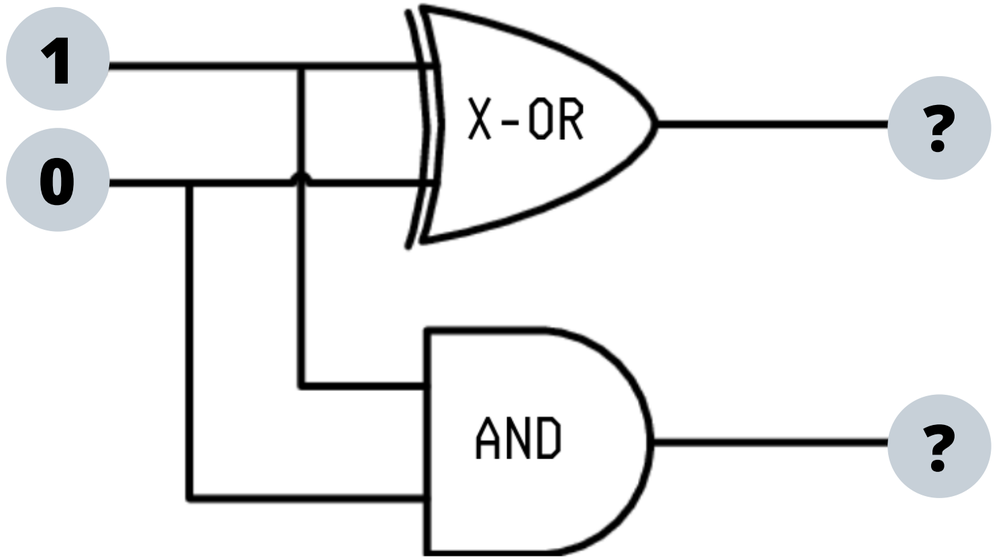
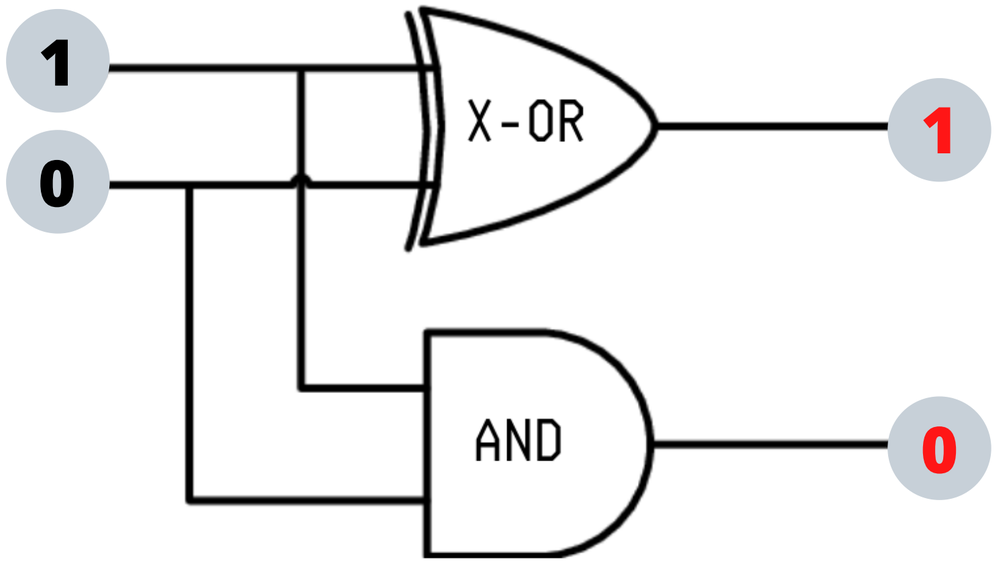
Klasszikus bitek - ismétlés

A klasszikus számítógép alapegységei a **bitek**. Ezek **logikai értékű** változók, melyeket **logikai kapukkal** összekötve összetett műveleteket végezhetünk.

