早く来た人にクイズ（今日の話に関係があります）

- ある国では郵便配達を泥棒たちが請け負っている．彼らは鍵のかかっていない小包は何でも勝手に開けて中身を盗ってしまう．ただし鍵がかかっているものには手を出さない．この国でボブが婚約者のアリスに指輪を送ろうとしている．どうやったら安全に送り届けることができるだろうか？
- しっかりした箱に錠前をつけて送れば途中で盗まれることはないが，アリスはその鍵を持っていないから箱を開けることができない．錠前はどこでも買うことができるが，買った錠前の鍵は自分の手もとにあって，相手は持っていない．鍵を別の郵便で送ることも考えられるが，鍵をかけた郵便ででも送らない限り，やはり途中で盗られてしまう．
- 困り果てたボブは電話でアリスに相談した．アリスはとてもうまい方法を考えついた．錠前をいくつでもつけられる箱で送ってもらうことによって，無事にボブからの指輪を受け取ることができた．いったいどうやったのだろう？

東京大学
THE UNIVERSITY OF TOKYO

2005年12月5日
学術俯瞰講義
「物質の科学」

第6回　物性物理学とは何をする学問か
第7回　量子力学と人工構造物質
　　－ ハイテクと先端物理
第8回　原子を操る，量子を操る
**　　－ナノサイエンスと量子情報**
第9回　多様な物質，多様な物性

東京大学物性研究所
家 泰弘

前回の復習 (1)

- 量子力学について
  - 波動関数，シュレーディンガー方程式，不確定性原理，確率解釈
  - トンネル効果と量子干渉効果
- 量子干渉
  - ヤングの二重スリットの実験
  - 電子干渉の実験
  - アハロノフ･ボーム効果

前回の復習 (2)

- 人工物質．メゾスコピック系
  - ハイテク，微細化 (超LSI，ハードディスク)
  - メゾスコピック系
    人工物質作製，微細加工
- 量子伝導現象
  - 伝導電子，電気伝導
  - 量子コンダクタンス　$e^2/h = (25.813\,\mathrm{k}\Omega)^{-1}$
    量子ポイントコンタクト，量子ホール効果
  - 量子干渉　ABリング
  - 単電子トンネル　量子ドット

今日のお話

- 原子を見る，操る
  - STM, AFM, ナノサイエンス
- 巨視的量子現象
  - 量子統計
  - 量子液体
  - ボース･アインシュタイン凝縮
- 量子情報処理
  - 暗号について
  - 量子コンピューター
  - 量子暗号 (秘密鍵配信)

原子を見る，操る

スケールの小さな話

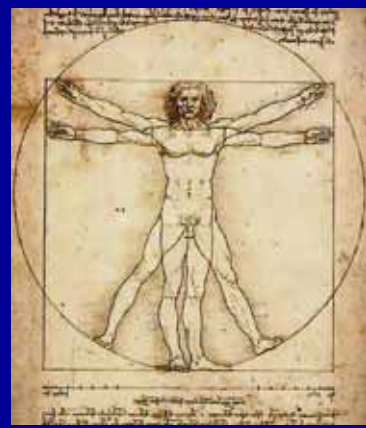
10^{-12} m　10^{-9} m　10^{-6} m　10^{-3} m　1 m

1 pm ピコメートル

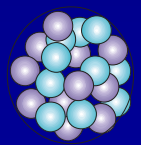
1 nm ナノメートル

1 μm マイクロメートル (ミクロン)

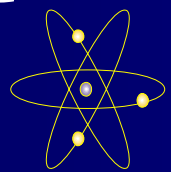
1 mm ミリメートル



原子核の大きさ



原子の大きさ



ウィルス

細菌

針の穴 髪の毛

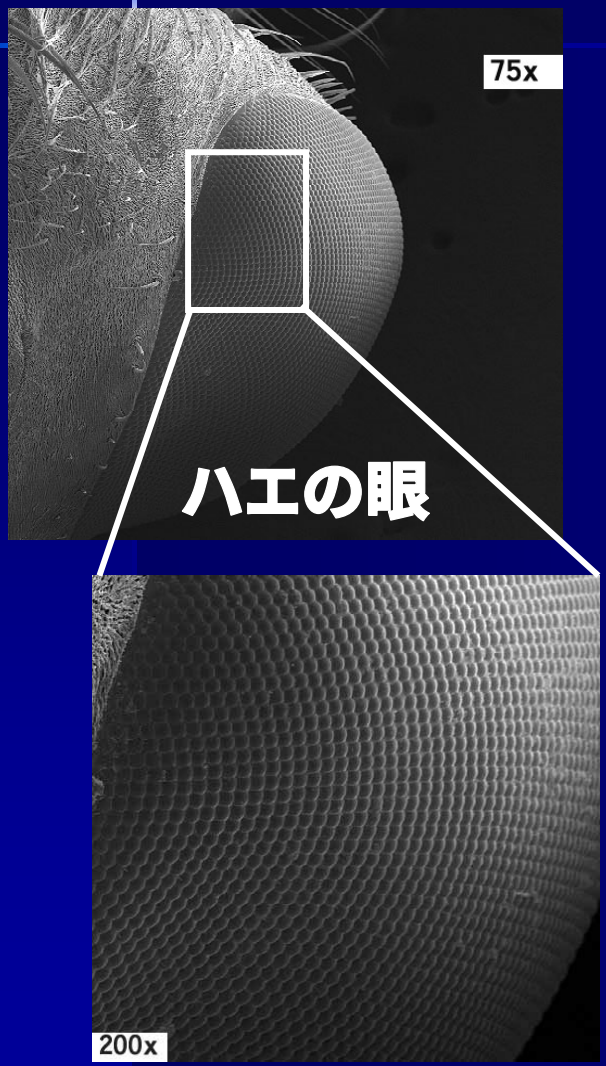
可視光の波長

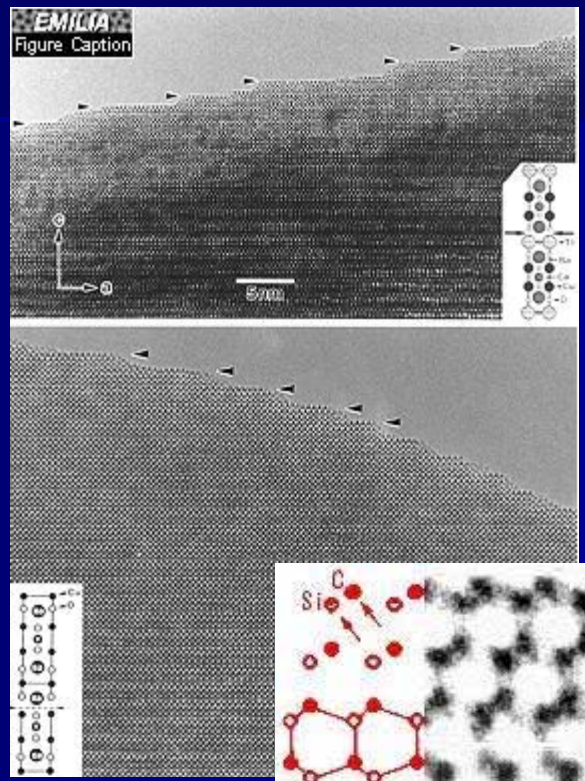
光学顕微鏡

電子顕微鏡

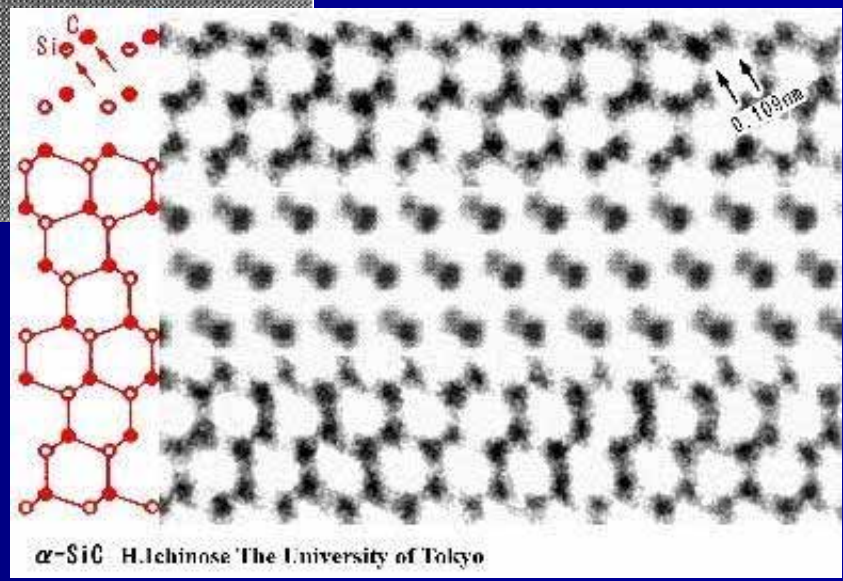
走査プローブ顕微鏡

小さなものを見る：電子顕微鏡

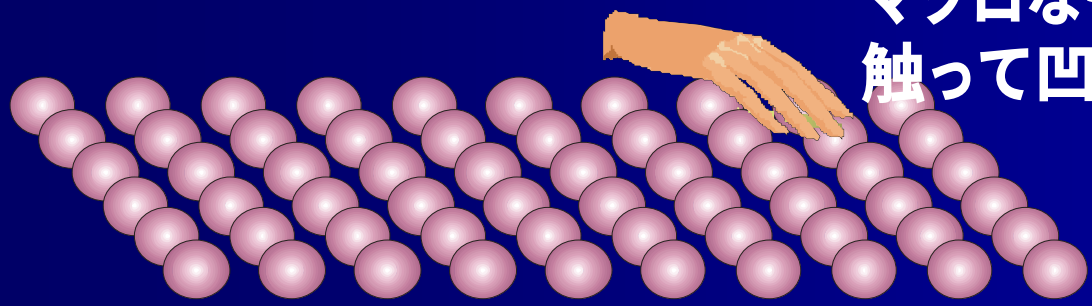




高分解能電子顕微鏡で原子の配列を見る



固体表面の原子の並びを見る

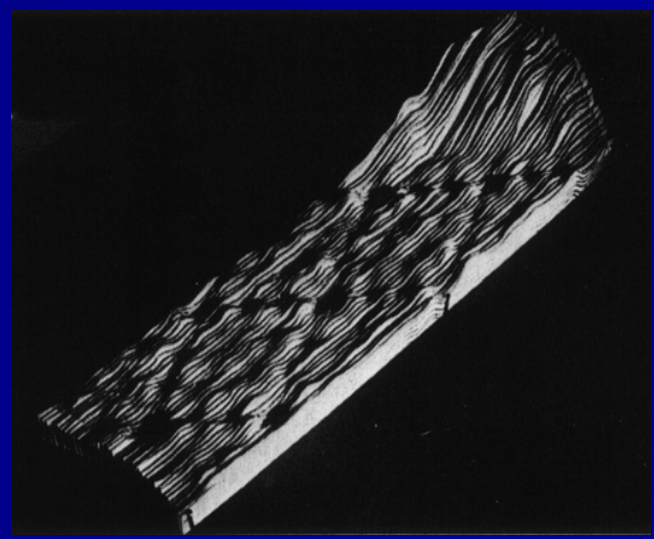


マクロなものなら
触って凹凸を見ればよい

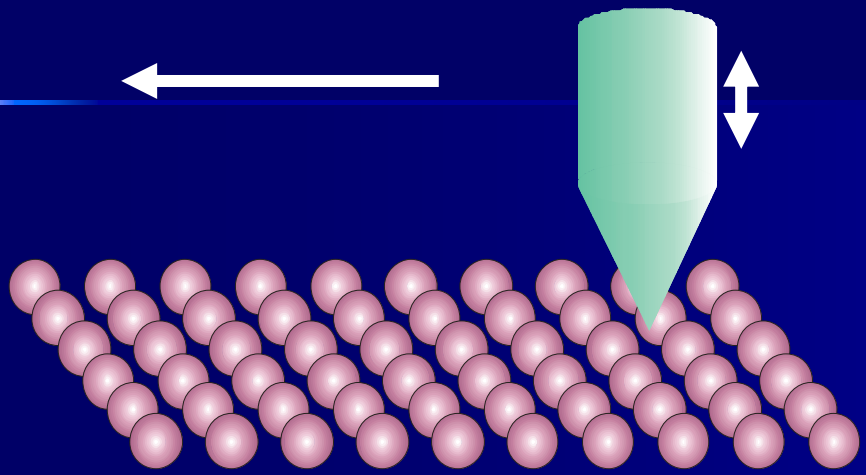
これと同じようなことが原子スケールで可能だろうか？
⇒ 「不可能」と考えるのが常識

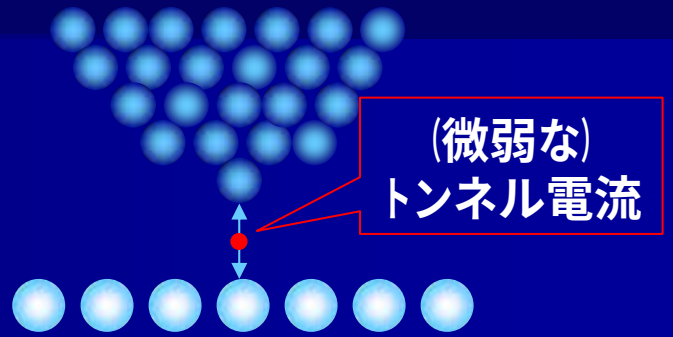
走査トンネル顕微鏡
1984年 ビニッヒ＆ローラー

シリコン結晶の
表面の原子の
並びを初めて
とらえた像

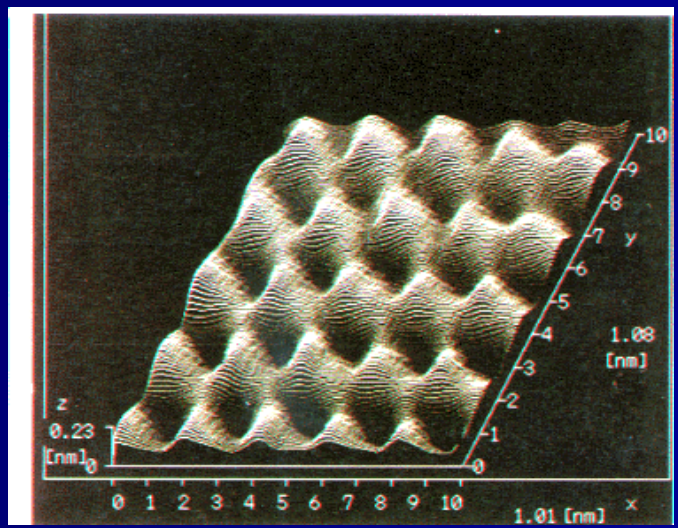


走査トンネル顕微鏡（ＳＴＭ）



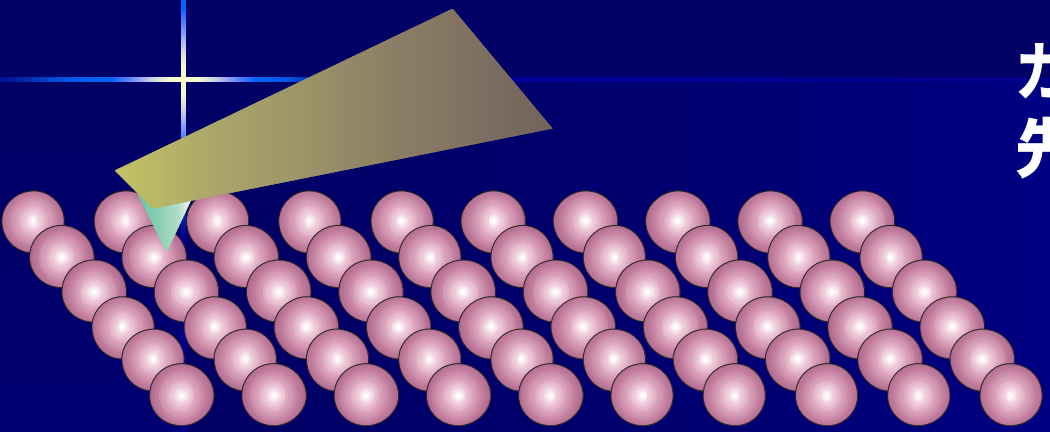


針先の原子と表面の原子を１nm程度に近づけるとトンネル電流が流れる．
トンネル電流が一定になるように針を上下しながら横方向に動かせば原子スケールの凹凸を観察することができる



