量子計算量理論入門

Vol. 3

話題

- 量子プロトコル
- 量子計算量理論

量子プロトコル

- 量子ワンタイムパッド
- 量子テレポーテーション
- 量子ゲーム

混合状態と密度行列

Global phase

- **$|\psi\rangle$と$|\psi_\theta\rangle := e^{i\theta}|\psi\rangle$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

量子状態の一意的表現

- **$|\psi\rangle$と$|\psi_\theta\rangle := e^{i\theta}|\psi\rangle$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**
- 一意的な表現法
  - ベクトルの代わりに行列（密度行列）を使う
  - $\rho_\psi := |\psi\rangle\langle\psi|$
  - $\rho_\psi = |\psi_\theta\rangle\langle\psi_\theta|$ for any phase θ!!
- 時間発展
  - ベクトルの場合：$|\psi\rangle \mapsto U|\psi\rangle$
  - 行列の場合：$\rho_\psi \mapsto U\rho U^\dagger = U|\psi\rangle\langle\psi|U^\dagger$

量子状態の一意的表現

- **$|\psi\rangle$と$|\psi_\theta\rangle := e^{i\theta}|\psi\rangle$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**
- 一意的な表現法
  - ベクトルの代わりに行列（密度行列）を使う
  - $\rho_\psi := |\psi\rangle\langle\psi|$
  - $\rho_\psi = |\psi_\theta\rangle\langle\psi_\theta|$ for any phase θ!!
- 測定
  - ベクトルの場合：$|\psi\rangle$を基底$\{|\varphi_k\rangle\}$で測ると確率$|\langle\varphi_k|\psi\rangle|^2$で測定値$k$を得る
  - 行列の場合：ρ_ψを基底$\{|\varphi_k\rangle\}$で測ると確率$\langle\varphi_k|\rho_\psi|\varphi_k\rangle = |\langle\varphi_k|\psi\rangle|^2$で測定値$k$を得る

1量子ビットの場合

- $|\psi_{\theta,\gamma}\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\gamma}\sin\left(\frac{\theta}{2}\right)|1\rangle$
  - ただし，$\theta \in [0,\pi]$，$\gamma \in [0,2\pi]$
- $|\psi_{\theta,\gamma}\rangle\langle\psi_{\theta,\gamma}| = \frac{1}{2}(I + (\cos\gamma\sin\theta)X + (\sin\gamma\sin\theta)Y + (\cos\theta)Z)$
- 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

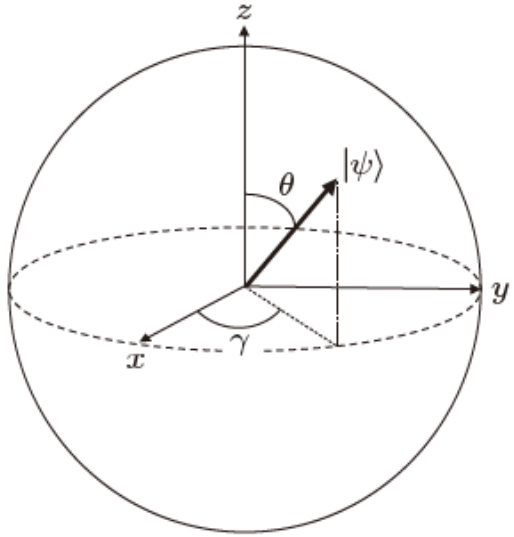


図 3.2　一般の量子ビットの描像（ブロッホ球）

「基礎から学ぶ量子計算」より

混合状態と密度行列

- 密度行列による表現にはさらなるご利益あり！
  - 状態の確率分布（混合状態）も表現できることになる
  - 確率p_jで状態$|\psi_j\rangle$であるような確率分布は

$$\sum_j p_j \, |\psi_j\rangle\langle\psi_j|$$

- 完全混合状態
  - 完全にランダムな状態
  - m量子ビット状態の場合，確率$\frac{1}{2^m}$で正規直交基底$\{|x\rangle : x \in \{0,1\}^m\}$の各要素が取られているような状態

$$\sum_{x\in\{0,1\}^m} \frac{1}{2^m} |x\rangle\langle x| = \frac{1}{2^m} I_{2^m}$$

1量子ビットの場合

- $|\psi_{\theta,\gamma}\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\gamma}\sin\left(\frac{\theta}{2}\right)|1\rangle$
  - ただし，$\theta \in [0,\pi]$，$\gamma \in [0,2\pi]$
- $|\psi_{\theta,\gamma}\rangle\langle\psi_{\theta,\gamma}| = \frac{1}{2}(I + (\cos\gamma\sin\theta)X + (\sin\gamma\sin\theta)Y + (\cos\theta)Z)$
- 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

- 混合状態はブロッホ球の内部に対応
- 完全混合状態$=\frac{1}{2}I_2$
  - ブロッホ球の原点に対応

量子ワンタイムパッド

- ワンタイムパッド
  - ビットを安全に送る方法
  - $b \in \{0,1\}$をAliceがBobに安全に送りたい
  - AliceとBobがランダムなビット$r \in \{0,1\}$を共有していれば
  - Aliceは（盗聴されるかもしれない通信路で）Bobに$b' = b \oplus r$を送る
  - Bobは$b' \oplus r$を計算することでbを得る
  - rを知らない盗聴者にとってb'はランダムビット

Q1. 量子ビットはどうやって安全に送る?

Q2. 量子ビットを安全に送るには何ビット共有していればOK?

量子ワンタイムパッド

- 量子ビットを安全に送る方法
  - $|\psi\rangle$をAliceがBobに安全に送りたい
  - AliceとBobがランダムな2ビット$r \in \{0,1\}^2$を共有していれば
  - Aliceは（盗聴されるかもしれない量子通信路で）Bobに以下の状態を送る
    - $r = 00$のとき$|\psi\rangle$
    - $r = 01$のとき$X|\psi\rangle$
    - $r = 10$のとき$Z|\psi\rangle$
    - $r = 11$のとき$Y|\psi\rangle$
  - Bobは受け取った状態に以下のユニタリを適用することで$|\psi\rangle$を得る
    - $r = 00$のときI
    - $r = 01$のときX
    - $r = 10$のときZ
    - $r = 11$のときY
  - rを知らない盗聴者にとっては量子通信路を通る状態は完全混合状態

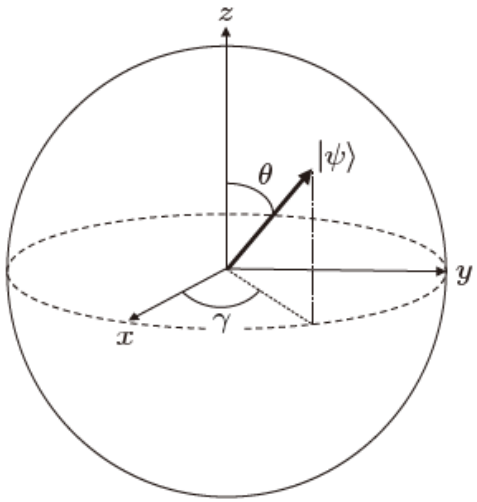


図 3.2　一般の量子ビットの描像（ブロッホ球）

「基礎から学ぶ量子計算」より

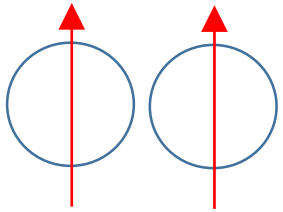
Quantum Protocols based on Entanglement

2量子ビット

- （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？

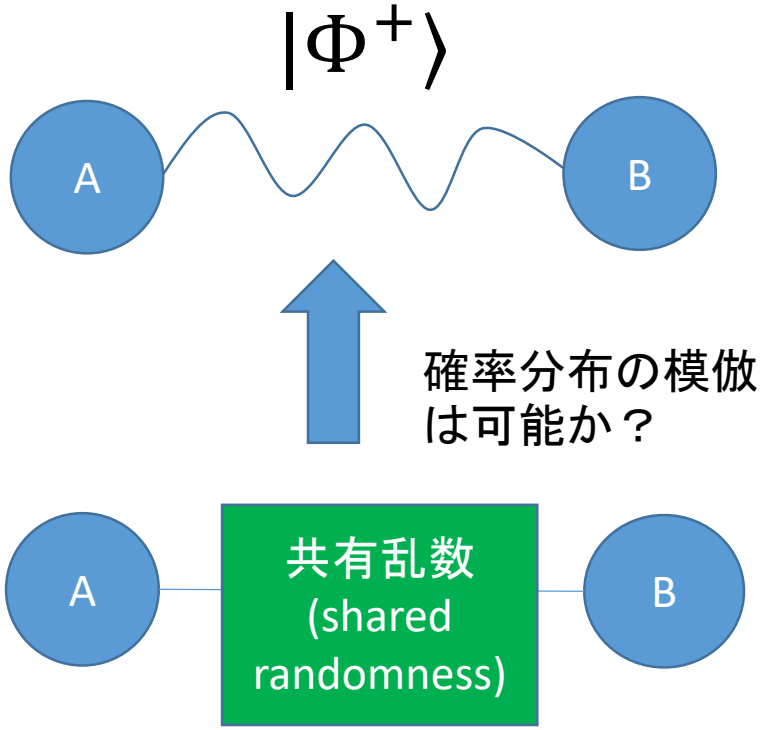
（反例） $|\Phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

2つの量子ビットはエンタングルしている

エンタングルメント(Entanglement)

- 量子状態に特有の性質
- 古典情報では作り出せないような複数の系の相関(correlation)
  - Spooky action at a distance (Einstein)

例：EPR対 $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$

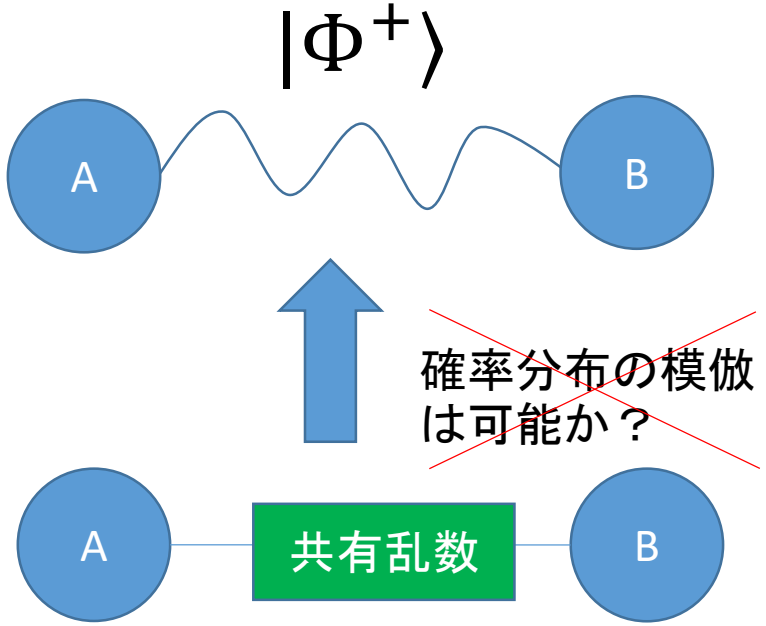


Entanglement

- 量子状態に特有の性質
- 古典情報では作り出せないような複数の系の相関(correlation)

例 : $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$

$= \frac{1}{\sqrt{2}}(|+\rangle_A|+\rangle_B + |-\rangle_A|-\rangle_B)$



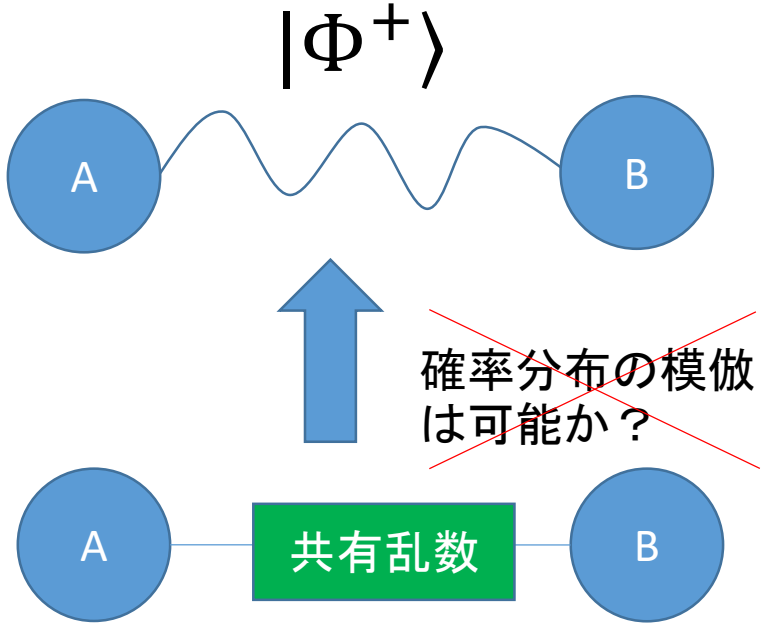
Entanglement

- 量子状態に特有の性質
- 古典情報では作り出せないような複数の系の相関(correlation)

例 : $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$

$= \frac{1}{\sqrt{2}}(|\varphi\rangle_A|\varphi\rangle_B + |\varphi^\perp\rangle_A|\varphi^\perp\rangle_B)$

ただし，$|\varphi\rangle$は実係数を振幅に持つ1量子ビット状態



Quantum Protocols based on Entanglement

- 非局所性ゲーム(non-local game)
- 量子テレポーテーション(quantum teleportation)

Bellの不等式(Bell Inequality)

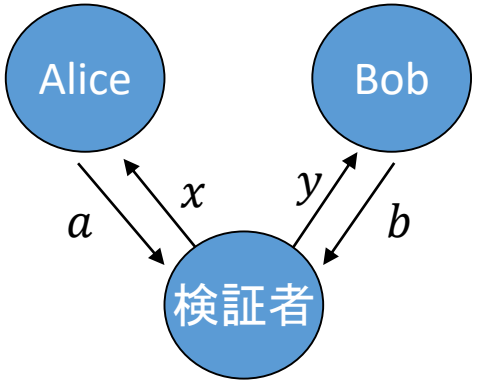
- Bellの不等式
  - 古典力学による世界観(局所決定論)に基づいた不等式
  - 局所決定論(≒局所実在論):隠れた変数を固定することで観測値が決定的になるような局所理論
  - 通信できない複数のパーティ(局所性をみたすパーティ)が,「古典的に」作り出せる確率分布に関する不等式はBellの不等式をみたす
- Bellの不等式の破れ(violations of Bell inequalities)
  - 複数のパーティが量子状態を共有すればBellの不等式をみたさないような確率分布が作れる!

