# HOGYAN HASZNÁLJUK MAJD A KVANTUM-SZÁMÍTÓGÉPEKET?

Gilyén András
HUN-REN Rényi Alfréd Matematikai Kutatóintézet, Budapest
E-mail: gilyen.andras@renyi.hu

Az ezredforduló táján már az is komoly eredménynek számított, ha kutatók fel tudtak vázolni egy részletes, kísérletileg megalapozott tervet, amely elméletben elvezethet egy általánosan alkalmazható, úgynevezett univerzális kvantumszámítógép megépítéséhez [1]. Neves kutatók szilárdan hittek a technológia megvalósíthatóságában, de jócskán akadtak szkeptikusok, akik úgy vélték, hogy a fúziós erőművek és a kvantumszámítógépek megépítése is folyamatosan a 30 éves távlatban fog kirajzolódni a mindenkori jelenhez képest. Alig három évtized elteltével azonban örömmel láthatjuk, hogy ma már több nagy egyetem és cég is rendelkezik saját fejlesztésű kvantumszámítógéppel, amelyek – bár kis méretük és instabil működésük miatt még nem alkalmazhatóak univerzálisan – már képesek lehetnek tudományosan érdekes eredményeket is elérni. A 2025-ös fizikai Nobel-díjasok – John Clarke, Michel H. Devoret és John M. Martinis – úttörő munkássága jelentős szerepet játszott abban, hogy ilyen gyorsan ilyen messzire jutott a kvantumtechnológia.

## Hibajavítás – az aktuális technológiai mérföldkő

A legnagyobb kihívást jelenleg az jelenti, hogy a klasszikus áramkörök *logikai kapuinak* megfelelő *kvantumkapuk* zajosak, ezért minden egyes lépésben egy kis pontatlanság, hiba jön bele a számításba. A ma elérhető legjobb kvantumkapuk hibája nagyságrendileg $10^{-4}$ körül mozog, ami azt jelenti, hogy tízezer lépés után már jelentős eséllyel rossz eredményt kapunk, százezer lépés után pedig szinte bizonyosan.

Ezzel szemben a klasszikus számítógépek logikai kapuit működtető tranzisztorok hibarátája mintegy húsz nagyságrenddel kisebb [2]. A precíz működéshez ez a megbízhatóság elengedhetetlen, hiszen egy modern processzor sok milliárd tranzisztorból épül fel és az órajel is másodpercenként akár több milliárd számítási ciklust tesz lehetővé. Egy átlagos számítógép- vagy okostelefon-felhasználó számára ez az apró hibaráta szinte észrevehetetlen, és csak néhány kritikus rendszer (pl. a repülőgépek vagy az űreszközök irányítási rendszerei) vagy szuperszámítógép esetében érdemes óvintézkedéseket tenni a potenciálisan megjelenő hibák kiküszöbölésére.

A kvantumos jelenségek törékenysége miatt nem várható, hogy a kvantumkapuk működése belátható időn belül megközelítse a tranzisztorok megbízhatóságát. Ennek az égető problémának a megoldására fejlesztették ki a kutatók a kvantumos hibajavítás és a hibatűrő számítások elméletét, amelynek révén több, kevésbé megbízható *kvantumbit* (vagy röviden *qubit*) és kvantumkapu együttes használatával az itt-ott megjelenő hibák kiszűrhetőek és kijavíthatóak.

A *hibatűrő számítások* során több fizikai, zajos qubit tárolja el redundáns módon a kvantuminformációt, amelyek együttesen úgy viselkednek mint egyetlen sokkal megbízhatóbb qubit – ezt hívjuk *logikai qubitnek*. Viszont ahhoz, hogy a hibajavító módszerek működni tudjanak, az egyes kapuknak önmaguknak is legalább valamennyire megbízhatónak kell lenniük. Ha a kvantumkapuk *fizikai hibarátája* jelentősen nagyobb, mint $10^{-2}$, akkor elméletileg sem ismert olyan módszer, amelynek révén tetszőlegesen csökkenthető volna a *logikai hibaráta*.

A tranzisztorok megbízhatóságának megközelítéséhez jelenlegi ismereteink szerint logikai qubitenként több száz vagy akár ezer fizikai qubit együttes működtetésére is szükség lehet, méghozzá olyan fizikai kvantumkapuk segítségével, amelyek mindegyikének legalább olyan jól kell működnie, mint a ma elérhető legjobb kvantumkapuk. Noha már léteznek körülbelül ezer qubitet tartalmazó csipek, ezek ehhez még összességében túlságosan zajosak. Csak az elmúlt egy-két évben sikerült olyan csipeket létrehozni, amelyek egyszerre elég nagyok és precízek is voltak ahhoz, hogy az összetett hibajavító protokollok alkalmazása ne rontsa, hanem kicsit javítsa a számítások végeredményét.

## A méret a lényeg?

Most, hogy túljutottunk a kvantumos hibajavítás kísérleti demonstrációjának első lépésein, az elkövetkező egy-két évben az várható, hogy ezek a hibajavító eljárások egyre több fizikai qubit alkalmazásával egyre precízebb logikai műveleteket tesznek majd elérhetővé, és akkor már „csak” a fizikai qubitek számának növelése szükséges az univerzálisan alkalmazható hasznos kvantumszámítógépek létrehozásához.

