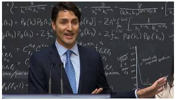
Kvantumszámítógépek - elméletben és gyakorlatban

Zimborás Zoltán

Az atomoktól a csillagokig
ELTE, 2018. április 26.

A kvantumszámítógép bekerült a köztudatba

- Naponta találkozunk olyan hírekkel, hogy a hamarosan megépítendő kvantumszámítógépek új korszakot nyitnak:
    - Döntéshozók beszélnek erről - a kanadai miniszterelnöktől az EU biztosokig.



"We need to act together at European level to turn our scientific successes in Quantum technologies into benefits for our industry and society. No single country can make it on its own, cooperation is essential to succeed"

Günther H. Oettinger

- Hírportálok tudományos népszerűsítő rovatai veszik fel nevüket kvantuminformatikai fogalmakról: QUBIT.
- Nobel-díj indoklásokban érintik a kvantuminformatikát (Haroche, Wineland).

- Multinacionális cégek és startup-ok nagyszámban vesznek fel fizikusokat erre a célra.

Google - kétfajta kvantummérnöki beosztást is létrehozott

PI

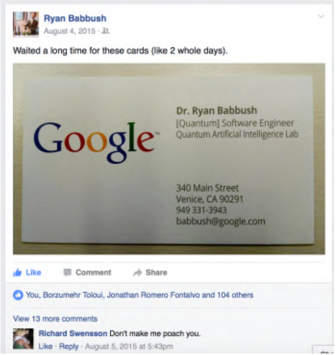
John M. Martinis
Professor at UC Santa Barbara since 2004
Research Scientist at Google since 2014
martinis (at) physics (dot) ucsb (dot) edu
jmartinis (at) google (dot) com

Quantum Electronics Engineers, Google

Rami Barends
Post Doctoral Fellow, 2010-2014
Quantum Electronics Engineer at Google since 2014
rbarends (at) physics (dot) ucsb (dot) edu
barends (at) google (dot) com

Yu Chen
Post Doctoral Fellow, 2010-2014
Quantum Electronics Engineer at Google since 2014
ychen (at) physics (dot) ucsb (dot) edu
bryanchen (at) google (dot) com

Austin Fowler
Staff Scientist, 2013-2014
Quantum Electronics Engineer at Google since 2014
agfowler (at) google (dot) com



Ryan Babbush
August 4, 2015 ·

Waited a long time for these cards (like 2 whole days).

Google

Dr. Ryan Babbush
[Quantum] Software Engineer
Quantum Artificial Intelligence Lab

340 Main Street
Venice, CA 90291
949 331-3943
babbush@google.com

You, Borzumehr Toloui, Jonathan Romero Fontalvo and 104 others

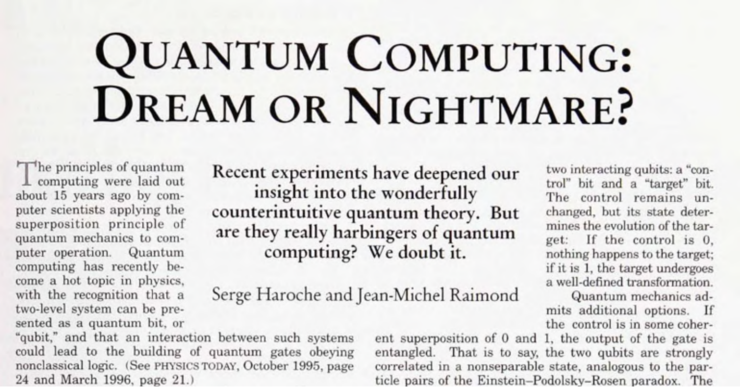
View 13 more comments

Richard Swensson Don't make me poach you.
Like · Reply · August 5, 2015 at 5:43pm