$p(a, b|x, y)$

CHSH Game

$$\left|\langle A_0 B_0\rangle + \langle A_1 B_0\rangle + \langle A_0 B_1\rangle - \langle A_1 B_1\rangle\right| \le 2$$

Clauser-Horne-Shimony-Holtの不等式(1969)を
ゲームとして解釈すると



入力: 1 bit x (Alice); 1 bit y (Bob) ,
一様分布πにそって選択される

出力: 1 bit a (Alice); 1 bit b (Bob)

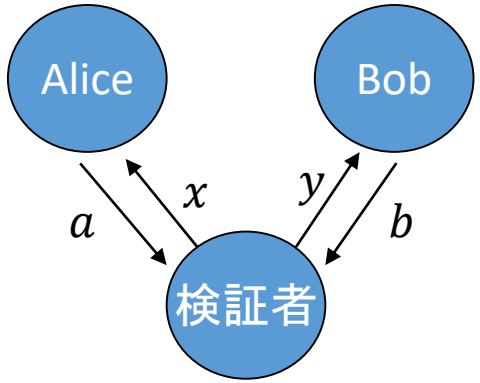
Alice と Bob が勝つ条件: $xy = a \oplus b$

ゲーム前はAliceとBobは打合せOK

x	y	勝つ条件
0	0	$a \oplus b = 0$
0	1	$a \oplus b = 0$
1	0	$a \oplus b = 0$
1	1	$a \oplus b = 1$

- (打合せ及びAlice＆Bobの操作が)古典の勝率 (classical winning probability) 0.75
- 量子の勝率(quantum winning probability) 約0.85

古典の勝率=0.75



- AliceとBobが取れる戦略: WLOG,
  - ゲーム前に共有した情報r（確率的に選択してOK）に従って入力x, yに応じて決定的な値を返す
- $a_{x,r}$:=Aliceが入力xに対して返すビット値
- $b_{y,r}$:=Bobが入力yに対して返すビット値
- 以下が求められている
  - $a_{0,r} \oplus b_{0,r} = 0$
  - $a_{0,r} \oplus b_{1,r} = 0$
  - $a_{1,r} \oplus b_{0,r} = 0$
  - $a_{1,r} \oplus b_{1,r} = 1$

4つ同時に満たすのは無理！

入力: 1 bit x (Alice); 1 bit y (Bob) ,
一様分布πにそって選択される

出力: 1 bit a (Alice); 1 bit b (Bob)

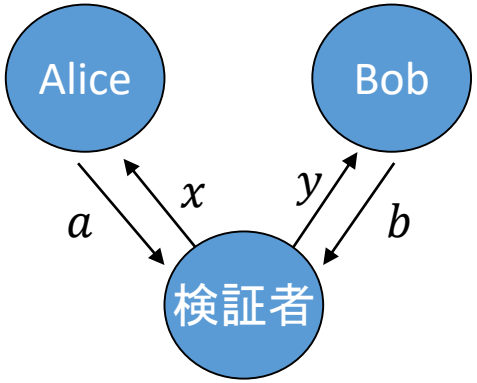
Alice と Bob が勝つ条件: $xy = a \oplus b$

x	y	勝つ条件
0	0	$a \oplus b = 0$
0	1	$a \oplus b = 0$
1	0	$a \oplus b = 0$
1	1	$a \oplus b = 1$

CHSH Game

$$\left|\langle A_0B_0\rangle+\langle A_1B_0\rangle+\langle A_0B_1\rangle-\langle A_1B_1\rangle\right|\le 2$$

Clauser-Horne-Shimony-Holtの不等式(1969)を
ゲームとして解釈すると



入力: 1 bit x (Alice); 1 bit y (Bob) ,
一様分布πにそって選択される

出力: 1 bit a (Alice); 1 bit b (Bob)

Alice と Bob が勝つ条件: $xy = a \oplus b$

ゲーム前はAliceとBobは打合せOK

x	y	勝つ条件
0	0	$a \oplus b = 0$
0	1	$a \oplus b = 0$
1	0	$a \oplus b = 0$
1	1	$a \oplus b = 1$

- 古典の勝率(classical winning probability) 0.75
- 量子の勝率(quantum winning probability) 約0.85
  - (2,1,0.85)-QRAC ⇒ CHSH

(2,1,0.85)-QRAC

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

$j \in \{1,2\}$

- Aliceによる符号化(coding)

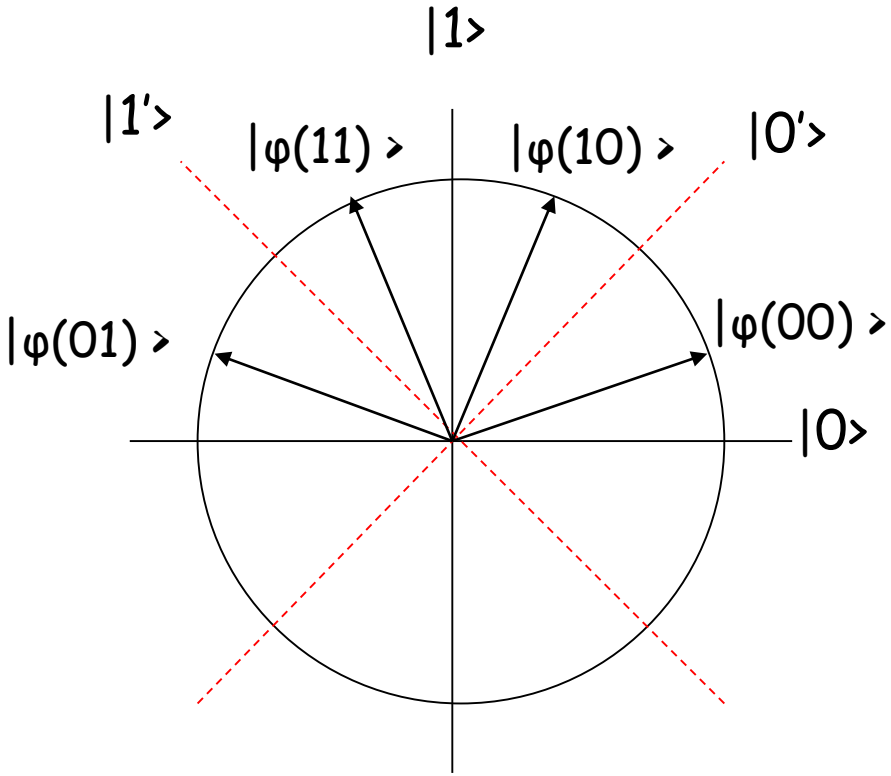
$$\varphi(00) = \cos\left(\frac{\pi}{8}\right)|0\rangle + \sin\left(\frac{\pi}{8}\right)|1\rangle$$

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

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

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

- 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）



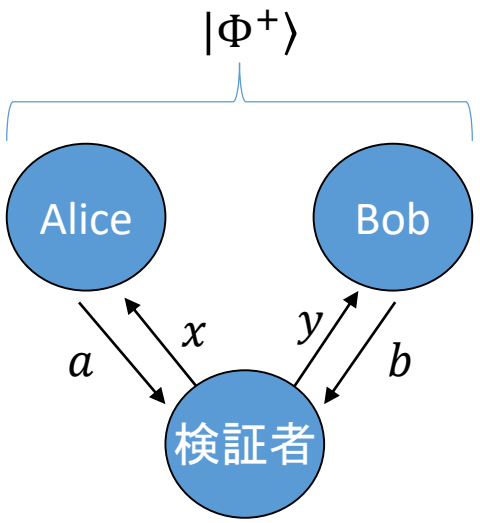
QRAC ⇒ CHSH

Alice と Bob は1組のEPRペア $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$を共有

任意の実係数1量子ビット状態 |φ>に対して $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|\varphi\rangle|\varphi\rangle + |\varphi^\perp\rangle|\varphi^\perp\rangle)$

ゆえに

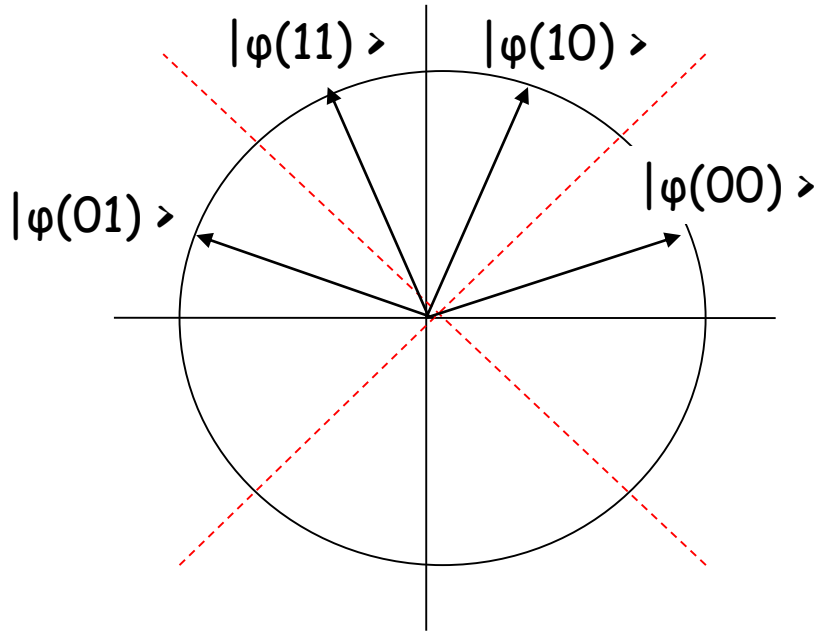
$$\frac{1}{\sqrt{2}}(|\varphi(00)\rangle|\varphi(00)\rangle + |\varphi(11)\rangle|\varphi(11)\rangle) = \frac{1}{\sqrt{2}}(|\varphi(01)\rangle|\varphi(01)\rangle + |\varphi(10)\rangle|\varphi(10)\rangle)$$



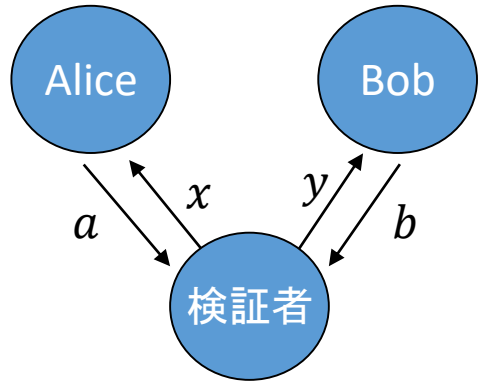
入力: 1 bit x (Alice); 1 bit y (Bob) ,
一様分布πにそって選択される

出力: 1 bit a (Alice); 1 bit b (Bob)

Alice と Bob が勝つ条件: $xy = a \oplus b$



QRAC ⇒ CHSH



Alice と Bob は1組のEPRペア $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$を共有

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

入力: 1 bit x (Alice); 1 bit y (Bob) ,
一様分布πにそって選択される

出力: 1 bit a (Alice); 1 bit b (Bob)

Alice と Bob が勝つ条件: $xy = a \oplus b$

Aliceの戦略:

$x = 0$ (resp. $= 1$)なら, $|\Phi^+\rangle$のAliceの部分を

$\{|\varphi(00)\rangle, |\varphi(11)\rangle\}$ (resp. $\{|\varphi(01)\rangle, |\varphi(10)\rangle\}$)で測定

$a = 0$ ($|\varphi(00)\rangle$ (resp. $|\varphi(01)\rangle$) が得られたとき)

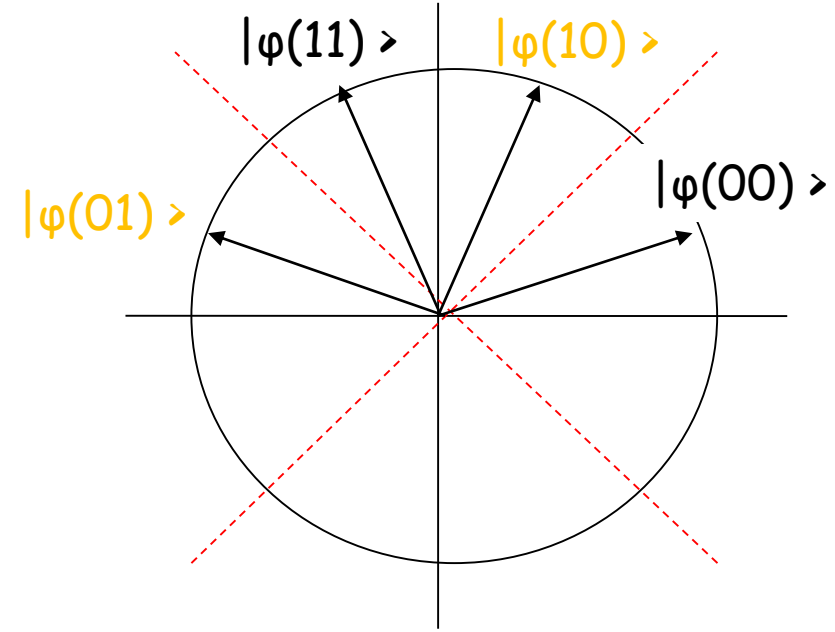
$a = 1$ ($|\varphi(11)\rangle$ (resp. $|\varphi(10)\rangle$) が得られたとき)

Bobの戦略

$y = 0$ (resp. $= 1$)なら(2,1,0.85)-QRACの第1ビット復号

(resp. 第2ビット復号)を実行.

