutatunk be, ahol a kvantuminformatika témakörei a képzések bizonyos szintjein már bekerültek az oktatásba.

Kulcsszavak: kvantuminformatika, kvantumfizika, általános iskola, középiskola, felsőoktatás, specializáció, STEM, oktatás.

1. Bevezetés

A kvantumszámítógépek kutatásairól szóló hírek begyűrűztek hétköznapi életünkbe, az online és nyomtatott sajtó tudományos rovatainak hasábjain mindennaposak a kvantuminformatikával kapcsolatos hírek, találgatások, spekulációk és a nagyvállalatok [11] fejlesztéseiről szóló tudósítások. Megjelentek a tengerentúlon az Európai Unióban és Magyarországon is a poszt-kvantum titkosítással kapcsolatos és a kvantumszámítógépek fejlesztésének támogatására irányuló jogszabályok és rendelkezések is [22, 23, 24, 41, 52, 63].

Ezek megszületése egyértelműen felszínre hozza a kvantumszámítógépekkel kapcsolatos érdeklődést, találgatást, adatbiztonsági és jelszóvédelmi kérdéseket. Egyre sürgetőbbé válik, hogy az emberek hiteles forrásokból szerezzenek ismereteket a kvantumszámítógépek működéséről, fizikai alapjairól, alkalmazási területeiről, jelenlegi fejlesztésekről, valamint a témával kapcsolatosan várható társadalmi és gazdasági hatásokról.

Fontossá vált néhány kérdés: pontosan mit is jelent a kvantumszámítógép, milyen fogalmak kapcsolódnak hozzá, mi a kvantumadatok tárolásának, továbbításának az alapegysége, ezt hogy értelmezzük, hogyan tároljuk és egyáltalán hogyan működnek a kvantumszámítógépek? Milyen fizikai elvek mentén lehet ezeket a gépeket megépíteni? Várhatóan felváltják-e a kvantumszámítógépek a mai számítógépeinket, hol lehet látni, kipróbálni, beszerezni ilyen újszerű elven működő gépet?

2. Rövid történeti áttekintés

A klasszikus értelemben vett kvantummechanika gyökerei az 1800-as évek elejére, empirikus fizikai-kémiai kutatásokra vezethetők vissza. A hőmérsékleti sugárzás és színképelemzés kapcsolatának vizsgálatakor fekete vonalakat találtak a színképben [7, 8, 54, 55]. Ez az anomália számos újabb és újabb kérdés elé állította a kutatókat, amelyek megválaszolása közben az 1900-as évek elejére a kérdések, már a közben önálló tudománnyá váló kvantummechanika területéről érkeztek.

Az 1900-as évek elejére a spektrumokat helyesen leíró, de a klasszikus elméleti megközelítéseket használó kutatások sorra kudarcot vallottak. Planck új utat választott az atomi oszcillátorok fizikai tulajdonságainak értelmezéséhez a fenomenologikus termodinamika helyett az entrópiából indul ki [49, 50]. Az entrópiafüggvény és a termodinamikai valószínűség közötti kapcsolat már ismert volt, illetve az is, hogy egy izolált rendszer egyensúlyi állapotában veszi fel a maximális értékét. Feltevése az volt, hogy egyes termodinamikai valószínűséghez tartozó mikroállapotok száma megszámlálható, ez pedig csak abban az esetben lehetséges, amennyiben az energiát részekre (véges nagyságú energiaadagokra) osztjuk. Másképp megfogalmazva, a hőmérsékleti sugárzás (mechanikai oszcillátor) energiája nem folytonos, hanem kvantált. Kvantumhipotéziséről 1900. december 14-én Berlini Királyi Porosz Akadémia tudományos ülésén számolt be "Ueber das Gesetz der Energieverteilung im Normalspectrum" című előadásában, ezt a napot tekintjük a kvantumfizika születésnapjának.

Ez igazi paradigmaváltás volt, amelyet a tudományos irányvonalat meghatározó vezető fizikusokból álló közösség fenntartásokkal fogadott, és csak évekkel később ratifikált. A kezdeti bizonytalanság azonban nem szabott gátat az új irányzat kibontakozásának az 1900-as évek első három évtizedében évről-évre sorra dőltek meg a régi, és az újonnan született eredmények egyaránt. Az első évtized végére a kvantumfizikával párhuzamosan, egy új tudományág is napvilágot látott, a relativitáselmélet.

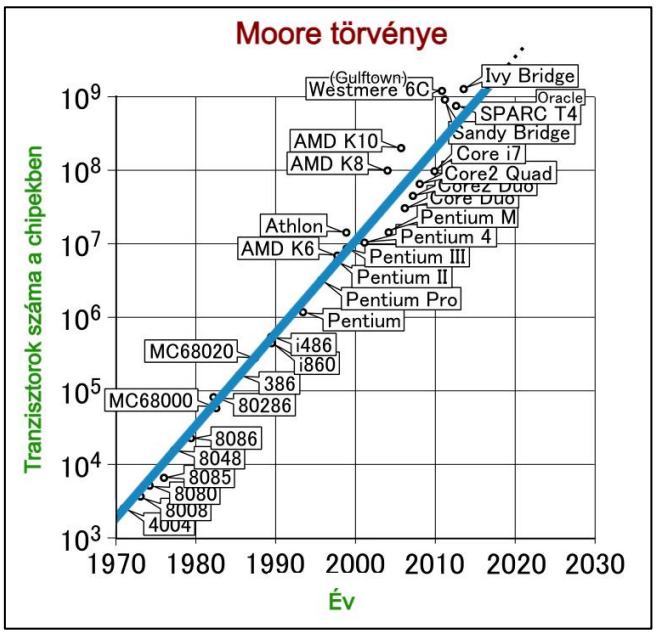
3. A hagyományos számítógépek fejlődésének határai

A kvantumszámítógépek építésére, mint új technológiára amiatt is van nagy igény, mert a jelenleg használatban lévő, Neumann-elvű számítógépek hamarosan elérik – sőt, néhány szempontból már el is érték − technológiai fejlődésük határát, erre a következő három grafikon által megjelenített tendenciák, világosan rámutatnak.

Moore-törvénye nagyon jól szemlélteti a klasszikus számítógépek rohamos mértékű, technológiai fejlődését. Valójában nem törvényről, hanem egy tapasztalati megfigyelésről van szó, miszerint az integrált áramkörökben lévő tranzisztorok száma 1,5 évente megkétszereződik. A megfigyelés Gordon E. Moore-nak, az Intel egyik alapítójának a nevéhez fűződik, aki az 1965-ben az *Electronics Magazine*-ban megjelent cikkében írt először az általa megfigyelt tendenciáról [27]. Habár Moore eredeti megfogalmazása nem pontosan úgy szólt, ahogyan az elterjedt, mindenesetre a processzorgyártók fejlesztési tempójára nagy hatással volt. Az eredeti megfogalmazás szerint a legalacsonyabb árú komponens összetettsége évenként nagyjából a kétszeresére nő és a jövőre tekintve ez a fejlődési ütem nem fog jelentősen változni. A chipfejlesztő cégek számára ez a megfigyelés tulajdonképpen egy teljesítendő célkitűzéssé vált, s a jövőre vonatkozóan is mintegy önmegvalósító jóslat működött, azaz teljes egészében prognosztizálta a gyártási menetet sok éven keresztül.

