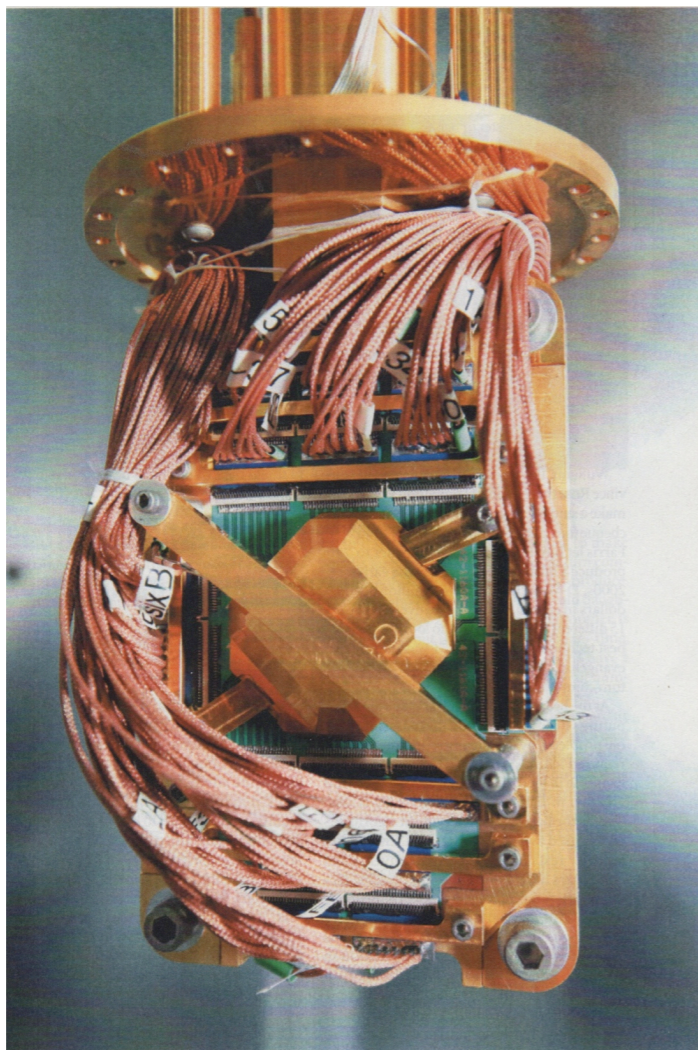
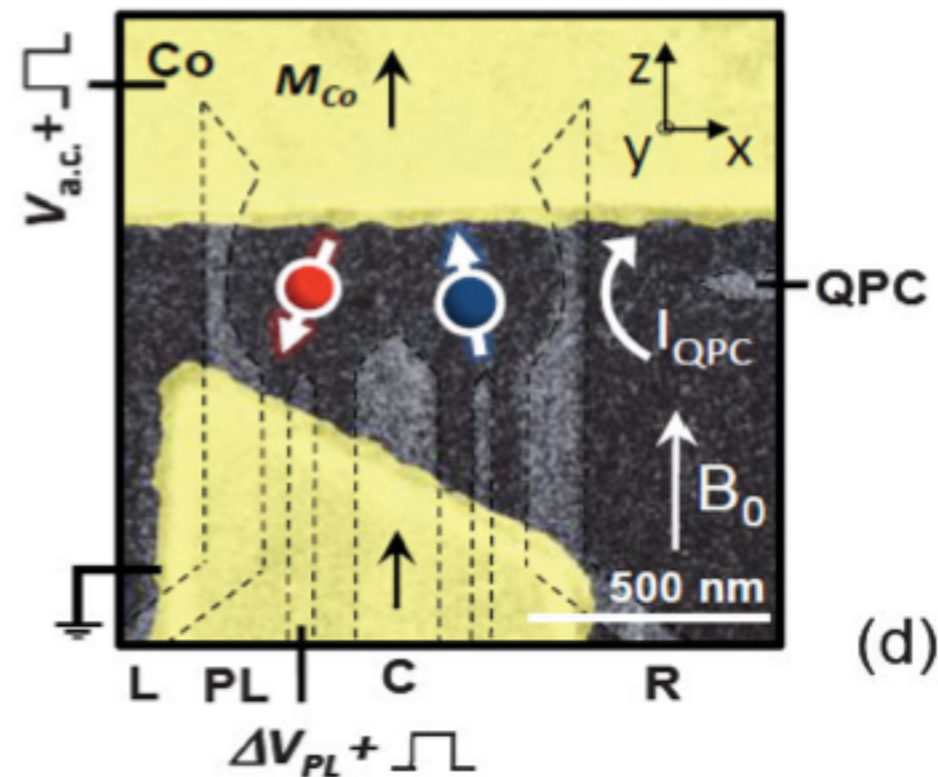


# 量子力学を活用した情報科学に触れる

物性理論グループ 都倉康弘、吉田恭、TA(予定)



Nature 498, 286 (2013)



Phys. Rev. Lett. 107, 146801 (2011).

# 情報理論

クロード・エルウッド・シャノン

修士論文 "A Symbolic Analysis of Relay and Switching Circuits"において、電気回路（ないし電子回路）が論理演算に対応することを示した。



1948年論文「通信の数学的理論」を公表、それまで曖昧な概念だった「情報」(information)の尺度（ビット）を定義し、情報についての理論（情報理論）という新たな数学的理論を創始した。