$b =$ 復号によって得られた結果.



QRAC ⇒ CHSH

Aliceの戦略実行後を考えると・・:

$a = 0$ かつ $x = 0$ のとき EPRペアのBob側＝$|\varphi(00)\rangle$

$a = 1$ かつ $x = 0$ のとき EPRペアのBob側＝$|\varphi(11)\rangle$

$a = 0$ かつ $x = 1$ のとき EPRペアのBob側＝$|\varphi(01)\rangle$

$a = 1$ かつ $x = 1$ のとき EPRペアのBob側＝$|\varphi(10)\rangle$

つまり，Bob は状態 $|\varphi(a, x \oplus a)\rangle$ を得る.

Bob は $b = xy \oplus a$

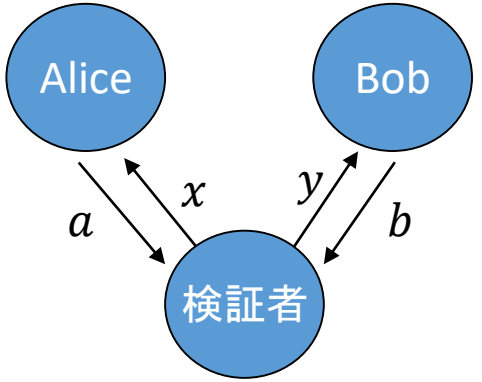
$=a$（$y = 0$の場合），

$=x \oplus a$（$y = 1$の場合）

を得ればゲームに勝利

(2,1,0.85)-QRACの復号化により，
最悪勝率0.85を達成

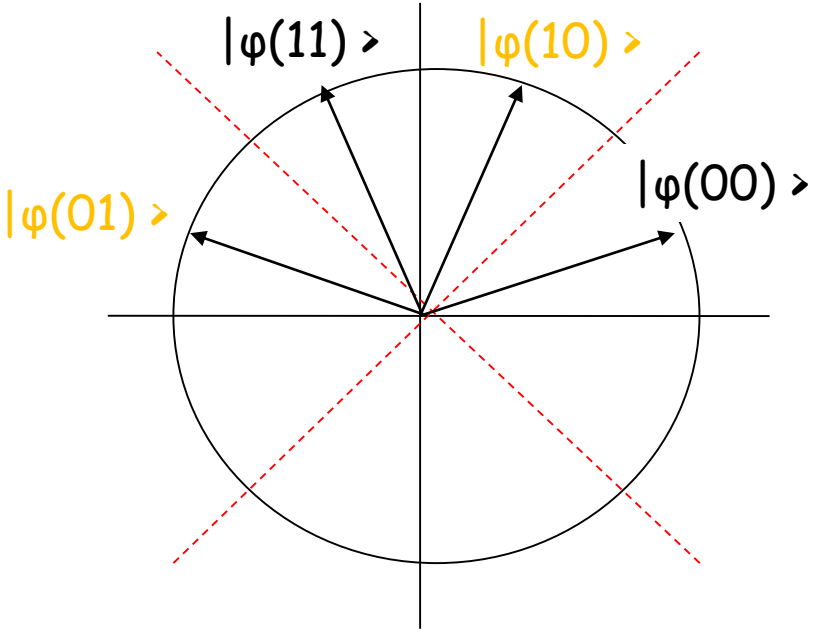
Aliceの測定値aが
$a = 0$に転んでも
$a = 1$に転んでも0.85
で勝てる



入力: 1 bit x (Alice); 1 bit y (Bob) ,
一様分布πにそって選択される

出力: 1 bit a (Alice); 1 bit b (Bob)

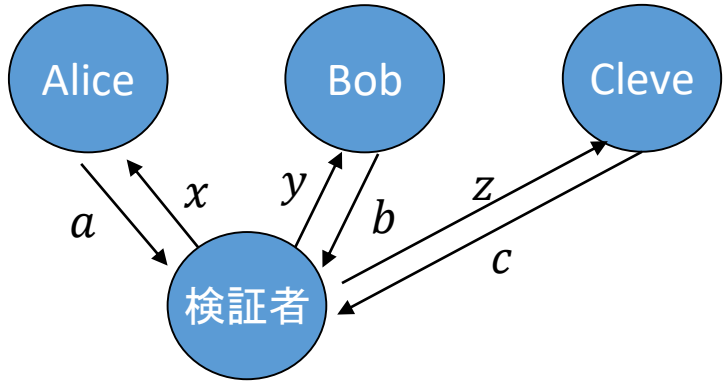
Alice と Bob が勝つ条件: $xy = a \oplus b$



Quantum Pseudo-Telepathy Games

- 古典で確率1で勝てないけど量子だと確率1で勝てるゲームは？
  - Quantum winning probability =1 vs Classical winning probability < 1
  - CHSH: (Q) ≒0.85 (C) 0.75
- Quantum Pseudo-Telepathy game
  - Magic-square game
  - GHZ game

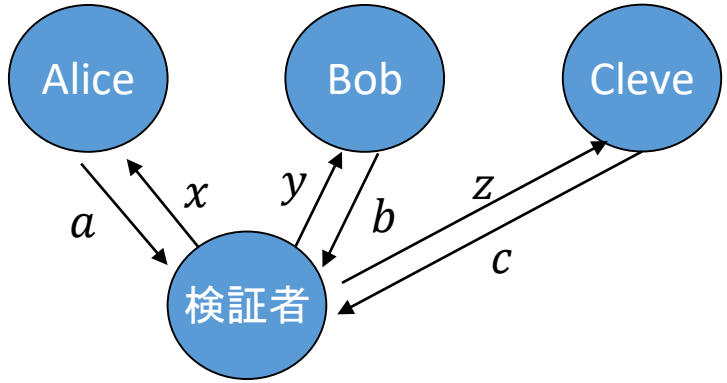
GHZ game



- GHZ (Greenberger-Horne-Zeilinger) state
  - $|GHZ\rangle := \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$
- GHZ game (Mermin parity game)
  - 入力: Alice $x \in \{0,1\}$, Bob $y \in \{0,1\}$, Cleve $z \in \{0,1\}$ (一様ランダム)
  - 約束: $x + y + z$は偶数
  - 出力: Alice $a \in \{0,1\}$, Bob $b \in \{0,1\}$, Cleve $c \in \{0,1\}$
  - 勝利条件: $a + b + c = \frac{x+y+z}{2} \bmod 2$
- 勝率(winning probability)
  - 古典(Classical) 3/4 vs 量子(Quantum) 1

x	y	z	勝つ条件
0	0	0	$a \oplus b \oplus c = 0$
0	1	1	$a \oplus b \oplus c = 1$
1	0	1	$a \oplus b \oplus c = 1$
1	1	0	$a \oplus b \oplus c = 1$

Quantum Strategy



勝利条件

$a + b + c = \frac{x+y+z}{2} \bmod 2$

1. A, B & C shares $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$
2. Each player changes the phase to i iff the input is 1
   - $\frac{x+y+z}{2} = 0$: the shared state is $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$
   - $\frac{x+y+z}{2} = 1$: it is $\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$
3. Each player applies H, and output the value measured in the comp. basis
   - $\frac{x+y+z}{2} = 0$: the shared state is $\frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)$
   - $\frac{x+y+z}{2} = 1$: it is $\frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle)$

x	y	z	勝つ条件
0	0	0	$a \oplus b \oplus c = 0$
0	1	1	$a \oplus b \oplus c = 1$
1	0	1	$a \oplus b \oplus c = 1$
1	1	0	$a \oplus b \oplus c = 1$

Quantum Protocols based on Entanglement

- 非局所性ゲーム(non-local game)
- 量子テレポーテーション(quantum teleportation)

Q. Can quantum states be sent without quantum channel?

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

Q. Can quantum states be sent without quantum channel?

If A knows $|\psi\rangle$

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

Q. Can quantum states be sent without quantum channel?

If A does not know $|\psi\rangle$

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

Q. Can quantum states be sent without quantum channel?

If A and B shares entanglement

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

量子テレポーテーション(Quantum teleportation)

設定：AliceとBobはEPR対$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$を共有している

目的：Aliceは Bobに2ビットを通信することで，自分が持つ未知の量子ビット

$|\chi\rangle = a|0\rangle + b|1\rangle$をBobに送る

量子テレポーテーション

設定：AliceとBobはEPR対$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$を共有している

目的：AliceはBobに2ビットを通信することで，自分が持つ未知の量子ビット$|\chi\rangle = a|0\rangle + b|1\rangle$をBobに送る

プロトコル：$|\chi\rangle$のレジスタをXとする

1. AliceはX,AをBell基底で測定：$|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$に対応する測定値を00,01,10,11としたとき，その測定値をBobに送る

ただし，$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), |\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$

量子テレポーテーション

設定：AliceとBobはEPR対$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$を共有している

目的：AliceはBobに2ビットを通信することで，自分が持つ未知の量子ビット$|\chi\rangle = a|0\rangle + b|1\rangle$をBobに送る

プロトコル：$|\chi\rangle$のレジスタをXとする

1. AliceはX,AをBell基底で測定：$|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$に対応する測定値を00,01,10,11としたとき，その測定値をBobに送る：$\left|\Phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \left|\Psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$
2. BobはBに次のユニタリを行う
   - 00のときはI（何もしない）
   - 01のときはZ
   - 10のときはX
   - 11のときはXZ

量子テレポーテーション（解析）

設定：AliceとBobはEPR対$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$を共有している

目的：Aliceは2ビットを通信することで自分が持つ未知の量子ビット$|\chi\rangle = a|0\rangle + b|1\rangle$をBobに送る

プロトコル：$|\chi\rangle$のレジスタをXとする

1. AliceはX,AをBell基底で測定：$|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$に対応する測定値を00,01,10,11としたとき，その測定値をBobに送る:
   $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), |\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$
2. BobはBに次のユニタリを行う
   - 00のときはI（何もしない）
   - 01のときはZ
   - 10のときはX
   - 11のときはXZ

Point:

$$|\chi\rangle|\Phi^+\rangle = \frac{1}{2}(|\Phi^+\rangle|\chi\rangle + |\Phi^-\rangle Z|\chi\rangle + |\Psi^+\rangle X|\chi\rangle + |\Psi^-\rangle XZ|\chi\rangle)$$

Merits of Quantum Teleportation

- 決まった量子状態（EPR対）さえ用意しておけば，後は測定（＋古典通信）だけで量子状態が送れる
- 測定型量子計算(measurement based quantum computing)

量子計算量クラス
(Quantum Complexity Classes)

Complexity Zoo

- 計算量クラス(complexity class)
  - 計算量に関する条件のもとで定義された計算問題，とくにYES/NO問題，の集まり
  - 様々な計算問題を計算の複雑さの観点からクラス分けしたい
  - Complexity Zoo (https://complexityzoo.net/Complexity_Zoo)

A

A_0PP - AC - AC^0 - $AC^0[m]$ - AC^1 - ACC^0 - AH - AL - ALL - ALOGTIME - AlgP/poly - Almost-NP - Almost-P - Almost-PSPACE - AM - AM_{EXP} - AM ∩ coAM - AM[polylog] - AmpMP - AmpP-BQP - AP - APP - APX - ATIME - AUC-SPACE(f(n)) - AuxPDA - AVBPP - AvgE - AvgP - AW[P] - AWPP - AW[SAT] - AW[*] - AW[t] - AxP - AxPP

