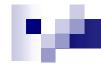
NMR量子コンピュータ

近畿大学理工学部 中原 幹夫



講演予定

- 1. はじめに:物理で計算?
- 2. 量子ビット, 量子ゲート, 量子コンピュータ
- 3. DiVincenzoの判定条件
- 4. NMR量子コンピュータ
- 5. 例: Shorのアルゴリズム
- 6. おわりに



1. はじめに:物理で計算?

tの2乗は落下物の落下距離Lを測れば求められる:

$$L = \frac{1}{2}gt^2.$$

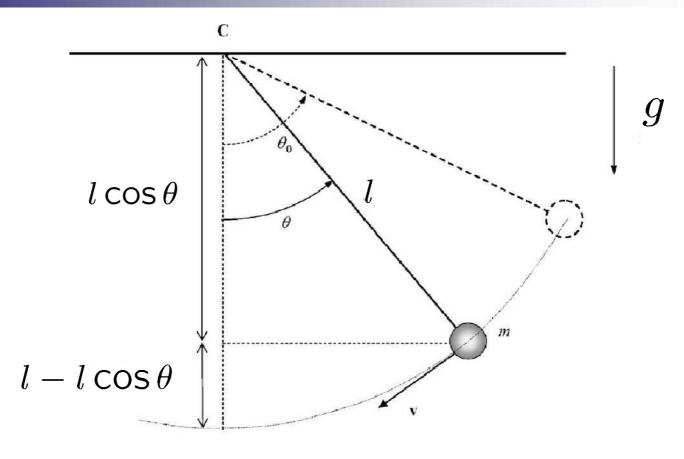
lの平方根は振り子の微小振動の周期を測れば求められる:

$$T = 2\pi \sqrt{\frac{l}{g}}.$$

 $l=g/4\sim 2.45$ mにとるとTの測定で π が「計算」できる.

振幅が増えればもっと複雑な「計算」ができる:





$$T = 4\sqrt{\frac{l}{g}} \int_0^{\pi/2} \frac{1}{\sqrt{1 - k^2 \sin^2 \phi}} d\phi = 4\sqrt{\frac{l}{g}} K(k),$$

ただし $k = \sin(\theta_0/2)$. K(k) は第1種完全楕円積分.



量子情報,量子コンピューティングとは

- 量子コンピューティング,量子情報処理では情報を記憶し,処理するのに量子系を資源として用いる.
- 古典的に存在しない状態や操作を使うと古典コンピューティング, 古典情報処理をはるかに超える演算, 処理ができる. (超並列計算による計算の指数関数的なスピードアップ, 絶対安全な暗号システム, 量子テレポーテーションなど)



講演予定

- 1. はじめに:物理で計算?
- 2. 量子ビット, 量子ゲート, 量子コンピュータ
- 3. DiVincenzoの判定条件
- 4. NMR量子コンピュータ
- 5. 例: Shorのアルゴリズム
- 6. おわりに



2.1 量子ビット

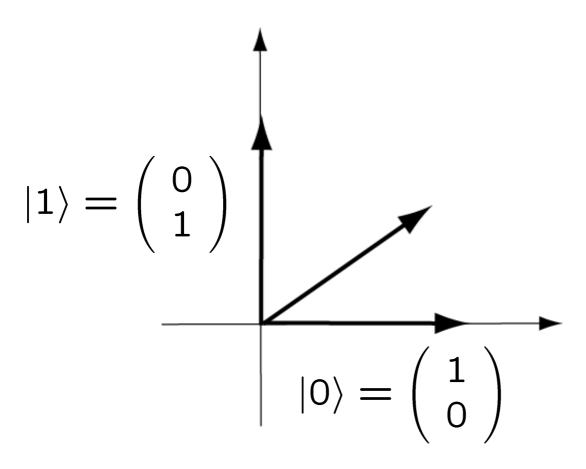
- 古典情報は {0,1} に値をとるビットを情報の単位とする.
- 量子情報は2次元複素ベクトル空間 C² の単位ベクトル「量子ビット」を情報の単位とする。

$$|\psi\rangle = a|0\rangle + b|1\rangle$$
, $a, b \in \mathbb{C}$, $|a|^2 + |b|^2 = 1$, 基底 (基本) ベクトル $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. $|0\rangle \leftrightarrow 0$, $|1\rangle \leftrightarrow 1$ と対応させる.

• ただし $|\psi\rangle$ と $e^{i\alpha}|\psi\rangle$ は区別できない.



量子ビット |Ψ



$$|\psi\rangle = a|0\rangle + b|1\rangle$$
$$a, b \in \mathbb{C}$$
$$|a|^2 + |b|^2 = 1$$

$$|\psi\rangle$$
は $|0\rangle$ と同時に $|1\rangle$ でもある; $a|0\rangle$ と $b|1\rangle$ の **重ね合わせ状態**



2.2 2量子ビット系ともつれた状態

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \ |01\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$|10\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \ |11\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

EPR対(エンタングルした状態)

物理学で最も賞味期間長い論文は?