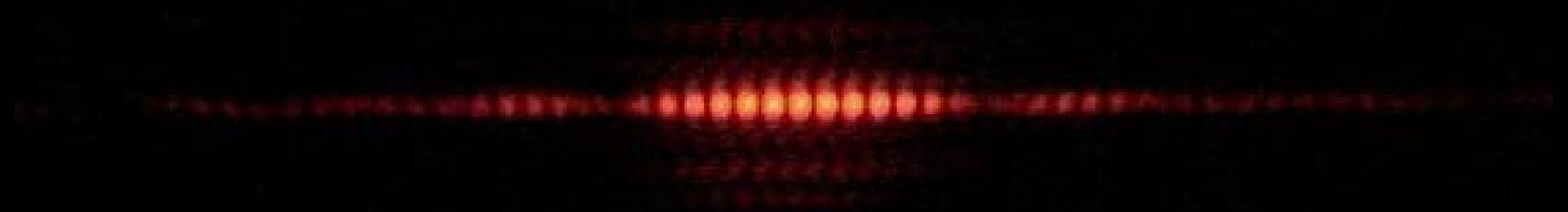


Klasszikus bitek - ismétlés

A klasszikus számítógép alapegységei a **bitek**. Ezek **logikai értékű** változók, melyeket **logikai kapukkal** összekötve összetett műveleteket végezhetünk.



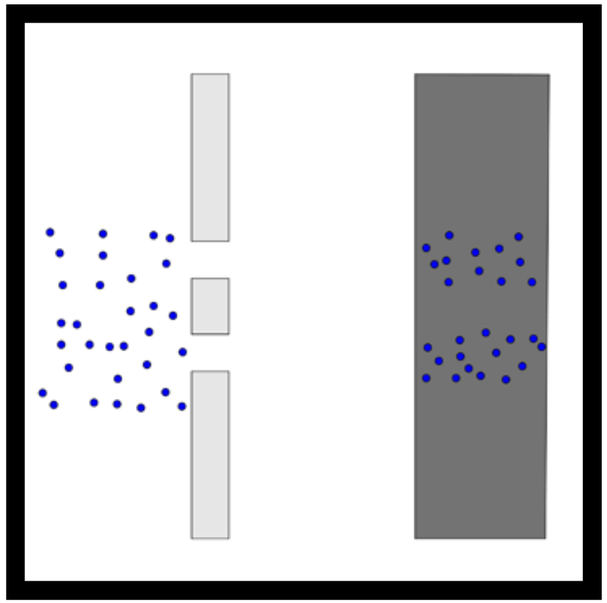
Mi lehet ez?



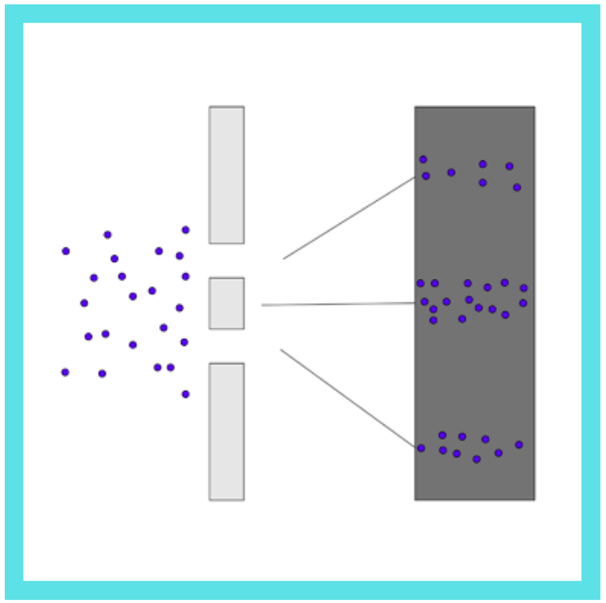
Double-slit experiment

Mi történik, ha részecskéket lövünk át két résen egy lemezre, és megfigyeljük, hova érkeznek?

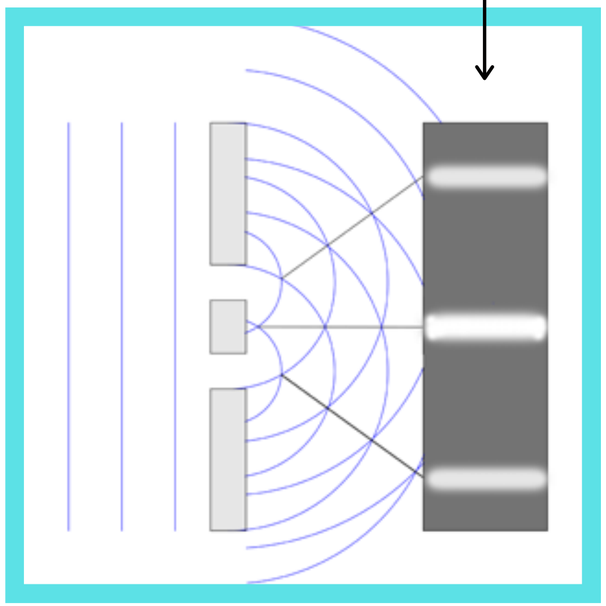
A fenti képen ez a mintázat látszik



Labdák: áthaladnak vagy az egyik, vagy a másik résen, és ennek megfelelően két sávban érik a falat.