B

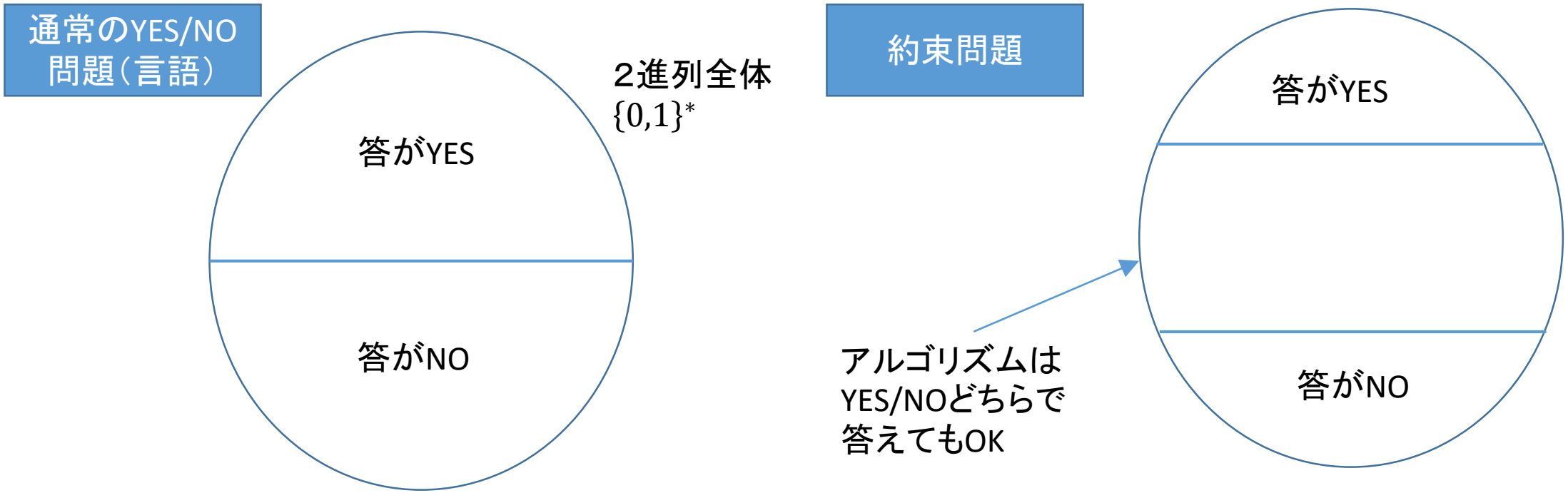
βP - BH - $BP_d(P)$ - BPE - BPEE - $BP_HSPACE(f(n))$ - BPL - BP•NP - BPP - BPP^{cc} - BPP^{cc} - BPP^{KT} - BPP/log - BPP/mlog - BPP//log - BPP/rlog - BPP-OBDD - BPP_{path} - BPQP - BPSPACE(f(n)) - BPTIME(f(n)) - BQNC - BQNP - BQP - BQP/log - BQP/poly - BQP/mlog - BQP/mpoly - BQP/qlog - BQP/qpoly - BQP-OBDD - BQPSPACE - BQP_{CTC} - BQP_{tt}/poly - BQTIME(f(n)) - k-BWBP

C

…

（約束）問題: Promise Problems

- 量子計算が扱う問題には物理の確率的な現象の問題に関連するものもあり，YES，NOの境目にある程度のギャップがないと量子計算の手におえないものもある　⇒　約束問題（promise problem）



P & NP & PSPACE

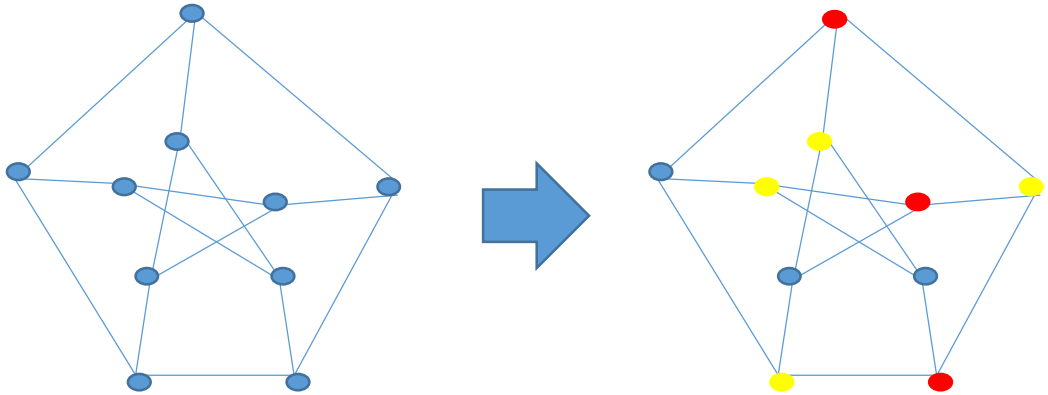
- P (Polynomial-time)
  - 多項式時間で判定可能な問題のクラス
- NP (Nondeterministic Polynomial-time)
  - 多項式時間で答えがYESであることを検証可能な問題のクラス
- P vs NP問題 : P≠NP?
  - 計算量の分野の創世記以来の最大の未解決問題
  - クレイ研究所により数学における7大未解決問題に選定（解けば100万ドル）
- PSPACE : 多項式量のメモリ(space)で判定可能な問題のクラス
  - P⊆NP⊆PSPACE ⊆EXP
  - P≠NPどころかPSPACEとPが違うかさえわかってない

NP

問題$A = (A_{yes}, A_{no})$がNP に属するとは，以下の2条件をみたす多項式時間アルゴリズム M が存在：任意の入力 x に対して
(完全性) $x \in A_{yes}$ なら，ある証明(proof) w が存在して $M(x,w) = \text{accept}$;
(健全性) $x \in A_{no}$なら，どんなw に対しても $M(x,w) = \text{reject}$.

3彩色問題 3COL

入力: グラフ $G = (V, E)$
Yes: すべての隣り合う2頂点が異なる色になるように3色で塗り分け可能
No: そのような塗り分けが存在しない



乱択アルゴリズムのクラスBPP

- 乱択アルゴリズム(randomized algorithm)

アルゴリズムの動作をコインを振って決めてよし．ちょっとくらい間違ってもOK.

  - そもそもハードウェアにエラーはつきもの
  - ソフトウェアも無視できる程度のエラーはOKでしょ！
  - 素数判定など応用多数

- BPP (Bounded-error Probabilistic Polynomial-time)

多項式時間乱択アルゴリズムで（どんな入力においても）確率2/3以上で正しく判定可能な問題のクラス

  - 今日理論計算機科学を語る上で欠かせない基本概念
  - 誤り確率1/3は多項式回の繰り返しで1/expに下げられる.
  - 多くのクラスはNPとBPPの概念を基本にしている
  - $P \subseteq BPP \subseteq PSPACE$

内容

- 古典計算量クラス
- BQP
- 量子対話型証明

BQP：効率的に量子コンピュータで解ける問題のクラス

- BQP (Bounded-error Quantum Polynomial-time)
  - 多項式時間量子アルゴリズムで確率2/3以上で判定可能な問題のクラス [BV97]
- BQP vs BPP
  - 量子計算>古典計算?
  - FACTORING={(N,k)| Nはkより小さい素因数を持つか}はBQPに入るがBPPに入りそうにない [Sho97]

Q. BQP vs NP

- NP ⊄ BQP?
- BQP ⊄ NP

量子計算の古典計算による模倣

- ユニタリ行列による全体的な状態変化を古典計算機で模倣
  - n量子ビット回路の場合，2^n次ユニタリ行列を2^n次ベクトルに順次かけていく
  - 指数時間を必要とする
- 量子ゲートによる局所的な変化を計算基底状態の振幅ごとに追跡する（Feynman’s approach）
  - やはり指数時間を必要とする
  - メモリは多項式時間にできる

Simulations of BQP Computation

- BQP ⊆ EXP: 指数時間あれば古典計算で模倣できる
  - 量子計算は振幅を重みとしてもつ計算木として書ける
  - 多項式時間計算の場合，計算木のサイズは指数
- BQP ⊆ PSPACE: 多項式メモリが使えれば古典計算で模倣できる
  - 計算木の各パスの振幅の積を1つ1つ計算してゆく
  - 最終状態は$\alpha|L(x)\rangle + \beta|\neq L(x)\rangle$のようにできる（by Bennett）
- P ⊆BQP ⊆ PSPACE & P ⊆NP ⊆ PSPACE

Q. BQP vs NP

- NP ⊄ BQP?
- BQP ⊄ NP

NP ⊈ BQPとなるオラクル

- 問題OR

入力（オラクル）: $f: \{0,1\}^n \to \{0,1\}$

YES: $\exists x\ [f(x) = 1]$

NO: $\forall x\ [f(x) = 0]$

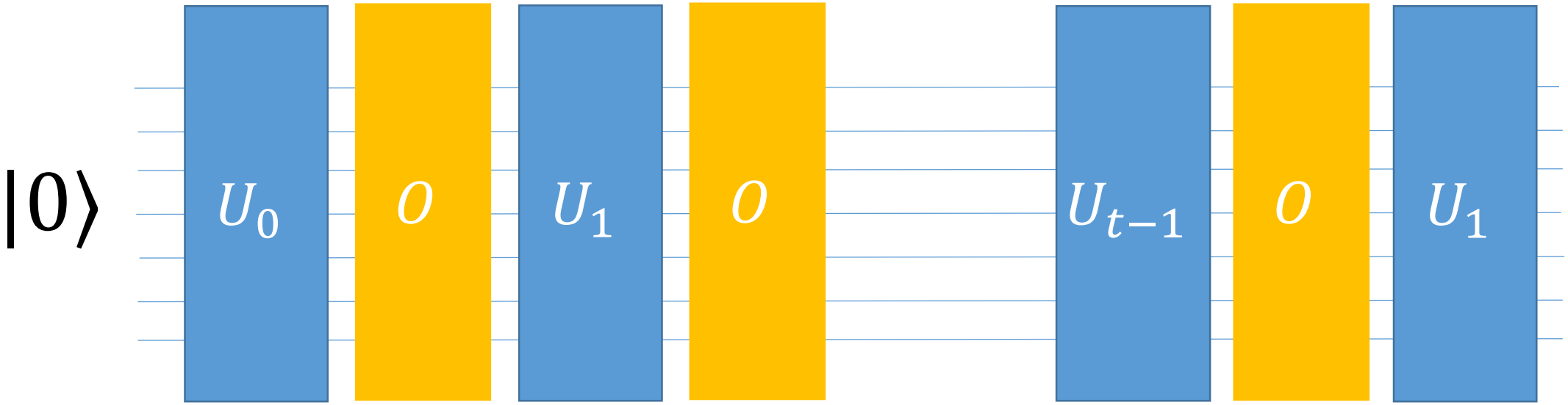
- NPアルゴリズムでは1回の質問で解ける

✓BQPアルゴリズムでは$\Omega(\sqrt{2^n})$回の質問が必要（Groverがベスト）

- ➢敵対者論法 [BBBV97, Amb02]
- ➢多項式法 [BBCMW01]

量子質問計算量(quantum query complexity)

- オラクルへの質問回数だけ考える場合，量子回路はオラクルを表すユニタリ$O\colon |x,b,z\rangle \mapsto |x,b \oplus f(x),z\rangle$とオラクルに無関係なユニタリ$U_i$の繰り返しと考えられる [BBCMW01]



多項式法(polynomial method)

- $f:\{0,1\}^n \to \{0,1\}$を$N = 2^n$ビット列$y = y_1 y_2 \cdots y_N$とみなす（y_jはj番目のnビット列）と量子アルゴリズム

$$\left|\psi_t^y\right\rangle = U_t O_y U_{t-1} O_y \cdots O_y U_0 |0\rangle$$

がYESを出力する確率は高々次数$2t$のN変数多項式として表現できる

- OR(y):=1 if $\exists y_j [y_j = 1]$; =0 otherwise を量子アルゴリズムが質問回数tで高確率で解くには次数$2t$で関数ORを近似する必要がある
- しかし，関数ORを近似する多項式は$\Omega(\sqrt{N})$の次数を必要とする

敵対者論法(adversary method)

- OR$(y) = 1$なる$y \neq 0^N$とOR$(z) = 0$なるz $= 0^N$に対して量子アルゴリズムの最終状態$|\psi_t^y\rangle$と$|\psi_t^z\rangle$は（出力部がかなり違うので）ほぼ直交してるべし
- 一方，双方の初期状態は同じ
- 途中の状態の内積の「重みつき平均」

$$W_k = \sum_y w(y,z)\langle\psi_k^z|\psi_k^y\rangle \text{ (ただし，重みの総和} \sum_y w(y,z) = 1)$$

を考えると$W_0 = 1, W_t \approx 0$

- $|W_{k+1} - W_k| \leq O(\frac{1}{\sqrt{N}})$となるよう重み$w(y,z)$を選択

BQP：効率的に量子コンピュータで解ける問題のクラス

BQP vs NP

- ✓NPはBQPに入りそうにない（NP完全問題は量子コンピュータで速く解けそうにない）
- Q. BQPはNPに入るのか?
- A. やはり入りそうにない:
- BQP ⊄ NPなるオラクルが存在（例：Simon’s problem）

Power & Limitation of BQP

- BQP ⊆ EXP: 指数時間あれば古典計算で模倣できる
  - 量子計算は振幅を重みとしてもつ計算木として書ける
  - 多項式時間計算の場合，計算木のサイズは指数
- BQP ⊆ PSPACE: 多項式メモリが使えれば古典計算で模倣できる
  - 計算木の各パスの振幅の積を1つ1つ計算してゆく
  - 最終状態は$\alpha|L(x)\rangle + \beta|\neq L(x)\rangle$のようにできる（by Bennett）
- BQP ⊄ NPなるオラクルが存在

