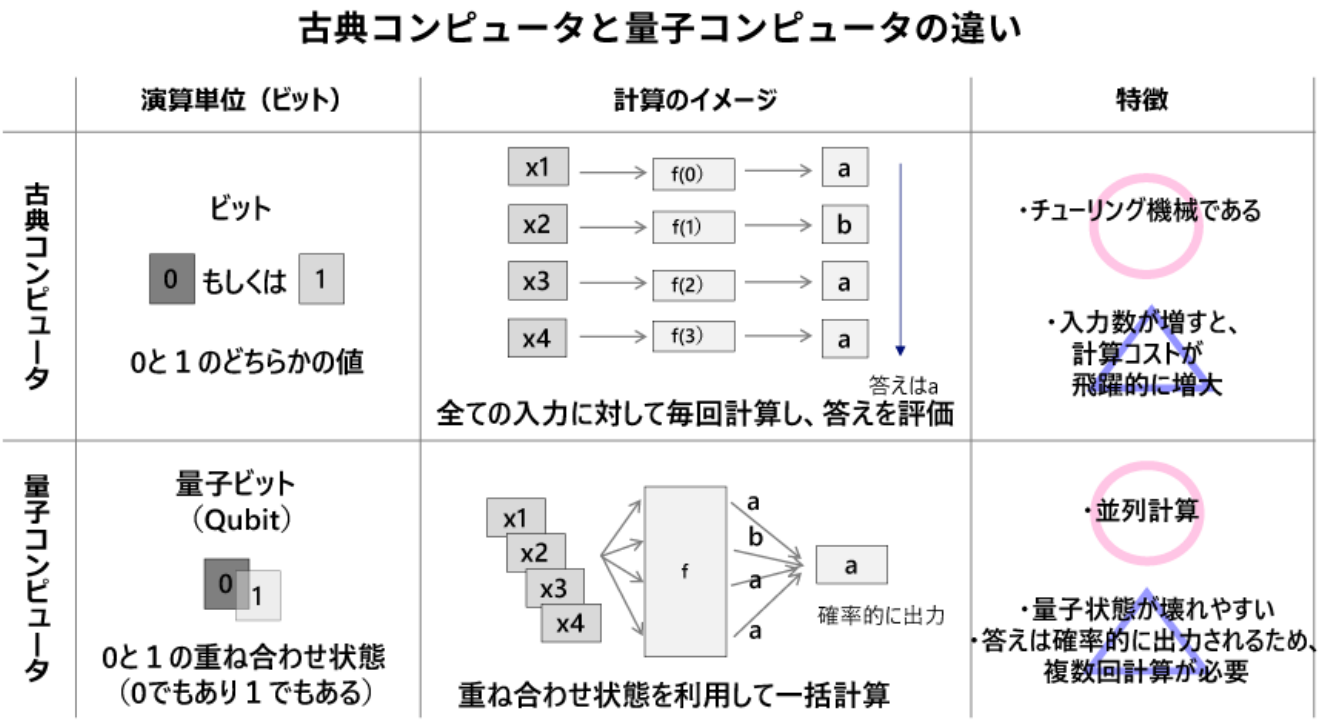
19. 量子コンピュータ（Quantum Computer）

量子コンピュータは、物質を構成する原子や電子などの「量子」の持つ性質を利用して情報処理を行うコンピュータです。量子の運動は「量子力学」に支配されており、量子の世界においては「量子重ね合わせ」と呼ばれる現象、即ち相反する 2 つ以上の状態が共存出来る現象を用いて並列計算を行うことで、これまで以上の速度・規模の情報処理を可能にするとされる次世代コンピューターのことです。

量子コンピューターにおける基本単位「量子ビット」は、0 と 1 が重なり合って存在する状態を意味します。



(注)チューリング機械：1936 年アラン・チューリングが発表したコンピュータの仕組み・原理＝現在のコンピュータ

コンピュータは「0」と「1」の組み合わせで情報を処理します。たとえばアルファベットの A は「0000」、B は「0001」、C は「0010」といったように、文字や画像、音や計算などすべてが 0 と 1 の組み合わせでできているのです。この単位を「ビット=bit」といいます。

従来型コンピュータ(古典コンピュータ)でのビットは 0 か 1 のどちらかであり、ふたつ以上の状態は同時に表せません。

これを「0 でもあり 1 でもある」としたのが量子コンピュータにおける「量子ビット」の考えです。このように 0 と 1 が重ね合わさった状態を「重ね合わせ」といいます。