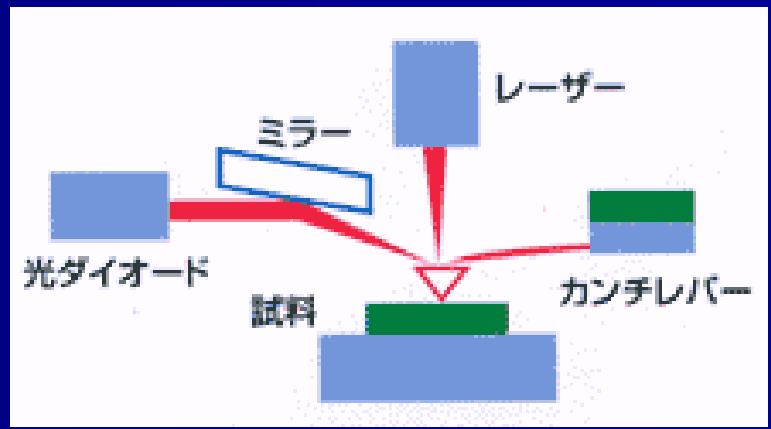
安定性の問題
機械的振動
電気的雑音

原子間力顕微鏡 (AFM)



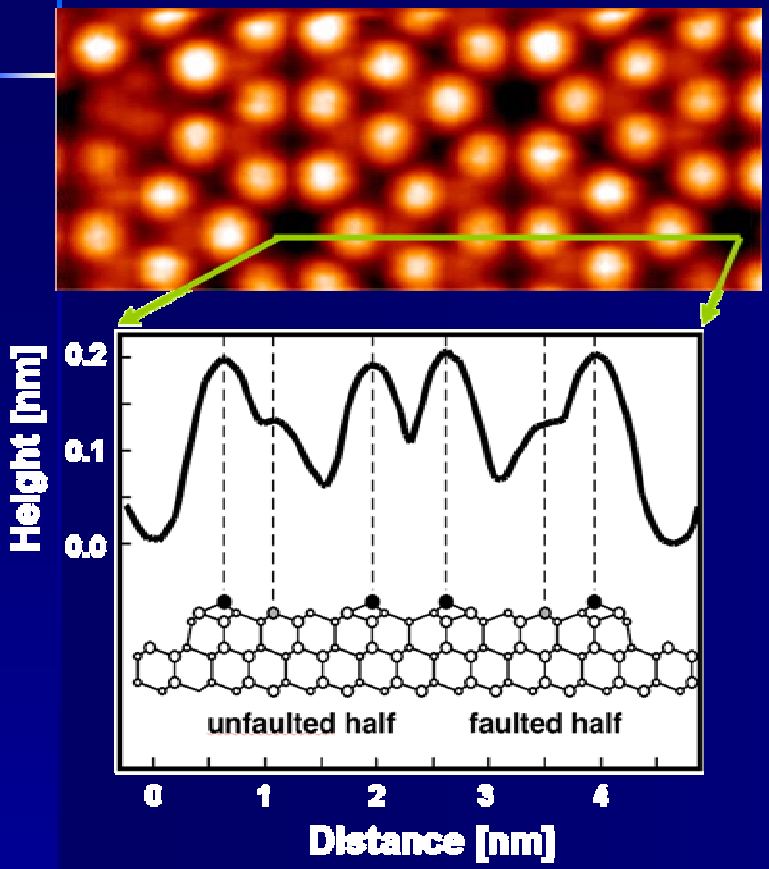
カンチレバー (片持ち梁) の
先に探針がついたもの

探針先端の原子と表面の
原子が近づいたときに働く
力を検出する。

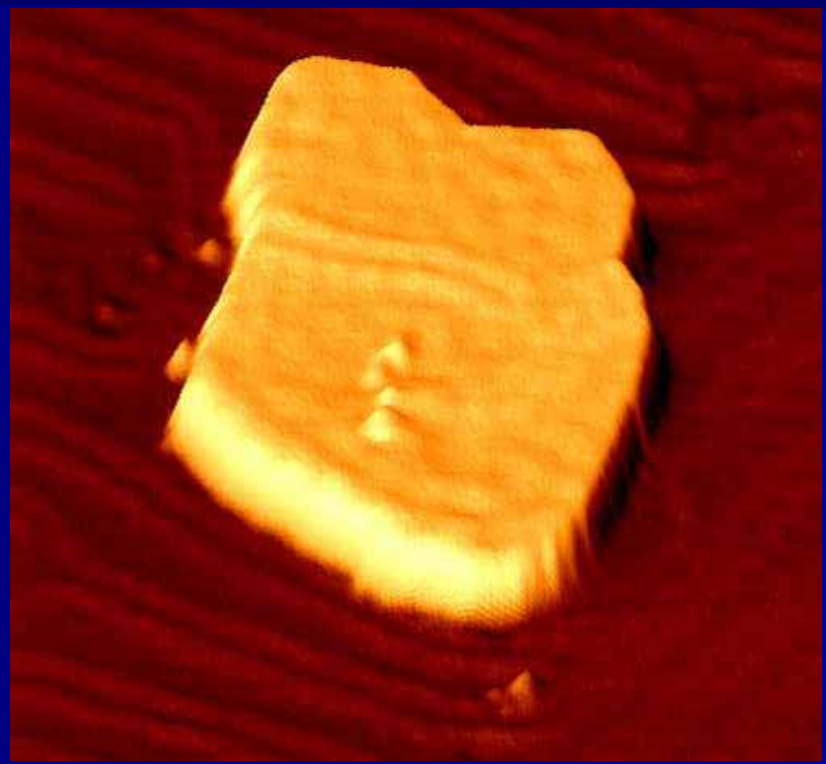


カンチレバーの曲がり具合を
レーザー光を使って検出する

走査プローブ顕微鏡による表面の観察



NC-AFM

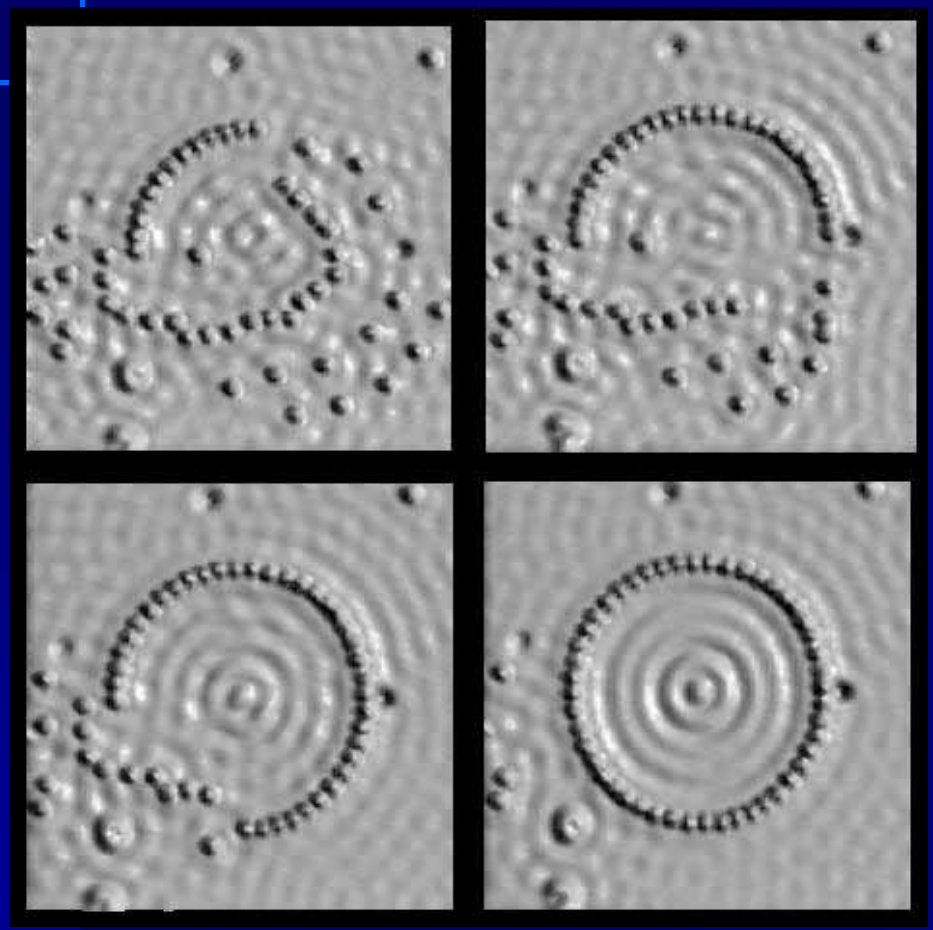


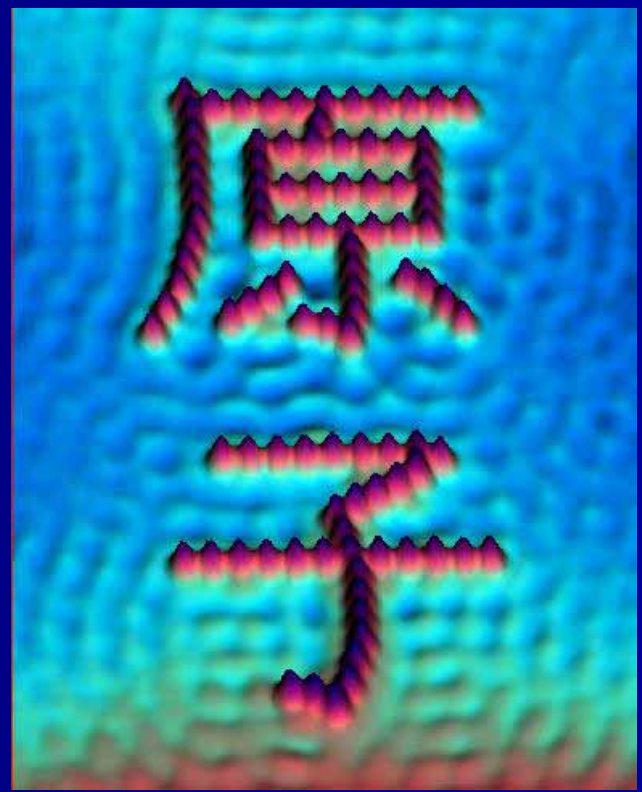
STM

物性研究所　長谷川研究室

原子を操る

IBM Almaden研究所
Eiglerグループ





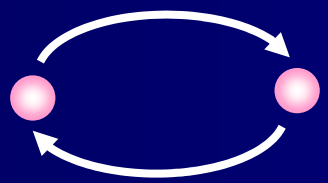
銅の表面に鉄原子を並べる．
さざ波のように見えるのは表面電子の波の干渉による．

巨視的量子現象

量子力学的粒子

同種の量子力学的粒子は識別できない

2個の同種粒子を交換しても元と同じ状態
（ただし，波動関数には一般に数因子がつく）



$$\Psi(\mathrm{b,a}) = C\,\Psi(\mathrm{a,b})$$

$$\Psi(\mathrm{a,b}) = C\,\Psi(\mathrm{b,a}) = C^2\,\Psi(\mathrm{a,b})$$

$$\Rightarrow \quad C^2 = 1$$

$$\Rightarrow \quad C = 1 \quad \text{または} \quad -1$$

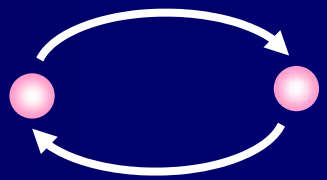
ボース粒子

フェルミ粒子

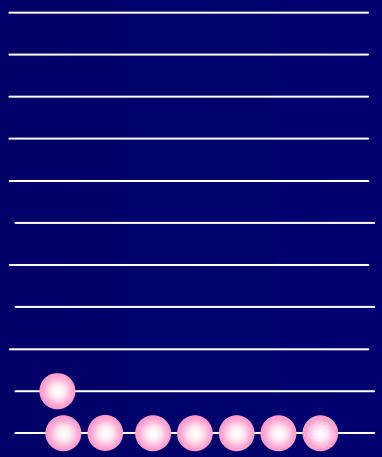
量子統計

ボース粒子（ボソン）

スピン： 0, 1, ・・・



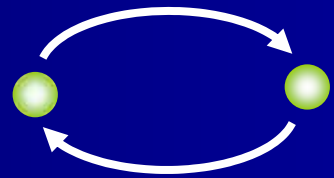