Rengeteg startup foglalkozik a témával

Company	Date initiated	Area	Affiliate University or Research Institute	Headquarters
1QBit	1 December 2012	Computing		Vancouver, Canada
Accenture[1]	14 June 2017	Computing		
imec[2]		Silicon Quantum Computing		Belgium
Airbus[3]	2015	Computing		Blagnac, France
Aliyun (Alibaba Cloud)[4]	30 July 2015	Computing/Communication[4][5]	Chinese Academy of Sciences [6][5][7]	Hangzhou, China
AT&T[8]	2011	Communication		Dallas, TX, USA
Atos[9]		Communication		Bezons, France
Booz Allen Hamilton[10]		Computing		Tysons Corner, VA, USA
BT[11]		Communication		London, UK
Carl Zeiss AG[12]			University College London	Oberkochen, Germany
Cambridge Quantum Computing Limited[13]		Communication		Cambridge, UK
D-Wave	1 January 1999	Computing		Burnaby, Canada
Fujitsu[14]	28 September 2015	Communication	University of Tokyo	Tokyo, Japan
Google QuAIL[15]	16 May 2013	Computing	UCSB	Mountain View, CA, USA
HP[16][17]		Computing[16]/Communication[17]		Palo Alto, CA, USA
Hitachi		Computing	University of Cambridge, University College London	Tokyo, Japan
Honeywell[18][19]		Computing	Georgia Tech,[18] University of Maryland[19]	Morris Plains, NJ, USA
HRL Laboratories		Computing		Malibu, CA, USA
Huawei Noah's Ark Lab[20]		Communication	Nanjing University	Shenzhen, China
IBM[21]	10 September 1990[22]	Computing	MIT[23]	Armonk, NY, USA
ID Quantique	1 July 2001	Communication		Geneva, Switzerland
IonQ[24][25]		Computing	University of Maryland, Duke University	College Park, MD, USA
Intel[26]	3 September 2015	Computing	TU Delft	Santa Clara, CA, USA
KPN[27]		Communication		The Hague, Netherlands
Lockheed Martin		Computing	University of Southern California, University College London	Bethesda, MD, USA
MagiQ		Communication		Somerville, MA, USA
Microsoft Research QuArC	19 December 2011	Computing	TU Delft, Niels Bohr Institute, University of Sydney, Purdue University, University of Maryland, ETH Zurich, UCSB	Redmond, WA, USA
Microsoft Research Station Q	22 April 2005	Computing	UCSB	Santa Barbara, CA, USA
Mitsubishi[28]		Communication		Tokyo, Japan
NEC Corporation[29]	29 April 1999[30]	Communication	University of Tokyo	Tokyo, Japan
Nokia Bell Labs[31][32]		Computing	University of Oxford	Murray Hill, NJ, USA
Northrop Grumman		Computing		West Falls Church, VA, USA
NTT Laboratories[33]		Computing	Bristol University	Tokyo, Japan
Q-Ctrl[34][35][36]	2017	Computing[note 1]		Sydney, Australia

Korai vélemények I.



QUANTUM COMPUTING: DREAM OR NIGHTMARE?

Recent experiments have deepened our insight into the wonderfully counterintuitive quantum theory. But are they really harbingers of quantum computing? We doubt it.

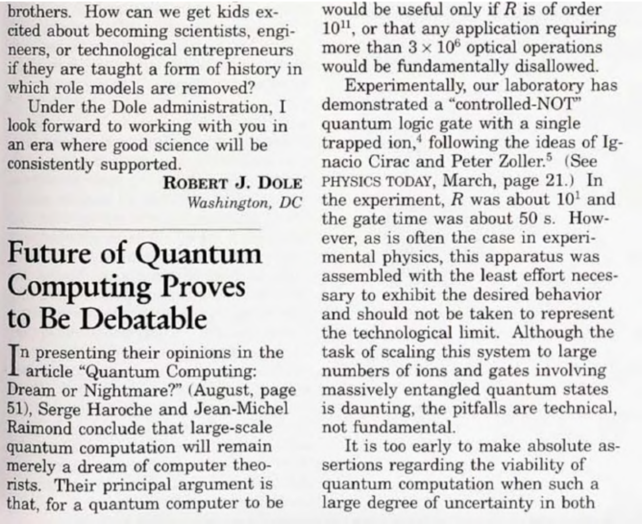
Serge Haroche and Jean-Michel Raimond

The principles of quantum computing were laid out about 15 years ago by computer scientists applying the superposition principle of quantum mechanics to computer operation. Quantum computing has recently become a hot topic in physics, with the recognition that a two-level system can be presented as a quantum bit, or "qubit," and that an interaction between such systems could lead to the building of quantum gates obeying nonclassical logic. (See PHYSICS TODAY, October 1995, page 24 and March 1996, page 21.)

two interacting qubits: a "control" bit and a "target" bit. The control remains unchanged, but its state determines the evolution of the target: If the control is 0, nothing happens to the target; if it is 1, the target undergoes a well-defined transformation.

Quantum mechanics admits additional options. If the control is in some coherent superposition of 0 and 1, the output of the gate is entangled. That is to say, the two qubits are strongly correlated in a nonseparable state, analogous to the particle pairs of the Einstein–Podolsky–Rosen paradox. The

Korai vélemények II.



brothers. How can we get kids excited about becoming scientists, engineers, or technological entrepreneurs if they are taught a form of history in which role models are removed?

Under the Dole administration, I look forward to working with you in an era where good science will be consistently supported.