シャノン・エントロピー 
$$H = - \sum_i p_i \log_2 p_i$$

# 量子力学

- 量子力学の不思議な性質

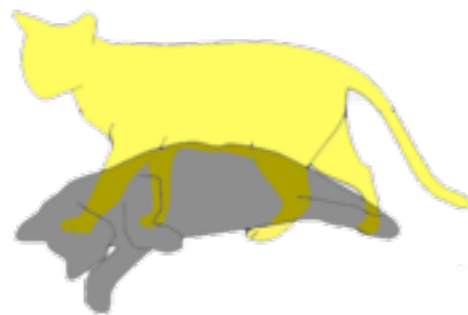
重ね合わせの原理

量子もつれ

波束の収縮



*Y. Aharonov and D. Rohrlich, "Quantum Paradoxes", Wiley-VCH 2nd, 2009*



*Schrödinger* の猫

フォンノイマン・エントロピー

$$S_{vN} = -\text{Tr} [\hat{\rho} \ln \hat{\rho}]$$

# 量子力学を使った計算

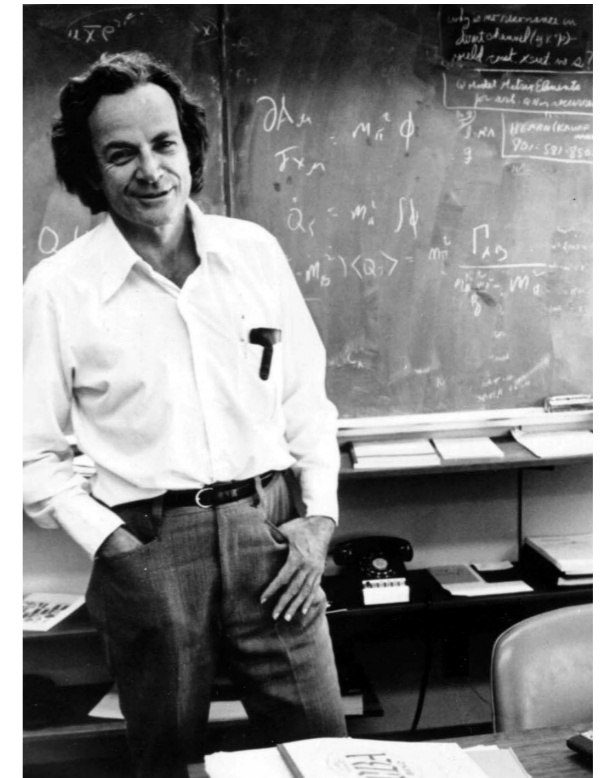
- ・ 「計算」に活用できるのではないか？

量子シミュレーター R. P. Feynman (1982)

量子チューリング機械 D. Deutsch (1985)



- ・ 量子コンピューター

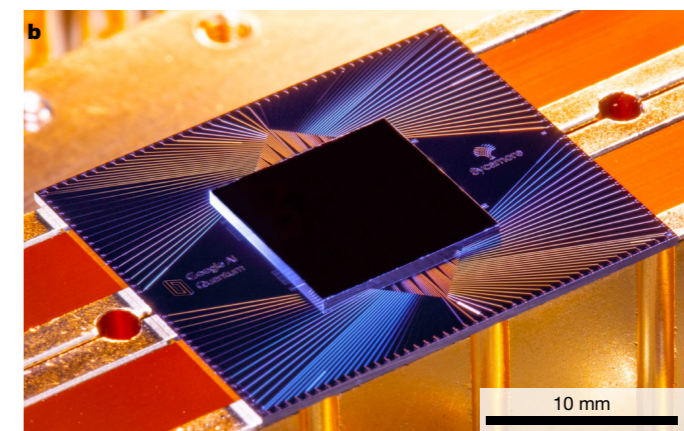


## 量子超越性

グーグルの発表(2019年10月23日)

*F. Arute, et al., Nature 574, 505 (2019).*

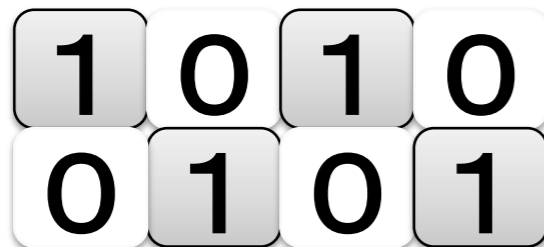
53量子ビット(超伝導体を使ったもの)



