量子計算量理論入門

Introduction to Quantum Computational Complexity

名古屋大学大学院情報学研究科
西村治道

2023年10月25日～27日

量子ビット(Qubit)

Mathematics of Quantum mechanics

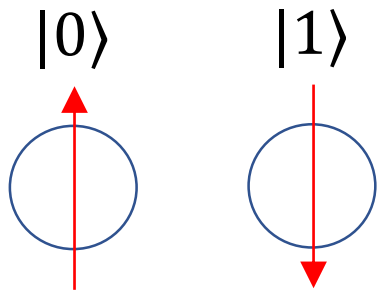
- 量子力学系(quantum mechanical system):＝複素内積空間（あるいはHilbert空間）
- 量子状態(quantum state):＝複素内積空間上の単位ベクトル

Mathematics of Quantum mechanics

- 量子力学系(quantum mechanical system):＝複素内積空間（あるいはHilbert空間）
- 量子状態(quantum state):＝複素内積空間上の単位ベクトル
- ブラケット表記(bra-ket notations; Dirac notations)
  - 縦ベクトル $|\psi\rangle$
  - 横ベクトル $\langle\varphi|$
  - 内積(inner profuct) $(|\varphi\rangle, |\psi\rangle) = (|\varphi\rangle)^{\dagger}|\psi\rangle = \langle\varphi|\psi\rangle$

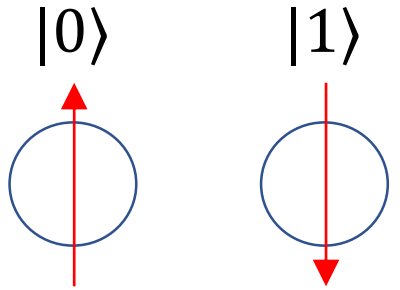
量子ビット(quantum bit, qubit)

- 通常の情報の最小単位はビット 0 & 1
- 量子力学系を基にした情報（量子情報: quantum information）の最小単位は**量子ビット(quantum bit/qubit)**
- 量子ビットは２つの基底状態を持つ量子力学系で実現可能
  - 原子核のスピン（up, down）
  - 光の偏光（縦偏光，横偏光）



量子ビット(quantum bit, qubit)

- 通常の情報の最小単位はビット０＆１
- 量子力学系を基にした情報（量子情報: quantum information）の最小単位は量子ビットと呼ばれ，複素2次元の単位ベクトルで表現される.
- 量子ビットは2つの基底状態を持つ量子力学系で実現可能
  - 原子核のスピン（up, down）
  - 光の偏光（縦偏光，横偏光）
- 数学的には**複素2次元空間上の単位ベクトル**で表現される

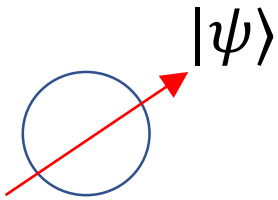


$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

直交

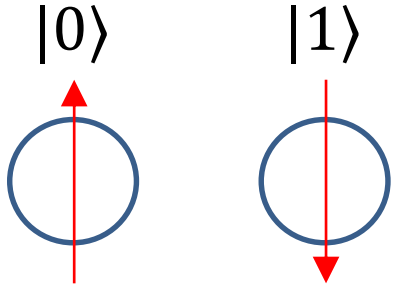
$$|\psi\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$$

（確率）振幅
(probability) amplitude



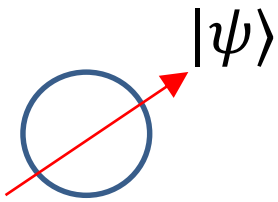
量子ビット(quantum bit, qubit)

- 通常の情報の最小単位はビット０＆１
- 量子力学系を基にした情報（量子情報: quantum information）の最小単位は量子ビットと呼ばれ，複素2次元の単位ベクトルで表現される.
- 数学的には**複素2次元空間上の単位ベクトル**で表現される
- **重ね合わせの原理(superposition principle)**：＝量子状態と量子状態を足し合わせた（重ね合わせた）ものはやはり量子状態



$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \Longrightarrow |\psi\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$$

直交



量子状態の位相因子(phase factor)

- $|\psi\rangle$と$e^{i\theta}|\psi\rangle$は数学的には異なるベクトルであるが同一の量子状態を表す
- $e^{i\theta}$は**位相因子（phase factor）**と呼ばれる
  - θは位相と呼ばれる

Global phase vs Relative phase

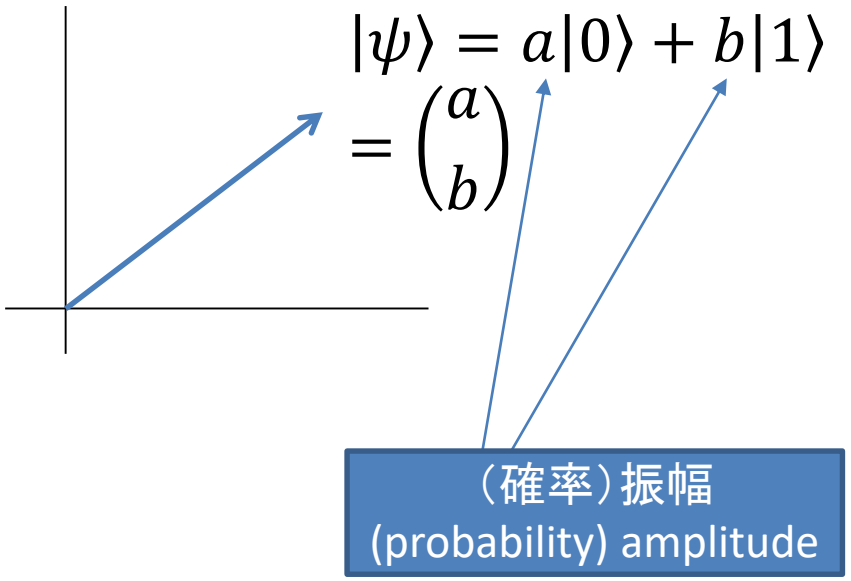
- $|\psi\rangle$と$e^{i\theta}|\psi\rangle$は数学的には異なるベクトルであるが同一の量子状態を表す
  - θは**絶対位相（global phase）**と呼ばれることがある
- $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}|1\rangle\right)$はすべての$\theta \in [0,2\pi)$について異なる状態
  - θは**相対位相（relative phase）**と呼ばれることがある

Mathematics of Quantum mechanics

- 量子力学系:＝複素内積空間（あるいはHilbert空間）
- 量子状態:＝複素内積空間上の単位ベクトル
- 時間発展(time evolution):=ユニタリ作用素(unitary operator)
- 測定(measurement):=射影作用素(projection)

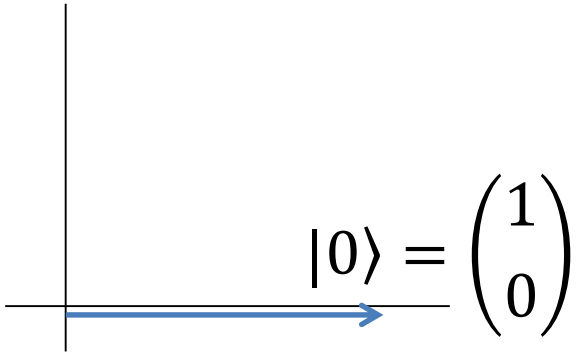
量子ビットの測定(measurement)

- 最も基本的な測定＝**計算基底(computational basis)** $\{|\mathbf{0}\rangle, |\mathbf{1}\rangle\}$による射影

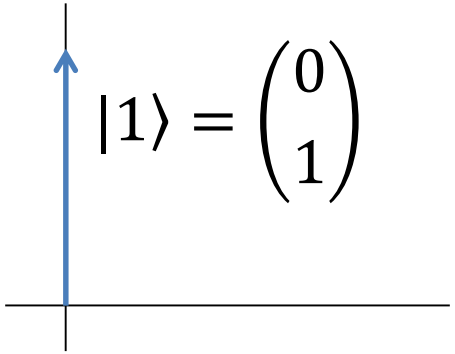


測定

測定値0を確率 $|a|^2$で得る

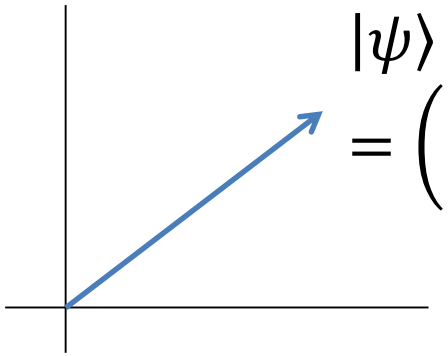


測定値1を確率 $|b|^2$で得る



量子ビットの測定(measurement)

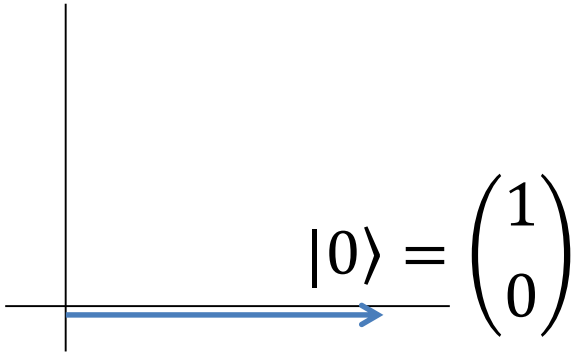
- 最も基本的な測定＝**計算基底(computational basis)**による射影



$$|\psi\rangle = a|0\rangle + b|1\rangle$$
$$= \begin{pmatrix} a \\ b \end{pmatrix}$$

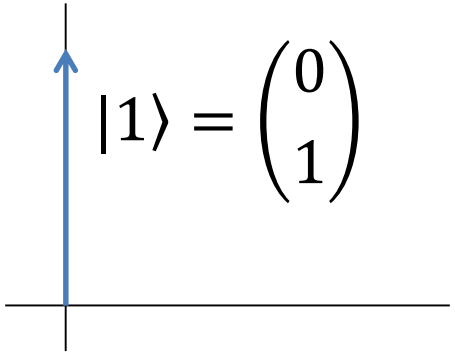
測定

測定値0を確率 $|a|^2$で得る



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

測定値1を確率 $|b|^2$で得る

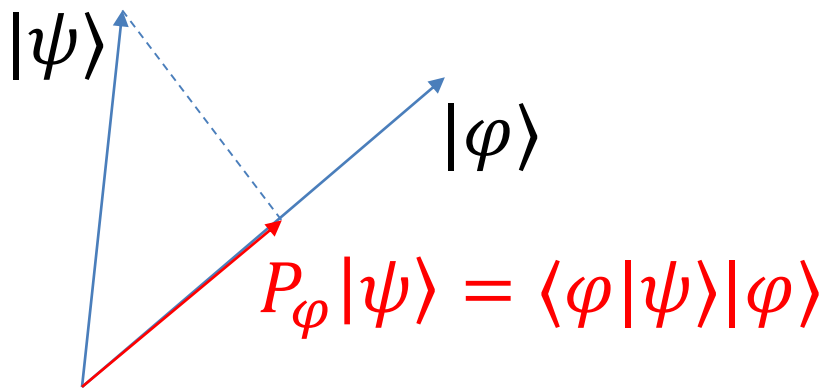


$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Points:
- 測定によって状態は変化する
  - 測定後は射影先の状態（$|0\rangle$ ないし$|1\rangle$）に変化