Robert J. Dole
Washington, DC

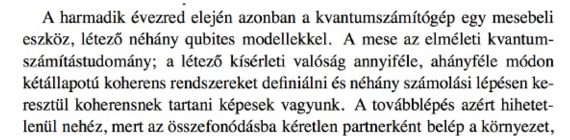
Future of Quantum Computing Proves to Be Debatable

In presenting their opinions in the article "Quantum Computing: Dream or Nightmare?" (August, page 51), Serge Haroche and Jean-Michel Raimond conclude that large-scale quantum computation will remain merely a dream of computer theorists. Their principal argument is that, for a quantum computer to be would be useful only if R is of order 10^{11}, or that any application requiring more than 3×10^6 optical operations would be fundamentally disallowed.

Experimentally, our laboratory has demonstrated a "controlled-NOT" quantum logic gate with a single trapped ion,[4] following the ideas of Ignacio Cirac and Peter Zoller.[5] (See PHYSICS TODAY, March, page 21.) In the experiment, R was about 10^1 and the gate time was about 50 s. However, as is often the case in experimental physics, this apparatus was assembled with the least effort necessary to exhibit the desired behavior and should not be taken to represent the technological limit. Although the task of scaling this system to large numbers of ions and gates involving massively entangled quantum states is daunting, the pitfalls are technical, not fundamental.

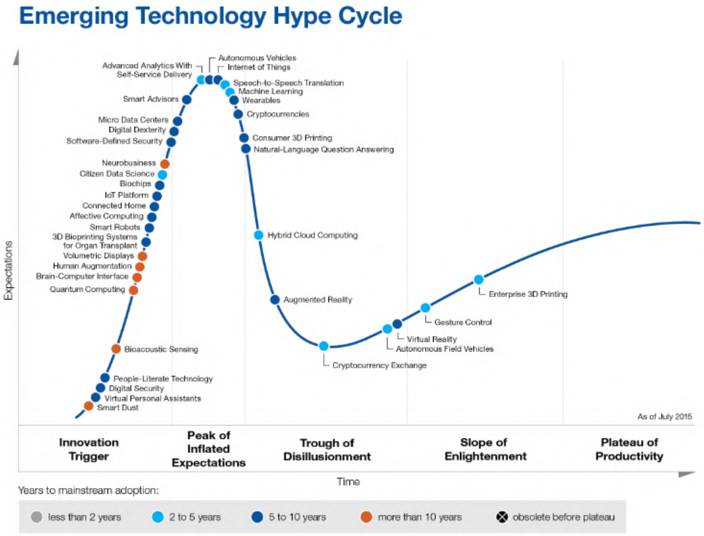
It is too early to make absolute assertions regarding the viability of quantum computation when such a large degree of uncertainty in both

Korai vélemények III.



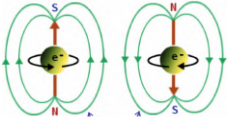
A harmadik évezred elején azonban a kvantumszámítógép egy mesebeli eszköz, létező néhány qubites modellekkel. A mese az elméleti kvantumszámítástudomány; a létező kísérleti valóság annyiféle, ahányféle módon kétállapotú koherens rendszereket definiálni és néhány számolási lépésen keresztül koherensnek tartani képesek vagyunk. A továbblépés azért hihetetlenül nehéz, mert az összefonódásba kéretlen partnerként belép a környezet,

A kifejlődő technológiák felvillanyozódási ciklusa

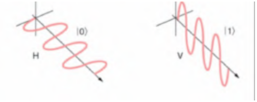


A kvantummechanikai kétállapotú rendszer: a qubit

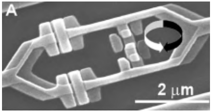
Az elektron (vagy egy atommag) mágneses dipólusmomentuma:



A fény polarizációja:



Szupravezetők fluxusa, áramiránya:

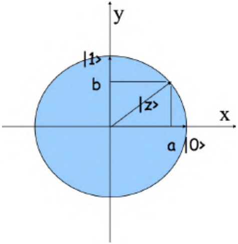


Szuperpozíció elve

Szuperpozíció elve szerint egy qubit általános (tiszta) állapota

$$|z\rangle = a|0\rangle + b|1\rangle.$$

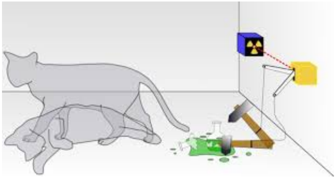
Itt $|a|^2$ mondja meg a valószínűségét, hogy $|0\rangle$ állapotban látjuk, és $|b|^2$, hogy $|1\rangle$ állapotban. Fel kell tennünk, hogy $|a|^2 + |b|^2 = 1$

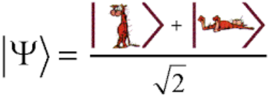


A leghíresebb szuperponált qubit

A leghíresebb szuperponált qubit

Schrödinger macskája

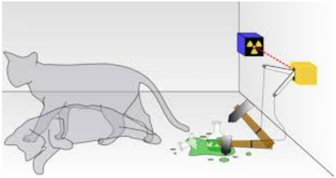


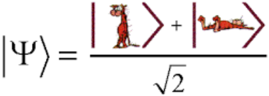


De mi a különbség $a|0\rangle + b|1\rangle$ és $a|0\rangle - b|1\rangle$ között?