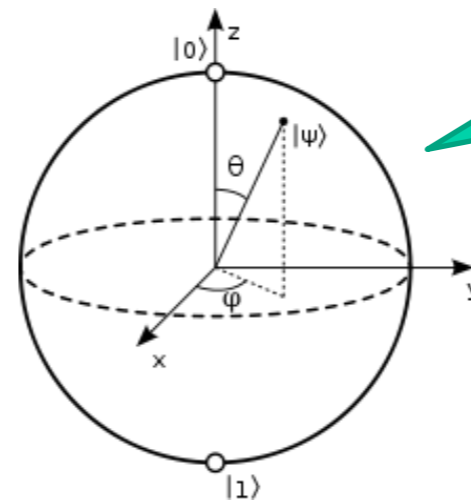
# 量子ビットとは何だろうか

- 量子ビットの性質

古典コンピューター  
のビット



## 量子ビット



1と0が確率的に重なり合っている



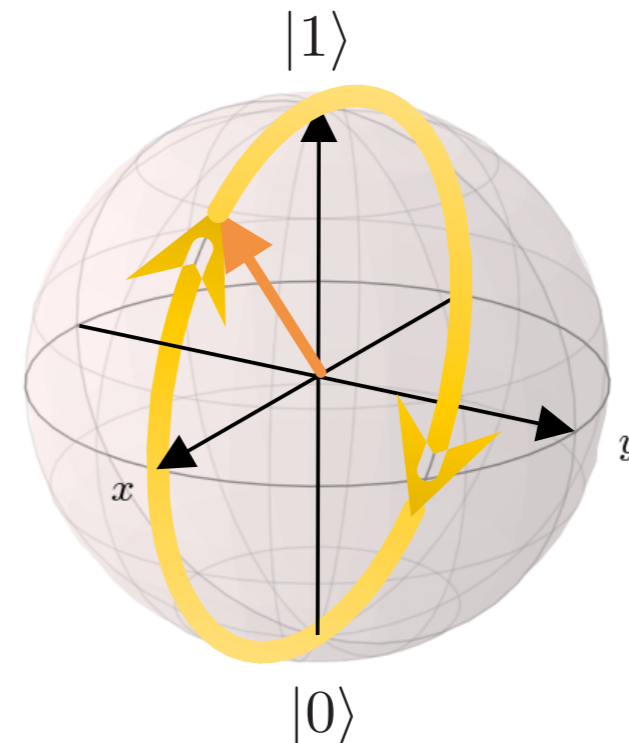
例えば、0が30%, 1が70%

- 単一量子ビット操作

状態の初期化

状態の制御

状態の読み出し



# 課題探求実習の講義について

---

- ・ 受け入れ可能人数

4名まで

量子力学未履修の場合も対応いたします。

- ・ 頻度、曜日、時間

週1回1限程度を予定

曜日、時間、実施方法は相談の上決定します

- ・ その他

テキストやマニュアルなどを適宜配布

自主課題について必要に応じて教員、TA が指導します

# 具体的内容(相談の上決定します)

- 量子情報理論の基礎の演習

量子力学（離散系）の学び

学類の授業で学ぶ量子力学を別の視点から眺めてみる  
(量子) 情報理論のエッセンスに触れる

物理的に実現している実験系について学ぶ

量子コンピューターができたなら何がすごいのか？  
現在、世界中で研究はどれくらい進んでいるのか？

- 自主課題の選定と実習、結果のポスター発表

課題選定に関わる議論

課題に対してグループでの実習

雙峰祭などでのポスター発表、最終レポートにまとめる

# 2017年度ポスタ一発表

## 双峰祭(2017 11/4)

### 量子暗号ってなあに？



課題探求実習セミナー2017

筑波大学理工学群物理学類 3年葛西紘人 2年植木雄大

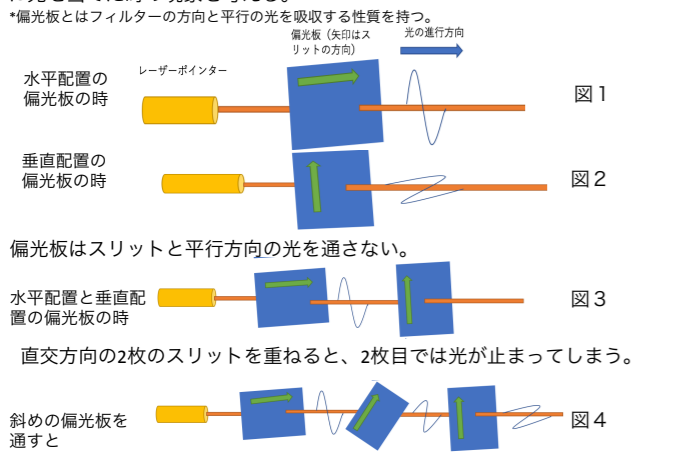


#### 量子暗号

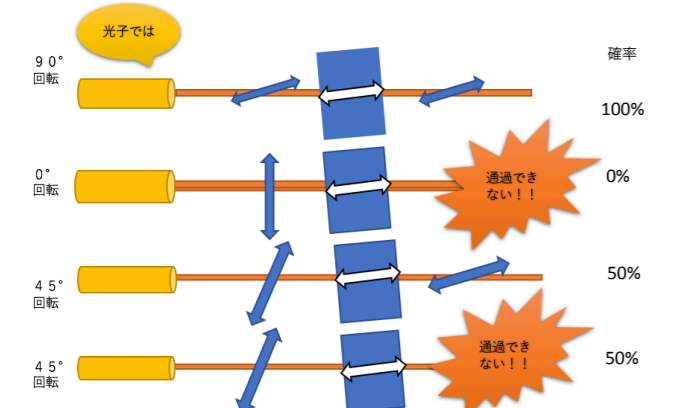
##### 背景

量子暗号とは、量子力学の原理と情報理論を融合させた、誰にも解読することができない暗号のことである。

これを理解するために必要な光の現象について見てみよう。まず、偏光板\*に光を当てた時の現象を考える。



ここから、量子暗号に用いるための光子との違いを比較する。光とは明るさを弱めていくと一つ一つの粒のような性質もつ。この粒のことを光子と呼ぶ。



#### 必要な量子力学の原理

##### 重ね合わせの原理:

斜めに偏極された光子は、縦の偏極と横の偏極の状態を同時に合わせ持つ、重ね合わせで表すことができる。

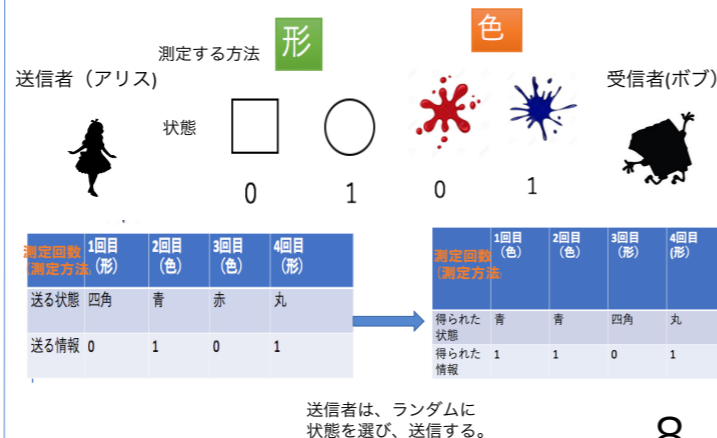
##### 不確定性原理:

横に偏極された光子を掛け算のマークのスリットで観測する。この観測の結果として、横の偏極の状態が破壊される。破壊された後に、足し算マークのスリットで観測しても、横に偏極された光子が観測されず、残りの50%では、縦に偏極された光子が観測される。