$\Psi(b,a) = \Psi(a,b)$



同じ状態にいくつでも入れる

フェルミ粒子（フェルミオン）

スピン： 1/2, 3/2, ・・・

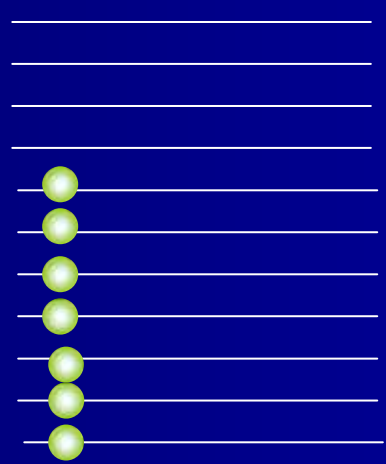


$\Psi(b,a) = -\Psi(a,b)$

a=bならば

$\Psi(a,a) = -\Psi(a,a)$

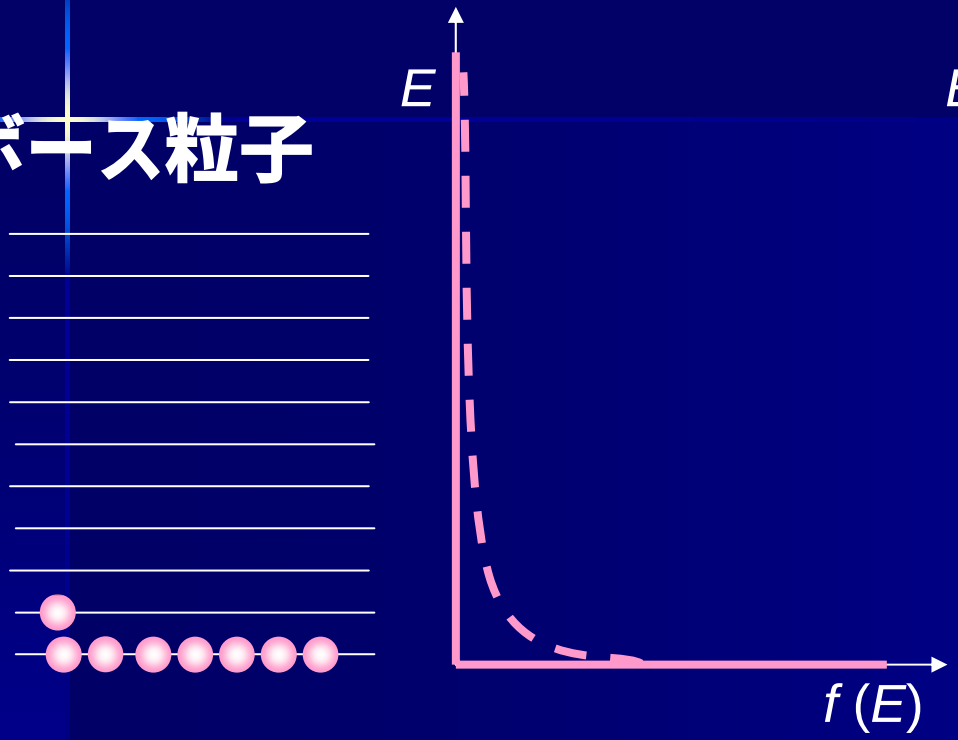
⇒ $\Psi(a,a) = 0$



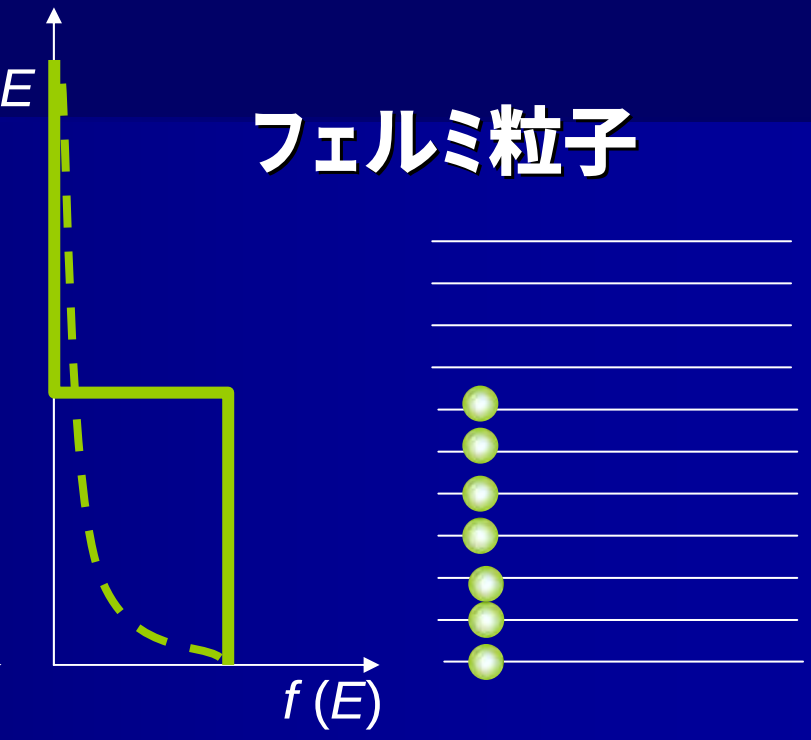
同じ状態には1個しか入れない
（パウリの排他律）

ボース・アインシュタイン分布と フェルミ・ディラック分布

ボース粒子



フェルミ粒子



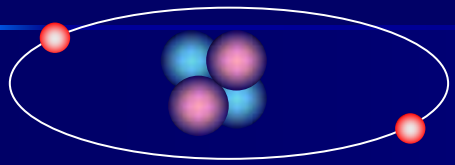
$$f_{\mathrm{BE}}(E)=\frac{1}{e^{(E-\mu)/k_{\mathrm{B}}T}-1}$$

$$f_{\mathrm{FD}}(E)=\frac{1}{e^{(E-\mu)/k_{\mathrm{B}}T}+1}$$

高温極限ではマクスウェル・ボルツマン分布

$$f(E)=e^{-(E-\mu)/k_{\mathrm{B}}T}$$

ヘリウムの同位体

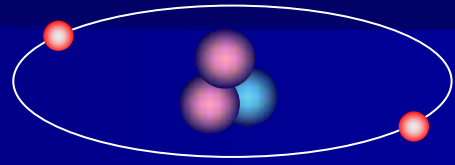


^{4}He

陽子　　2個
中性子　2個
電子　　2個

全スピン＝0

ボース粒子



^{3}He

陽子　　2個
中性子　1個
電子　　2個

全スピン＝1/2

フェルミ粒子

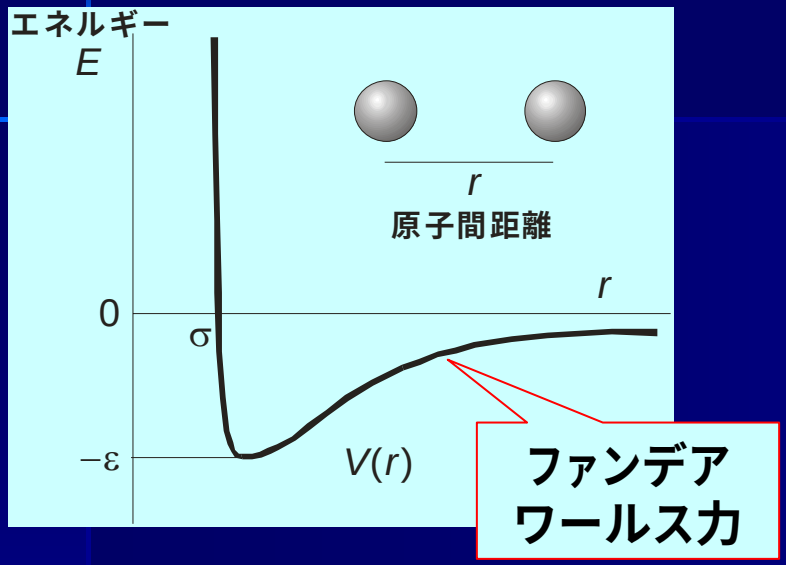
極低温をつくる

量子統計性が効くような現象を見るには極低温が必要

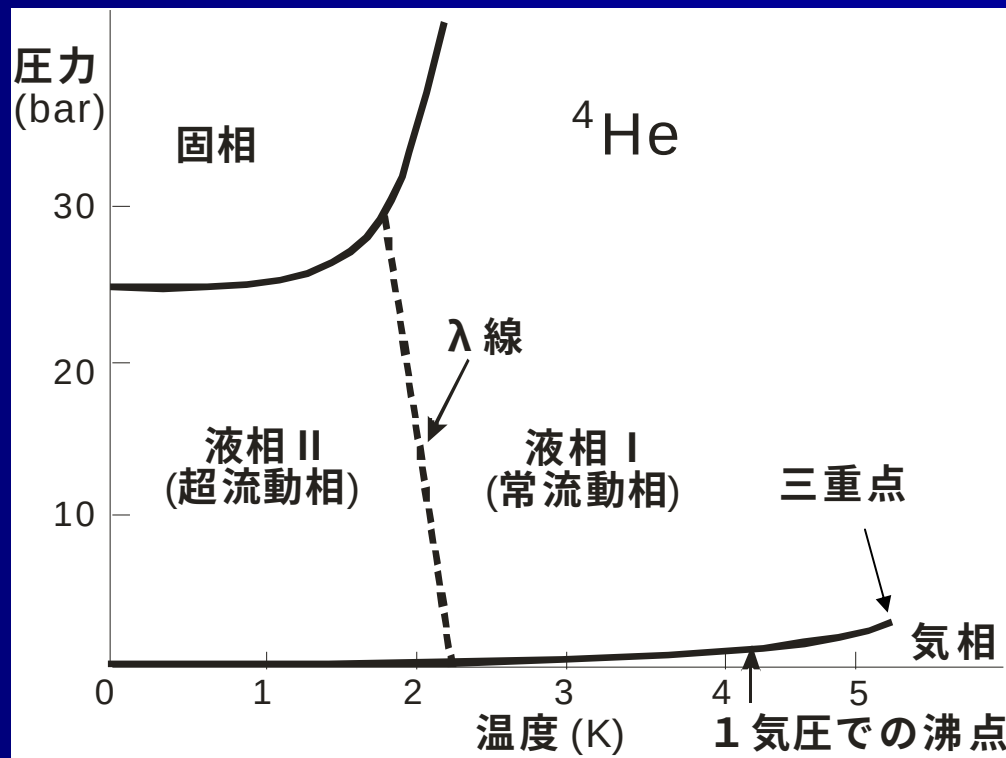
液体ヘリウム容器の
内部構造

液体窒素	77K
液体ヘリウム (^{4}He)	4.2K
真空ポンプで減圧	~ 1.2K
液体ヘリウム3 (^{3}He)	3.2K
真空ポンプで減圧	~ 0.3K
^{3}He-^{4}He希釈冷凍機	~ mK
核断熱消磁	~ μK