*Gilyén András* matematikus, a HUN-REN Rényi Alfréd Matematikai Kutatóintézet tudományos munkatársa, illetve a Kvantumszámítástudomány Lendület Kutatócsoport vezetője. Az Amszterdami Egyetemen doktorált a kvantumszámítógépes algoritmusok elmélete területén, majd két évet töltött posztdoktorként a Kaliforniai Műszaki Egyetemen (Caltech). 2025-ben ERC Starting pályázatot nyert a természet által inspirált véletlent használó kvantumos algoritmusok kutatására.

Ahhoz, hogy egy kvantumszámítógépnek esélye legyen a klasszikus gépeinket túlszárnyalni, legalább 50 qubitre van szükség, mert a jelenlegi számítógépekkel 40–50 qubit méretig többé-kevésbé szimulálható tetszőleges kvantumszámítógép. Márpedig 50 megbízható logikai qubithez több tízezer szorosan együttműködő stabil fizikai qubitre lesz szükség. Persze hibajavítás nélkül is lehet olyan kvantumáramköröket futtatni, amelyek nem használnak túl sok kvantumkaput, és ezek érdekfeszítő eredményeket is adhatnak, pl. néhány viszonylag egyszerű kvantumrendszer szimulációja során [3]. Mindazonáltal a szakmai konszenzus szerint a kvantumszámítógépek igazán hasznos alkalmazásaihoz szükséges lesz a hibajavított logikai qubitek és kvantumkapuk használata [4].

Az eddigi fejlődés ütemét és az utóbbi évek áttöréseit látva várható, hogy a következő évtizedben megépülnek majd az első olyan kvantumszámítógépek, amelyek képesek lesznek bizonyos feladatokban megbízható módon túlszárnyalni a klasszikus számítógépeket.

## A kvantumszámítógépek valódi ereje

Annak a feltérképezéséhez, hogy mire lesz érdemes kvantumszámítógépeket használni, először is meg kell érteni, hogy hogyan viszonyulnak a kvantumos gépek a jelenlegi klasszikus számítógépeinkhez. A könnyebb összehasonlítás érdekében gondoljunk úgy a klasszikus számítógépekre, mint nagyméretű (elektronikailag megvalósított) logikai áramkörökre, amelyek egy-két bitre ható NEM, ÉS, illetve VAGY kapuból állnak. Ezek a logikai áramkörök közvetlenül lefordíthatóak egy kvantumkapu-hálózatra, vagy röviden kvantumáramkörre. Arra kell csak figyelni, hogy a kvantummechanika *reverzibilis,* ezért bizonyos részszámítások eredményét nem szabad úgy „eldobni" vagy „elfelejteni", mint ahogy egy klasszikus áramkör esetében, hanem végig meg kell tartani a számítások során. Ez azonban nem jelent lényeges megkötést, azaz a klasszikus számítógépekre lényegében tekinthetünk úgy, mint „lebutított" kvantumszámítógépekre, mivel elméletben a kvantumszámítógépeknek minden feladat terén legalább olyan jól kell teljesíteniük, mint a klasszikus számítógépeknek.

### A kvantumszámítógépek gyorsabbak?

Csak azokat az egy-két bites logikai műveleteket tekintve, amelyeket egy klasszikus számítógép is el tud végezni, jelenleg nagy lemaradást láthatunk. Míg a klasszikus számítógépek milliárdnyi logikai műveletet tudnak elvégezni egy másodperc alatt, addig a szupravezetőáramkör-alapú kvantumszámítógépek jelenleg néhány millió kétqubites műveletet képesek elvégezni, a csapdázott ionok esetében pedig csak nagyságrendileg ezer műveletre számíthatunk másodpercenként, míg a semleges atomok teljesítménye az előző kettő közé esik. Ha pedig a hibatűrő számítások logikai szintű működését tekintjük és logikai qubitenként ezer fizikai qubittel számolunk úgy, hogy minden fizikai qubitre átlagosan legalább 20 kétqubites fizikai kvantumkapu hat, akkor alsó becslésként még egy $10^4$-szeres redundanciával kell számolnunk. Ha az erőforrások elemzésében az elemi műveletek számát és idejét összeszorozzuk, akkor azt kapjuk, hogy a szupravezető áramkörök műveletei legalább $10^7$-szer költségesebbek, azaz effektíve „lassabbak", míg a csapdázott ionos rendszerek műveletei $10^{10}$-szer költségesebbek! Noha ezekben a paraméterekben is történt némi javulás az elmúlt évtizedben, alapjában véve azzal kell számolnunk, hogy belátható időn belül a kvantumszámítógépek műveletei sokkal lassabbak maradnak.

### A kvantumszámítógépek hőskora?

Ha ránézünk a ma elérhető kvantumszámítógépekre akkor sok hasonlóságot fedezhetünk fel a klasszikus számítógépek múlt század közepi hőskorával. Az 1940–50-es évek fordulóján a számítógépek szobányi méretűek voltak és működésük tranzisztorok helyett méretes elektroncsöveken alapult. Ha valaki Neumann János mellé állt volna, és azt mondta volna, hogy bő fél évszázad múlva egy ennél sokkal jobb gép ott fog lapulni egy átlagos ember farzsebében, minden bizonnyal bolondnak nézték volna. A mai napig tartó miniatürizációt a tranzisztorok technológiai forradalma tette lehetővé az ötvenes évek végétől kezdve.

