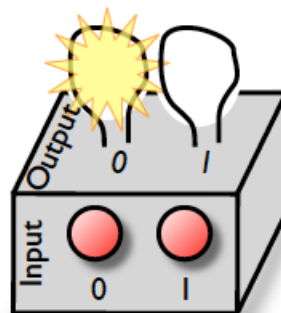
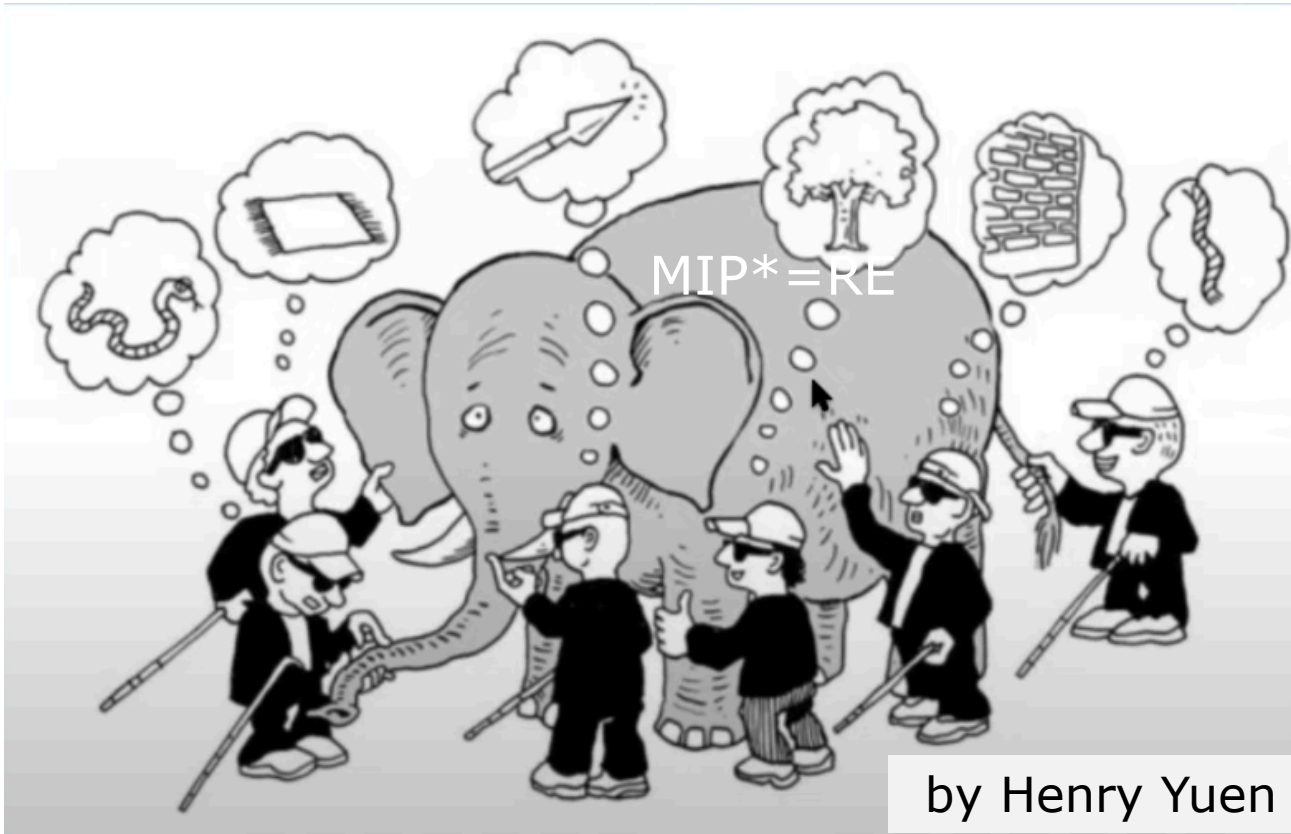


MIP*=RE 入門

-- Interactive Proofとnonlocal ゲーム --



12月25日 クリスマスのマルゼミ



by Umesh Vazirani

Agenda

MIP*=RE 入門

-- Interactive Proofとnonlocal ゲーム

□ Part I

Nonlocal Game

-- エンタングルメントとCHSHゲーム

□ Part II

Interactive Proof

-- 複雑性理論の古典論とその転換

□ Part III

MIP*=RE 定理

-- 量子論と複雑性理論の交わるところ

Agenda Part I

Nonlocal Game -- エンタングルメントとCHSHゲーム

□ CHSHゲーム

- Alice ペアの戦略
- ある戦略の元でのゲームの勝率
- CHSHゲームは「局所実在論」を否定する
- Tsirelson BoundとSelf-Test

□ Magic Square Game

- Magic Square Gameのルール
- Magic Square Gameの最大勝率

□ nonlocal game とInteractive Proof

- nonlocalゲームの定式化
- 最適な戦略の元でのゲーム G の最大勝率 $\omega(G)$
- nonlocal ゲームは、Interactive Proofである

Agenda Part II

Interactive Proof -- 複雑性理論の古典論とその転換

- 計算可能性理論と帰納的可算
- 計算複雑性理論の古典論
 - $P=NP?$ 問題とNP-完全問題
- 転換1 Interactive Proof の登場
 - 証明概念の転換
 - 数学的証明問題はNP完全問題である
 - Interactive Proofの想定とパターン
- Interactive Proofの基本的達成 – MIP^* へ
 - $IP=PSPACE$
 - $MIP=NEXP$
 - PCP定理
- 転換2 量子複雑性理論 -- 確率と複雑性クラス

Agenda Part III

MIP*=RE 定理 -- 量子論と複雑性理論の交わるところ

□ MIP*はどのようなクラスか？

- MIP*の複雑性=Q-GAPの複雑性
- $\text{MIP} \subseteq \text{MIP}^*$
- $\text{NEEXP} \subseteq \text{MIP}^*$

□ 量子的な相関の階層

- $\mathcal{C}_c \subseteq \mathcal{C}_q \subseteq \mathcal{C}_{qs} \subseteq \mathcal{C}_{qa} \subseteq \mathcal{C}_{qc}$
- Tsirelsonの問題: $\mathcal{C}_{qa} = \mathcal{C}_{qc}$
- Connes Embedding Conjecture = Tsirelsonの問題

□ Q-GAP計算のアルゴリズムとMIP*=RE の証明

MIP*=RE 論文

“MIP*=RE” 論文

Zhengfeng Ji, Anand Natarajan, Thomas Vidick,
John Wright, Henry Yuen **[JNVWY]**

2020年1月:<https://arxiv.org/pdf/2001.04383.pdf>

2020年9月:<https://arxiv.org/pdf/2001.04383.pdf>



Henry Yuen



Thomas Vidick



Zhengfeng Ji



Anand Natarajan



John Wright

論文 “ $MIP^*=RE$ ” の概要

1. $MIP^*=RE$:

我々は、古典論的検証者が、エンタングルメントを共有する全能の量子論的証明者と相互作用して、決定することが出来る MIP^* 言語のクラスが、帰納的可算な言語 RE のクラスに等しいことを示した。

2. Halting Problem :

我々の結果の直接の副産物は、「停止問題」から、二人のプレーヤーによるnonlocalゲームがエンタングルした値1を持つかあるいは最大でも $1/2$ の値を持つかどうかの決定する問題への、実効的な還元が存在するということである。

3. Tsirelson's problem :

エンタングルした値の決定不可能性は、「ティレルソンの問題」に対する否定的な答えを導く。

4. Connes' embedding conjecture :

我々の結果は、「コンヌの埋め込み予想」の反証を与える。

論文 “ $MIP^*=RE$ ” の概要

1. $MIP^*=RE$:

我々は、古典論的検証者が、エンタングルメントを共有する全能の量子論的証明者と相互作用して、決定することが出来る MIP^* 言語のクラスが、帰納的可算な言語 RE のクラスに等しいことを示した。

2. Halting Problem :

我々の結果の直接の副産物は、「停止問題」から、二人のプレイヤーによるnonlocalゲームがエンタングルした値1を持つかあるいは最大でも $1/2$ の値を持つかどうかを決定する問題への、実効的な還元が存在するということである。

3. Tsirelson's problem :

エンタングルした値の決定不可能性は、「ティレルソンの問題」に対する否定的な答えを導く。

4. Connes' embedding conjecture :

我々の結果は、「コンヌの埋め込み予想」の反証を与える。

論文 “ $MIP^*=RE$ ” の概要

1. $MIP^*=RE$:

我々は、古典論的検証者が、エンタングルメントを共有する全能の量子論的証明者と相互作用して、決定することが出来る MIP^* 言語のクラスが、帰納的可算な言語 RE のクラスに等しいことを示した。

2. Halting Problem :

我々の結果の直接の副産物は、「停止問題」から、二人のプレイヤーによるnonlocalゲームがエンタングルした値1を持つかあるいは最大でも $1/2$ の値を持つかどうかを決定する問題への、実効的な還元が存在するというものである。

3. Tsirelson's problem :

エンタングルした値の決定不可能性は、「ティレルソンの問題」に対する否定的な答えを導く。

4. Connes' embedding conjecture :

我々の結果は、「コンヌの埋め込み予想」の反証を与える。

論文 “ $MIP^*=RE$ ” の概要

1. $MIP^*=RE$:

我々は、古典論的検証者が、エンタングルメントを共有する全能の量子論的証明者と相互作用して、決定することが出来る MIP^* 言語のクラスが、帰納的可算な言語 RE のクラスに等しいことを示した。

2. Halting Problem :

我々の結果の直接の副産物は、「停止問題」から、二人のプレーヤーによるnonlocalゲームがエンタングルした値1を持つかあるいは最大でも $1/2$ の値を持つかどうかなのかを決定する問題への、実効的な還元が存在するというものである。

3. Tsirelson's problem :

エンタングルした値の決定不可能性は、「ティレルソンの問題」に対する否定的な答えを導く。

4. Connes' embedding conjecture :

我々の結果は、「コンヌの埋め込み予想」の反証を与える。



Part I

Nonlocal Game

-- エンタングルメントとCHSHゲーム --

Agenda Part I

Nonlocal Game -- エンタングルメントとCHSHゲーム

□ CHSHゲーム

- Alice ペアの戦略
- ある戦略の元でのゲームの勝率
- CHSHゲームは「局所実在論」を否定する
- Tsirelson BoundとSelf-Test

□ Magic Square Game

- Magic Square Gameのルール
- Magic Square Gameの最大勝率

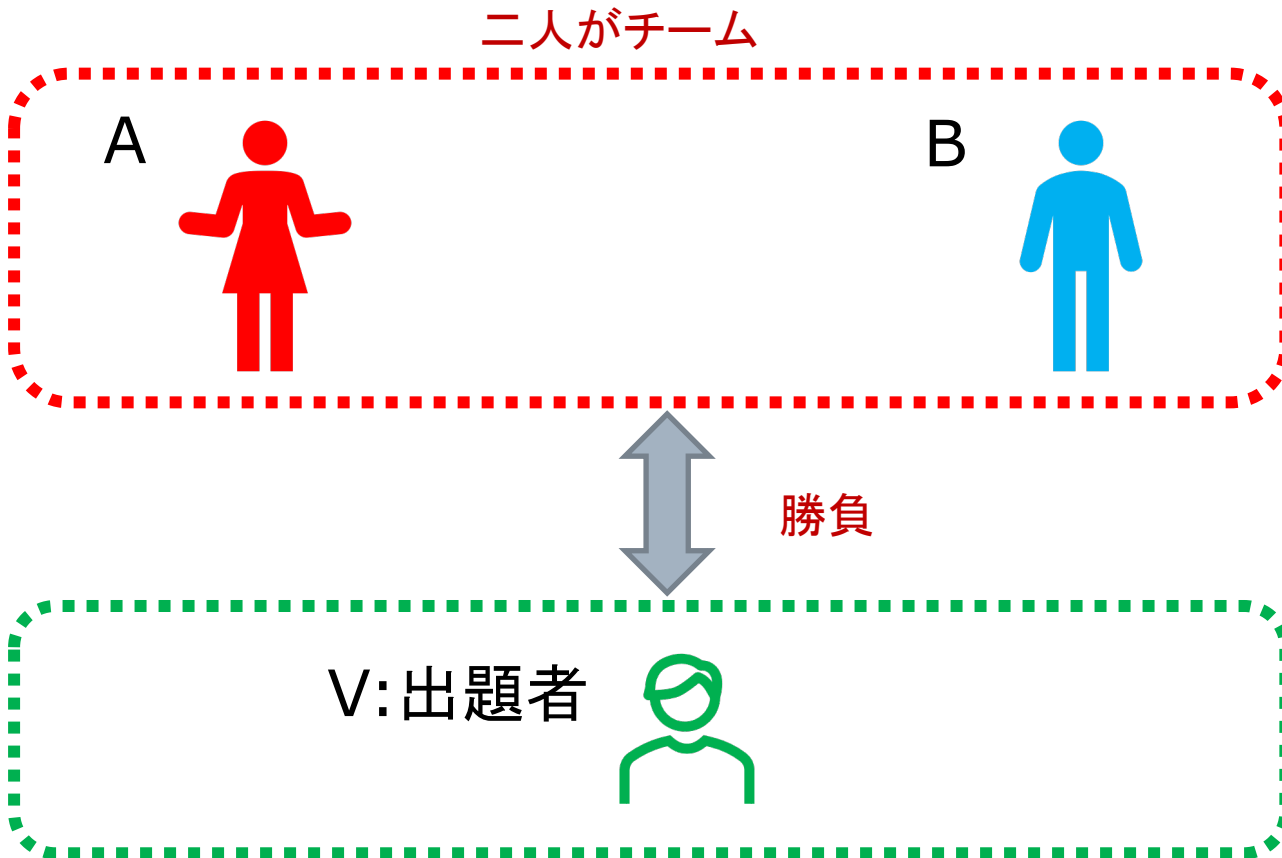
□ nonlocal game とInteractive Proof

- nonlocalゲームの定式化
- 最適な戦略の元でのゲーム G の最大勝率 $\omega(G)$
- nonlocal ゲームは、Interactive Proofである

CHSHゲーム

ゲームの概要

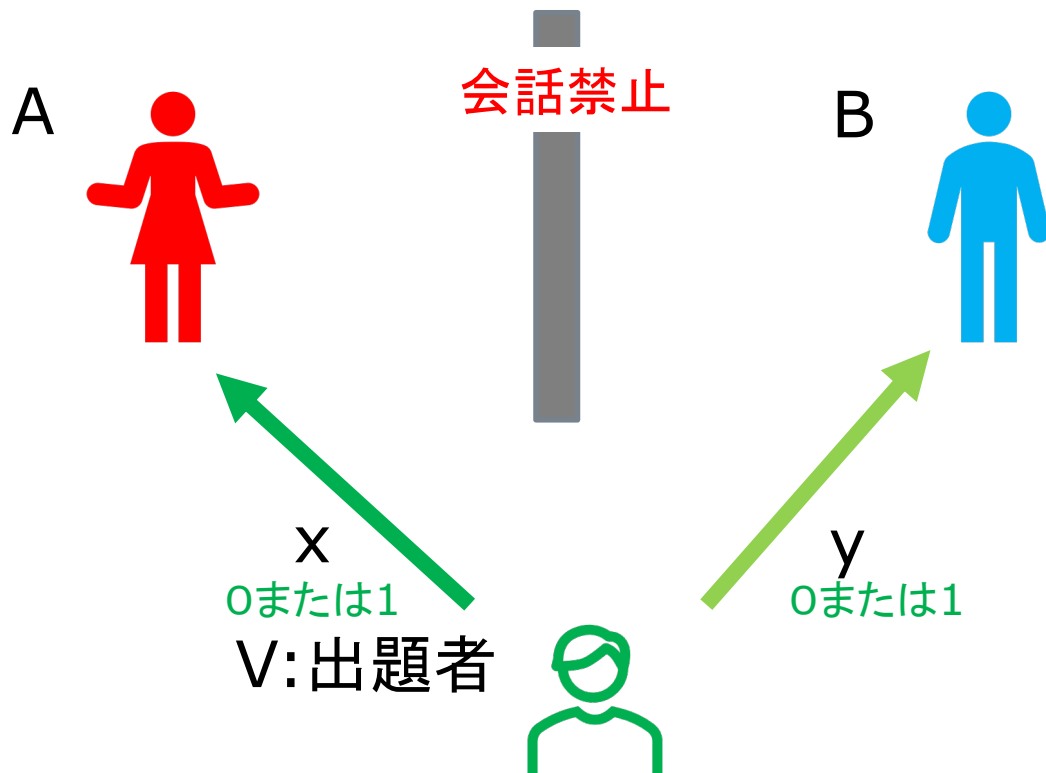
A, B二人のチームが、出題者V の出す問題に答えて、二人のA, Bチームが勝つか出題者Vが勝つかを競うゲームである。