アインシュタインが発表 71年前の「量子力学批判」

の記述を完全と考えるこ

た「量子力学による自然

ングルメント)」と呼ばれ か「量子もつれ(エンタ という、「非局所性」と できず相関関係を持つ」 ら遠く離れていても分離 力学に従うものは、 つに選んでいる。 の論文を「今、 ある。レドナー たが、95年ごろから急増 はあまり引用されなかっ 6年もあった。発表直後 る。この賞味期間は59・ 者
る
人
の
頭
文
字
を
取っ
て 35年に発表した。 共著 とができるか?」は、 トな論文トップ10」の一 インシュタインらが19 「EPR論文」と呼ばれ EPR論文は、 最近は年8件程度も 「量子 5

文だという人もいる。今 とがわかった。 の「量子コンピュータ 能な量子暗号や、超高速 この性質から盗聴が不可 られていなかったが、 験で検証できるとは考え 後、影響はさらに大きく 大きかったのはEPR論 論文の中で、最も影響が は「アインシュタインの 究機構の筒井泉・助教授 際に確かめられ、さらに 高エネルギー加速器研 への道が開かれるこ 「非局所性」が実

参加者を、科学技術振興



2.2 多量子ビット系ともつれた状態 (n>2)

- n量子ビット系の一般の状態:
- $|\Psi\rangle = a_{0...00}|0...00\rangle + a_{0...01}|0...01\rangle + ... + a_{1...11}|1...11\rangle$. n量子ビット系の次元 = $a_{i_1...i_n}$ の数 = 2^n ,
- テンソル積 $(a_1|0\rangle + b_1|1\rangle)\otimes ...\otimes (a_n|0\rangle + b_n|1\rangle)$ は古典的記述を許す.

テンソル積状態の次元= a_i, b_i の数=2n.

- n = 1000で $2n/2^n \sim 10^{-297} \rightarrow n$ が大きいときはほとんどすべての状態がもつれている.
- 基底ベクトル $|i_{n-1}i_{n-2}...i_0\rangle$ を $|x\rangle$ と書くときもある. ただし $x=i_{n-1}2^{n-1}+i_{n-2}2^{n-2}+...+i_0$, 例: $|00\rangle=|0\rangle, |01\rangle=|1\rangle, |10\rangle=|2\rangle, |11\rangle=|3\rangle$



2.3 量子アルゴリズム = ユニタリー行列

情報はベクトルが担う. その操作(ゲート) はユニタリー 行列(ベクトルの長さを不変にする行列)で行なう.

例:
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
とおくと

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

同様に $X|1\rangle = |0\rangle \rightarrow X = NOT$.

Xは、重ねあわせ状態 $a|0\rangle + b|1\rangle$ にも作用する:

$$X(a|0\rangle + b|1\rangle) = a|1\rangle + b|0\rangle.$$

$$2^{n}-1$$
 $2^{n}-1$

一般に:
$$U_f \sum_{x=0} |x\rangle|0\rangle = \sum_{x=0} |x\rangle|f(x)\rangle.$$

 2^n 個のプロセッサーの超並列処理!



n 量子ビットの操作

● 「古典」的:

 $U_1 \otimes U_2 \otimes \ldots \otimes U_n : |\psi_1\rangle \otimes |\psi_2\rangle \ldots \otimes |\psi_n\rangle \mapsto U_1 |\psi_1\rangle \otimes U_2 |\psi_2\rangle \ldots \otimes U_n |\psi_n\rangle$, U_k は2×2ユニタリー行列.

• n量子ビット系では $2^n \times 2^n$ ユニタリー行列をフルに使うことができる。自由度(操作できるパラメタの数)の比較: $2^{2n} \gg 4n$

ほとんどの操作は古典的な対応物を持たない.

線形代数 (ベクトルと行列) を使えば古典計算を超える計算と情報処理ができることがわかった. ではどんな物理系を使えばこれを実現できるか?



量子力学

H₁ H₂ ··· H₂ Newton の運動方程式

質量·加速度一力
$$m\frac{d^2\vec{x}}{dt^2} = \vec{F}$$

$$|\Psi(0)\rangle |\Psi(t_1)\rangle |\Psi(t_2)\rangle \cdots$$

$$|\Psi(T=t_n)\rangle$$

$$U(T) = \lim_{n \to \infty} e^{-iH_n(T - t_{n-1})} \dots e^{-iH_2(t_2 - t_1)} e^{-iH_1t_1}$$



講演予定

- 1. はじめに:物理で計算?
- 2. 量子ビット, 量子ゲート, 量子コンピュータ
- 3. DiVincenzoの判定条件
- 4. NMR量子コンピュータ
- 5. 例: Shorのアルゴリズム
- **■** 6. おわりに



正しく動くパソコンの必要条件

- ハードウエァ (メモリー, CPU)がそろっているか
- 最初にメモリーをリセットできるか
- 計算が終了するまでにパソコンが壊れないか (10年かかる計算では危うい)
- ■どんな論理回路でも構成できるか
- 計算結果をプリンターやディスプレイに出力できるか

ある物理系が量子コンピュータの候補と なるための必要条件 (DiVincenzo条件)