##### 量子複製不可能定理:

光子は、観測を行うことで状態が壊れてしまう。よって、観測後の光子は観測前の状態とは限らない。ここで、光子を観測せずに、観測前の状態を得ることを考える。これを実現するために、光子を複製しようと試みる。しかし、この定理により、光子を観測することなしに、複製をすることができない。よって、観測前の状態を壊さずに得ることは不可能である。

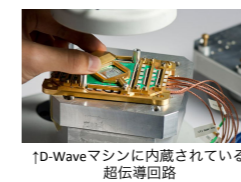
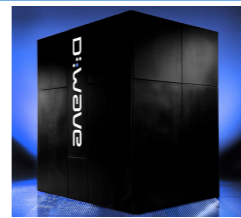
#### BB84の原理



##### fund

チャー企業のD-Wave社が、**量子コンピュータ**を発表した。コンピュータとは動作原理が根本的に異なる量子力学という背景には量子力学という異なる原理が提案されたアルゴリズムである。

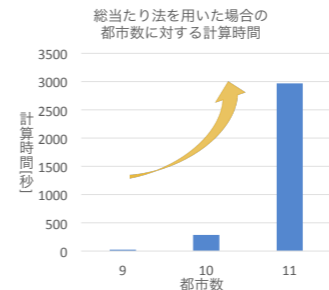
発した量子コンピュータで「**リング**」という、東京工大が提案したアルゴリズムをD-Waveマシンに実装し、具体動作するのを知りたいと思ふためとした。



##### ion

がかかる問題の一つとして「**旅行セールスマン問題**」を取り扱う方法で解き、計算を比較することを目標とする。

方法として「**ヒルソーク法(SA法)**」「**量子アニーリング(QA法)**」を用いる。「ヒルソーク法」は、旅行セールスマン問題の元になったアニーリング法と比べて計算できる。



旅行セールスマン問題は、複数の都市を1回ずつ回る時の最短経路を求める問題である。ルートの個数は $5 \times 4 \times \dots \times 1 = 120$ 通りだが、都市が増えていくと、ルートの個数は急激に増加していく。(10都市なら約363万通り)。このように急激に計算量が「**NP困難問題**」と言う。

#### 研究方法

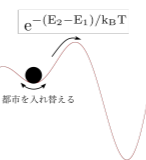
Think Pad (CPU: Core i-5-6200U RAM: 8.00GB)であり、使用言語はPython

##### 最適解の導出

ヒルソーク法とも呼ばれる。「焼きなまし」とは、金属材料を適当な温度に加熱して冷やしていくことである。これによって、内部のエネルギーを均一にしたり、化学組成を均質にしたりする。この原理を「**焼きなまし**」を徐々に下げ、最適解を求める。

1) 経路を一つ決め、総距離 $E_{t1}$ を求める。  
2) 都市を入れ替えて、総距離 $E_{t2}$ を求める。  
3)  $E_{t2}$ を次の $E_{t1}$ として考える。  
4)  $E_{t2} < E_{t1}$ の確率で $E_{t2}$ を次の $E_{t1}$ として考える。  
5) 低くして2~4を繰り返す。  
6)  $E_{t1}$ が最適解である。

は右図のように、 $e^{-\frac{E_{t2}-E_{t1}}{k_B T}}$ の確率で $E_{t2}$ を採用することで、最適解を求めることができる。



#### 量子力学を用いた最適化問題

課題探求実習セミナー「量子ビットを体験してみよう」より



筑波大学理工学群物理学類 上村俊介 大滝恒輝

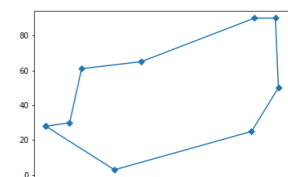


#### 研究の背景・動機

#### 総当たりによるシミュレーション

##### 厳密解の導出結果

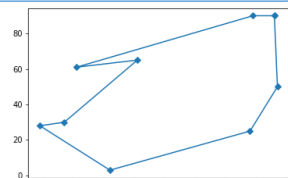
右図のようにに配置された9都市を、最も短い経路で1回ずつ回ることが出来るルート(厳密解)を**総当たり**で求めた。  
【総距離】263.9  
【計算時間】29.2秒



#### SA法によるシミュレーション

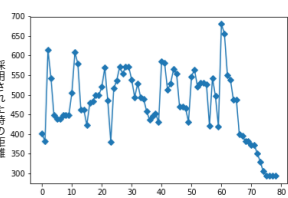
##### 最適解の導出結果

SA法を用いて最適解を求めた。  
【総距離】270.7  
【計算時間】7.4秒



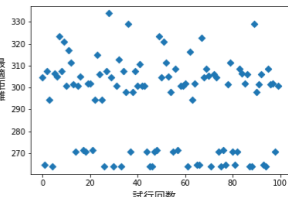
##### 最適解の導出過程

SA法ではどのようにして最適解を見つけ出していくのか、その過程を右の図に示した。試行回数が増えていくに従い、厳密解に近づいている。また、あるところでは、 $e^{-\frac{E_{t2}-E_{t1}}{k_B T}}$ の確率で長い距離を採用していることで、より最適解へと近づいていることがわかる。



##### 成功率

SA法を100回繰り返し、計算された最適解を右の図にプロットした。厳密解を求めた割合は**12%**であった。また、右図で最適解に近い距離(270以下)を求めた割合は**18%**であった。



#### QA法についての研究結果

「QA法のアルゴリズム」の中でも書いたように、QA法を古典コンピュータでシミュレートしようとすると、計算量が急激に増えてしまう。**(総当たり法を用いた場合よりも速く増加する!)**ただし、量子コンピュータでは、最適解に向かって自然に状態が変わっていく。そうなるように、自然法則に組み込まれているのである。量子力学がコンピュータのあり方どのように影響を与えるのか、QA法を一例として、確かめることができたと思う。