従来型コンピューティングの情報の基本単位がバイナリービット(Binary bit)、量子コンピューティングの情報の基本単位が量子ビット (Qubit) です。

バイナリービット(Binary bit)は

コンピュータが扱うバイナリデータとしては、2 進数の 1 または 0 が格納される 1 桁を「ビット」と呼びます。さらに 16 進数でバイナリデータを扱う際の基本単位は「バイト(Byte)」と呼び、1 バイトは 2 進数でいう 8 ビットで構成されます。

量子ビット(Quantum bit, Qbit)は

量子情報の最小単位です。従来の情報量の単位「bit」に対する単位の表現としては、quantum bit と書くよりは Qubit(キュービット・キュビット・クビットなど)と書くことが多いです。また、古典的な(非量子的)ビットを明示する場合、古典ビット (classical bit, Cbit) などと書くことがあります。

量子情報処理において Qubit は量子力学的 2 準位系の状態ベクトルで表現されます。一方古典ビットは 2 状態です(以下ではその 2 つの状態をそれぞれ、0 と 1 とする)。それに対して量子ビットは、そのような 2 状態の量子力学的重ね合わせ状態もとることができます。ブラ-ケット記法*では、1 量子ビットは、

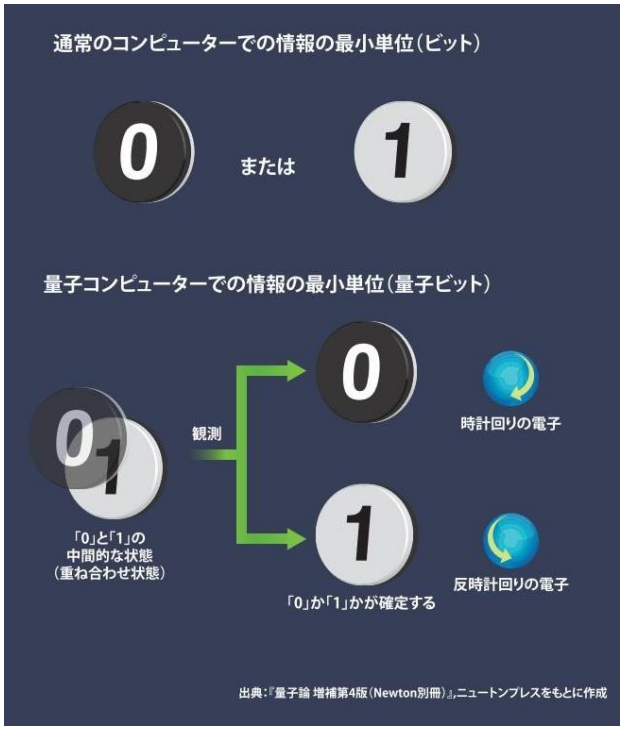
$\alpha|0\rangle+\beta|1\rangle$と表現されます。ここで、$\alpha,\beta$は $|\alpha|^2+|\beta|^2=1$の関係を満たす複素数である。これを観測した

際、状態$|0\rangle$を得る確率は $|\alpha|^2$であり、状態$|1\rangle$を得る確率は$|\beta|^2$である。同じ記法で古典ビットを表現すると、α,βは、どちらかが 0 で、もう一方が 1 です。
つまり、ビットは 0 と 1 の状態しかとれないことに対して量子ビットは 0 と 1 と、その重ね合わせの状態を取れるということです。

＊ブラ-ケット記法(bra-ket notation)は量子力学における
量子状態を記述するための標準的な記法。
ブラケット(bra-ket)という呼称は、量子状態をブラ(bra)
$\langle\phi|$とケット(ket) $|\phi\rangle$と呼ばれる

