プログラミング教室のテクノロ

プログラミングの世界の歩き方

「量子コンピュータ②」

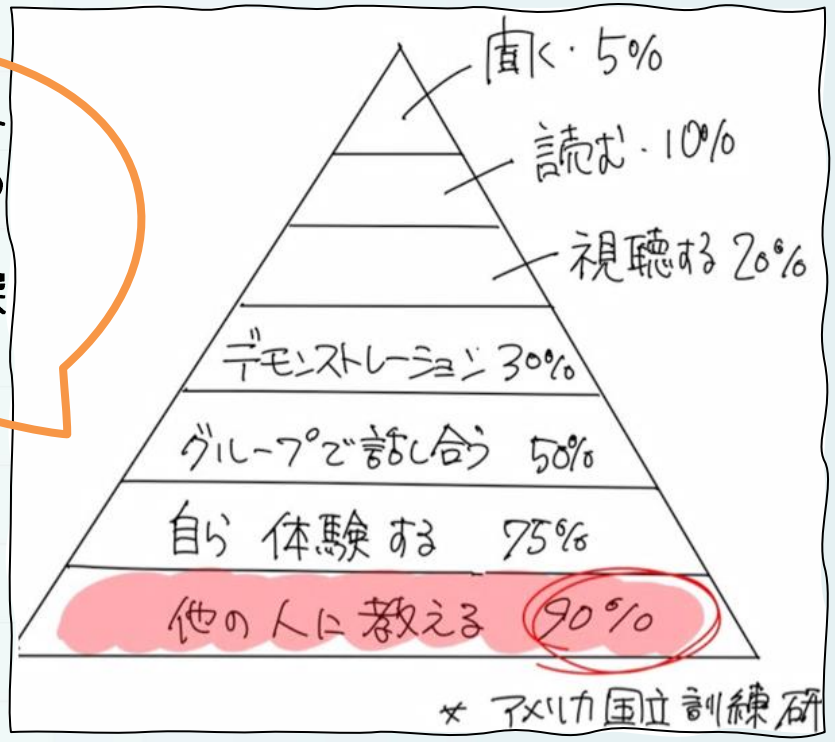
プログラミングの世界を歩こう！

プログラミングの世界を知るにはその世界で使われている
ことばを知ることが大切だ。

これはプログラミングに限らず、スポーツでも音楽でも何かを
習得するには、その世界のことばを知ることから始まるよ。

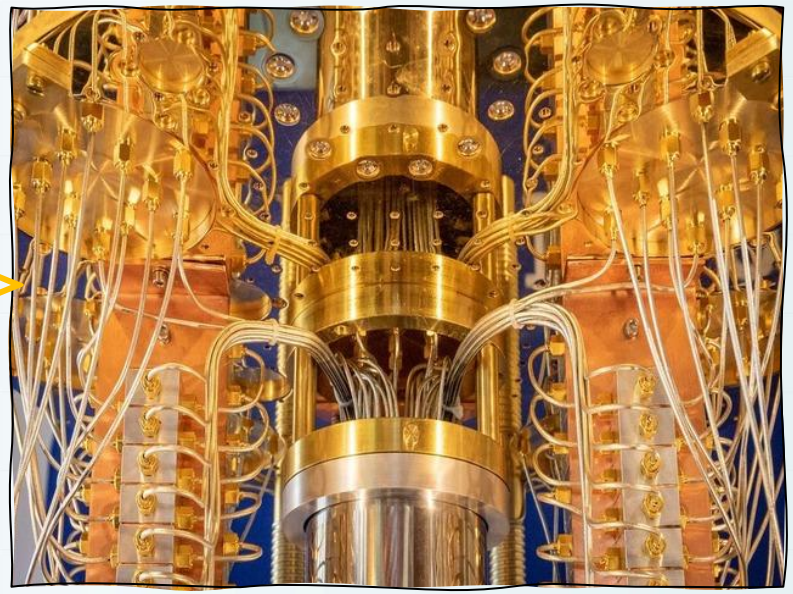
学んだことはみんなに教えてあげよう！
もっと理解が深まるよ！

ラーニングピラミッド



量子コンピュータって？（復習）

量子コンピュータとは、量子の持つ性質を使って従来型のコンピュータ（古典コンピュータ）では容易に解くことのできない複雑な計算を解くことができるコンピュータのこと。



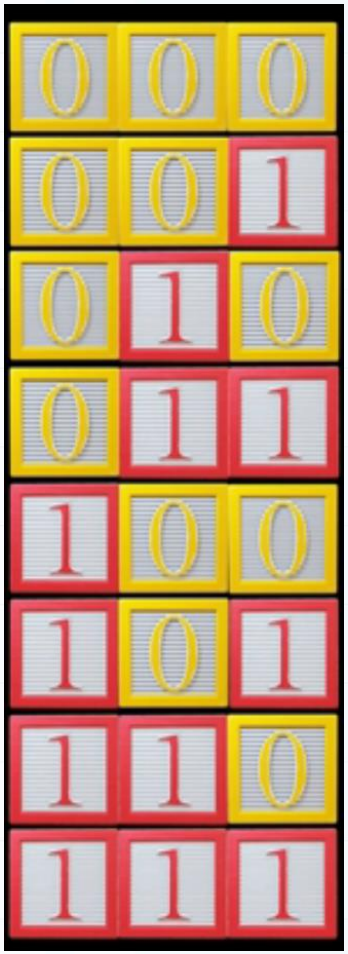
2019年10月、Google社は量子プロセッサを使い、世界最速のスーパーコンピュータでも1万年かかる処理を200秒で処理したと発表した。