Részecskék: a hullámra jellemző interferencia-mintázatban érik a falat! Ez akkor is így van, ha egyenként lőjük ki őket. (**Animáció!**)

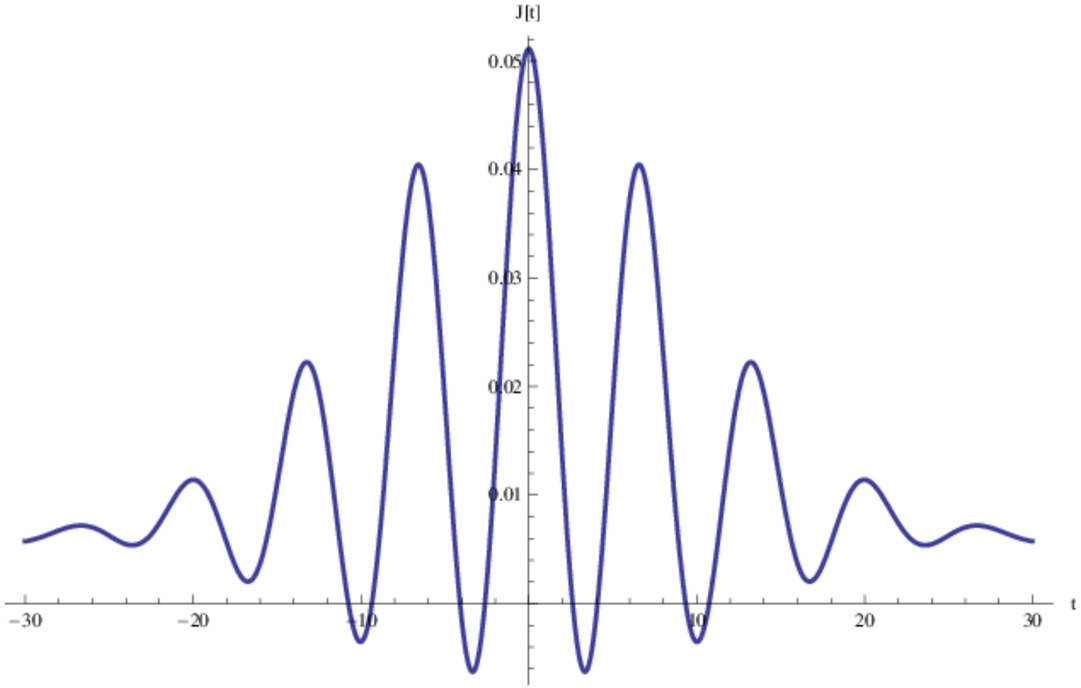


Hullám: a két résen áthaladó hullám interferenciába kerül önmagával, és mintázatot alkot (**Animáció!**).