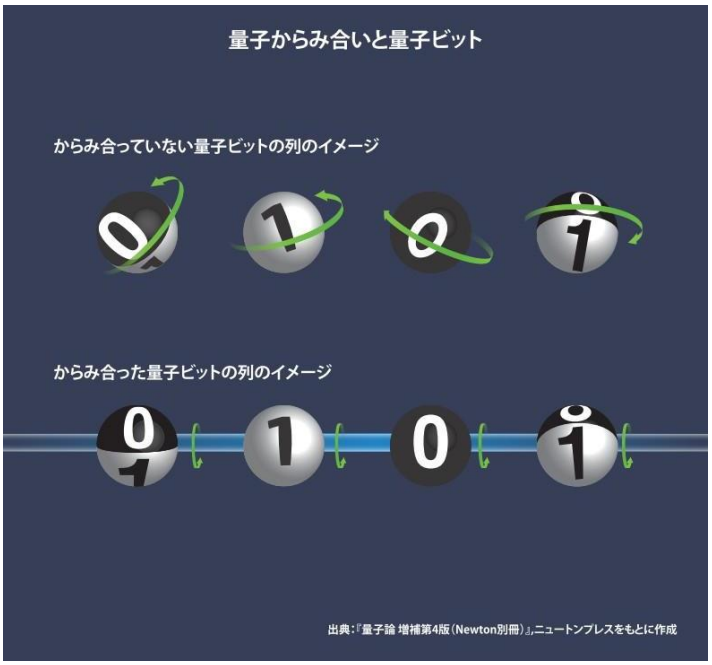
2 つのベクトルで表すこと、またブラとケットの内積
$\langle\phi|\phi\rangle$ が括弧(bracket)を成すことに由来しています。

量子ビットは、1 つのものが同時に複数の場所
に存在する、複数の状態を持ちます。
この「重ね合わせ状態(共存した状態)」を使
ってビットを表現します。



たとえば、粒子の持つ物理量の 1 つである「スピン（≒自転）」を使って、ある電子の右回りのスピンを「0」、左回りのスピンを「1」としたとき、重ね合わせ状態にある電子はこの「0」と「1」を同時に持つことができる。こうした電子を 2 つ用いて、「00」「01」「11」「10」を表現できるということになります。

もう 1 つ重要なのが「量子もつれ（エンタングルメント、量子からみ）」と呼ばれる、量子の特徴です。量子もつれの状態にある 2 つの電子があるとき、一方の電子において右回りのスピンが“観測”された場合にもう一方は左回りのスピンが確定します。つまり、1 つが右（左）回りであるとき、もう 1 つは左（右）回りであり、という状態が量子もつれです。量子もつれの状態にある 2 つの電子は、このようにスピンの値を打ち消し合います。



これが量子コンピューターになぜ必要なのかというと、高速に並列計算を行うためです。
絡み合っていない量子ビットのビット列は個々に動いてしまいます。複数の量子ビットが絡み合っていれば、1 つの量子ビットに対する作用を、瞬時に、全体へ及ぼすことができるのです。

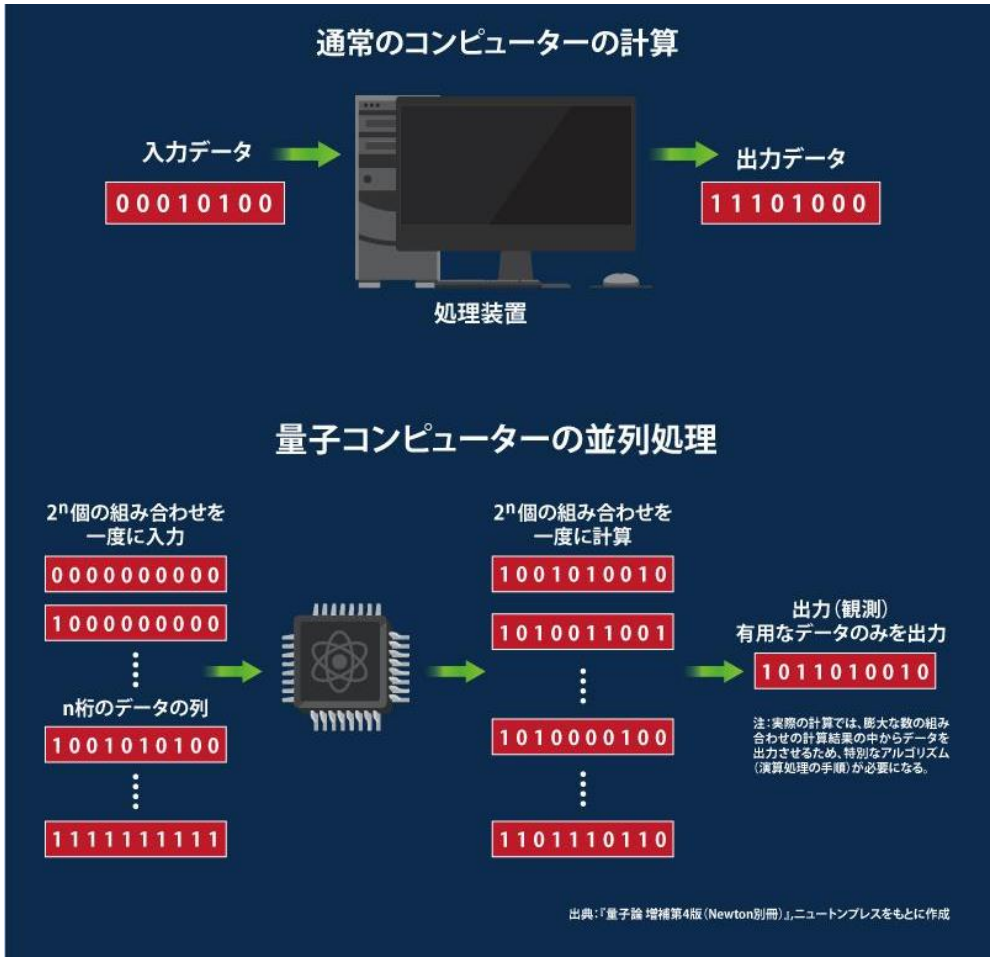
量子コンピュータは問題を解く方法の違いにより、「量子ゲート方式」と「量子アニーリング方式」の大きく 2 つに分類されます。

