量子情報社会の可能性を探る

山本 喜久
国立情報学研究所、スタンフォード大学

NIIオープンハウス基調講演（学術総合センター）
平成20年6月5日

- 量子情報技術が作り出す未来社会
- ウォーミングアップ： 量子と古典の世界の違い
- 量子情報科学技術:コンセプト、背景、ロードマップ
- 量子暗号・量子通信
- 量子テレポーテーション・量子中継
- 量子標準・量子精密計測
- 量子シミュレーション
- 量子コンピュータ

量子情報技術が作り出す未来社会

- 非常に複雑な問題を処理できる能力を持つコンピュータ、シミュレータの開発

気象現象　生命現象　経済活動　トラヒック制御　新材料/物理現象

→ 量子コンピュータ
量子シミュレータ

- 個人情報・プライバシーが保護されている安全な通信網の開発

電子商取引　電子投票　暗号通信

→ 量子鍵配送
量子テレポーテーション
量子中継
量子通信

- 高精度な時間標準や精密計測技術の開発

ブロードバンド通信網
GPS (Global Positioning System)
磁力計、ジャイロスコープ

→ 量子標準
量子精密計測

3

量子の世界の不思議 ―線形重ね合わせ原理と量子-古典の境界―

ミクロな量子の世界では、１つの粒子は２つの相反する状態に同時に存在できる。これを線形重ね合わせの原理という。

位置A　位置B

$$|\psi\rangle = A|r_A\rangle + B|r_B\rangle \quad \text{(量子ビット)}$$

$|\psi\rangle$：粒子の状態　A：位置Aにいる確率振幅　B：位置Bにいる確率振幅

我々が日常体験しているマクロな古典の世界では、このような線形重ね合わせ状態は存在しない。

$$|\Phi\rangle \neq A|\text{猫}_{\text{生}}\rangle + B|\text{猫}_{\text{死}}\rangle$$

$|\Phi\rangle$：猫の状態　$|\text{猫}_{\text{生}}\rangle$：生きている猫の状態　$|\text{猫}_{\text{死}}\rangle$：死んでいる猫の状態

→ 一匹の猫が同時に生きている状態と死んでいる状態にまたがって存在する、のは明らかにナンセンスだ。
(シュレディンガー)

4

量子の世界の豊かさ ―ヒルベルト空間―

- １つの粒子は２つの相反する状態（情報）を同時に表すことができる。

$|r_A\rangle$、$|r_B\rangle$

- 別のもう１つの粒子をこれに組み合わせると、２つの粒子で同時に表すことができる状態は、$|r_A\rangle_1|r_A\rangle_2$、$|r_A\rangle_1|r_B\rangle_2$、$|r_B\rangle_1|r_A\rangle_2$、$|r_B\rangle_1|r_B\rangle_2$ の４通りになる。
- N個の粒子が全体として同時に表すことのできる状態（情報）の数は、

$2\times 2\times \cdots\cdots \times 2 = 2^N$
（粒子1の自由度　粒子2の自由度　粒子Nの自由度）

N	2^N
1	2
10	10^3
20	10^6
30	10^9
⋮	⋮
140	10^{42}

→ たった30個の二準位粒子は、世界の全人口に相当する異なった状態（情報）を同時に表すことができる！

→ たった140個の二準位粒子は、地球を構成する全ての原子の数に相当する異なった状態（情報）を同時に表すことができる！！

5

古典計算と量子計算の違い

古典計算： 2^N個の可能な入力値のうちの１つの入力値に対して計算が終了したのち、次の入力値に対して計算が行われ、これを2^N回繰り返さなければならない。

入力x ●→●→●→●→……→● 出力y

量子計算： 2^Nの異なった入力に対して計算が同時に行われるので、たった１回の計算で答えが得られる。

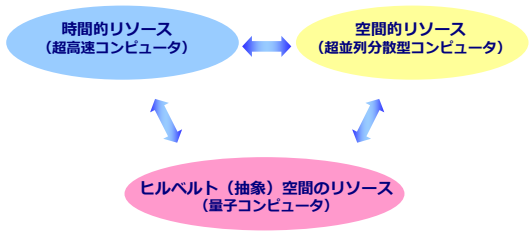
入力x_1 ○→○→○→○→……→○ 出力y_1
入力x_2 ○→○→○→○→……→○ 出力y_2
⋮
入力x_{2^n} ○→○→○→○→……→○ 出力y_{2^n}