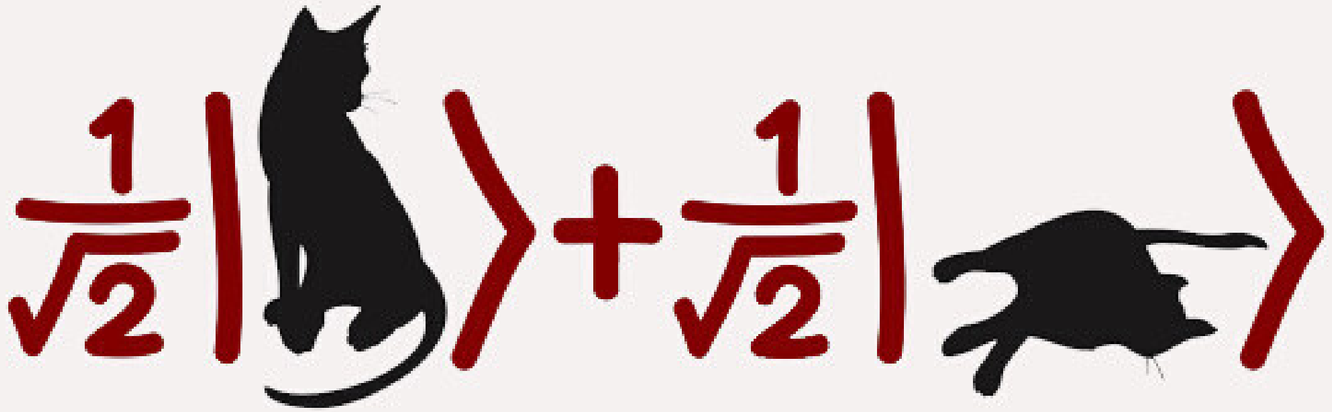
Hullám-részecske kettősség

A részecskék **egyszerre viselkednek részecskeként és valószínűségi hullámként.** A balra látható hullámfüggvény írja le a részecske állapotát és mozgását.

A hullámfüggvény mérés hatására összeomlik. Ha a már résnél megfigyeljük a részecskéket, megszűnik az interferencia-mintázat.

