量子コンピュータとは？

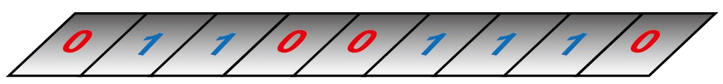
計算のこれまでと、これから

量子計算とは

計算原理自体にミクロで成り立つ物理法則「量子力学」を活用した新しいタイプの計算の一つ

- 従来型計算

フォン・ノイマン型計算
（チューリングマシン）



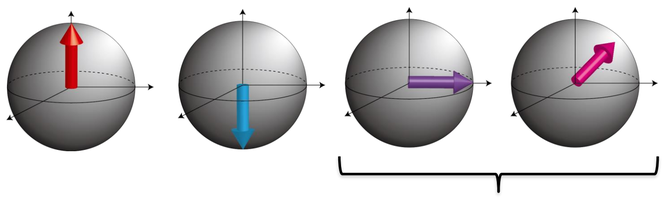
・・・

従来型コンピュータ

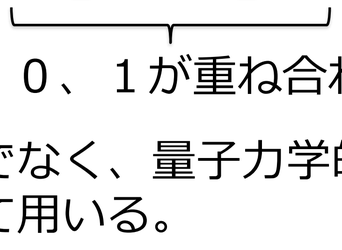
「０」と「１」のみを表す古典ビットを用いて計算を行う。

- 量子計算

量子ビット

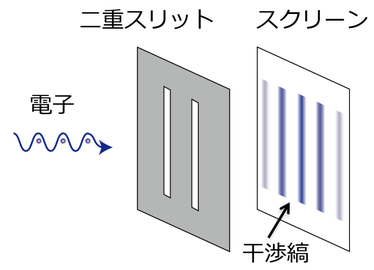


・・・

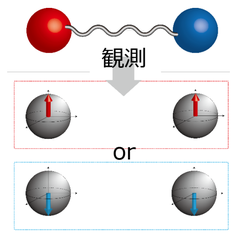


「０」と「１」だけでなく、量子力学的に重ね合わされたものも計算資源として用いる。

量子力学の奇妙な性質：
① 干渉
単一量子であっても、波の性質(干渉)を示す。



②エンタングルメント
古典的には説明のできない相関(非局所的相関)がある。



量子アルゴリズム

- 提唱論文

D. Deutsch, Proc. R. Soc. Lond. A, 400, 97 (1985)

Quantum theory, the Church–Turing principle and the universal quantum computer

By D. Deutsch

Department of Astrophysics, South Parks Road, Oxford OX1 3RQ, U.K.

(*Communicated by R. Penrose, F.R.S. – Received 13 July 1984*)

It is argued that underlying the Church–Turing hypothesis there is an implicit physical assertion. Here, this assertion is presented explicitly as a physical principle: 'every finitely realizible physical system can be perfectly simulated by a universal model computing machine operating by finite means'. Classical physics and the universal Turing machine, because the former is continuous and the latter discrete, do not obey the principle, at least in the strong form above. A class of model computing machines that is the quantum generalization of the class of Turing machines is described, and it is shown that quantum theory and the 'universal quantum computer' are compatible with the principle. Computing machines resembling the universal quantum computer could, in principle, be built and would have many remarkable properties not reproducible by any Turing machine. These do not include the computation of non-recursive functions, but they do include 'quantum parallelism', a method by which certain probabilistic tasks can be performed faster by a universal quantum computer than by any classical restriction of it. The intuitive explanation of these properties places an intolerable strain on all interpretations of quantum theory other than Everett's. Some of the numerous connections between the quantum theory of computation and the rest of physics are explored. Quantum complexity theory allows a physically more reasonable definition of the 'complexity' or 'knowledge' in a physical system than does classical complexity theory.

© David Deutsch 2008-

- 素因数分解を高速に行える可能性

P. W. Shor, Proc. 35th Annu. Symp. Found. Compt. Sci., 124 (1994)

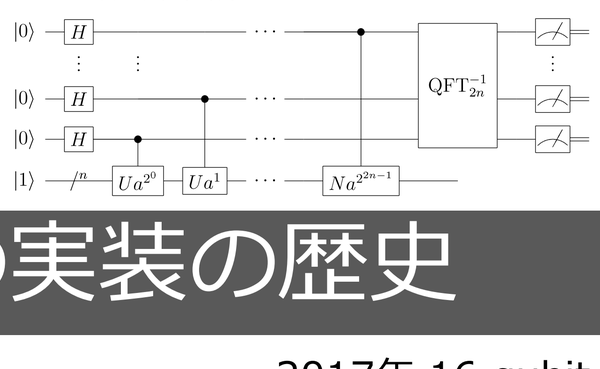
Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Abstract

A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting

[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.



- データベース検索を高速に行える可能性

L. K. Grover, Proc. 28th Ann. ACM Symp. Theory Compt. (STOC), 212 (1996)

A fast quantum mechanical algorithm for database search

Lov K. Grover
3C-404A, Bell Labs
600 Mountain Avenue
Murray Hill NJ 07974
lkgrover@bell-labs.com

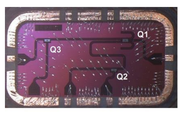
Summary

Imagine a phone directory containing N names arranged in completely random order. In order to find someone's phone number with a probability of $\frac{1}{2}$, any classical algorithm (whether deterministic or probabilistic) will need to look at a minimum of $\frac{N}{2}$ names. Quan-

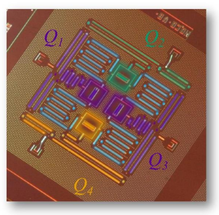
This paper applies quantum computing to a mundane problem in information processing and presents an algorithm that is significantly faster than any classical algorithm can be. The problem is this: there is an unsorted database containing N items out of which just one item satisfies a given condition - that one item has to be retrieved. Once an item is examined, it is possible to tell whether or not it satisfies the condition in one step. However, there does not exist any sorting on

量子コンピュータの実装の歴史

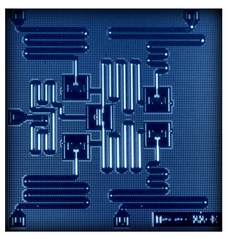
2012年 3 qubit



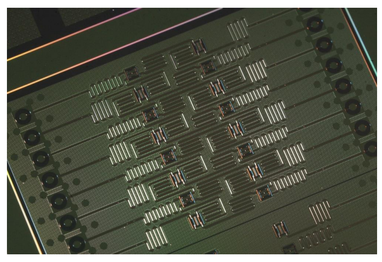
2015年 4 qubit



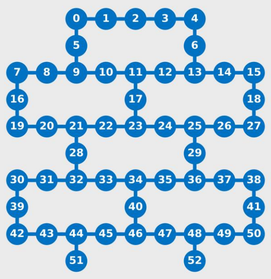
2015年 5 qubit



2017年 16 qubit

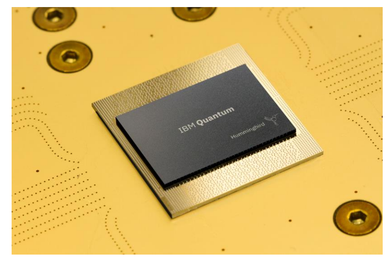


2019年 53 qubit



© IBM Corporation

2020年 65 qubit



© IBM Connie Zhou

大規模集積化