A leghíresebb szuperponált qubit

Schrödinger macskája





De mi a különbség $a|0\rangle + b|1\rangle$ és $a|0\rangle - b|1\rangle$ között?

Megengedett műveletek a qubiten

$$V|0\rangle = a|0\rangle + b|1\rangle,$$
$$V|1\rangle = c|0\rangle + d|1\rangle,$$
$$V|z\rangle = V(e|0\rangle + f|1\rangle) = eV|0\rangle + fV|1\rangle \quad = (ea + fc)|0\rangle + (eb + fd)|1\rangle.$$

Ezeket a számokat szokás egy táblázatban (mátrixban) szokás összegyűjteni

$$V = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

Hasonlóan bevezethetünk több qubites állapotokat és azokon műveleteket:

$$q|0\rangle|0\rangle + r|0\rangle|1\rangle + s|1\rangle|0\rangle + t|1\rangle|1\rangle$$

Megengedett műveletek a qubiten

$$\begin{aligned} V|0\rangle &= a|0\rangle + b|1\rangle, \\ V|1\rangle &= c|0\rangle + d|1\rangle, \\ V|z\rangle &= V(e|0\rangle + f|1\rangle) = eV|0\rangle + fV|1\rangle \quad = (ea + fc)|0\rangle + (eb + fd)|1\rangle. \end{aligned}$$

Ezeket a számokat szokás egy táblázatban (mátrixban) szokás összegyűjteni

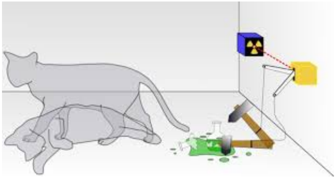
$$V = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

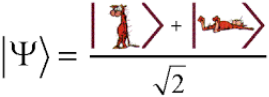
Hasonlóan bevezethetünk több qubites állapotokat és azokon műveleteket:

$$q|0\rangle|0\rangle + r|0\rangle|1\rangle + s|1\rangle|0\rangle + t|1\rangle|1\rangle$$

A leghíresebb szuperponált qubit

Schrödinger macskája

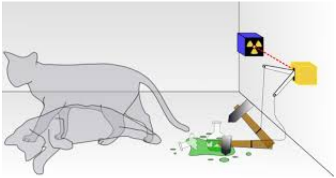


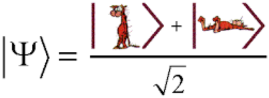


Schrödinger gondoltakísérletben nem az a meglepö, hogy a macska 50% valószínűséggel él és 50% valószínűséggel halott, hanem az, hogy létezik feltámasztó operátor. (Reinhard Werner)

A leghíresebb szuperponált qubit

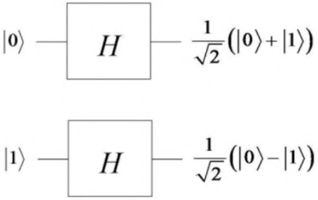
Schrödinger macskája





Schrödinger gondoltakísérletben nem az a meglepö, hogy a macska 50% valószínűséggel él és 50% valószínűséggel halott, hanem az, hogy létezik feltámasztó operátor. (Reinhard Werner)

A Hadamard-kapu



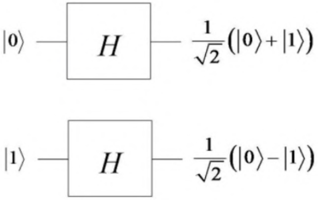
Mit csinál ez a kapu a Schrödinger-macska állapottal?

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

Mit csinál ez a kapu egy alternatív Schrödinger-macska állapottal?

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

A Hadamard-kapu



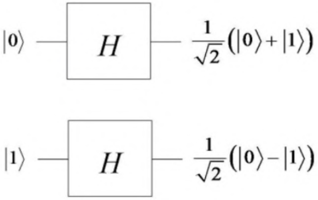
Mit csinál ez a kapu a Schrödinger-macska állapottal?

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

Mit csinál ez a kapu egy alternatív Schrödinger-macska állapottal?

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

A Hadamard-kapu



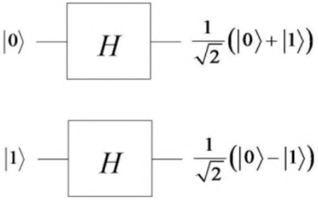
Mit csinál ez a kapu a Schrödinger-macska állapottal?

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

Mit csinál ez a kapu egy alternatív Schrödinger-macska állapottal?