*1. ábra. Balra:* Neumann János a vezetésével tervezett és épített IAS számítógéppel a háttérben (1952) [5]. *Jobbra:* John M. Martinis a 2025-ös fizikai Nobel-díjas kvantumszámítógép-vezérlő elektronikával a háttérben a svédországi Chalmers Egyetemen (2021) [6]

A tranzisztorokból épített integrált áramkörök megjelenése egy olyan rendkívüli esemény volt a számítástechnikában, amely lehetővé tette a Moore-törvény által leírt, hosszú évtizedeken át tartó exponenciális fejlődést. Előfordulhat, hogy a kvantum-számítástechnikában is bekövetkezik egy ilyen szinguláris esemény, amely egészen új pályára állítja majd a kvantumszámítógépek fejlődését, de egyelőre ennek nincs különösebb előjele, és ilyen egyszeri fejlődési ugrásokat nem is nagyon lehet megjósolni, főleg a jövőre vonatkozólag.

### A Moore-törvény csak kvantumosan tartható fenn?

Moore megfigyelése szerint az integrált áramkörökben található tranzisztorok száma két évente duplázódik. Ennek a miniatürizációból fakadó exponenciális fejlődésnek a kora napjainkban közelít a végéhez, mivel a mikroelektronikai tranzisztorok mérete egy-két nagyságrendnyire megközelítette a szilíciumatomok méretét. Ebben és az ennél kisebb mérettartományban valóban felerősödnek a kvantumos effektusok, de ezek nem

kontrollált módon jelennek meg, ezért a miniatürizáció önmagában nem vezet univerzális kvantumszámítógépekhez. Ráadásul a kvantumszámítógépek különböző komponensei is atomokból épülnek fel, ezért a kvantumszámítógépek megjelenése nem ad közvetlenül lehetőséget a miniatürizáció további folytatására, tehát a Moore-törvény fenntartásáról nincsen szó.

### Akkor miért építsünk kvantumszámítógépeket?

A kvantumszámítógépek igazi előnye, hogy újfajta műveleteket tesznek lehetővé, amelyek bizonyos problémák megoldására sokkal hatékonyabban használhatóak. Egy kicsit hasonló a helyzet a 32 bites és a 64 bites processzorarchitektúrák közötti váltáshoz, ahol az órajel nem feltétlenül lett gyorsabb, tehát a szó szoros értelmében nem lettek gyorsabbak az új generációs processzorok. Mindazonáltal egy 64 bites processzor elemi utasításkészlete gazdagabb, pl. képes nagy pontosságú 64 bites számokat egy lépésben összeadni, amelyre a 32 bites processzornak több lépésre volt szüksége, így effektíve mégis sokkal hatékonyabban tud dolgozni ilyen műveltekkel. Természetesen a klasszikus számítógépek és a kvantumszámítógépek közötti váltás ennél sokkal fundamentálisabb technológiai ugrás. Ennek megértéséhez viszont kicsit bele kell tekintenünk a kvantumos működési elvekbe.

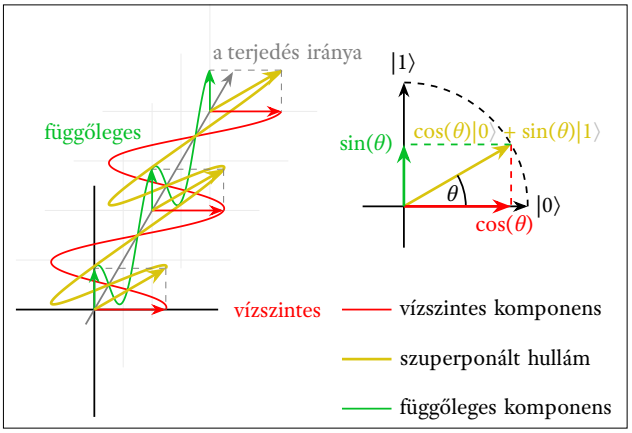
## A kvantumszámítások működése

Mostantól az egyszerűség kedvéért feltételezzük, hogy a kvantumszámítógép hibája elhanyagolható, tehát *logikai* szinten vizsgáljuk csak a működését.

A kvantumszámítógépek qubitekkel dolgoznak, amelyek hasonlóan a klasszikus bitekhez felvehetik a 0 és 1 értékeket. Bármely klasszikus rendszerrel meg tudunk valósítani egy bitet, amelynek van két jellegzetes megkülönböztethető állapota, például egy felfelé vagy lefelé álló kapcsoló, 5 V-os vagy 0 V-os feszültségszint egy áramköri elemben, vagy akár a fekete-fehér négyzetek egy QR kódban.

### A qubitek tulajdonságai és együttműködése

Hasonlóképpen, bármely kvantumrendszer meg tud valósítani egy qubitet, amelynek van két jól megkülönböztethető állapota, amelyeket absztraktul $|0\rangle$-val és $|1\rangle$-gyel jelölünk, ahol a $|\cdot\rangle$ Dirac-jelölés jelzi a kvantummechanikai kontextust. Például egy foton vízszintes és függőleges síkban polarizált állapotát megfeleltethetjük a $|0\rangle$ és $|1\rangle$ qubitállapotoknak. Ezek az állapotok egyértelműen megkülönböztethetőek egy polárszűrő segítségével. Viszont akárcsak egy fénynyaláb esetében, egy foton polarizációjának síkja tetszőleges lehet, például állhat $\theta$ szögben. Egy $\theta$ szögben polarizált hullám függőleges tengelyű amplitúdója $\sin(\theta)$-szorosa a teljes amplitúdónak, míg a vízszintes tengelyű amplitúdója $\cos(\theta)$-szorosa, ezért a $\theta$ szögben polarizált foton a $\cos(\theta)|0\rangle + \sin(\theta)|1\rangle$ qubitállapotnak felel meg, amely a $|0\rangle$ és $|1\rangle$ qubitállapotok *szuperpozíciója*.