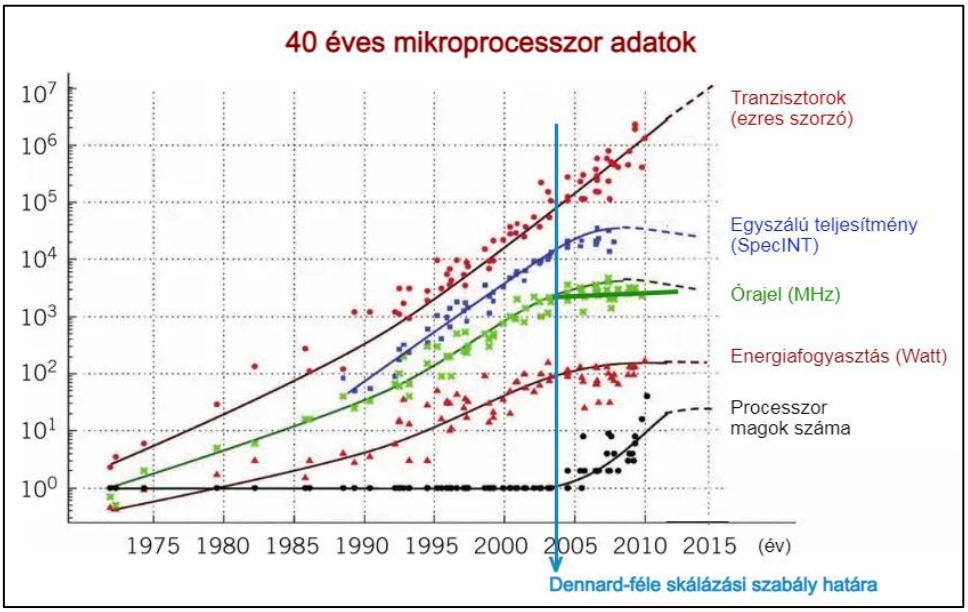
Olyannyira, hogy ennek megfelelően a tranzisztorok korát felváltotta az integrált áramkörök ideje, tehát a klasszikus működési elv megmaradt, csak más technológiai elemekkel oldották meg a kívánt fejlődési ütemet.

Az alábbi grafikonon [56] jól nyomon követhető az integrált áramkörök összetettségének növekedése, amely első ránézésre egy lineáris növekedést mutat, de ha jobban megnézzük, a függőleges tengely logaritmikus skálázású, így érzékelhető, hogy exponenciális növekedésről van szó. A vízszintes tengelyen az egyes processzorok kiadásának éve, a függőleges tengelyen pedig az egyes chipekben lévő tranzisztorok száma került ábrázolásra. Ez azt jelenti, hogy egyre kisebb tranzisztorokat építenek a számítógépchipekbe, ma a legmodernebb processzorok esetében 20x20-as szilíciumatomnyi területen fér el egy tranzisztor. Egyértelmű, hogy ez a fejlődés tarthatatlan, hiszen előbb-utóbb a miniatürizálással elérjük az atomi léptéket és akkor a klasszikus típusú, Neumann-elven felépült számítógépek fejlődése e tekintetben eléri a határt.



1. ábra: Moore-törvény tendenciája. Szerkesztette Prantner Csilla [56] alapján.

Az alábbi extrapolációs grafikonon a mikroprocesszorok jellemzői láthatók az idő függvényében, ezek a következők: tranzisztorok száma, egyszálú teljesítmény, CPU-frekvencia, energiafogyasztás, magok száma [36]. 2004-nél a grafikonon látható egy jelzés, erre az évszámra teszik a Dennard-féle skálázási szabály megdőlését.

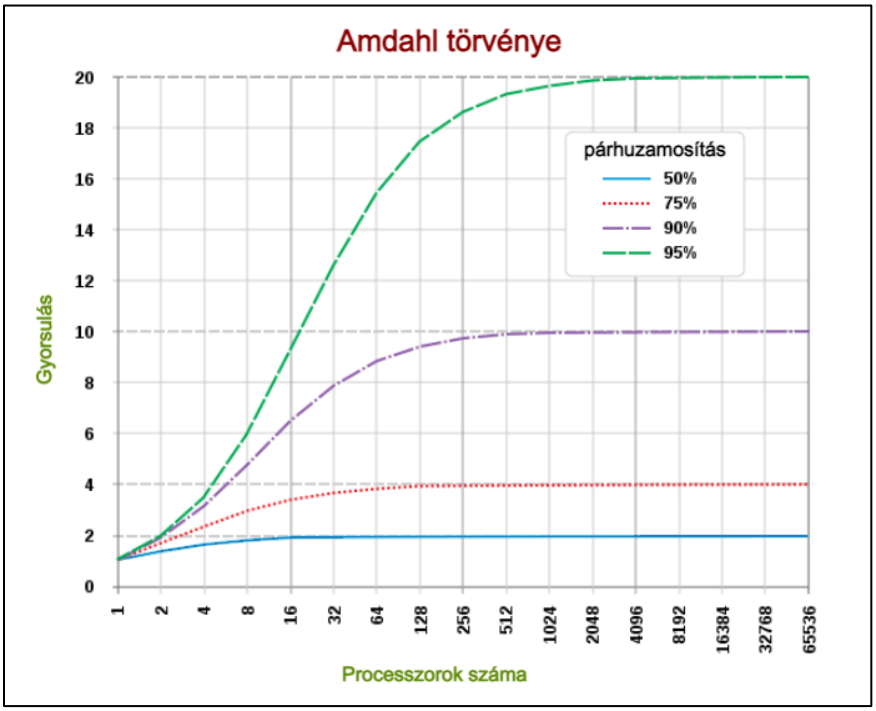


2. ábra: Dennard-féle skálázási szabály. Szerkesztette Prantner Csilla [36] alapján.

A szabályt Dennard skálázási törvényének is nevezik, amely azt mondja ki, hogy a tranzisztorok méretének csökkentésével a teljesítménysűrűség állandó marad, azaz hiába válnak kisebb méretűvé a tranzisztorok, azok ugyanolyan teljesítményre lesznek képesek. Ez a felfedezés előirányozta és biztosította a processzorok nagyiramú fejlesztését jó pár évre. A törvényt eredetileg Robert H. Dennard 1974-es cikkére alapozva MOSFET-ekre fogalmazták meg. [17].

A grafikon a jobb oldalán megjelenő tényezők közül a középsőt vizsgáljuk, ahol az órajel változásának üteme található. 2004-től már lineáris függvényt látunk, azaz 2004 óta 3-4 Hz órajelesek a processzorok. Az utóbbi években tehát nem tudták már az órajelsebességet növelni, márpedig, mivel a számítógépek az órajel ütemére végzik el az utastásokat, ezek elvégzési sebessége sem növelhető. Ez is a jelenlegi, klasszikus számítógépek fejlődésének határát mutatja.

A harmadik diagram Amdahl törvényét szemlélteti, amely a párhuzamos programozással kapcsolatos. Elviekben a párhuzamos programozás lehetőséget ad arra, hogy gyorsítsunk az algoritmusok lefutásán, hiszen egyidőben több processzor tud dolgozni ugyanazon a problémán.



3. ábra: Amdahl törvénye. Szerkesztette Prantner Csilla [17] alapján.