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

A Hadamard-kapu



Mit csinál ez a kapu a Schrödinger-macska állapottal?

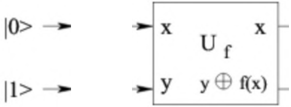
$$H\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)=\frac{1}{2}|0\rangle+\frac{1}{2}|1\rangle+\frac{1}{2}|0\rangle-\frac{1}{2}|1\rangle=|0\rangle.$$

Mit csinál ez a kapu egy alternatív Schrödinger-macska állapottal?

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

Deutsch-problémája

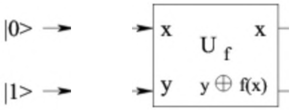
Legyen f egy Boole-függvény, ami egy bitből bitbe képez. Hány rákérdezéssel (függvénykiértékeléssel) állapítjuk meg, hogy f konstans-e?



Nyilvánvalóan kettő.

Deutsch-problémája

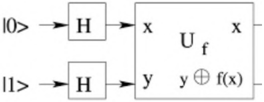
Legyen f egy Boole-függvény, ami egy bitből bitbe képez. Hány rákérdezéssel (függvénykiértékeléssel) állapítjuk meg, hogy f konstans-e?



Nyilvánvalóan kettő.

Deutsch-problémája kvantumos esetben

Szuperpozíciót is beadhatunk



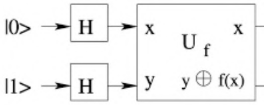
Az eredő állapotban már benne van a válasz

$$\frac{1}{4}|0\rangle|1+f(0)\rangle + \frac{1}{4}|1\rangle|1+f(1)\rangle + \frac{1}{4}|0\rangle|f(0)\rangle - \frac{1}{4}|1\rangle|f(1)\rangle.$$

De hogyan szedjük ki belőle?

Deutsch-problémája kvantumos esetben

Szuperpozíciót is beadhatunk



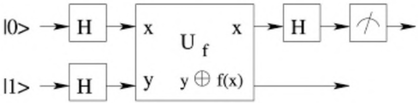
Az eredő állapotban már benne van a válasz

$$\frac{1}{4}|0\rangle|1{+}f(0)\rangle + \frac{1}{4}|1\rangle|1{+}f(1)\rangle + \frac{1}{4}|0\rangle|f(0)\rangle - \frac{1}{4}|1\rangle|f(1)\rangle.$$

De hogyan szedjük ki belőle?

Deutsch-algoritmus

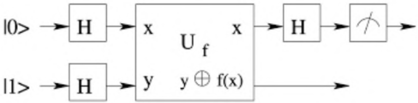
Rakjunk rá még egy Hadamard-kaput



Az eredő állapot első qubit-je 100% valószínűséggel $|0\rangle$ állapotban van, ha f konstans, és $|1\rangle$ állapotban van, ha f nem konstans. Tehát egy rákérdezés elég!

Deutsch-algoritmus

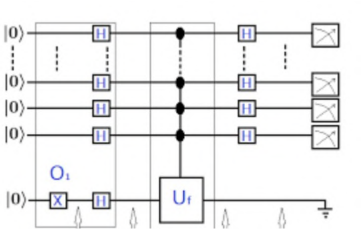
Rakjunk rá még egy Hadamard-kaput



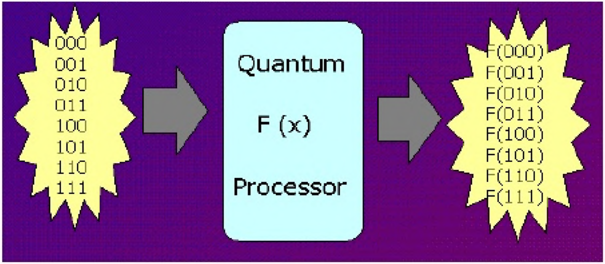
Az eredő állapot első qubit-je 100% valószínűséggel $|0\rangle$ állapotban van, ha f konstans, és $|1\rangle$ állapotban van, ha f nem konstans. Tehát egy rákérdezés elég!

Deutsch-Jozsa-algoritmus

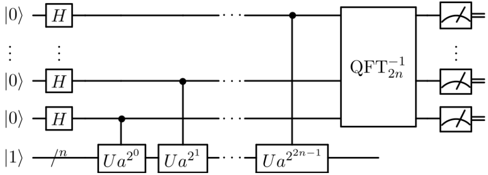
Többváltozós Boole-függvény esetére is



A naiv kvantumos párhuzamosítás ötlete



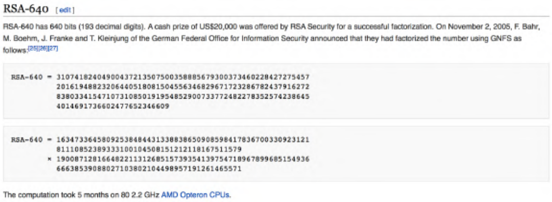
Shor-algoritmus



$$15 = 3 \cdot 5 \quad (2001)$$

$$143 = 11 \cdot 13 \quad (2012)$$

$$56153 = 241 \cdot 233 \quad (2014)$$



RSA-640 [edit]