- 卅分な数の量 矛ゼリナを開意) あきるか ているか
- 最初にの量子を小を基準の状態にセットできるか (たとえば|00…00 など)
- 計算が終了するまで星飛状態/あっていいのはの神戸がまた。 (400神戸がまた) (400神戸がまた) (400神戸がまた) (400神戸がまた)
- どんな
 翻理
 図路
 で
 を
 精動で
 きる
 ふか
- 計算結果を読み取るでもずできるか に出力できるか



万能定理

定理(Barenco たち)

任意の $U \in U(2^n)$ は1-qubitゲートとCNOTゲート に分解できる. すなわちU(2)とCNOTゲートはユニ バーサルである. (基本量子ゲート)

input output

第1量子ビットが $|0\rangle$ であれば第2量子ビットはそのまま,第1量子ビットが $|1\rangle$ であれば第2量子ビットを反転.

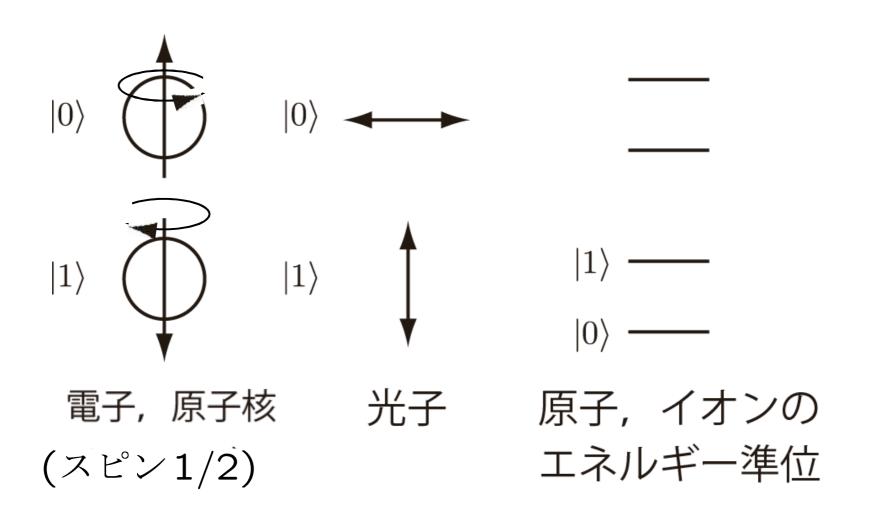
м

DiVincenzo 2004@近畿大学



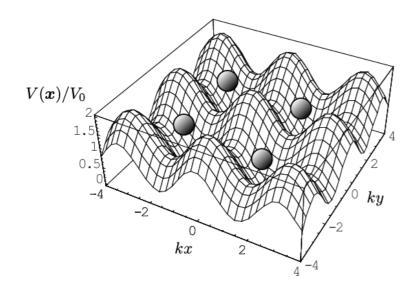


物理系の候補:





量子ビットの候補として提唱されている量子系



$$\begin{array}{c|c}
\mathbf{F} & \mathbf{F} \\
\mathbf{F} & \mathbf{C} = \mathbf{C} \\
\mathbf{F} & \mathbf{C} = \mathbf{C} \\
\mathbf{F} & \mathbf{F} \\
\mathbf{C}_{5} \\
\mathbf{H}_{5} & (\mathbf{CO})_{2}
\end{array}$$

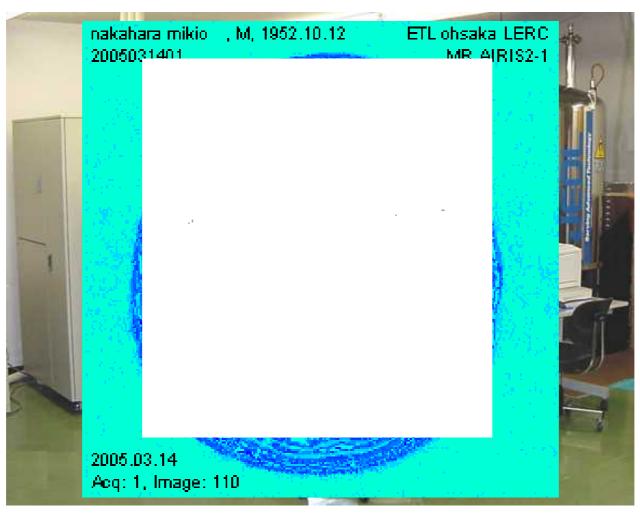


講演予定

- 1. はじめに:物理で計算?
- 2. 量子ビット, 量子ゲート, 量子コンピュータ
- 3. DiVincenzoの判定条件
- 4. NMR量子コンピュータ
- 5. 例: Shorのアルゴリズム
- **■** 6. おわりに

Ŋ.