Az IBM-nél is dolgozó, Gene Amdahl 1967-ben az *AFIPS konferencián* beszélt arról, hogy egy párhuzamos feldolgozású programban a viszonylag kevés, egymás után végrehajtandó utasítás, korlátozó tényezőt jelent a program gyorsulására, így több processzor hozzáadásával a program nem feltétlenül fut sokkal gyorsabban. A szakember egy pontos képletet is megfogalmazott megállapítására vonatkozóan [1]. Az alapvető probléma az, hogy kevés olyan feladat van, ami valóban jól párhuzamosítható, azaz hogy az egyes programszálak oly annyira elkülöníthetőek egymástól, hogy azok nem épülnek egymás számításaira, részeredményeire, vagyis egyik programrész futására nincs függésben és nincs befolyással sem egy másikra. A párhuzamosítható problémákra egy jó példa a térképelemzés, amikor például egy nagy területet ugyanakkora méretű, kisebb területekre osztunk fel, és párhuzamosan történik ezek elemzése, például mely részeken található víz vagy erdős terület stb. Az összegzéshez

ebben az esetben is össze kell várni az egyes elemzett területekről kapott eredményeket. A lényeg tehát az, hogy kevés jól párhuzamosítható probléma létezik. Az alábbi diagram jól szemlélteti azt, hogy a bizonyos százalékos arányban párhuzamosítható algoritmusok esetében, mennyit jelent programfutási sebességet illetően a processzormagok számának növelése [66].

Ha feltesszük, hogy olyan problémát oldunk meg, ami 95%-ban párhuzamosítható (zöld szaggatott vonal, csak nagyon speciális esetekben valósulhat meg), akkor is 2048 processzormagnál magasabb darabszám nem hoz már javulást. Amennyiben 50%-osan tudunk már problémákat párhuzamosítani (kék folytonos vonal, ami ritkaság), akkor már 16 magos processzornál nagyobb sem jelent nagyobb gyorsaságot. Tehát efölött a processzormagok gyarapítása inkább reklámfogás, mintsem valóban jól kihasználható lehetőség, hiszen az alapvető határ a programok logikai szinten történő jó párhuzamosításában van.

A bemutatott diagramok mindegyike arra világít rá, hogy elértük a Neumann-elvű számítógépek határait, és egy merőben más alapokon nyugvó technológiában érdemes gondolkodnunk, a különböző fizikai megoldásokon alapuló kvantumszámítógépek ígéretesek e szempontból, amelyek igazi paradigmaváltást jelentenek

4. Kvantumszámítógépek fejlesztése, felhasználási területei

4.1. Felhasználási területei

Az elmúlt évtizedben áttörésnek lehettünk szemtanúi, egyre-másra jelentek meg a kvantumszámítógépek fejlődésével kapcsolatos hírek, melyek hatása különböző területeken lesz érzékelhető. A fejlesztésekbe hatalmas összegeket invesztálnak a vezető nagyhatalmak mellett olyan országok is, mint Ausztrália vagy Svájc. A fejlesztések célja négy fő területre osztható.

Az elsődleges, egyúttal a legszélesebb körben ismert ilyen a mai számítási teljesítmény megsokszorozására irányul, erre alapozva a mai szuperszámítógépeket a jövőben kvantumgépek válthatják le. Az így elérhető számítási teljesítmény számos területen lenne alkalmazható az időjárás előrejelzés hatékonyságának javításától a tudományos kutatásokig [59].

Szintén népszerű alkalmazási terület az anyag- és gyógyszerkutatás, általában minden olyan kutatási terület, amelyben a nagy számítási teljesítményt gyakorlati kivitelezés és tesztelési folyamat kiváltására vagy szűkítésére lehetne alkalmazni [59].

A kvantuminternet a mai hálózati technológiák területén jelenthet ugrást, melynek alapja az összefonódott kvantumbitek kapcsolatán alapuló kommunikációs lehetőség. Ez a szupergyors internetkapcsolat megvalósításán túl egyértelművé teszi az átvitt adatok bizalmasságának sérülését is.

A negyedik fejlesztési irány célja maga a kvantumszámítógép tökéletesítése, egy ilyen gép megépítése még napjainkban is számos problémát vet fel.

4.2. Fizikai megoldási lehetőségek

Egy kvantumszámítógép fizikai működésének pontos megértése kvantumfizikai alapismeretek nélkül meglehetősen nehézkes, ezért esetenként még annak programozói sem ismerik teljes mélységében. Ilyen gépet számos, különböző fizikai jelenség alapján lehet építeni, működésük egyaránt alapulhat a fény polarizációján [31, 46], egy atommag spinjén [6, 37] vagy az elektronok pozícióján.

Mivel a legtöbb gép működése abszolút nulla fok körüli hőmérsékleten, legfeljebb néhány másodpercig tartható fenn, jelenleg is számos kutatás irányul további, kedvezőbb tulajdonságú, jobban használható fizikai alap megtalálására.

4.3. Alapvető fogalmak

A *quantum* latin eredetű szó, amely mennyiséget jelent, többes száma a quanta. A szót közvetlenül a latinból Max Planck vezette be a fizikába, 1900-ban, a "létező mennyiség minimális mennyisége"[1] fogalmával; Einstein megerősítette, 1905. A kvantumelmélet 1912-ből való, a kvantummechanika pedig 1922-ből [71]. Ez a lehető legkisebb egység a fizikában, amellyel egy mérhető egység értéke növelhető [53]. Általában az atomi vagy a szubatomi részecskék, például az elektronok, a neutrínók vagy a fotonok tulajdonságaira alkalmazzák [44].

A gép működésének alapja az ún. *qubit*, mely a gép elemi egysége, és leginkább a hagyományos számítógépek bitjéhez hasonlítható, attól azonban jelentősen eltér. Míg egy bitnek kétféle (nulla vagy egy) értéke lehet, addig egy qubit ezeket és ezek között bármilyen értéket felvehet, akár egyidőben is, ez az ún. *szuperpozíció*. Szuperpozícióban a kvantumrészecskék tehát az összes lehetséges állapotnak a kombinációjában vannak ugyanabban az időpillanatban, csak más-más valószínűséggel, ez teszi lehetővé, hogy egy kvantumgép egyszerre nagyon sok értékkel tud számolni, egyes források szerint egy 30 qubites gép a mai leggyorsabb szuperszámítógépek teljesítményével lenne összevethető. A bináris pozíció és a szuperpozíció közötti különbséget például egy pénzérmével jól lehet szemléltetni. A bináris állapotok (fej vagy írás) könnyen érthető. A szuperpozíció viszont ahhoz hasonló, mint amikor a pénzérmét feldobjuk és az folyamatosan pörög. Ekkor bármely érték lehet a végeredmény, minden időpillanatban bizonyos százalékkal (amplitúdóval) veszi fel a lehetséges értékeket, tehát bizonyos százalékkal a fej és bizonyos százalékkal az írás értéket. Egy másik példával élve, ha mondjuk 0-9 egész számok közül keressük egy számítás végeredményét, mindegyik érték egyidőben bizonyos százalékos bizonyossággal lehet a megoldás. A végeredmény az lesz, amely tartósan hozza a legnagyobb valószínűséget, a százalékos arány tehát ott csúcsosodik ki.

Nehézség a kvantuminformatikában, hogy a kvantumrészecskék változnak, ingadoznak folyamatosan, egészen addig, amíg meg nem mérjük őket. A qubitek rendkívül érzékenyek tehát, ennek pedig egyik leghátrányosabb következménye, hogy azok állapotát csupán egyszer lehet kiolvasni, ezt követően az azokban tárolt érték elvész. A kvantumrészecskéknek a szuperpozíció mellett van egy másik, nagyon érdekes tulajdonságuk, ez pedig az *összefonódás*. Amikor a qubitek összefonódnak, akkor egyetlen rendszert alkotnak, és hatással vannak egymásra. Az egyik qubitből származó mérések alapján következtetéseket vonhatunk le a másikra vonatkozóan és viszont. Ha több qubitet adunk hozzá összefonódással egy rendszerhez, akkor a számítógép hatványozottan több információt tud kiszámítani, és bonyolultabb, több változós problémákat is meg tud oldani. Emiatt jó olyan számításokra ez a technológia, ahol sok tényezőt/hatást/összetevőt szükséges egyidejűleg figyelembe venni és ezek egymásra való hatását is figyelembe venni. Az összefonódással korrelálni lehet az egyes kvantumrészecskék mérési eredményeit és a kvantuminformatikában ezt a tulajdonságot kitűnően lehet kamatoztatni.