ヘリウムの相図

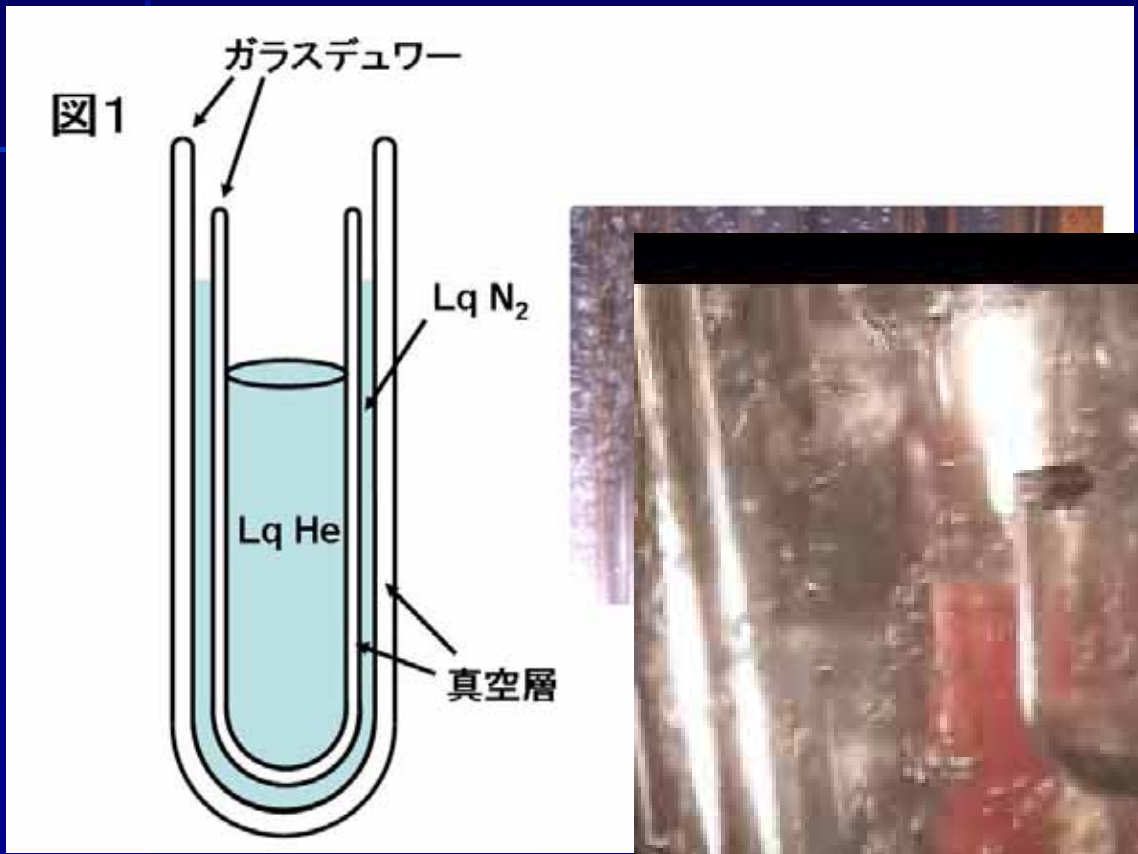


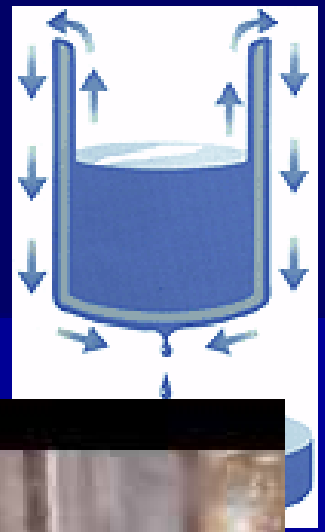
ヘリウムは（常圧では）絶対零度でも固体にならない
⇒ 量子液体



ヘリウム原子は
(1) 軽い
(2) 相互作用は弱い
運動エネルギー
＞ 相互作用エネルギー

液体ヘリウムの超流動

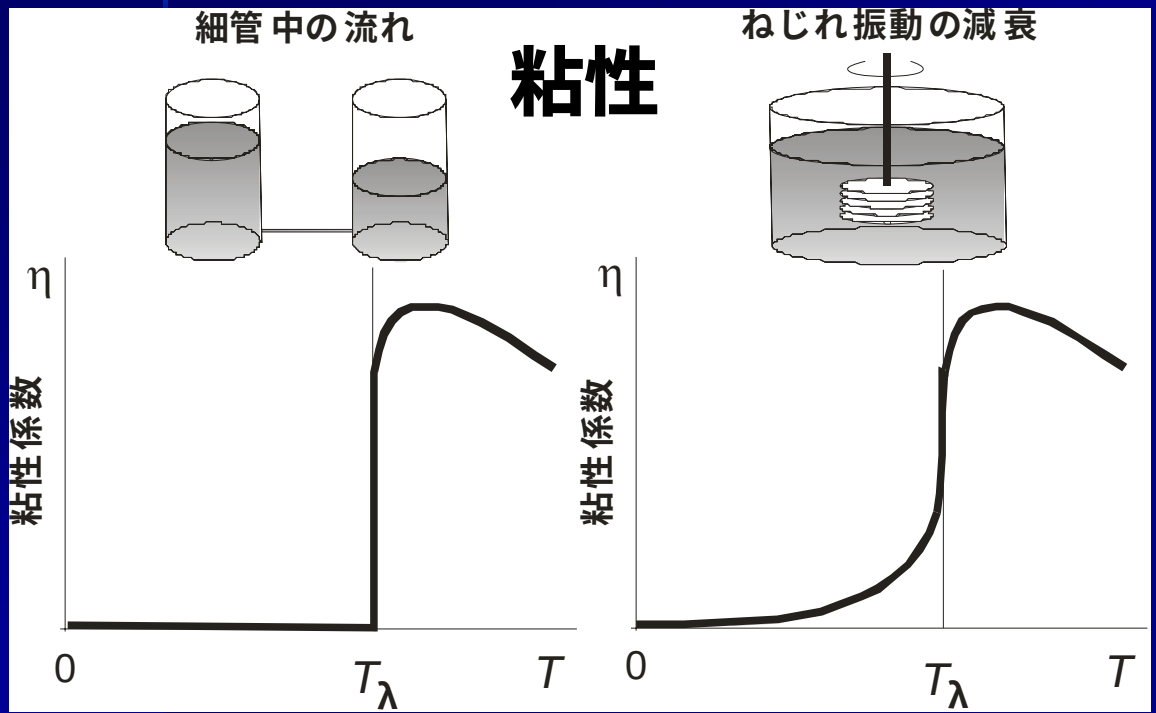




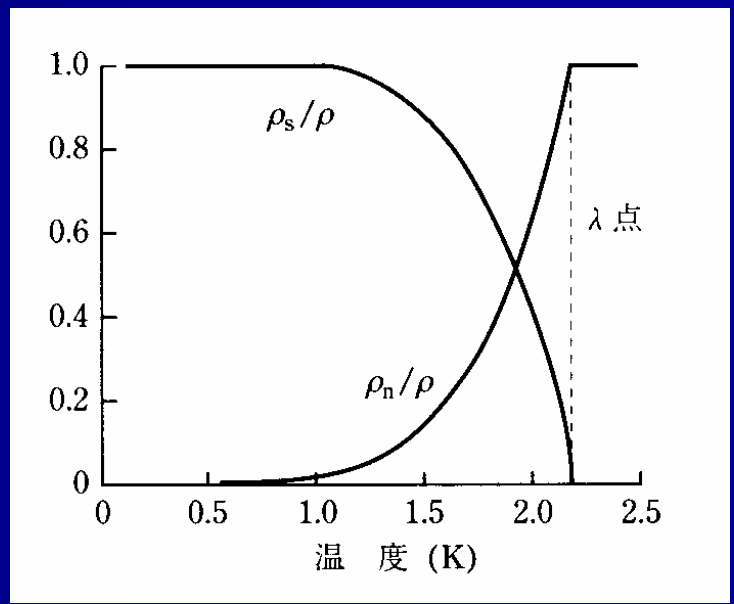
東京大学低温センター

液体ヘリウムの超流動

2流体モデル
超流動成分＋常流動成分

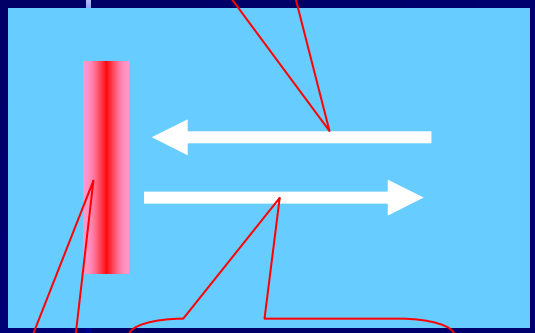


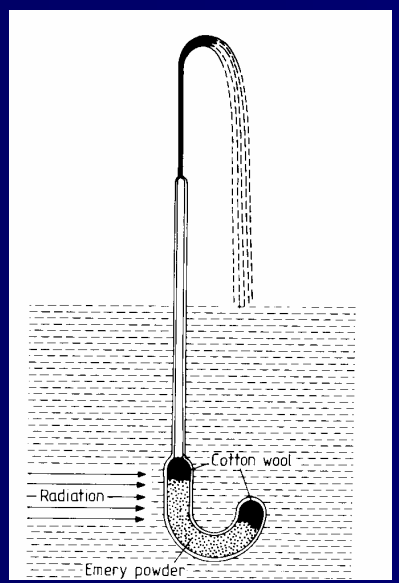
$$\rho = \rho_s + \rho_n$$



噴水効果

熱機械効果（内部対流）





東京大学低温センター

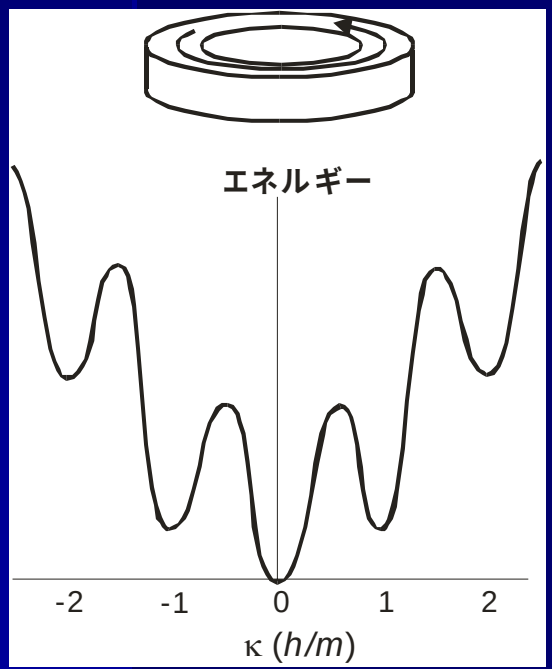
量子渦

巨視的波動関数 $\Psi = \Psi_0 e^{i\theta}$

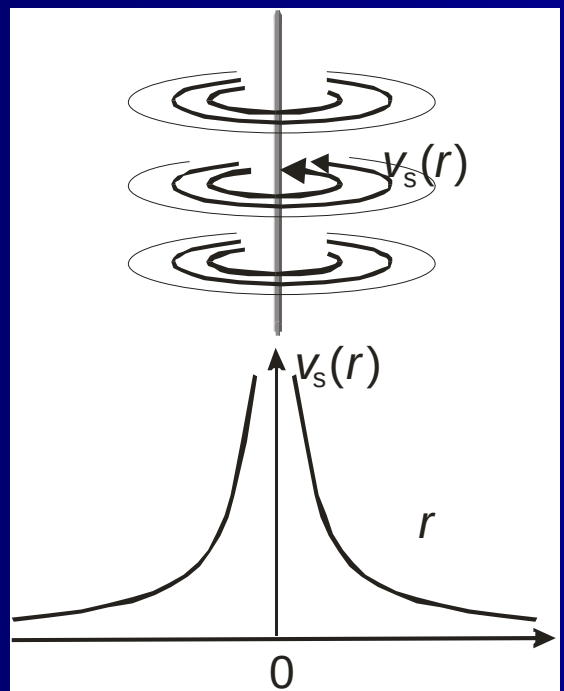
循環の量子化

$$\kappa \equiv \oint_C \mathbf{v}_s \cdot d\mathbf{s} = \frac{\hbar}{m}\oint_C \nabla\theta \cdot d\mathbf{s} = \frac{\hbar}{m} 2\pi m = n\frac{h}{m}$$

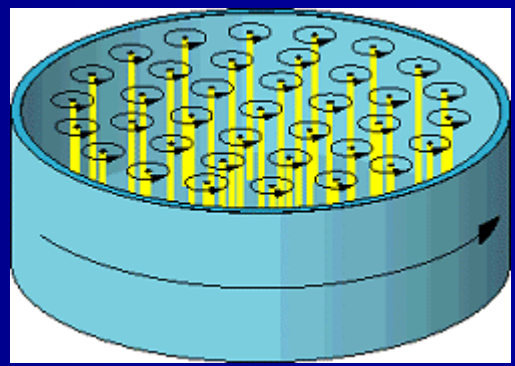
永久流

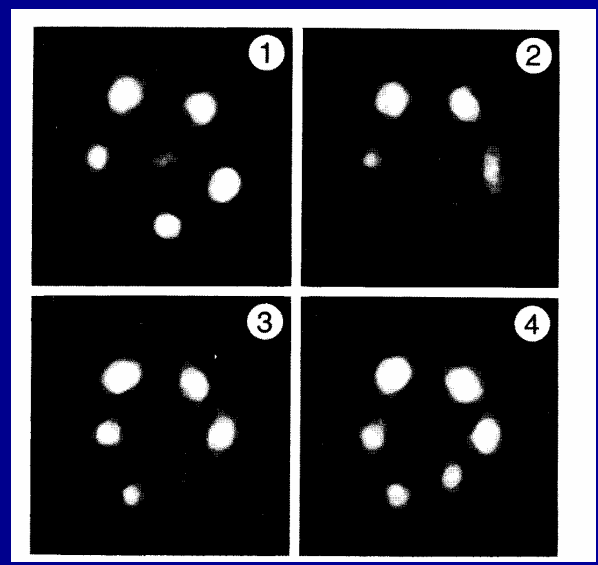


量子渦糸

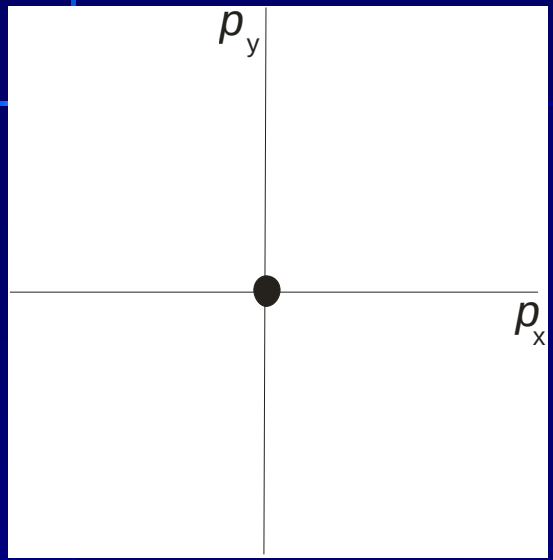


回転バケツの実験

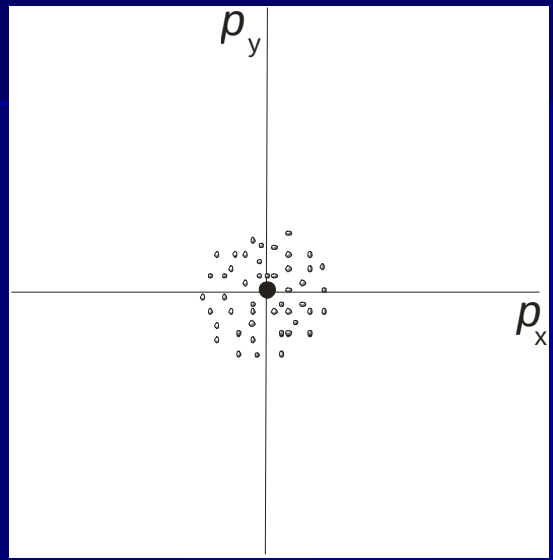




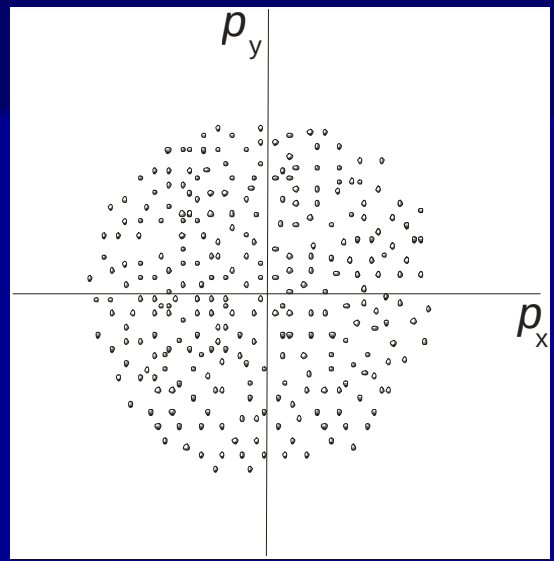
ボース・アインシュタイン凝縮



$T = 0$



$T = T_{BE}$



$T > T_{BE}$

熱的ド・ブロイ波長

$$\lambda_T = \left(\frac{2\pi\hbar^2}{mk_B T} \right)^{1/2}$$

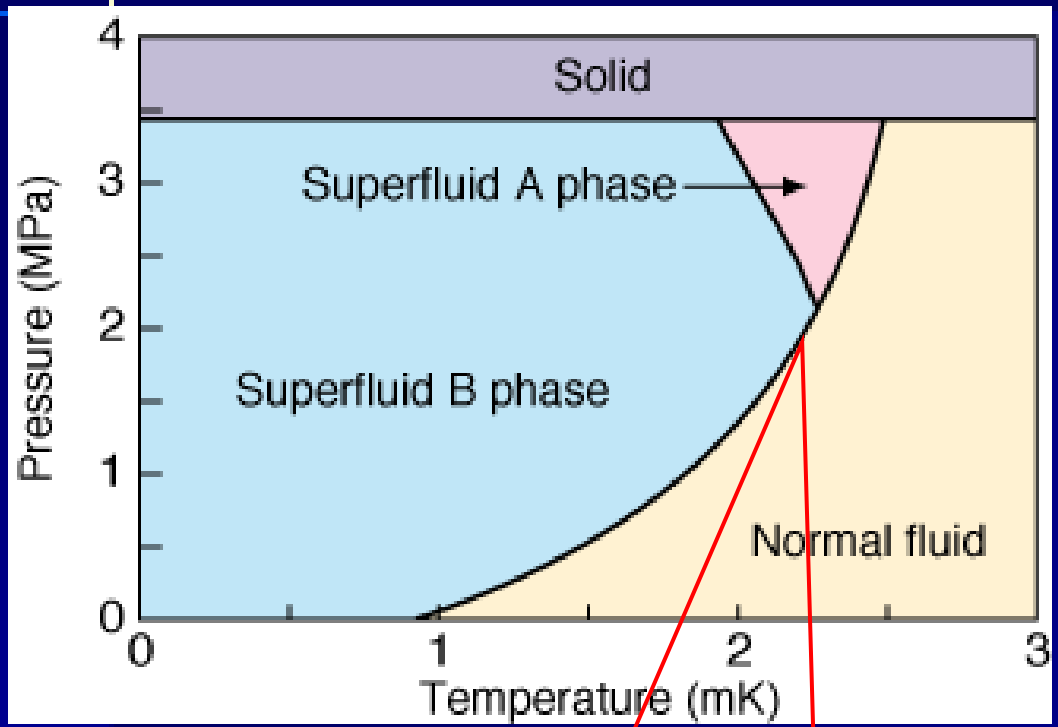
熱的ド・ブロイ波長が粒子の間隔程度になるとボース凝縮

$$\lambda_T \approx n^{-\frac{1}{3}}$$

$$T_{BE} = \frac{2\pi\hbar^2}{mk_B} \left(\frac{n}{2.612} \right)^{\frac{2}{3}}$$

ヘリウム3の超流動

^{3}Heの相図



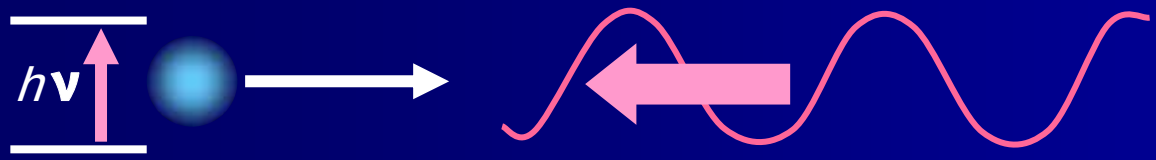
^{3}Heは～2mKという極低温で超流動になる

フェルミ粒子である^{3}Heはボース凝縮を起こさないが，
2個の^{3}Heが対（ペア）になってボース粒子のようにふるまうことによって超流動相に転移する
（超伝導と同じ機構）

原子気体のレーザー冷却

原子（たとえばRb）の気体（蒸気）をトラップに溜めて冷やす

ドップラー冷却



・原子の共鳴振動数よりわずかに低い振動数の光を照射する．
・光と逆向きに走っている原子にとってはドップラー効果によってこの光の振動数が高く見えて共鳴に近くなり，吸収確率が高くなる．光を運動量を吸収することにより原子は減速される．
・光を再放出するときには等方的に放出されるので，平均として原子は減速される．
・6本のレーザービームを x，y，zの正負から照射することによってあらゆる方向についてドップラー冷却が起こる．
・ドップラー冷却の限界は$T \sim 100\,\mu\mathrm{K}$ 程度
⇒ この温度をさらに3～4桁下げる

