

Kvantumszámítógép a munkára fogott kvantummechanika

Széchenyi Gábor
ELTE, Anyagfizikai Tanszék



Atomoktól a csillagokig, 2019. április 25.

Kvantumszámítógép a hírekben

Az IBM bedobozolja a kvantumszámítógépet

Eddig csak laborkörülmények között lehetett használni őket, de a CES-en teljes pompájában működött az IBM Q System One.



Mégse fordították meg az időt az orosz fizikusok :(

Egy kvantumszámítógépben állították vissza az egyik elektron állapotát a korábbi stációba, képletesen szólva visszafordították az idő kerekét. Több se kellett a médiának!



Láttam a jövőt, és olyan volt, mint egy villanybojler

Az IBM svájci kutatóközpontjában megnézhattünk egy működő kvantumszámítógép-prototípust. Kész időutazás volt; egyszerre idézte az informatika hajnalát és a két évtized múlva beköszöntő jövőt.



A Google ettől a csiptől várja a kvantumszámítógépes áttörést

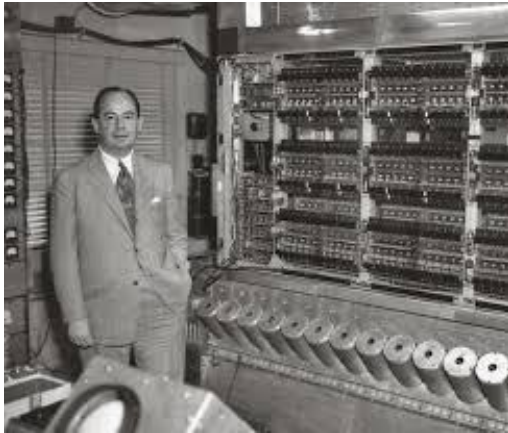
A cég szerint az új processzoruk lehet majd első, ami gyorsabb lesz a hagyományos gépeknél.

Megalakult a nagy magyar kvantumösszefogás

3,5 milliárdos állami támogatással elindult a Nemzeti Kvantumtechnológiai Program. A kvantumverseny fokozódik, a hazai kutatók se akarnak lemaradni. Készül az európai kvantuminternet, csak legyen hozzá elég nanogyémánt.