量子コンピュータの計算

量子コンピュータは重ね合わせた状態で計算することができる。
しかし、計算結果として取り出すことができるのは重ね合わせたパターンの１つだけ。

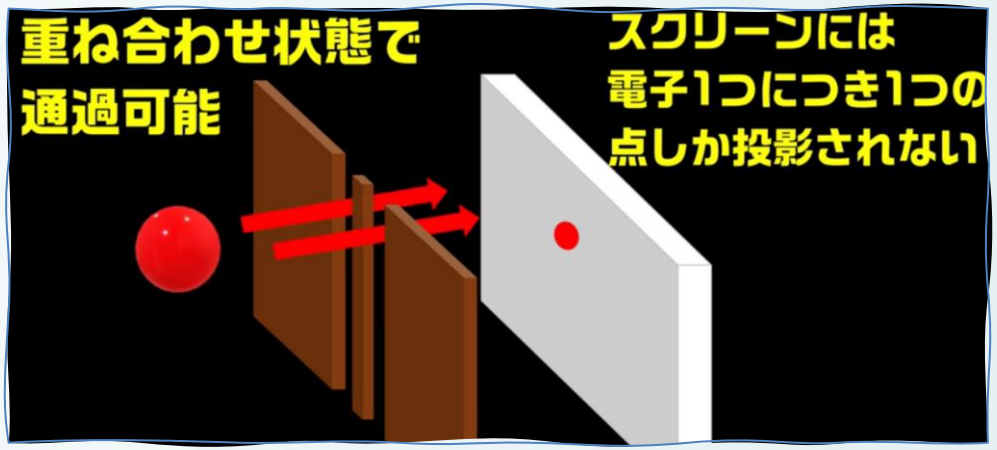
3ビット

1度に表現できるのは8パターンの内の1つだけ。
計算するときも同様に8パターンの内のどれか1つを選択し、計算している。



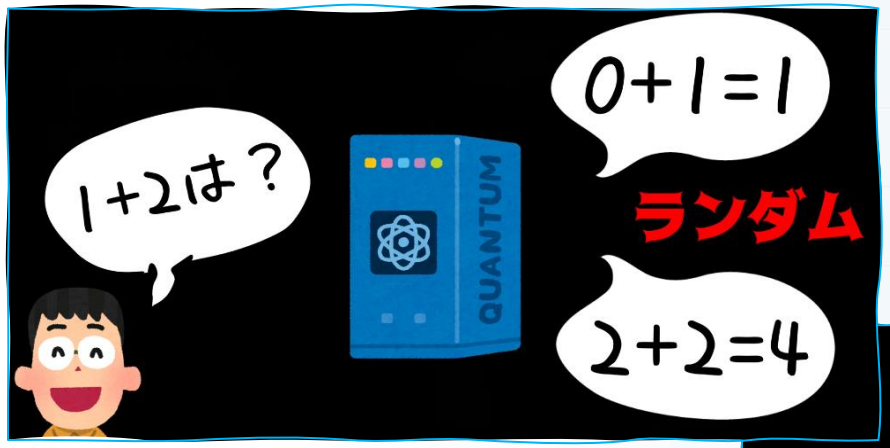
3量子ビット

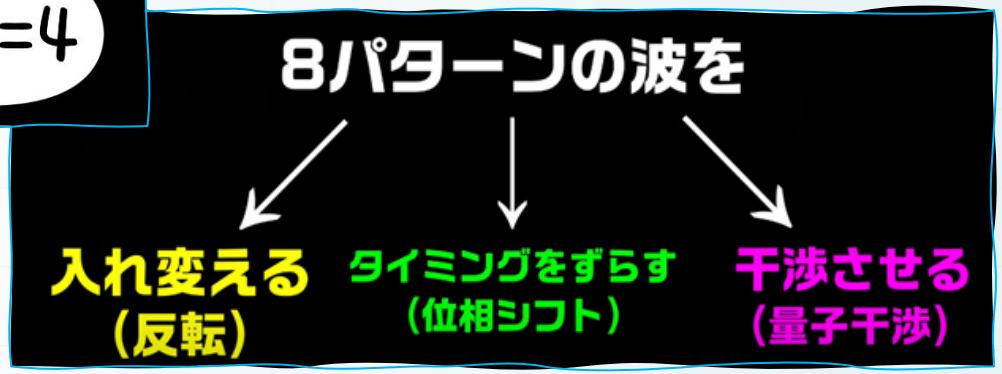
8パターンを重ね合わせて同時に表現することが可能。
計算するときも同様に8パターンを重ね合わせて計算することができる。



量子コンピュータの計算

量子コンピュータは量子ビットを利用し、複数の計算を同時に行うことができるが、欲しい計算結果を取り出すことが非常に難しい。このことが量子コンピュータの実用化を妨げている。

