1. 量子コンピュータへの誘い

量子コンピュータはいま、最も注目されている技術の一つと言っても過言ではないでしょう。注目されている理由は、従来のコンピュータでは時間が掛かり過ぎて不可能だった様々な計算が、現実的な時間で計算できるようになる可能性を秘めているからです。例えば、

- RSA暗号や楕円曲線暗号といった**暗号への攻撃**
- ポートフォリオ最適化やデリバティブの価格付けなど**金融への応用**
- 様々な**機械学習**アルゴリズムの高速化

などなど、実現すれば熱い話がたくさんあります。暗号理論では既に「**耐量子計算機暗号**」として格子暗号などの研究が進められています。

そんな量子コンピュータの「今」を、ここでは3つの側面から紹介しましょう。

1. これまでの歴史
2. 動作原理：量子状態
3. 量子コンピュータの実機が出来るまで

1.1 量子コンピュータの歴史

1950年代から1980年代まで

1950年代から1980年代にかけて、量子コンピュータは量子力学の権威でありノーベル物理学賞を受賞した**リチャード・ファインマン**（R. Feynmann）、ロシアの天才数学者**ユーリ・マニン**（Y. Manin）、核化学の若き天才**ポール・ベニオフ**（P. A. Benioff）の着想に端を発し、物理学者の**デイビッド・ドイッチェ**（D. Deutsch）によって定式化されました。

ファインマン

マニン

ベニオフ

ドイッチェ

※ wikipediaから抜粋

1990年代

1990年代になると、量子コンピュータの魅力的な応用が発見されるようになります。特に1994年に発表された**ピーター・ショア（P. Shor）の素因数分解アルゴリズム**とそのRSA暗号への攻撃への応用は衝撃的な話題になりました。また、金融への応用や機械学習アルゴリズムの高速化を支える**ロブ・グローバー（L. Grover）のアルゴリズム**も1996年に発表されます。

Peter Shor

Lob Grover

※ お二方のホームページから抜粋

2000年代

2000年代になると量子コンピュータの実機の開発に関わる大きな進捗が生まれました。「15=3×5」という小さな素因数分解ではあるものの、この素因数分解が計算できる程度の量子コンピュータが

- 核磁気共鳴
- 光子

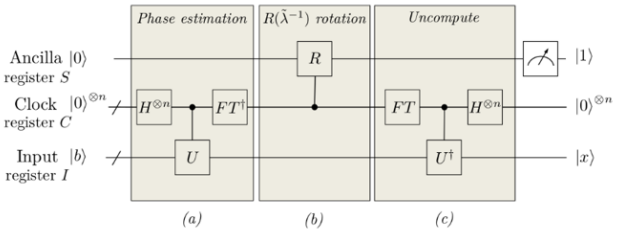
など複数の手法で実現し、実際にショアの素因数分解アルゴリズムによって15の素因数分解も行われました。

また実世界への応用に関するトピックでも非常に重要な発見がありました。2009年、アラム・ハロウ（Aram Harrow）, アビナタン・ハッシディム（Avinatan Hassidim）, セス・ロイド（Seth Lloyd）による連立1次方程式の解を求めるための量子コンピュータのアルゴリズムの発見です。このアルゴリズムは発見した

3名の名前の頭文字をとって、**HHLアルゴリズム**と呼ばれています。連立1次方程式はさまざまな分野の計算の基本になっているだけに、HHLアルゴリズムの発見は量子コンピュータの可能性を格段に広げたセンセーショナルな結果でした。

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &= b_2 \\ \vdots & \vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &= b_m \end{cases}$$

連立一次方程式



HHL algorithm

Quantum circuit design for solving linear systems of equations (Cao et al, 2012)

2010年代

そして2010年代、グローバーのアルゴリズムとHHLアルゴリズムなどが主な基礎となって、魅力的な応用がたくさん提案されてきました。金融ではポートフォリオ最適化やデリバティブの価格付け、機械学習ではさまざまな機械学習アルゴリズム（k-近傍法やニューラルネットワーク、k-median法など）が量子コンピュータのアルゴリズムとして提案され、従来のコンピュータより高速に計算できる可能性が期待されています。

1.2 5分で眺める動作原理：量子状態

1.2.1 状態

量子コンピュータは物理学で深く研究されてきた「**量子状態**」という面白い現象が動作原理になっています。量子状態の詳しい考え方は「4. qubit」で数学的に厳密な解説を行いますが、ここでは物理学でのイメージを用いて少しだけ垣間見ておきましょう。以下では、光の波の状態の表現方法を考えます。

1.2.2 状態の測定と偏光板の実験

一般的に私たちが考えている状態と光の「状態」は、「**測定**」という操作を入れると大きく事情が異なってくることが知られています。**偏光板の実験**という有名な実験があるので、せっかくなので動画で見てみましょう。

https://www.youtube.com/watch?v=1Jo9AkQUBgw (https://www.youtube.com/watch?v=1Jo9AkQUBgw)