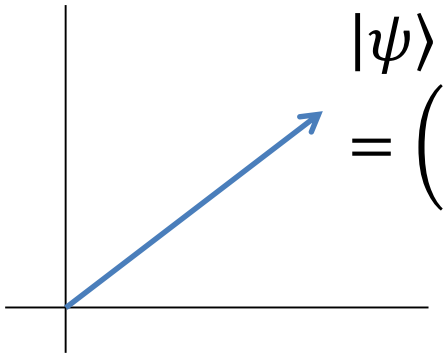
射影(projection)

- ベクトル$|\psi\rangle$をベクトル$|\varphi\rangle$の方向（$|\varphi\rangle$の張る1次元空間）へ射影P_φを取ると，ベクトル$P_\varphi|\psi\rangle = (|\varphi\rangle, |\psi\rangle)|\varphi\rangle$が得られる



量子ビットの測定(measurement)

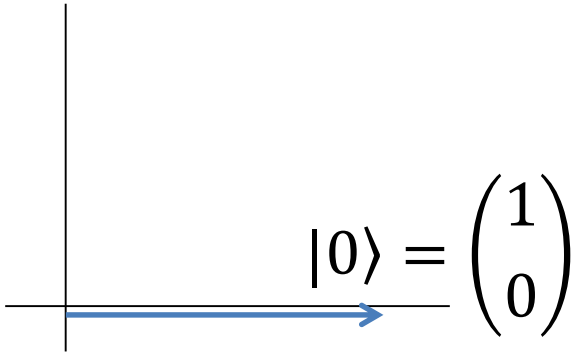
- 測定は射影(projection)によって表現できる



$$|\psi\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$$

測定

測定値0を確率 $|a|^2 = |\langle 0|\psi\rangle|^2$ で得る



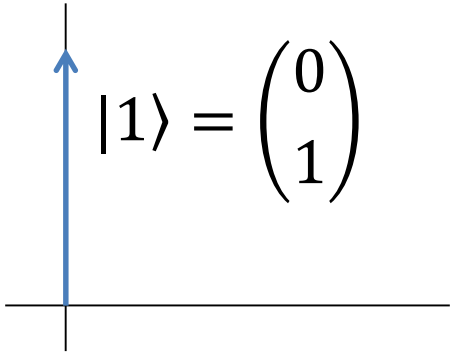
$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$|0\rangle$方向への射影P_0をとったベクトル

$$P_0|\psi\rangle = \langle 0|\psi\rangle|0\rangle$$

の長さの2乗

測定値1を確率 $|b|^2$ で得る



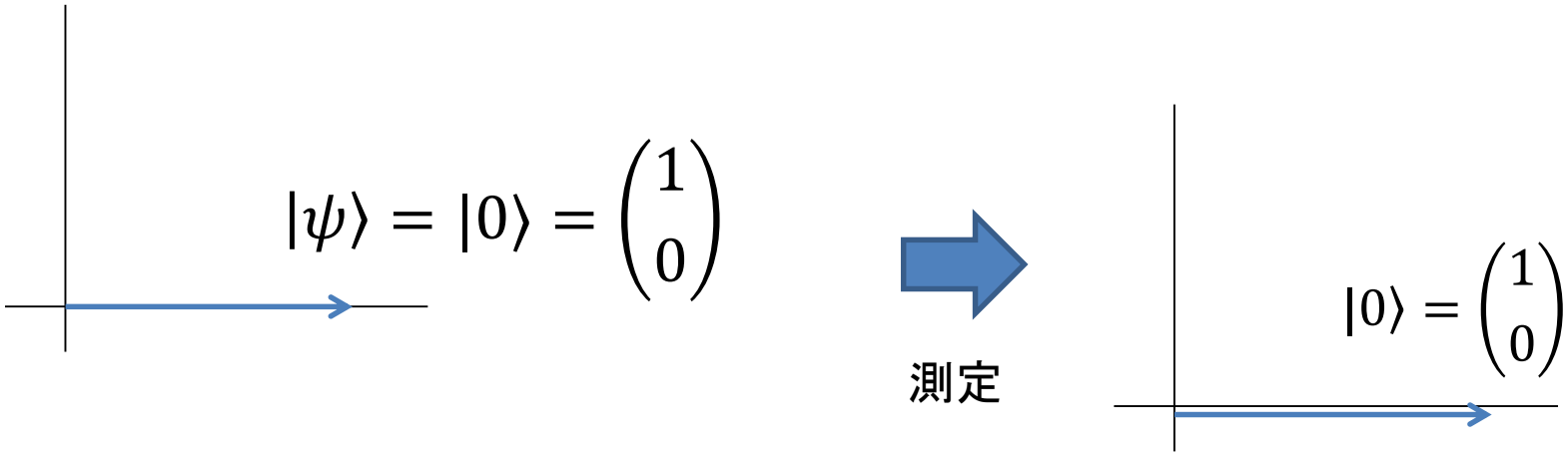
$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

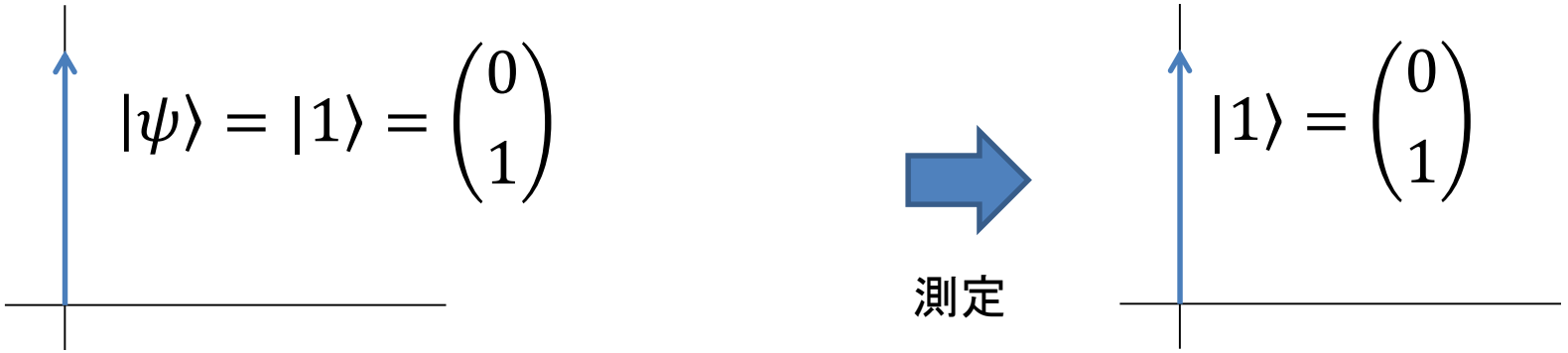
Points:

- 測定によって状態は変化する
  - 測定後は射影されたベクトルを正規化した状態($|0\rangle$ないし$|1\rangle$)に変化

量子ビットの測定(measurement)

- $|0\rangle$ と $|1\rangle$ は確実に識別可能





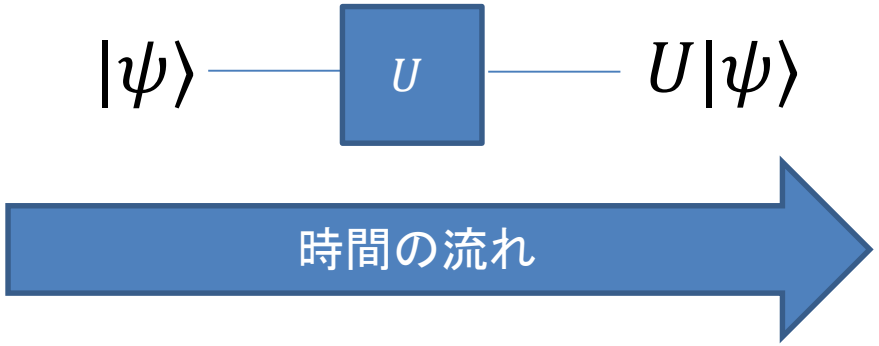
量子状態の位相因子(phase factor)

- $|\psi\rangle$と$e^{i\theta}|\psi\rangle$は数学的には異なるベクトルであるが同一の量子状態を表す
- どんな測定でも完全に識別不能

量子ビットの時間発展(time evolution)

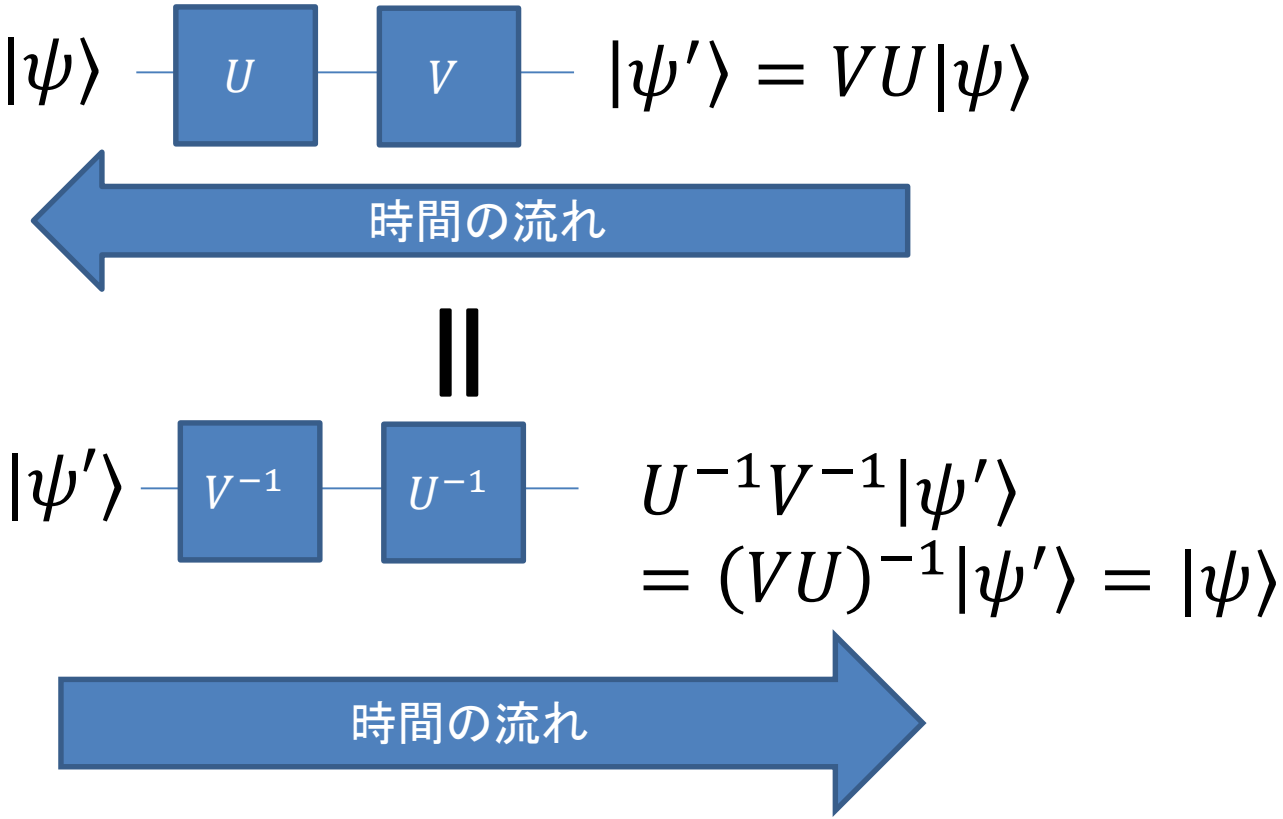
- 量子力学では時間発展はユニタリ(unitary)作用素
- Uがユニタリ作用素⇔$UU^\dagger = U^\dagger U = I$
  - $U^\dagger$はUの転置共役(transpose conjugate)