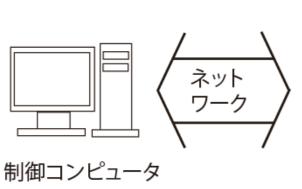
NMR (Nuclear Magnetic Resonance 核磁気共鳴) = MRI (Magnetic Resonance Imaging 磁気共鳴像)



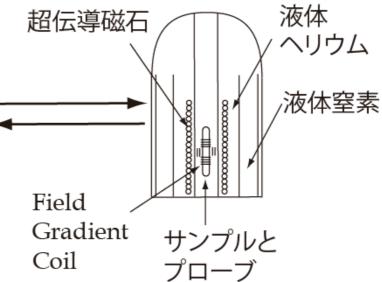
NMR装置





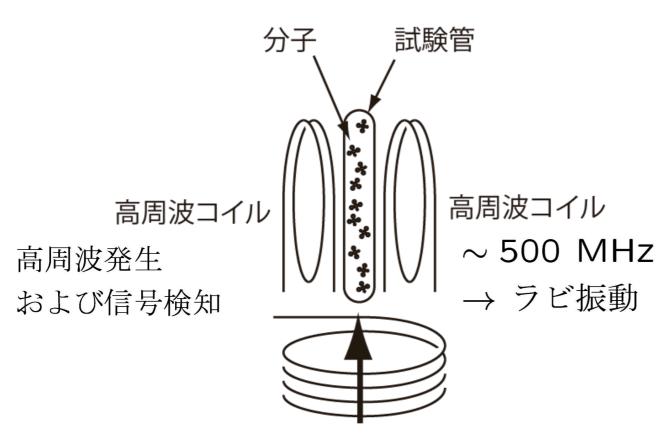


Spectrometer control
(Control computer,
Acquisition processor,
Sequencer, IF frequency
oscillator)
RF Transmitter
RF Receiver
Power supply
Power amplifier





NMRの概念図



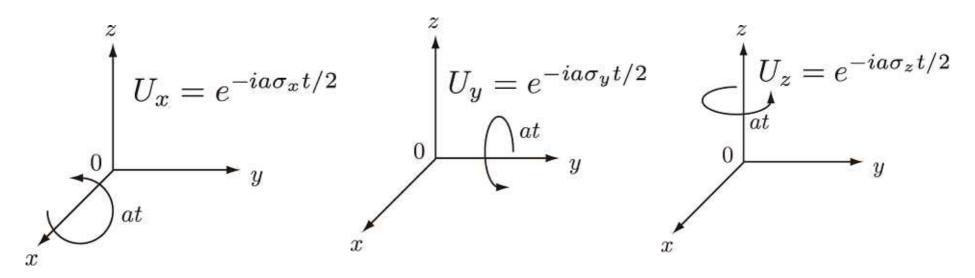
巨力な静磁場 $B_0 \sim 10$ T \sim 地球磁場の 20 万倍.

→ 核スピンの準位分裂(ゼーマン効果)



量子ビット操作の基本

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
はそれぞれスピンの x, y, z 軸周りの回転を生成する.



$$|0\rangle \to U_x(at)|0\rangle = \cos\frac{at}{2}|0\rangle + i\sin\frac{at}{2}|1\rangle$$
; 重ねあわせ状態!



$$|\psi\rangle = \cos\frac{\alpha}{2}|0\rangle + i\sin\frac{\alpha}{2}|1\rangle$$

$$|\psi\rangle = \cos\frac{\alpha}{2}|0\rangle + i\sin\frac{\alpha}{2}|1\rangle$$

$$i\sin\frac{\alpha}{2}|1\rangle$$

$$U_x(\alpha) = e^{-i\alpha\sigma_x/2}$$

$$= e^{-ia\sigma_x t/2}$$

 $\alpha = at$ すなわち t を変えればいろいろな重ねあわせ状態を実現できる.



しかし...

- $\sigma_x, \sigma_y, \sigma_z$ を変えることは静磁場の向きを変えることに等しい.
- 超伝導磁石は1t程度の質量で、これを瞬時に動かす ことは実用的ではない.
 - → 高周波で振動する微小磁場を使った Rabi 振動を 利用する.
- まず古典的なアナロジーを調べよう.



磁場中のスピン: 古典的描像1

磁場中の磁気モーメントの運動方程式 ; $\frac{d\vec{\mu}}{dt} = \gamma \vec{\mu} \times \vec{B}$

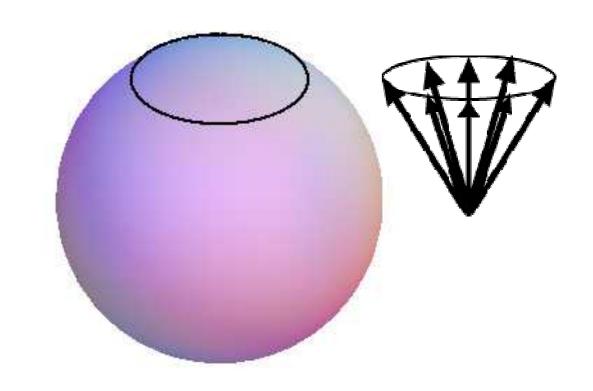
例: $\vec{B} = (0,0,B)$, $\vec{\mu}(0) = \mu(\sin\frac{\pi}{10},0,\cos\frac{\pi}{10})$

$$\frac{d\mu_x}{dt} = \gamma B_0 \mu_y$$

$$\frac{d\mu_y}{dt} = -\gamma B_0 \mu_x$$

$$\frac{d\mu_z}{dt} = 0.$$

$$\mu_z = \text{const.}$$





磁場中のスピン: 古典的描像2

x方向に振動磁場 $\omega_1 \cos(\gamma Bt)$ $\omega_1/\gamma B = 0.05$.