古典ビットへ加工

量子パラレリズム（David Deutsch, 1985）

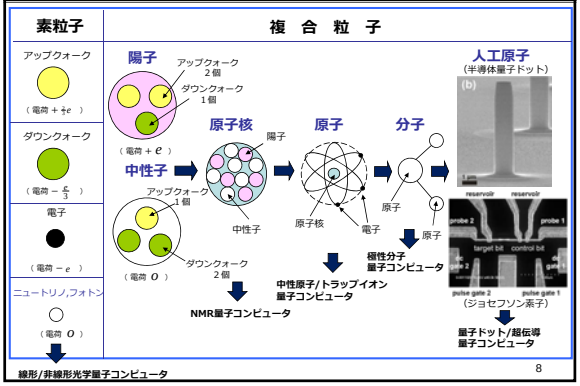
6

コンピュータに使えるリソース



7

量子ビットとして使える2準位粒子？

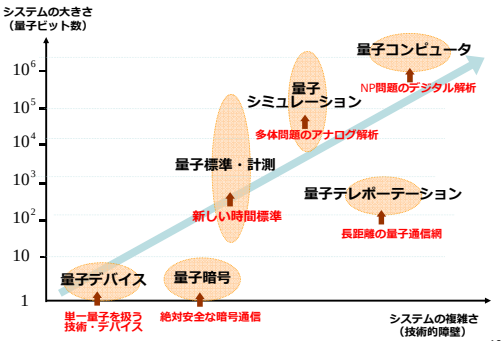


8

量子情報技術を形成した2つの学問的潮流

9

量子情報技術ロードマップ



10

量子暗号

―絶対に盗聴不可能な秘密鍵を作る ―

- プロトコルの発明
- 安全性の数学的証明
- システム実験

暗号の歴史

Kryptos (hidden) + logos (word)

- 紀元前400年スパルタ → Scytale (transposition)

- 紀元前50年ローマ帝国 (substitution) → Caesar Cipher
  A→D
  B→E
  COLD→FROG
- 1940's ドイツ → ENIGMA ciphers
  ⇩
  英国チーム(Alan Turing)により解読 ⇨ Bomba

暗号解読は、計算機科学の助産婦である。

12

暗号通信のしくみ

テキスト

$E_k(P) = C$ ⟶ $D_k(C) = P$

暗号アルゴリズム　秘密鍵　暗号文　解読アルゴリズム

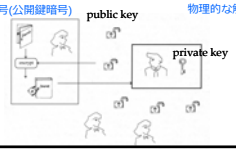
One-time pad: (Gilbert Verman : 1917)

	A	B	C	D	E	…	…	X	Y	Z	?	,	.
	00	01	02	03	04	…	…	23	24	25	26	27	28	29
	S	H	A	K	E	N		N	O	T		S	T	I	R	R	E	D
テキスト	18	07	00	10	04	13	26	13	14	19	26	18	19	08	17	17	04	03
鍵 k	15	04	28	13	14	06	21	11	23	18	09	11	14	01	19	05	22	07
$C = P + k \pmod{30}$	03	11	28	23	18	19	17	24	07	07	05	29	03	09	06	22	26	10

Claud Shannon:
もし、鍵が完全にランダムでテキストと同じ長さを持ち、一回だけしか使われなければ、one-time pad暗号通信は絶対に安全である。

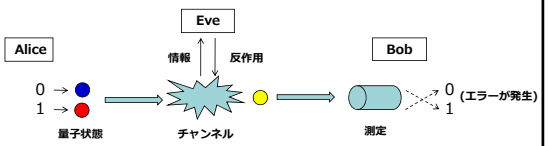
どのようにして、鍵を配送するか？

数学的な解： 古典暗号(公開鍵暗号)　物理的な解： 量子暗号(量子鍵配送)