ゲームの概要

ゲーム中の会話は禁止される

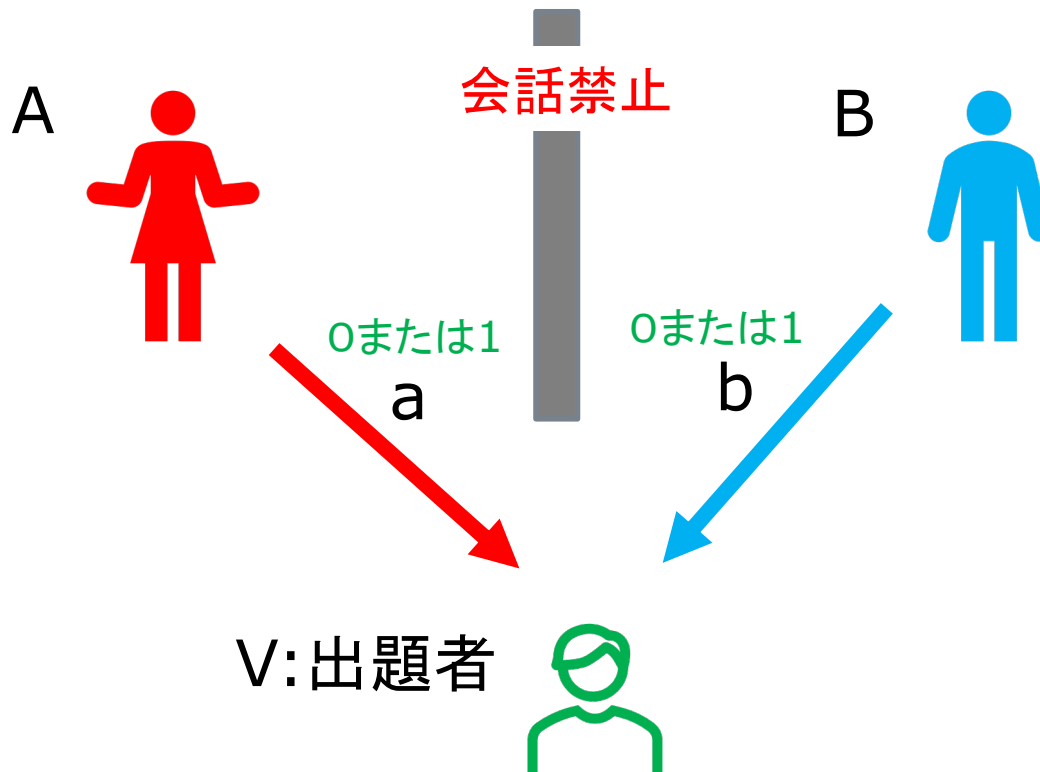
Vは A, Bに、問題として、0または1を送る。



ゲームの概要

ゲーム中の会話は禁止される

A, Bは Vに、答えとして、0または1を送る。

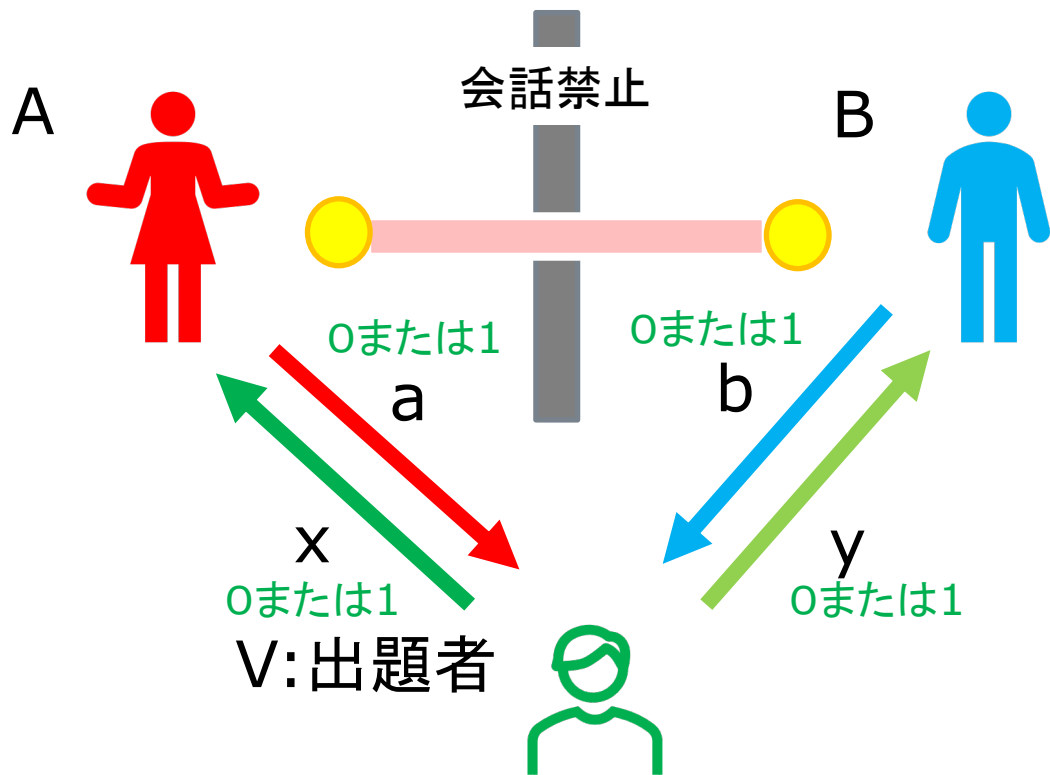


CHSHゲーム

A, Bはentangleした量子を共有する

Vは A, Bに、問題として、0または1を送る。

A, Bは Vに、答えとして、0または1を送る。

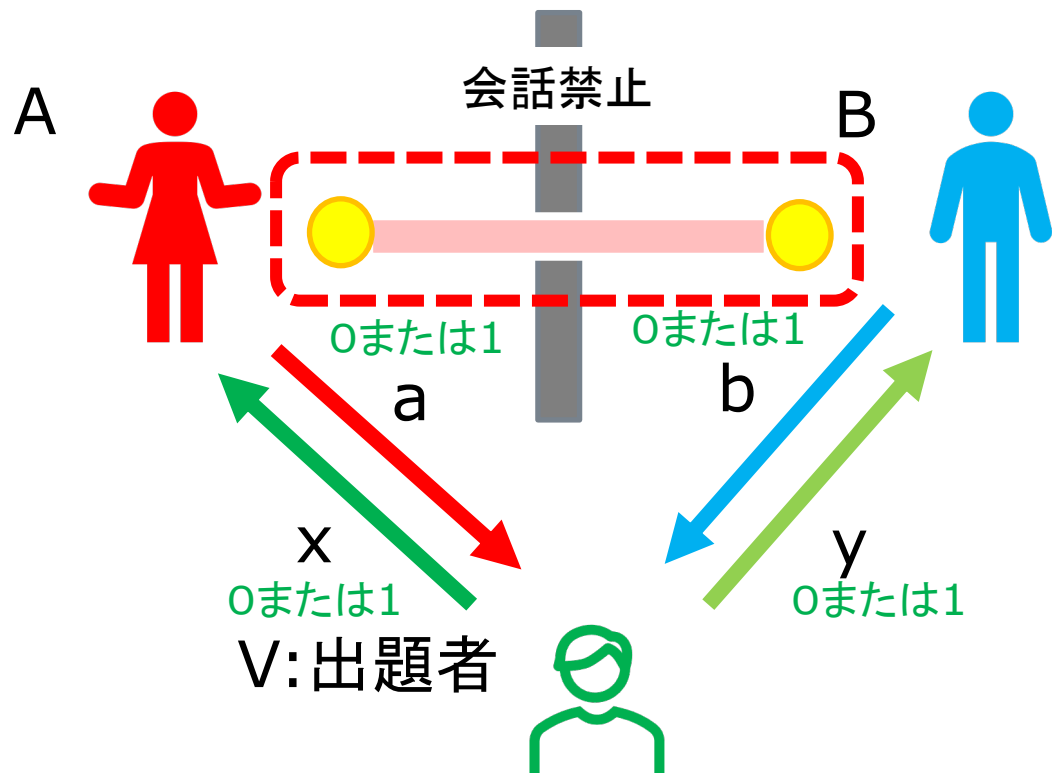


CHSHゲーム

A, Bはentangleした量子を共有する

Vは A, Bに、問題として、0または1を送る。

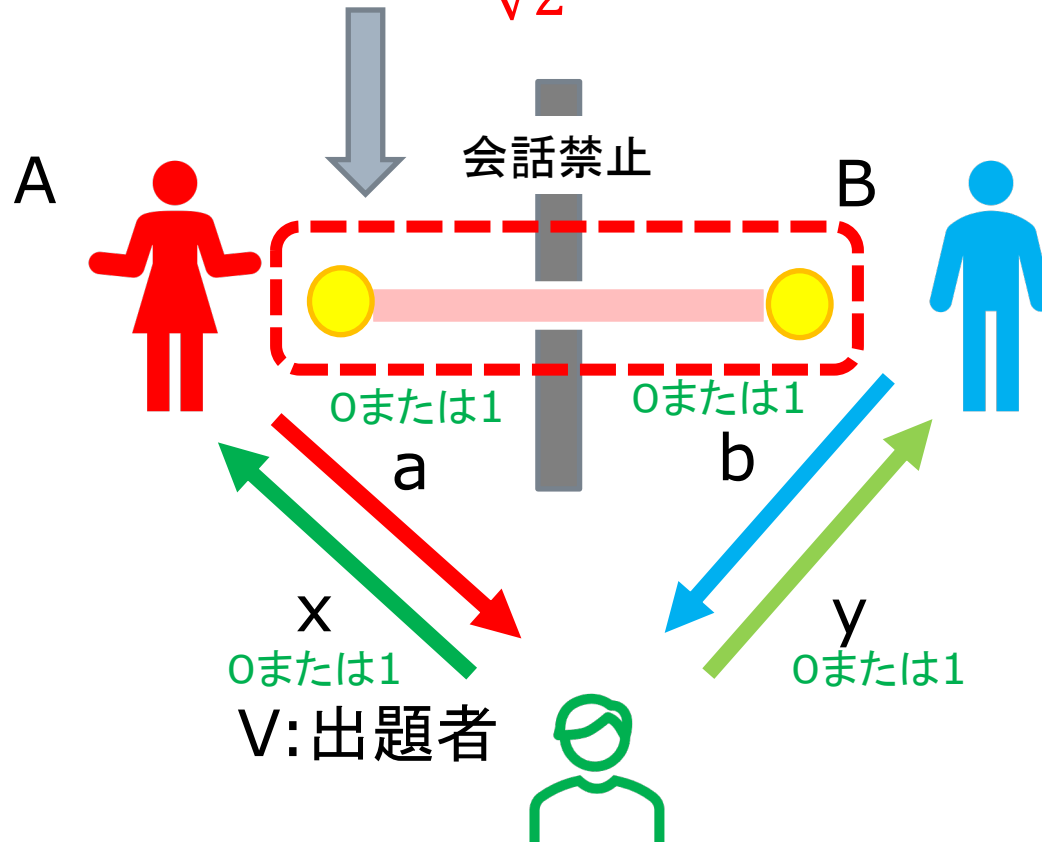
A, Bは Vに、答えとして、0または1を送る。

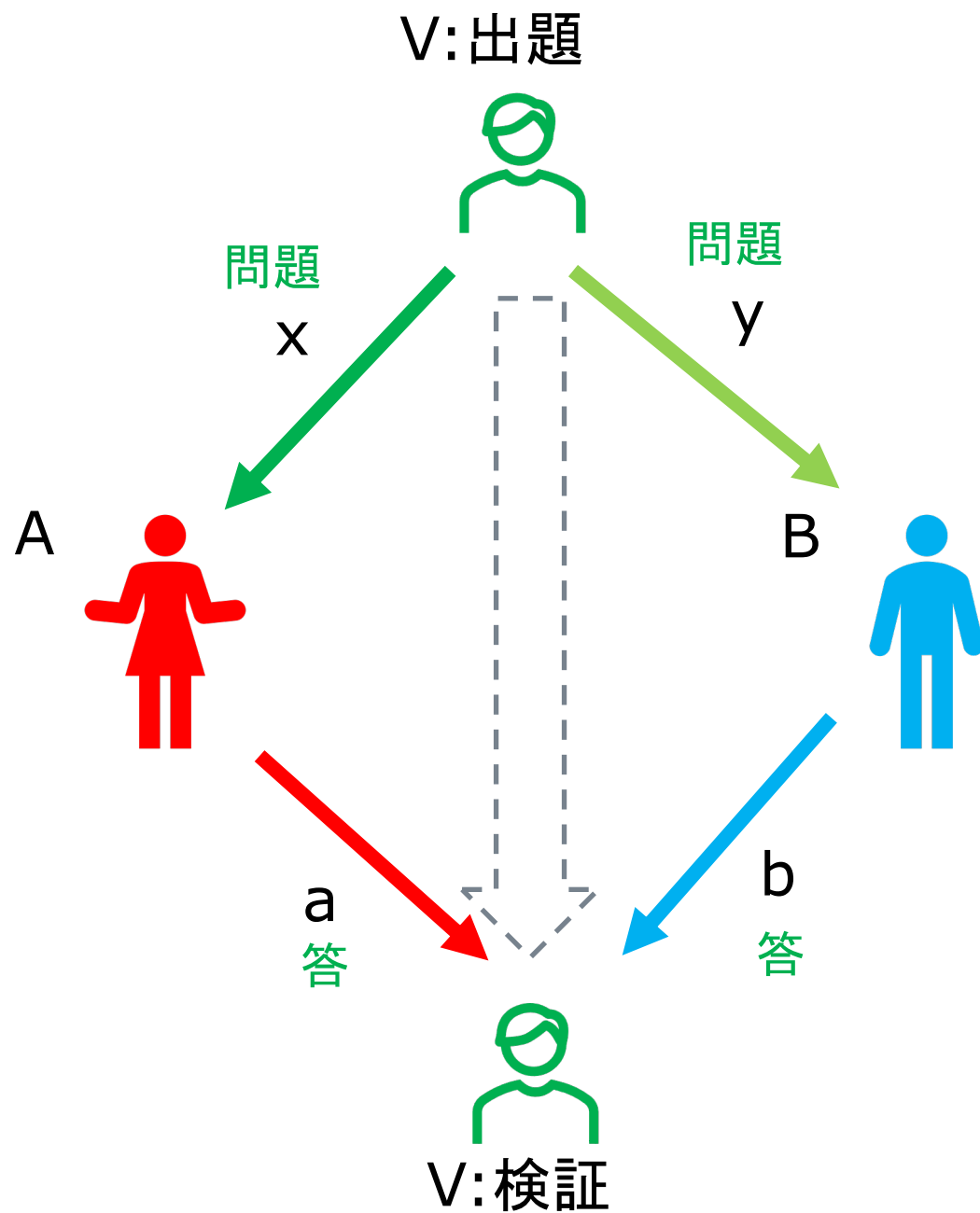


CHSHゲーム

A,Bはentangleした量子を共有する

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





A,Bチームが勝つのは、問題 x, y の値に対して、
答え a, b が、次の値を取る場合である。

1. V が出す x, y のどちらかが0の場合、
Aの答え a とBの答え b が一致していれば、A,Bチームの勝ち。
2. $x = y = 1$ の場合、
 a と b が違っていれば、A,Bチームの勝ち。

$x=0,$ $y=0$	$x=0,$ $y=1$	$x=1,$ $y=0$	$x=1,$ $y=1$
$a=0$ $b=0$	$a=0$ $b=0$	$a=0$ $b=0$	$a=0$ $b=1$
$a=1$ $b=1$	$a=1$ $b=1$	$a=1$ $b=1$	$a=1$ $b=0$