$$\omega_1/\gamma B = 0.05$$

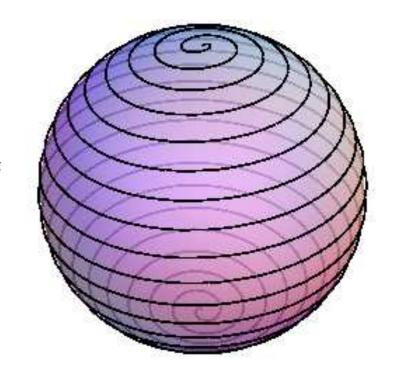
を加える:

$$\frac{d\mu_x}{dt} = \gamma B_0 \mu_y$$

$$\frac{d\mu_y}{dt} = -\gamma B_0 \mu_x + \omega_1 \cos(\gamma B t) \mu_z$$

$$\frac{d\mu_z}{dt} = +\omega_1 \cos(\gamma B t) \mu_y.$$

$$\vec{\mu}(0) = \mu(0,0,1)$$

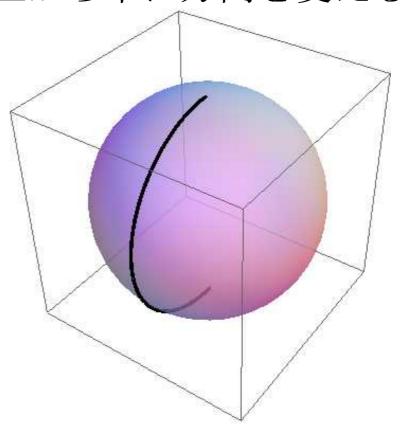


磁気モーメントはz軸周りを回りながら上から下に向き を変える.



回転系から見ると・・・

 γB の角速度で回転する系では磁気モーメント (スピン) は回転せずにまっすぐ上から下に方向を変える.



日本物理学会2008年度公開講座



磁場中のスピン:量子的描像1

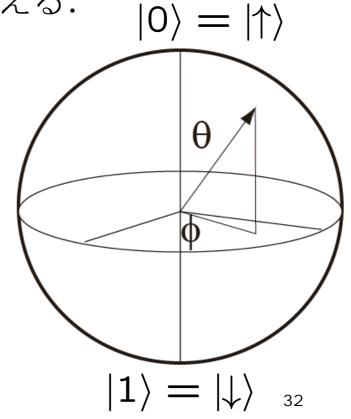
スピンの状態 $|\psi\rangle = a|0\rangle + b|1\rangle \Leftrightarrow 球上の点.$

$$|0\rangle = |\uparrow\rangle, \ |1\rangle = |\downarrow\rangle \ \text{hif } a = \cos\frac{\theta}{2}, b = e^{i\phi}\sin\frac{\theta}{2}$$

とおくと (θ, ϕ) は球面の極座標を与える.

例:
$$\theta = 0$$
で $a = 1, b = 0$ より | ↑ ⟩,

$$\theta = \pi \, \mathcal{C} \, a = 0, b = 1 \, \mathcal{L} \, \mathcal{V} \, | \downarrow \rangle.$$



日本物理学会2008年度公開講座

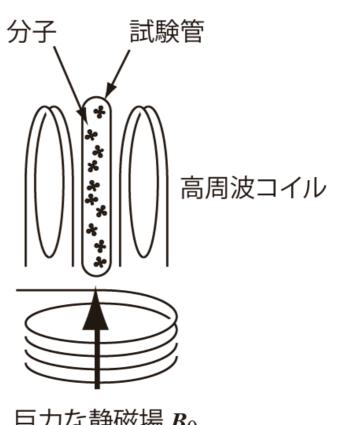


1量子ビットハミルトニアン

 $H = -\gamma B_0 \frac{\sigma_z}{2} + 2\omega_1 \cos(\omega_{rf} t - \phi) \frac{\sigma_x}{2}$ 共鳴条件 $\omega_{rf} = \gamma B_0$ が満たされる とき、角速度 γB_0 の回転系に乗る.

 $\rightarrow H' = \omega_1(\cos\phi\sigma_x/2 + \sin\phi\sigma_y/2)$

- $\phi = 0 \rightarrow x$ 軸周りの回転,
- $\phi = \pi/2 \rightarrow y$ 軸周りの回転.
- 任意の回転はこれらを組み合わせて 得られる.