A *kvantuminterferencia* a qubitnek, a szuperpozíciós tulajdonságuk okán kialakult viselkedése, amellyel az egyik vagy másik értékkel való egybeesés valószínűsége befolyásolható. A kvantumszámtógépek létrehozásának egyik legnagyobb kihívás, hogy az interferenciát a lehető legnagyobb mértékben csökkentsék a pontosabb eredmények érdekében [43].

E cél elérésére többféle technológiát is alkalmaznak, mindegyik esetében a cél a kvantumrészecskék stabilizációjának elérése úgy, hogy manipulálják azok szerkezetét, ezt elérhető például hűtéssel vagy azzal, hogy olyan kémiai vegyületekkel veszik körbe a kvantumrészecskéket, amelyek védik őket a külső interferenciától.

[1] Megfogalmazás angolul az Online etimológia szótárban: "minimum amount of a quantity which can exist;".

A *kvantumszámítógépeknél* a kvantumfizika speciális viselkedési formáit használja ki az informatikai számításoknál úgy, mint például a szuperpozíciót, az összefonódást és a kvantuminterferenciát. Mindezek új elgondolásokat hoznak a hagyományos algoritmusokhoz és programozási módszerekhez képest

5. Kvantumalgoritmusok

A kvantumgépek elméleti kutatásában már a 80-as években komoly eredményeket értek el. David Deutsch megalkotta a logikai kapuk kvantumgépre adaptált változatait [18], 1994-ben pedig Peter Shor publikálta az egyik leghíresebb algoritmust [60], amely a napjainkban alkalmazott rendszerek adatbiztonságát alapjaiban képes megrendíteni.

5.1. Legfontosabb kvantumalgoritmusok

A Deutsch-Jozsa algoritmus [16] volt az első olyan kvantumalgoritmus, amely azon túl, hogy rávilágított a kvantumalgoritmusokban rejlő lehetőségekre, képes volt egy bit-paritás függvény klasszikus algoritmusoknál gyorsabban történő meghatározására. Az ismeretlen logikai függvény bementként egyetlen bitet vár, és egyetlen bitet ad vissza úgy, hogy vagy minden bemeneti bit páros, vagy minden bemeneti bit páratlan. Az algoritmus segítségével egyetlen kvantummméréssel meghatározható az ismeretlen függvény jellege.

A Bernstein-Vazirani algoritmus [21] az előzőtől (Deutsch-Jozsa algoritmus) összetettebb problémák, függvények vizsgálatára ad lehetőséget. Az f függvény a következő: f(x) = a_1x_1 + a_2x_2 + ... + a_n*x_n + b, ahol x az n-bit hosszú bemenet, a_i az x_i-re vonatkozó súly, és b egy konstans. Az algoritmus segítségével egyetlen kvantummméréssel meghatározható az a_i és b értéke.

Grover-algoritmus [30] rendezetlen sorozatok esetében egy optimalizált keresési algoritmus, amely 2^(n/2)-szer gyorsabb, mint a klasszikus keresési eljárások.

Shor-algoritmus [60] tulajdonképpen a faktorizáció optimális algoritmusa.

Simon-algoritmus[15] bit-paritás meghatározására használt algoritmus, amely a klasszikus algoritmusoknál jóval alacsonyabb energiafogyasztással és rövidebb idő alatt képes megoldani a feladatot.

Harrow-Hassidim-Lloyd (HHL) algoritmus[32]: a lineáris egyenletrendszerek megoldására alkalmazott algoritmus, amely kisebb memóriaigény mellett, sokkal gyorsabb, mint a hasonló feladatra használt klasszikus algoritmusok.

A VQE-algoritmus [14] a kvantummechanika alapján alkalmazott hibrid algoritmus, amelynek segítségével optimális egyensúlyi állapotokat lehet meghatározni.

5.2. Részletesebben a Shor-algoritmusról

A jelenleg széles körben elterjedt titkosítási algoritmusok jelentős részben a prímtényezős felbontás[2] jelentette matematikai problémán alapulnak. A védelmet az eljárás során keletkező hatalmas prímszámok szorzata nyújtja, melynek ismeretében az azt alkotó prímszámok kiszámítása a hagyományos számítástechnikai környezetben gyakorlatilag kilátástalan.

Shor kvantum algoritmusa ezt a problémát oldja meg: egy szám prímtényezős felbontását végzi el rendkívül nagy sebességgel, így alkalmazása a prímtényezős felbontáson alapuló algoritmusokkal védett informatikai rendszerek egy részét védtelenné teszi.[3] Bár egyes esetekben a működési paraméterek, pl. kulcsméretek módosításával maga az algoritmus használható marad, a gyakorlatban ezeket a

[2] Egy szám prím, amennyiben 1-en és önmagán kívül nincs más osztója. Prímszám pl. a 17. A prímtényezős felbontás egy olyan matematikai művelet, mely egy számot prímszámok szorzatára alakít, pl. a 42 prímtényezős felbontása 2x3x7.

[3] Shor algoritmusa már egy hatqubites kvantumgépen működtethető, ilyen gép már évek óta rendelkezésre áll.

módosításokat gyakran csak az egyes rendszerek fejlesztői képesek elvégezni. A ma legelterjedtebb kriptoalgoritmusok védelmi képességeit a poszt-kvantum[4] világban az alábbi táblázat írja le.

Algoritmus	Alkalmazási terület	Fenntarthatóság
AES	Titkosítás	nagyobb kulccsal biztonságos
SHA-2, SHA-3	Lenyomatképzés	Hosszabb kimenet szükséges
RSA	Digitális aláírás, kulcs egyeztetés	Nem biztonságos
ECDSA, ECDH	Digitális aláírás, kulcscsere	Nem biztonságos
DSA	Digitális aláírás, kulcscsere	Nem biztonságos

1. táblázat: A titkosítási algoritmusok alkalmazhatósága a poszt-kvantum világban. Szerkesztette Koczka Ferenc.

A Shor algoritmus csak egy példa a kvantumgép paradigmaváltó hatására, olyan algoritmusokat kell találni és a jelenlegi rendszerekbe is beépíteni, amelyek képesek ellenállni kvantumgép hatalmas számítási teljesítményének. Az Amerikai Nemzeti Szabványügyi Hivatal (NIST) Számítógépbiztonsági Központja által folytatott kutatás harmadik fázisában több kvantumbiztos algoritmus is publikálásra került, melyek megoldást nyújtanak a hash lenyomatok képzéstől az elektronikus aláírásig. A problémakör kezelését a magyar jogalkotás is megkezdte, ennek eredményeként a 2013 évi L. törvénybe[5] is bekerült a poszt-kvantum algoritmusok alkalmazására való felkészülés követelménye az állami és önkormányzati szervek számára. Bár számos szervezet, így a gazdasági vállalkozások és az oktatási intézmények sem tartoznak a törvény hatálya alá, a tulajdonosi-fenntartói köröknek a jövőben számolniuk kell a rendszereik esetleges kitettségével.