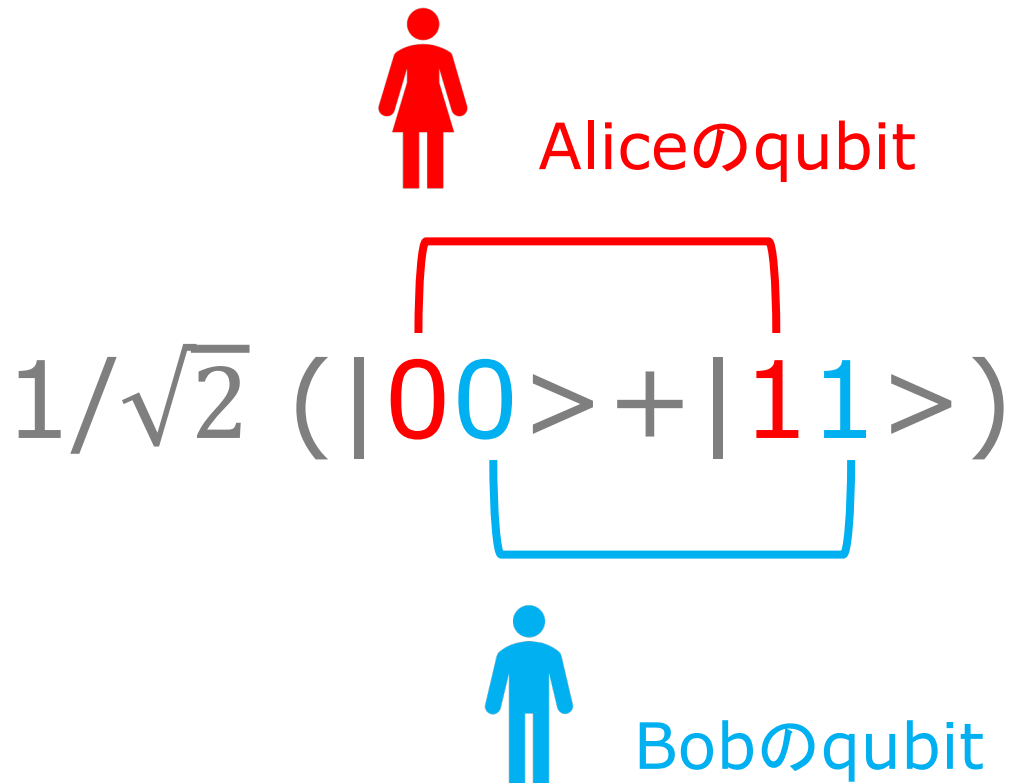

$$|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Alice ペアの戦略

entangleした
量子を操作して
観測する

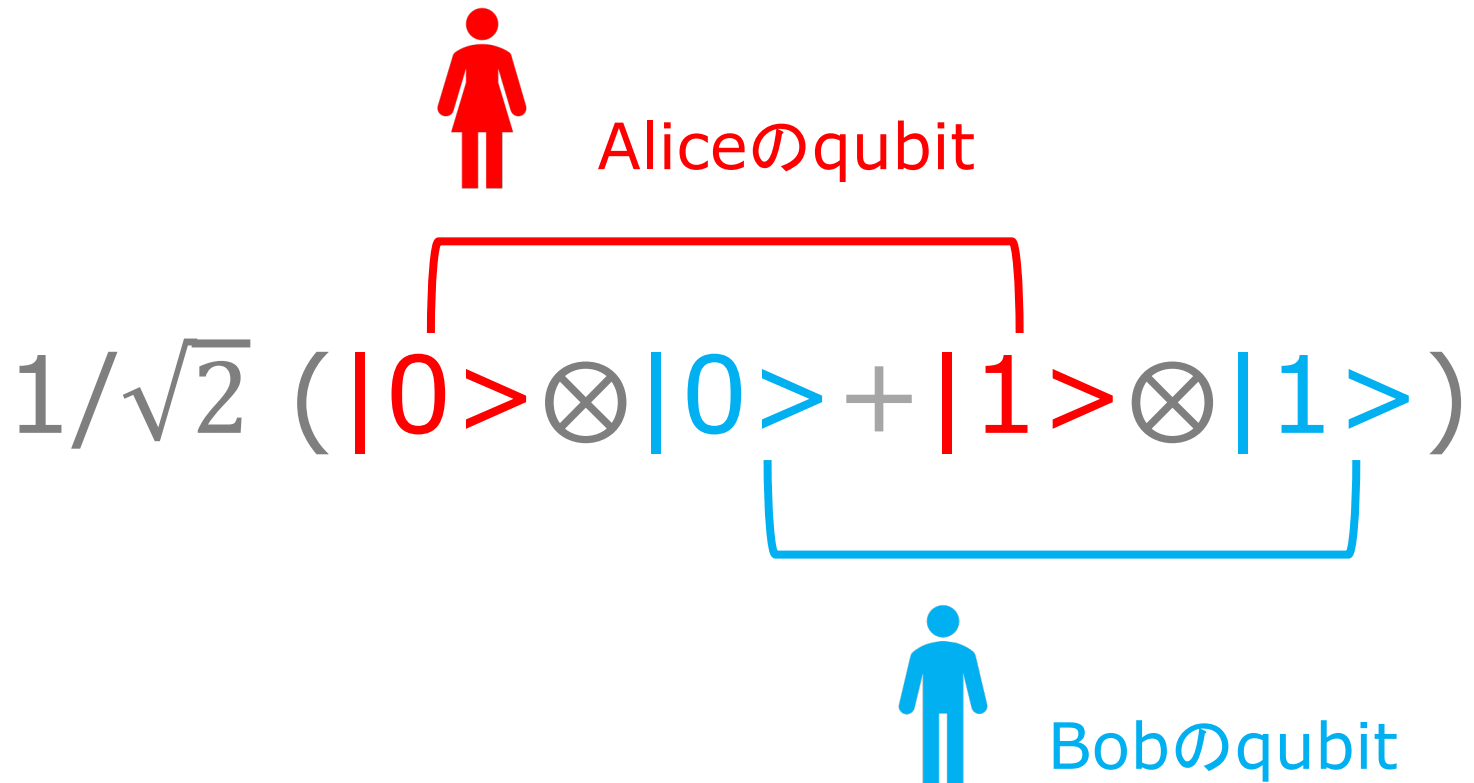

$$|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

EPRペア: entangleした二つのqubit



$1/\sqrt{2} (|00\rangle + |11\rangle)$ で表される状態は、二つのqubitの状態である。
一方のqubitをAliceが、他方のqubitをBobが持つことができる。

EPRペア: entangleした二つのqubit



The diagram illustrates the EPR pair state, $1/\sqrt{2} (|00\rangle + |11\rangle)$. A red bracket above the equation groups the first qubit of each term ($|0\rangle$ and $|1\rangle$) and is labeled "Aliceのqubit" with a red female icon. A blue bracket below the equation groups the second qubit of each term ($|0\rangle$ and $|1\rangle$) and is labeled "Bobのqubit" with a blue male icon. The tensor product symbol $\otimes$ is represented by a circle with an 'X' inside.

$$1/\sqrt{2} (|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$$

$1/\sqrt{2} (|00\rangle + |11\rangle)$ で表される状態は、二つのqubitの状態である。
一方のqubitをAliceが、他方のqubitをBobが持つことができる。

Aliceのqubitの状態を操作する ユニタリ変換UをAliceのqubitに作用させる



変化したAliceのqubit

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

Aliceのqubitのみに
Uは作用している。



Bobのqubit

qubitの状態は、ユニタリ変換を作用させることで変化する。
ここでは、Aliceのqubitのみに、ユニタリ変換Uが作用している。
Bobのqubitの状態は変わらない。

Bobのqubitの状態を操作する ユニタリ変換VをBobのqubitに作用させる



Aliceのqubit

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

Bobのqubitのみに
Vは作用している。



変化したBobのqubit

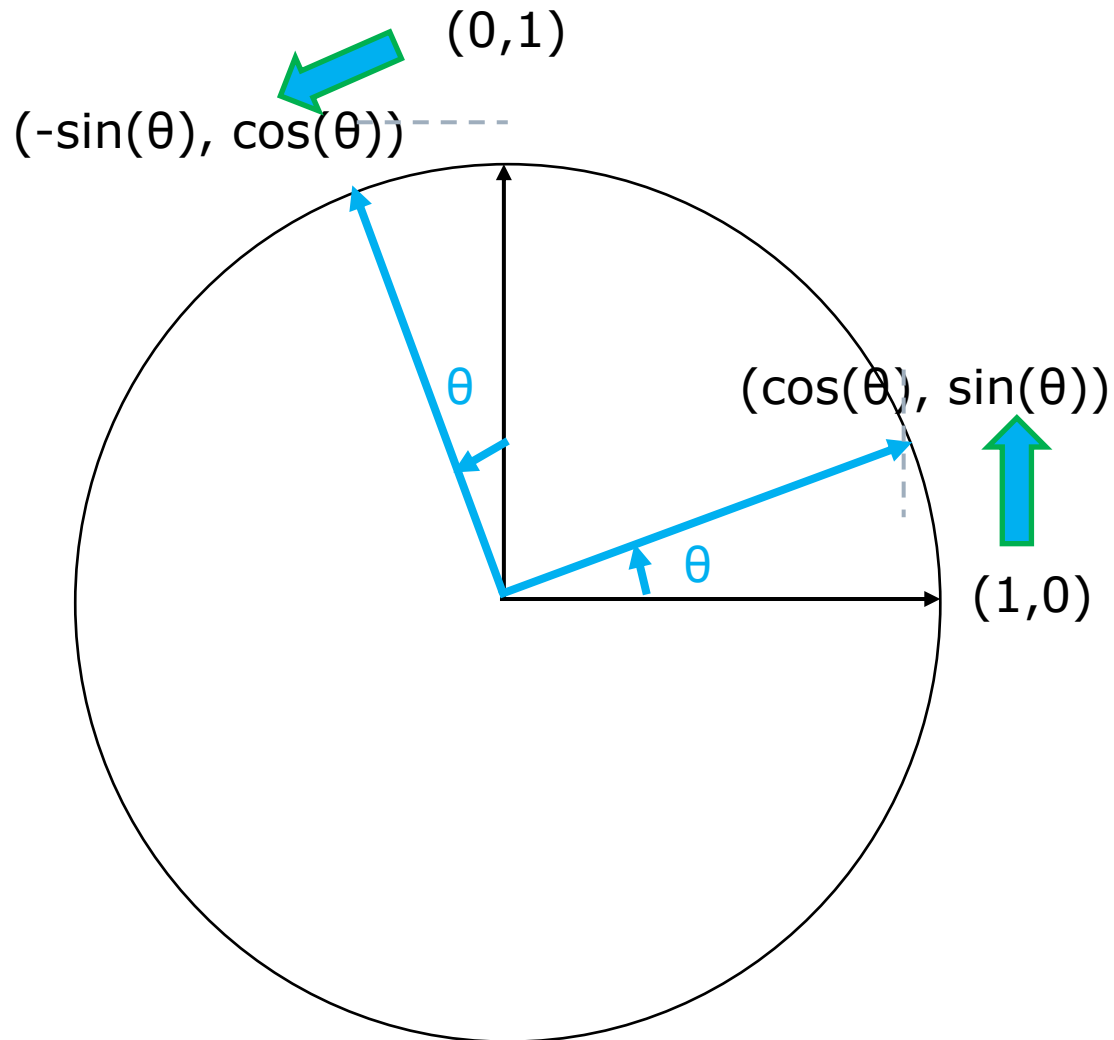
qubitの状態は、ユニタリ変換を作用させることで変化する。
ここでは、Bobのqubitのみに、ユニタリ変換Vが作用している。
Aliceのqubitの状態は変わらない。



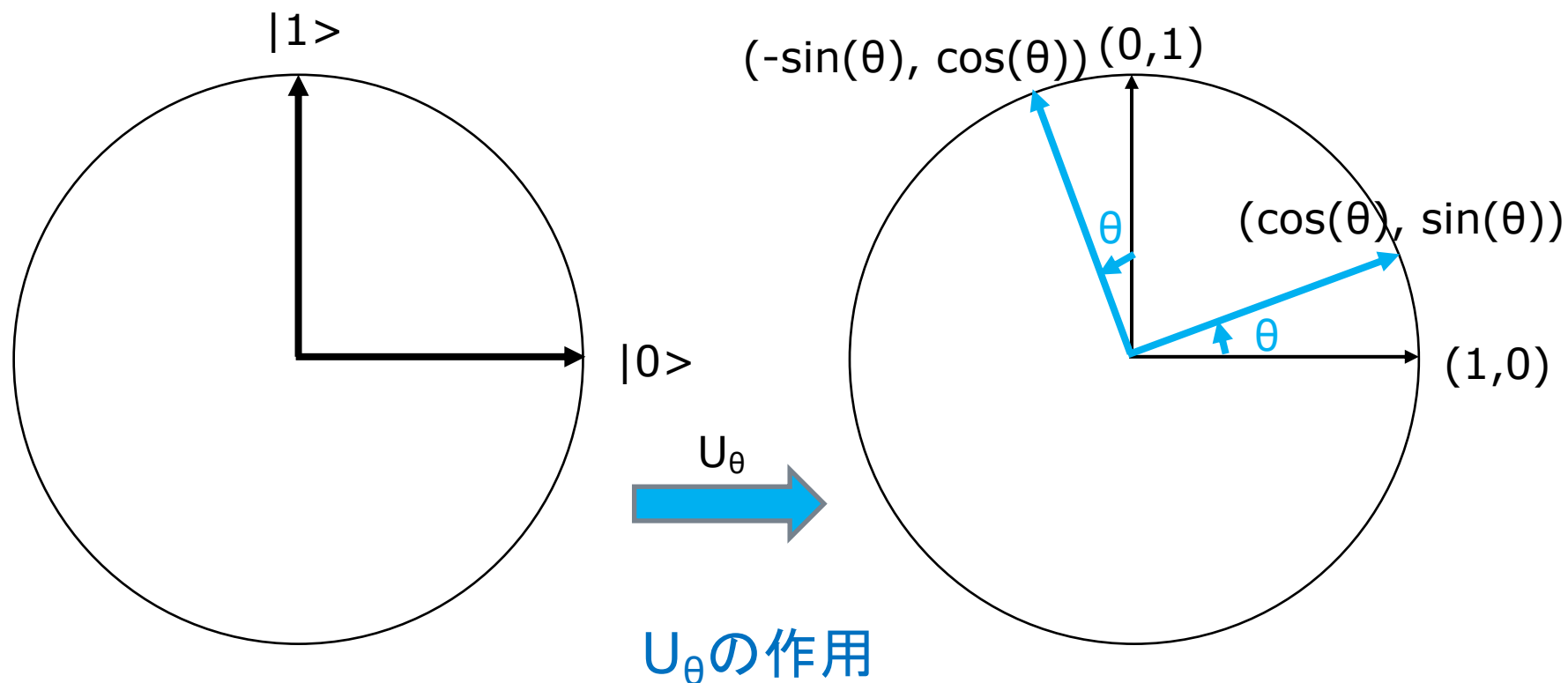
ある戦略の元での
ゲームの勝率



基底を変えて状態を見る



反時計回りに θ だけ基底を回転する

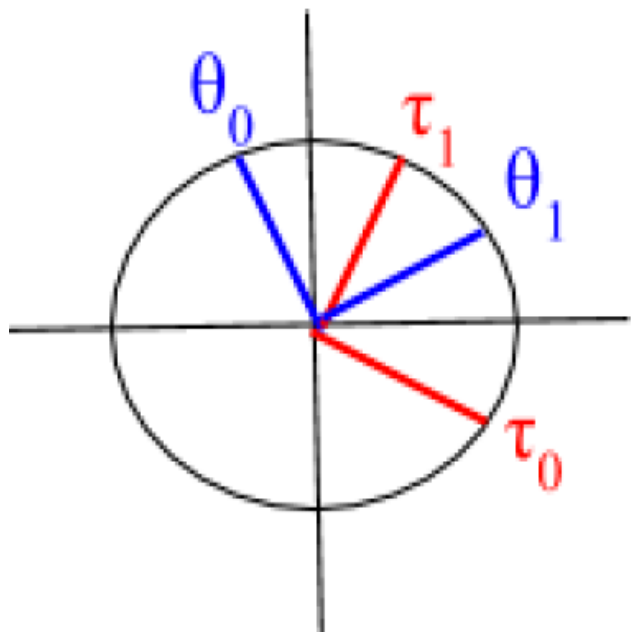


$$U_\theta|0\rangle \longrightarrow \cos(\theta)|0\rangle + \sin(\theta)|1\rangle$$