Egy új technológia



1940-es



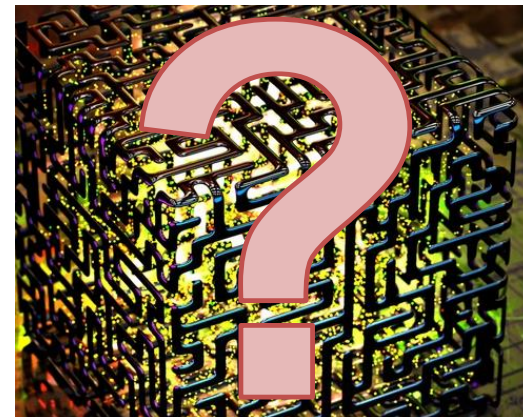
1980-as



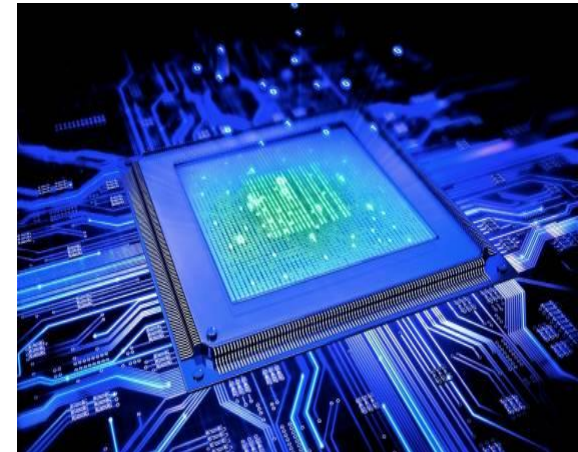
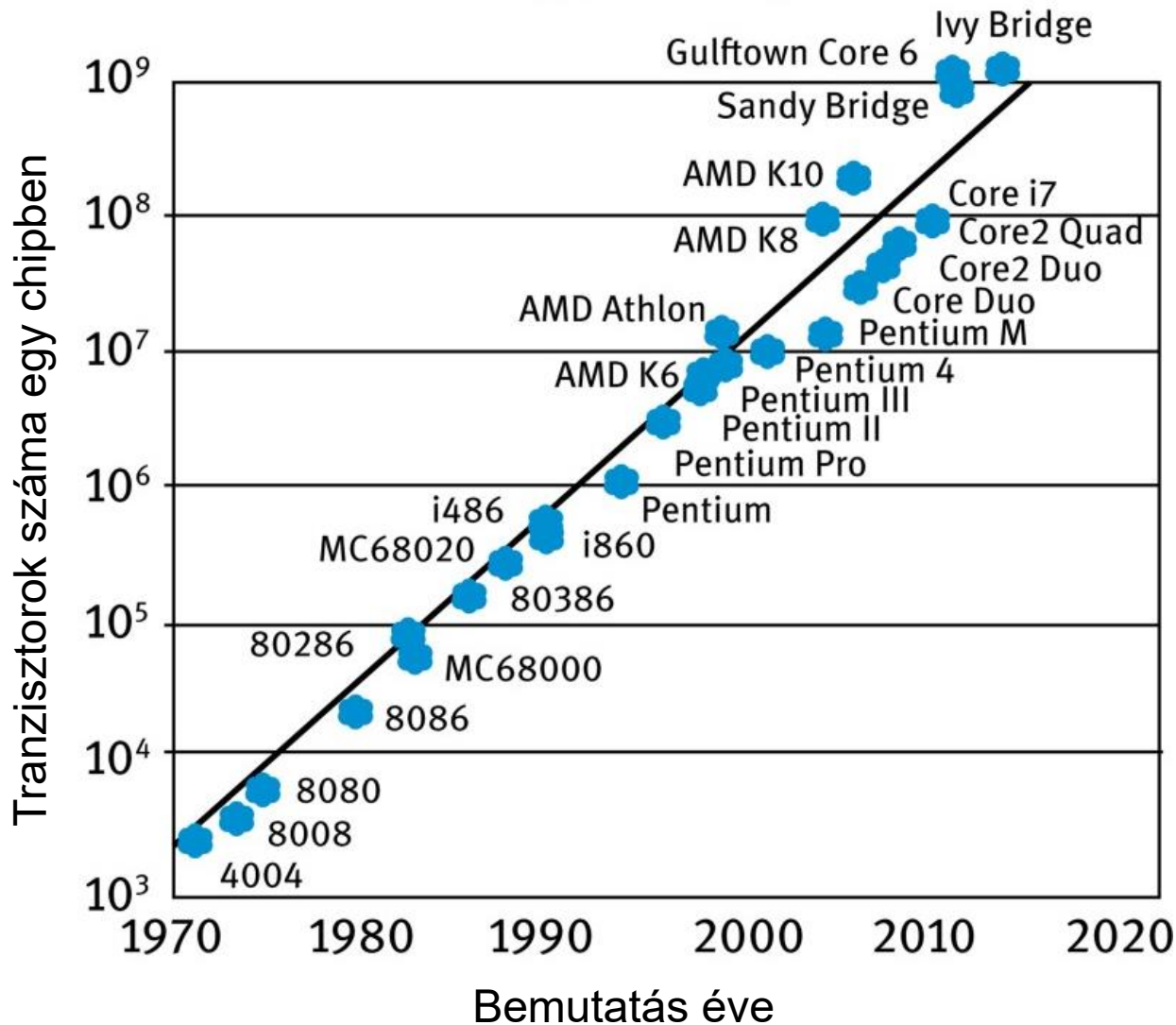
2010-es

Kvantumszámítógép:

- 20??
- Más fizikai alapok
- Bonyolult technológia
- Más problémák megoldására
- Nem váltja ki a klasszikust



Moore-törvény



Csíkszélesség:
10 nm = 20 Si atom

Klasszikus számítógép

10111010101011111010
1010101010101010100000
1111010110101110000000
0111110111100010101010
011010101010100



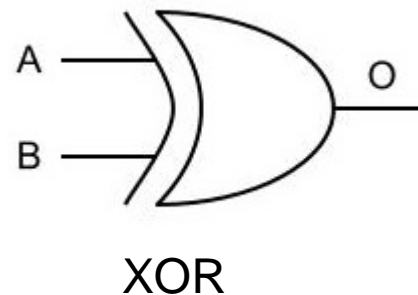
Műveletek végzése:

Egybites kapuk:

BEMENET	KIMENET
0	1
1	0

Kétbites kapuk:

BEMENET		KIMENET
A	B	
0	0	0
0	1	1
1	0	1
1	1	0



Univerzális kapukészlet

Kvantumbit és szuperpozíció

Klasszikus bit

$|0\rangle$ vagy $|1\rangle$

Kvantumbit

$$\alpha |0\rangle + \beta |1\rangle$$

számok (súlyok)

Szuperpozíció:

- Klasszikusan nehezen érthető
 - Egyszerre vagyok otthon és atomcsill előadáson
 - Egyszerre élő és holt egy macska
 - Elektron az atommag körül
 - ...
- Több lehetséges állapot mint klasszikusan (N kvantumbit $\rightarrow 2^N$ bit)
- Sérülékeny állapotok
 - Mérés
 - Környezettel való kölcsönhatás tönkre teszi



Mi az értelme?

Kvantumbiteken gyorsabb algoritmusok:

- **Grover-algoritmus**

Telefonkönyv

Kinek a száma a 229-3033?

Klasszikusan $\sim n$

Kvantumosan $\sim \sqrt{n}$

- **Shor-algoritmus**

Kvantumrendszerek effektívebb szimulálása:

- Molekulák szimulálása
- Új anyagok keresése
- Gyógyszerkutató
- Akkumulátorok, napelemek ...
- Az algoritmusok még kezdetlegesek ☹️
- Lesz hardver jönnek a jobb szoftverek, algoritmusok?

Balázs Emília Dr. közgazdász 1173 524. u. 10	257 4905	Balázs Géza 1214 Erdősor u. 175/a	277 9894	Balázs Imre 1205 Baross u. 57	284 5653	Balás
— Emma 1055 Vámhízt krt. 8	317 6520	— Géza 1225 Jókai M. u. 44/b	227 3352	— Imréné 1046 Szent Imre u. 16	389 0442	—
— Emma 1097 Országgy. 9	215 7158	— Géza 1223 Jókai u. 44/b	228 2346	— Imréné 1112 Cirmos u. 4	310 0097	Balás
— Endre Dr. 1026 Endrői S. u. 25	394 4701	— Géza 1223 Nyélt. u. 18	362 1827	— Imréné 1125 Felső Svábhegyi út 1	395 5478	
— Endre Dr. 1021 Szerb A. u.	200 7283	— Gézané 1105 Harmat u. 36 4. em. 14	260 8013	— Imréné 1185 Felsőcsatári út 95	295 5705	
— Endre Dr. 1023 Zsigmond tér	355 1161	— Gizella 1181 Madách I. u. 11	295 4765	— Imréné 1205 Csányi u. 17	285 1219	
— Endre vállalkozó, kiadványszerkesztő	240 8168	— Gusztáv 1152 Szilas park 13	418 0037	— Imréné 1214 II. Rákóczi F. út 297	420 2849	
1055 Kőház u. 21 fsz.	301 577 2907	— Gyöngyi 1165 Sashegy sétány 50	403 2050	— Irén 1026 Rügy u. 5	354 4061	
— Erika 1041 Szigeti J. u. 9 7. em. 40	389 0255	— Gyöngyike 1126 Bartha u.	274 4651	— Irén 1221 Kossuth L. u.	229 3033	
— Erika 1075 Akácfa u.	344 6726	— György 1023 Felhívás út	326 3527	— Irma 1117 Siroki u. 5/a	365 2508	
— Erika 1185 Ipolyföld u.	291 3458	— György 1024 Forint u. 12	316 2518	— István 1021 Völgy u. 13/a	274 2373	
— Erika 1191 Ady E. út	378 2674	— György 1024 Lovóház u. 32 2. em.	315 8041	— István 1035 Harrer P. u.	368 1572	
— Ernő 1161 Vörösmarty u.	405 9194	— György memók közgazdász	1026 Volkmann u. 6. 5. em. 3	— István 1039 Hollós Korvin L. u. 1 3. em. 22	243 1853	
— Ernő 1171 Lemberg u. 50	257 9628	— György Dr. memók 1052 Váci u. 25	274 2599	— István 1058 Pusztadombi u. 19	244 5554	
— Ernőné 1089 Vajda P. u.	353 8297	— György Dr. memók 1052 Váci u. 25	337 7585	— István 1048 Börtendős u. 50 7. em. 19	230 1233	
— Ernőné 1211 Kiss J. altábornagy u. 61	277 4646	— György Dr. orvos 1065 Sányai M. u. 6	332 7450	— István gépkezelő 1046 Enkel Gy. u. 2/3	380 4865	
— Ervin Dr. 1124 Korompai u. 21/25	319 4668	— György 1071 Dembinszky u. 18	351 5209	— István 1046 Galopp u.	230 2201	
— Erzsébet 1026 Garas u.	213 5414	— György 1082 Kistalud u.	314 4518	— István Dr. 1042 József A. u. 16 2. em. 12	369 3485	
— Eszter 1046 Erdősor út	233 1387	— György Dr. ügyvéd 1108 Andezit u. 14	262 2095	— István Dr. 1048 József A. u. 16 2. em. 12	369 4990	
— Eszter 1068 Király u. 82 4. em. 2A	322 7726	— György 1105 Gerégy u. 46	261 3925	— István 1041 Laborfalvi R. u. 2	231 0480	
— Eszter 1204 Ady E. u.	286 2605	— György 1118 Gazságréti tér 1 5. em. 35	246 5688, § (70) 310 3798	— István társvezető egyetemi docens	1048 Sárpatok u.	§ 231 4980
— Eva 1056 Lajos u. 27 10. em. 57	387 2818	— György Dr. memók 1118 Kelenhegyi út 70/b	386 9586	— István Dr. társvezető egyetemi docens	1048 Sárpatok u.	§ 380 9178
— Eva 1055 Miklós u. 11 2. em.	387 4521			— István Dr. társvezető egyetemi docens	1048 Sárpatok u.	§ 380 9178
— Eva 1064 Szondi u. 61 1. em. 18	302 6792			— István Dr. társvezető egyetemi docens	1048 Sárpatok u.	§ 380 9178
— Eva Dr. 1086 Árpád tér 1. em.				— István Dr. társvezető egyetemi docens	1048 Sárpatok u.	§ 380 9178