量子ゲート方式

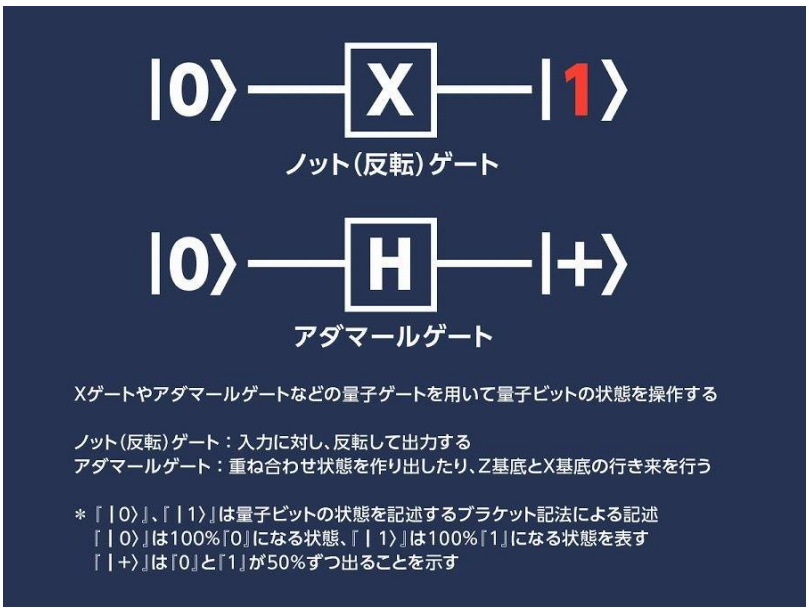
量子ゲート方式は、従来のコンピューターのビットに相当する量子ビットを用意し、論理ゲートに相当する量子ゲートが作用を行い、演算処理（可逆計算）を行う。いわば、従来のコンピューター（古典的コンピューター）の拡張版です。
ただ、従来のコンピューターの拡張版と言っても、計算の仕組みはまったく異なります。2^n の組み合わせからある暗号鍵を求めるとき、従来のコンピューターでは 2^n 通りの組み合わせを計算し、その 1 つ 1 つで暗号が解けるかを確認します。それに対し、量子コンピューターでは 2^n の組み合わせを一度に入力し、2^n の組み合わせを一度に計算し、そこから 1 つの答えを出します。

量子アニーリング方式

量子アニーリング方式は、組合せ最適化問題に特化した量子アルゴリズムの一つです。量子ゲート方式に比べればシンプルに実現できるため、比較的多くの量子ビットで量子コンピュータを実現することに成功しています（2017/07 現在、2048 qubit）。



量子ビットの計算例



ただし、量子コンピューターとして期待される性能を出すには大量の量子ビットが必要となります。数千個クラスの量子ビットを生成し、いかに制御するか、それが量子ゲート方式のハードウェア実装における大きな課題となっています。