A jelenlegi fejlesztések ellenére kevéssé valószínű, hogy a kvantumgépek ki tudnák váltani a ma használatos számítógépeket. A technikai nehézségeken túl alkalmazási körük rendkívül szűk, a hétköznapi és a gazdasági élet szoftvereinek futtatására nem képesek. A rendkívül felgyorsult fejlesztési folyamat azonban nyilvánvalóvá teszi, a technológia megjelenését a programozók, a fizikusok képzésében és az általános oktatásban is.

6. Oktatás

Nem csak a híreket figyelő emberek számára lényeges tájékozódni ezekről az újszerű számítógépekről, hanem célszerű elgondolkodnunk azon, hogy miként lenne érdemes behozni a témakört az oktatás

[4] A poszt-kvantum azt az informatikai korszakot jelenti, melyben a kvantumszámítógépek alkalmazásának lehetőségével már számolni kell.

[5] Ez a törvény az állami és önkormányzati szervek elektronikus információbiztonságát foglalja keretekbe, az ehhez kapcsolódó végrehajtási rendelet a 41/2015 BM Rendelet, mely a törvénnyel kapcsolatos konkrét teendőket definiálja.

meghatározott szintjeire és szakterületeire annak érdekében, hogy a kvantumszámítógépek megjelenésére és az általuk generált változásokra a társadalmunk fel legyen készítve. Legyen elég szakember a kvantumgépek működtetésére, az általuk esetlegesen okozott károk megelőzésére, kezelésére, a kvantum-adatbiztonság megőrzésére és a kvantumgépek támogatásával végezhető kutatások, fejlesztések véghezvitelére. A kvantumszámítógépek építése kapcsán például a fizikus-, az adatvédelem, a kutatások és fejlesztések kapcsán a programozóképzés erősen érintett.

Gondolni kell a szakemberképzések előkészítésére is, emiatt néhány fogalmat talán már a közoktatás felsőbb évfolyamain érdemes bevezetni. Fontos, hogy a fiatal korosztály tanulói ne legyenek magukra hagyva kérdésekkel a fejükben, hanem a tanárok által előszűrve, rendszerbe szedve és emészthető formába öntve, hiteles forrásból tájékozódhassanak e terület érdemi tartalmáról és tisztában legyenek az összefüggésekkel.

6.1. El vagyunk késve?

Függetlenül, hogy jelenleg hol tart a kvantuminformatika, az oktatás területén, elkéstünk már? A kérdésbe kódolt állítás túl erős lenne, de abban az esetben igaz, ha az elmúlt 15 évben megfigyelhető fejlődési trend ugyanilyen intenzitással folytatódik tovább e területen. Természetesen tudjuk, hogy a kvantuminformatika nem 15, hanem közel 70 éves múltra tekint vissza, a 2000-es évek közepén viszont valamilyen jelentős előrelépésnek kellett történnie. Hogy pontosan mi volt ez, azt nem célunk, és nem is tisztünk fejtegetni. Fogalmazzunk úgy, hogy valami olyan eseménysorozat, ami azt indukálta, hogy napjainkban már akkora a verseny a különböző technológiai óriások [11] között ezen a területen, hogy szinte hetente-havonta jelennek meg cikkek, hírek az újabb fejlesztésekről és eredményekről. Vizsgáljuk meg az okokat, miért van az a félelmünk, hogy valamiről már lekéstünk!

Egyik oka, amit már korábban is említettünk, hogy az informatika ezen új területének fejlődését tekintve az utóbbi 15 évben exponenciális robbanásnak lehettünk szemtanúi. Ismerve a klasszikus oktatási rendszereket, legalább egy évtized, mire az általános iskolától kezdve, egészen a felsőoktatásig, az életkori sajátosságoknak, és a célcsoportnak megfelelő tananyagok − alsóbb évfolyamokon a témával való érintettség, alapozás − megjelennek, illetve beépülnek a tantervekbe. Ami a tananyagba való beépítést még tovább nehezíti, az a következő ok: az informatikai ismereteken kívül ez a terület, magas szintű kémiai, kvantumfizikai és matematikai ismereteket, illetve az eddigiektől eltérően egy sokkal komplexebb problémamegoldási képességet igényel [3]. Problémának tartjuk azt, hogy a felsőoktatás utóbbi években végzett informatikatanárai nem lettek felkészítve ennek az új területnek a fogadására és a jövő nemzedéknek való továbbadására.

Hogy hol tart most a kvantumszámítástechnika? Napjainkban számos kvantumszámítógép [34, 67], illetve szimulátor [13] elérhető, kipróbálható, illetve programozható [35]. A különböző elven működő kvantumszámítógépek szemléltetésére rengeteg online kurzus [12, 20, 65], tutorial [42, 51, 67], illetve animáció érhető el.

6.2. Általános iskola

A digitális átalakulással az informatika az élet szinte minden területét átszövi, a gyerekek egyre gyakrabban találkoznak olyan fogalmakkal, mint a beágyazott rendszerek, a big data, az IoT, a mesterséges intelligencia vagy a kvantuminformatika. Néhány gondolatébresztő kérdést szeretnénk feltenni a korosztályra vonatkozóan:

- Meg kell-e jelennie az általános iskolában a kvantuminformatikai ismereteknek alapozásának?
- Életszerű, hogy az általános iskolában beszéljünk erről a területről?
- Mit jelent ennek a korosztálynak a kvantuminformatika?

A média már napi szinten tesz említést valamilyen színezettel a kvantuminformatikáról. Sajnos elég gyakran negatív aspektusból mutatja be úgy, mint egy, az egész életünket megváltoztató, illetve befolyásoló technológiát, amelynek segítségével a kiberbűnözők képesek akár a bankszámlákat védő

számítógépes rendszereket feltörni. Az ilyen típusú, negatív tartalmú hírek belső feszültséget kelthetnek és kérdéseket indukálhatnak a gyerekekben, amelyekre megnyugtató és kimerítő válaszokat várnak. Úgy gondoljuk fel kell készíteni az informatikatanárokat az ilyen jellegű kérdésekre, fontos, hogy tájékozottak legyenek és szakszerű válaszokat tudjanak adni ezekre. Nem csak a negatív érzelmű kérdésekre kell válaszokat adniuk, hanem azt is el kell tudniuk mondani, hogy a kvantumszámítógép új lehetőségeket teremt például a biztonságos adatátvitelre, új utakat nyit a szimulációk területén, forradalmasíthatja a gyógyszerkutatást, új anyagok fejlesztését, pontosabbá és hosszabb átvon érvényessé teheti a meteorológiai előrejelzéseket stb. A kvantumtechnológia tehát egyszerre lehetőség és kockázat a társadalom számára [10, 58].

Az informatikaoktatás elsődleges célja, hogy a digitális világban történő eligazodáshoz a megfelelő alapokat megteremtse. Az informatika oktatással kapcsolatos kutatásokban egyetértés van abban, hogy a rövidtávon használatos technológiák ismertetése helyett, nagyobb hangsúlyt kell fektetni az alapfogalmak, az algoritmusok, illetve az alapelvek megismertetésére. [2, 48, 64].

Úgy gondoljuk, hogy napjaink informatikatanárának a kvantuminformatika alapjaival tisztában kell lenniük, azért, hogy a közoktatásban tanuló gyerekeket megfelelően tudják tájékoztatni e terület fejlődési irányairól; elkerülhetetlen tehát, hogy az informatikatanárok egyetemi képzésének része legyen.