- **量子ゲート(quantum gate)**：＝量子ビットに施される時間発展



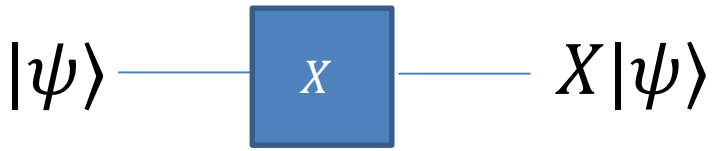
量子ゲートの可逆性

- 量子ゲートは可逆（invertible）
  - ユニタリUに対して$U^{-1} = U^{\dagger}$もユニタリなので時間発展として認められる操作



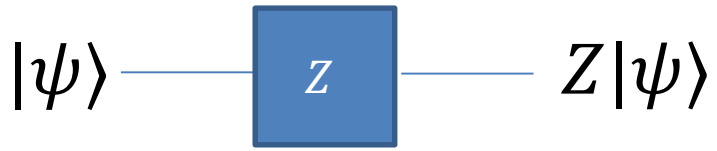
Example of quantum gates: NOT gate/X gate

- **NOTゲート/Xゲート** $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- $X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle$
- $\alpha|0\rangle + \beta|1\rangle$を$\alpha|1\rangle + \beta|0\rangle$に変化させる



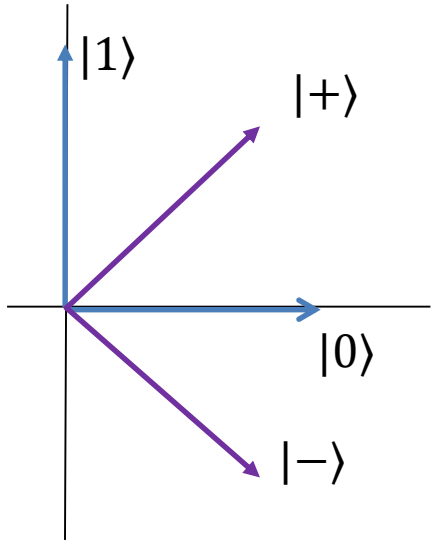
Z gate

- **Zゲート** $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
- $\alpha|0\rangle + \beta|1\rangle$を$\alpha|0\rangle - \beta|1\rangle$に変化させる



X gate vs Z gate

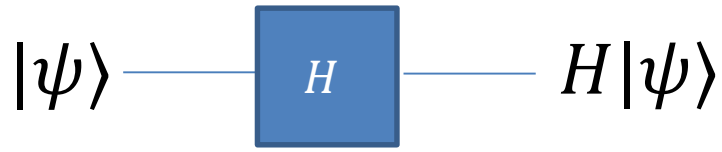
- Xゲートの固有状態(eigenstate)は$|+\rangle, |-\rangle$（X基底）
  - $X|+\rangle = |+\rangle$
  - $X|-\rangle = -|-\rangle$
- $|0\rangle, |1\rangle$はXゲートでたがいに移り合う
  - $X|0\rangle = |1\rangle$
  - $X|1\rangle = |0\rangle$
- Zゲートの固有状態は$|0\rangle, |1\rangle$（Z基底）
  - $Z|0\rangle = |0\rangle$
  - $Z|1\rangle = -|1\rangle$
- $|+\rangle, |-\rangle$はZゲートでたがいに移り合う
  - $Z|+\rangle = |-\rangle$
  - $Z|-\rangle = |+\rangle$

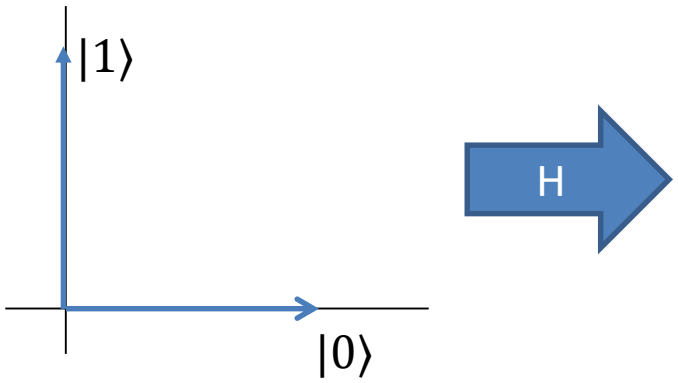


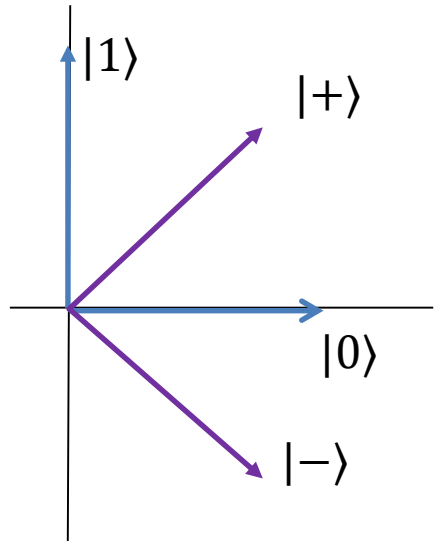
Hadamard gate

アダマール(Hadamard)ゲート $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

- $H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = |+\rangle$
- $H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = |-\rangle$
- $H|+\rangle = |0\rangle,\ H|-\rangle = |1\rangle$





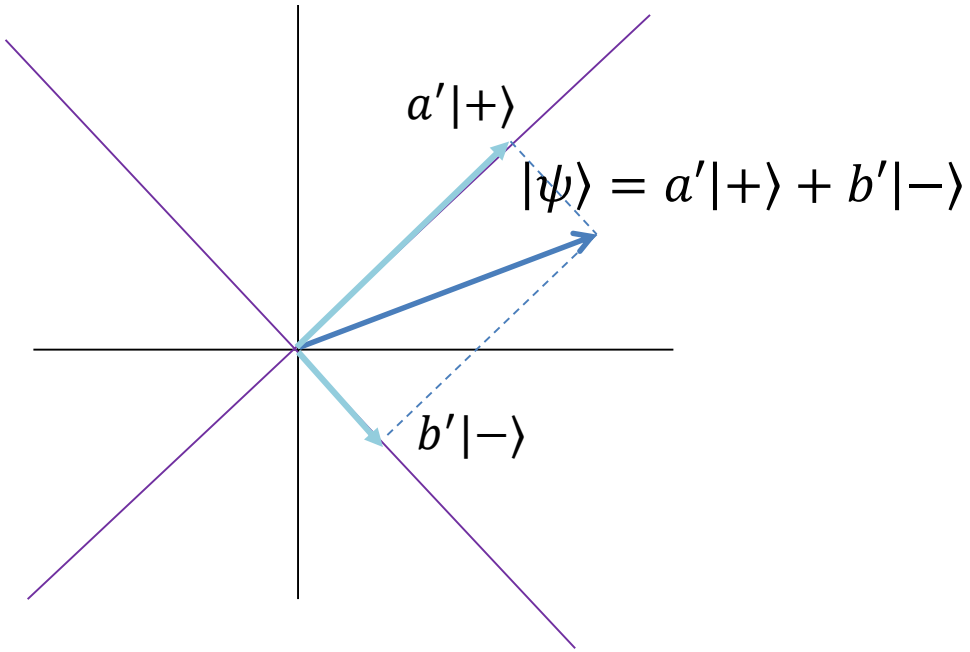


量子ビットの時間発展(time evolution)

- 量子力学では時間発展はユニタリ(unitary)
- 量子ゲート(quantum gate) : ＝量子ビットに施される時間発展
- 量子ゲートの例
  - NOTゲート $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
  - 位相(phase)ゲート$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
  - Hadamardゲート$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

量子ビットの測定(2)
Measurement in different basis

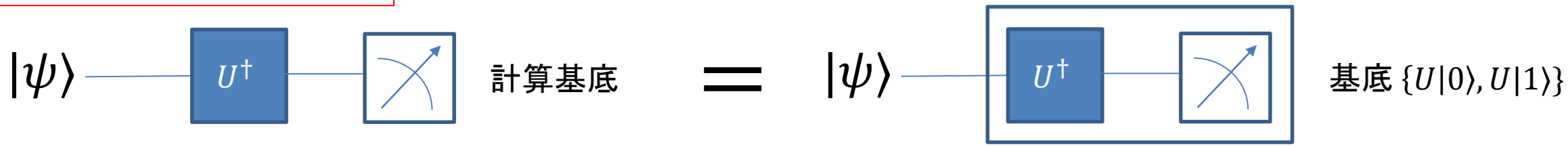
- 測定は基底 $\{|0\rangle, |1\rangle\}$（計算基底(Z基底)）への射影だけではない
- 時間発展Uと組合すことで基底$\{U|0\rangle, U|1\rangle\}$への射影による測定も実現可能



Measurement in different basis

- 測定は基底 $\{|0\rangle, |1\rangle\}$（計算基底: computational basis）への射影だけではない
- 時間発展Uと組合すことで基底$\{U|0\rangle, U|1\rangle\}$への射影による測定も実現可能

測定後の状態を考えなければ

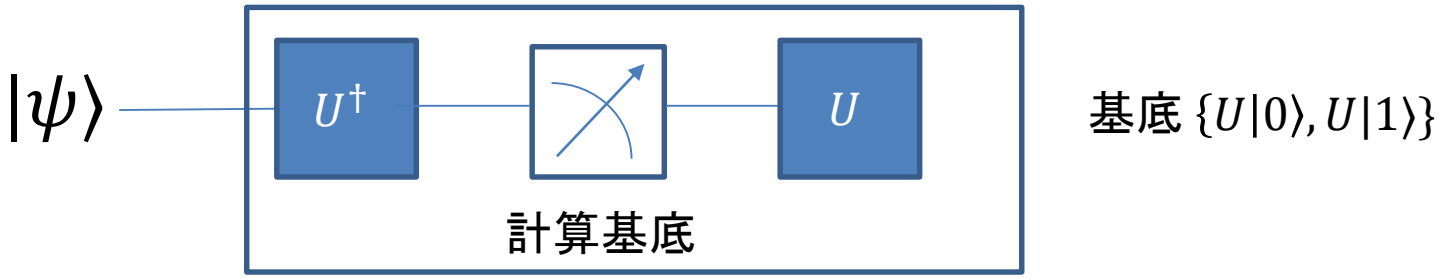


➢ $U|0\rangle$に対応する値を得る確率$= \left|\left(|0\rangle, U^\dagger|\psi\rangle\right)\right|^2 = |(U|0\rangle, |\psi\rangle)|^2$