原子気体のボース･アインシュタイン凝縮

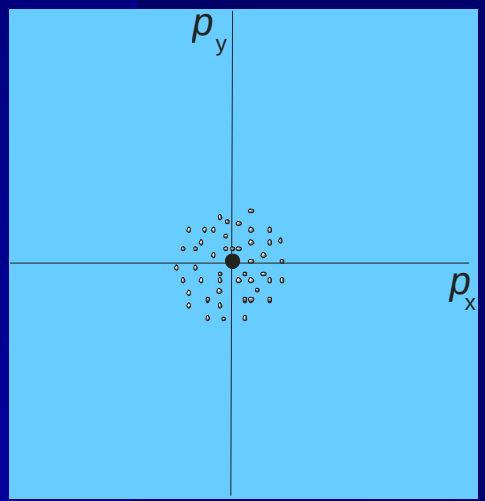
磁気光学トラップに冷却した原子気体を集める

蒸発冷却によって温度を下げてボース･アインシュタイン凝縮の条件を実現する

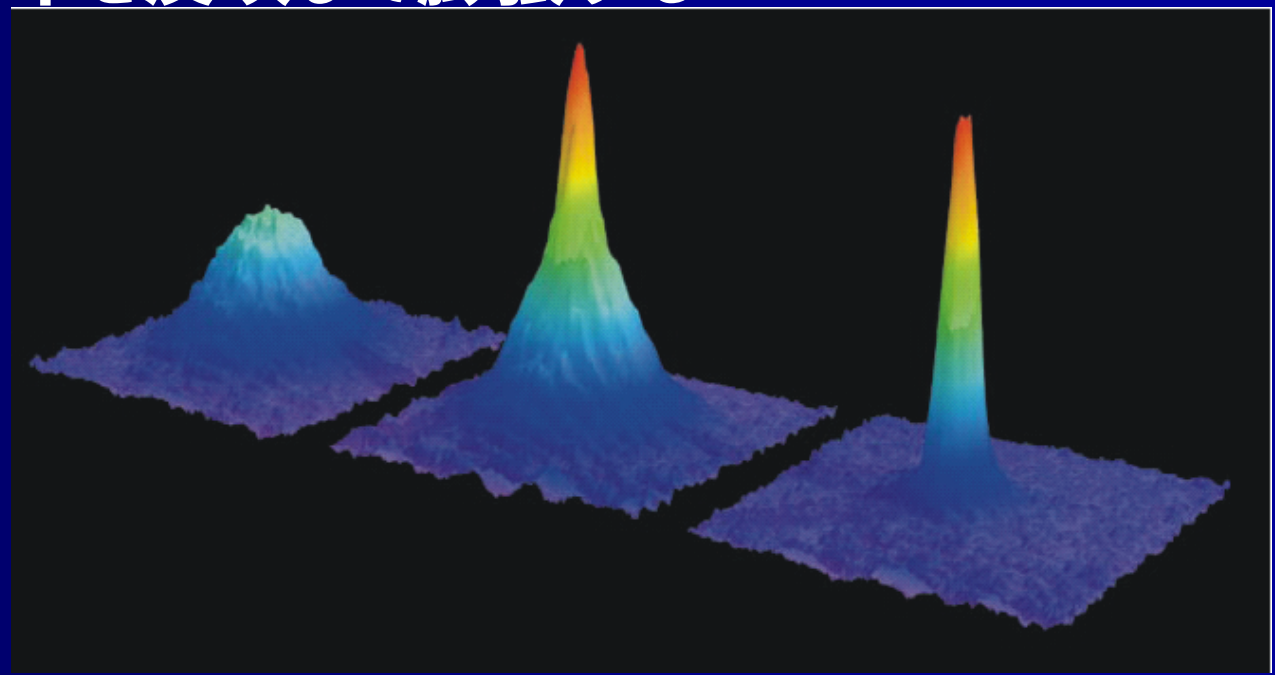
$$\lambda_T \approx n^{-1/3}$$

$T \sim 10^{-7}$K

トラップを切ると原子雲は重力で落下しながらその速度分布を反映して膨張する

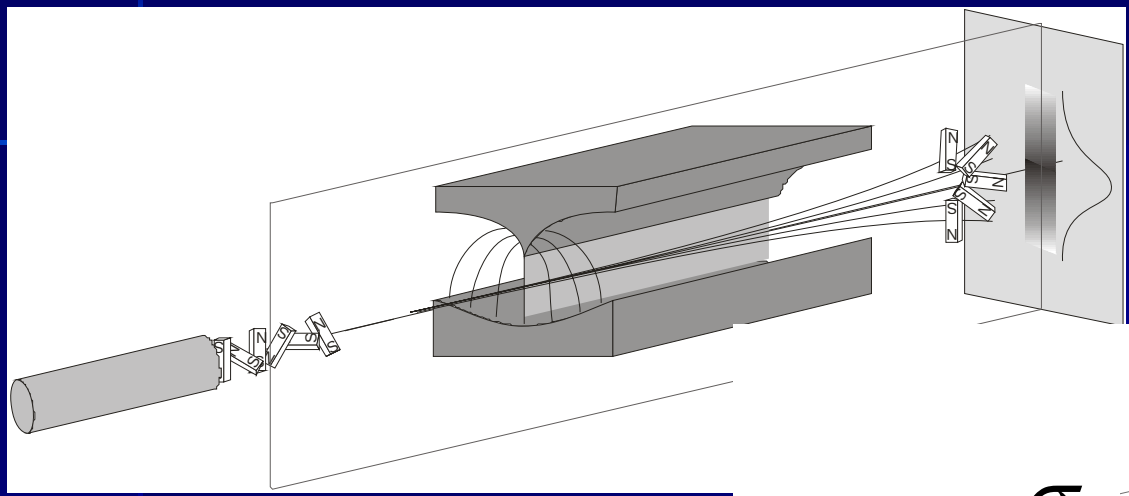


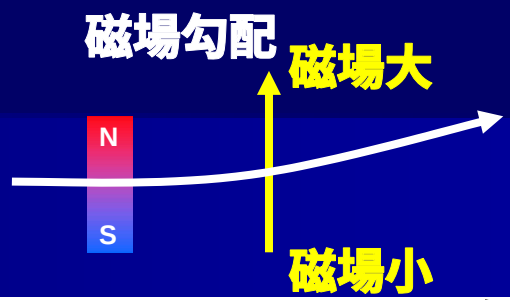
$T = T_{BE}$



量子力学における測定

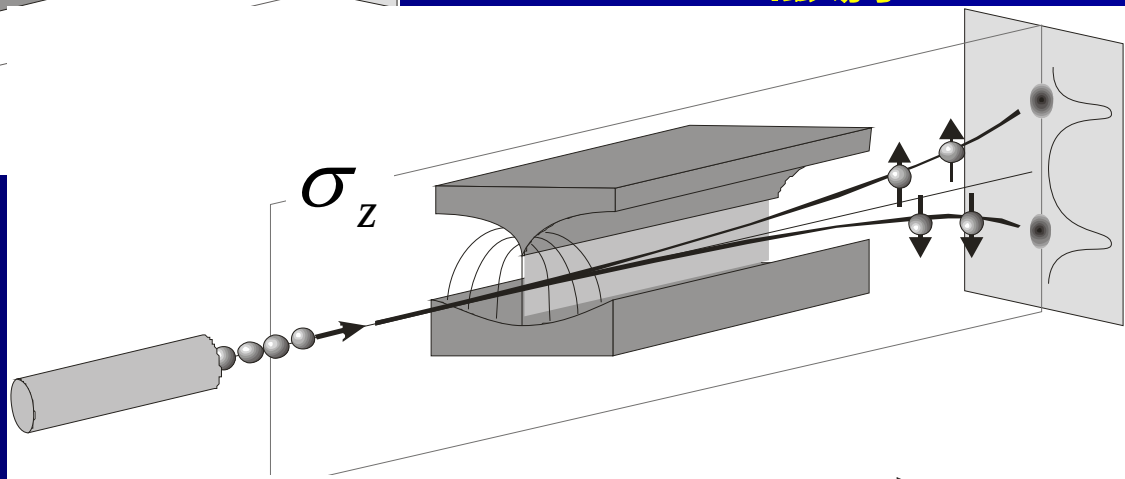
シュテルン･ゲルラッハの実験

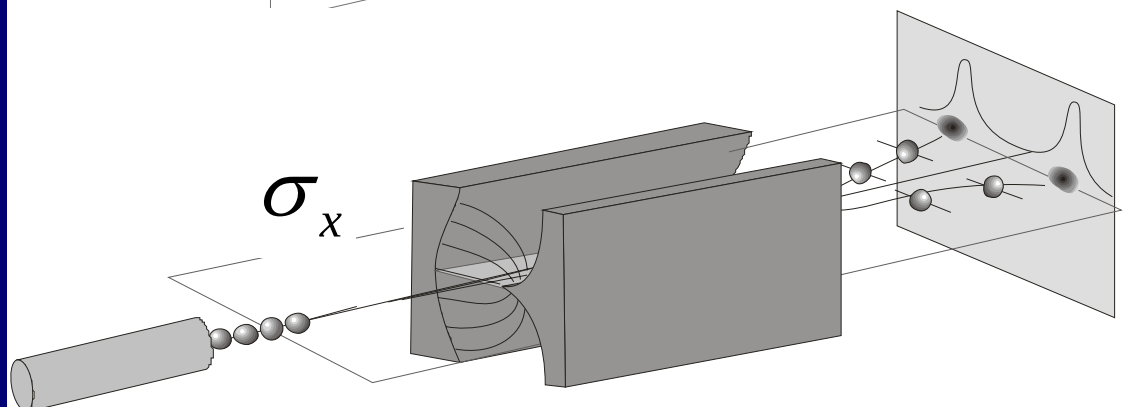




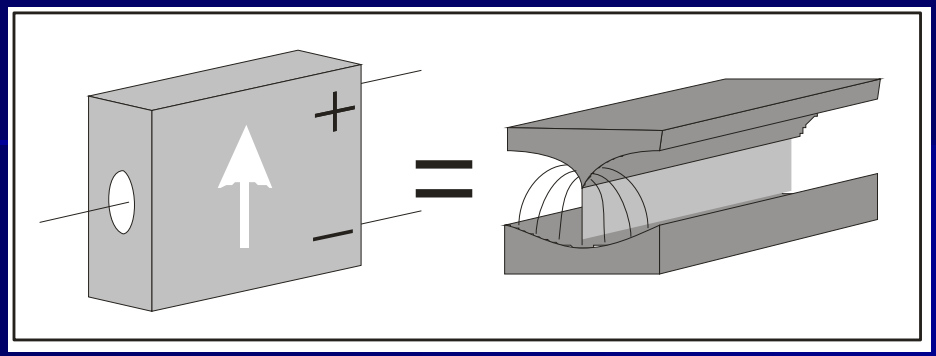
(古典的な) 棒磁石

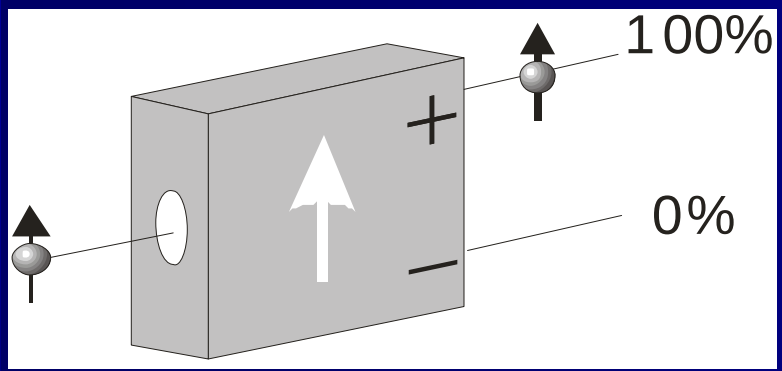
スピン1/2の粒子

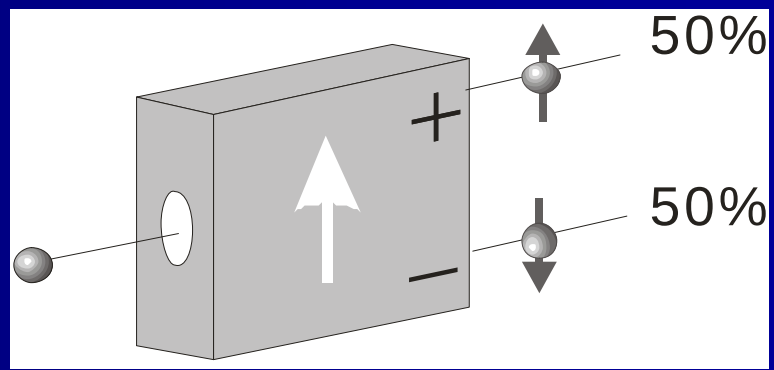




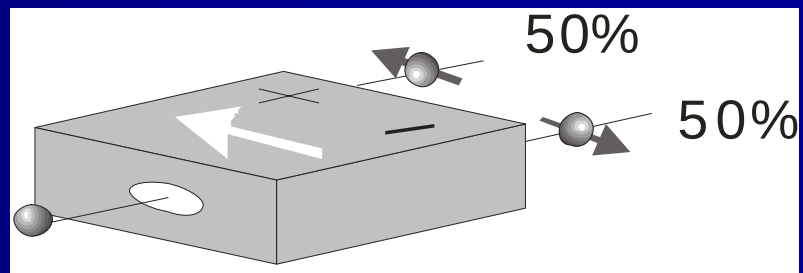
シュテルン・ゲルラッハ装置







スピンのZ成分を測定

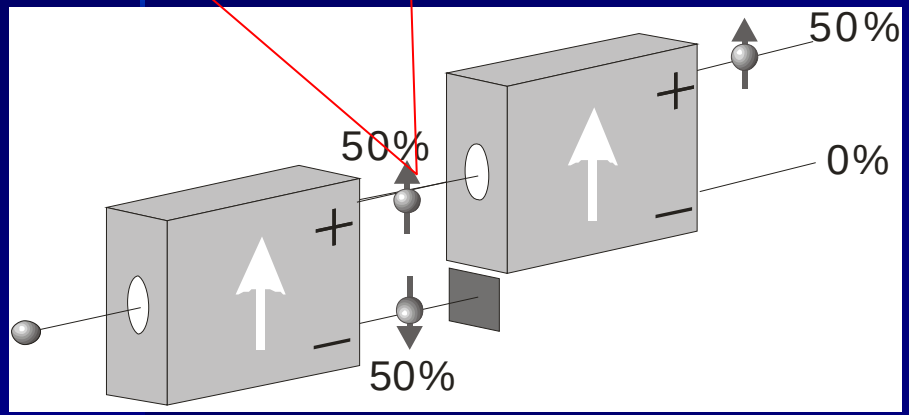


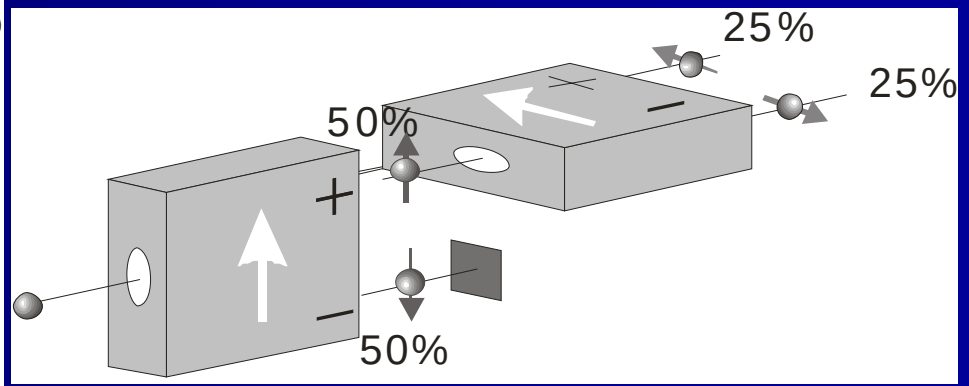
スピンのX成分を測定