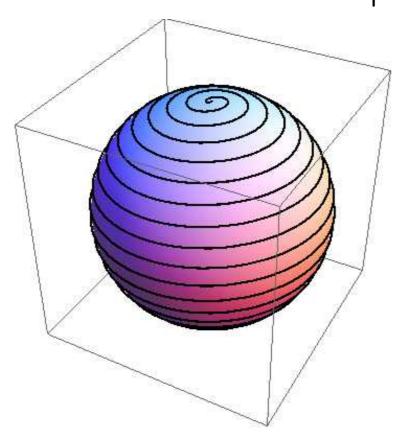


巨力な静磁場 B₀

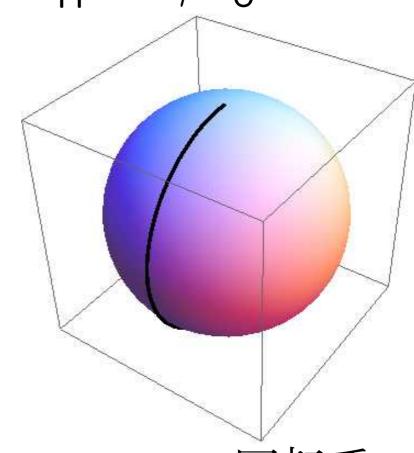


極座標 (θ, ϕ) でみたスピンの運動

t=0 $\langle 0\rangle$, $\omega_{\rm rf}=\gamma B_0$



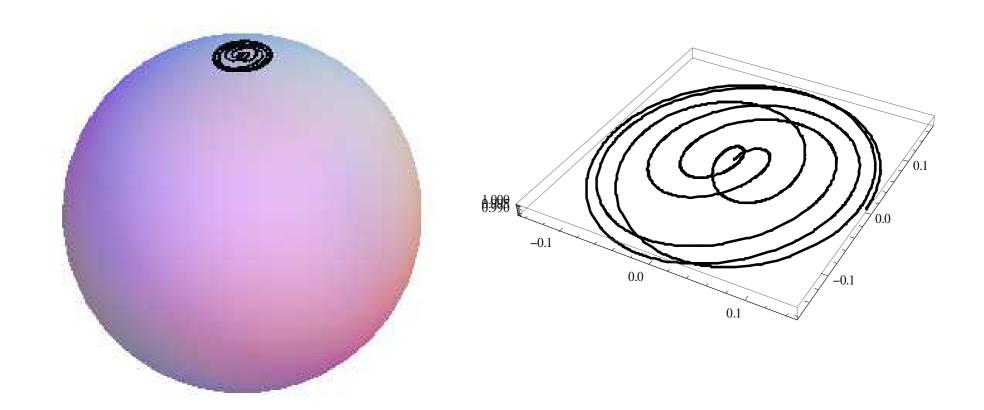
実験室系



回転系



$\omega_{\rm rf} \neq \gamma B_0$ のとき ($\omega_{\rm rf}/\gamma B_0 = 1.3$)

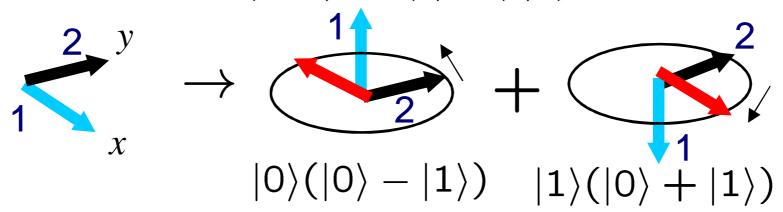


 $\omega_{\rm rf} \sim \gamma B_0$ のスピンだけが反転する.



2量子ビット操作

回転系における2量子ビット相互作用: $J\sigma_z \otimes \sigma_z$. 初期状態が $|\Psi\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + i|1\rangle)$ のとき (第1量子ビットはx軸向き,第2量子ビットはy軸向き)第1量子ビットの作る磁場の中での第2量子ビットの運動を考える. $|\to_x\rangle = (|\uparrow\rangle + |\downarrow\rangle)/\sqrt{2}$ より



 $Jt = \pi/2$ だけ待つと量子ビット2はそれぞれ-x方向と十x方向を向く.



$$\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + i|1\rangle)$$

$$\rightarrow \frac{1}{\sqrt{2}}(|0\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle + |1\rangle)$$

$$= \frac{1}{\sqrt{2}}(|00\rangle - |01\rangle + |10\rangle + |11\rangle)$$

この状態はテンソル積ではかけない縺れた状態である. 相互作用 $J\sigma_z\otimes\sigma_z$ はテンソル積状態を縺れさす作用を持つ.