Azt is elkerülhetetlennek tartjuk, hogy idővel az általános iskolai tananyag része legyen érintőlegesen a felső tagozaton a kvantuminformatika. Ez a korosztály már nap mint nap szembesül a "kvantum" kifejezéssel a médiából, nem csak a kvantumszámítógéppel, hanem például a kvantummobilokkal, a kvantumtelevíziókkal stb. Számukra el kellene mondani azt, hogy egyáltalán mit takar a kvantum szó, milyen fizikai jelenségekre épülhetnek kvantumszámítógépek, segíteni lehet őket abban, hogy el tudják képzelni a működésüket, megértsék ezek célját, megismerjék a kvantumbit fogalmát, érzékeltetni tudjuk velük ennek mértékét és az adattárolásban, számításokban rejlő lehetőségeit, még akkor is, ha egy szakterület felnőtt tanárának sem feltétlenül könnyű ezek megértése.

Mégis fontosnak érezzük, hogy a fogalmakkal találkozzanak és tudják, hogy mire utal a kvantum szó. Sőt, cél volna az is, hogy képesek legyenek felismerni, megszűrni a reklámokban megjelenő tartalmakat, látni, hogy a reklámozott termékekben sokszor nem valódi kvantumszámítógépek vannak, hanem csupán egyfajta "kvantumos" jellemzővel rendelkező készülékekről beszélhetünk. Mint ahogyan az a porszívó sem rendelkezik mesterséges intelligenciával, amely tanulási folyamaton nem esik át, csak infravörös szenzort használva tud az akadály előtt pár centivel megállni. Gondolkodni kell megtanítani a gyerekeket ezekről a dolgokról.

6.3. Középiskola

Míg a 10-14 éves korosztály számára csak az alapfogalmak ismertetésére van lehetőség, addig a középiskolás korosztály számára már egy szinttel mélyebb, elméleti háttérrel megalapozott ismeretkör nyújtható. Az elméleti alapokkal lefektetett tudás átadásának elengedhetetlen feltétele a megfelelő matematikai, illetve kvantumfizikai háttér. Számos tanulmány megerősíti, hogy a kvantuminformatika bevezetése az általános- és középiskolás tananyagba nem csak lehetséges, de szükséges is [3, 25, 33, 45, 47, 57, 58, 67].

Stadermann és munkatársai [61] különböző nézőpontok szerint elemezték 15 ország kvantumfizika tantervét és tanmenetét. A középiskolai szintű kvantumfizika tárgyak nemrég jelentek csak meg a nemzeti tantervekben, beépítésük közel sem volt zökkenőmentes, gyerekcipőben járnak [3]. A fontosabb tartalmi elemek célja, hogy a tanulók betekintést nyerjenek a modern fizikába és alkalmazásaiba, valamit képessé tegye őket e tudományág természetének és aspektusainak megvitatására. A vizsgált országok tanterveinek közös elemei: diszkrét atomi energiaszintek, a fény és az anyag közötti kölcsönhatások, hullám-részecske dualitás, de Broglie-elmélet, Planck-hullámhossz, műszaki alkalmazások, Heisenberg-féle határozatlansági elv, és a kvantumfizika természete is helyet kapnak [40]. A

kihívást jelentő részeket, mint például a kvantumfizika interpretációit, illetve ismeretelméleti aspektusait csak néhány országban tanítják. Általános tapasztalat, hogy az elkészített tantervek még gyerekcipőben járnak, így nem feltétlenül a legjobb tantervek. A jelenlegiek zöme megegyezik egy egyszerűsített egyetemi kvantummechanika kurzus elemeivel. A tantervi innovációk időigényesek, a nemzeti szabályok kidolgozása és módosítása pedig egy összetett, bonyolult folyamat [25]. Olyan elemek [5, 44, 38, 70], amelyek elősegítenék a megértést, mint pl. a kvantumfizika filozófiai vonatkozásai, a kvantumösszefonódás és alkalmazásai, csak a norvég és a német tantervekben szerepelnek.

Anastasia Perry és munkatársai [47] egy tíz fejezetből álló tananyagot készítettek 15-18 éves középiskolások számára, amelyet egy ötnapos kurzus keretében ismertettek velük. A kurzus célja a középiskola és az egyetem közötti kapcsolatteremtés volt. A tananyagot a kvantuminformatika kulcsfontosságú alapfogalmai köré szervezték, melyben nevezetesen a következőkről volt szó: szuperpozíció, kvantummérés és összefonódás. A tananyagban az alapfogalmaktól kezdve a kvantumkapukon és a kvantumalgoritmusokon keresztül eljutnak egészen kvantum-alapú teleportálásig. Fontos megjegyezni, hogy nem feltételezik, az elektromosság, a mágnesesség és a hullámok magas szintű ismeretét, és számítógépes programozási tapasztalat sem szükséges. A kurzus elvégzése előtt és után is kérték a résztvevő diákoktól, hogy soroljanak fel minél több olyan kvantummechanikai, kvantuminformatikai fogalmat, amely eszükbe jut. Azt tapasztalták, hogy a diákok azon túl, hogy jelentősen javítottak a kurzus elején írt felméréshez képest, olyan motivációt kaptak, amely a visszajelzések alapján a fizika és az informatika irányába tereli őket [33].

Pashaei és munkatársai egy olyan online elérhető tananyagot készítettek, amely segítségével hatékonyan bevezethető a kvantuminformatika alapkoncepciói már általános és középiskolai szinten. Azon túl, hogy egy jól használható online tananyagot készítettek, meg is kongatták a vészharangot Kanadában. A kvantummechanika fogalmai nem részei a mindennapi életnek, holott ezek megismerése a tanulókra pozitív hatással lehet motivációs szempontból. Kiemelik, hogy a kvantumfizika és a kvantuminformatika az oktatás korai szakaszában történő bevezetése egy olyan társadalom kialakulásához járulhat hozzá, amely megérti a tudomány fontosságát, illetve hozzá tud járulni a fejlődéséhez, és ezzel az élvonalba emeli azt [45].

A kvantumszámítástechnika területe már kiforrott, és a diákok számára elérhető. Angara és munkatársai kvantuminformatikai workshopok eredményeiről számoltak be. Elsődlegesen olyan diákoknak tartottak rövid workshopokat akiknek a kvantuminformatikával kapcsolatban semmilyen előismeretük és tapasztalatuk nem volt. A programozásalapú megközelítést választották, a Qiskit-en [51] keresztül vezették be a diákokat az IBM Q Experience világába. Tapasztalataik alapján megállapították, hogy a kvantuminformatikai fogalmak középiskolás diákok számára is érthetők, feldolgozhatók. Ők is kiemelik, hogy tapasztalataik szerint a kvantuminformatikával történő korai megismerkedés fejleszti a diákok problémamegoldó képességét, bővíti és hozzájárul az egyetemre történő belépés előtt megszerzendő kompetenciákhoz [3].

7. Konklúzió

Összefoglalva nagyon jó kérdés tehát az, hogy kell-e egyáltalán komolyan foglalkozni ezzel a területtel? Állíthatjuk, hogy hamarosan már része lehet az oktatásnak, akár az általános iskolás oktatásnak érintőlegesen, és a középfokú oktatásnak a fogalmak bevezetésének és a szimulációs kvantumgépek használatának szintjén, hiszen külföldön már látunk erre is jó pár példát?

Jelenlegi ismereteink alapján egyelőre az jelezhető előre, hogy a kvantumszámítógépek nem fogják leváltani a hagyományos, Neumann-elvű számítógépeket, de az elmúlt másfél évtized eredményei [4, 9, 63], illetve a tech-óriások [11] és a nemzeti kormányok jövőbeli tervei [26, 29] alapján szinte biztosan állítható, hogy az elkövetkezendő tíz évben ez egy már szabad szemmel is jól látható szegmense lesz az informatikának.