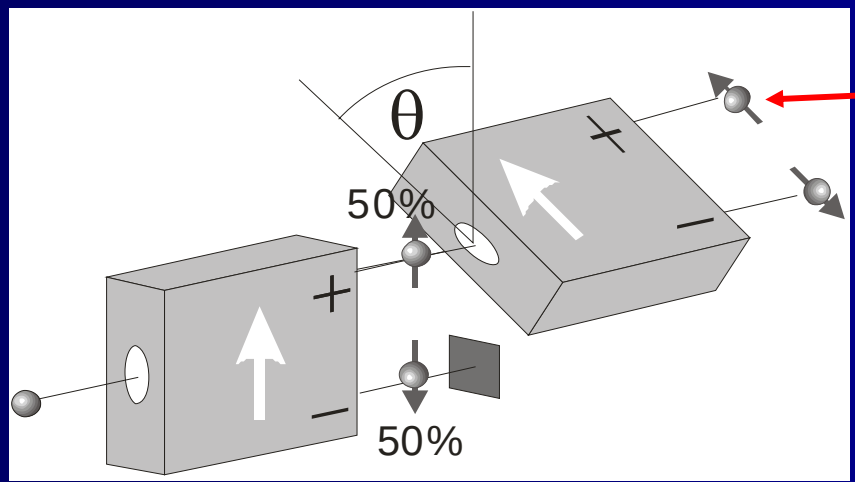
測定による状態の確定（状態の収縮）

スピンのZ成分を測定して上向きスピンであることが確定した状態

測定によって状態が準備される

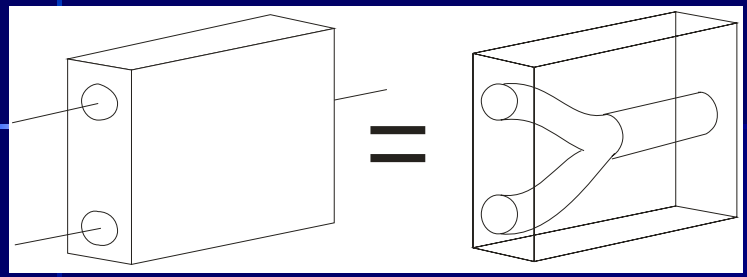




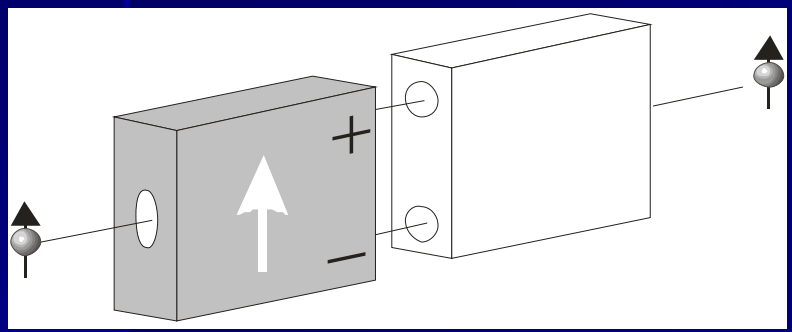


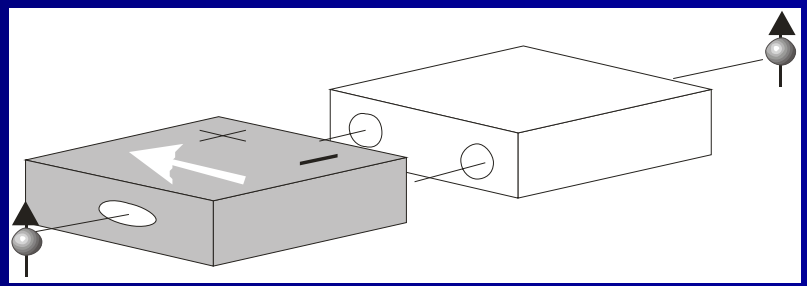
$$P_+(\theta) = \frac{1+\cos\theta}{2}$$

合流装置と干渉計



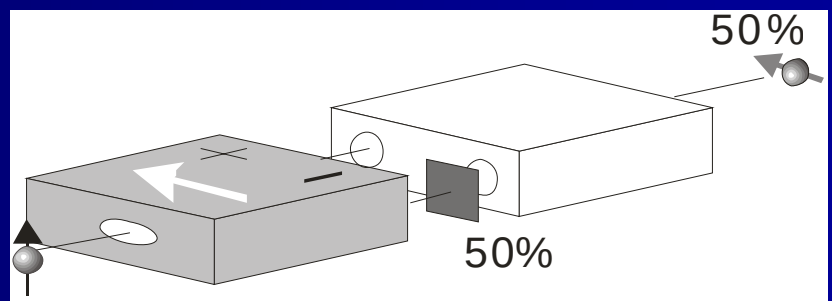
シュテルン･ゲルラッハ装置の出力を合流させる



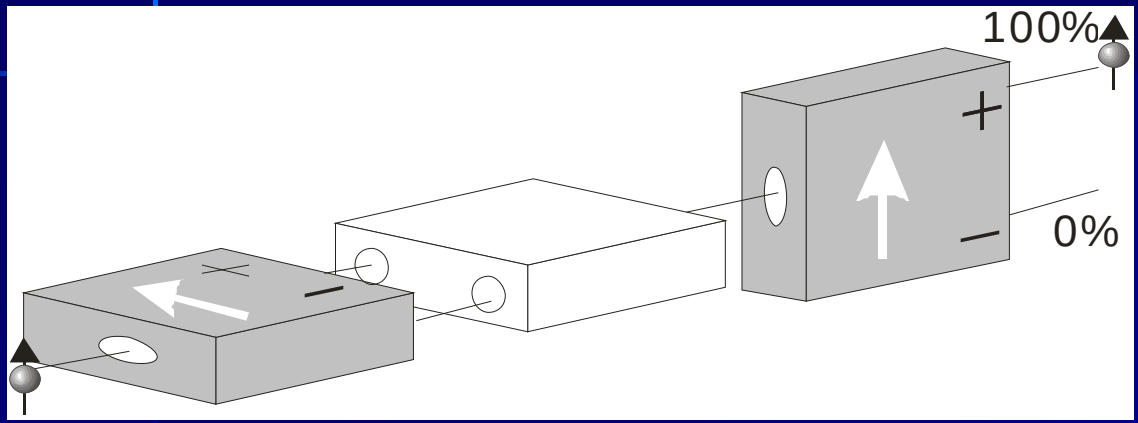


観測せずに合流させれば何もしなかったのと同じ
（どちらの経路を通ったかの情報がない場合）

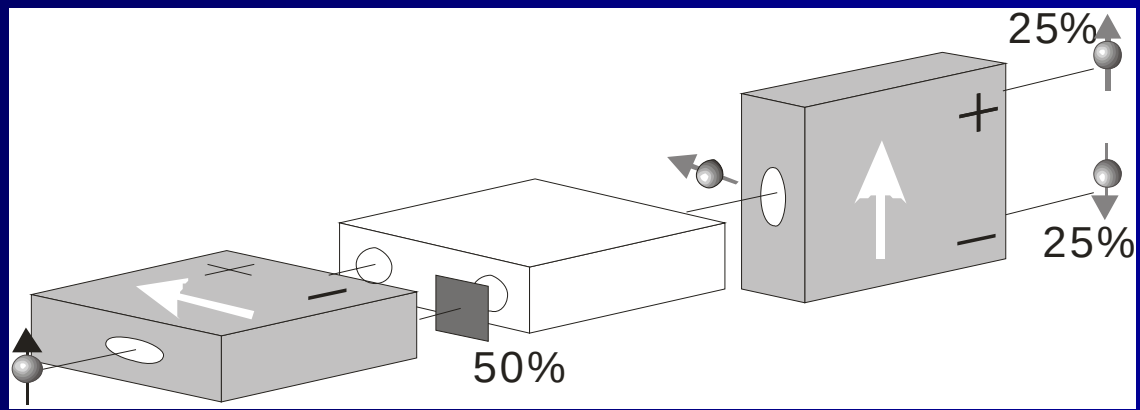
出力の一方を塞ぐと



干渉計の出力

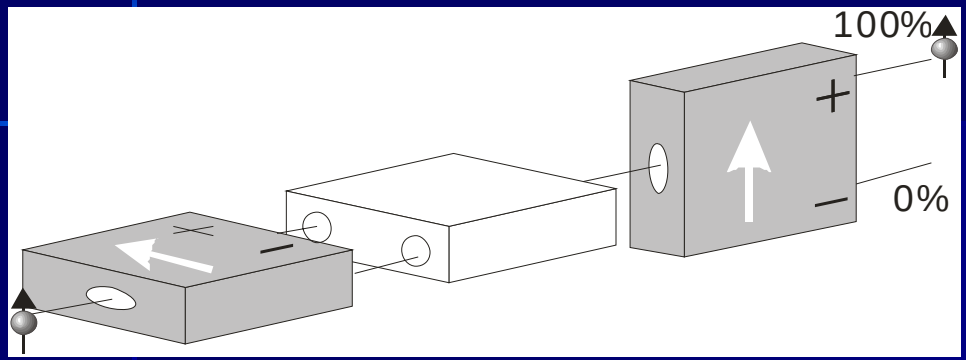


観測せずに合流させれば
何もしなかったのと同じ
ー側に現われる確率は0



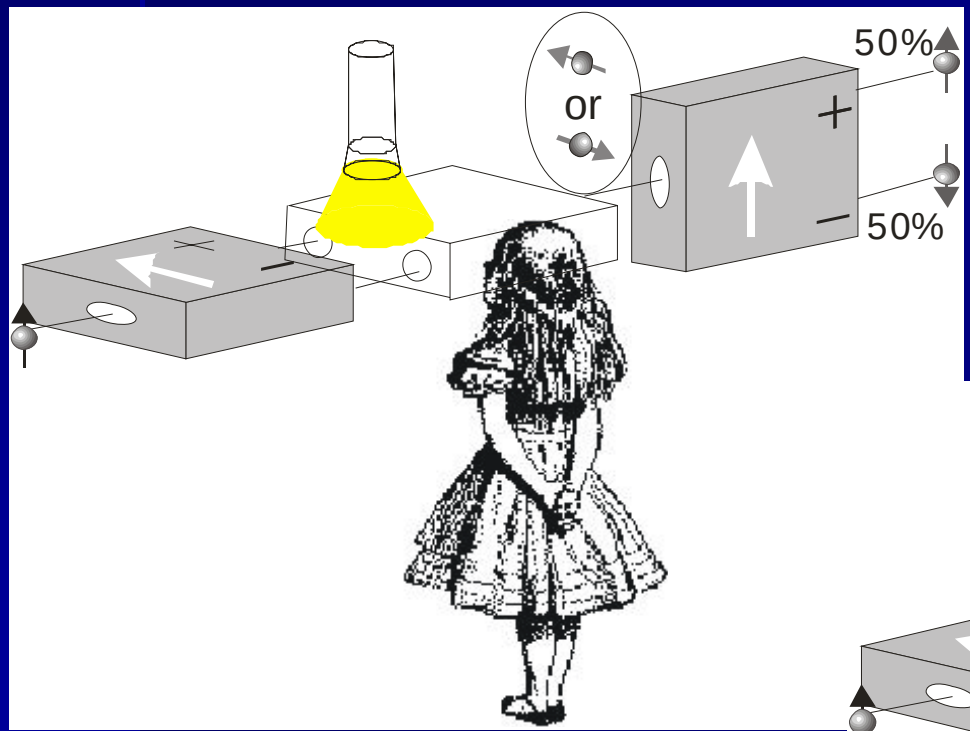
経路の一方を塞ぐことによってー側に現われる確率が0%から25%に増加する

観測によるデコヒーレンス

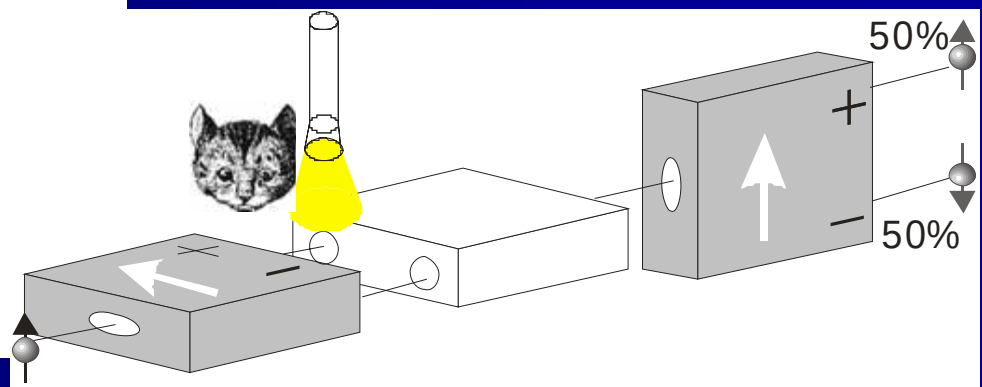


$$|\uparrow\rangle = \frac{1}{\sqrt{2}}\left(|\leftarrow\rangle + |\rightarrow\rangle\right)$$