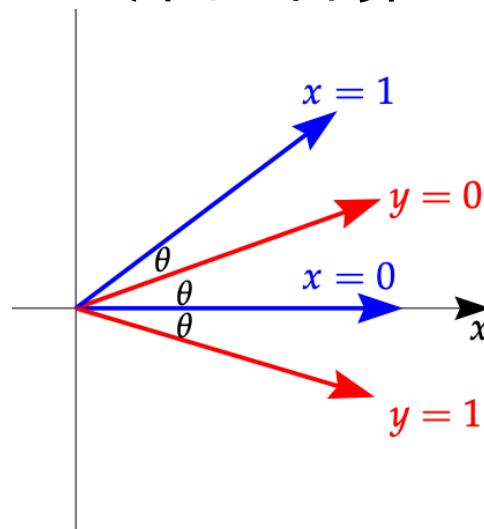
$$U_\theta|1\rangle \longrightarrow -\sin(\theta)|0\rangle + \cos(\theta)|1\rangle$$

今回取る戦略

一般の場合

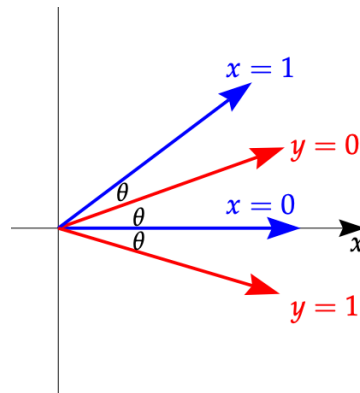


今回の計算



Alice, Bob チームの戦略

1. $x=0$ の時、Aliceは何もせず、自分のqubitを観測し、その値を出題者に返す。
2. $x=1$ の時、Aliceは自分のqubitに、 $U(2\theta)$ を適用し、自分のqubitを観測し、その値を出題者に返す。
3. $y=0$ の時、Bobは自分のqubitに、 $U(\theta)$ を適用し、自分のqubitを観測し、その値を出題者に返す。
4. $y=1$ の時、Bobは自分のqubitに、 $U(-\theta)$ を適用し、自分のqubitを観測し、その値を出題者に返す。



先の戦略を取った時の Alice, Bobの共有qubitの状態

1. $x=0, y=0$ の時、
$$|\psi_1\rangle = 1/\sqrt{2} (|0\rangle \otimes U(\theta)|0\rangle + |1\rangle \otimes U(\theta)|1\rangle)$$
2. $x=1, y=0$ の時、
$$|\psi_2\rangle = 1/\sqrt{2} (U(2\theta)|0\rangle \otimes U(\theta)|0\rangle + U(2\theta)|1\rangle \otimes U(\theta)|1\rangle)$$
3. $x=0, y=1$ の時、
$$|\psi_3\rangle = 1/\sqrt{2} (|0\rangle \otimes V|0\rangle + |1\rangle \otimes V|1\rangle)$$
4. $x=1, y=1$ の時、
$$|\psi_4\rangle = 1/\sqrt{2} (U|0\rangle \otimes V|0\rangle + U|1\rangle \otimes V|1\rangle)$$

$U=U(\theta)$ は、
 $|0\rangle, |1\rangle$ を次のように変換する

$U=U(\theta)$ の作用

$$U|0\rangle \longrightarrow \cos(\theta)|0\rangle + \sin(\theta)|1\rangle$$

$$U|1\rangle \longrightarrow -\sin(\theta)|0\rangle + \cos(\theta)|1\rangle$$

以下、場合わけ

$x=0, y=0$ の時

$$\begin{aligned} |\psi_1\rangle &= 1/\sqrt{2} (|0\rangle \otimes U(\theta)|0\rangle + |1\rangle \otimes U(\theta)|1\rangle) \\ &= 1/\sqrt{2} ((|0\rangle \otimes (\cos(\theta)|0\rangle + \sin(\theta)|1\rangle) \\ &\quad + |1\rangle \otimes (-\sin(\theta)|0\rangle + \cos(\theta)|1\rangle)) \\ &= 1/\sqrt{2} (\cos(\theta)|00\rangle + \sin(\theta)|01\rangle \\ &\quad - \sin(\theta)|10\rangle + \cos(\theta)|11\rangle) \end{aligned}$$

AliceとBobが同じ答えを返すのは、観測された状態が、 $|00\rangle$ または $|11\rangle$ の場合である。その確率は、

$$(1/\sqrt{2} \cos(\theta))^2 + (1/\sqrt{2} \cos(\theta))^2 = \cos^2(\theta) \text{ である。}$$

$x=0, y=1$ の時

$$\begin{aligned} |\psi_2\rangle &= 1/\sqrt{2} (|0\rangle \otimes U(-\theta)|0\rangle + |1\rangle \otimes U(-\theta)|1\rangle) \\ &= 1/\sqrt{2} (|0\rangle \otimes (\cos(-\theta)|0\rangle + \sin(-\theta)|1\rangle) \\ &\quad + |1\rangle \otimes (-\sin(-\theta)|0\rangle + \cos(-\theta)|1\rangle)) \\ &= 1/\sqrt{2} (\cos(\theta)|00\rangle - \sin(\theta)|01\rangle \\ &\quad + \sin(\theta)|01\rangle + \cos(\theta)|11\rangle) \end{aligned}$$

AliceとBobが同じ答えを返すのは、観測された状態が、 $|00\rangle$ または $|11\rangle$ の場合である。その確率は、
 $(1/\sqrt{2} \cos(\theta))^2 + (1/\sqrt{2} \cos(\theta))^2 = \cos^2(\theta)$ である。

$x=1, y=0$ の時

$$\begin{aligned}
 |\psi_2\rangle &= \frac{1}{\sqrt{2}} (U(2\theta)|0\rangle \otimes U(\theta)|0\rangle \\
 &\quad + U(2\theta)|1\rangle \otimes U(\theta)|1\rangle) \\
 &= \frac{1}{\sqrt{2}} ((\cos(2\theta)|0\rangle + \sin(2\theta)|1\rangle) \\
 &\quad \otimes (\cos(\theta)|0\rangle + \sin(\theta)|1\rangle) \\
 &\quad + (-\sin(2\theta)|0\rangle + \cos(2\theta)|1\rangle) \\
 &\quad \otimes (-\sin(\theta)|0\rangle + \cos(\theta)|1\rangle)) \\
 &= \frac{1}{\sqrt{2}} ((\cos(2\theta)\cos(\theta) + \sin(2\theta)\sin(\theta))|00\rangle \\
 &\quad + (\cos(2\theta)\sin(\theta) - \sin(2\theta)\cos(\theta))|01\rangle \\
 &\quad + (\sin(2\theta)\cos(\theta) - \cos(2\theta)\sin(\theta))|10\rangle \\
 &\quad + (\sin(2\theta)\sin(\theta) + \cos(2\theta)\cos(\theta))|11\rangle)
 \end{aligned}$$

$x=1, y=0$ の時 (続き)

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

AliceとBobが同じ答えを返すのは、観測された状態が、 $|00\rangle$ または $|11\rangle$ の場合である。その確率は、

$$(\frac{1}{\sqrt{2}}\cos(\theta))^2 + (\frac{1}{\sqrt{2}}\cos(\theta))^2 = \cos^2(\theta) \text{ である。}$$

$x=1, y=1$ の時

$$\begin{aligned}
 |\psi_4\rangle &= 1/\sqrt{2} (U(2\theta)|0\rangle \otimes U(-\theta)|0\rangle \\
 &\quad + U(2\theta)|1\rangle \otimes U(-\theta)|1\rangle) \\
 &= 1/\sqrt{2} ((\cos(2\theta)|0\rangle + \sin(2\theta)|1\rangle) \\
 &\quad \otimes (\cos(-\theta)|0\rangle + \sin(-\theta)|1\rangle) \\
 &\quad + (-\sin(2\theta)|0\rangle + \cos(2\theta)|1\rangle) \\
 &\quad \otimes (-\sin(-\theta)|0\rangle + \cos(-\theta)|1\rangle)) \\
 &= 1/\sqrt{2} (\\
 &\quad (\cos(2\theta)\cos(-\theta) + \sin(2\theta)\sin(-\theta))|00\rangle \\
 &\quad + (\cos(2\theta)\sin(-\theta) - \sin(2\theta)\cos(-\theta))|01\rangle \\
 &\quad + (\sin(2\theta)\cos(-\theta) - \cos(2\theta)\sin(-\theta))|10\rangle \\
 &\quad + (\sin(2\theta)\sin(-\theta) + \cos(2\theta)\cos(-\theta))|11\rangle)
 \end{aligned}$$

$x=1, y=1$ の時 (続き)

$$= 1/\sqrt{2} (\\ \cos(\theta)|00> \\ -\sin(3\theta)|01> \\ +\sin(3\theta)|10> \\ +\cos(\theta)|11>)$$

AliceとBobが違う答えを返すのは、観測された状態が、 $|01>$ または $|10>$ の場合である。

この場合、その確率は、

$$(1/\sqrt{2} \sin(3\theta))^2 + (1/\sqrt{2} \sin(3\theta))^2 = \sin^2(3\theta) \text{ である。}$$

Alice, Bobチームが勝つ確率

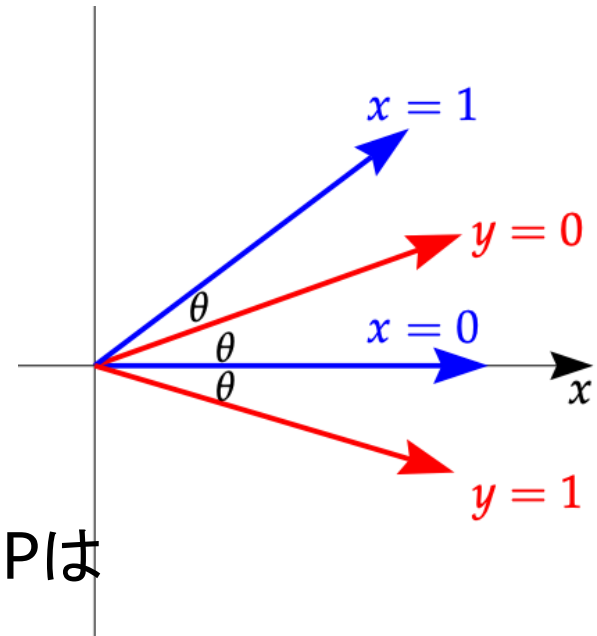
この戦略を取った時、Alice, Bobチームがそれぞれの場合に勝つ確率は、次のようになる。

$x=0, y=0$ の時、 $\cos^2(\theta)$

$x=1, y=0$ の時、 $\cos^2(\theta)$

$x=0, y=1$ の時、 $\cos^2(\theta)$

$x=1, y=1$ の時、 $\sin^2(3\theta)$



よって、Alice, Bobチームが勝つ確率Pは

$$P = \frac{3}{4} \times \cos^2(\theta) + \frac{1}{4} \times \sin^2(3\theta)$$

Alice, Bobチームが勝つ確率

Alice, Bobチームが勝つ確率Pは

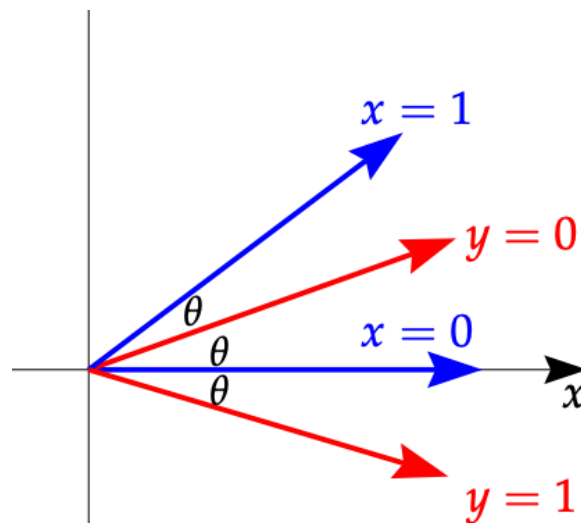
$$P(\theta) = \frac{3}{4} \times \cos^2(\theta) + \frac{1}{4} \times \sin^2(3\theta)$$

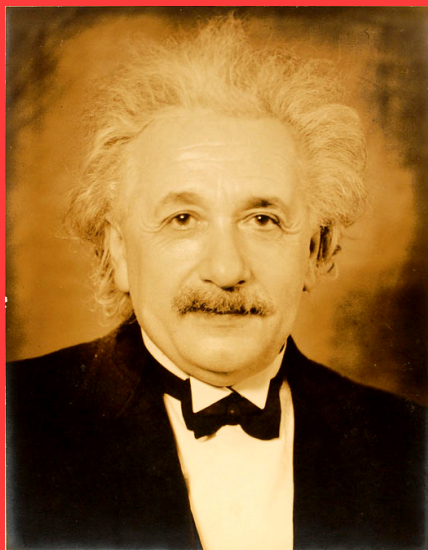
$$P(0) = \frac{3}{4}$$

$$p\left(\frac{\pi}{4}\right) = \frac{3}{4} \times \frac{1}{2} + \frac{1}{4} \times \frac{1}{2} = \frac{1}{2}$$