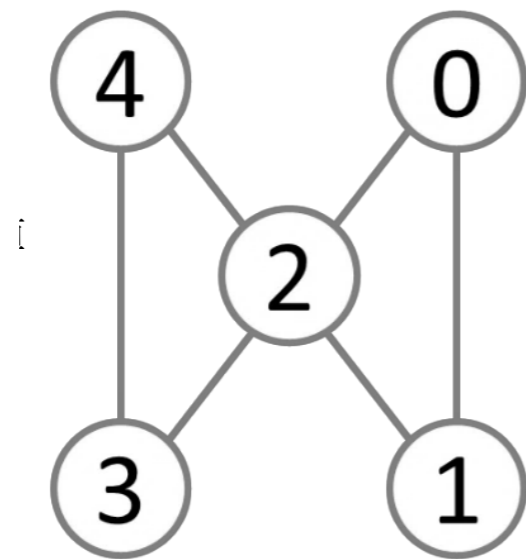
#### まとめ

SA法では、十分な時間計算させることにより、必ず厳密解に行き着くことがわかった。また、計算時間も、総当たりの方法に比べて短い。また、QA法については、古典コンピュータでシミュレートすることは極めて**非効率**である。量子力学を再現する、D-Waveマシンのようなデバイスがもっと精度をあげて開発されれば、実社会への応用も実現されるだろう。

#### 今後の発展の方向



# 2018年度の内容



player1's turn

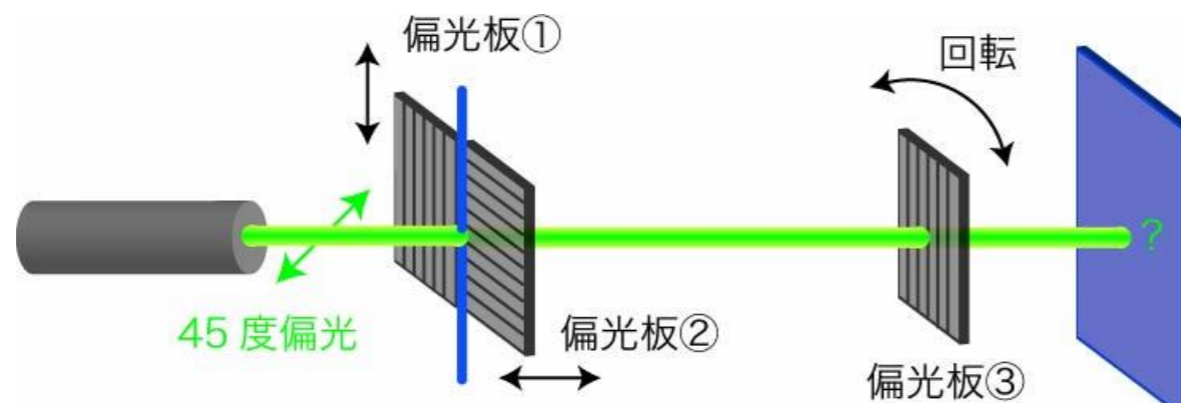
Press Enter to see the results for Player



> エンターキーを押してください

## Quantum Battleshipの実装

## IBM-Q で実演



## 量子消しゴムの実験



# 2019年度ポスター一発表

## 双峰祭(2019 11/3, 4)



### ざっくり量子コンピュータ

筑波大学理工学群物理学類3年 松本大輝



#### このポスターの概要

米グーグル、「量子超越性」達成と発表 スパコンを超える

右のようなニュースを目にして「量子コンピュータって結局なに？」と思った方、ぜひ立ちかこのポスターをご覧ください。量子コンピュータをざっくりと理解するための最低限の基礎知識の説明と、それをもとにした量子コンピュータのざっくりとした基本事項の解説がござい

10/24(木) 3:07配信  
https://headlines.yahoo.co.jp/hl?aq=20191024-35144382-cnn-int

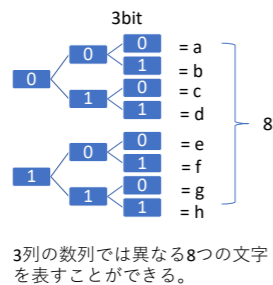


#### 1. 現在の情報技術の簡単なおさらい

まずは現在のコンピュータやスマートフォンがどのように「情報」をあつかっているか簡単におさらいしてみましょう。

#### コンピュータで「情報」はどのように表される？

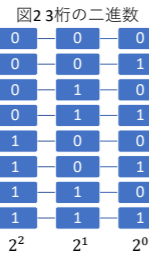
コンピュータ上では文字や数字などのすべての情報は0と1からなる数列で表されています。右の図のように一つの数列に文字を一つ対応させると、0と1だけでいろいろな文字を表現することができます。コンピュータ内では微視的な磁石や電圧の高低などで0と1を表現しています。このように「0か1か」を表すものをbitといいます。bitの数が多いほど多くのことを表せます。



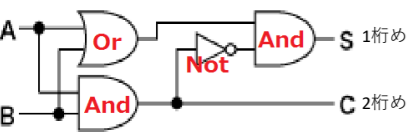
S N N = e  
N S S = e  
1 0 0 = e  
磁石をbitとし、S極が上向きするとき1、N極が上向きするとき0とすることで「100」を表現。

#### コンピュータはどのように計算を行っている？

今度は文字ではなく数をbit列で表してみよう。右の図のような数の表し方を二進法といいます。コンピュータ内で二進数の四則演算は、電気信号をbitとして二進数で数を表し「論理回路」というものを通して行われています。また、いくつかの基本的な論理回路を組み合わせることで任意の計算を行うことができます。ここでは、このように論理回路を用いて任意の計算を実行できるコンピュータを「汎用ゲート型コンピュータ」と呼ぶことにします。現在のコンピュータはこのタイプのもので、



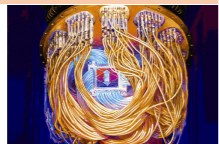
#### 一桁の足し算を行う回路



A,B:入力, S,C:出力  
And: 入力が両方とも1であれば0以外0を出力。  
Or: どちらか一方でも1であれば、両方とも0であれば0を出力  
Not: 入力信号を反対にして