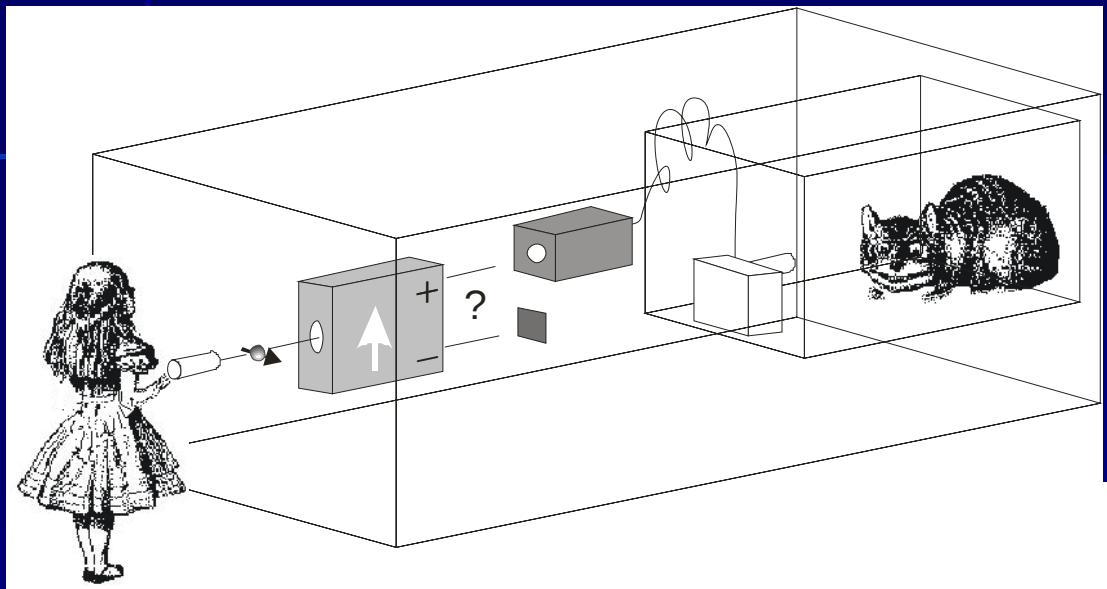
どっちの経路を通ったか観測すると干渉は起こらなくなる



片側の経路のみを観測する場合でも，「どっちの経路」の情報が得られるなら同じ

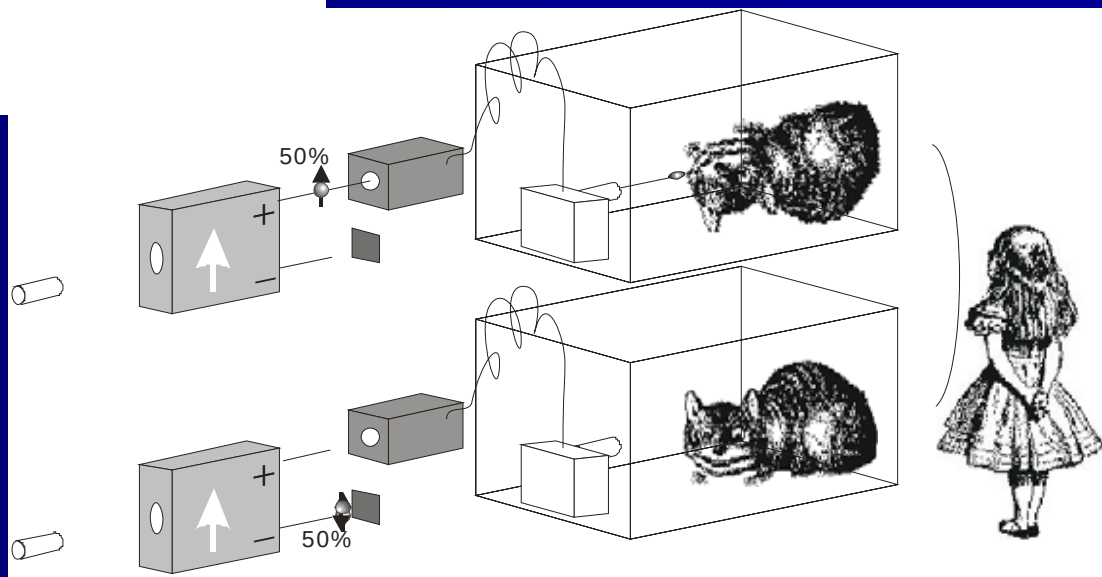


シュレーディンガーの猫



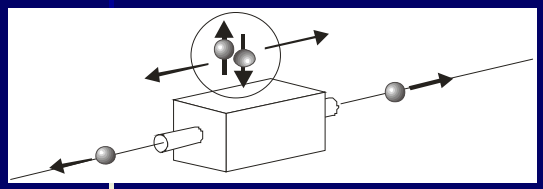
上向きスピンが検出されると銃弾が発射されて猫が死ぬ

猫が生きている状態と死んでいる状態の重ね合わせ？？？



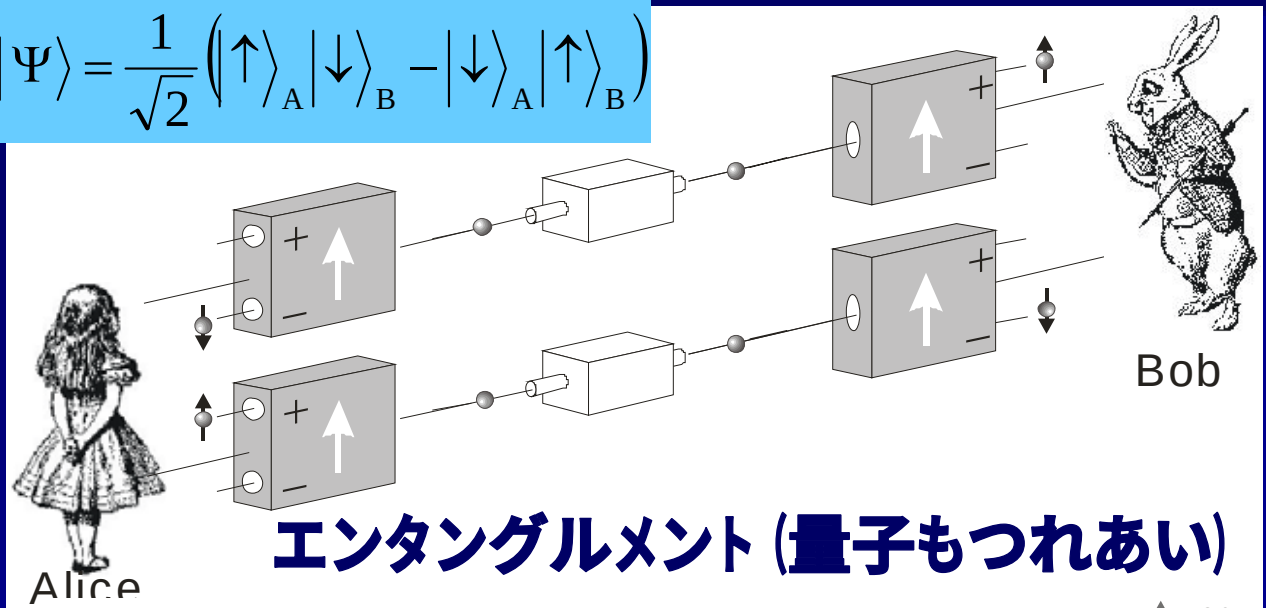
$$|\Psi\rangle = |\uparrow\rangle|\text{猫死}\rangle + |\downarrow\rangle|\text{猫生}\rangle$$

Einstein-Podolsky-Rosen(EPR)の実験



互いに逆向きのスピンをもつ2個の粒子

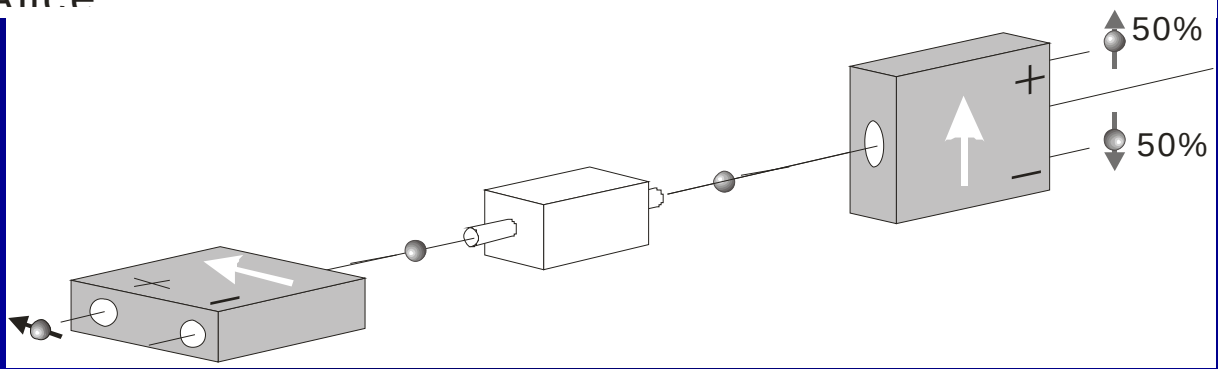
$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle_A|\downarrow\rangle_B - |\downarrow\rangle_A|\uparrow\rangle_B\right)$$



エンタングルメント（量子もつれあい）

アリスが↑を観測すればボブは↓を観測する．（測定結果に完全な相関がある）

アリスとボブが，互いに異なる向きのスピン測定をする場合は？（量子力学特有の相関：エンタングルメント）



遠く離れたアリスの測定がボブの測定結果に影響を及ぼす？？

ベル (Bell) の不等式

どの向きのスピン測定がなされるか粒子にはわからない
それぞれの測定に対する結果が「隠れた変数」によってあらかじめ決まっているとする考え方（「**局所実在論**」）によれば

$F \equiv \sigma_z^{\mathrm{A}}\sigma_z^{\mathrm{B}} + \sigma_y^{\mathrm{A}}\sigma_y^{\mathrm{B}} + \sigma_y^{\mathrm{A}}\sigma_z^{\mathrm{B}} - \sigma_z^{\mathrm{A}}\sigma_y^{\mathrm{B}}$ という量を考えると

$-2 \le \langle F \rangle \le 2$ というベルの不等式が成立するはず

A	z	+	+	+	+	+	+	+	+	−	−	−	−	−	−	−	−
A	y	+	+	+	+	−	−	−	−	+	+	+	+	−	−	−	−
B	z	+	+	−	−	+	+	−	−	+	+	−	−	+	+	−	−
B	y	+	−	+	−	+	−	+	−	+	−	+	−	+	−	+	−
F		2	2	-2	-2	-2	2	-2	2	2	-2	2	-2	-2	-2	2	2

量子力学によれば，ある条件ではベルの不等式が破れる

アスペ (Aspect)の実験（スピンの替わりに光子の偏光を用いたもの）によりベルの不等式が破れることが実証されている．

暗号について

暗号の必要性

- 情報通信におけるセキュリティ
  - インターネットショッピングにおけるクレジットカード番号のやりとり
  - 情報の正当性の認証（本人確認）
- 盗聴への対処
  - 「データは盗聴される」ことを前提としてセキュリティを考える ⇒ **暗号化** (cryptography)
  - 送りたいデータ列と同じ長さの乱数列を一回限り使って暗号化したものは解読不可能

    ⇒　送信者と受信者が必要な長さの乱数列を（他人に知られずに）共有できればよい **(秘密鍵配信)**

クイズ

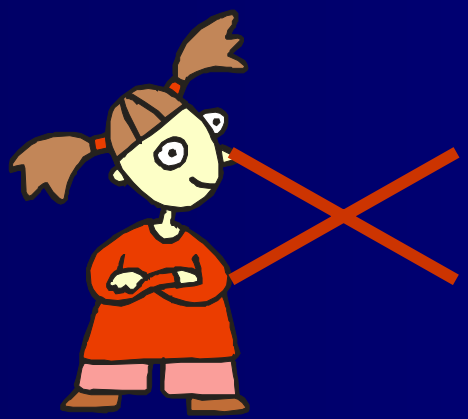
- ある国では郵便配達を泥棒たちが請け負っている．彼らは鍵のかかっていない小包は何でも勝手に開けて中身を盗ってしまう．ただし鍵がかかっているものには手を出さない．この国でボブが婚約者のアリスに指輪を送ろうとしている．どうやったら安全に送り届けることができるだろうか？
- しっかりした箱に錠前をつけて送れば途中で盗まれることはないが，アリスはその鍵を持っていないから箱を開けることができない．錠前はどこでも買うことができるが，買った錠前の鍵は自分の手もとにあって，相手は持っていない．鍵を別の郵便で送ることも考えられるが，鍵をかけた郵便ででも送らない限り，やはり途中で盗られてしまう．
- 困り果てたボブは電話でアリスに相談した．アリスはとてもうまい方法を考えついた．錠前をいくつでもつけられる箱で送ってもらうことによって，無事にボブからの指輪を受け取ることができた．いったいどうやったのだろう？