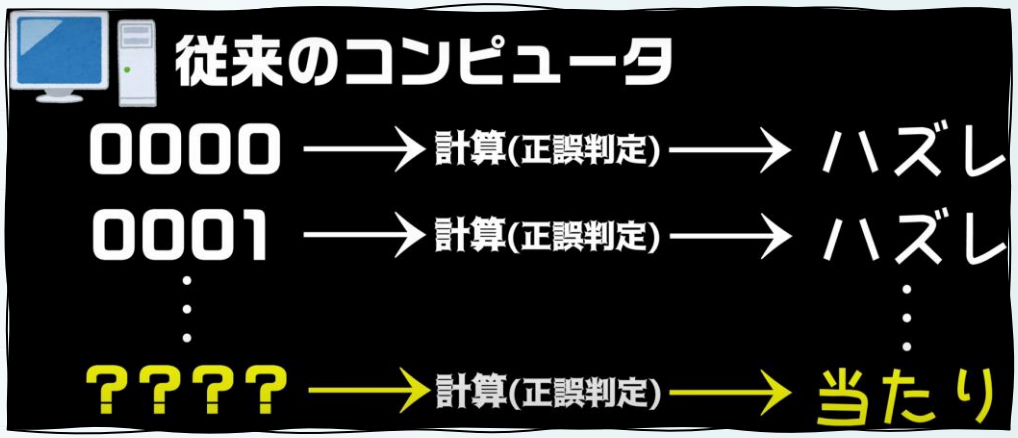


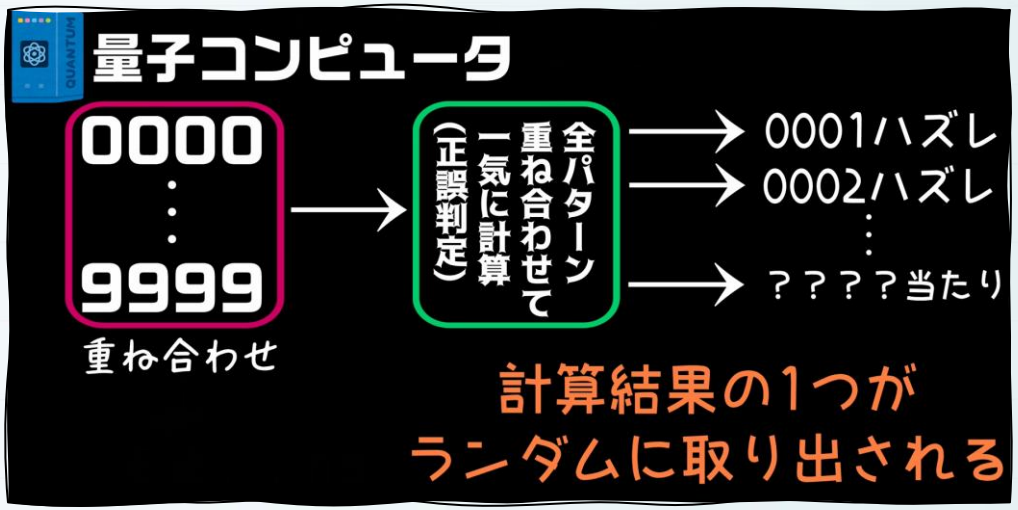


3量子ビッドが表していいるものは、000から111までの8パターンの波がどのような大きさの比と振動のタイミングで重ね合わさっているかという情報になる。8パターンの波をうまく操作して結果を取り出す必要がある。

量子コンピュータの計算

量子コンピュータを使って4桁の暗証番号を解読する場合、量子コンピュータは1度の計算で答えにたどり着くことができる。しかし、そこから正解の暗証番号を取り出すことが非常に難しい。





量子コンピュータの計算

量子コンピュータで高速化できる計算は60種類程、見つかっており、「Quantum Algorithm Zoo」というサイトにまとめられている。

Quantum Algorithm Zoo

This is a comprehensive catalog of quantum algorithms. If you notice any errors or omissions, please email me at stephen.jordan@microsoft.com. (Alternatively, you may submit a pull request to the repository on github.) Your help is appreciated and will be acknowledged.

Algebraic and Number Theoretic Algorithms

Algorithm: Factoring
Speedup: Superpolynomial
Description: Given an *n*-bit integer, find the prime factorization. The quantum algorithm of Peter Shor solves this in $\widetilde{O}(n^3)$ time [82,125]. The fastest known classical algorithm for integer factorization is the general number field sieve, which is believed to run in time $2^{\widetilde{O}(n^{1/3})}$. The best rigorously proven upper bound on the classical complexity of factoring is $O(2^{n/4+o(1)})$ via the Pollard-Strassen algorithm [252, 362]. Shor's factoring algorithm breaks RSA public-key encryption and the closely related quantum algorithms for discrete logarithms break the DSA and ECDSA digital signature schemes and the Diffie-Hellman key-exchange protocol. A quantum algorithm even faster than Shor's for the special case of factoring “semiprimes”, which are widely used in cryptography, is given in [271]. If small factors exist, Shor's algorithm can be beaten by