Q. NPより高いクラスにとって難しくBQPで優しいものは?

3 interpretations of NP

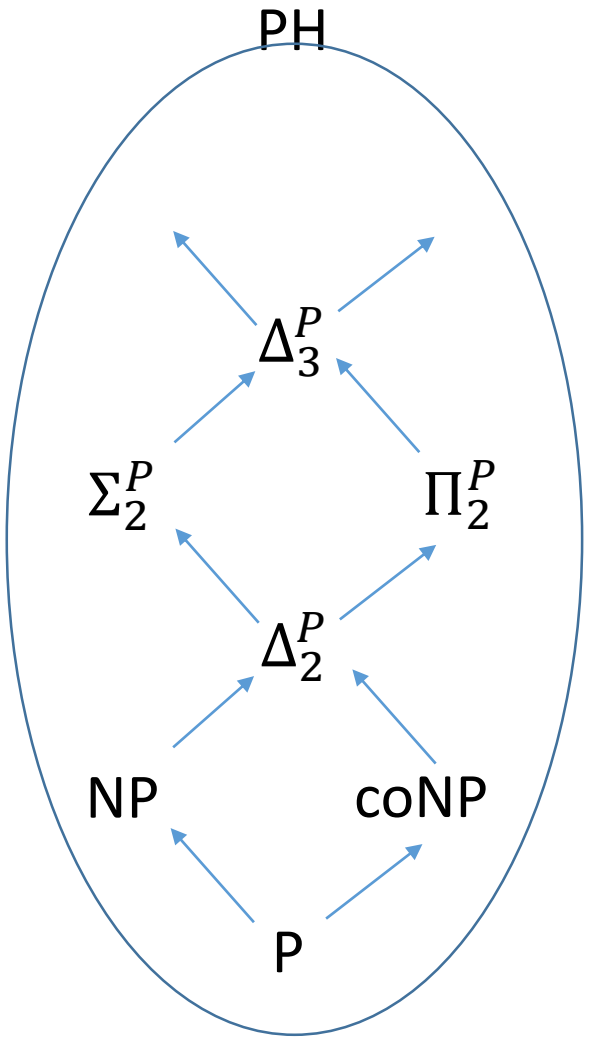
- 非決定性アルゴリズムとしての解釈
  - クラス名NP (Nondeterministic Polynomial-time)の由来
  - 類するクラス：PP, #Pなど
- 論理構造(logical structure)としての解釈
  - NPの条件を存在記号ヨで解釈
  - NP=ヨP, coNP=∀P, …
  - 類するクラス: PH（多項式階層）
- 証明系(proof system)としての解釈
  - NPを通信プロトコルとして解釈
  - 類するクラス：MA, AM, IPなど

NP & coNP

- $A = (A_{yes}, A_{no}) \in$ NP:=∃P ⇔ ∃ $B = (B_{yes}, B_{no}) \in$ P, ∃q: 多項式
  - $x \in A_{yes} \rightarrow \exists y \in \{0,1\}^{q(|x|)}[\langle x, y\rangle \in B_{yes}]$
  - $x \in A_{no} \rightarrow \forall y \in \{0,1\}^{q(|x|)}[\langle x, y\rangle \in B_{no}]$
- $A = (A_{yes}, A_{no}) \in$ coNP:=∀P ⇔ ∃ $B = (B_{yes}, B_{no}) \in$ P, ∃q: 多項式
  - $x \in A_{yes} \rightarrow \forall y \in \{0,1\}^{q(|x|)}[\langle x, y\rangle \in B_{yes}]$
  - $x \in A_{no} \rightarrow \exists y \in \{0,1\}^{q(|x|)}[\langle x, y\rangle \in B_{no}]$

多項式階層（Polynomial Hierarchy）

- $A = (A_{yes}, A_{no}) \in$ NP:=∃P ⇔ ∃ $B = (B_{yes}, B_{no}) \in$ P, ∃q: 多項式
  - $x \in A_{yes} \rightarrow \exists y \in \{0,1\}^{q(|x|)}[\langle x, y\rangle \in B_{yes}]$
  - $x \in A_{no} \rightarrow \forall y \in \{0,1\}^{q(|x|)}[\langle x, y\rangle \in B_{no}]$
- $A = (A_{yes}, A_{no}) \in$ co-NP:=∀P ⇔ ∃ $B = (B_{yes}, B_{no}) \in$ P, ∃q: 多項式
  - $x \in A_{yes} \rightarrow \forall y \in \{0,1\}^{q(|x|)}[\langle x, y\rangle \in B_{yes}]$
  - $x \in A_{no} \rightarrow \exists y \in \{0,1\}^{q(|x|)}[\langle x, y\rangle \in B_{no}]$
- $A = (A_{yes}, A_{no}) \in \Sigma_2^P$:= ∃∀P ⇔ ∃ $B = (B_{yes}, B_{no}) \in$ P, ∃q: 多項式
  - $x \in A_{yes} \rightarrow \exists y \in \{0,1\}^{q(|x|)} \forall z \in \{0,1\}^{q(|x|)}[\langle x, y, z\rangle \in B_{yes}]$
  - $x \in A_{no} \rightarrow \forall y \in \{0,1\}^{q(|x|)} \exists z \in \{0,1\}^{q(|x|)}[\langle x, y, z\rangle \in B_{no}]$
- PH:=$\bigcup_k \Sigma_k^P$



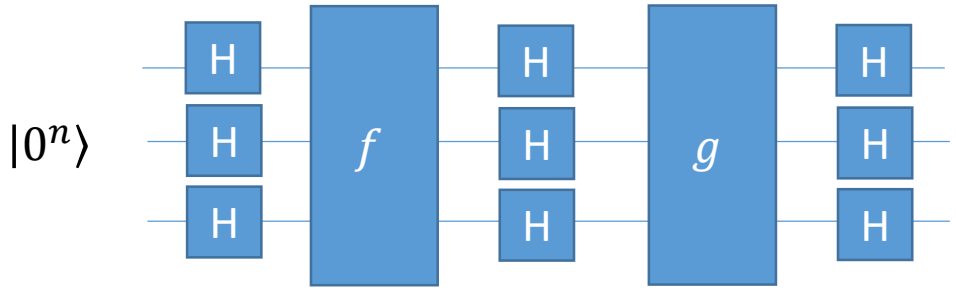
多項式階層（Polynomial Hierarchy）vs BQP

✓BQP⊈PHなるオラクルの存在 [RT19]

- 「2つのブール関数のフーリエ基底での相関を見る」という量子計算に有利な問題
- Fourier Checking [Aar10]
  - 入力: $f, g: \{0,1\}^n \to \{-1,1\}$
  - 約束

    (a) $\mathrm{Col}(f,g) \coloneqq \frac{1}{2^{3n}} \left(\sum_{x,y \in \{0,1\}^n} f(x)(-1)^{x \cdot y} g(y) \right)^2 \geq 0.05$

    (b) $\mathrm{Col}(f,g) \leq 0.01$
  - 出力: (a) ならYES, (b)ならNO



内容

- 古典計算量クラス
- BQP
- 量子対話型証明(quantum interactive proofs)

Why QMA（＝量子NP）& 量子対話型証明?

- 古典計算量クラスで最重要概念だから
  - なぜ重要か：効率的な検証の概念をうまく捉えている
- 多くの自然な問題がQMAや量子対話型証明で特徴づけられる
- エンタングルメントなどの量子性に対する計算量理論的アプローチ
  - 多証明者量子対話型証明
  - QMA(2)

3 interpretations of NP

- 非決定性アルゴリズムとしての解釈
  - クラス名NP (Nondeterministic Polynomial-time)の由来
  - 類するクラス：PP, #Pなど
- 論理構造(logical structure)としての解釈
  - NPの条件を存在記号ヨで解釈
  - NP=ヨP, coNP=∀P, …
  - 類するクラス: PH（多項式階層）
- 証明系(proof system)としての解釈
  - NPを通信プロトコルとして解釈
  - 類するクラス：MA, AM, IPなど

NP: Interpretation as proof systems

証明者(prover)
能力無制限

証明(proof)
w

検証者(verifier)
多項式時間アルゴリズム

yes/no ?

$A = (A_{yes}, A_{no}) \in \mathrm{NP} \Leftrightarrow$

以下の2条件をみたす多項式時間アルゴリズム V が存在:

(完全性: completeness) $x \in A_{yes} \rightarrow \exists w\ [V(x,w) = \mathrm{accept}]$

(健全性: soundness) $x \in A_{no} \rightarrow \forall w\ [V(x,w) = \mathrm{reject}]$

QMA (Quantum Merlin-Arthur): 量子版NP

- $A \in$ QMA ⇔多項式時間量子アルゴリズム V が存在:
  - (完全性) $x \in A_{yes} \rightarrow \exists|\varphi\rangle$: $\Pr[V(x,|\varphi\rangle) = \text{accept}] \geq 2/3$
  - (健全性) $x \in A_{no} \rightarrow \forall|\varphi\rangle$: $\Pr[V(x,|\varphi\rangle) = \text{reject}] \geq 2/3$

証明者 (Merlin)
能力無制限
＝任意の量子的
操作

量子証明
$|\varphi\rangle$

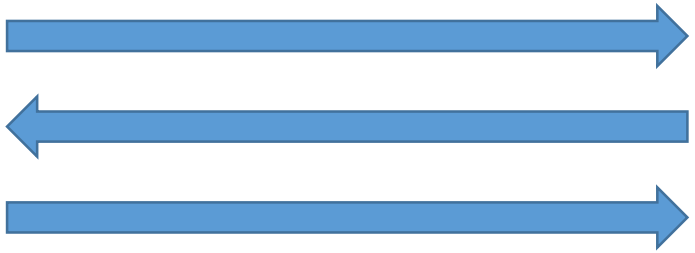
検証者 (Arthur)
多項式時間
量子アルゴリズム

yes/no ?

対話型証明(Interactive Proof)

- 検証を「証明者との対話」に拡張
  - 暗号的動機（ゼロ知識証明）: Goldwasser-Micali-Rackoff [GMR85]
  - 群論的問題の計算複雑さ: Babai [Bab85]
- 計算量理論や暗号理論の基礎概念
  - ゼロ知識証明(zero knowledge)
  - 確率検査証明（PCP: probabilistic checkable proof）
  - 近似アルゴリズムの限界

対話型証明のクラス IP



yes/no ?

証明者
能力無制限

対話による通信

検証者
多項式時間乱択アルゴリズム

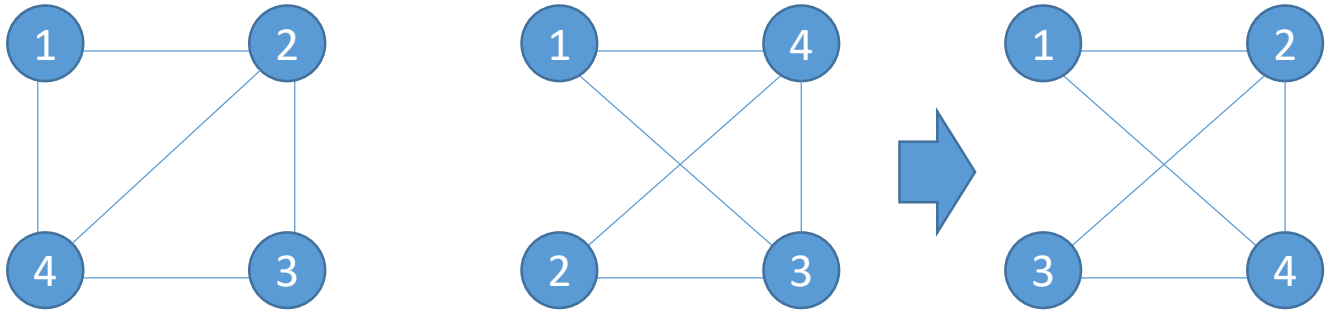
$A = (A_{yes}, A_{no}) \in$ IP ⇔

以下の2条件をみたす多項式時間プロトコルが存在:

(完全性) $x \in A_{yes}$ → 検証者が確率2/3以上で受理する(acceptを出力する)ような証明者の(対話に関する)戦略が存在する
(健全性) $x \in A_{no}$ → 証明者がどんな戦略をとっても検証者は確率2/3以上で拒否(rejectを出力する)

GNI: Example of Interactive Proofs

グラフ同型性判定 (GI)
入力: グラフ $G_1 = (V, E_1),\ G_2 = (V, E_2)$
Yes: G_1 と G_2 が同型: $\exists V$上の置換 π $\forall$2頂点$v, w[(v, w) \in E_1 \Leftrightarrow (\pi(v), \pi(w)) \in E_2]$
No: G_1 と G_2 が同型でない



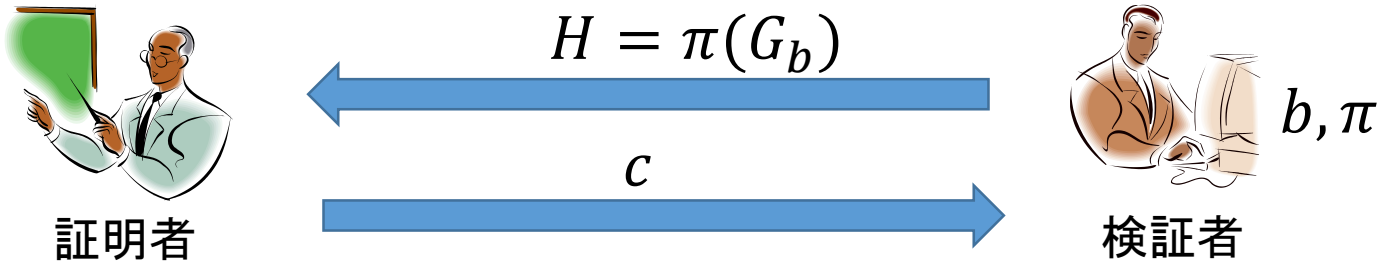
GNI ∈NP?

グラフ非同型性判定 (GNI)
入力: グラフ $G_1 = (V, E_1),\ G_2 = (V, E_2)$
Yes: G_1 と G_2 が同型でない
No: G_1 と G_2 が同型

Interactive Proof for GNI

GNIに対する対話型証明

1. 検証者は $b \in \{0,1\}$ とV上の置換 π を一様ランダムに選択し$H = \pi(G_b)$を送付
2. 証明者は $c \in \{0,1\}$ を送付
3. 検証者は $b = c$ なら受理, そうでなければ拒否



グラフ非同型性判定 (GNI)

入力: グラフ $G_1 = (V, E_1),\ G_2 = (V, E_2)$

Yes: G_1 と G_2 が同型でない

No: G_1 と G_2 が同型

量子対話型証明(Quantum Interactive Proof)

証明者
能力無制限

量子通信

検証者
多項式時間
量子アルゴリズム

yes/no ?