Measurement in different basis

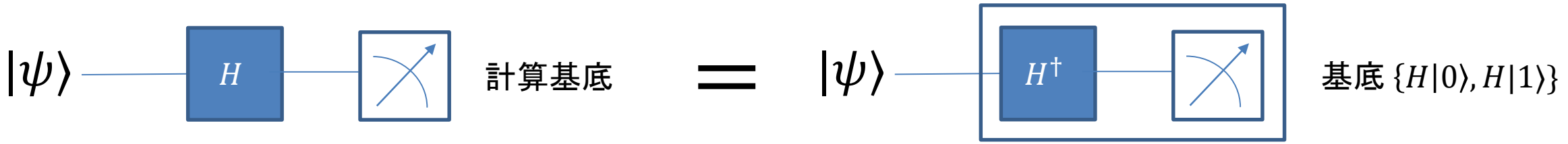
- 測定は基底 $\{|0\rangle, |1\rangle\}$（計算基底: computational basis）への射影だけではない
- 時間発展Uと組合すことで基底$\{U|0\rangle, U|1\rangle\}$への射影による測定も実現可能

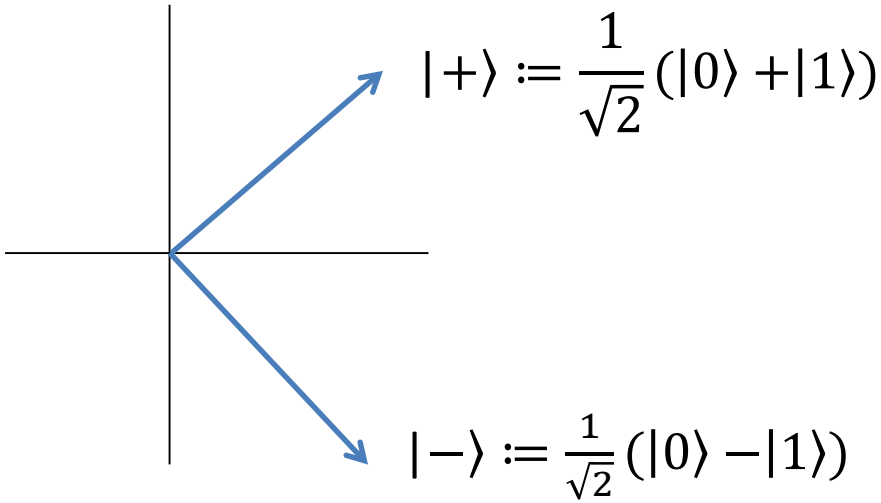
測定後の状態を考えると



Measurement in the X basis

- 測定は基底 $\{|0\rangle, |1\rangle\}$（計算基底: computational basis）への射影だけではない
- 時間発展Uと組合すことで基底$\{U|0\rangle, U|1\rangle\}$への射影による測定も実現可能

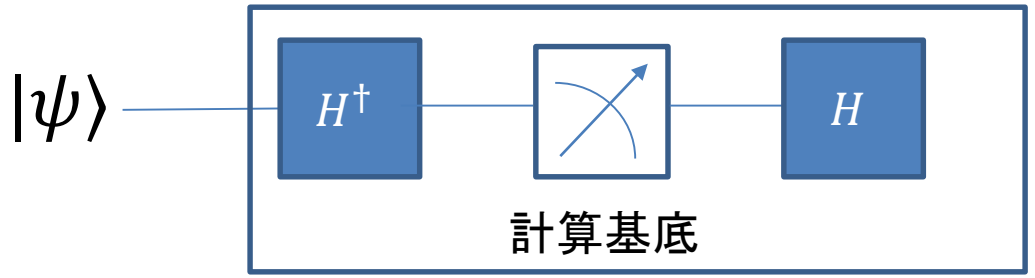




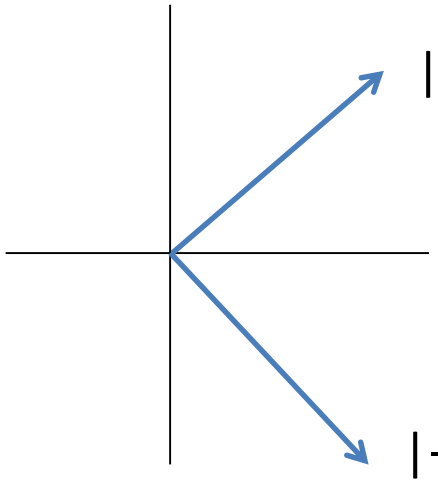
Measurement in the X basis

- 測定は基底 $\{|0\rangle, |1\rangle\}$（計算基底: computational basis）への射影だけではない
- 時間発展Uと組合すことで基底$\{U|0\rangle, U|1\rangle\}$への射影による測定も実現可能

測定後の状態を考えると



基底 $\{H|0\rangle, H|1\rangle\}$

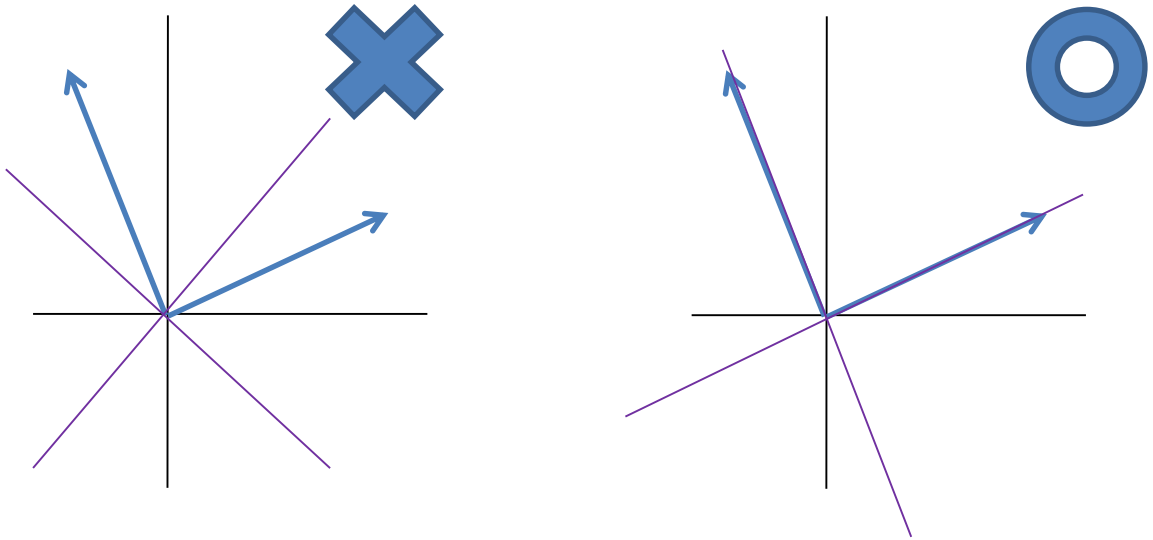


$$|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

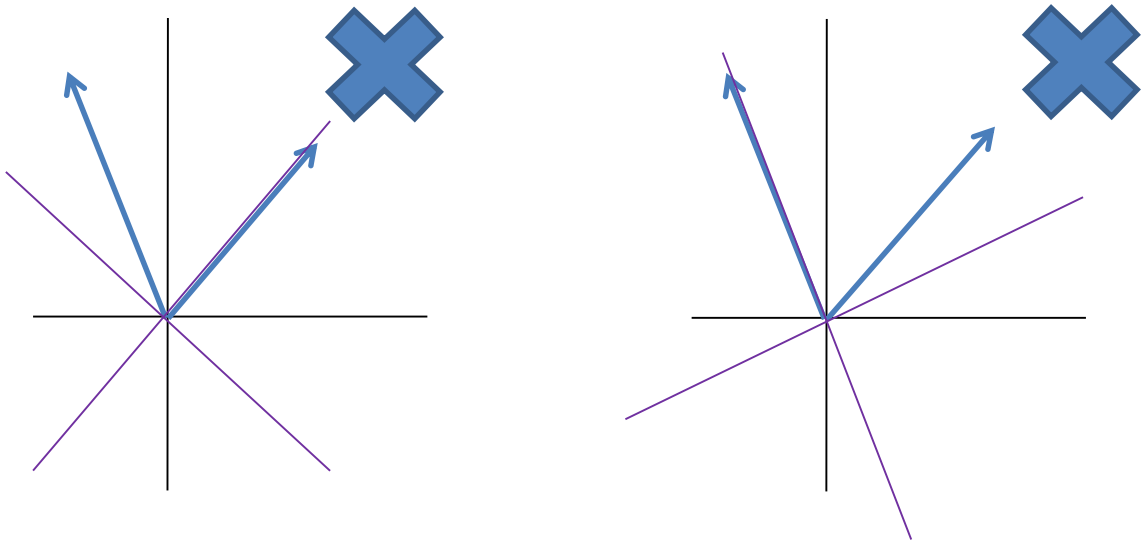
2 orthogonal states are distinguishable

- 直交する状態$|\psi\rangle, |\psi^{\perp}\rangle$は基底$\{|\psi\rangle, |\psi^{\perp}\rangle\}$による射影測定で確実に識別可能



2 non-orthogonal states are indistinguishable

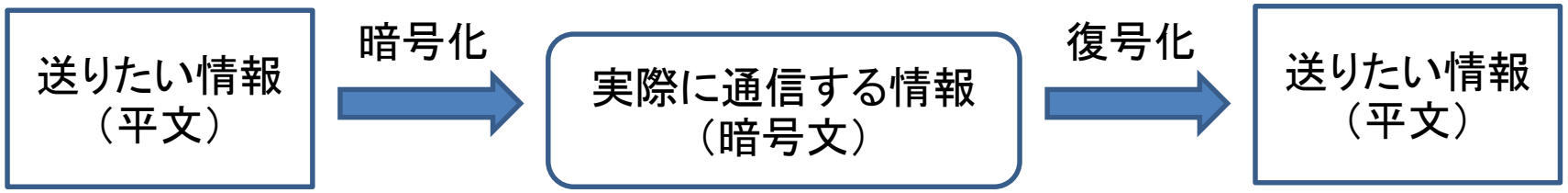
- 直交する状態$|\psi\rangle, |\psi^{\perp}\rangle$は基底$\{|\psi\rangle, |\psi^{\perp}\rangle\}$による射影測定で確実に識別可能
- 非直交な2つの状態の確実（確率１）な識別は不可能



Application 1 : 量子鍵配送
(QKD: quantum key distribution)

暗号(Cryptography)

- 情報を第3者に分からない形で送る方法



- 古く（紀元前，古代ローマ）から存在（古代暗号）
  - 代表的なのはシーザー暗号(Caesar cipher)
  - 軍事目的
- 1970年代後半に暗号の新しい概念（公開鍵暗号: public key cryptosystem）が提唱される（現代暗号）
  - Diffie-Hellman-Merkle 1976
  - 暗号は日常的に使用される技術となる

Secret & Public Key Cryptosystems

- 暗号化及び復号化には鍵が必要
- 鍵の使い方で暗号は2種類に分かれる
- 秘密鍵暗号（共通鍵暗号）: secret key cryptosystem
  - 送信者と受信者は共通の鍵を持ち，鍵は第3者には秘密である（秘密鍵）
  - 鍵は暗号化にも復号化にも使用
- 公開鍵暗号: public key cryptosystem [Diffie-Hellman-Merkle 1976]
  - 受信者は2タイプの鍵を用意
  - 1つは暗号化専用で誰でも使える（公開鍵: public key）
  - もう1つは復号化専用で受信者のみが持つ（秘密鍵: private key）

Secret Key Cryptosystems

- 換字式暗号(substitution cipher)