NMRにおけるDiVincenzo条件の現状

- 十分な数の量子ビットを用意できるか
- すべての量子ビットを基準の状態にセットできるか (たとえば|00…00 など)
- 計算が終了するまで量子状態は安定か (外界 との相互作用によるデコヒーレンスが小さい)
- どんな量子ゲートでも構成できるか
- 計算結果を読み取ることができるか



実際の分子

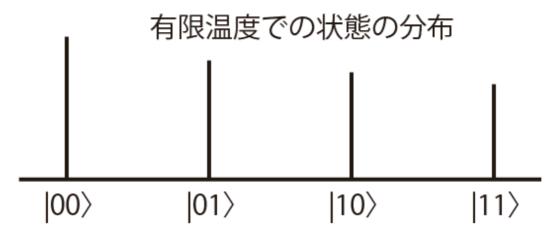


問題点

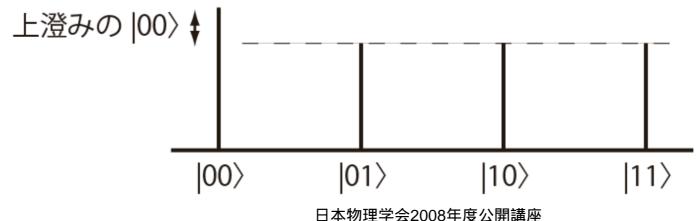
- 同種核は共鳴周波数が近いが、化学シフトにより選択的に操作できる. しかし~ **10**量子ビット程度が限界か?
- 液体 NMR は $|00...0\rangle$ から $|11...1\rangle$ まですべての 状態がほぼ同じウエイトで混ざっている. $|00...0\rangle$ を わずかな「上澄み」として取り出すテクニックが必要. ただ信号強度は $\sim 1/2^n$ で小さくなる. $n \sim 10$ くらい が限界か?
- しかしNMRは唯一お金を出しさえすれば買える量子 コンピュータである. 我々はいろいろな理論のデモンス トレーションなどに用いている.



時間平均法による擬似初期状態の生成(メモリーのリセット)

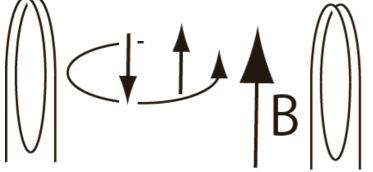


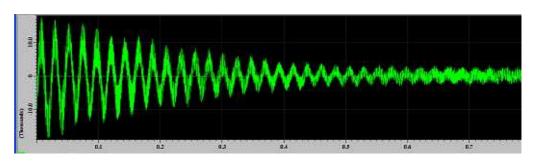


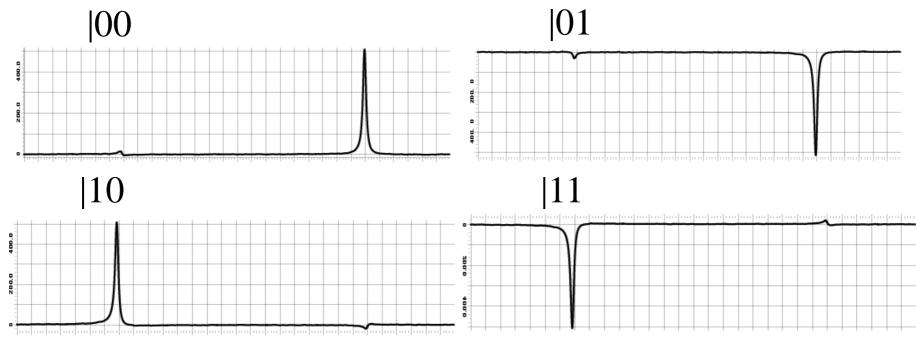




量子ビットの測定 (FID)



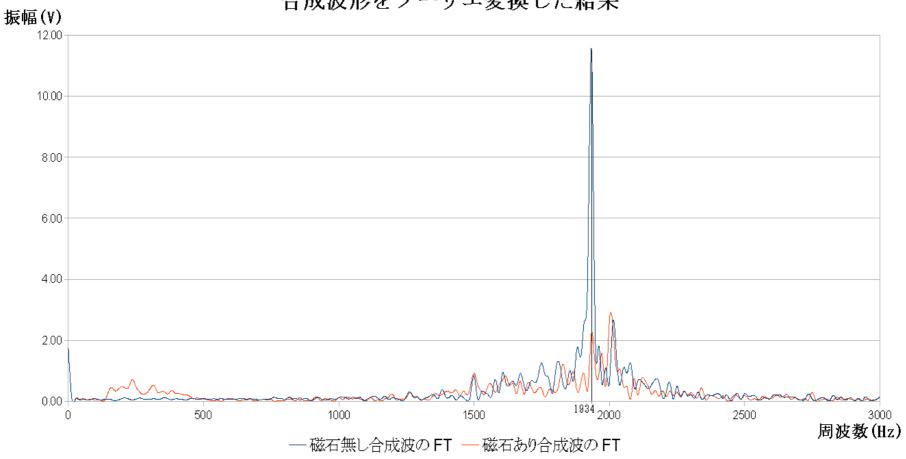






地球磁場のNMR (~¥10,000)

合成波形をフーリエ変換した結果





講演予定

- 1. はじめに:物理で計算?
- 2. 量子ビット, 量子ゲート, 量子コンピュータ
- 3. DiVincenzoの判定条件
- 4. NMR量子コンピュータ
- 5. 例: Shorのアルゴリズム
- 6. おわりに



素因数分解の困難

- N=8902083681874790795683198927209 1600303613264603794247032637647625 631554961638351の素因数分解は困難。
- p=92810132054041315184759024472769 73338969とq =9591715349237194999547 050068718930514279の積がNであること は小学生でも計算できる . (多分)
- この事実はRSA (Rivest-Shamir-Adleman) 暗号に用いられ,インターネットなどで我々の生活に日常的に用いられている.