#### 量子

量子コンピュータは現在のコンピュータよりも①高い計算能力を持ち②省エネルギーであることが期待されています。



↑Googleの量子コンピュータ

ゲート型 ←Googleの量子コンピュータはこっち！

#### 2. 量子力学

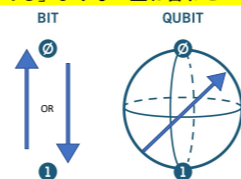
原子や電子などが活躍する非常に小さな世界では、私たちの直観に反するような現象が起こっています。量子力学はこうした微視的な世界での現象を説明し、という物理学の一分野です。「目に見えない世界を探索する」例として、放射線検定することでラドンを検出できる「ラドン検出器」の展示がこのポスターの隣にあります。その検出器では、じつは放射線が特定のエネルギーを持った粒のように測定されます。ぜひご覧になってください。ここでは量子力学において大切な「重ね合わせの原理」の解説をします。

#### 重ね合わせの原理

今までのbitは0か1のどちらかの状態に限られていました。しかし量子力学によれば量子力学的なbit(Qubitといいます)は「0であり1である」ような「重ね合わせの状態」をとることができます。  
→なんのこっちゃ?? (想定される反応)  
→偏光を題材にこのことを考えてみよう!

#### 光の基礎知識

光は進行方向に垂直な方向に振動する横波である。一定の方向にのみ振動する光を「偏った」光と呼ぶ。  
光は「光子」と呼ばれる粒子の集合である。bitは0と1の二通りの状態しかとれないけれど、Qubitは上の球上のどの状態もとることができます。なぜQubitがこのと



偏光板の実験 ←実験装置あります!!

### 量子暗号について

Yuta Hiemori, Haru Yoshida  
College of Physics, University of Tsukuba



量子暗号とは何か理解するために最低限必要であると思われる箇所にこのクローバーのマークを添えてあります。ポスターをお読みになる際の参考としていただければ幸いです。

#### 1. 暗号(Encryption)とは?

暗号: 第三者に内容を見られることなく情報を伝達するために用いられる手法, またそのアルゴリズム。

#### 用語の定義

- 平文 ⇔ 送りたい情報
- 暗号化 ⇔ 第三者に分からないように平文を変換すること
- 暗号鍵 ⇔ 暗号化に用いる特定の文字列 (アルゴリズムに用いるナニカ。基本的には送信者と受信者で共有)
- 暗号文 ⇔ 暗号化の施された平文
- 復号 ⇔ 暗号文を平文に直すこと

### 量子力学をもとにした、量子暗号解読体験



丸澤賢司

概要 去年授業の中でpythonというプログラミング言語を学んだので、それと今年の授業内のゼミで学んだ量子力学の知識をより量子暗号を理解できるようにゲームを作成しました。量子コンピュータがなぜ早急に興味があります

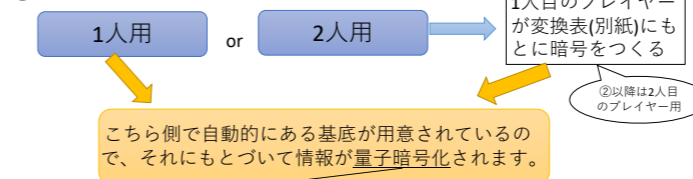
#### 量子暗号解読体験ゲームの遊び方

パソコン上で量子測定を表現できるような暗号解読ゲームを作成しました。1人用をプレイして暗号を解読し、それをもとに以下のクイズに正解された方には記念缶バッジ(限定50個)をプレゼントさせていただきます。ぜひ挑戦してみてください! 右の説明などを読むとより解きやすいと思います。2人用でも声をかけていただくとプレゼントできます。

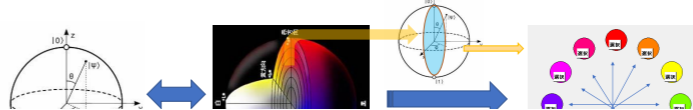
#### クイズ:暗号が示す、物理に関連がある年号は?

(一般の方にはなじみがないと思うので携帯で検索していただいて大丈夫です。〇〇 year of physics 量子で検索) →解けた方は金庫にその4ケタの数字を入れて解錠してください。

#### ①プレイモードを選ぶ



#### どんなふう?? → 量子状態を色で対応させて表現



#### ブロッホ球と測定

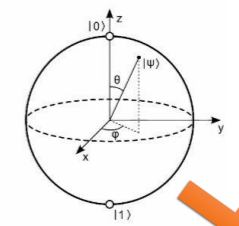
当然ですがあらゆる物体は観測を経て初めて状態が分かります。身近なことでは、私たちはそこにボールがあることを見ることで測定し、認識しています。物理における測定とは、もう少し踏み込んで何かしらの物理量のことです。(物理量とは位置や温度、回転速度等の注目する物理現象を解するのに必要な数値で表された何かの尺度のこと)



量子力学の主張を大雑把に説明するとすれば、「測定の前までは対象の物理量は確定していません。ただ〇〇という値が出やすいという確率的に出やすい物理量が決まっているだけ」である。測定しては測定対象の物理量が決定される。」というようになります。

まるでサイコロみたいですね。あのアインシュタインも「神はサイコロを振らない」というこの不思議な理論について慎重に思考をめぐらせた。

ここで、物理量を測定したい対象である、なんらかの量子状態 $|\psi\rangle$ を考えます。(抽象的ですが、ここではケットベクトルといいますがあまり気にしなくても大丈夫です。) この量子状態に、「あなたは $|0\rangle$ ですか $|1\rangle$ ですか」と聞くような測定を行うと、どちらかの状態にある確率でいきます。(この測定に使う量子状態は、簡単のために直交しているペアを選ぶとします。交している状態とは、矢印の上向きと下向き等全く逆の状態というイメージです。) この確率を視覚的にわかりやすくしてくれるものとしてブロッホ球が便利です。



ブロッホ球

ブロッホ球の球面上の点は任意の量子状態を表します。実際に指定するときは、地球上の緯度経度を指定すれば、一つの場所が定まるように感じて、 $\theta$ と $\phi$ (角度)で指定します。

端的に言えば、量子状態 $|\psi\rangle$ は測定に使用している2つの状態のうち、より近いほうに傾いていきます。(確率的に支配されている速いほうが出る時もあります)

この図だと $|\psi\rangle$ を $|0\rangle$ と $|1\rangle$ で測定したら $|0\rangle$ がやすい!