- One-time Pad

平文(plaintext)	0101010101 0100010101 0100010101 0101010100 010101
鍵(key)	1101001001 0000110110 1010010011 1001010101 001001
暗号文(ciphertext)	1000011100 0100100011 1110000110 1100000001 011100
鍵(key)	1101001001 0000110110 1010010011 1001010101 001001
平文(plaintext)	0101010101 0100010101 0100010101 0101010100 010101

Pros & Cons of One-time Pad

- 長所(Pros)
  - 鍵となるビット列がランダムに選択されるため「無条件に安全」，つまり盗聴者は「当てずっぽうで鍵を推測し，復号する」より良い方策を持たない
  - 暗号化・復号化の処理が非常に高速に可能
- 短所(Cons)
  - 鍵が暗号文と同じくらい長い
  - １回使ったら別の鍵にしないと無条件安全性は保てない
  - 最大の問題は，どうやって鍵を共有するか？（鍵配送問題: key distribution）

量子鍵配送
(QKD:quantum key distribution)

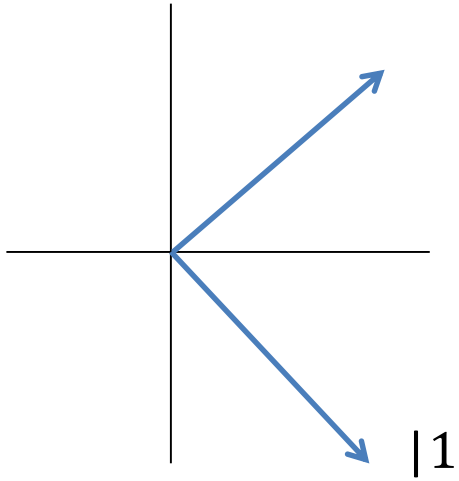
BB84

- Bennett & Brassardの量子鍵配送(1984)
  - 量子力学系の不確定性を利用して，無条件に安全な秘密鍵配送を実現
  - 盗聴者が鍵を盗もうとすると，量子力学系を利用した暗号文を壊してしまう
  - 数ある量子情報技術の中で最も実用化に近い
    - ベンチャー企業（id Quantique, MagiQ Tecnologies）
    - 国内ではNICT（情報通信研究機構），三菱電機, NEC, NTTなどで実用化へ向けた試作品
    - 2010年，東京4拠点（大手町，本郷，小金井，白山）間での大規模デモ
    - 世界的には中国が存在感大（衛星，地上間での量子鍵配送実験 2017）

量子ビットの測定(measurement)

- 測定は射影によって表現できるので異なる射影で
  異なる測定をすることもできる.

X基底による測定（cf. |0>, |1>は+基底での測定という）



$$|0'\rangle := |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|1'\rangle := |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|0\rangle := \frac{1}{\sqrt{2}}(|0'\rangle + |1'\rangle)$$

と書けるので
X基底で測ると測定値0'と
1'をともに確率1/2で得る

Points:
- $|0'\rangle$ と $|1'\rangle$ はX基底で測定すれば確実に識別可能
- 一般に直交する2つの量子ビットは何らかの測定により確実に識別可能
- すべての測定で識別不可能な状態（$|1'\rangle$と $-|1'\rangle$など）は同一状態

Non-orthogonal states are indistinguishable

- $|0\rangle, |1\rangle, |0'\rangle, |1'\rangle$の４状態を確実に識別することは不可能（＋基底で測定する物理量とX基底で測定する物理量の不確定性関係）
  - $|0\rangle, |1\rangle$ をX基底で測定すると得られる測定値（0’か1’か）はどちらもランダムに出現するので完全に識別不可能
  - $|0'\rangle, |1'\rangle$ を+基底で測定すると得られる測定値（0か1か）はどちらもランダムに出現するので完全に識別不可能
- ４状態を暗号化に用いたら盗聴できないかも？ → BB84

BB84

秘密鍵を共有したい２人をAlice, Bobとする

1. Aliceはランダムなビット列を選択したのち，各ビットについてランダムに＋かXかを選択して
   ＋なら 0 を$|0\rangle$, 1を$|1\rangle$ としてBobへ送信
   X なら 0 を $|0'\rangle$，1を$|1'\rangle$ としてBobへ送信
2. Bobは各ビットについてランダムに＋かXかを選択して
   ＋ならAliceからの量子ビットを＋基底で測定
   X ならAliceからの量子ビットをX基底で測定
3. AliceとBobは各ビットについて＋とXのどっちを選択したかを（電話などで）教えあう．その結果選択が一致しなかったビットは捨てる
4. Aliceは残ったビットの中で半分のビットをランダムに選択し，選択したビットがどれかという情報とそれらのビットの値が0か1かをBobに教える．
5. Bobは4.でAliceが選択したビットの値が2.で行った測定の結果と一致しているかどうか（ただしBobの測定値0’は0，測定値1’は1と解釈）をチェックし，１つでも一致していないものがあれば「盗聴者(eavesdropper)がいる」と認定する
6. 「盗聴者(eavesdropper)がいる」と認定されなかった場合，3.で捨てられなかったビットでかつ4.でAliceが値をばらさなかったビット達を共有鍵とする．

BB84（盗聴者なし:without eavesdropper ）

Bit	0	1	1	0	1	0	0	0	0	1	0	1	1	0	1	1
A	＋	X	＋	X	X	＋	＋	X	＋	X	X	＋	＋	＋	X	＋
状態	0	1′	1	0′	1′	0	0	0′	0	1′	0′	1	1	0	1′	1
B	＋	＋	＋	X	＋	X	＋	X	X	＋	X	＋	X	＋	＋	X
側	0	0	1	0’	1	0’	0	0’	1’	1	0’	1	0’	0	0	1’

3.		**捨**			**捨**	**捨**			**捨**	**捨**			**捨**		**捨**	**捨**
4.	**選**			**選**				**選**						**選**		
5.	○			○				○						○		
6.			**1**				**0**				**0**	**1**				

共有の秘密鍵(shared secret key) 1001

BB84（解析:analysis）

N:=Aliceが1. で用意するランダムビット列の長さ

＊盗聴者がいないとき

- 3.でAlice, Bobが捨てなかったビット（＋，Xが一致したもの）は約半分（＝N/2ビット）
- 4.でチェックのためAliceが値を教えるビットは平均N/4ビットで，残る平均N/4ビットが共有鍵となる

BB84（盗聴者あり: with eavesdropper）

盗聴者EveはAliceが送る量子ビットを＋基底かX基底で
当てずっぽうに測定して情報を盗もうとすると

Bit	0	1	1	0	1	0	0	0	0	1	0	1	1	0	1	1
A	＋	X	＋	X	X	＋	＋	X	＋	X	X	＋	＋	＋	X	＋
状態	0	1′	1	0′	1′	0	0	0′	0	1′	0′	1	1	0	1′	1
E	＋	X	＋	＋	＋	X	＋	X	X	X	＋	X	＋	X	＋	X
状態	0	1’	1	0	1	1’	0	0’	0’	1’	0	0’	1	0’	0	0’
B	＋	＋	＋	X	＋	X	＋	X	X	＋	X	＋	X	＋	＋	X
側	0	0	1	0’	1	1’	0	0’	0’	1	1’	1	0’	1	0	0’

3.		**捨**			**捨**	**捨**			**捨**	**捨**			**捨**		**捨**	**捨**

4.	**選**			**選**				**選**						**選**		

5.	○			○				○						×		

BB84 (解析:analysis)

N:=Aliceが1. で用意するランダムビット列の長さ

＊盗聴者がいないとき

- 3.でAlice, Bobが捨てなかったビット（＋，Xが一致したもの）は約半分（＝N/2ビット）
- 4.でチェックのためAliceが値を教えるビットは平均N/4ビットで，残る平均N/4ビットが共有鍵となる

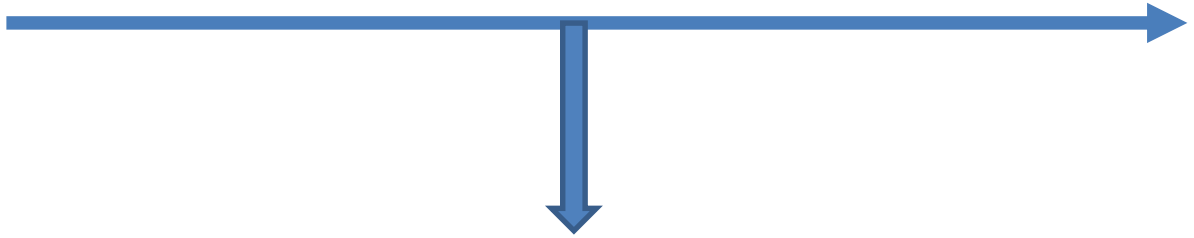
＊盗聴者EveはAliceが送る量子ビットを＋基底かX基底で当てずっぽうに測定して情報を盗もうとすると

- 4.でチェックのためAliceが値を教えるKビット（＝平均N/4ビット）のそれぞれはAliceとBobで＋，Xが一致してるが，Eveはその一致した方向を知らないので，1/2の確率で (E) 間違った方向を選択
- さらに間違った方向を選択したという条件 (E) のもとで，対応するビットはEveの測定により状態が変化するので，1/2の確率で (F) 測定値がAliceのビットと一致しない
- ゆえに4.でチェックのためAliceが値を教えるKビットのそれぞれはPr[E]×Pr[F|E]=1/4の確率でBobの測定値がAliceのビットと異なる.
- 盗聴者を発見されない確率は$(1-1/4)^K \fallingdotseq 0$

＊実際の安全性証明はもっと一般的なEveの攻撃とともに通信路で生じるエラーも含めて解析を行う.

量子ビットは複製できない
（quantum no-cloning theorem）

- 未知の量子ビット$|\psi\rangle = a|0\rangle + b|1\rangle$は複製不可
- $|\psi\rangle$が$|0\rangle, |1\rangle, |0'\rangle, |1'\rangle$に制限されても成立

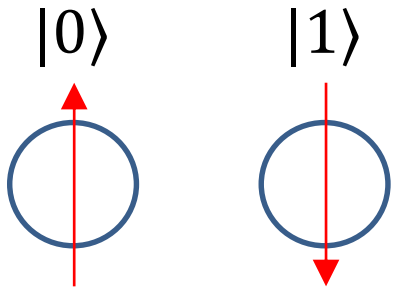


盗聴者

量子ビット（続）

量子ビット(quantum bit, qubit)

- 通常の情報の最小単位はビット０＆１
- 量子力学系を基にした情報（量子情報）の最小単位は量子ビットと呼ばれ，複素2次元の単位ベクトルで表現される．
- 量子ビットは2つの基底状態を持つ量子力学系で実現可能
  - 原子核のスピン（up, down）
  - 光の偏光（縦偏光，横偏光）