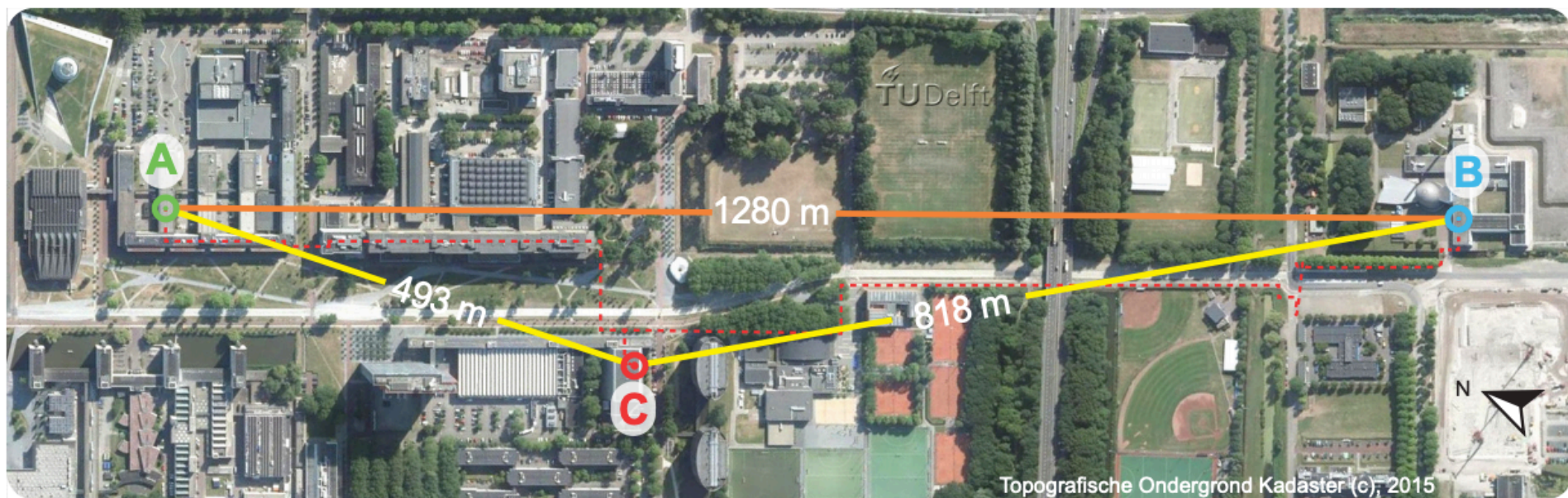
$$p\left(\frac{\pi}{8}\right) = \frac{3}{4} \times \cos^2\left(\frac{\pi}{8}\right) + \frac{1}{4} \times \sin^2\left(\frac{3\pi}{8}\right) = \cos^2\left(\frac{\pi}{8}\right) = \frac{1 + \cos\frac{\pi}{4}}{2}$$

$$= \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.8535... > 0.75$$

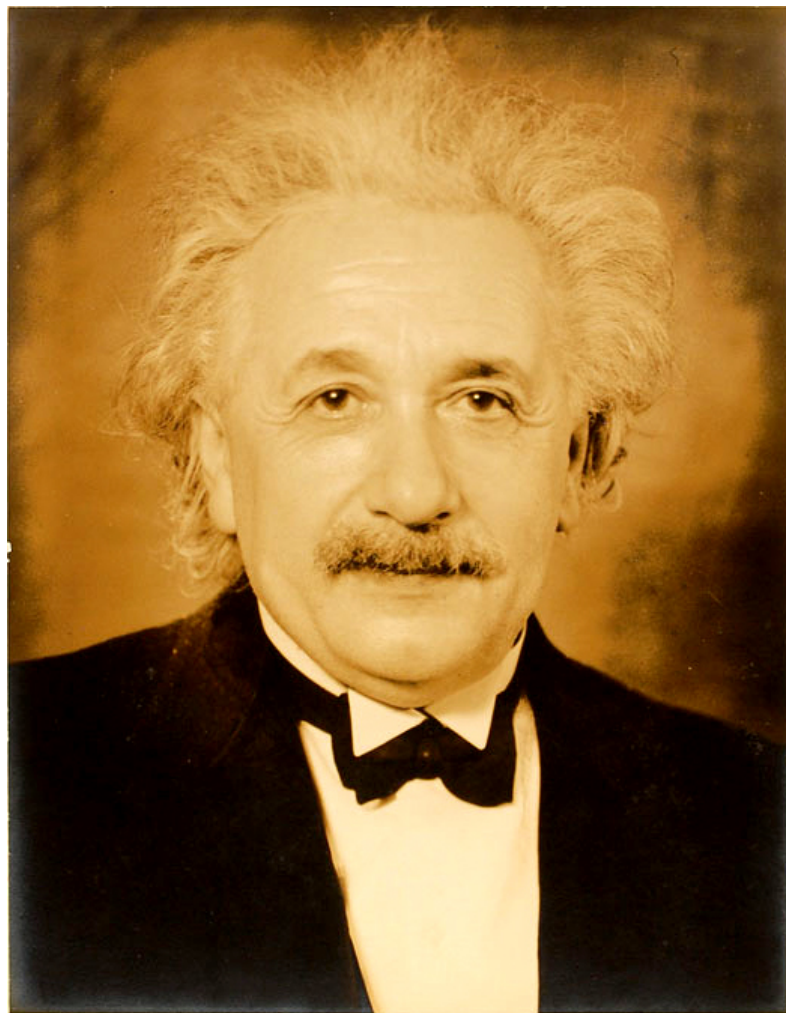




CHSHゲームは 「局所实在論」を否定する



アインシュタインとベル

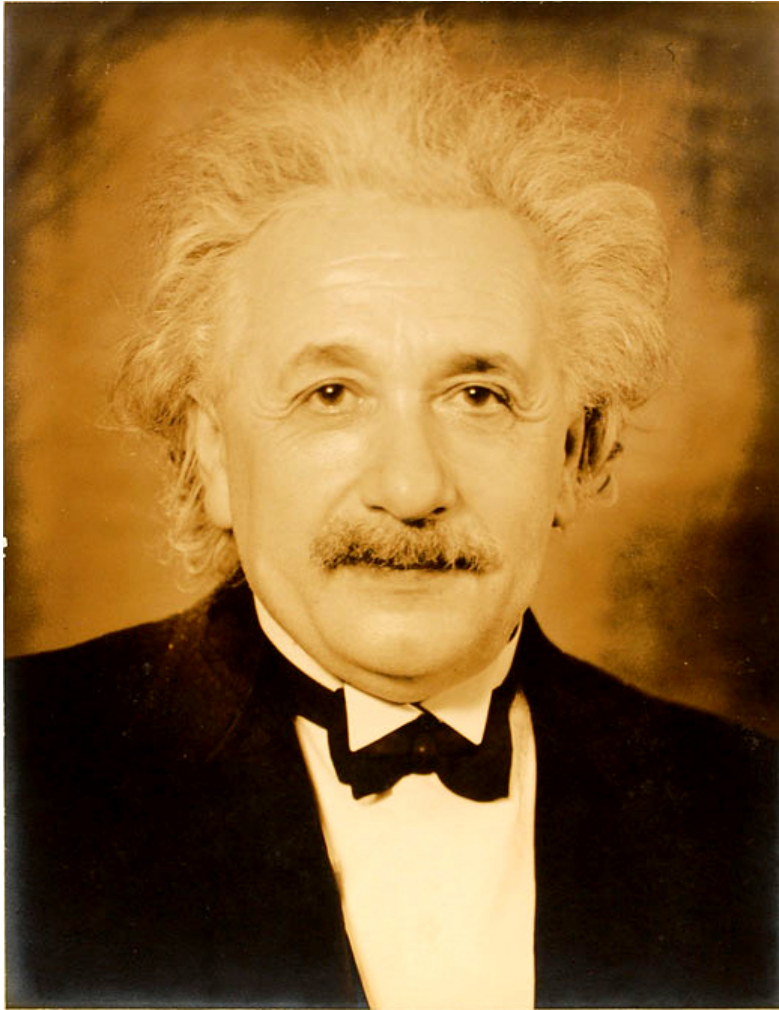


1935年
エンタングルメントの発見



1964年
ベルの定理

アインシュタインの「局所实在論」



1935年
EPR論文

量子論は、自然の物理学的
記述としては不完全な理論だ。

实在性 (reality)

客観的な实在は、どんな物理理論
やその理論の概念的操作からも独
立に存在する。

「月は、我々が目を離れた時に、存
在しなくなるわけではない」

局所性 (locality)

ある場所にある物理的实在は、同
時に行われる、遠く離れた場所
にある实在の観測によっては影響を
受けることはない。

「エンタングルメントは、馬鹿げた
遠隔作用だ」

ベルの定理

ベルの不等式

古典論で、アインシュタインのいう「隠れた変数」を仮定した場合でも、観測の確率分布は、ある不等式を満たすことを示すことができる。

量子論は、この不等式を破る

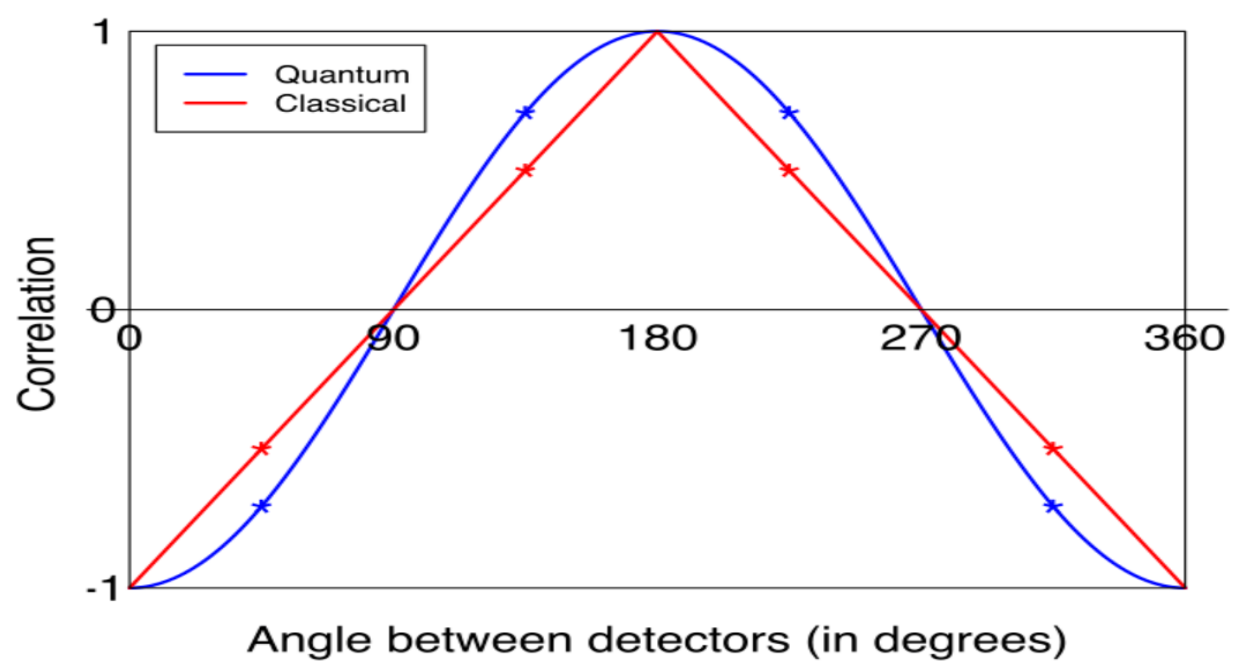
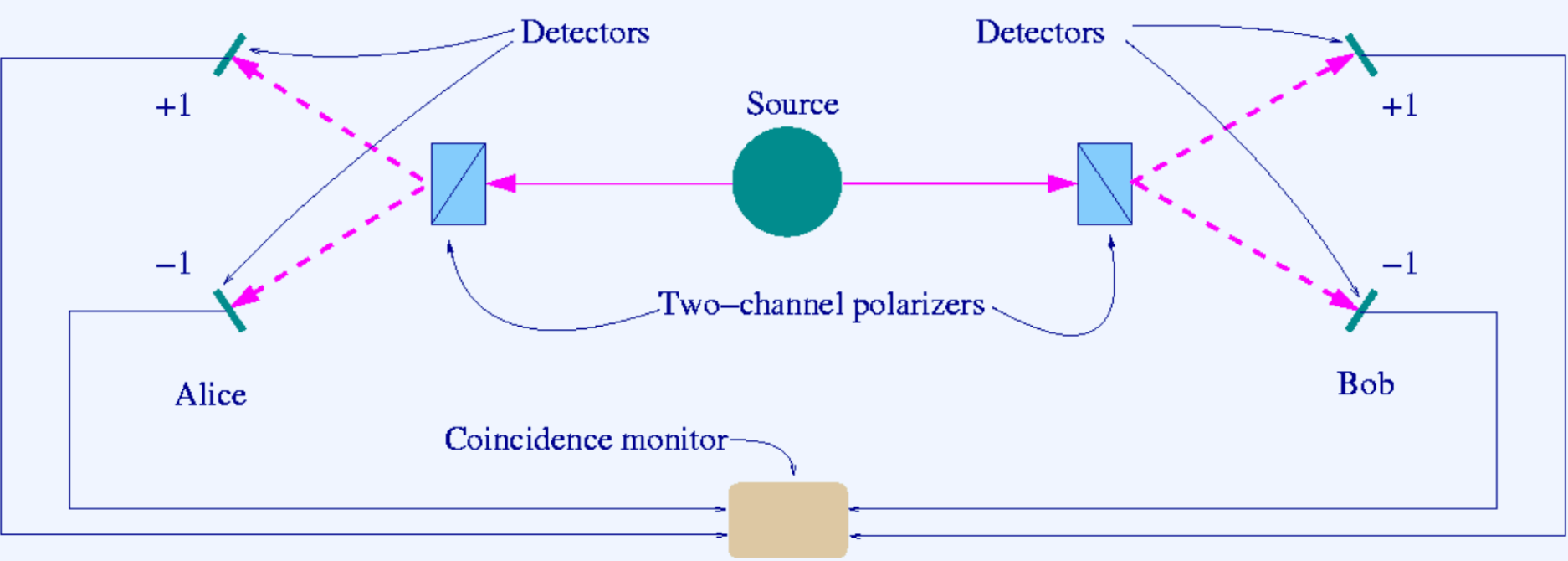
量子論的観測は、この不等式を破ることが、理論的に証明できる。