$A = (A_{yes}, A_{no}) \in$ QIP ⇔

以下の2条件をみたす多項式時間プロトコルが存在:

(完全性) $x \in A_{yes}$ → 検証者が確率2/3以上で受理する(acceptを出力する)ような証明者の(対話に関する)戦略が存在する
(健全性) $x \in A_{no}$ → 証明者がどんな戦略をとっても検証者は確率2/3以上で拒否(rejectを出力する)

量子対話型証明(Quantum Interactive Proof)

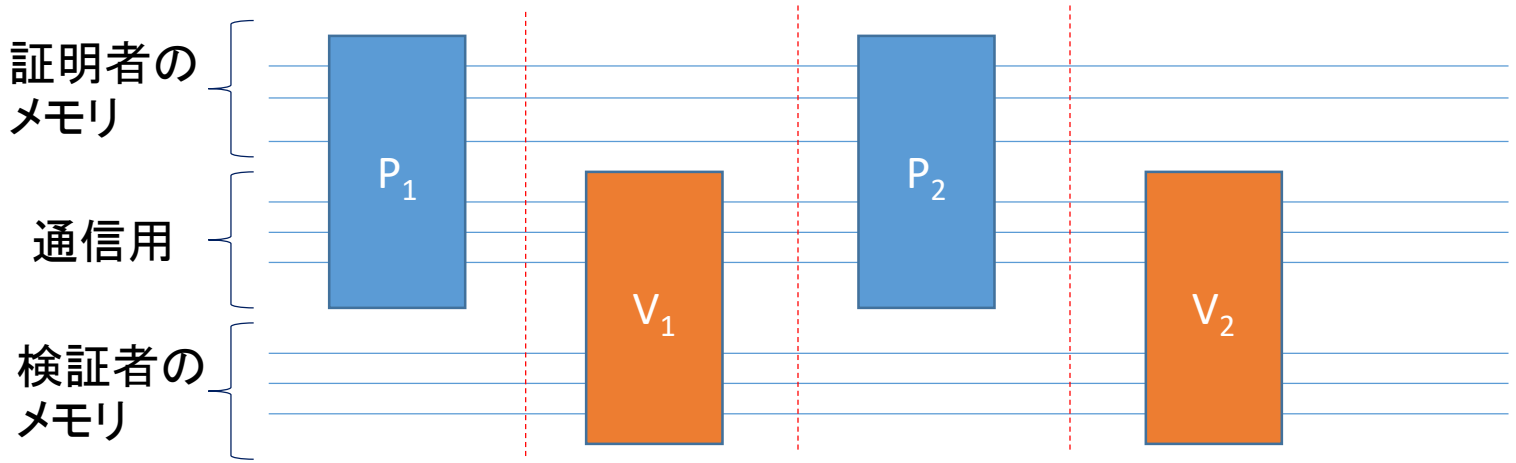
$A \in \mathrm{QIP}(k)$ ⇔

以下の2条件をみたすk回通信多項式時間プロトコルが存在:

(完全性) $x \in A_{yes}$ → 検証者が確率2/3以上で受理する(acceptを出力する)ような証明者の(対話に関する)戦略が存在する

(健全性) $x \in A_{no}$ → 証明者がどんな戦略をとっても検証者は確率2/3以上で拒否(rejectを出力する)

QIP(3)

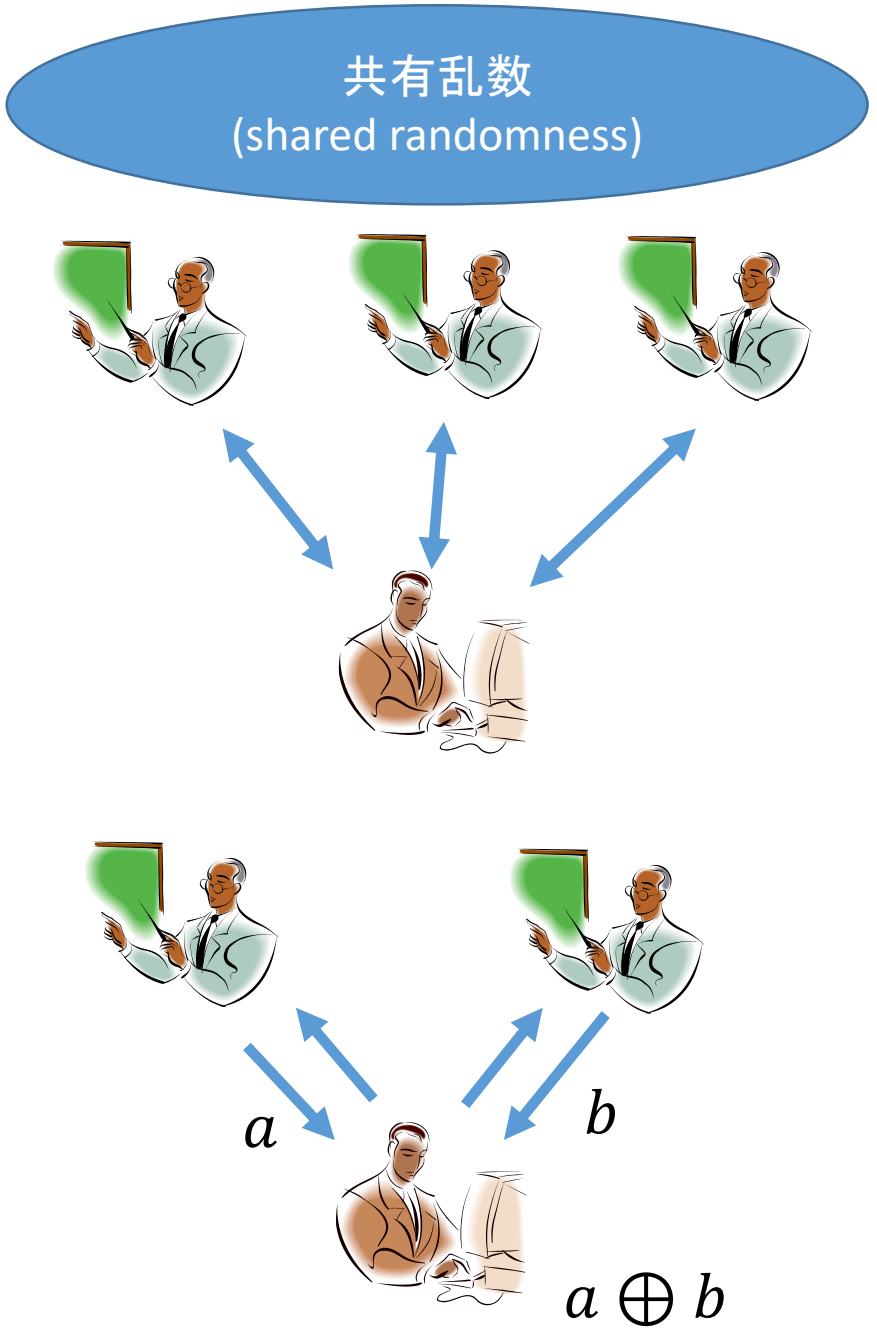


IP vs QIP

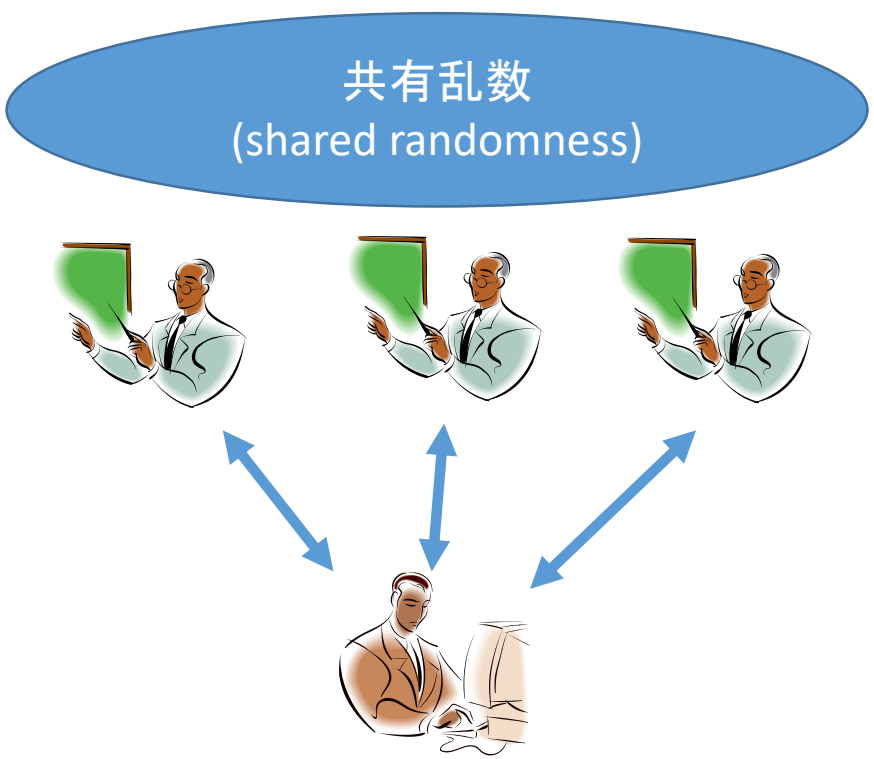
- 計算量クラスとしては古典=量子!
  - IP=PSPACE [LFKN92, Sha92]
    - PSPACE計算を多項式に符号化することで効率的にチェック
  - QIP=PSPACE [JJUW11]
- 通信回数を制限すると(多分)古典<量子
  - QIP=QIP(3)：量子対話型証明は3回の通信でOK！[Wat03, KW00]
  - 任意の定数$k \geq 3$に対して，IP(k)=IP(2)=AM < PSPACE [Bab85, GS86]
  - QIP(2)の能力は未開

MIP: 多証明者対話型証明 (multi-prover interactive proof)

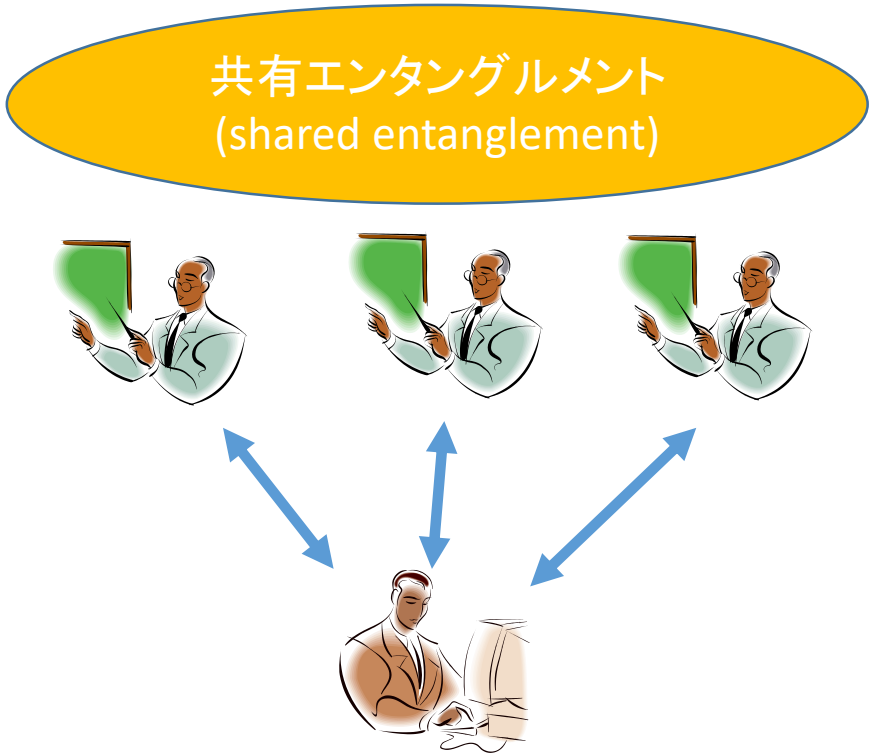
- 証明者の人数が複数になる（証明者同士はプロトコルの実行中通信できない）
- MIP=NEXP [BFL91]
  - NEXP=NPの指数時間版（PSPACEよりはるかに上のクラス）
  - 多証明者を利用することの計算量的有効性
- NEXP=XOR-MIP(2,2) [FL92]
  - MIP(m,k):=m人の証明者と各々高々k回通信するMIPプロトコルで検証可能な問題のクラス
  - XOR-は各証明者から1ビットもらってXOR取ったものを検証者の答えとすることを意味する



MIP*: What if provers share entanglement?