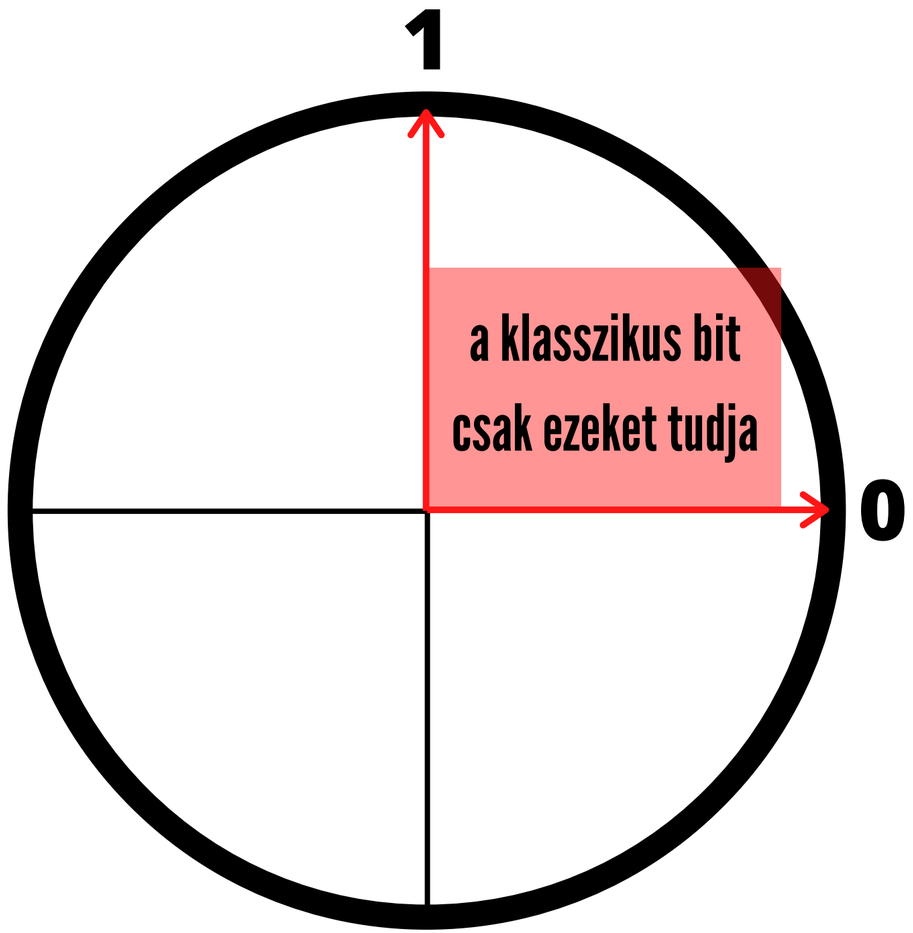


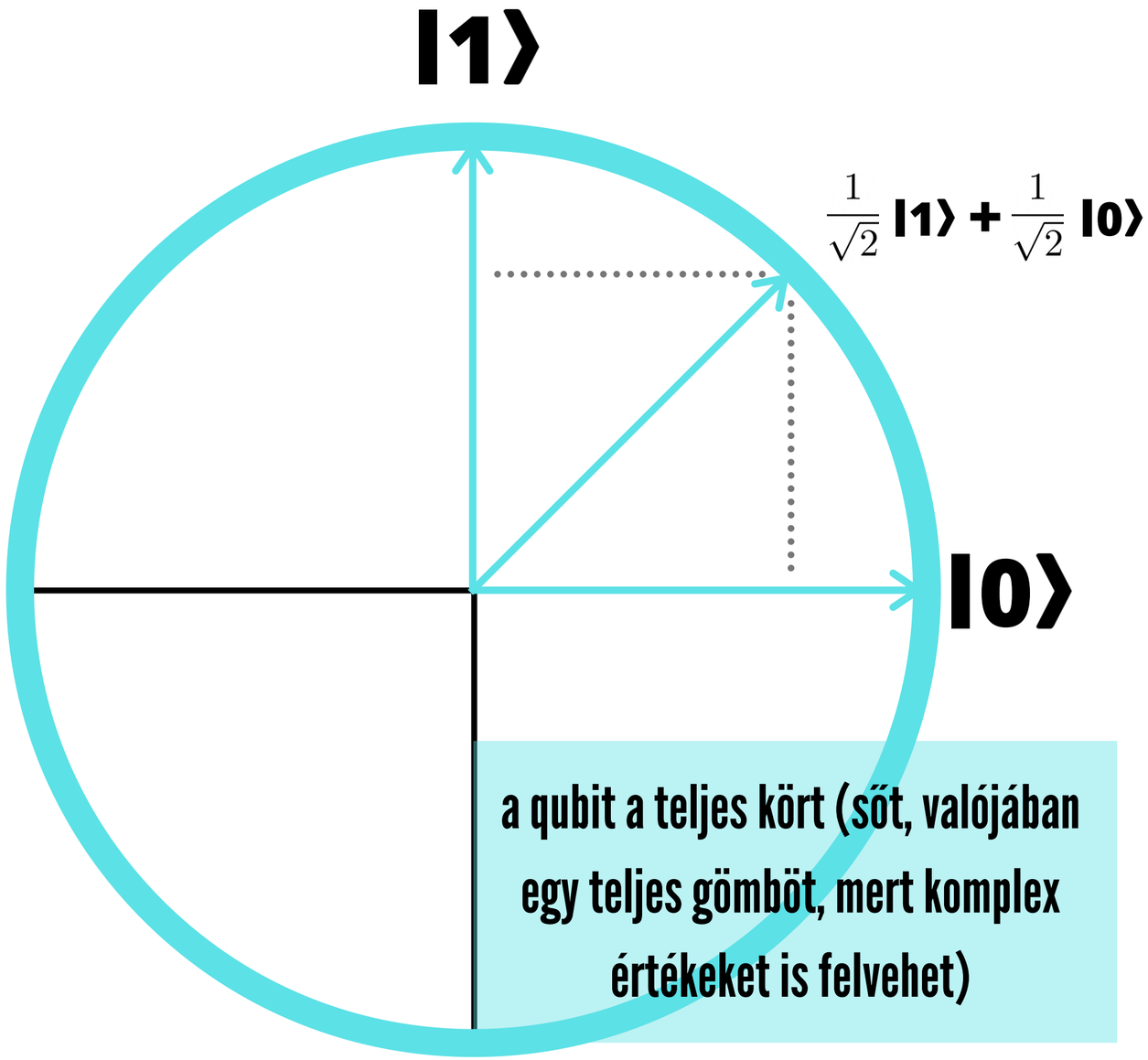
Scrödinger macskája



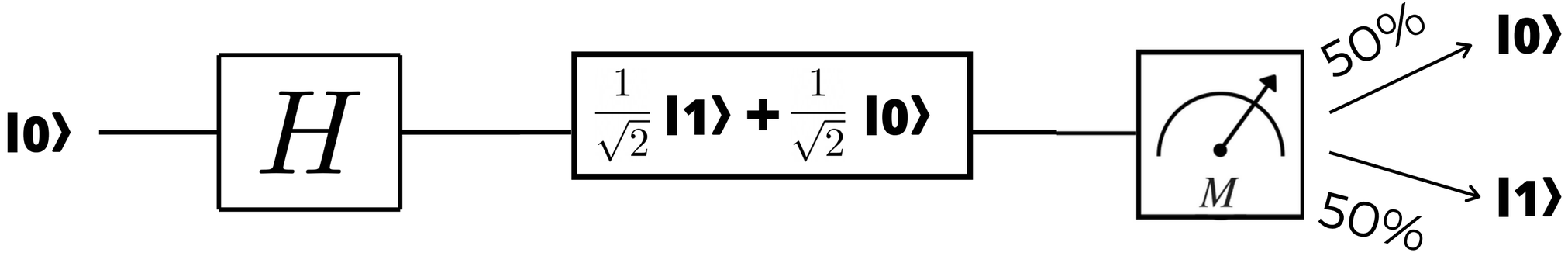
50% valószínűséggel lesz halott, illetve élő állapotban, **ha megfigyeljük**! De a megfigyelés pillanatáig **egyszerre** halott, és élő.