Nyilvánvaló, hogy mint minden irányzatnak, ennek is vannak olyan követői, illetve kutatói, akik jelentős fenntartásokkal kezelik az eredményeket és a jövőképük közel sem tekinthető bizakodónak. Véleményük szerint lehetetlen általános célú, akár csak a jelenlegi számítási kapacitás eléréséhez szükséges qubittel rendelkező, elfogadható hibahatáron belül dolgozó kvantumszámítógépet készíteni [39].

Mindezek tükrében azt tudjuk mondani, hogy érződik, és érthető az oktatás területén a kísérletezési kedv és a bizonytalanság egyaránt. De úgy látjuk, ha a kvantumszámítógépek megrekednek a jelenlegi szinten, azaz csak jól specifikált részfeladatok és valódi véletlenszámok generálására lesznek alkalmasak, már akkor is bevethetők a problémamegoldó képesség fejlesztésére, a látókör bővítésére, az időkomplexitás fogalmának mélyítésére, a fizika népszerűsítésére vagy a kvantumfizika megértésének elősegítésére [19].

8. Irodalom

1. Amdahl, G. M.: *Validity of the single-processor approach to achieving large scale computing capabilities.* In AFIPS Conference Proceedings vol. 30 (Atlantic City, N.J., Apr. 18-20). AFIPS Press, Reston, Va., (1967) 483–485
2. Andreas Schwill. 1997. Computer science education based on fundamental ideas. In Information Technology. Springer, 285–291.
3. Angara, P. P., Stege, U., & MacLean, A. (2020, October). Quantum Computing for High-School Students An Experience Report. In 2020 IEEE International Conference on Quantum Computing and Engineering (QCE). IEEE. (2020) 323–329
4. Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., ... & Martinis, J. M.: *Quantum supremacy using a programmable superconducting processor*. Nature, 574(7779), (2019) 505–510.
5. B. C. Grau, How to teach basic quantum mechanics to computer scientists and electrical engineers, IEEE Trans. Ed. 47, 220 (2004).
6. Bauman NP., Liu H., Bylaska EJ. (et all):*Toward quantum computing for high-energy excited states in molecular systems: quantum phase estimations of core-level states* In Journal of Chemical Theory and Computation (2021) 201–210
7. Berg, H.: *Historical roots of bioelectrochemistry* Experientia 36 (1980) 1247–1249
8. Berg, H., Richter K., Ritter J W.: *Entdeckungen zur Elektrochemie, Bioelektrochemie und Photochemie* In Ostwalds Klassiker der Exakten Wissenschaften, Bd 271. Leipzig, Harri Deutsch; 2., Aufl. edition (1997)
9. Boixo, S., Isakov, S. V., Smelyanskiy, V. N., Babbush, R., Ding, N., Jiang, Z., ... & Neven, H.: *Characterizing quantum supremacy in near-term devices*. In Nature Physics, 14(6), . (2018) 595–600
10. Cao, Y., Romero, J., & Aspuru-Guzik, A. (2018). Potential of quantum computing for drug discovery. IBM Journal of Research and Development, 62(6), 6-1.
11. Chakraborty M.: *Top 10 Quantum Computing Companies to Watch Out in 2021* In Analytics Insight (2021) https://www.analyticsinsight.net/top-10-quantum-computing-companies-to-watch-out-in-2021/ (utoljára megtekintve: 2022.11.11.)
12. Class Centra Portal: *Quantum Computing Courses*. https://www.classcentral.com/subject/quantum-computing (utoljára megtekintve: 2022.11.20.)
13. Dargan J.: *Top 63 Quantum Computer Simulators For 2022*. The Quantum Insider Portal (2022) https://thequantuminsider.com/2022/06/14/top-63-quantum-computer-simulators-for-2022/ (utoljára megtekintve: 2022.11.20.)
14. Colless, J. I., Ramasesh, V. V., Dahlen, D., Blok, M. S., Kimchi-Schwartz, M. E., McClean, J. R., ... & Siddiqi, I. (2018). Computation of molecular spectra on a quantum processor with an error-resilient algorithm. Physical Review X, 8(1), 011021.
15. Daniel R. Simon (1997) "On the Power of Quantum Computation" SIAM Journal on Computing, 26(5), 1474–1483,
16. David Deutsch and Richard Jozsa (1992). "Rapid solutions of problems by quantum computation". Proceedings of the Royal Society of London A. 439: 553–558.

17. Dennard, Robert H.; Gaensslen, Fritz; Yu, Hwa-Nien; Rideout, Leo; Bassous, Ernest; LeBlanc, Andre: *Design of ion-implanted MOSFET's with very small physical dimensions*. IEEE Journal of Solid-State Circuits. SC-9 (5) (1974) 256–268
18. Deutsch, David: *Quantum theory, the Church–Turing principle and the universal quantum computer.* Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences 400.1818 (1985) 97–117
19. Dyakonov, M.: *When will useful quantum computers be constructed? Not in the foreseeable future, this physicist argues. Here's why: The case against: Quantum computing.* Ieee Spectrum, 56(3), (2019) 24–29
20. Edx Portal: https://www.edx.org/learn/quantum-computing (utoljára megtekintve: 2022.11.20.)
21. Ethan Bernstein and Umesh Vazirani (1997) "Quantum Complexity Theory" SIAM Journal on Computing, Vol. 26, No. 5: 1411-1473
22. Európai Parlament*: A digitális évtizedre vonatkozó uniós kiberbiztonsági stratégia (2022/C 67/08)* (2022) https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=OJ:C:2022:067:FULL&from=EN (utoljára megtekintve: 2022.11.11.)
23. Európai Parlament: *Az Európai Parlament 2022. május 3-i állásfoglalása a digitális korban a mesterséges intelligenciáról* (2022) https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_HU.html (utoljára megtekintve: 2022.11.11.)
24. Európai Tanács: *A Tanács (EU) 2022/576 Rendelete*, I. melléklet (2022) https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=OJ:L:2022:111:FULL&from=HU (utoljára megtekintve: 2022.11.11.)
25. Fullan Michael: *Change Forces: Probing the Depth of Educational Reform* (Falmer Press, London, UK, 1993).
26. Gidney, C., & Ekerå, M.: *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits*. Quantum, 5, 433. (2021)
27. Gordon E. Moore: *Cramming more components onto integrated circuits.* Electronics, Volume 38, Number 8, April 19 (1965) https://hasler.ece.gatech.edu/Published_papers/Technology_overview/gordon_moore_1965_article.pdf (2013) (utoljára megtekintve: 2022.11.11.)
28. Gesche Pospiech: *Teaching the EPR paradox at high school?*, Phys. Educ. 34, 311 (1999).
29. Gouzien, E., & Sangouard, N.: *Factoring 2048-bit rsa integers in 177 days with 13 436 qubits and a multimode memory*. Physical Review Letters, 127(14), 140503 (2021)
30. Grover, L. K. (1996, July). A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 212-219).
31. Harrison J., Sellars MJ., Manson NB.: *Measurement of the optically induced spin polarisation of N-V centres in diamond* In Diamond and Related Materials, Volume 15, Issues 4–8, April–August (2006) 586–588
32. Harrow, A. W., Hassidim, A., & Lloyd, S. (2009). Quantum algorithm for linear systems of equations. Physical review letters, 103(15), 150502.
33. Hughes, C., Isaacson, J., Turner, J., Perry, A., & Sun, R. (2022). Teaching quantum computing to high school students. The Physics Teacher, 60(3), 187-189.
34. IBM Quantum Portal: *Real quantum computers.* https://quantum-computing.ibm.com/ (utoljára megtekintve: 2022.11.20.)
35. IBM Quantum Portal: *IBM Quantum Composer.* https://quantum-computing.ibm.com/composer/docs/iqx/ (utoljára megtekintve: 2022.11.20.)
36. Jim X. Chen: *The Evolution of Computing: AlphaGo*. Computing in Science & Engineering Volume: 18, Issue: 4, July-Aug. (2016) https://ieeexplore.ieee.org/abstract/document/7499782 (utoljára megtekintve: 2022.11.11.)
37. Kloeffel C., Loss D.: *Prospects for spin-based quantum computing in quantum dots* In Annual Review of Condensed Matter Physics, Vol. 4:51-81 (Volume publication date April 2013) (2013)