MIP

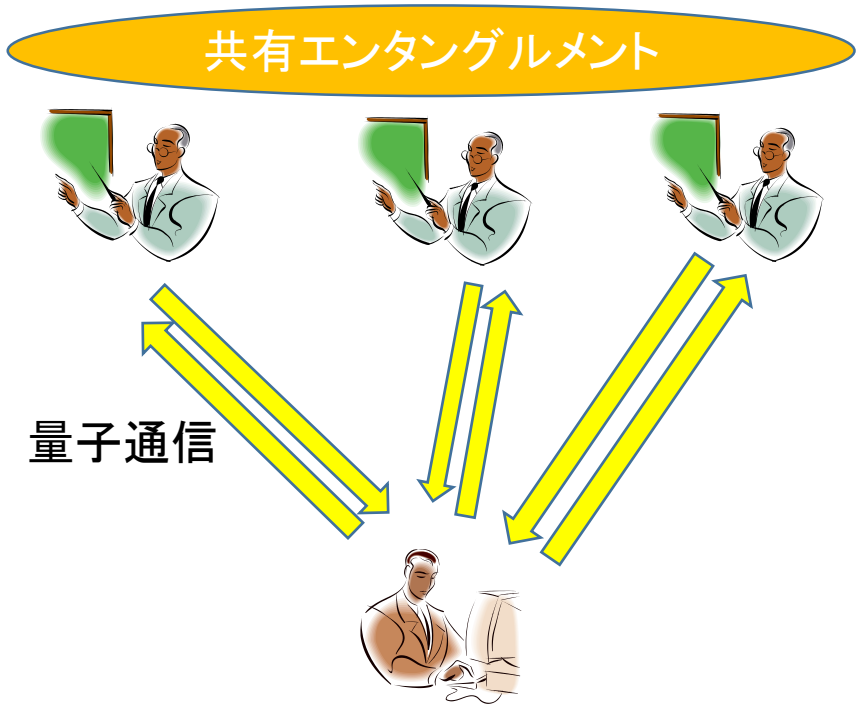


MIP*

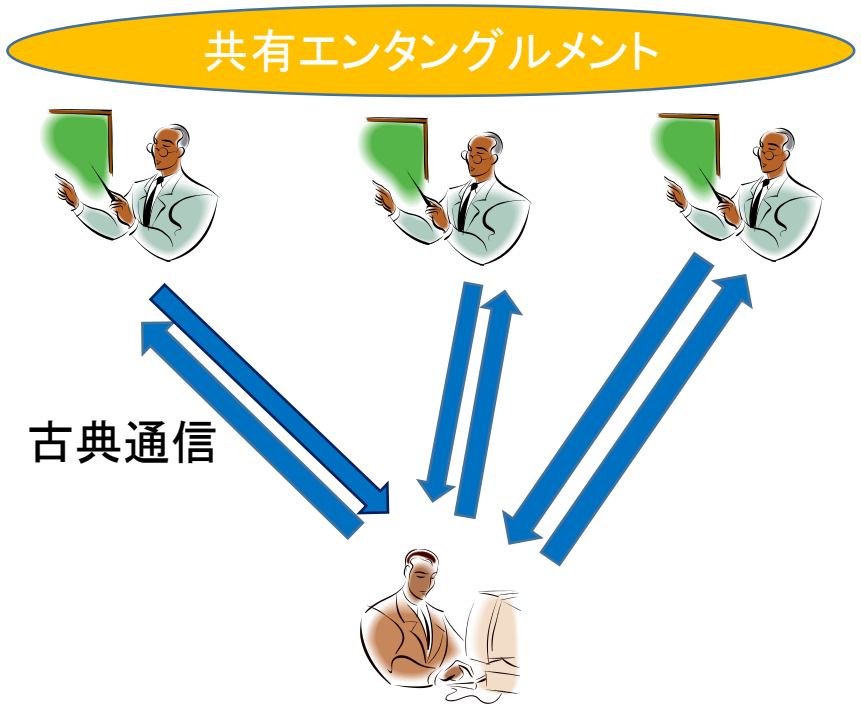
Classical verifier & communication are enough for entangled provers

- QMIP*=MIP*　[RUV13]
  - 検証者と証明者の間の通信と検証者は古典でも量子でも差がない

QMIP*



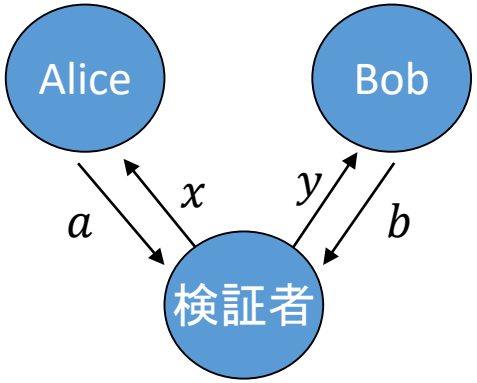
MIP* [CHTW04]



Rigidity of CHSH game

$$\left|\langle A_0B_0\rangle+\langle A_1B_0\rangle+\langle A_0B_1\rangle-\langle A_1B_1\rangle\right|\le 2$$

Clauser-Horne-Shimony-Holtの不等式(1969)を
ゲームとして解釈すると



入力: 1 bit x (Alice); 1 bit y (Bob) ,
一様分布πにそって選択される

出力: 1 bit a (Alice); 1 bit b (Bob)

Alice と Bob が勝つ条件: $xy = a \oplus b$

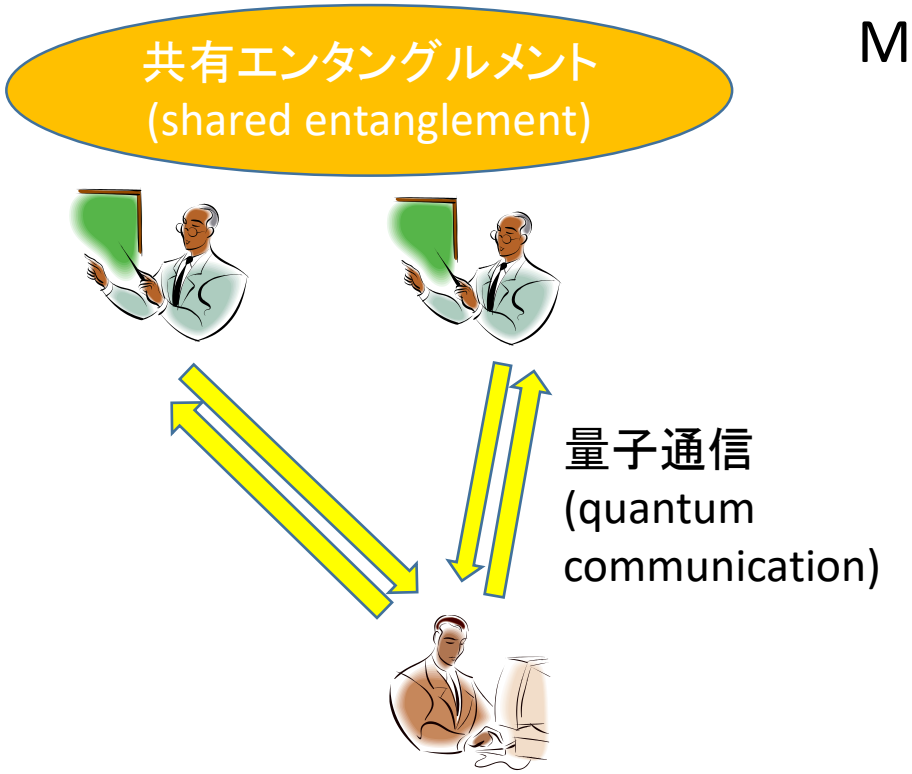
x	y	勝つ条件
0	0	$a \oplus b = 0$
0	1	$a \oplus b = 0$
1	0	$a \oplus b = 0$
1	1	$a \oplus b = 1$

- 古典の勝率 0.75
- 量子の勝率 約0.85

この勝率を達成する方法は唯1つ

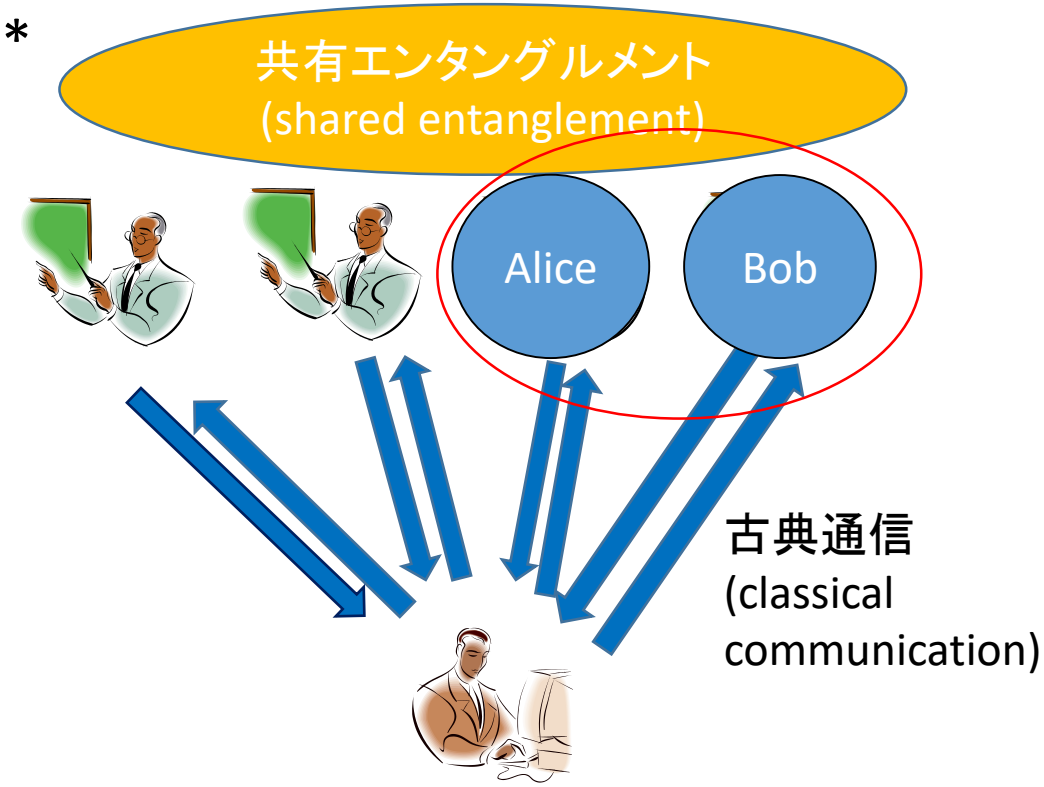
QMIP*=MIP*

QMIP*



検証者 量子アルゴリズム

MIP*



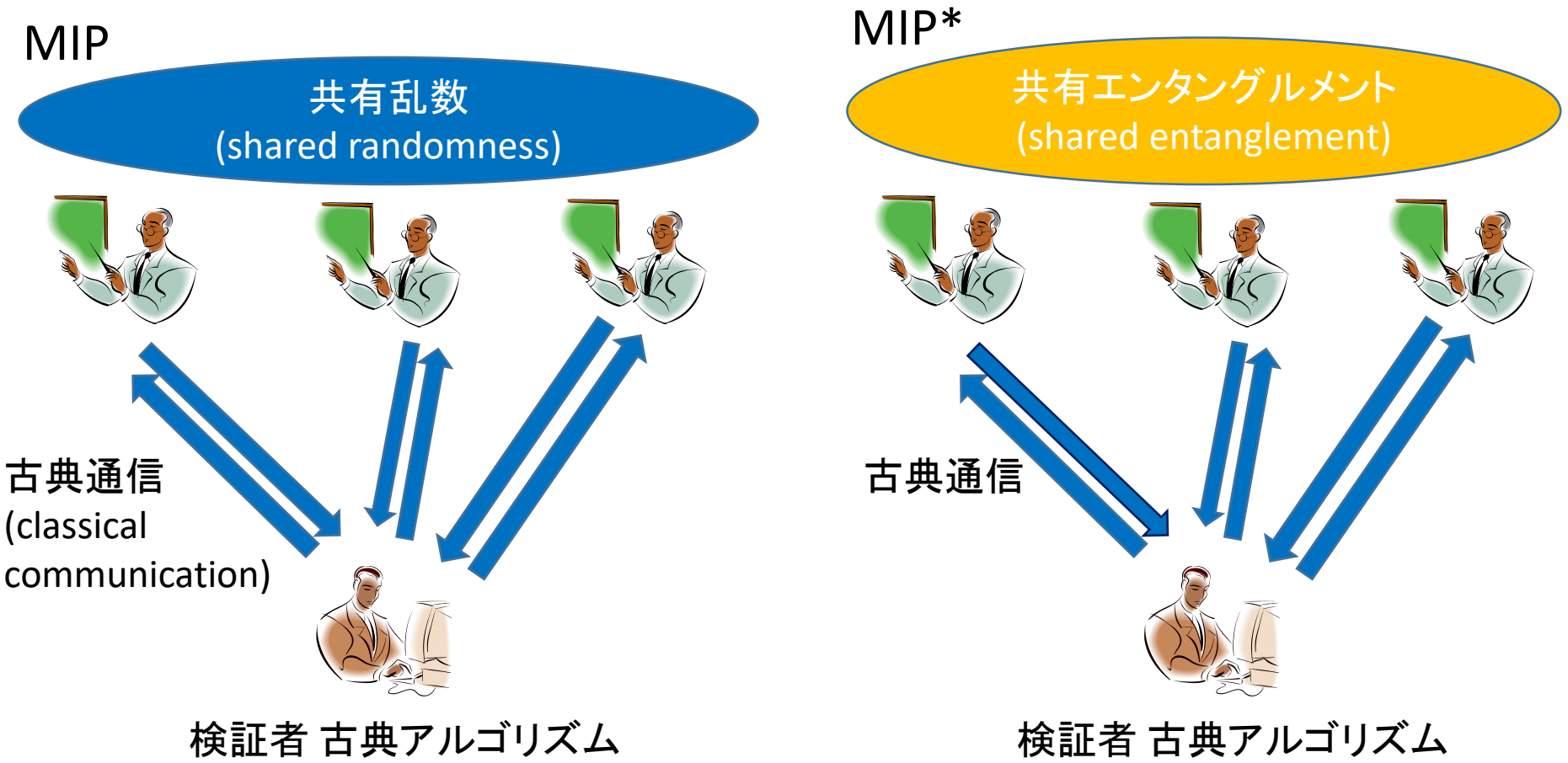
検証者 古典アルゴリズム

key point

- QMIP*のプロトコルを証明者2名追加することで証明者達にシミュレートさせる
- 量子ゲートテレポーテーション[GC00]をもとに検証者の計算を委託
- 証明者が正しく委託された計算を行っているかをCHSHゲームを交えることでテスト