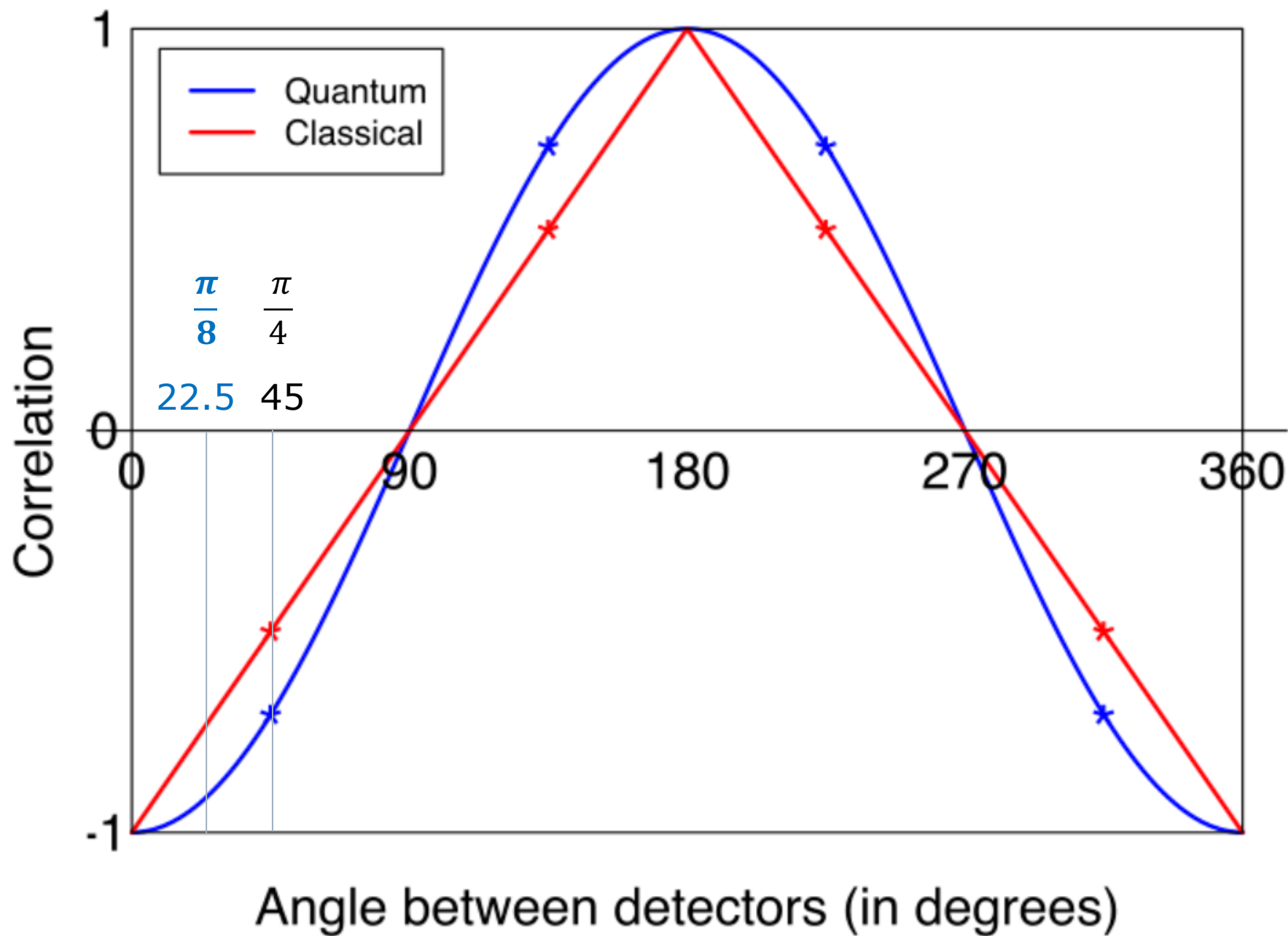
実験的な検証可能性

自然が、古典論に従うか量子論に従うかは、この違いを検出できれば、実験的に検証することが可能である。

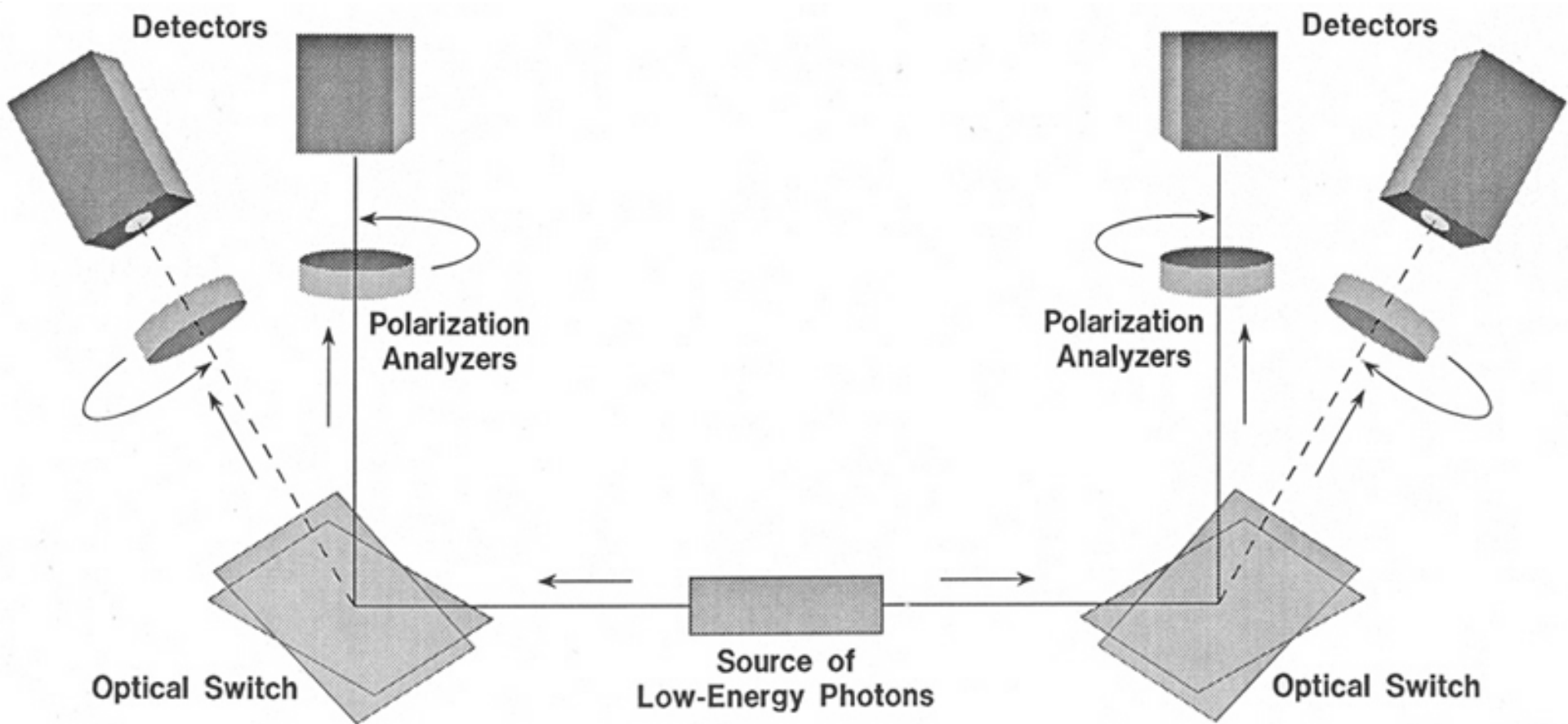


1964年
ベルの定理



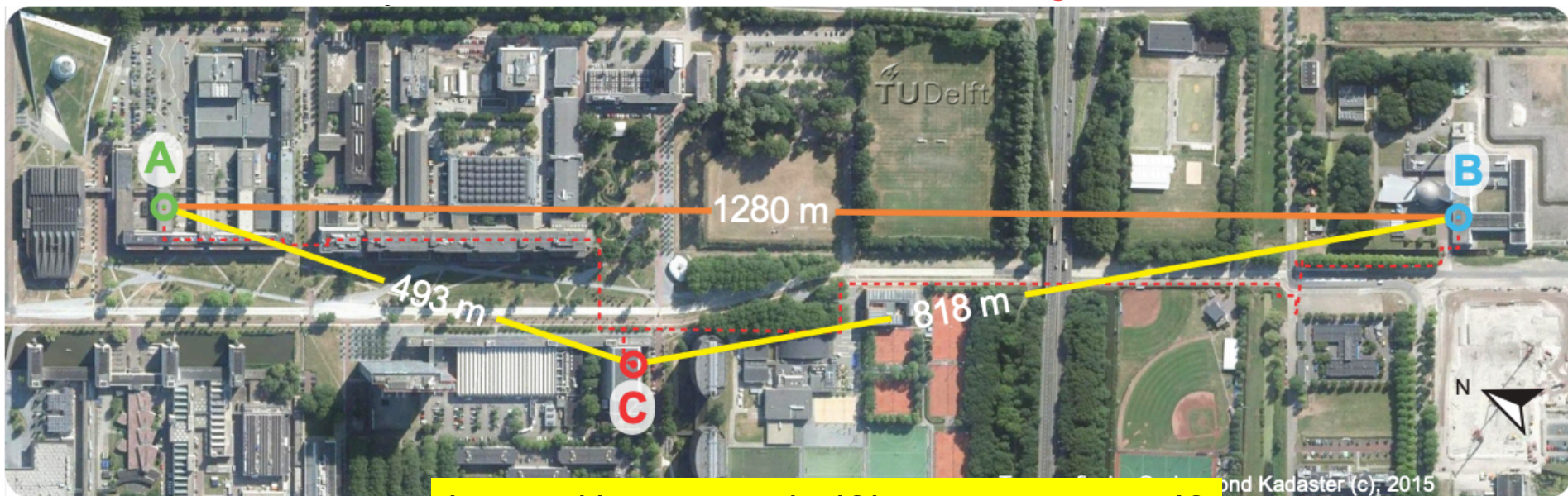
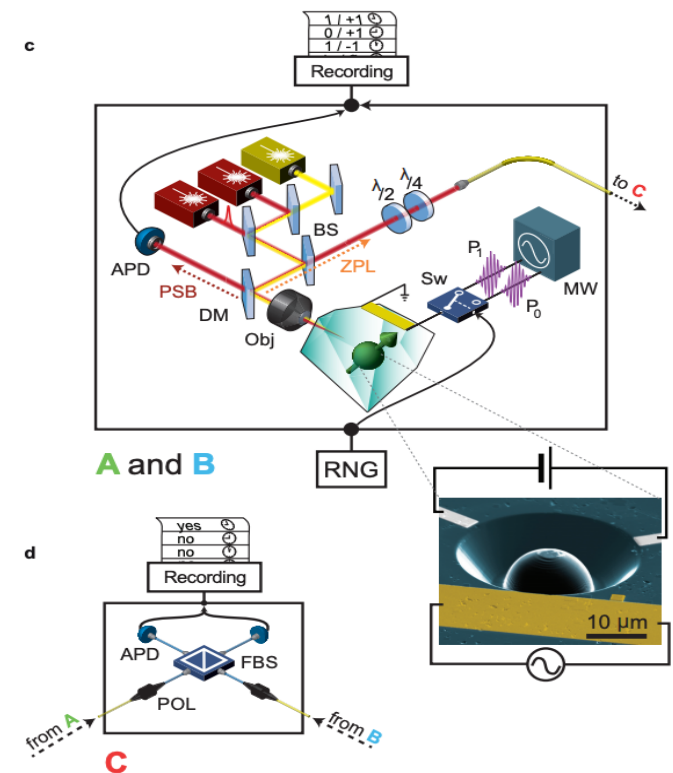
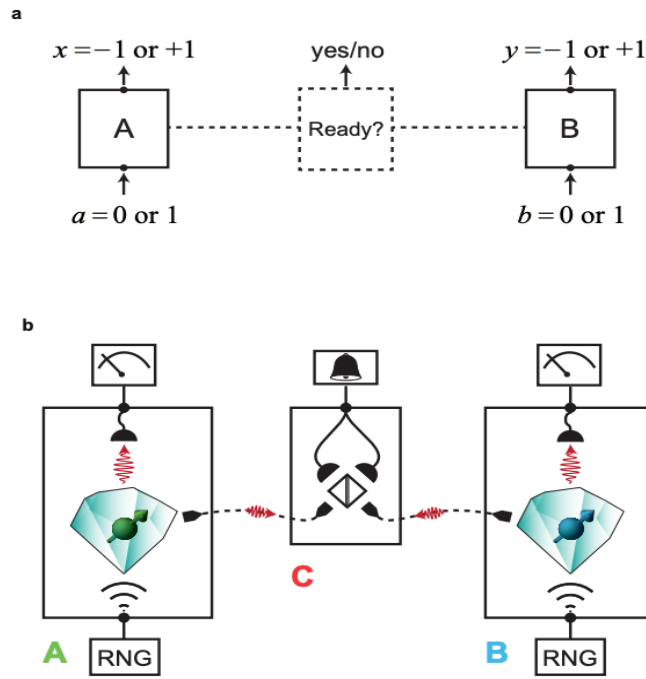


1982年 Aspectの実験



Bellの定理が成り立っていることの実験での確認

2015年 Delft University での実験



<https://arxiv.org/pdf/1508.05949.pdf>



Tsirelson Bound とSelf-Test



CHSH Game のTsirelson's Bound

CHSH Game $a+b=xy(\text{mod } 2)$

$$S = \underbrace{A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0}_{\text{win}} - \underbrace{A_1 \otimes B_1}_{\text{lose}}$$

$$|\psi\rangle = (|00\rangle + |11\rangle) / \sqrt{2}$$

$$\langle\psi|S|\psi\rangle = 4(\text{Prob}(\text{勝ち}) - \text{Prob}(\text{負け}))$$

古典論的には $\langle\psi|S|\psi\rangle \leq 2$

量子論的には $\langle\psi|S|\psi\rangle \leq 2\sqrt{2}$ **Tsirelson's Bound**

Tsirelson's Bound

$$\|\cdot\|_\infty \leq 2$$

$$\|\cdot\|_\infty \leq 2$$

$$S^2 = 4 I \otimes I - [A_0, A_1] \otimes [B_0, B_1]$$

交換子 $[A_0, A_1] = A_0 A_1 - A_1 A_0$

$$\|S^2\|_\infty \leq 8$$

$$\Rightarrow \|S\|_\infty \leq 2\sqrt{2}$$

この不等式を満たすためには、

A_0, A_1 は、反可換
 B_0, B_1 は、反可換

である必要がある。

古典論では、演算子は可換である。

Self-Test

- CHSHゲームで、3/4以上の勝率をあげることができるのは、古典論では存在しない、純粋に量子論的と言っていいエンタングルメントの働きであるのは確かである。
- しかし、それだけでは問題は終わらない。もし、AliceとBobのペアが、最適値と思われる $\cos^2(\pi/8)$ の勝率をマークしたとすれば、二人は、必ずEPRペアを共有していると言えるのだろうか？

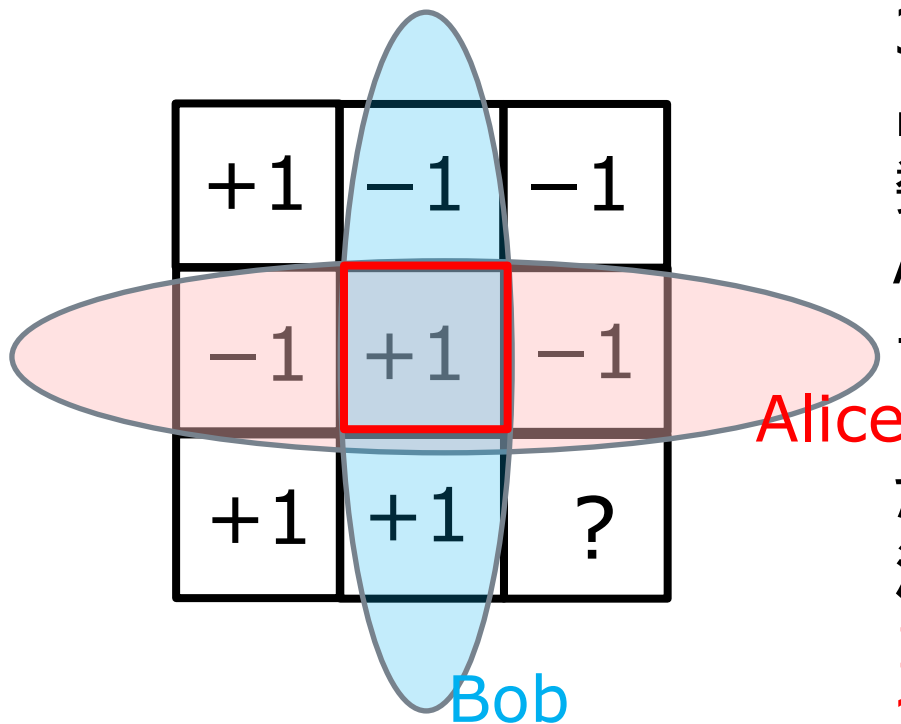
$$|EPR\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$