A kvantum-számítógép speciális bit-jei, a **qubit**-ek, képesek schrödinger macskájaként viselkedni.


1
0
a klasszikus bit
csak ezeket tudja


|1⟩
$\frac{1}{\sqrt{2}}$ |1⟩ + $\frac{1}{\sqrt{2}}$ |0⟩
|0⟩
a qubit a teljes kört (sőt, valójában egy teljes gömböt, mert komplex értékeket is felvehet)

Példák kvantum-logikai kapura



A **Hadamard-kapu** egyenletes eloszlású **szuperpozícióba** helyezi a qubitet.

A **Mérés-kapu** értelemszerűen mérést végez a qubit-en, ezzel összeomlik a hullámfüggénye, és klasszikus bit-állapotot vesz fel.

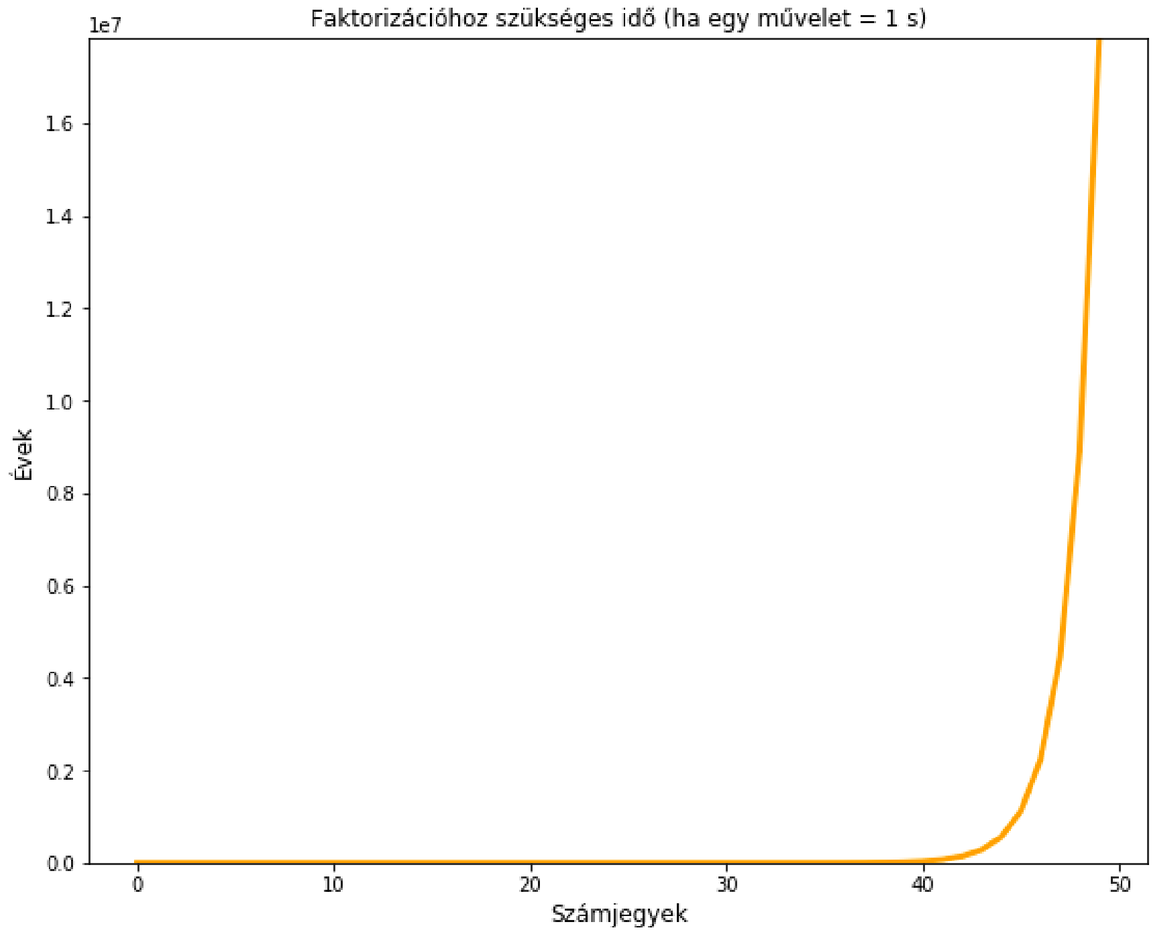
Mire jó mindez?