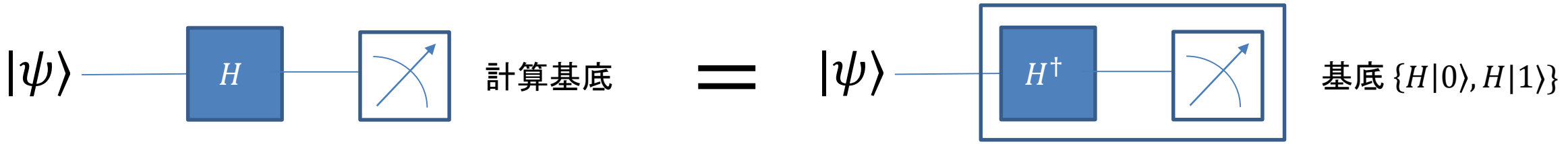


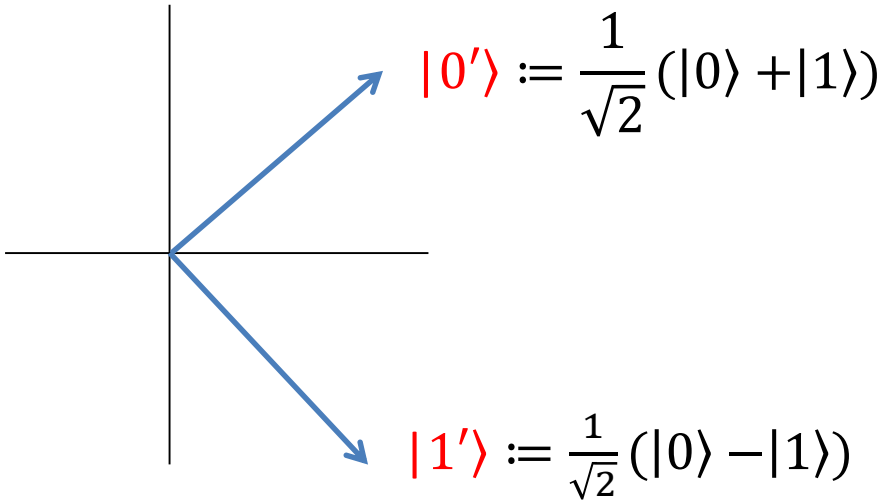
$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \longrightarrow |\psi\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$$

量子状態の波としての一面
量子状態と量子状態の重ね合わせはやはり量子状態
（重ね合わせの原理: superposition principle）

Measurement in different basis

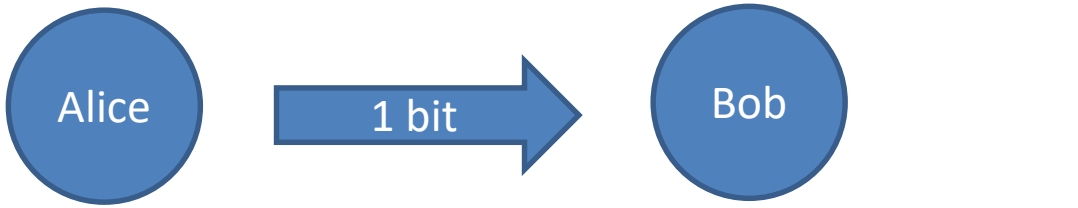
- 測定は基底 $\{|0\rangle, |1\rangle\}$（計算基底）への射影だけではない
- 時間発展Uと組合すことで基底$\{U|0\rangle, U|1\rangle\}$への射影による測定も実現可能





Application 2: ランダムアクセス符号 (RAC: random access code)

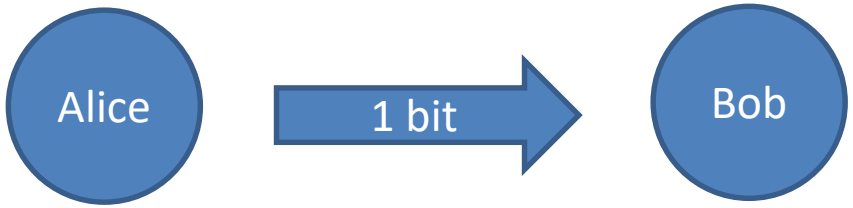
- 設定(setting)
  - Aliceは入力 $x \in \{0,1\}^n$ を持つ，Bobは入力 $j \in \{1,2,\dots,n\}$を持つ
  - AliceはBobに1ビットを送ることができる
  - Bobはx_j(Aliceのj番目のビット)をAliceのメッセージから復号したい



$x \in \{0,1\}^n$ $j \in \{1,2,\dots,n\}$

RAC

- 設定
  - Aliceは入力 $x \in \{0,1\}^n$ を持つ，Bobは入力 $j \in \{1,2,\ldots,n\}$を持つ
  - AliceはBobに1ビットを送ることができる
  - Bobはx_j(Aliceのj番目のビット)をAliceのメッセージから復号したい
- どのくらいの成功率(success probability)で復号できるか？
  - 成功率は最悪の場合（worst-case:どんな入力においても達成される成功確率）を考える

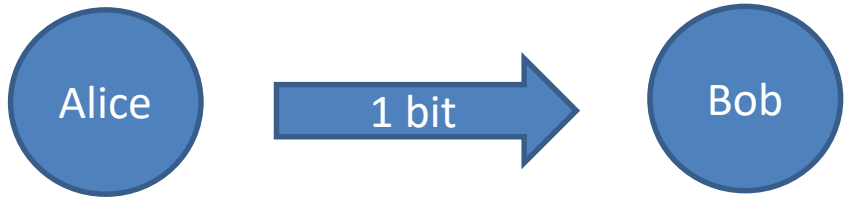


$x \in \{0,1\}^n$ $j \in \{1,2,\ldots,n\}$

RAC

- 設定
  - Aliceは入力 $x \in \{0,1\}^n$ を持つ，Bobは入力 $j \in \{1,2,\ldots,n\}$を持つ
  - AliceはBobに1ビットを送ることができる
  - Bobはx_j(Aliceのj番目のビット)をAliceのメッセージから復号したい
- どのくらいの成功率で復号できるか？
  - 成功率は最悪の場合（どんな入力においても達成される成功確率）を考える

(答) $n = 1$だと成功率 1だが，$n \geq 2$だと成功率は1/2（ランダム）



$x \in \{0,1\}^2$ $j \in \{1,2\}$

RAC

- 設定
  - Aliceは入力 $x \in \{0,1\}^n$ を持つ，Bobは入力 $j \in \{1,2,\dots,n\}$を持つ
  - AliceはBobに1ビットを送ることができる
  - Bobはx_j(Aliceのj番目のビット)をAliceのメッセージから復号したい
- どのくらいの成功率で復号できるか？
  - 成功率は最悪の場合（どんな入力においても達成される成功確率）を考える

(答) $n = 1$だと成功率 1だが，$n \geq 2$だと成功率は1/2（ランダム）

Q. Aliceの通信に量子ビットを使うとどうなるか？

$x \in \{0,1\}^2$　　$j \in \{1,2\}$

量子ランダムアクセス符号
(QRAC: quantum random access code)

- 設定
  - Aliceは入力 $x \in \{0,1\}^n$ を持つ，Bobは入力 $j \in \{1,2,\dots,n\}$を持つ
  - AliceはBobに1量子ビットを送ることができる
  - Bobはx_j(Aliceのj番目のビット)をAliceのメッセージから復号したい
- どのくらいの成功率で復号できるか？
  - 成功率は最悪の場合（どんな入力においても達成される成功確率）を考える

(答) $n = 2$で約0.85の成功率を達成できる

$x \in \{0,1\}^2$　　$j \in \{1,2\}$

Decoding of QRAC ($n = 2$)

- Aliceによる符号化(coding)

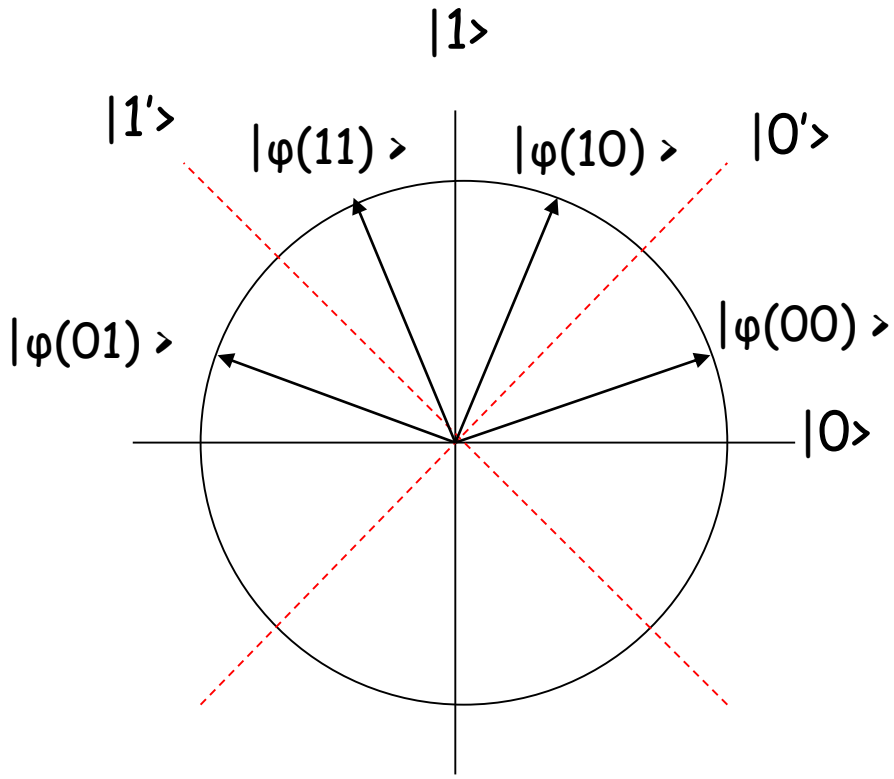
$$\varphi(00) = \cos\left(\frac{\pi}{8}\right)|0\rangle + \sin\left(\frac{\pi}{8}\right)|1\rangle$$

$$\varphi(01) = \cos\left(\frac{7\pi}{8}\right)|0\rangle + \sin\left(\frac{7\pi}{8}\right)|1\rangle$$

$$\varphi(10) = \cos\left(\frac{3\pi}{8}\right)|0\rangle + \sin\left(\frac{3\pi}{8}\right)|1\rangle$$

$$\varphi(11) = \cos\left(\frac{5\pi}{8}\right)|0\rangle + \sin\left(\frac{5\pi}{8}\right)|1\rangle$$

- Bobによる復号(decoding)
  - $j = 1$のとき基底 $\{|0\rangle, |1\rangle\}$(計算基底)で測定
  - $j = 2$のとき基底 $\{|0'\rangle, |1'\rangle\}$ で測定(結果がb' ならbと判定)



QRAC ($n = 3$)

- 設定
  - Aliceは入力 $x \in \{0,1\}^n$ を持つ，Bobは入力 $j \in \{1,2,\dots,n\}$を持つ
  - AliceはBobに1量子ビットを送ることができる
  - Bobはx_j(Aliceのj番目のビット)をAliceのメッセージから復号したい
- どのくらいの成功率で復号できるか？
  - 成功率は最悪の場合（どんな入力においても達成される成功確率）を考える

(答) $n = 2$で約0.85の成功率を達成できる

Q. $n = 3$だとどうか？

QRAC ($n = 3$)

- 設定
  - Aliceは入力 $x \in \{0,1\}^n$ を持つ，Bobは入力 $j \in \{1,2,\dots,n\}$を持つ
  - AliceはBobに1量子ビットを送ることができる
  - Bobはx_j(Aliceのj番目のビット)をAliceのメッセージから復号したい
- どのくらいの成功率で復号できるか？
  - 成功率は最悪の場合（どんな入力においても達成される成功確率）を考える

(答) $n = 2$で約0.85の成功率を達成できる

- $n = 3$だとどうか？ ⇒ 約0.79
  - Bloch 球 (Bloch sphere)

Bloch sphere

- 任意の量子ビットは

$$\cos\frac{\theta}{2}|0\rangle + e^{i\gamma}\sin\frac{\theta}{2}|1\rangle \ (0 \le \theta \le \pi, 0 \le \gamma \le 2\pi)$$