量子鍵配送の原理

量子状態は、それに対して測定が行われると、その測定結果で決められる別の量子状態へジャンプする（波束の収縮： von Neumannの原理）。



ビット列の一部を公開し合ってエラーレートを計算する。
安全だと判定されれば次のステップへ進む。

0100101 ⟶ 0100111 シフト鍵

誤り訂正

0100101 ⟶ 0100101

プライバシー増幅

0101 ⟶ 0101 安全鍵

量子鍵配送の研究

理論

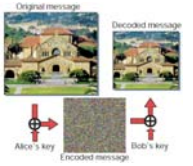
- BB84プロトコルの発見（Bennett & Brassard, 1984）　単一光子を用いる方式
- Ekert91プロトコルの発見　エンタングル光子対を用いる方式
  （Ekert, 1991; Bennett, Brassard & Mermin, 1992）
- BB84プロトコルの安全性証明（Mayers, 1996; Shor & Preskill, 2000）
- 差動位相シフト（DPS）プロトコルの発見　コヒーレント光を用いる方式
  （Inoue, Waks & Yamamoto, 2002）
- DPSプロトコルの安全性証明（Wen, Tamaki & Yamamoto, 2008）

実験

- 最初のBB84量子鍵配送実験
  （Bennett, Bessette, Brassard, Salvail & Smolim, 1992）
- 単一光子光源を用いたBB84量子鍵配送実験（Stanford team, 2002）
- 長距離（200km）量子鍵配送実験（NTT – NII – Stanford – NIST team, 2007）
- 高速（2Mbit/s @ 5km、1.6Mbit/s @ 10km）量子鍵配送実験
  （Toshiba – Cambridge team、NTT – NII –Hamamatsu- Stanford team, 2008）

量子鍵配送の実験

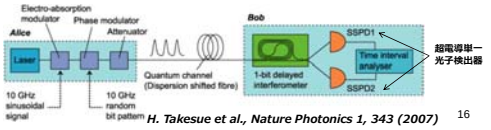
単一光子光源を用いたBB84量子鍵配送実験



E. Waks et al., Nature 420, 762 (2002)

半導体量子ドットをマイクロキャビティに閉じ込めた単一光子光源

長距離(200km)DPS量子鍵配送実験



H. Takesue et al., Nature Photonics 1, 343 (2007)

量子テレポーテーション・量子中継

―エンタングル状態を長距離間に形成する ―

- エンタングルメント配信
- エンタングルメント純粋化とスワッピング
- ハードウェア：　量子メモリ
  量子プロセッサー
  量子通信網へのインターフェース

エンタングル状態とは何か？

2粒子状態

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle_A|\downarrow\rangle_B - |\downarrow\rangle_A|\uparrow\rangle_B\right)$$

- 粒子Aと粒子Bは、相反する2つの状態に同時に存在する（線形重ね合わせ）
- 粒子Aが$|\uparrow\rangle$ $(|\downarrow\rangle)$ ならば粒子Bは $|\downarrow\rangle$ $(|\uparrow\rangle)$　（量子相関）

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|+\rangle_A|-\rangle_B - |-\rangle_A|+\rangle_B\right)$$

- 粒子Aと粒子Bは別の基底（測定量）に対しても同様の性質を持っている。

$$|\pm\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle \pm |\downarrow\rangle\right)$$

古典とのアナロジー
- 2匹の猫は生きている状態と死んでいる状態に同時にまたがって存在する。
- 猫Aが生(死)の状態ならば、猫Bは死(生)の状態にある。
- そうであるならば、猫Aがオス(メス)ならば、猫Bはメス(オス)である。
- 2匹の猫は1つの状態の一部なので分離することはできない。

量子中継の原理
ーエンタングル状態を長距離間に形成するため、量子状態をテレポートするー

エンタングル光子対

単一光子の到達確率： $P(L) = e^{-L/L_0}$ （L_0：吸収長）

成功までの平均繰り返し数： $n(L) = \frac{1}{P(L)} = e^{L/L_0}$ ⇨ 指数関数で増加 (L=500km → 10^{13}回) 2000年!!

分割

Bell-pair　Bell-pair　Bell-pair

ベル測定　ベル測定(量子テレポーテーション)

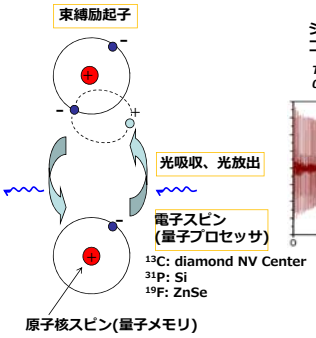
各セクションでの繰り返し数： e^{L/NL_0}

全繰り返し数： $n'(L) = Ne^{L/NL_0}$ ⟶ $n'(L) = e\frac{L}{L_0}$

if $N = \frac{L}{L_0}$ ⇨ 線形関数で増加(L=500km⟶ 90回)
パラレル動作可能 $\frac{1}{100}$秒!!