素因数分解のアルゴリズム

大きな複合数 N = pq を素因数分解したい.

- [1] N より小さな正数 m をランダムに選び $\gcd(m,N)$ を計算. $\gcd(m,N) \neq 1$ であれば m=p or q. 以下 $\gcd(m,N)=1$ と仮定.
- [2] $f_N: \mathbb{N} \to \mathbb{N}$ を $a \mapsto m^a \mod N$ で定義. $m^P \equiv 1 \mod N$ となる最小の $P \in \mathbb{N}$ (位数) を求める. (Shor のアルゴリズム)
- [3] P が奇数であれば廃棄して[1] へ戻り、別のm で P が偶数となるまで反復する.
- [4] 偶数のPに対して $(m^{P/2}-1)(m^{P/2}+1)=m^P-1\equiv 0 \bmod N$ が成立。もし $m^{P/2}+1\equiv 0 \bmod N$ であれば $\gcd(m^{P/2}-1,N)=1$ となり [1] へ戻って別のm から始める。もし $m^{P/2}+1\not\equiv 0 \bmod N$ であれば $m^{P/2}-1$ はpまたはqを素因数として含む。
- [5] $d = \gcd(m^{P/2} 1, N)$ は p or q で素因数分解は完了.

1000 A



NMRを用いた実現 (15=3×5)

L. M. K. Vandersypen 他 (Nature 2001)



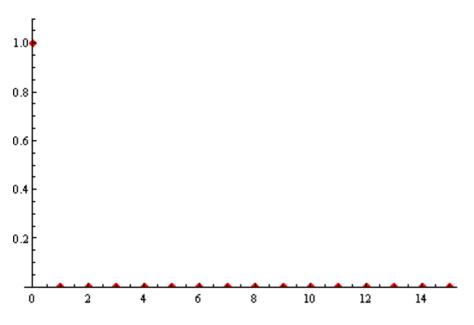
NMRの分子とパルス列(~300 pulses)

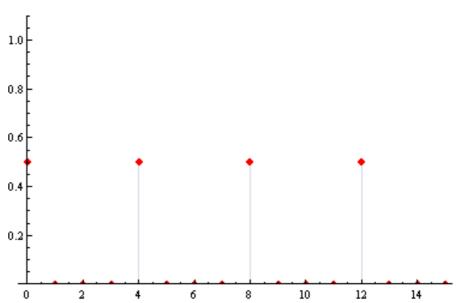
$$\begin{array}{c|c}
\mathbf{F} & \mathbf{F} \\
\mathbf{F} & \mathbf{C} = \mathbf{C} \\
\mathbf{F} & \mathbf{C} = \mathbf{C} \\
\mathbf{F} & \mathbf{F} \\
\mathbf{C}_{5} \mathbf{H}_{5} & (\mathbf{CO})_{2}
\end{array}$$

perfluorobutadienyl iron complex with the two 13C-labelled inner carbons



ピークの間隔 = N/P = 4



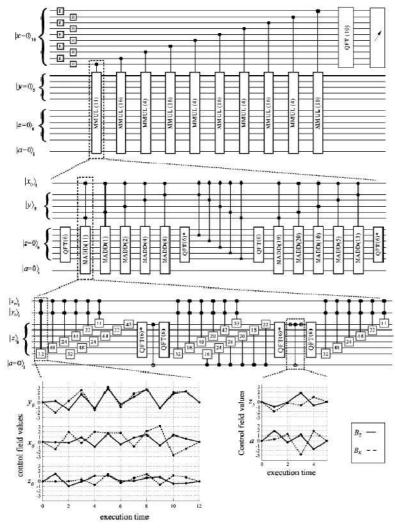


初期状態 |0>

最終状態
$$\frac{1}{2}(|0\rangle + |4\rangle + |8\rangle + |12\rangle)$$

しかしfoolproofな実装では...

Vartiainen, Niskanen, Nakahara, Salomaa (2004)



Shorのアルゴリズムをfoolproofに実装しようとすると21=3×7の素因数分解では少なくとも22量子ビットが必要.ステップ数は約82,000!



講演予定

- 1. はじめに:物理で計算?
- 2. 量子ビット, 量子ゲート, 量子コンピュータ
- 3. DiVincenzoの判定条件
- 4. NMR量子コンピュータ
- 5. 例: Shorのアルゴリズム
- **■** 6. おわりに



おわりに

- 量子コンピュータは古典的に存在しない状態を使って古典コンピュータをはるかに越える計算ができる。
- 液体NMRは、現状では量子ビット数の問題、リセットの問題などで、究極の量子コンピュータの候補とはなりえない、しかし、さまざまな理論のテクニックを検証するのに有用・
- 実用的な量子アルゴリズムを実装するには,理論, 実験とも飛躍的な発展が必要.
- そのためには物理,化学,数学,情報学などの専門 家の共同研究が不可欠.
- 共同研究者募集中.
- 高校への出張講義も承ります.