*2. ábra.* Transzverzális hullámok szuperpozíciójának szemléltetése. A $\theta$ szögben polarizált hullám felbontható függőleges és vízszintes komponensekre, amelyek amplitúdói trigonometrikus függvényekkel írhatóak le

Ismeretes, hogy egy polárszűrő a fénynek csak az adott irányú komponensét engedi keresztül, a fény intenzitása pedig az amplitúdó négyzetével arányos. Egy foton, ami egy fényrészecske, már tovább nem bontható, ezért az valamekkora valószínűséggel fog csak keresztüljutni, egyébként elnyelődik vagy visszatükröződik. Ha pl. egy függőleges tengelyű polárszűrőt használunk, amely a vízszintes polarizációjú fényt tökéletes tükörként visszaveri, akkor az a fotont csak $\sin^2(\theta)$ valószínűséggel engedi keresztül és $\cos^2(\theta)$ valószínűséggel visszapattan róla. Ha a fotont mindkét irányban egy-egy kamerával detektáljuk, akkor valójában egy kvantummechanikai mérést hajtunk végre, és a fent leírt valószínűségekkel detektáljuk a fényt valamelyik irányban. Viszont mivel a foton egy fényrészecske, a kvantummechanika törvényeinek megfelelően minden alkalommal pontosan az egyik irányban fogjuk érzékelni a fotont, továbbá az áthaladó foton már függőleges polarizációjú lesz, míg a visszapattanó minden esetben vízszintes.

Az egyfoton-qubitek viselkedése könnyen megérthető, ha (lézer-) fénynyalábokként gondolunk rájuk. Az igazán különleges – klasszikus tapasztalatainktól idegen – dolog akkor történik, amikor több (fotonikus) qubit együttes állapotát vizsgájuk. Ha van $n$ qubitünk, akkor ezek külön-külön lehetnek akár $|0\rangle$ vagy $|1\rangle$ állapotban. Például, ha három párhuzamosan terjedő fotonból az első és utolsó függőlegesen polarizált, a középső pedig vízszintesen, akkor jelölhetjük ezt az állapotot $|101\rangle$-gyel, hasonlóképpen az összes függőleges és vízszintes kombinációt leírhatjuk egy 3-hosszú bitsorozattal $|b_1 b_2 b_3\rangle$, ahol $b_i \in \{0,1\}$. A kvantummechanika törvényei szerint viszont ezek a qubitek tetszőlegesen *összefonódhatnak,* vagyis bármely

$$\sum_{b_1 b_2 b_3 \in \{0,1\}^3} \alpha_{b_1 b_2 b_3} \left| b_1 b_2 b_3 \right\rangle$$

szuperpozíció megengedett, azzal a megkötéssel, hogy az $\alpha_{b_1 b_2 b_3}$ amplitúdók abszolútértékének négyzetösszege 1. A vízszintes és függőleges polarizációs irányok mérésekor (hasonlóan az egy qubites esethez) $|\alpha_{b_1 b_2 b_3}|^2$ valószínűséggel detektáljuk a $b_1 b_2 b_3$ polarizációkonfigu-

rációt, és a mérés után a fotonok a mért irányokban lesznek polarizáltak. Tehát a mérés, akárcsak a fenti egyfotonos esetben, visszafordíthatatlanul megváltoztatja a qubitek állapotát.

## Műveletek qubiteken

A kvantumszámítógépek működése logikai szinten rendszerint a következő séma szerint megy. Először minden qubitet beállítunk egy fix, pl. $|0\rangle$ kezdőállapotba, utána különböző egy- és kétqubites kvantumkapukkal módosítjuk a qubitek állapotát, végül megmérjük a qubiteket.

A kvantumfizikai műveletek *lineárisak,* ennek megfelelően a kvantumkapuk is azok. Vegyük például a logikai tagadást mint egybites műveletet; NEM: $0 \mapsto 1$, $1 \mapsto 0$. Az ennek megfelelő $X$ kvantumkapu ugyanígy működik; $X$: $|0\rangle \mapsto |1\rangle$, $|1\rangle \mapsto |0\rangle$. A linearitásból pedig az következik, hogy ez a kvantumkapu szuperponált állapotokon a következőképpen működik: $\alpha|0\rangle + \beta|1\rangle \mapsto \alpha|1\rangle + \beta|0\rangle$.

Általánosságban elmondható, hogy elég ismerni egy kvantumkapu hatását a bemeneti qubitek összes nulla-egy értékekből álló bitsorozatnak megfelelő *bázisállapotán,* a linearitás miatt ez már egyértelműen meghatározza a hatást egy tetszőleges szuperponált állapotra.

Egy másik természetes követelmény, hogy kvantumkapuk csak úgy hathatnak, hogy a qubitek kvantumállapota egy új lehetséges kvantumállapotra változzon. Mivel kikötöttük, hogy a kvantumállapotok amplitúdóinak négyzetösszege 1, ha a kvantumállapotokra úgy gondolunk, mint az amplitúdókból álló vektorra, akkor ez azt jelenti, hogy a kvantumkapuk által leírt lineáris műveletek megőrzik az euklideszi hosszat. Az ilyen műveleteket *unitér operátoroknak* hívják, amelyek a hosszőrzés miatt mindig invertálhatóak (visszafordíthatóak) egy másik unitér operátor által. Ez az oka annak, hogy a mérést leszámítva a kvantumszámítógép műveletei *reverzibilisek*.