Shor-algoritmus

Prím faktorizáció:

15 \rightarrow 3 · 5

1247 \rightarrow 29 · 43

Kiszámolni: nehéz
Ellenőrizni: könnyű

Számolási igény (laptop):

33 jegyű szám 0,06 s

60 jegyű szám 1 perc

1024 jegyű szám 10^{54} év

RSA és más titkosítások alapja

Kvantumosan: Shor-algoritmus
exponenciális \rightarrow polinomiális
600 jegyű szám \rightarrow 4000 tökéletes qubit
„véges” idő alatt feltörhetőek a ma használt titkosítások

Milyen más problémákat tudunk kvantumosan gyorsabban megoldani? Nem tudjuk.



Építsünk kvantumszámítógépet!

Kellnek **kvantumbitek** (lehetőségek):

Elektron, vagy atommag spinje

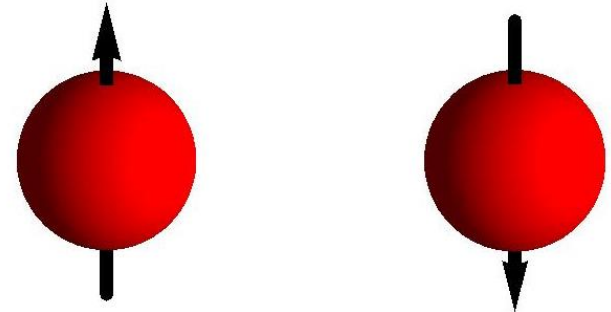
Fény polarizációja

Elektron pozíciója

Elektronok vagy fotonok száma

Áram iránya egy szupravezető karikában

...