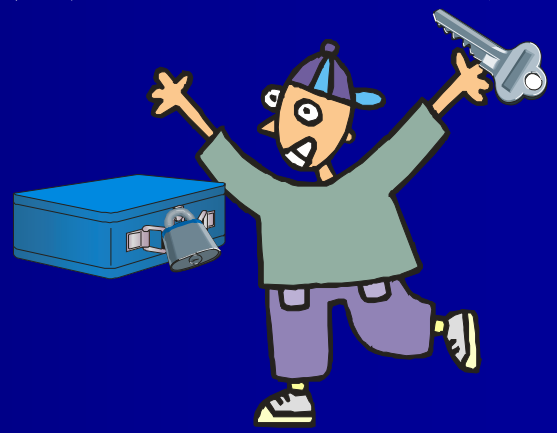
ボブはアリスに指輪を送りたい

アリス

ボブ

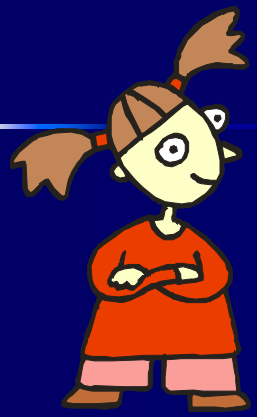
①ボブは錠前をつけた箱に指輪を入れてアリスに送る

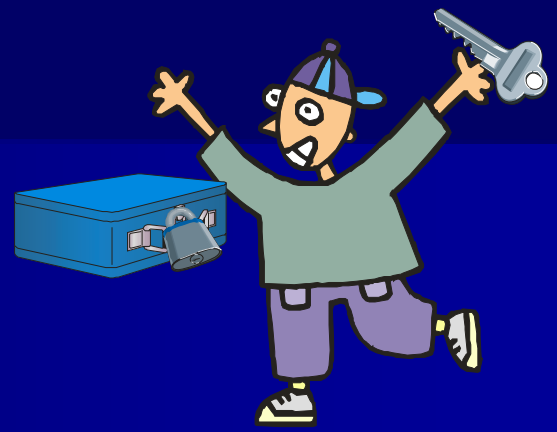




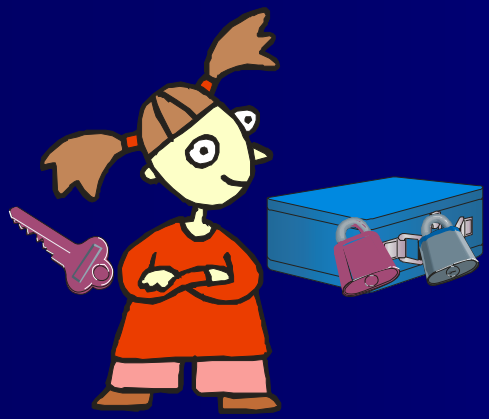
でも，アリスは鍵を持っていないので錠前を開けられない

①ボブは指輪を錠前をつけた箱に入れてアリスに送る





②アリスは自分の錠前をかけてボブに送り返す



③ボブは最初にかけた錠前を自分の鍵で外して，アリスに送る

④アリスは自分の鍵で錠前を開けて無事に指輪を受け取ることができる

暗号とは

伝えたい情報の文章（平文（plain text））をある規則によって暗号文(cypher text)に変換する．

⇒ 鍵をかけるのと同じ

通信したい相手のみが暗号文を元の平文に戻すことができ，他の人にはできないようにする．

⇒ 鍵を持っていない人には開けられない
通信したい相手にだけ鍵を渡す

問題はいかにして安全に鍵を渡すか

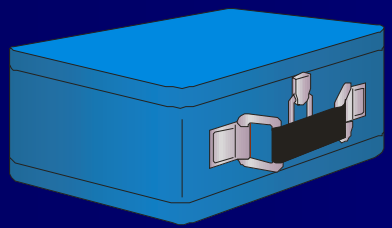
アリスがボブに出すラブレターがイヴに読まれないように暗号化して送る

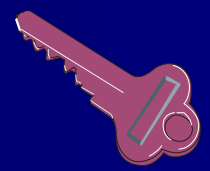
通信したい2人だけが秘密鍵を持っていれば2人の間の通信は安全

しかし，秘密鍵は電話やインターネットなど公共通信で送るわけにはゆかない．

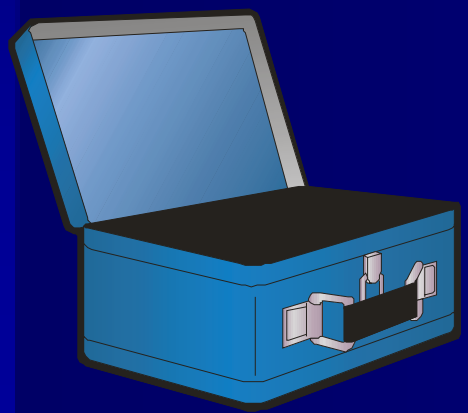
また，通信する2人の組ごとに秘密鍵を決めなければならない．

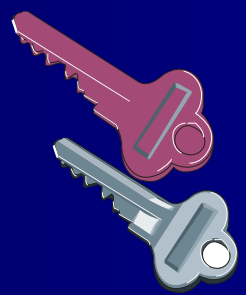
こんな鍵があったら





鍵をかけるときは**紫の鍵**（誰でも持っている）だけでよい

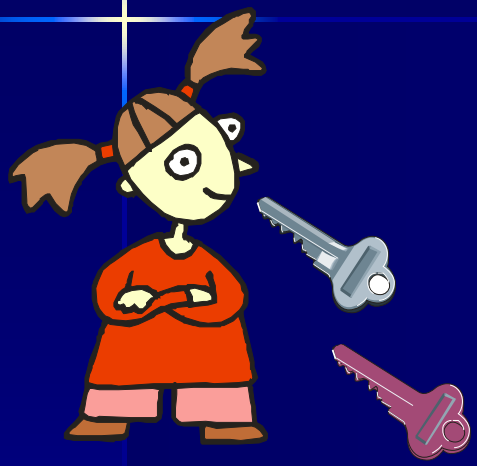


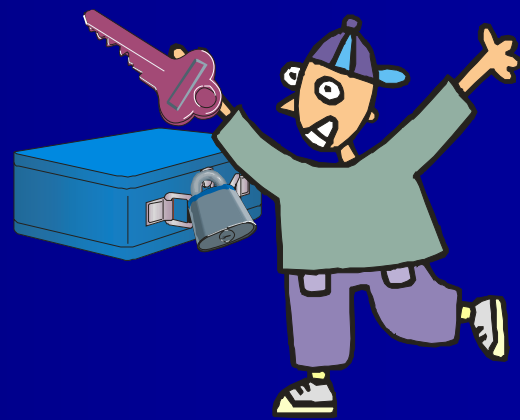


鍵を開けるには**紫の鍵**と**銀色の鍵**（本人しか持っていない）が両方必要

公開鍵暗号

暗号化する鍵は公開してしまう.





暗号を復号化するにはもう一つの鍵 (秘密鍵) が必要.

公開鍵暗号

暗号化するのは1つの鍵でよいが，暗号を復号化するにはその鍵ともう一つの鍵が必要な暗号のやりかた．

① アリスは自分あての通信のための**公開鍵**と**秘密鍵**を決め，**公開鍵**のほうを一般に公開する．

② ボブは**アリスの公開鍵**を使って通信を暗号化してアリスに送る．

③ アリスは**自分の公開鍵**と**秘密鍵**を使ってボブからの暗号通信を復号化して読む

④ **秘密鍵**を持っていないアリス以外の人は暗号を解読することができない．

公開鍵と秘密鍵

公開鍵で閉めたものを秘密鍵で開けることができるわけだから，公開鍵と秘密鍵の間にはある関係がある．

公開鍵を公開しても，そこから秘密鍵が推測されてしまわないものでなければならない．

「ある方向には簡単だが，逆方向には難しい計算」を利用する： **素因数分解**

114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147147599290026879543541

=

349052951084765094914784961990389813341776463849338784399082057 7

×

327691329926670954996198819083446141317764296799294253997828853 3

公開鍵暗号（ＲＳＡ暗号）（1）

ボブは公開鍵と秘密鍵を設定する．

(1) ボブは2つの素数を適当に選ぶ。ここでは p = 5, q = 11 を選んだとする．

(2) 選んだ2つの数字をかけ算した結果，n = p×q = 55を計算する．これは公開鍵の一部になる。

(3) 次に，(p-1)×(q-1)＝4×10＝40 と互いに素になる数 e を適当に選定する。ここでは e=7 を選ぶ．

この e = 7 と n = 55 とがボブの公開鍵となる．

(4) 次に秘密鍵を計算する。d×e = 1 mod(p-1)(q-1) となる d，つまり(p-1)(q-1)で d×e を割ったときに余りが1となるような d を選ぶ．(p-1)(q-1) = 40, e = 7だから，例えば d = 23 とすればよい．　（d×e = 23×7 = 161であり，確かに40で割れば余りは 1 である．）　**この d がボブの秘密鍵となる．**

公開鍵暗号（ＲＳＡ暗号）（2）

アリスが暗号文を作る.

（1）アリスは例えば Ｍ＝“2”という数字を暗号化してボブに送信しようとする. 暗号化メッセージＣはボブの公開鍵 e と n を使って,

$C = M^e \pmod{n} = 2^7 \pmod{55} = 128 \pmod{55} = 18$

というように作られる. ボブはこれをアリスに送信する.

ボブがその暗号文を復号化する.

（2）アリスから18, というメッセージを受け取ったボブは, 持っている秘密鍵 d（および n）を使って次のように復号化を行う.

$M = C^d \pmod{n} = 18^{23} \pmod{55} = 2$

このようにしてアリスが送りたかったメッセージ”2”を得ることができる.

量子コンピューター

量子コンピューター

量子コンピューターは古典コンピューターに取って代わるようなものではない

ある種の問題については量子コンピューターは古典コンピューターよりもはるかに高速な計算ができる

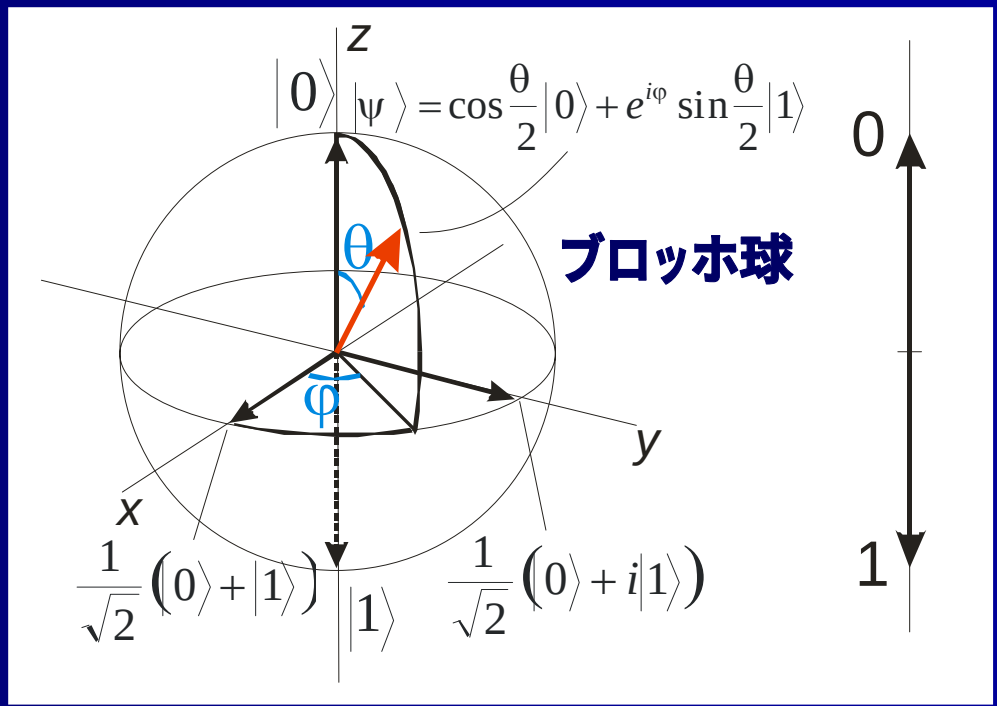
- データベース検索に関するグローバー (Grover)のアルゴリズム
- 素因数分解に関するショア (Shor) のアルゴリズム
  ⇒ 公開鍵暗号が破れる？

量子ビット (qubit)

【古典ビット】　2つの状態 0，1 のどちらかをとる

【量子ビット】　2つの状態，$|0\rangle$，$|1\rangle$ の任意の重ね合わせ

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$



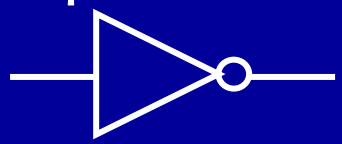
N個の量子ビットで 2^N 個の状態の重ね合わせを実現することができ，2^N 個の入力値に関する並列計算ができる

量子コンピューター：　重ね合わせとエンタングルメントを利用して古典コンピューターでは不可能な計算を行う

論理ゲート

古典コンピューターの論理演算

NOTゲート



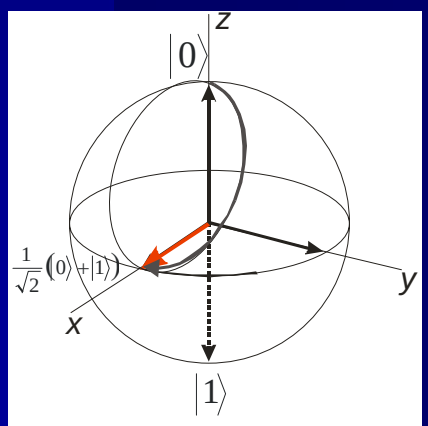
ANDゲート

$\|a\rangle$	$\|b\rangle$	$\|c\rangle$	$\|d\rangle$
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

量子コンピューターの論理演算

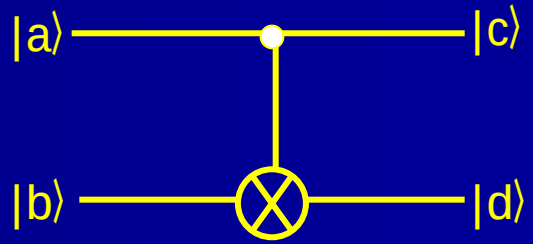
アダマール･ゲート

$$|0\rangle \Rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$



重ね合わせ状態を準備する

制御NOTゲート



入力：　$|a,b\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)|0\rangle$

出力：　$|c,d\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right)$

エンタングル状態をつくる

量子コンピューター実現のための条件

- 量子ビットの初期化ができること
- 量子ビットの読み出しができること
- 基本ゲート（アダマール・ゲートと制御NOT）が構成できること
- 量子ビットの数が増やせる（スケーラブルである）こと
- 演算時間に比べてデコヒーレンス時間が十分に長いこと（「環境」からの隔離）

量子ビットの候補

古典ビットは物理的にはいろいろな形で実現されている

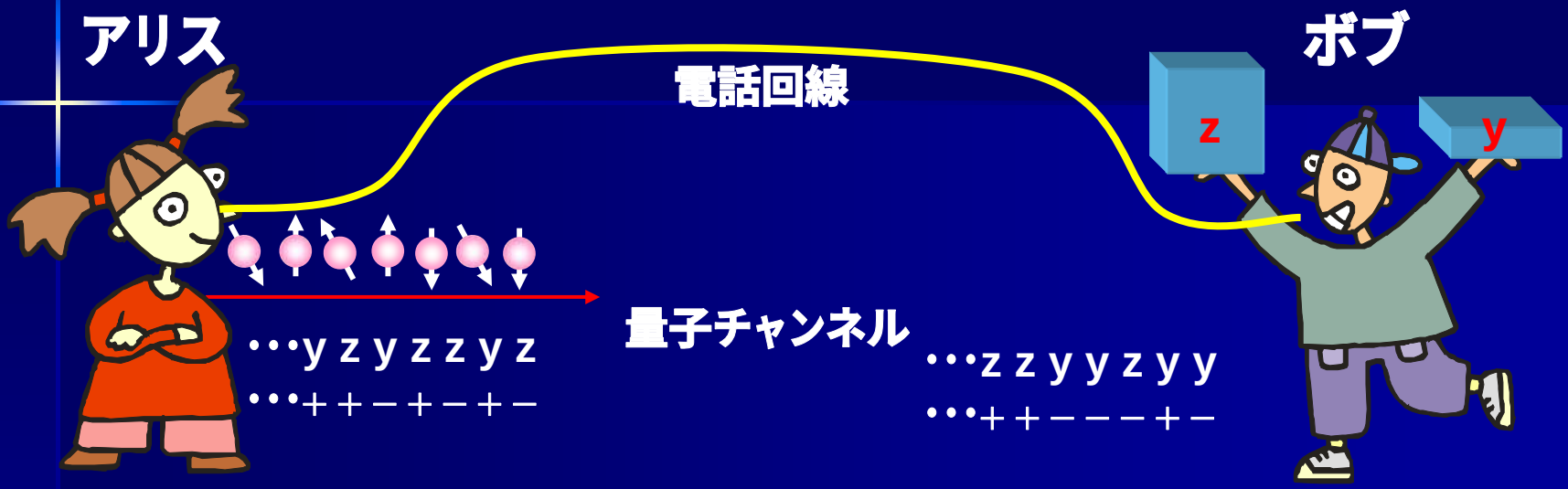
電圧の高低，光のon/off，磁化の向き，電荷の有無，‥

量子2準位系ならばなんでも量子ビットの候補になり得る

光子
トラップされたイオン
微小共振器
量子ドット（電荷，スピン，核スピン）
超伝導量子ビット（ジョセフソン接合）
核磁気共鳴（分子の核スピン）
ヘリウム液面電子

量子暗号（秘密鍵配信）

量子暗号（秘密鍵配信）



アリス側設定	・・・y z y z z y z
測定値	・・・＋＋－＋－＋－
ボブ側設定	・・・z z y y z y y
測定値	・・・＋＋－－－＋－
	・・・×○○×○○×
採用コード	・・・ 1 0　0 1

盗聴されていた場合

・・・z z y y z y y
・・・＋＋＋－－＋－

採用コードの一部を使って検証することにより盗聴を発見できる

量子暗号（秘密鍵配信）

・アリスはボブにスピンの向きが（↑，↓，→，←）のどれかをランダムに向いた粒子を次々に送る（量子チャンネル）．
・ボブは次々にやってくる粒子に対して，スピンのz成分またはy成分をランダムに選んで測定してその測定結果を記録する．
・一連の測定が終わった後，アリスとボブは古典チャンネルで連絡をとり，設定のみを伝える（測定値は秘密にしておく）．
・互いの設定が一致していた場合のデータのみを採用する．
・盗聴が行われていないかを検証するために，その一部の答え合わせをする．
・盗聴によって量子状態が乱されていれば完全な相関が成立していないので，それとわかる．
（盗聴者には設定がわからないので確率1/2で間違った設定をする）

アリスの設定	z	y	z	z	y	z	y	y	z	y	・・・
スピンの値	＋	−	−	＋	＋	＋	−	−	−	＋	・・・
ボブの測定	y	z	z	y	y	z	y	z	z	y	・・・
スピンの値	−	−	−	−	＋	＋	−	−	−	＋	・・・
設定の一致	×	×	○	×	○	○	○	×	○	○	・・・
秘密鍵			0		1	1	0		0	1	・・・

まとめ

原子を操る，量子を操る

- 原子を見る，操る
  - STM, AFM, ナノサイエンス
- 巨視的量子現象
  - 量子液体，超流動ヘリウム
  - 原子気体のボース･アインシュタイン凝縮
- 量子情報処理
  - 暗号のしくみ
  - 量子コンピューター
  - 量子暗号 (秘密鍵配信)