19

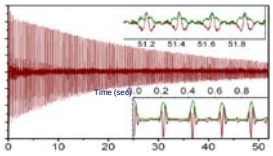
半導体中のドナー不純物：
原子核スピン、電子スピン、束縛励起子



^{13}C: diamond NV Center
^{31}P: Si
^{19}F: ZnSe

シリコン結晶中の原子核スピンの
コヒーレンス時間（T_2=1 min）

T. Ladd et al., Phys. Rev. B. 71, 014401 (2005)



20

量子標準・計測
-光時計を作る-

- 原子分光
- 光周波数の絶対測定
- 標準量子限界を克服する非古典原子分光

原子時計：光時計 対 マイクロ波時計

秒の精度： $\frac{\Delta\nu}{\nu_0} = \frac{\delta\nu}{\nu_0}\frac{1}{\sqrt{N_{\mathrm{atom}}T}}$

（発光線幅／遷移周波数／原子数 x 測定時間）

- 単一トラップ・イオン
  - ☺ 狭い線幅、長い測定時間
  - ☹ 単一の原子
- 原子ボーズ凝縮体
  - ☺ 多数の原子
  - ☹ 広い線幅、短い測定時間
- 光格子モット絶縁体
  - ☺ 狭い線幅、長い測定時間、多数の原子
  - ☹ 遷移周波数のシフト

⇩

マジック波長 ***(M. Takamoto et al., Nature 435, 321 (2005))***

⇩

$\sigma_y(\tau) \sim 10^{-17}/\sqrt{\tau}.$

22

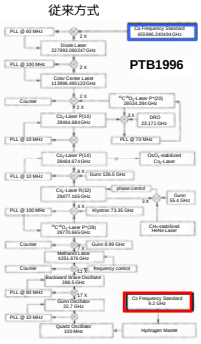
原子分光へ与えられたノーベル賞

1902	Pieter Zeeman and Hendrik A. Lorentz (Zeeman Splitting)	**1964**	Charles H. Towns, Nikolai G. Basov and Aleksandr M. Prokhorov (laser)
1904	John W. Strutt (argon, Rayleigh scattering)	**1966**	Alfred Kastler (optical pumping)
1919	Johannes Stark (Stark splitting)	**1971**	George Herzberg (Chemistry) (molecular spectroscopy)
1921	Albert Einstein (photoelectric)	**1977**	John Van Vleck (electric and magnetic susceptibility)
1922	Niels Bohr (atomic structure)	**1981**	Nicolas Bloembergen and Arthur Schawlow (laser spectroscopy)
1925	James Frank (experimental study on Bohr's atomic model)	**1989**	Norman F. Ramsey, Hans G. Dehmelt and Wolfgang Paul (single electron & ion spectroscopy)
1930	Sir Chandrasekhara Raman (Raman spectroscopy)	**1997**	Steven Chu, Clude Cohen-Tannoudji and William D. Phillips (laser cooling)
1944	Isidor Rabi (NMR with atomic beam)	**2001**	Eric A. Cornell, Wolfgang Ketterle and Carl E. Wieman (BEC)
1952	Edward M. Purcell, Felix Bloch (NMR, intersteller hydrogen emission)	**2005**	John Hall and Theodor W. Hänsch (optical frequency measurement) R.Glauber (quantum coherence)
1955	Willis Lamb, Jr. (Lamb shift)		

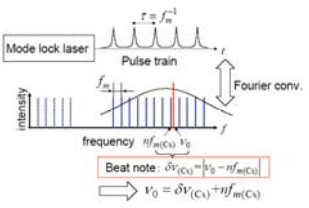
23

光周波数の絶対測定

従来方式



モード同期レーザと非線形光ファイバー
(2005 Nobel Prize of Physics)



24

量子シミュレーション

- 多体系の複雑な振舞いを模擬実験で解明する -

- ボーズハバードモデル
- フェルミハバードモデル（高温超伝導体）
- スピンモデル（磁性）

光格子、イオントラップ、ジョセフソン接合、
半導体(2次元電子ガス、励起子ポラリトンガス)