Self-Testing

- 量子的な戦略がユニークなものであるなら(最大の勝率をマークする戦略は、ユニークである)、それに対応した相関が存在する。こうした関係を Self-Testingと呼ぶ。
- 非形式に言えば、実際に観測された相関のみに基づいて、量子状態と観測について検証することを、Self-Testingと呼ぶ。
- 形式的定義:
 $\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}$ を質問と答の集合とする。 $\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}$ 上の相関 p_* を、量子的な戦略
 $(|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B, \{A_x\}, \{B_y\})$
をSelf-Testするという。
ただし、局所的にisometryなものを同じものとみなして、この戦略が、 p_* を達成する唯一の戦略であるものとする。

Magic Square Game

Magic Square Gameのルール



3 x 3 の升目を+1か-1で埋める。
出題者は、ランダムに1から3までの
数字*i*と*j*を、AliceとBobに提示する。
Aliceは、*i*行目を、Bobは*j*列目を、
+1か-1で埋めて答える。

ただし、二人の答えは、次の条件を
満たすこと。

1. 行の数字の積は、+1。
2. 列の数字の積は、-1。
3. 行と列が交わる場所は、一致。

V: 出題者



問題

“2行目を埋めて”

問題

“2列目を埋めて”

Alice



Bob



$\{-1, +1, -1\}$

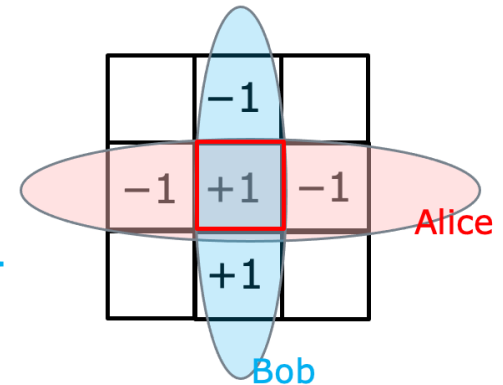
答

$\{-1, +1, +1\}$

答



V: 検証



$-1 \times +1 \times -1 = +1$
 $-1 \times +1 \times +1 = -1$
共通部は一致 合格！

最良の戦略 勝率8/9

- このゲーム、Aliceチームに必勝の戦略は存在しない。
三つの行の積が、それぞれ+1になるということは、 3×3 の9つの数字の積が+1になるということである。
三つの列の積が、それぞれ-1になるということは、 3×3 の9つの数字の積が-1になるということである。
行の積の条件と、列の積の条件を全て満たす9つの数字を選ぶことは不可能である。
- Aliceチームが取りうる最良の戦略は、事前に、例えば、先のページで示した配置を記憶して、それをそのまま答えることである。この時、“3行目と3列目を埋めよ”という問題には、?の部分を適当に答えても、失敗する。
- ただし、行と列の指定には、9通りの可能性があるのだが、この例以外は、条件をクリアできる。よって勝率は8/9となる。

Magic Square Gameの 最大勝率

- ただし、驚くべきことに、Magic Square Gameには、必勝法が存在するのである。
- CHSHゲームでは、一つのエンタングルした量子をAliceとBobが共有することで、勝率をアップすることができたのだが、このゲームでは、二つのエンタングルした量子を共有することで、出題者のどんな問題に対しても、完全な答えを返すことができる。
- ここでは、数字 $+1, -1$ ではなく、演算子 I ($+1$ に対応)と、演算子 $-I$ (-1 に対応)で考える。

基本的な準備

Pauli演算子 $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ は、次のような性質を持つ。

$$X^2 = Z^2 = I, XZ = -ZX$$

$$(XI)^2 = (IX)^2 = (ZI)^2 = (IZ)^2 = I$$

$$[XI, IX] = [XI, IZ] = [ZI, IX] = [ZI, IZ] = 0$$

$$(XI)(ZI) = -(ZI)(XI), (IX)(IZ) = -(IZ)(IX)$$

Magic Square Gameの戦略

$I \otimes X$	$X \otimes I$	$X \otimes X$	I
$Z \otimes I$	$I \otimes Z$	$Z \otimes Z$	I
$-Z \otimes X$	$-X \otimes Z$	$(XZ) \otimes (ZX)$	I
$-I$	$-I$	$-I$	

Magic Square Gameの戦略

$I \otimes X$	$X \otimes I$	$X \otimes X$	I
$Z \otimes I$	$I \otimes Z$	$Z \otimes Z$	I
$-Z \otimes X$	$-X \otimes Z$	$(XZ) \otimes (ZX)$	I
$-I$	$-I$	$-I$	

$$(IXX) \otimes (XIX) = I \otimes I$$

Magic Square Gameの戦略

$I \otimes X$	$X \otimes I$	$X \otimes X$	I
$Z \otimes I$	$I \otimes Z$	$Z \otimes Z$	I
$-Z \otimes X$	$-X \otimes Z$	$(XZ) \otimes (ZX)$	I
$-I$	$-I$	$-I$	

$$(ZIZ) \otimes (IZZ) = I \otimes I = I$$

Magic Square Gameの戦略

$I \otimes X$	$X \otimes I$	$X \otimes X$	I
$Z \otimes I$	$I \otimes Z$	$Z \otimes Z$	I
$-Z \otimes X$	$-X \otimes Z$	$(XZ) \otimes (ZX)$	I
$-I$	$-I$	$-I$	

$$(ZX XZ) \otimes (XZZX) = I \otimes I$$

Magic Square Gameの戦略

$I \otimes X$	$X \otimes I$	$X \otimes X$	I
$Z \otimes I$	$I \otimes Z$	$Z \otimes Z$	I
$-Z \otimes X$	$-X \otimes Z$	$(XZ) \otimes (ZX)$	I
$-I$	$-I$	$-I$	

$$-(IZZ) \otimes (XIX) = -I \otimes I$$

Magic Square Gameの戦略

$I \otimes X$	$X \otimes I$	$X \otimes X$	I
$Z \otimes I$	$I \otimes Z$	$Z \otimes Z$	I
$-Z \otimes Z$	$-X \otimes Z$	$(XZ) \otimes (ZX)$	I
$-I$	$-I$	$-I$	

$$-(XIX) \otimes (IZZ) = -I \otimes I$$

Magic Square Gameの戦略

$I \otimes X$	$X \otimes I$	$X \otimes X$	I
$Z \otimes I$	$I \otimes Z$	$Z \otimes Z$	I
$-Z \otimes Z$	$-X \otimes Z$	$(XZ) \otimes (ZX)$	I
$-I$	$-I$	$-I$	

$$(XZXZ) \otimes (XZZX) = -(XZZX) \otimes (XZZX) = -I \otimes I$$

V: 出題者



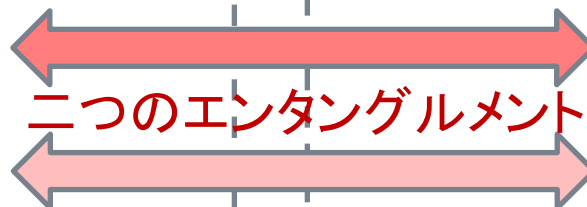
問題

"i 行目を埋めて"

問題

"j 列目を埋めて"

Alice



Bob



$\{-1, +1, -1\}$

答

$\{-1, +1, +1\}$

答



V: 検証

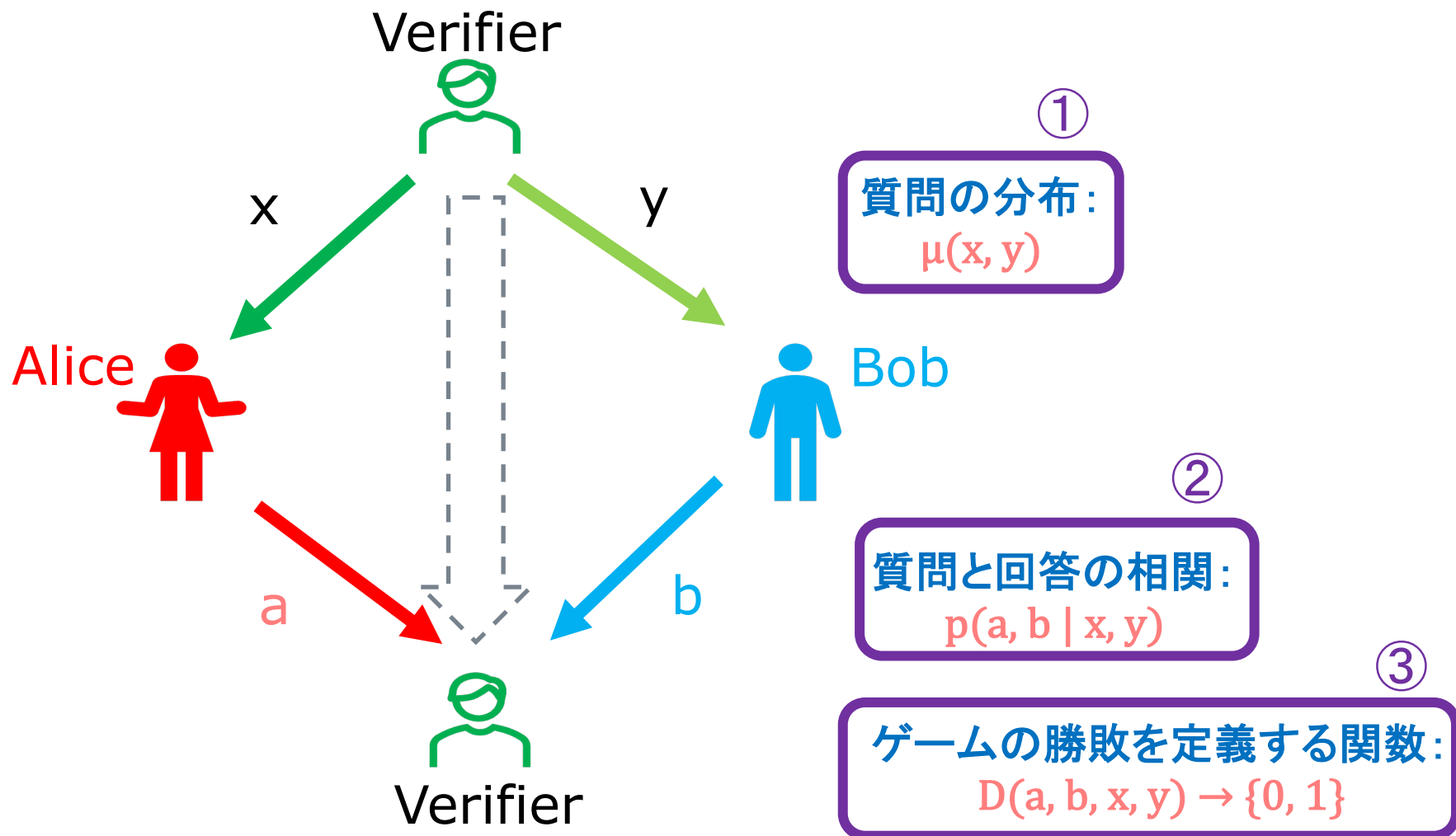
$I \otimes X$	$X \otimes I$	$X \otimes X$	I
$Z \otimes I$	$I \otimes Z$	$Z \otimes Z$	I
$-Z \otimes X$	$-X \otimes Z$	$(XZ) \otimes (ZX)$	I
$-I$	$-I$	$-I$	

nonlocal game と Interactive Proof

nonlocal game と Interactive Proof

- CHSHゲームやMagic Squareゲーム等をnonlocal gameと呼ぶ。nonlocal というのは、非局所的なエンタングルメントの性質を利用して、古典的な相関を超える高い勝率を実現しているからである。
- nonlocalゲームは、量子論が古典論とは異なるものであることを、理論的・実験的に明らかにしようとする取り組みの中で生まれたものであるが、それは次章で見る、Interactive Proofと、同じ構造をしている。
- それは、エンタングルメントを含む点で、単純なIPやMIPより、さらに進んだInteractive Proofである。

nonlocalのゲームの定式化



ゲームの定式化

それぞれのゲームは、次の三つの式で特徴付けられる。

1. 質問の分布: $\mu(x, y)$
2. 質問と回答の相関: $p(a, b \mid x, y)$
入力 x, y が与えられた時 a, b を出力する、条件付き確率である
3. ゲームの勝敗を定義する関数: $D(a, b, x, y) \rightarrow \{0, 1\}$

CHSHゲームの場合、

- $\mu(x, y)$ は、0と1の一樣にランダムな分布、
- $p(a, b \mid x, y)$
 $= p(a, b \mid 0, 0) + p(a, b \mid 0, 1) + p(a, b \mid 1, 0) + p(a, b \mid 1, 1)$ 、
- $D(a, b, x, y)$ は、
 $a + b = xy \pmod{2}$ の時に1を、それ以外の時に0を返す関数である。

ゲームの定式化

それぞれのゲームは、次の三つの式で特徴付けられる。

1. 質問の分布: $\mu(x, y)$
2. 質問と回答の相関: $p(a, b \mid x, y)$
入力 x, y が与えられた時 a, b を出力する、条件付き確率である
3. ゲームの勝敗を定義する関数: $D(a, b, x, y) \rightarrow \{0, 1\}$

CHSHゲームの場合、

- $\mu(x, y)$ は、0と1の一樣にランダムな分布、
- $p(a, b \mid x, y)$
 $= p(a, b \mid 0, 0) + p(a, b \mid 0, 1) + p(a, b \mid 1, 0) + p(a, b \mid 1, 1)$ 、
- $D(a, b, x, y)$ は、
 $a + b = xy \pmod{2}$ の時に1を、それ以外の時に0を返す関数である。

相関pが与えられた時のゲームの勝率

相関pが与えられたときのゲームGの勝率 $\omega(G, p)$ は、次の式で与えられる。

$$\omega(G, p) = \sum_{x,y,a,b} \mu(x, y) \cdot D(x, y, a, b) \cdot p(a, b|x, y)$$

古典論的なCHSHと、エンタングルメントを利用したCHSHとの違いは、相関pが古典論的相関に属するか $p \in C_c$ 、量子論的相関に属するか $p \in C_q$ の違いに帰着する。

どのような相関を選択するかで勝率は変わる。こうして選択された相関をゲームの「戦略」という。

最適な戦略の元でのゲームGの最大勝率 $\omega(G)$

戦略 p の元でのゲームGの勝率を $\omega(G, p)$ で表す。

古典論的相関 C_c のもとでの最大勝率を $\omega_c(G)$ 、
量子論的相関 C_q のもとでの最大勝率を $\omega_q(G)$ と表すと

$$\omega_c(G) = \sup_{p \in C_c} \omega(G, p)$$

$$\omega_q(G) = \sup_{p \in C_q} \omega(G, p)$$

- $\omega_c(\text{CHSH}) = 3/4$
- $\omega_q(\text{CHSH}) = \cos^2(\pi/8)$
- $\omega_c(\text{Magic Square}) = 8/9$
- $\omega_q(\text{Magic Square}) = 1$