#### 3. 量子力学における測定(Measurement)

#### 測定(Measurement):

量子力学を述べる上で欠かすことのできない重要な概念。量子暗号においてもこの特性が重要な結果をもたらす



P.A.M Dirac

「測定された系はある1つの固有状態に確率的に飛び移る」

P.A.M Dirac  
Stern-Gerlach の実験



#### 量子力学の数学的基礎②(とばしても大丈夫)

実験事実として、「注目している量子状態を観測したとき、どの確率で状態が変化していくかを計算したいときは、その量子状態と観測量子状態の内積の絶対値の2乗を計算すれば良い」ということが確かである。ゲーム内ではこれにもとづいて確率が計算されています。

例  $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$  が測定後に $|0\rangle$ になる確率  

$$|(0|\psi\rangle|^2 = |(0|\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|^2 = |\frac{1}{\sqrt{2}}(0|0\rangle + \frac{1}{\sqrt{2}}(0|1\rangle|^2$$

$$|0\rangle, |1\rangleは正規直交基底であるから、自分自身との内積は1になるので$$

$$= |\frac{1}{\sqrt{2}} + 0|^2 = \frac{1}{2}$$

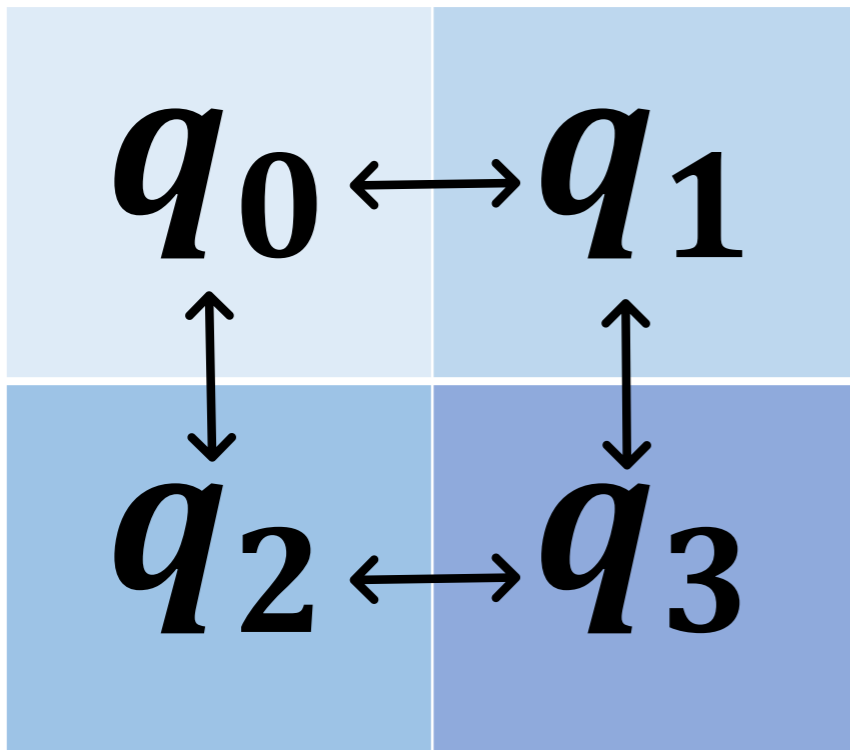
...ドウウコト?