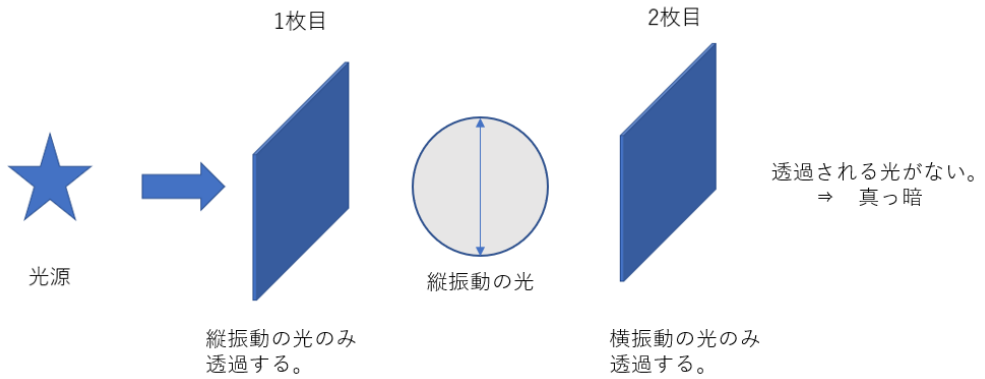
2枚の偏光板を通して光源を見たとき、次の現象が見られたことでしょう。

- 光が暗く見える。
- 2枚目の偏光板を回転させると、光が見えたり見えなくなったりする。

暗く見えるだけならわかる気もしますが、見えたり見えなくなったりするのは何とも不思議な現象ですね...。この現象が、物理学でどう説明されるのか紹介しましょう。

実験と矛盾する解釈

光子が偏光板を通ると、光が「縦振動」か「横振動」だったかが測定され、「縦振動」だった光だけが透過される仕組みになっています。さて、光源から出る光は様々な方向に振動しているはずです。1枚目の偏光板によって、光が「縦向き」だったものだけが透過されたとしましょう。さて2枚目の偏光板を少し斜めにしたとき、光は偏光板を通ることが出来るでしょうか。偏光板が斜めになったことによって「縦振動」の光は透過できなくなったので、光は全く透過できなくなるように考えられます。



しかしこれは**実験と矛盾**しています。なぜなら、この説明だと偏光板を少し斜めにだけで光源はすっかり見えなくなってしまいます。しかし実際には暗くはなるものの、見えなくなるケースは限られていたからです。では、上の説明のどこが間違っていたのでしょうか。

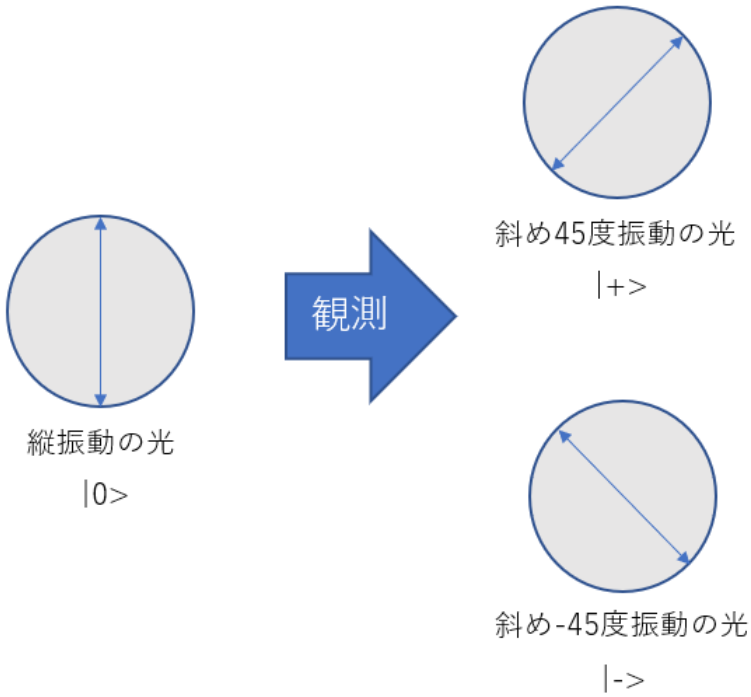
実験結果を説明できる解釈

ここで、直感的ではない次の考え方を導入します。

- 量子状態特有の法則：**測定が状態を変化させる。**

今回であれば、1枚目の偏光板を光が通る際に、様々な方向に振動している光は一度「縦振動」か「横振動」かのどちらかに**状態が変化**するのです。このように測定によって状態が「縦振動」か「横振動」かに変化した光のうち、「縦振動」の光だけが偏光板を透過できます。

同様に考えると、斜めに回転した2枚目の偏光板は「斜め45度向きの振動」と「斜め-45度向きの振動」の光どちらかを測定します。1枚目の偏光板を透過した「縦振動」の光たちは、この測定によって「斜め45度向きの振動」か「斜め-45度向きの振動」かのどちらかに状態が変化し、「斜め45度向きの振動」だったものだけがこの偏光板を透過する。そういう仕組みだと考えればこの現象は説明できます。



2枚目の偏光板を回転させることで光が見えなくなったりする理由も、次のように考えられます。2枚目の偏光板が1枚目の偏光板に対して横向きになったとき、2枚目の偏光板は「縦振動」か「横振動」かを測定し、「横振動」の光を透過します。ところで、1枚目の偏光板から透過されてくるのは「縦振動」の光のみです。「縦振動」の光子は「横振動」と測定することが出来ないために、2枚目の偏光板を透過できる光が存在せず、光が見えなくなるわけです。

1.2.3 状態の重ね合わせ

偏光板の実験から、光子の状態は

- 「縦振動」・「横振動」の状態
- 「斜め45度向きの振動」・「斜め-45度向きの振動」の状態

など、何らかの相反する振動の方向のいずれかに測定すると決めたとき、測定後の状態もそのいずれかに変化することが分かりました。

これは光の状態がそのような相反する振動方向の重ね合わせで表現できると解釈することもできます。例えば、「縦振動」の状態は「斜め45度向きの振動」の状態と「斜め-45度向きの振動」の状態が1/2ずつで重ね合わさっていると考えれば、1枚目の偏光板から斜めになった2枚目の偏光板に光を通した後に測定される光の明るさが1/2になっても納得がいくわけです。これを**状態の重ね合わせ**といいます。