Míg klasszikusan az egyetlen nem triviális egybites művelet a logikai tagadás, addig kvantumosan még sok más izgalmas egyqubites kapu létezik. Például az Hadamard-kapu, amely a következőképpen hat

$$H\colon \begin{cases} |0\rangle \mapsto \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big), \\ |1\rangle \mapsto \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big). \end{cases} \tag{1}$$

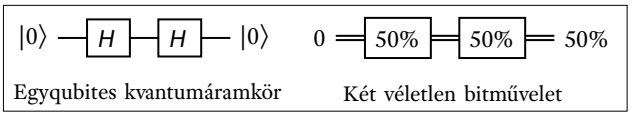
Ezen felül vannak még pl. $\theta$ szögű forgatásnak megfelelő egyqubites kapuk, amelyek a következőképpen hatnak:

$$|0\rangle \mapsto \cos(\theta)|0\rangle - \sin(\theta)|1\rangle,$$
$$|1\rangle \mapsto \sin(\theta)|0\rangle + \cos(\theta)|1\rangle.$$

Egy kvantumszámítógépet *univerzálisnak* hívunk, ha tetszőleges unitér operátor megvalósítható rajta. Ehhez szükség van legalább egy kétqubites műveletre is, mint amilyen például a CNOT (vezérelt negálás), amely a második (qu)bit értékét negálja, ha az első (qu)bit értéke 1:

$$\mathrm{CNOT}\colon \begin{cases} |00\rangle \mapsto |00\rangle, & |01\rangle \mapsto |01\rangle, \\ |10\rangle \mapsto |11\rangle, & |11\rangle \mapsto |10\rangle. \end{cases}$$

## Kvantumáramkörök

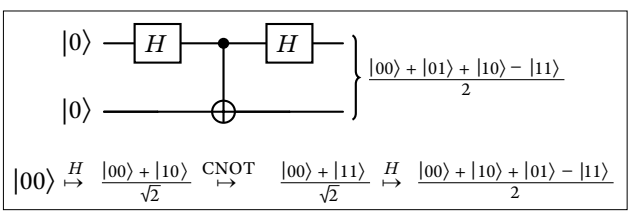



*3. ábra.* Kvantuminterferencia és klasszikus véletlenség

A kvantumkapukból álló hálózatot, ami leírja a kvantumszámítógép műveleteit, kvantumáramkörnek hívják. Például a *3. ábra* bal oldalán egy két kvantumkapuból álló kvantumáramkör látható. Ez az áramkör azt szemlélteti, hogy az Hadamard-kapu önmaga inverze, két lépés után visszaérünk a kezdeti $|0\rangle$ állapotba. Az első Hadamard-kapu után az állapot $(1/\sqrt{2})\,(|0\rangle + |1\rangle)$, amely szuperponált állapot a második Hadamard-kapu hatására *interferenciát* eredményez, és így a kezdeti $|0\rangle$ állapotba jutunk. Ez abból fakad, hogy az (1) egyenletben lévő azonos előjelű amplitúdók *konstruktívan erősítik* egymást, míg az ellentétes előjelűek *destruktívan kioltják* egymást.

Ha azonban az első Hadamard-kapu után egy mérést végzünk, akkor fele-fele eséllyel kapunk $|0\rangle$ vagy $|1\rangle$ állapotot. Ezután a második Hadamard-kaput is végrehajtva a két lehetséges végállapot $(1/\sqrt{2})\,(|0\rangle \pm |1\rangle)$ lesz, amelyeket megmérve ismét fele-fele eséllyel kapnánk $|0\rangle$ vagy $|1\rangle$ eredményt. Tehát ha mindkét Hadamard-kapu után közvetlenül végeznénk egy mérést, akkor egy klasszikus véletlent használó áramkört kapnánk, amely fele-fele eséllyel vagy megtartja vagy negálja a bit értékét, lásd a *3. ábra* jobb oldalát.

Ugyanez a jelenség figyelhető meg, ha a két Hadamard-kapu között nem egy mérést végzünk, hanem „átírjuk" a felső qubit állapotát egy másik qubitéba egy *CNOT* kapu segítségével. Az áramkör után a qubitjeink mérése itt is egyenletes eloszlású véletlen eredményre vezetne:




A *3. ábra* és a fenti áramkör teljesen analóg a híres *kétrés-kísérlethez*, ahol a két résen áthaladó elektron (vagy akár foton) önmagával interferál az ernyőn. Ha azonban megmérjük, hol haladt keresztül az elektron, az interferencia eltűnik. Hasonlóképpen itt az interferencia révén kialakuló $|0\rangle$ végállapot annak az eredménye, hogy az áramkör közepén a $|0\rangle$ és $|1\rangle$ állapot szuperpozíciója van jelen. Ezzel szemben ha középen egy mérést végzünk, akkor a mérési eredménynek megfelelően a $|0\rangle$ *vagy* $|1\rangle$ állapotba kerül a qubit. A felső qubit CNOT-os „átírása" egészen hasonló eredményre vezet, és valójában tekinthető egyfajta közbenső mérésnek is, hiszen az alsó qubit eltárolja, hogy milyen állapotban volt a felső qubit a két Hadamard-kapu között, ami a végén egy méréssel akár ki is olvasható.

Itt érdemes megjegyezni, hogy ilyen és ehhez hasonló középiskolás szintű matematikai leírással számos izgalmas kvantuminformatikai érdekesség megérthető, lásd a *Fizikai Szemle* jelenlegi számában [7], illetve a világ első, ebben a témában írt középiskolás szakköri jegyzetét, amely már magyar fordításban is elérhető [8].