MIP vs MIP*

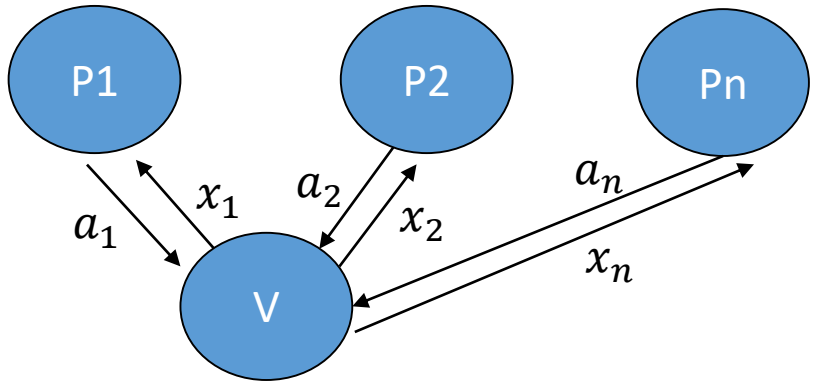
- MIPとMIP*の違いは証明者間のエンタングルメントの有無だけ



MIP vs MIP*

- MIPとMIP*の違いは証明者間のエンタングルメントの有無だけ
- しかし，証明者間のエンタングルメントは対話型証明系の能力に正にも負にも働きうる！
  - MIP* ⊆ MIPは非自明：完全性においては証明者がエンタングルメントを利用して検証者をうまく受理に導けるかも
  - MIP ⊆ MIP*も非自明！：健全性においては証明者がエンタングルメントを悪用して検証者が間違って受理するように導くかも

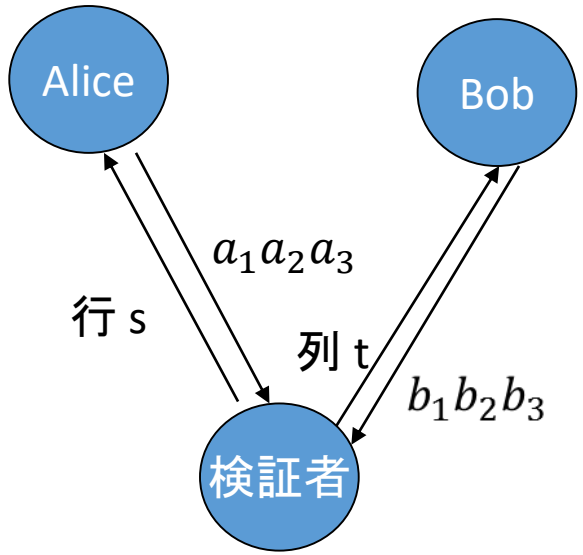
Nonlocal game vs MIP*



- 非局所ゲーム$G = (Q, A, \pi, V)$
  - Q: 質問の集合
  - A: 答の集合
  - π: $Q^n \to [0,1]$: 質問の確率分布
  - V: $Q^n \times A^n \to \{0,1\}$: 勝利条件
- Classical (Quantum) Game Value
  - 入力：非局所ゲーム
  - 出力：n人の古典(量子)プレーヤーの最大勝利確率
- 非局所ゲームは指数的にサイズダウンしたMIPプロトコルとみなせる
  - 非局所ゲームによる量子プロトコルはMIP*における多証明者のCheatingプロトコルとみなせる

Magic-Square Game

3×3の0-1行列
を想像して



Alice,Bobの勝利条件：

(i)　parity条件

$$a_1 \oplus a_2 \oplus a_3 = 0$$
$$b_1 \oplus b_2 \oplus b_3 = 1$$

(ii) $a_t = b_s$

古典だと勝率は8/9

1	1	0
0	0	0
?	0	1

(ii)はOKも
(i)が×

Alice

1	1	0
0	0	0
1	0	1

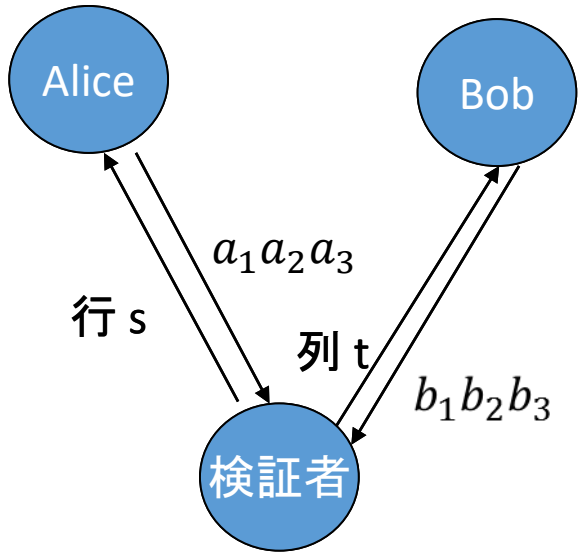
Bob

1	1	0
0	0	0
0	0	1

(i)はOKも
(ii)が×

Magic-Square Game

3×3の0-1行列
を想像して



Alice,Bobの勝利条件：

(i)　parity条件

$$a_1 \oplus a_2 \oplus a_3 = 0$$
$$b_1 \oplus b_2 \oplus b_3 = 1$$

(ii) $a_t = b_s$

量子だと必勝！

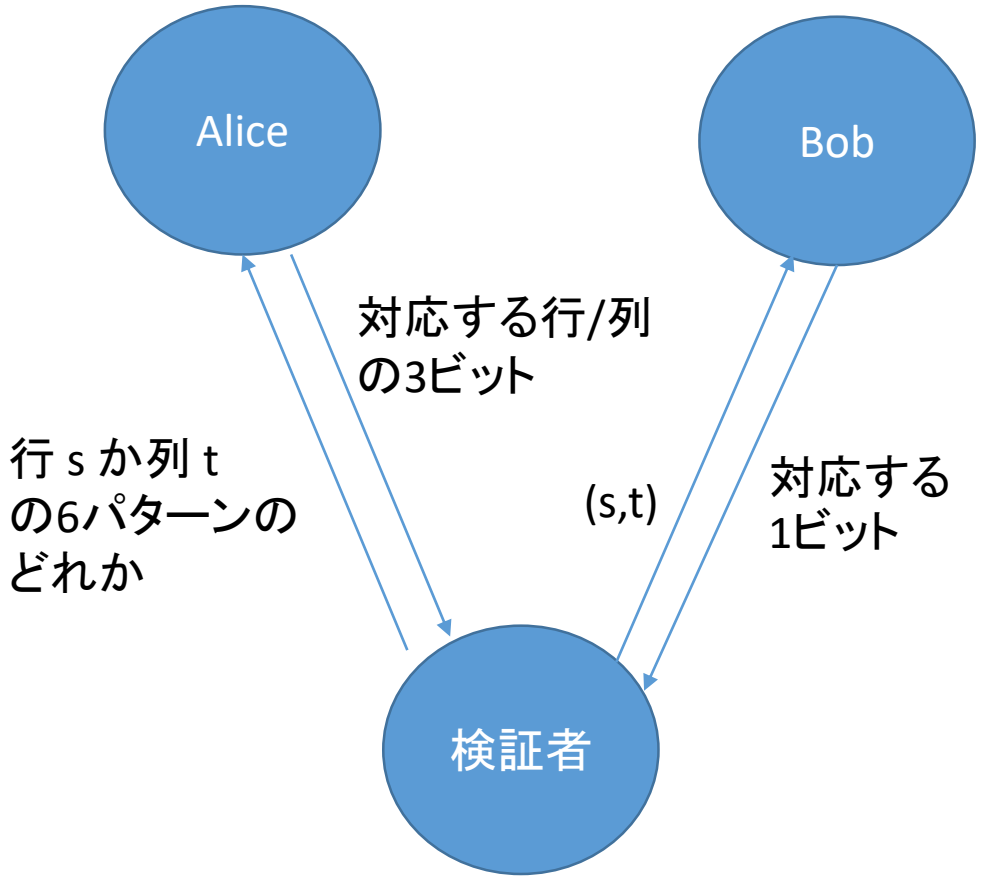
Protocol

1．Alice & Bobは開始前に
$|\Psi^-\rangle_{A1B1} \otimes |\Psi^-\rangle_{A2B2}$ を共有
2．Alice & Bobは各々A1B1, A2B2上で

	t=1	t=2	t=3
s=1	$X \otimes X$	$Y \otimes Z$	$Z \otimes Y$
s=2	$Y \otimes Y$	$Z \otimes X$	$X \otimes Z$
s=3	$Z \otimes Z$	$X \otimes Y$	$Y \otimes X$

の中でs,tに応じた行列にある3つの観測量を各々測定．
　Aliceの j 行（Bobの i 行）に対応する測定値が$\alpha_j = +1(\beta_i = +1)$なら$a_j = 0$（$b_i = 0$）とし，$-1$なら1とする．

Magic-Square game⇒3SAT game



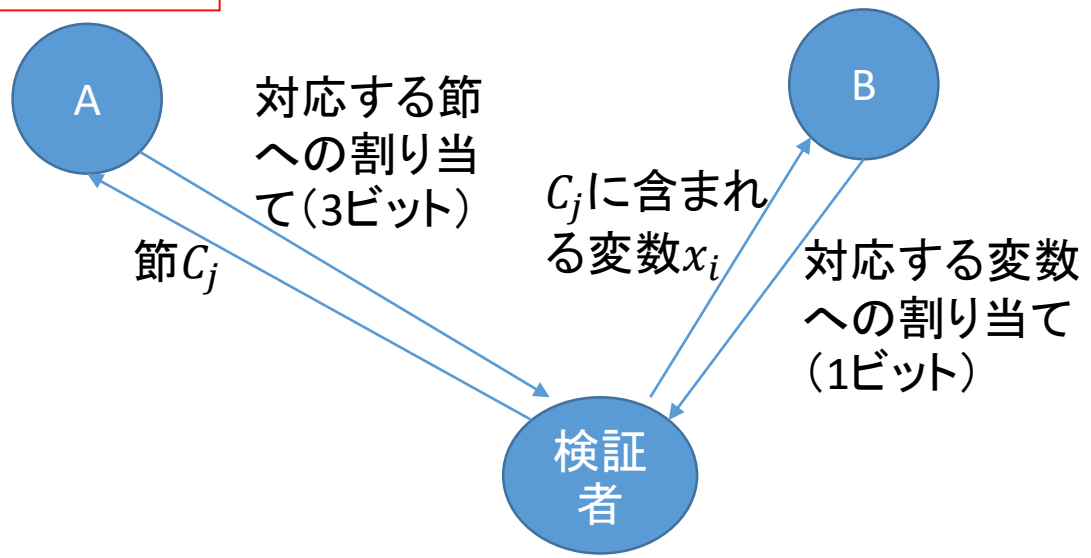
Alice,Bobが勝つ条件：
(i) Aliceの3ビットがparity条件満たす
(ii) Bobの1ビットがAliceの3ビットのうち対応するビットと一致

古典だと勝率17/18も量子は勝率1

帰着

古典だとUNSATゆえ勝率$1-\frac{1}{\text{節の個数}}$も量子は勝率1

3SAT game



MIP⊆MIP*

- MIP (=NEXP)⊆MIP* [IV12]
  - 証明者間のエンタングルメントが負に働くことは防ぐことができる！
  - NEXP計算に対するMIPプロトコル[BFL91]（NEXP計算を符号化する多項式の線形性チェック）は，たとえ証明者間にエンタングルメントがあっても通用

MIP≠MIP*

- MIP (=NEXP)⊆MIP* [IV12]
  - 証明者間のエンタングルメントが負に働くことは防ぐことができる
  - NEXP計算に対するMIPプロトコル[BFL91]（NEXP計算を符号化する多項式の線形性チェック）は，たとえ証明者間にエンタングルメントがあっても通用
- NEEXP⊆MIP* [NW19]
  - MIP*はMIPより真に大きなクラスである
  - エンタングルメントは検証において有用である

MIP* is not computable!

- MIP (=NEXP)⊆MIP* [IV12]
  - 証明者間のエンタングルメントが負に働くことは防ぐことができる
- NEEXP⊆MIP* [NW19]
  - MIP*はMIPより真に大きなクラスである
- MIP*=RE [Ji-Natarajan-Vidick-Wright-Yuen 20]
  - 証明者の量子もつれは計算不可能な問題まで検証可能にする!
  - 量子力学の難問（Tsirelson's problem）を解決!!
  - 作用素論の予想（Conne's Embedding Conjecture）を反証!!!

Summary

- BQP vs NP
  - BQP は NPの拡張クラスPH にさえ含まれない問題を含むかも
  - NP完全はBQPでは（多分）解けない
- 量子対話型証明
  - QIP=QIP[3]=IP=PSPACE
  - MIP*=RE: 証明者間のエンタングルメントの想定を超えた能力

Other Quantum Complexity Classes

- Pより低いクラス
  - BQL
  - QNC
- BPPとBQPの間にあるクラス
  - BPP^{QNC}
  - QNC^{BPP}
  - NISQ
- 暗号に関係するクラス
  - QZK
  - QSZK
- 2値問題でない問題のクラス