Meg kell **védni** a környezet hatásaitól:

mK hőmérséklet, vákuum

Műveleteket kell rajta végezni (jó hatékonysággal):

inicializálás

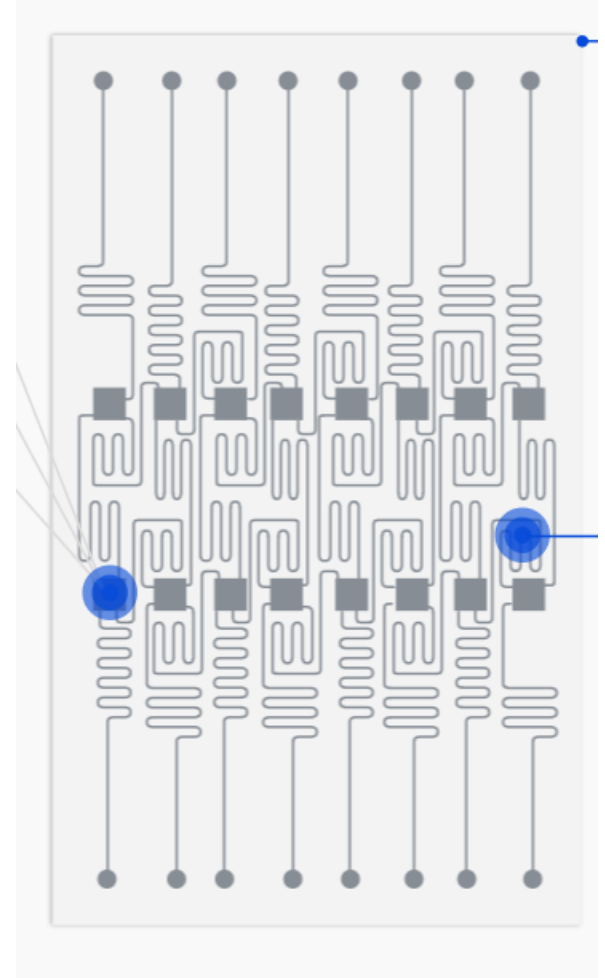
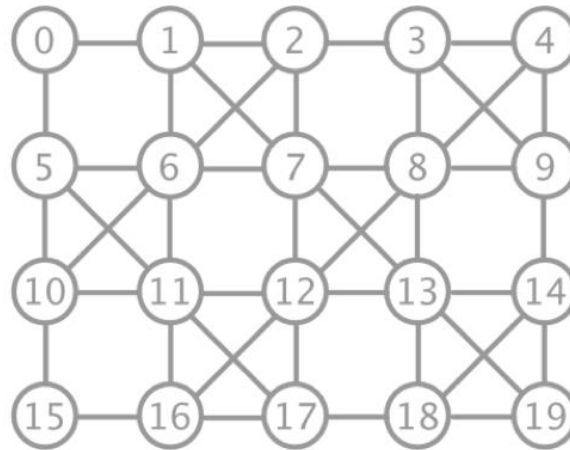
egykvantumbites kapuk

kétkvantumbites kapuk

kiolvasás

Legyen sok kvantumbit, és legyen skálázható a rendszer

IBM Q Experience



Előnyök:

Mindenki kipróbálhatja az 5 és 14 qubites verziót
Működik 😊

Hátrányok:

Nincs teljes összekötöttség
Viszonylag nagy (~cm)
Pontatlan (pl.: 8% kiolvasási hiba)

Szupravezető qubit
Rezonátorok

IonQ

Csapdázott ionok lézersugarakkal manipulálva

Előnyök:

11 teljesen összekötött qubit

Viszonylag pontos

Egykvantumbites kapuk 0,03%

Kétkvantumbites kapuk 1%

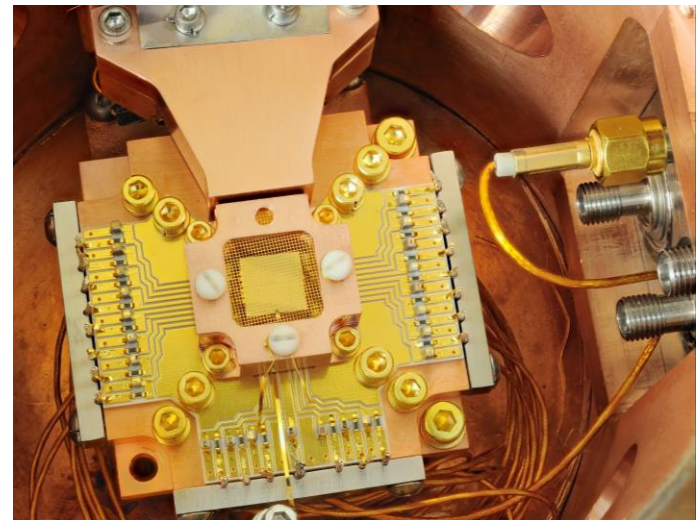
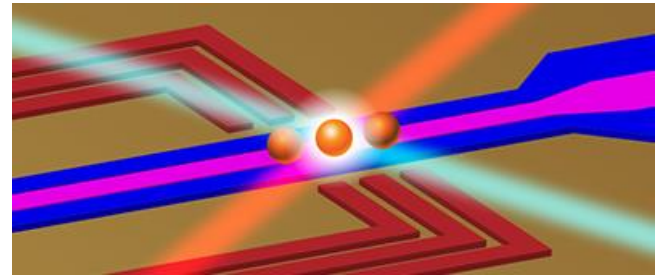
„60 hosszú” program futtatható rajta