a quantum algorithm using Grover search to speed up the elliptic curve factorization method [366]. Additional optimized versions of Shor's algorithm are given in [384, 386]. There are proposed classical public-key cryptosystems not believed to be broken by quantum algorithms, *cf.* [248]. At the core of Shor's factoring algorithm is order finding, which can be reduced to the Abelian hidden subgroup problem, which is solved using the quantum Fourier transform. A number of other problems are known to reduce to integer factorization including the membership problem for matrix groups over fields of odd order [253], and certain diophantine problems relevant to the synthesis of quantum circuits [254].

Algorithm: Discrete-log
Speedup: Superpolynomial
Description: We are given three *n*-bit numbers *a*, *b*, and *N*, with the promise that $b = a^s \mod N$ for some *s*. The task is to find *s*. As shown by Shor [82], this can be achieved on a quantum computer in poly(*n*) time. The fastest known classical algorithm requires time superpolynomial in *n*. By similar techniques to those in [82], quantum computers can solve the discrete logarithm problem on elliptic curves, thereby breaking elliptic curve cryptography [109, 14]. A further optimization to Shor's algorithm is given in [385]. The superpolynomial quantum speedup has also been extended to the

Navigation

Translations

This page has been translated into:
Japanese
Chinese

Other Surveys

For overviews of quantum algorithms I recommend:

Nielsen and Chuang
Childs
Preskill
Mosca
Childs and van Dam
van Dam and Sasaki
Bacon and van Dam
Montanaro
Hidary

Terminology

メモ

プログラミング教室のテクノロ

なまえ：