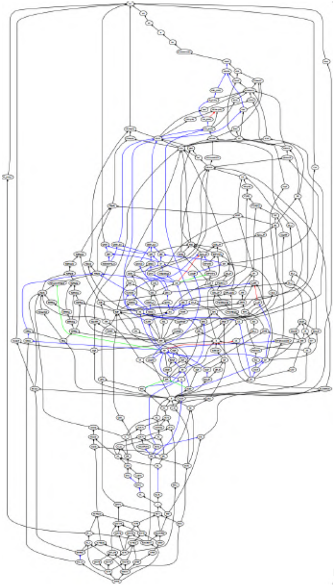
RSA-640 has 640 bits (193 decimal digits). A cash prize of US$20,000 was offered by RSA Security for a successful factorization. On November 2, 2005, F. Bahr, M. Boehm, J. Franke and T. Kleinjung of the German Federal Office for Information Security announced that they had factorized the number using GNFS as follows:[25][26][27]

```
RSA-640 = 31074182404900437213507500358885679300373460228427275457
          20161948823206440518081504556346829671723286782437916272
          83803341547107310850191954852900733772482278352574238645
          4014691736602477652346609
```

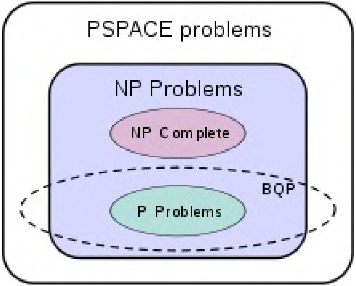
```
RSA-640 = 16347336458092538484431338838650908598417836700330923121
          81110852389333100104508151212118167511579
        × 19008712816648221131268515739354139754718967899685154936
          66638539088027103802104498957191261465571
```

The computation took 5 months on 80 2.2 GHz AMD Opteron CPUs.

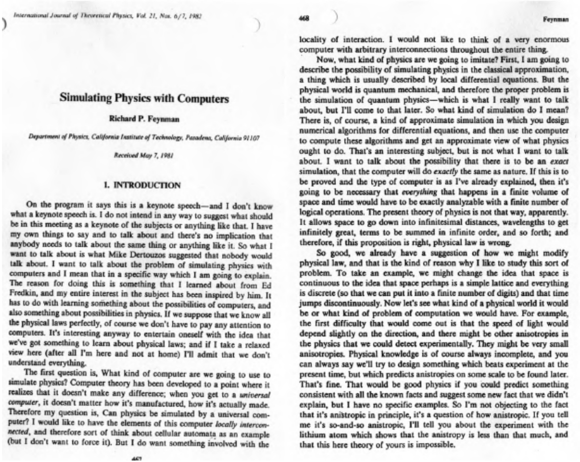
Bonyolultság-elmélet



Bonyolultság-elmélet



Feynman megjegyzése



International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

1. INTRODUCTION

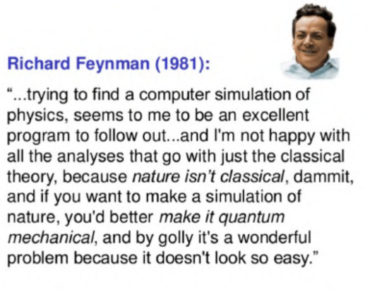
On the program it says this is a keynote speech—and I don't know what a keynote speech is. I do not intend in any way to suggest what should be in this meeting as a keynote of the subjects or anything like that. I have my own things to say and to talk about and there's no implication that anybody needs to talk about the same thing or anything like it. So what I want to talk about is what Mike Dertouzos suggested that nobody would talk about. I want to talk about the problem of simulating physics with computers and I mean that in a specific way which I am going to explain. The reason for doing this is something that I learned about from Ed Fredkin, and my entire interest in the subject has been inspired by him. It has to do with learning something about the possibilities of computers, and also something about possibilities in physics. If we suppose that we know all the physical laws perfectly, of course we don't have to pay any attention to computers. It's interesting anyway to entertain oneself with the idea that we've got something to learn about physical laws; and if I take a relaxed view here (after all I'm here and not at home) I'll admit that we don't understand everything.

The first question is, What kind of computer are we going to use to simulate physics? Computer theory has been developed to a point where it realizes that it doesn't make any difference; when you get to a *universal computer*, it doesn't matter how it's manufactured, how it's actually made. Therefore my question is, Can physics be simulated by a universal computer? I would like to have the elements of this computer *locally interconnected*, and therefore sort of think about cellular automata as an example (but I don't want to force it). But I do want something involved with the locality of interaction. I would not like to think of a very enormous computer with arbitrary interconnections throughout the entire thing.