と書ける

- 実3次元単位球の点

$$(\cos\gamma\sin\theta\,,\sin\gamma\sin\theta\,,\cos\theta)$$

と1対1対応が作れる

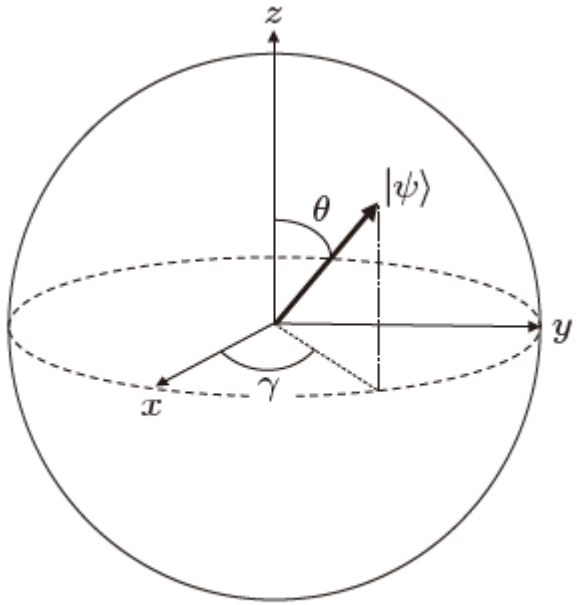


図 3.2　一般の量子ビットの描像
（ブロッホ球）

「基礎から学ぶ量子計算」より

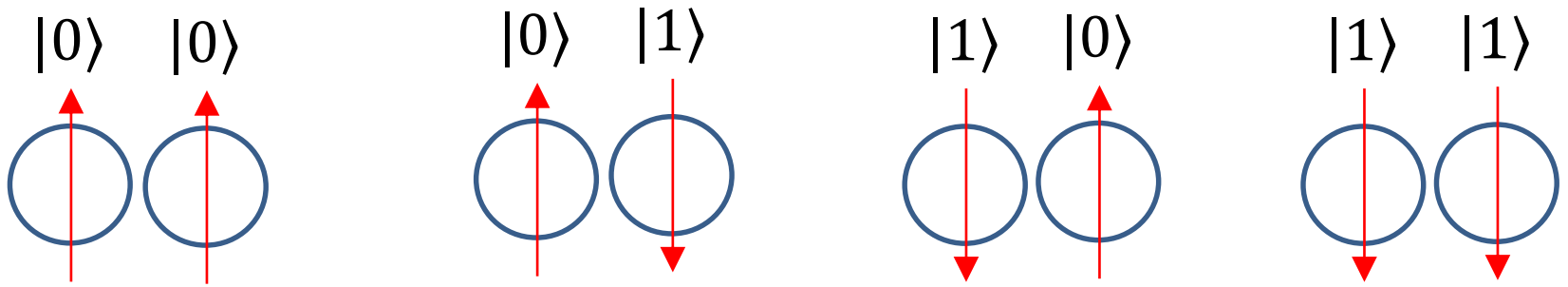
Qbit (Summary)

- 量子状態
  - 状態⇔ベクトル，時間発展⇔ユニタリ，測定⇔射影
- 量子ビット
  - $a|0\rangle + b|1\rangle$
  - 量子鍵配送
  - 量子ランダムアクセス符号

複数の量子ビット
(multiple qubits)

2qubit = 1qubit + 1qubit ?

- 2量子ビットは1量子ビットを2個並べたもの？
- 2ビット 00, 01, 10, 11



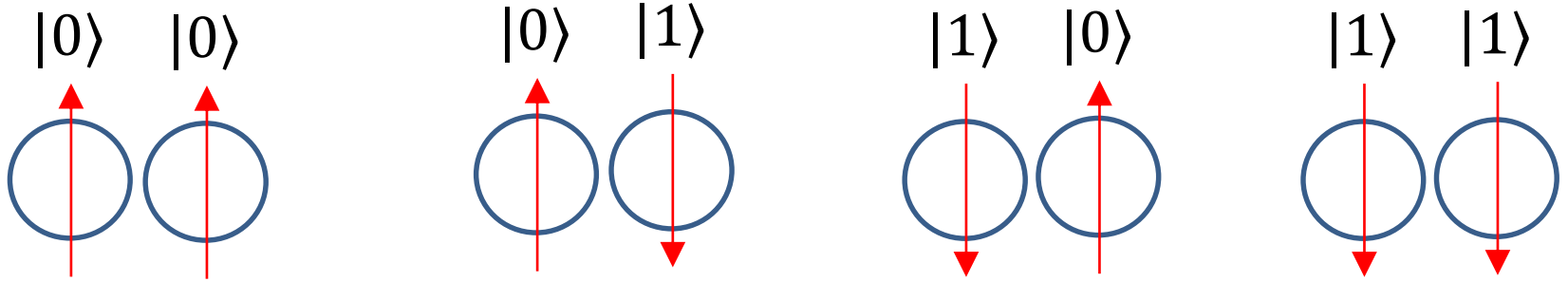
2qubit = superposition of 2bits ?

- 2量子ビットは2ビットに対応する基底状態の線形結合？
- （古典の）2ビット 00, 01, 10, 11
- 2量子ビットの状態は古典2ビットの量子重ね合わせ

$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ (単位ベクトル)

ただし,

$$|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$



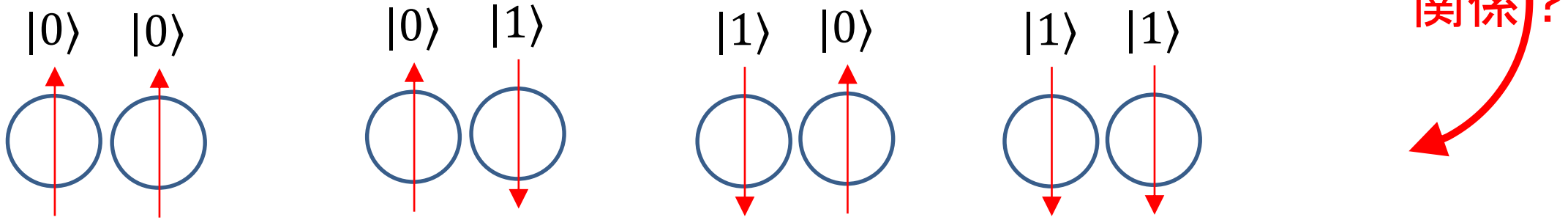
1qubit + 1qubit vs superposition of 2bits

- （古典の）2ビット 00, 01, 10, 11
- 2量子ビットの状態は古典2ビットの量子重ね合わせ

$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ (単位ベクトル)

ただし,

$$|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$



テンソル積(tensor product)

- $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \coloneqq \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{pmatrix}$

テンソル積の双線形性(bi-linearity)

$(a|\psi_1\rangle + b|\psi_2\rangle) \otimes |\varphi\rangle = a|\psi_1\rangle \otimes |\varphi\rangle + b|\psi_2\rangle \otimes |\varphi\rangle$

$|\psi\rangle \otimes (c|\varphi_1\rangle + d|\varphi_2\rangle) = c|\psi\rangle \otimes |\varphi_1\rangle + d|\psi\rangle \otimes |\varphi_2\rangle$

- ブラケット表示（bra-ket notations）だと

$(a_1|0\rangle + a_2|1\rangle) \otimes (b_1|0\rangle + b_2|1\rangle) \coloneqq a_1 b_1|00\rangle + a_1 b_2|01\rangle + a_2 b_1|10\rangle + a_2 b_2|11\rangle$

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

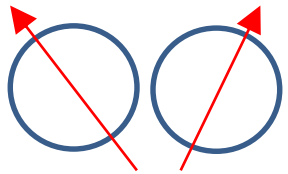
$|0\rangle \otimes |0\rangle$ $|0\rangle \otimes |1\rangle$ $|1\rangle \otimes |0\rangle$ $|1\rangle \otimes |1\rangle$

2qubits = 1qubit + 1qubit ?

- （古典の）2ビット 00, 01, 10, 11
- 2量子ビットの状態は古典2ビットの量子重ね合わせ

$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ (単位ベクトル)

$|\psi_1\rangle \otimes |\psi_2\rangle$



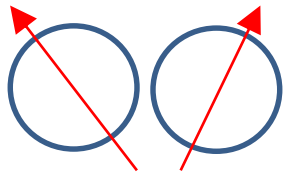
同じ？

2qubits ≠ 1qubit + 1qubit

- （古典の）2ビット 00, 01, 10, 11
- 2量子ビットの状態は古典2ビットの量子重ね合わせ

$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ (単位ベクトル)

$|\psi_1\rangle \otimes |\psi_2\rangle$



同じ？

（反例） $|\Phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

2つの量子ビットはエンタングルしている
(entanglement)

エンタングル状態(Entangled states)

- 2量子ビット状態$|\psi\rangle$が**エンタングル状態(entangled state)**⇔
$$|\psi\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle)$$
となる複素数a, b, c, dは存在しない
- $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$はエンタングル状態
- 他のエンタングル状態
  - $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
  - $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
  - $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$
- エンタングルしてない状態（直積状態: product state）の例
  - $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = |+\rangle|+\rangle$

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

n量子ビット状態(n-qubit states)

- 状態空間
  - $|0^n\rangle, |0^{n-1}1\rangle, \ldots, |1^n\rangle$で張られる$2^n$次元複素内積空間
- 状態
  - $|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$
- エンタングル状態
  - n個の量子ビット状態$|\psi\rangle$をA系とB系という2つの系に分けたとき，A系とB系が**エンタングル**している⇔$|\psi\rangle$がA系とB系の状態のテンソル積として書けない

  例

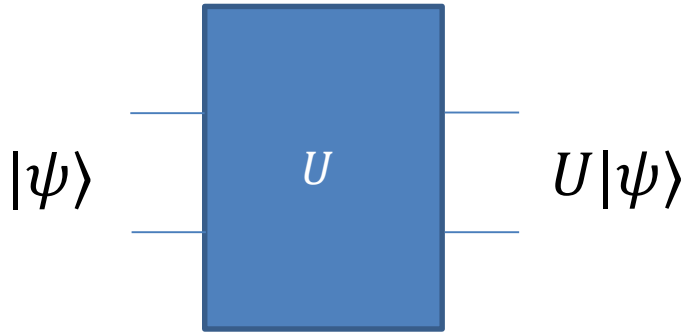
$$\frac{1}{\sqrt{2}}(|000\rangle + |101\rangle)$$

  は：
  - 最初の2量子ビットの系と第3量子ビットの系はエンタングルしている
  - 第2量子ビットの系は$|0\rangle$で残り2量子ビットの系は$|\Phi^+\rangle$なので，第2量子ビットと残りの2量子ビットはエンタングルしていない