Hátrányok:

Viszonylag nagy (~cm)

Nem olyan egyszerű kipróbálni

Nehezen skálázható



Cikkek:

Ground-state energy estimation of the water molecule on a trapped ion quantum computer (2019. márc.)

Benchmarking an 11-qubit quantum computer (2019. márc.)

Complete 3-Qubit Grover search on a programmable quantum computer (2017. dec.)

D-wave

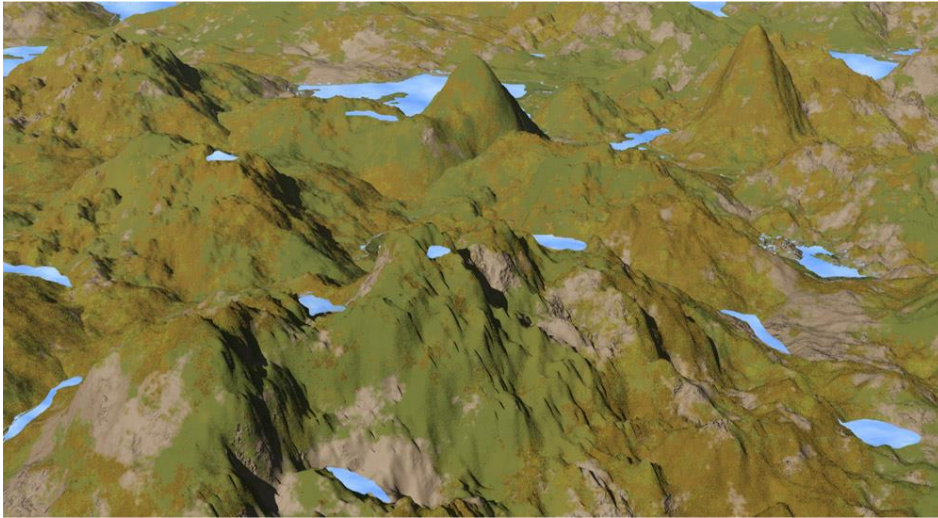
2048 qubit

A legnagyobb kvantumszámítógép, kvantumos jelenségeket mutató hűtőgép

Nem kvantumkapukat használ

Energiaminimumot keresi

Ez a kettő elvileg megfeleltethető egymásnak



Mennyire kvantumos?

Nem tisztázott.

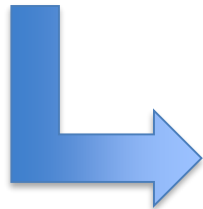
Lehet-e rajta a korábbi algoritmusokat futtatni?

Valószínűleg nem.



Hova tovább?

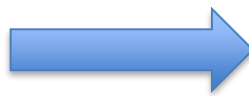
Növelni a kvantumbitek számát!
Skálázható rendszert választani!
Csökkenteni a kvantumbitek és chipek méretét!
Minél pontosabb kapukat készíteni!



Eredményként néhány 100 qubites gépünk
Kicsit hibás kapukkal
Valószínűleg nem rázza meg a világot!

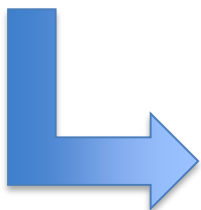
Következő nagy lépés:

Hibajavítás



Eredményként bizonyos problémákra
hatékonyabb gép mint a klasszikus

Mikor lesz kvantumszámítógép?
Lesz-e hatékony kvantumszámítógép?



Hosszú az út
Legyünk optimisták