つまり、ハードウェア的に実現する困難さがそのまま量子コンピューターの実現の難しさになっているのです。絶対零度を保つ巨大な冷蔵庫を作ってその中に量子状態の電子を大量に配置し、回路化する。それでも有用な量子ビットをどれだけ備えることができるのか、という状況にあります。
神奈川県川崎市に 2021 年に設置された IBM Quantum System One(量子コンピュータ)は、巨大な装置のほとんどが冷却装置です。

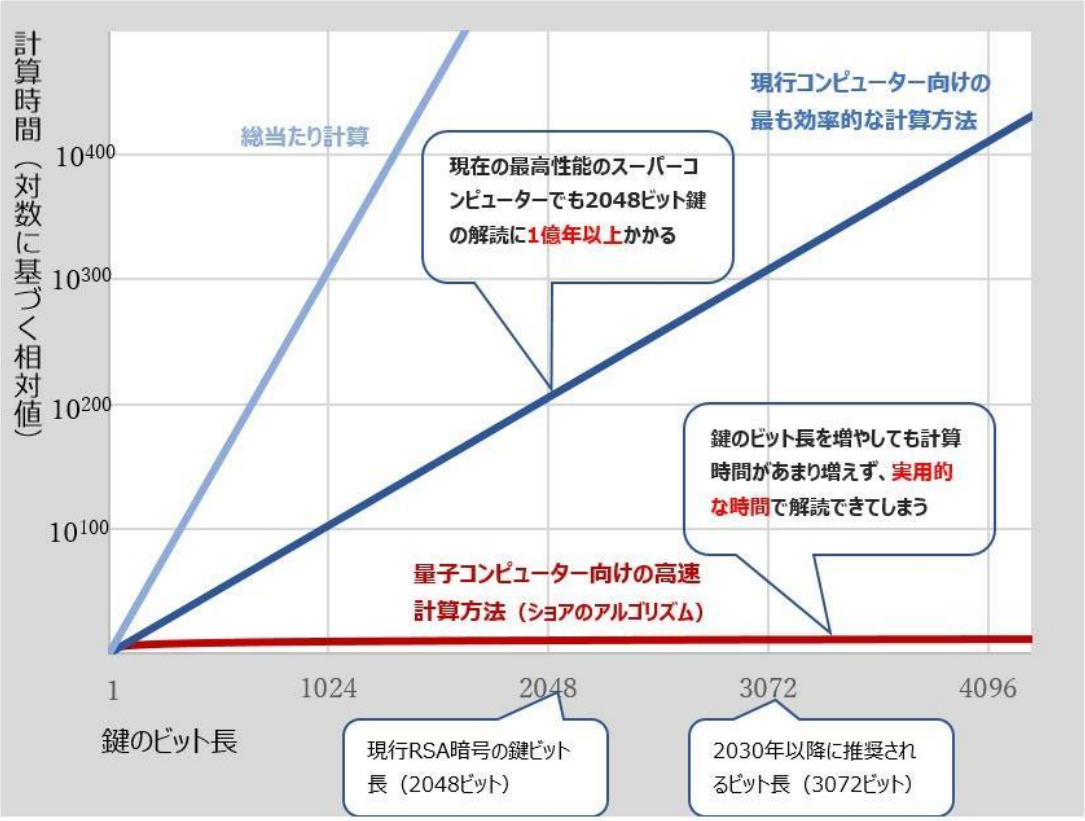
量子アルゴリズム

1994 年、ピーター・ショアが発表した因数分解の量子アルゴリズムが量子コンピューターの可能性を広く知らしめた。これは n 桁の整数の因数分解を O(n^3)以下の手順で効率的に解くというもので、量子計算を行うことで大量の桁数の因数分解が高速に解けることを数学的に証明した。

因数分解は組み合わせ(桁数)が増えれば増えるほど、計算量は莫大になっていく。現在使われている RSA 暗号の鍵の長さは 1024 ビット(208 桁)～最長 2048 ビット(617 桁)。300 桁以上の素数の積を因数分解するためには、スーパーコンピューターを用いても解読に 1 億年以上かかると推定されている。

RSA 暗号鍵の計算時間のイメージ

(RSA は発明した3人の名前「R. L. Rivest、A. Shamir、L. Adleman」に由来)



RSA 暗号

RSA 暗号とは、素数を掛けあわせた数字の素因数分解の仕組みを利用した暗号技術の一つです。
大きな数字を素因数分解するのは困難です。総当たりする以外に素因数を見つけ出す方法がないためです。したがって、コンピュータで素因数分解しようとしても、大きな数であれば膨大な時間が掛ります。

以　上