Bonyolultság és a Shor algoritmus

Veszünk két gigantikus prímszámot, és összeszorozzuk őket.

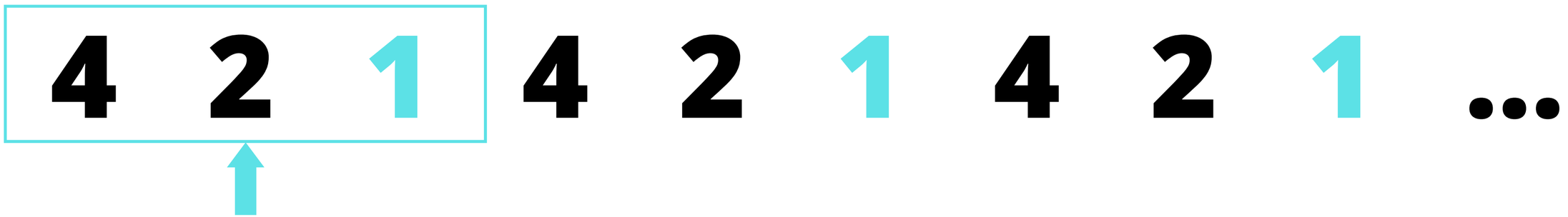
A feladat: a szorzatból **visszafejteni a prímtényezőket.** A Shor algoritmus ennek egy lehetséges (és eddig ismert leghatékonyabb) megoldása. Ennek a futási ideje **a számjegyek függvényében exponenciálisan növekszik**.

Ezért nem meglepő, hogy a legtöbb titkosítási protokoll erre alapszik, és elég jól működnek.



Megoldás kvantum-számítógéppel

Adott egy N hosszúságú mintázat:



Erre a periódusra vagyunk kíváncsiak, ami jelen esetben 3, de kellően nagy N mellett hatalmas lehet.
A legrosszabb esetben végigpróbálunk minden számot N-ig. Ennek a megtalálása kerül a számjegyek függvényében exponenciális időbe klasszikus számítógéppel.