Now, what kind of physics are we going to imitate? First, I am going to describe the possibility of simulating physics in the classical approximation, a thing which is usually described by local differential equations. But the physical world is quantum mechanical, and therefore the proper problem is the simulation of quantum physics—which is what I really want to talk about, but I'll come to that later. So what kind of simulation do I mean? There is, of course, a kind of approximate simulation in which you design numerical algorithms for differential equations, and then use the computer to compute these algorithms and get an approximate view of what physics ought to do. That's an interesting subject, but is not what I want to talk about. I want to talk about the possibility that there is to be an *exact* simulation, that the computer will do *exactly* the same as nature. If this is to be proved and the type of computer is as I've already explained, then it's going to be necessary that *everything* that happens in a finite volume of space and time would have to be exactly analyzable with a finite number of logical operations. The present theory of physics is not that way, apparently. It allows space to go down into infinitesimal distances, wavelengths to get infinitely great, terms to be summed in infinite order, and so forth; and therefore, if this proposition is right, physical law is wrong.

So good, we already have a suggestion of how we might modify physical law, and that is the kind of reason why I like to study this sort of problem. To take an example, we might change the idea that space is continuous to the idea that space perhaps is a simple lattice and everything is discrete (so that we can put it into a finite number of digits) and that time jumps discontinuously. Now let's see what kind of a physical world it would be or what kind of problem of computation we would have. For example, the first difficulty that would come out is that the speed of light would depend slightly on the direction, and there might be other anisotropies in the physics that we could detect experimentally. They might be very small anisotropies. Physical knowledge is of course always incomplete, and you can always say we'll try to design something which beats experiment at the present time, but which predicts anistropies on some scale to be found later. That's fine. That would be good physics if you could predict something consistent with all the known facts and suggest some new fact that we didn't explain, but I have no specific examples. So I'm not objecting to the fact that it's anistropic in principle, it's a question of how anistropic. If you tell me it's so-and-so anistropic, I'll tell you about the experiment with the lithium atom which shows that the anistropy is less than that much, and that this here theory of yours is impossible.

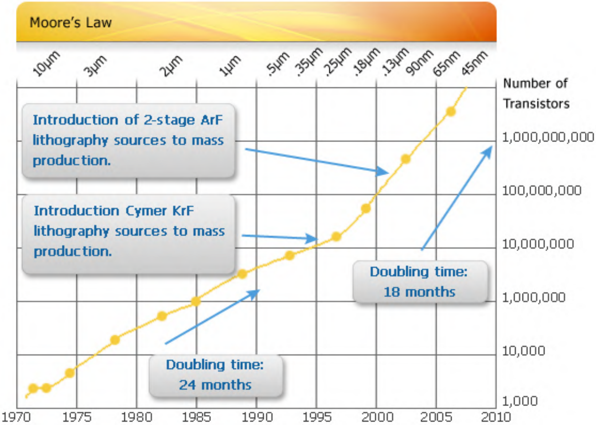
Feynman megjegyzése



Richard Feynman (1981):

"...trying to find a computer simulation of physics, seems to me to be an excellent program to follow out...and I'm not happy with all the analyses that go with just the classical theory, because *nature isn't classical*, dammit, and if you want to make a simulation of nature, you'd better *make it quantum mechanical*, and by golly it's a wonderful problem because it doesn't look so easy."

Moore-törvény



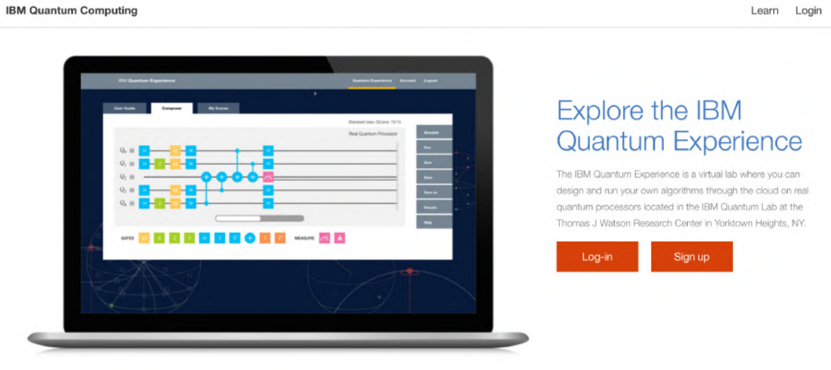
Introduction of 2-stage ArF lithography sources to mass production.

Introduction Cymer KrF lithography sources to mass production.