### Párhuzamos számítások szinte ingyen?

A kvantumszámítógépek lehetőséget adnak egy újfajta *kvantumos párhuzamosságra* a számítások során. Ez abból fakad, hogy ha $n$ qubitet veszünk a $|0\rangle$ állapotban, és mindegyikre alkalmazzuk az Hadamard-kaput, akkor az $n$ qubites *uniform szuperpozíciót* kapjuk, amelyben az összes $|b_1 b_2 \ldots b_n\rangle$ bázisállapot amplitúdója $1/\sqrt{2^n}$. Tegyük fel, hogy van egy bonyolult $f: \{0,1\}^n \to \{0,1\}^k$ bináris függvényünk, amely egy logikai áramkörrel adott! Ha az $n$ qubites uniform szuperpozíción felül veszünk $k$ darab csupa $|0\rangle$ állapotú qubitet, és az együttes állapotra alkalmazzuk a logikai áramkörnek megfelelő $U_f$ kvantumáramkört, akkor a következő kvantumállapotot kapjuk:

$$\left|0^n, 0^k\right\rangle \overset{H^{\otimes n}}{\mapsto} \sum_{s\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} \left|s, 0^k\right\rangle \overset{U_f}{\mapsto} \sum_{s\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} \left|s, f(s)\right\rangle. \quad (2)$$

(Az $n$ párhuzamosan ható $H$ kaput $H^{\otimes n}$-nel jelöljük.)

Ahogy a (2) egyenletből is látszik, a kvantumáramkör egyszeri használatával egy olyan kvantumállapotot állíthatunk elő, amely valamilyen értelemben tartalmaz információt a függvény összes lehetséges kiértékeléséről. Viszont nem tudjuk kiolvasni mind a $2^n$ futás eredményét, hiszen ha megmérjük a kvantumállapotot, akkor csak egy egyenletes eloszlású véletlen $n$-hosszú bitsorozatot fogunk kapni a hozzá tartozó függvényértékkel. Egy hatékony kvantumalgoritmus ezért ilyenkor még további lépéseket tesz, hogy az interferencia révén mégis ki tudjon valami olyan hasznos információt nyerni a sok függvényértékből, amelyet klasszikusan költséges volna kiszámítani.

## Hatékony kvantumalgoritmusok

Egy kvantumalgoritmus akkor tud a klasszikus számítógépeknél hatékonyabban működni, ha jól kiaknázza a probléma struktúráját és komplex interferenciák révén jut el gyorsan a megoldásra.

### Faktorizáció és periódus keresés

Talán a leghíresebb példa Shor kvantumalgoritmusa egész számok faktorizálására, azaz prímtényezőkre bontására. Az egyik leghíresebb titkosítási eljárás, az RSA (Rivest–Shamir–Adleman) azon a feltevésen alapszik hogy ha veszünk két több száz jegyű véletlen prímszámot, $p$-t és $q$-t, akkor a $p \cdot q$ szorzatból gyakorlatilag lehetetlen kiszámítani a $p$ és $q$ prímeket, ezért azokat használhatjuk egyfajta privát kulcsként.

Shor algoritmusának egy egyszerű változatával azonban könnyen kiszámítható a két prímtényező. Ehhez vegyünk egyenletes eloszlással egy véletlen $a \in \{2, 3, \ldots, m-1\}$ számot, és vizsgáljuk azt az $f: \mathrm{N} \to \{0,1,2, \ldots, m-1\}$ függvényt, amelyet $f(j) \equiv a^j \pmod m$ alapján definiálunk. Az $f$ függvény klasszikusan hatékonyan kiszámítható az ismételt négyzetre emelés módszerével. Továbbá ez a függvény periodikus $f(j) = f(j + h)$, és jó eséllyel a periódushossz maximális lesz: $h = (p-1)(q-1)$. Ha $h = (p-1)(q-1)$ ismert, akkor $m = p \cdot q$-val együtt kapunk két független egyenletet a $p$ és $q$ ismeretlenekre, és készen vagyunk.

Elegendő tehát, ha a periódushossz kiszámítására találunk egy kvantumalgoritmust. Tekintsük most a (2) egyenletben lévő $n$-hosszú bitsorozatokat úgy, mint binárisan leírt egész számokat 0 és $2^n - 1$ között, azaz

$$\sum_{s\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} \left|s, f(s)\right\rangle = \sum_{j=0}^{2^n-1} \frac{1}{\sqrt{2^n}} \left|j, f(j)\right\rangle.$$

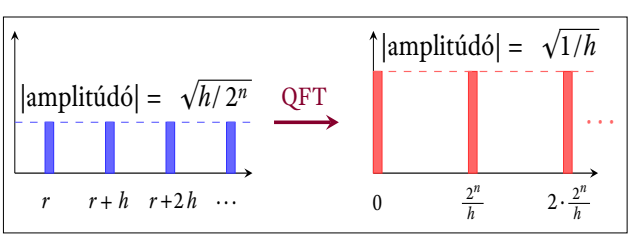
Ha az utolsó $k$ qubitet megmérve a mérési eredmény $f(r)$, akkor az első $n$ qubit az ezzel konzisztens (qu)bitsorozatok szuperpozíciójára redukálódik. Mivel $f(j)$ értéke csak $j$-nek $h$-val vett $r \in \{0,1, \ldots, m-1\}$ osztási maradékától függ, a mérés után kapott állapot felírható úgy, mint

$$\sum_{i=0}^{\ell_r} \frac{1}{\sqrt{\ell_r}} \left|r + i \cdot h, f(r)\right\rangle,$$

ahol $\ell_r = \left\lfloor \frac{2^n - r}{h} \right\rfloor$. Érezhető, hogy ez a kvantumállapot elegendő információt kell hordozzon a $h$ periódushosszról. Viszont ha az állapotot csak egyszerűen megmérnénk, akkor mindössze egy véletlen $g$ számot kapnánk, amelyre $f(g) = f(r)$ teljesül. Ehhez pedig elég lett volna csak egy véletlen $g$ számot venni és aztán kiszámítani $f(g)$ értékét.