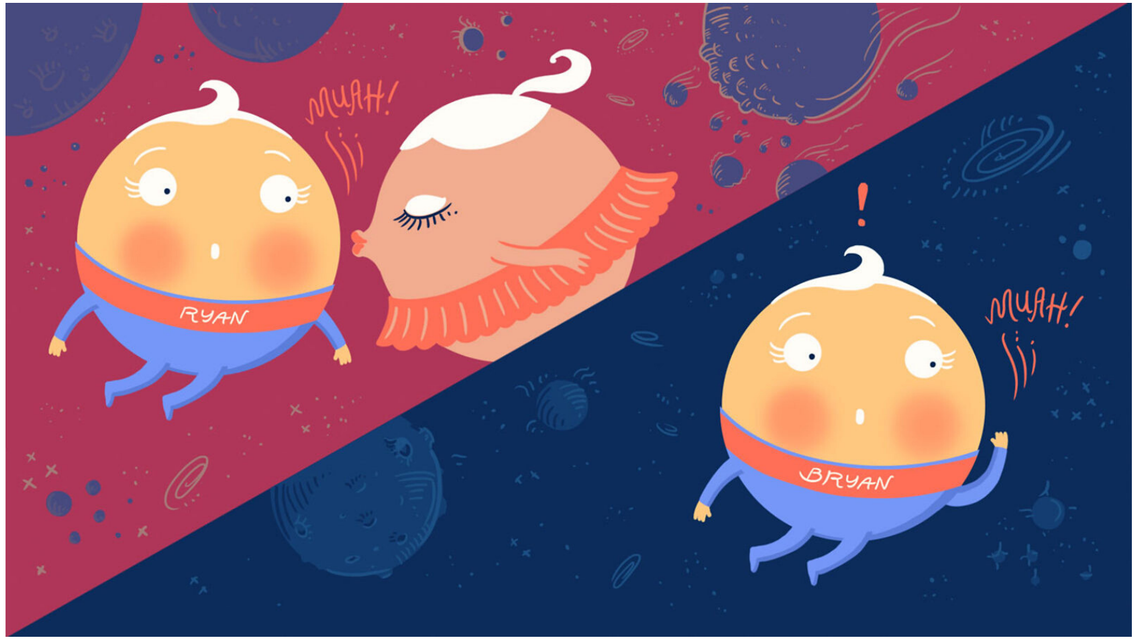
Megoldás kvantum-számítógéppel

4 2 1 4 2 1 4 2 1 ...

A kvantum-számítógép a szuperpozíció segítségével egyszerre próbálja ki az összeset. Bár egyszerre csak egy megoldást tudunk megmérni, lehet úgy manipulálni a szuperpozíciót, hogy a helyes megoldás jóval nagyobb valószínűséggel jöjjön ki. Így elég párszor lefuttatni a számítást, és a leggyakoribb érték lesz a megoldás. Ez lényegében olyan, mint a double slit experiment esetében az interferencia-mintázat: egy lefuttatás egy kilőtt elektronnak felel meg, és a helyes megoldásnál alakulnak ki a sávok.

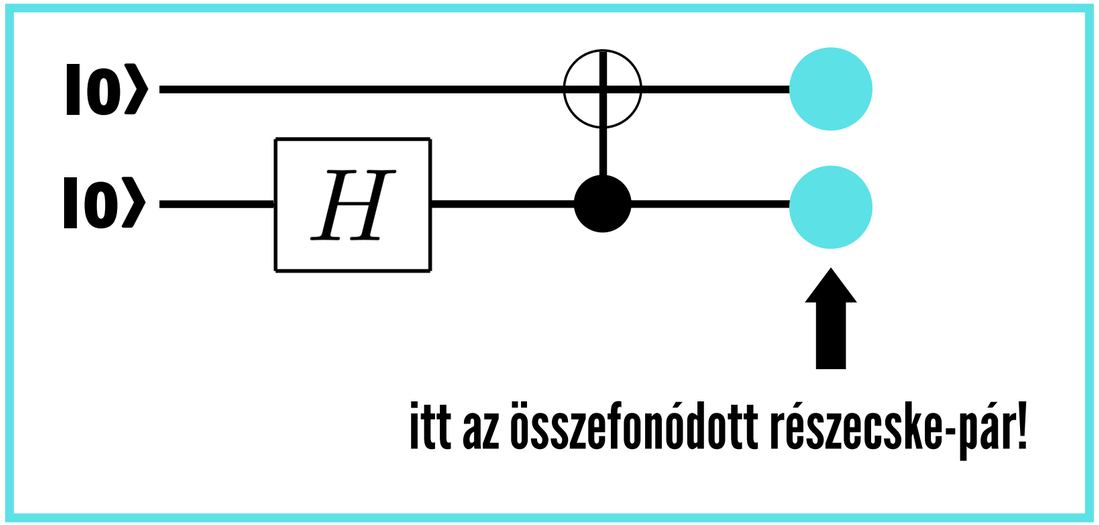
"Spooky action at a distance" avagy kvantum-összefonódás

Összefüggés két részecske kvantum-állapota között: ha az egyiket megmérjük, az állapota meghatározza a másik állapotát. **Ez nagy távolságokon keresztül is azonnal működik, tehát a fénysebesség nem korlátja!**



Hogyan készül és mire jó?

Csinálunk rengeteg összefonódott részecske-párt, és beletesszük két külön számítógépbe. Ezután ezek között a számítógépek között végtelen sebességgel lehet "teleportálni" qubitokat.



Kihívások

- **Kvantum-dekoherencia**: a környezet folyamatosan "meg akarja mérni" a qubiteket, ezért nehéz egy ekkora rendszert szuperpozícióban tartani

- Hipotézis: a qubitek számával **exponenciálisan növekszik a zaj**, ezért lehetetlen értelmezhető méretű kvantum-számítógépet építeni

- A Google Sycamore nevű kvantum számítógépe jelenleg 53 qubit-tel működik, ami azt jelenti, hogy több mint 10,000,000,000,000,000 kombinációt tud tárolni