#### ブロッホ球の数学的説明

(2)式を書き換える。まずa,bを以下のように極座標表示にする。

# 2021年度の内容

## Grover のアルゴリズムで数独パズルを解く



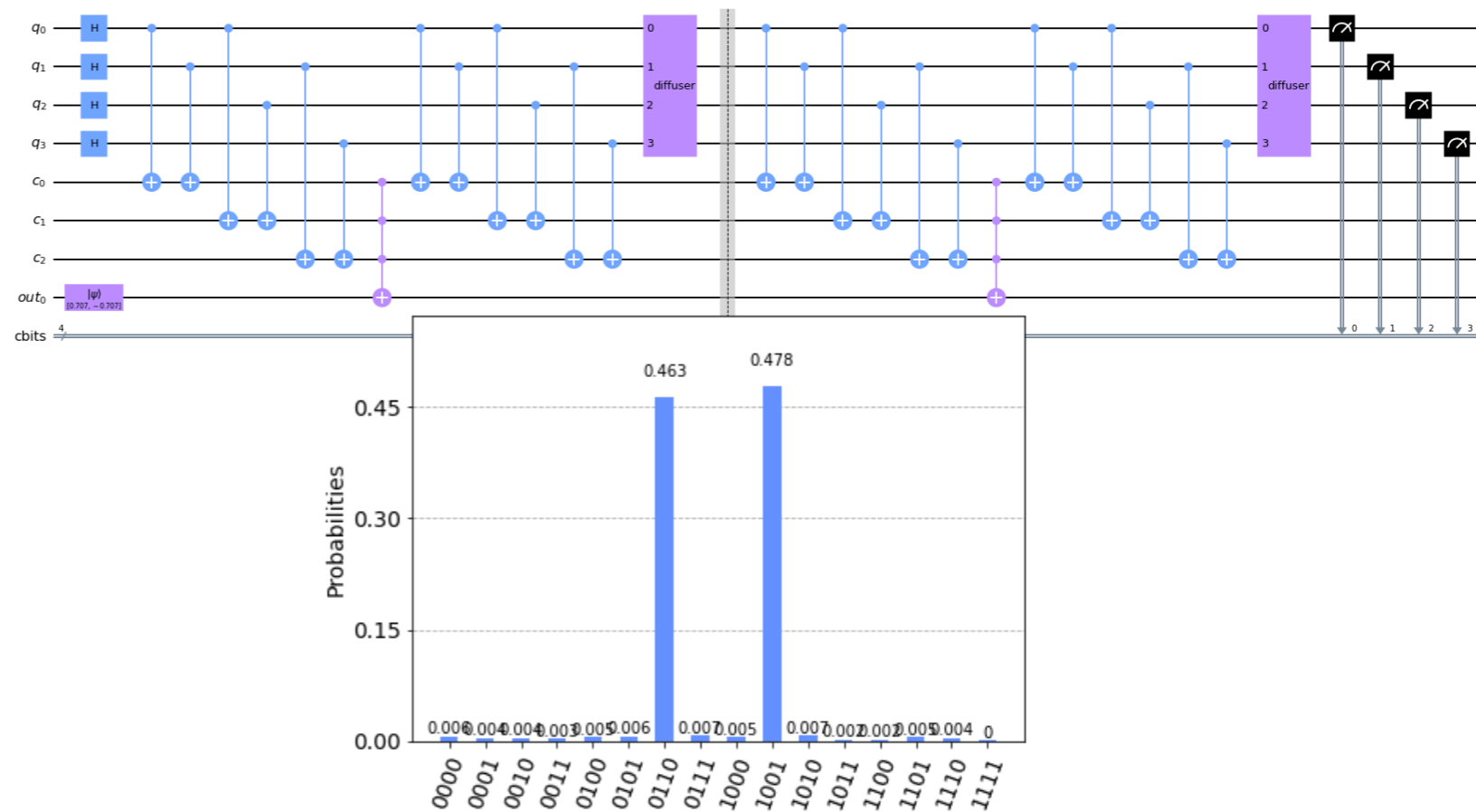
盤面に対応する量子状態

$|q_0 q_1 q_2 q_3\rangle$  (4qbit)

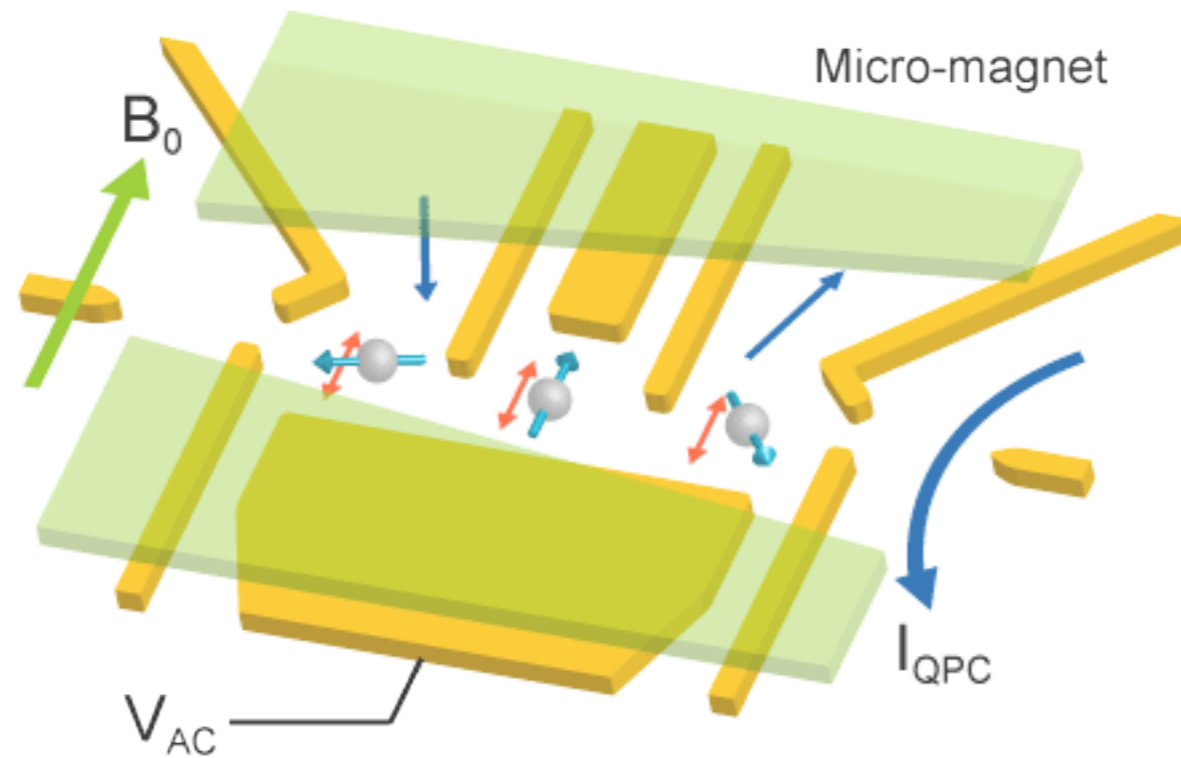
$q \in \{0, 1\}$

0	0	1	1	1	0
0	1	0	1	0	1

## IBM-Q シミュレーターで計算



# 以上です



連絡先：都倉 [tokura.yasuhiro.ft@u.tsukuba.ac.jp](mailto:tokura.yasuhiro.ft@u.tsukuba.ac.jp)

講義のweb page:

<http://www.u.tsukuba.ac.jp/~tokura.yasuhiro.ft/Lectures/Katan-2022.html>

内容に関して疑問があれば、いつでも  
気楽に連絡してください。