38. Kohnle, A., Bozhinova, I., Browne, D., Everitt, M., Fomins, A., Kok, P., ... & Swinbank, E.. A new introductory quantum mechanics curriculum. European Journal of physics, 35(1), 015001 (2013).
39. Landauer, R.: *Irreversibility and heat generation in the computing process*. IBM journal of research and development, 5(3), (1961) 183–191
40. Lobato, T., & Greca, I. M. (2005). Quantum Theory contents insertion in High School curricula. Ciência & Educação (Bauru), 11, 119-132.
41. Magyarország Kormánya: *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról* https://net.jogtar.hu/jogszabaly?docid=a1300050.tv (2013) (utoljára megtekintve: 2022.11.11.)
42. Microsoft Portal: *Tutorial: Explore quantum entanglement with Q#.* https://learn.microsoft.com/en-us/azure/quantum/tutorial-qdk-explore-entanglement?pivots=ide-azure-portal (utoljára megtekintve: 2022.11.20.)
43. Microsoft Portal: *Introduction to quantum computing.* https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-quantum-computing/#introduction (utoljára megtekintve: 2022.12.20.)
44. Nayak, T., & Dash, T. (2012). A comparative study on quantum pushdown automata, turing machine and quantum turing machine. International Journal of Computer Science and Information Technologies, 3(1), 2932-2935. (angolból idézve: „Quantum is a discrete quantity of energy proportional in magnitude to the frequency of radiation it represents."
45. Pashaei, P., Amiri, H., Haenel, R., Lopes, P. L., & Chrostowski, L. (2020, October). Educational Resources for Promoting Talent in Quantum Computing. In 2020 IEEE International Conference on Quantum Computing and Engineering (QCE) (pp. 317-322). IEEE.
46. Perez-Garcia B., Francis J., McLaren M. (et. all): *Quantum computation with classical light: The Deutsch Algorithm* In Physics Letters A, Volume 379, Issues 28–29, 28 August (2015)
47. Perry, A., Sun, R., Hughes, C., Isaacson, J., & Turner, J. (2019). Quantum computing as a high school module. arXiv preprint arXiv:1905.00282.
48. Peter J Denning. 2004. Great principles in computing curricula. In Proceedings of the 35th SIGCSE technical symposium on Computer science education. 336–341.
49. Planck, M. Ueber das princip der vermehrung der entropie. Annalen der Physik, 267(6), (1887) 189–203
50. Planck, M. *The theory of heat radiation. Entropie* 144(190), 164. (1900)
51. Qiskit Portal: *Tutorials.* https://qiskit.org/documentation/tutorials.html (utoljára megtekintve: 2022.11.20.)
52. Redaktor: *Hatályosak az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény kvantumtitkosításra vonatkozó szakaszai.* EGOV Közigazgatás és Informatika (2022) https://hirlevel.egov.hu/2022/07/10/hatalyosak-az-allami-es-onkormanyzati-szervek-elektronikus-informaciobiztonsagarol-szolo-2013-evi-l-torveny-kvantumtitkositasra-vonatkozo-szakaszai/ (utoljára megtekintve: 2022.11.11.)
53. Reddy, P. P. (2020). Quantum Generators: A Formulation of Computational Models of Multiplication. Google Scholar.
54. Ritter J. W.: *Entdeckungen zur Elektrochemie, Bioelektrochemie und Photochemie* Leipzig, 1986, 135 p.,figuras. Encuadernacion original. Nuevo.
55. Ritter J. W.: *Key texts of Johann Wilhelm Ritter* on the science and art of nature (Vol. 16). Brill. (2010) 1776–1810
56. Robert X. Cringely: *Breaking Moore's Law.* BetaNews. https://betanews.com/2013/10/15/breaking-moores-law/ (utoljára megtekintve: 2022.11.11.)
57. Satanassi, S., Fantini, P., Spada, R., & Levrini, O. (2021, May). Quantum Computing for high school: an approach to interdisciplinary in STEM for teaching. In Journal of Physics: Conference Series (Vol. 1929, No. 1, p. 012053). IOP Publishing.

58. Seegerer, S., Michaeli, T., & Romeike, R. (2021, October). Quantum computing as a topic in computer science education. In The 16th Workshop in Primary and Secondary Computing Education (pp. 1-6).
59. Sejuti Dast: *Top Applications Of Quantum Computing Everyone Should Know About.* (2020) https://analyticsindiamag.com/top-applications-of-quantum-computing-everyone-should-know-about/ (utoljára megtekintve: 2022.11.11.)
60. Shor, P.W.: *Algorithms for quantum computation: discrete logarithms and factoring*. Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc (1994) 124–134
61. Stadermann, H. K. E., van den Berg, E., & Goedhart, M. J. (2019). Analysis of secondary school quantum physics curricula of 15 different countries: Different perspectives on a challenging topic. Physical Review Physics Education Research, 15(1), 010130.
62. Terhal, B. M.: *Quantum supremacy, here we come* Nature Physics, 14(6), (2018) 530–531
63. The White House – National Quantum Coordination Office: *Quantum Frontiers Report on Community Input tot he Nation's Strategy for Quantum Inormation Science* (2020) https://www.quantum.gov/wp-content/uploads/2020/10/QuantumFrontiers.pdf (utoljára megtekintve: 2022.11.11.)
64. Tim Bell, Paul Tymann, and Amiram Yehudai. 2011. The Big Ideas of K-12 Computer Science Education
65. Udemy Portal: *The Complete Quantum Computing Course* https://www.udemy.com/course/quantum-computers (utoljára megtekintve: 2022.11.20.)
66. Wikipedia commons: Amdahl'sLAw. https://commons.wikimedia.org/wiki/File:AmdahlsLaw.svg (utoljára megtekintve: 2022.11.11.)
67. Wootton, J. R., Harkins, F., Bronn, N. T., Vazquez, A. C., Phan, A., & Asfaw, A. T. (2021, October). Teaching quantum computing with an interactive textbook. In 2021 IEEE International Conference on Quantum Computing and Engineering (QCE) (pp. 385-391). IEEE.
68. Xanadu Portal: *Quantum computational advantage on Xanadu Cloud.* https://www.xanadu.ai/ (utoljára megtekintve: 2022.11.20.)
69. Zurich Instruments Portal: *Qubit Control.* https://www.zhinst.com/ (utoljára megtekintve: 2022.11.20.)
70. Dür Wolfgang, and Heusler Stefan: *Visualization of the invisible: The qubit as key to quantum physics*, Phys. Teach. 52, 489 (2014).
71. Online Etymologie Dictonary: *Quantum* notion. https://www.etymonline.com/ (utoljára megtekintve: 2022.12.20.)

Támogató

A kutatást az Innovációs és Technológiai Minisztérium és a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal támogatta a Kvantuminformatika Nemzeti Laboratórium keretében.