Az ötlet az, hogy be kell vetni a jelfeldolgozásban széles körben használt Fourier-transzformációt, mégpedig annak diszkrét verzióját, amely történetesen egy $2^n$-dimenziós unitér operátor. Ezen $n$ qubites kvantum-Fourier-transzformáció (QFT) ráadásul közelítőleg $n \log(n)$ egy- és kétqubites kvantumkapuval implementálható. Ha ekkora dimenziós vektorokat akarnánk Fourier-transzformálni egy klasszikus számítógépen, az exponenciálisan sok számítási lépést igényelne!

Ha olyan szerencsénk van, hogy $h$ osztja $2^n$-et *(4. ábra),* akkor ez a Fourier-transzformáció a $h$ periódusú szuperpozícióból egy $2^n/h$ periódusú szuperpozíciót hoz létre, méghozzá $r$ eltolás nélkül! Ha ezután mérünk, akkor már egy $c \cdot (2^n/h)$ alakú számot kapunk egy egyenle-




*4. ábra.* A kvantum-Fourier-transzformáció után az amplitúdók abszolút értéke és a periódushossz invertálódik, viszont a kezdeti $r$ eltolás eltűnik!

tes eloszlású véletlen $c \in \{0,1, ..., h-1\}$ számra. A kapott számot elosztva $2^n$-nel megkapjuk a $c/h$ törtet, amelynek a nevezője egyszerűsítés után $h$ lesz, feltéve hogy $c$ és $h$ relatív prímek (amire jó esély van). Ha $h$ nem osztja $2^n$-et, de $n$ kellően nagy (pl. $2^n \geq h^2$), akkor egy hasonló, lánctörteken alapuló eljárással megállapítható $h$ értéke.

A kvantumszámítás azért tud ilyen hatékony lenni itt, mert van egy nagyon erős algebrai struktúra, amely lehetőséget ad erős interferencia létrehozására. Több más hasonló absztrakt probléma tekintetében is hatalmas kvantumos gyorsulást tesz lehetővé az algebrai struktúra, viszont ilyen problémák leginkább csak titkosítási eljárások feltörése kapcsán merülnek fel a gyakorlatban.

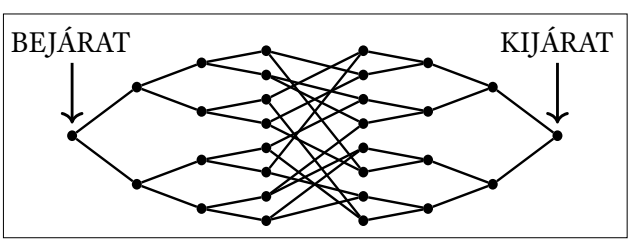
## Keresés anélkül, hogy minden elemre rákérdeznénk

Természetes kérdés, hogy lehet-e az erős struktúra hiányában is érdemben gyorsítani kvantumosan, amelyre Grover algoritmusa ad pozitív választ. Ha van egy $S$ halmazon értelmezett $f$ függvényünk, amelyről mindössze annyit tudunk, hogy egy adott $y$ értéket csak egyszer vesz fel, akkor klasszikusan várhatóan majdnem az összes $f(s)$ értéket ki kell számítanunk, hogy megtaláljuk azt az $x \in S$-beli elemet, amelyre $f(x) = y$. Kvantumosan azonban elég csak nagyjából $\sqrt{|S|}$ alkalommal használni az $f$-et kiszámító (kvantum-) áramkört.

Ez egy sokkal szélesebb körben használható kvantumos gyorsítás, mint pl. Shor faktorizáló algoritmusa, viszont az elérhető gyorsítás exponenciális helyett csupán kvadratikus. Gyakorlati alkalmazásokban azonban nehéz ezt a csekély előnyt aprópénzre váltani, mivel a kvantumszámítógépek jelenleg sok nagyságrenddel lassabbak és költségesebbek, mint klasszikus versenytársaik. Az általános nézet szerint ezért a belátható, egy-két évtizedes távlaton belül olyan alkalmazásokat kell keresnünk, ahol a kvadratikusnál nagyobb kvantumos előny érhető el.

## Kvantumos bolyongások

A véletlen bolyongások kvantumos megfelelőit régóta vizsgálják, mivel ezek sok esetben kvadratikusan gyorsabban terjednek, ezáltal hatékonyabb keresést tesznek lehetővé Grover algoritmusával rokon módon. Azonban ritka esetben ennél jóval nagyobb, exponenciális gyorsulásra is lehetőséget adnak ezek a bolyongások, például leveleik mentén kétszeresen, véletlenszerűen összekötött $n$-mélységű bináris fák esetében, mint az *5. ábrán* látható.




*5. ábra*. Két bináris fa, leveleik mentén összekötve

Ennek a gráfnak az a speciális tulajdonsága, hogy a be- és kijáratot leszámítva minden csúcshoz három él tartozik. Ezért, ha nincs ilyen szépen térben elrendezve a gráf, akkor a bejáratból indulva a gráfot lokálisan felderítve nagyon nehéz megtalálni a kijáratot, mert a levelek véletlenszerű összeköttetésein átjutva nem lehet tudni melyik él visz a be-, és melyik a kijárat felé. Viszont a kvantumbolyongás nem igényli az irányok ismeretét: az interferencia miatt a gráf úgy viselkedik, mintha egy egyszerű vonal lenne, így a kijárat gyorsan megtalálható.