Time Evolution of 2qubits

- 2量子ビットの時間発展

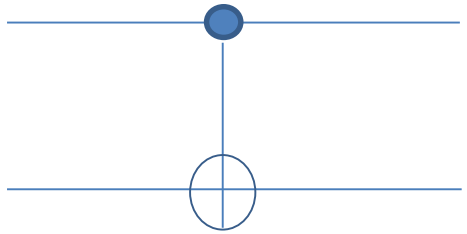
＝4次ユニタリ行列（**2量子ビットゲート**）



Example of 2qubit gates: CNOT

- 4次ユニタリ行列（2量子ビットゲート）
- 2量子ビットゲートの例

– CNOT $C\text{-}X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

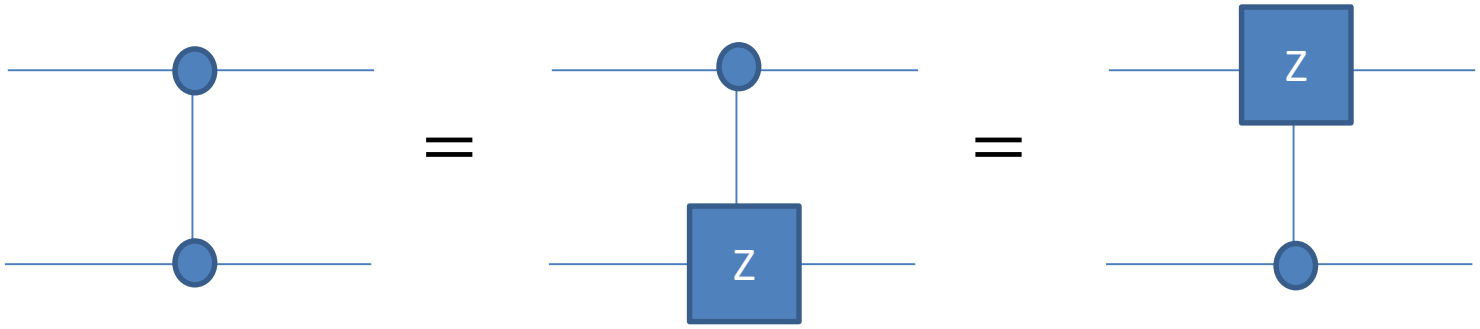


$C\text{-}X|00\rangle = |00\rangle, C\text{-}X|01\rangle = |01\rangle, C\text{-}X|10\rangle = |11\rangle, C\text{-}X|11\rangle = |10\rangle,$

CZ gate

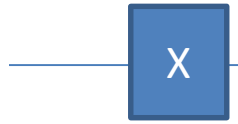
- 制御Z（Controlled-Z）ゲート $CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$
- $CZ|00\rangle = |00\rangle,\ CZ|01\rangle = |01\rangle, CZ|10\rangle = |10\rangle,\ CZ|11\rangle = -|11\rangle$

⇔ $CZ|ab\rangle = (-1)^{ab}|ab\rangle\ (a, b \in \{0,1\})$



Partial time evolution of 2qubit

- 2量子ビットの片側に1量子ビットゲートをかけるとどうなるか？



例1: $|00\rangle$の第1量子ビットにNOTゲート $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$をかけると

$$|00\rangle \mapsto |10\rangle$$

例2: $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$の第1ビットに$X$をかけると

$$|\psi\rangle \mapsto \alpha_{00}|10\rangle + \alpha_{01}|11\rangle + \alpha_{10}|00\rangle + \alpha_{11}|01\rangle$$

例3: $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$の第1ビットに$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$をかけると

$$|\psi\rangle \mapsto \alpha_{00}(H|0\rangle) \otimes |0\rangle + \alpha_{01}(H|0\rangle) \otimes |1\rangle + \alpha_{10}(H|1\rangle) \otimes |0\rangle + \alpha_{11}(H|1\rangle) \otimes |1\rangle$$

Measurement of 2qubits

- 2量子ビット状態

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

を基底$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$（計算基底）で測定すると確率$|\alpha_{kl}|^2$で測定値$kl \in \{0,1\}^2$を得る

Measurement of 2qubits

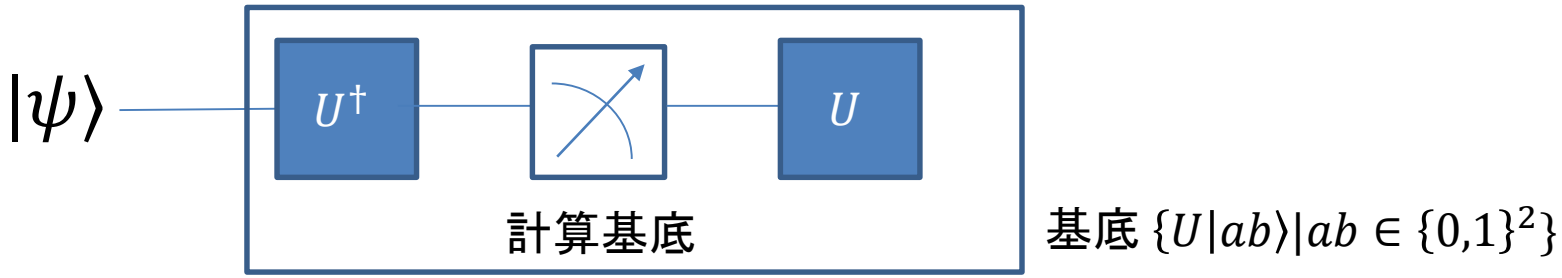
- 2量子ビット状態

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

を基底$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$（計算基底）で測定すると

確率$|\alpha_{kl}|^2$で測定値$kl \in \{0,1\}^2$を得る

- 任意の4次ユニタリ行列Uについて，基底$\{U|00\rangle, U|01\rangle, U|10\rangle, U|11\rangle\}$での測定も可能

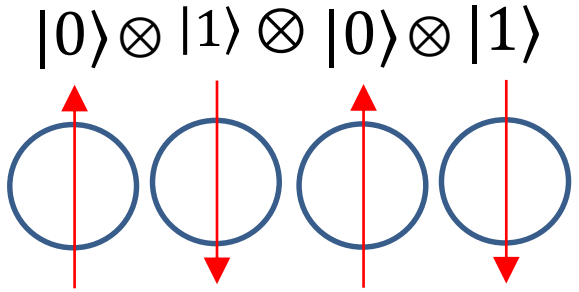


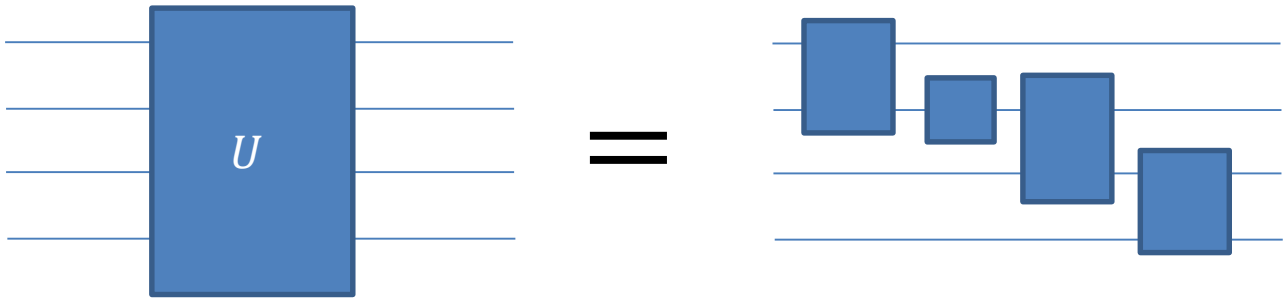
Measurement of n-qubit states

- 状態空間
  - $|0^n\rangle, |0^{n-1}1\rangle, \ldots, |1^n\rangle$で張られる$2^n$次元複素内積空間
- 状態
  - $|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$
- 測定
  - 計算基底で測定すると確率$|\alpha_x|^2$で測定値xを得て測定後の状態は$|x\rangle$となる

Time evolution of n-qubit states

- 状態空間
  - $|0^n\rangle, |0^{n-1}1\rangle, \ldots, |1^n\rangle$で張られる$2^n$次元複素内積空間
- 状態
  - $|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$
  - 計算基底で測定すると確率$|\alpha_x|^2$で測定値xを得る
- 時間発展
  - 2^n次ユニタリ行列（n個の量子ビットを変化させるような操作）←一発では無理
  - 1〜3量子ビットに作用するユニタリの列で表現（量子回路: quantum circuit）





部分的な測定(partial measurement)

例 : $|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$の第2量子ビットを計算基底で測定するとどうなるか？

- 第2量子ビットの測定値の影響を受ける
- 第2量子ビットを測定すると測定後の状態は :
  - 確率 $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$ で$|0\rangle|0\rangle$ (測定値は0)
  - 確率 $\frac{1}{2}$ で$|1\rangle|1\rangle$ (測定値は1)

Partial measurement

例：$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|11\rangle$の第2量子ビットを計算基底で測定するとどうなるか？

- 第2量子ビットの測定値の影響を受ける
- 第2量子ビットの測定値以上の影響は受けない
- $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \left(\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle\right)|1\rangle$
- 第2量子ビットを測定すると測定後の状態は：
  - 確率$\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$で$|0\rangle|0\rangle$ (測定値は0)
  - 確率$\left\|\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle\right\|^2 = \frac{1}{2}$で$\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)|1\rangle$ (測定値は1)

Axiom of Partial Measurement

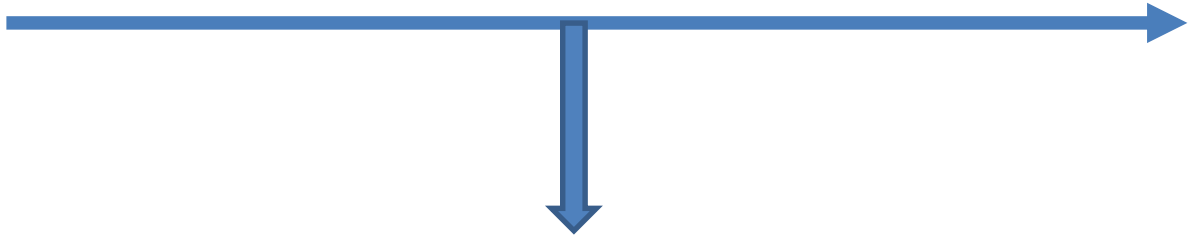
[部分測定の公理] $|\psi\rangle = \sum_x |\psi_x\rangle_A |x\rangle_B$と書けるときにBを計算基底で測定すると確率 $\||\psi_x\rangle\|^2$で測定値xを得て，測定後の状態は$\frac{1}{\||\psi_x\rangle\|}|\psi_x\rangle|x\rangle$になる

Multiple qubits (summary)

- テンソル積(tensor product)
- エンタングルメント(entanglement)
- 2量子ビットゲート(2-qubit gate)
  - CNOT
  - CZゲート
- 部分測定(partial measurement)

量子ビットは複製できない
（quantum no-cloning theorem）

- 未知の量子ビット$|\psi\rangle = a|0\rangle + b|1\rangle$は複製不可
- $|\psi\rangle$が$|0\rangle, |1\rangle, |0'\rangle, |1'\rangle$に制限されても成立



盗聴者

No-Cloning theorem (Proof)

No-Cloning theorem:

任意の量子ビットをコピーすることはできない⇔任意の量子ビット状態$|\varphi\rangle$について

$U(|\varphi\rangle|0\rangle) = |\varphi\rangle|\varphi\rangle$ (*)

をみたすユニタリUは存在しない

Proof: (*)をみたすUが存在するなら:

$$U(|0\rangle|0\rangle) = |0\rangle|0\rangle, U(|1\rangle|0\rangle) = |1\rangle|1\rangle,$$

より

$$U(|+\rangle|0\rangle) = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$$

となるが，これは

$$U(|+\rangle|0\rangle) = |+\rangle|+\rangle$$

と矛盾