Doubling time: 18 months

Doubling time: 24 months

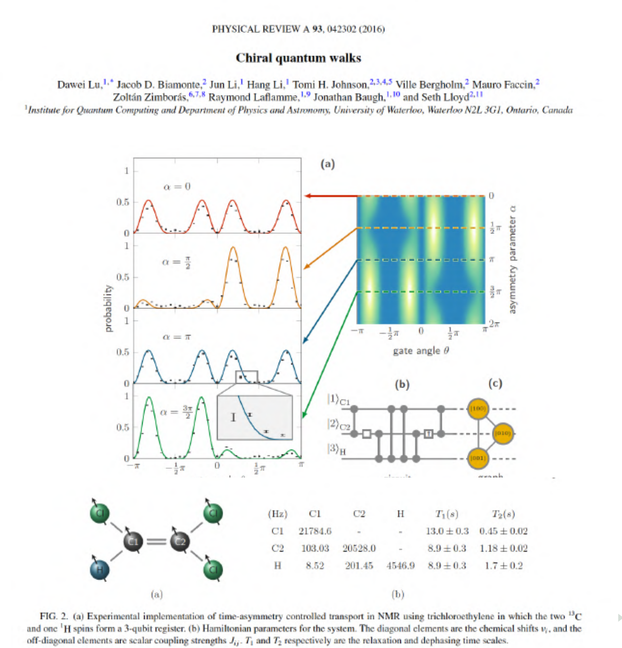
IBM Cloud Quantum Computing



Explore the IBM Quantum Experience

The IBM Quantum Experience is a virtual lab where you can design and run your own algorithms through the cloud on real quantum processors located in the IBM Quantum Lab at the Thomas J Watson Research Center in Yorktown Heights, NY.

A kevés qubites cikkek leáldoznak



PHYSICAL REVIEW A **93**, 042302 (2016)

Chiral quantum walks

Dawei Lu,[1,*] Jacob D. Biamonte,[2] Jun Li,[1] Hang Li,[1] Tomi H. Johnson,[2,3,4,5] Ville Bergholm,[2] Mauro Faccin,[2]
Zoltán Zimborás,[6,7,8] Raymond Laflamme,[1,9] Jonathan Baugh,[1,10] and Seth Lloyd[2,11]
[1]*Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo N2L 3G1, Ontario, Canada*

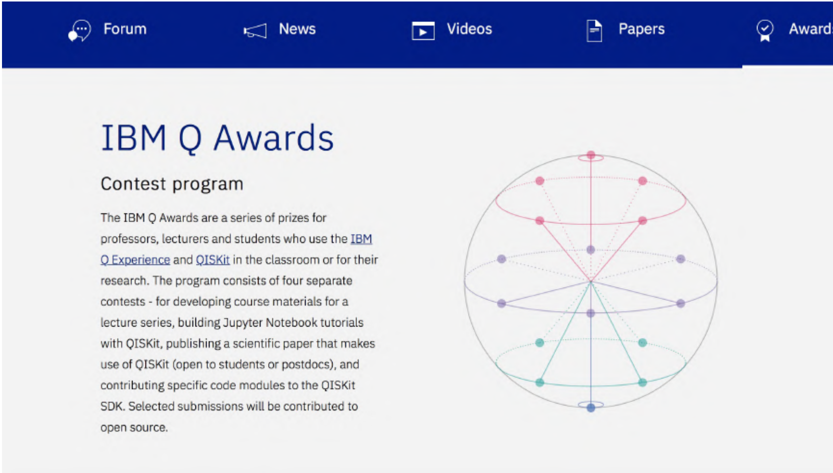
(a)

(Hz)	C1	C2	H	$T_1(s)$	$T_2(s)$
C1	21784.6	-	-	13.0 ± 0.3	0.45 ± 0.02
C2	103.03	20528.0	-	8.9 ± 0.3	1.18 ± 0.02
H	8.52	201.45	4546.9	8.9 ± 0.3	1.7 ± 0.2

(b)

FIG. 2. (a) Experimental implementation of time-asymmetry controlled transport in NMR using trichloroethylene in which the two ^{13}C and one ^{1}H spins form a 3-qubit register. (b) Hamiltonian parameters for the system. The diagonal elements are the chemical shifts ν_i, and the off-diagonal elements are scalar coupling strengths J_{ij}. T_1 and T_2 respectively are the relaxation and dephasing time scales.

IBM Cloud Quantum Computing



IBM Q Awards

Contest program

The IBM Q Awards are a series of prizes for professors, lecturers and students who use the IBM Q Experience and QISKit in the classroom or for their research. The program consists of four separate contests - for developing course materials for a lecture series, building Jupyter Notebook tutorials with QISKit, publishing a scientific paper that makes use of QISKit (open to students or postdocs), and contributing specific code modules to the QISKit SDK. Selected submissions will be contributed to open source.