Viszont ez a struktúra nem nagyon jelenik meg természetes problémákban. Ami talán még nagyobb gond, hogy hiába találja meg a kijáratot a kvantumos bolyongás, úgy tűnik, nem tud megtalálni egy utat a be- és kijárat között. Ha ugyanis az utat elkezdi megjegyezni a bolyongás, az interferencia a kétrés-kísérlethez hasonlóan megszűnik.

Sok másik kvantumalgoritmus is hasonló nehézségekkel küzd: erős strukturális feltételekhez kötött, és csak nagyon limitált információt tud hatékonyan kinyerni.

## Számítások magas dimenziós vektorokkal

A kvantumszámítógépek műveletei exponenciálisan nagy dimenziós vektorokkal és azokon vett unitér operátorokkal írhatóak le. Ezekbe az unitér operátorokba pedig beágyazhatóak más magas dimenziós lineáris operátorok is, amelyek számos tudományos számítás során hasznosak lehetnek, pl. sokváltozós lineáris egyenletrendszerek vagy differenciálegyenletek numerikus megoldásában. Noha a magas dimenziós vektorokat hűen reprezentálják a kvantumszámítógép belső állapotai, ezeket csak nehezen, sok-sok mérés és ismételt próbálkozás révén lehet egy klasszikusan kezelhető vektorrá lefordítani.

Ahhoz, hogy ki tudjuk aknázni ezt az exponenciális állapotteret, olyan problémákat kell keresni, ahol a kívánt végeredmény megkapható a vizsgált vektorok néhány egyszerű, alacsony dimenziós vetületével. A kvantumszimulációt leszámítva, ahol tipikusan csak néhány fizikai mennyiség érdekes, nagyon nehéz ilyen problémákat találni. Ez annyiban talán nem meglepő, hogy Richard Feynman éppen a kvantumos szimulációk lehetővé tétele céljából javasolta a kvantumszámítógépek kifejlesztését.

## Hogyan tovább?

A kvantumos szimuláció már egy évtizeden belül is kecsegtet olyan eredményekkel, amelyek klasszikus számítógépekkel elérhetetlennek tűnnek, és anyagtudományi, majd kvantumkémiai áttörésekre is elvezethetnek. Bizonyos heurisztikus optimalizálási algoritmusok is ígéretesnek tűnnek, de ezen kívül nem látszik más jól körvonalazott, lőtávolban lévő gyakorlati alkalmazás. Ez a Google kvantumalgoritmusokra specializált kutatócsoportját is aggasztja [9], ezért figyelemfelhívásul

az XPRIZE Alapítványon keresztül létrehoztak egy 5 millió dollár összdíjazású versenyfelhívást, amelynek keretében a pályázóknak a kvantumszámítógépek minél hamarabb elérhető alkalmazásait kell kidolgozniuk. 2025 decemberében e cikk szerzőjének csapata („Gibbs Samplers") is bekerült a verseny hét döntős csapata közé, szintén egy kvantumszimulációs eljárás továbbfejlesztésével, amely akár optimalizációs feladatokra is alkalmazható lehet [10].

Összegzésként elmondható, hogy több specifikus számítási problémában elengedhetetlen lesz a kvantumszámítógépek használata. Bár a megbízható kvantumszámítógépek megépítése egy óriási technológiai áttörés lesz, mégsem várható, hogy akkora hatással legyen a hétköznapi életre, mint a klasszikus számítógépek forradalma tette. Ugyanakkor bizakodásra ad okot, hogy a klasszikus számítógépek ekkora térnyerését sem lehetett előre jósolni azok hőskorában, és valószínűleg sok fontos alkalmazás a kvantumszámítógépek megjelenésével karöltve alakul majd ki.

## Irodalom


1. Cirac J. I., Zoller P. (1995): Quantum computations with cold trapped ions. *Physical Review Letters,* 74, 4091.
2. Zimborás Z. (2022): Kvantumszámítógépek – mítosz és valóság. MTA Tudományünnep+, 2022. november 8. (lásd: YouTube, 2022)
3. Zimborás Z., Koczor B., Holmes Z., Borrelli E.-M., Gilyén A., Huang H.-Y. et al. (2025): Myths around quantum computation before full fault tolerance: What no-go theorems rule out and what they don't. *arXiv:* 2501.05694.
4. Dalzell A. M., McArdle S., Berta M., Bienias P., Chen C.-F., Gilyén A., et al. (2025): Quantum algorithms: A survey of applications and end-to-end complexities. Cambridge University Press.
5. Richards A. felvétele. Köszönet a princetoni Institute for Advanced Study-nak a közlés engedélyezésért.
6. Köszönet a Chalmers Egyetemnek a közlés engedélyezésért.
7. Tóth Kristóf (2026): A kvantummechanikai valószínűségekről középiskolában. *Fizikai Szemle,* 2026/1, 27–33.
8. Ozols M., Walter M. (2018): Kvantumküldetés. https://gilyen.hu/kvantumkuldetes.html
9. Babbush R., King R., Boixo S., Huggins W., Khattar T., Low G. H., et al. (2025): The Grand Challenge of Quantum Applications. *arXiv:* 2511.09124.
10. Az XPRIZE Quantum Applications döntősei (2025): https://telex.hu/techtud/2025/12/11/xprize-quantum-applications-verseny-magyar-csapat-donto-gibbs-samplers-algoritmus-kvantumfizika