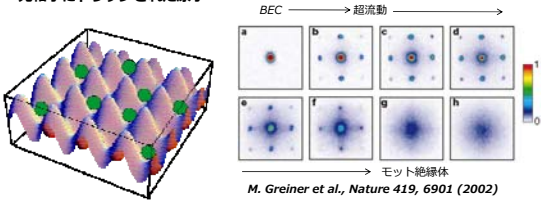
光格子中の原子で観測された超流動 – モット絶縁体相転移

ボーズハバードモデル

$$\hat{H} = \sum_j \epsilon_j \hat{n}_j - J \sum_{i,j} \hat{b}_i^\dagger \hat{b}_j + \frac{U}{2} \sum_j \hat{n}_j(\hat{n}_j - 1)$$

M.P.A. Fisher et al., PRB 40, 546 (1989)
D. Jaksch et al., PRL 81, 3108 (1998)

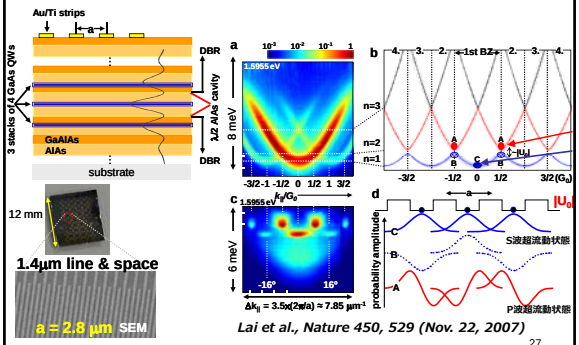
光格子にトラップされた原子



M. Greiner et al., Nature 419, 6901 (2002)

26

励起子ポラリトンで観測された2つの超流動状態の競合



Lai et al., Nature 450, 529 (Nov. 22, 2007)

27

量子コンピュータ

– ヒルベルト空間の豊かさを計算機リソースとして使う –

- 量子アルゴリズム
- 量子計算モデル
- ハードウェア

(イオントラップ、ジョセフソン素子、量子ドット、
光格子、NMR、cavity QED)

量子アルゴリズム

- **量子フーリエ変換**
  - Deutsch (1985), Deutsch-Jozsa (1992) ⇨ 量子パラレリズム
  - Simon (1994) ⇨ 周期計測
  - Shor (1994) ⇨ 因数分解、離散対数
  - Cleve et al. (1998) ⇨ 位相推定
  - Kitaev (1995) ⇨ アベーリアン・グループ
  - Abrams and Lloyd (1999) ⇨ 固有値、固有ベクトル測定
- **量子振幅増幅**
  - Grover (1997) ⇨ データベース検索
- **量子ランダムウォーク**
  - Childs et al. (1992) ⇨ データベース検索
- **量子統計（集団）**
  - Knill and Laflamme (1998) ⇨ 固有値、固有ベクトル測定

29

量子計算モデル – 量子アルゴリズムをどう実現するか？ –

- **ユニタリゲートを並べる方法**
  A. Barenco et al., PRA 52, 3457 (1995)
- **量子測定によりユニタリ変換を実現する方法**
  R. Raussendorf and H. J. Briegel, PRL 86, 5188 (2001)
- **系のハミルトニアンをゆっくりと変化させる方法**
  E. Farhi et al., Science 292, 472 (2001)
- **量子アニール（BEC）を用いる方法**

閉鎖系(より理論的アプローチ)

開放系(より実験的アプローチ)

30

結　論

Take home message

量子暗号、量子中継、量子テレポーテーションは、測定による波束の収縮を用いて
通信における安全性や新機能を実現している。量子コンピュータ、量子シミュレータは、
重ね合わせ原理を用いて計算の超並列化を実現している。

技術的困難さ

重ね合わせ状態は壊れやすい
（量子情報は外部へリークし易い）。 → シュレディンガーの猫のパラドクス

夜明け前

量子暗号、量子標準、量子シミュレーションは実用技術として使われるフェーズに
近づいている。量子コンピュータ、量子中継を実現しうる実用的手段はまだ
見つかっていない。

２１世紀の科学技術を支える知識と技術

単一の光子、電子、原子、分子の量子状態を人工的に制御する原理と実験技術。
あるいは、それらの集合体が自然に形成する秩序状態の利用技術。
実現すれば、現代科学を支える量子論の最初の直接的応用。

31