ゲームで利用されるエンタングルした量子の数

ゲームGで勝率 p を達成するために利用されるエンタングルした量子の数を $\varepsilon(G, p)$ で表す。

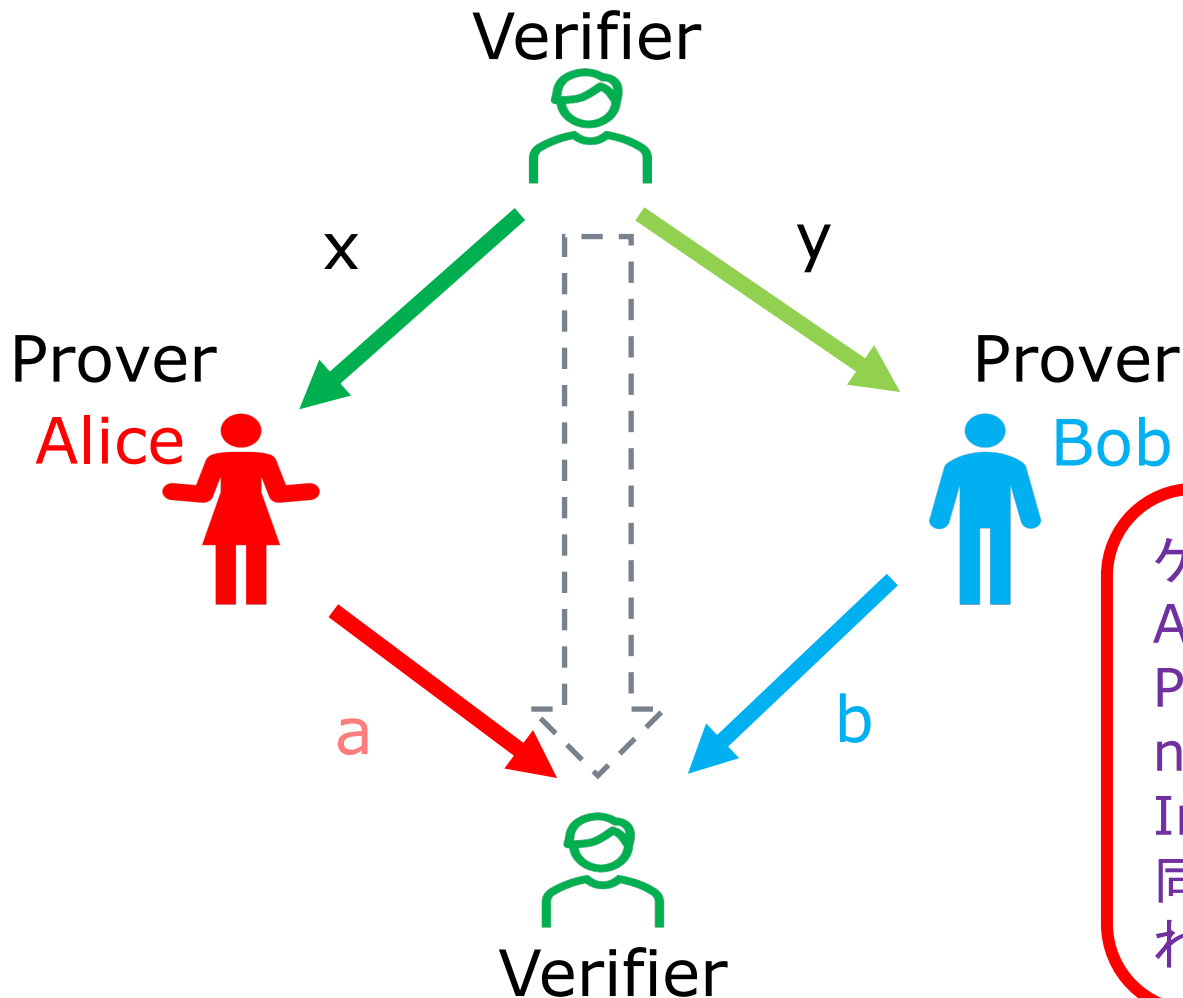
- $\varepsilon(\text{CHSH}, 3/4) = 0$
- $\varepsilon(\text{CHSH}, \cos^2(\pi/8)) = 2$
- $\varepsilon(\text{Magic Square}, 8/9) = 0$
- $\varepsilon(\text{Magic Square}, 1) = 4$

2004年、コンピュータ・サイエンティストのRichard Cleve, Peter Hoyer, Ben Toner, John Watrousらは、Bellの思考実験がInteractive Proofと極めて似ていることに気づく。

彼らは、量子的なMulti-Prover Interactive Proof MIP*を研究することを提案する。彼らが提起した問題は、次のようなものだった。

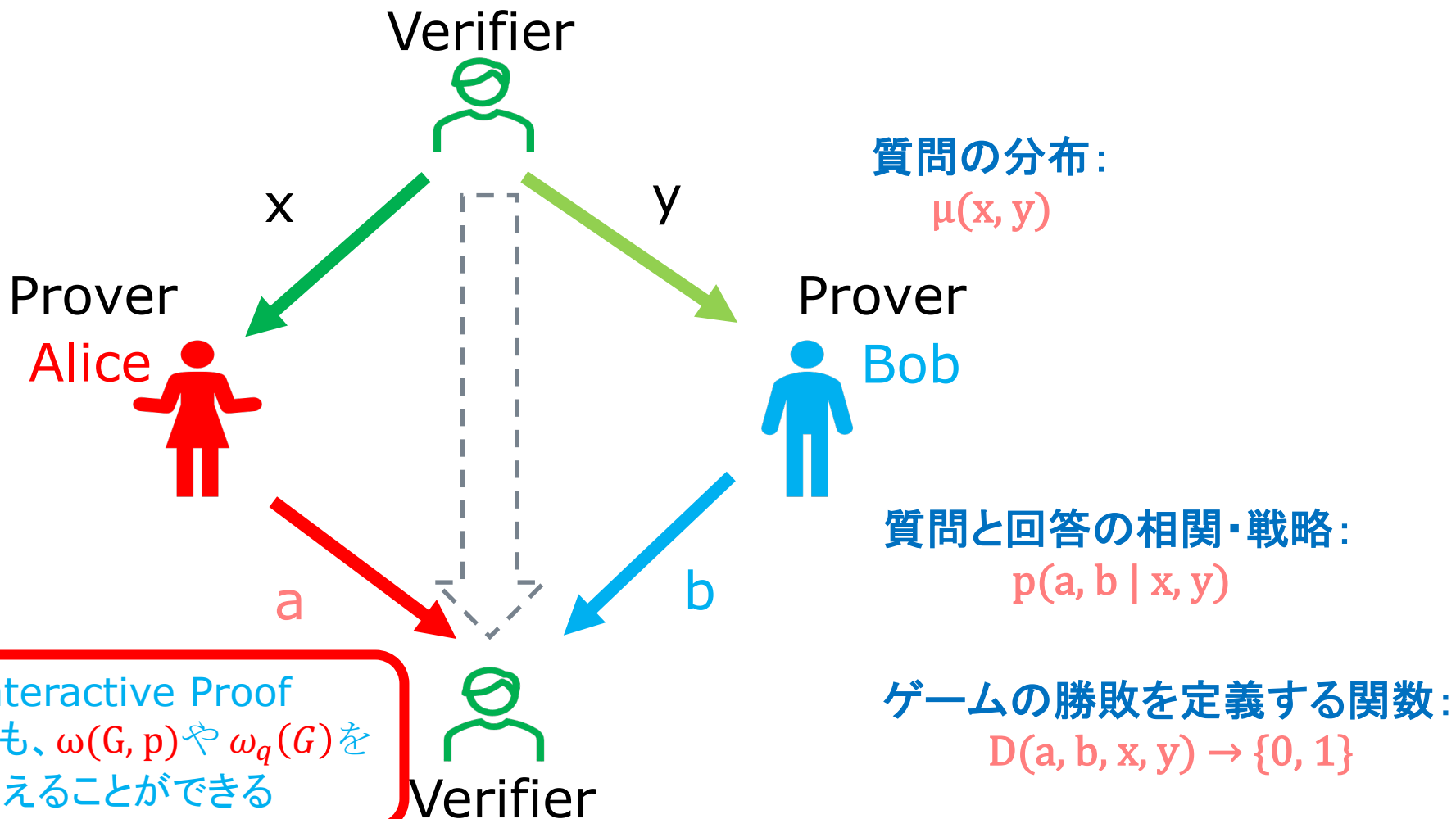
$\omega_q(G)$ を近似的に求めるアルゴリズムは存在するだろうか？

nonlocal ゲームは、Interactive Proofである



ゲームのプレイヤーの Alice と Bob を二人の Prover とみなせば、nonlocal ゲームは Interactive Proof と同じ構造をしていることがわかる。

Interactive Proofは、nonlocal ゲームである







Part II

Interactive Proof

-- 複雑性理論の古典論とその転換 --

Agenda Part II

Interactive Proof -- 複雑性理論の古典論とその転換

- 計算可能性理論と帰納的可算
- 計算複雑性理論の古典論
 - $P=NP?$ 問題とNP-完全問題
- 転換1 Interactive Proof の登場
 - 証明概念の転換
 - 数学的証明問題はNP完全問題である
 - Interactive Proofの想定とパターン
- Interactive Proofの基本的達成 – MIP^* へ
 - $IP=PSPACE$
 - $MIP=NEXP$
 - PCP定理
- 転換2 量子複雑性理論 -- 確率と複雑性クラス

計算可能性理論と 帰納的可算

計算可能性理論

- 1930年代に、ゲーデル、チャーチ、チューリングらによって行われた「計算可能性」「証明可能性」についての研究は、それぞれ見かけ上は全く異なるアプローチをとっていたのにも関わらず、それらの異なるアプローチによって定義される「計算可能性」「証明可能性」は、お互い全く同値であることが証明される。
- 1940年～50年代には、こうした一致した認識は、「計算可能性」についての「チャーチ＝チューリングのテーゼ」として広く共有されることになる。

チャーチ=チューリングのテーゼ

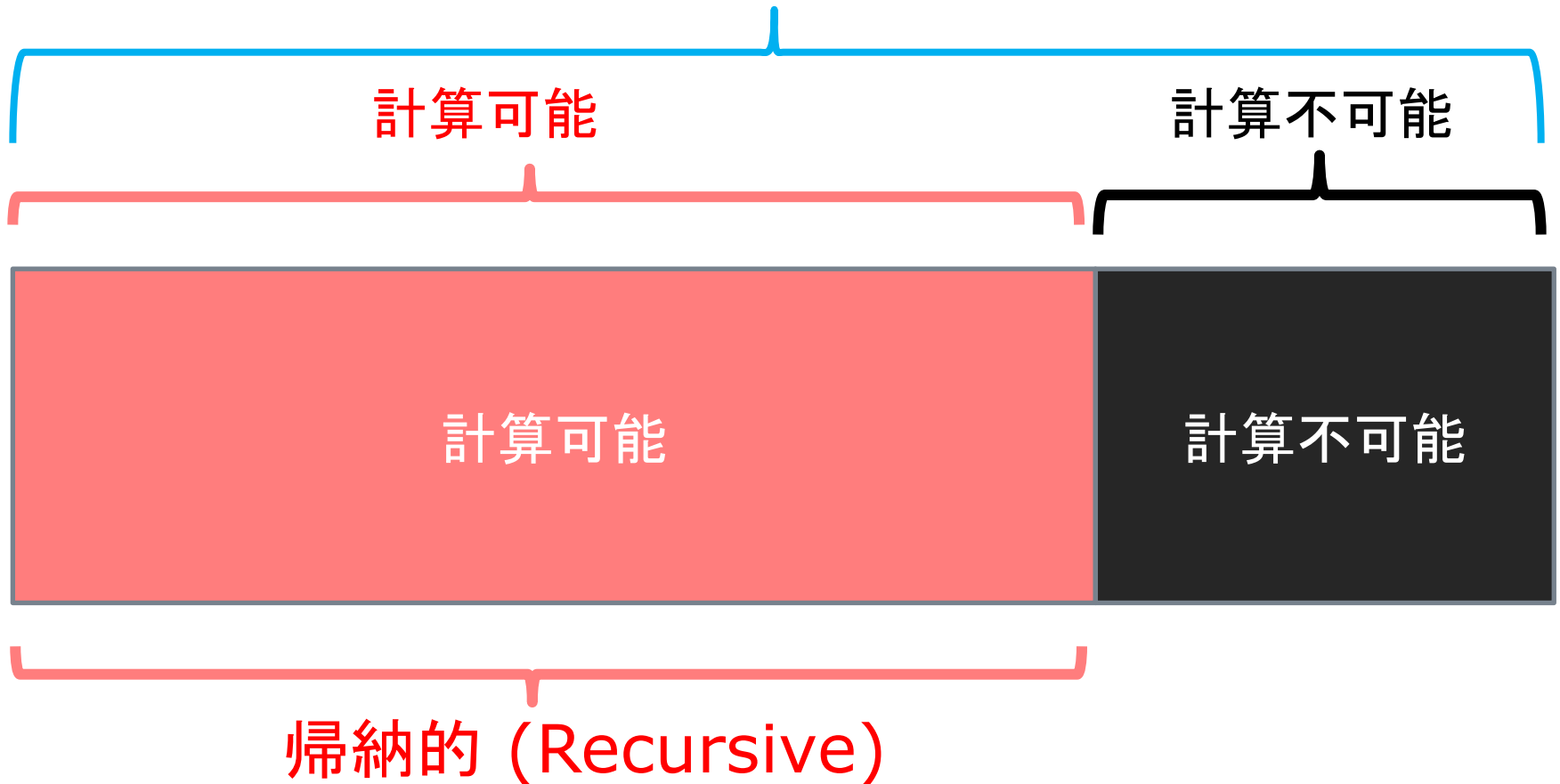
「チャーチ=チューリングのテーゼ」というのは、次のような提案である。これは帰納関数論的特徴づけである。

すべての実効的に計算可能な関数(実効的に決定可能な述語)は、一般帰納的である。

チューリング・マシンによって特徴づければ、次のようになる。計算可能な計算はすべて、ある帰納的Turingマシンによって実行される。

計算可能性理論

-- Church-Turing Thesis --



帰納的可算

recursively enumerable

- ある自然数の集合 S に対して、チューリング・マシン M が存在して、次の条件を満たす時、 S は「帰納的可算 recursively enumerable」であるという。
 - $n \in S$ なら、 M は停止して 1 を出力する。
- この定義でポイントが一つある。
 M は、 S に属するメンバーに対しては、停止して 1 を出力するのだが、 S に属さないメンバーに対しては、何も語っていない。
recursively enumerable なチューリング・マシン M では、全ての入力に対して M が停止するとは限らないということである。
- S に属さないメンバーに対しても、チューリング・マシン M が停止することを要求するのが、次の「帰納的 recursive」の定義である。

帰納的 recursive

- 自然数の集合 S は、次の条件を満たすチューリング・マシン M が存在する時、「帰納的 recursive な集合」と呼ばれる。
与えられた自然数 n について、
 - $n \in S$ なら、 M は停止して 1 を出力する。
 - $n \notin S$ なら、 M は停止して 0 を出力する。

- 自然数から自然数への関数 f は、次の条件を満たすチューリング・マシンが存在する時、「帰納的な関数」と呼ばれる。
 - 全ての入力 n に対して、 M は停止して、出力 $f(n)$ を返す。

計算可能な集合 / 関数は、帰納的であるという主張が、Church-Turing Thesis である。

帰納的可算

自然数の集合 S は、次の条件を満たすチューリング・マシン M が存在する時、「**帰納的可算**」と呼ばれる

帰納的

帰納的可算

計算
不可能

- $n \in S$ なら、 M は停止して 1 を出力する。

$MIP^* = RE$ 定理の
‘RE’は、このクラス
である。

帰納的

自然数の集合 S は、次の条件を満たす
チューリング・マシン M が存在する時、
「**帰納的**」と呼ばれる

帰納的

帰納的可算

計算
不可能

- $n \in S$ なら、 M は停止して 1 を出力する。
- $n \notin S$ なら、 M は停止して 0 を出力する。

歸納的と歸納的可算

計算可能

計算不可能

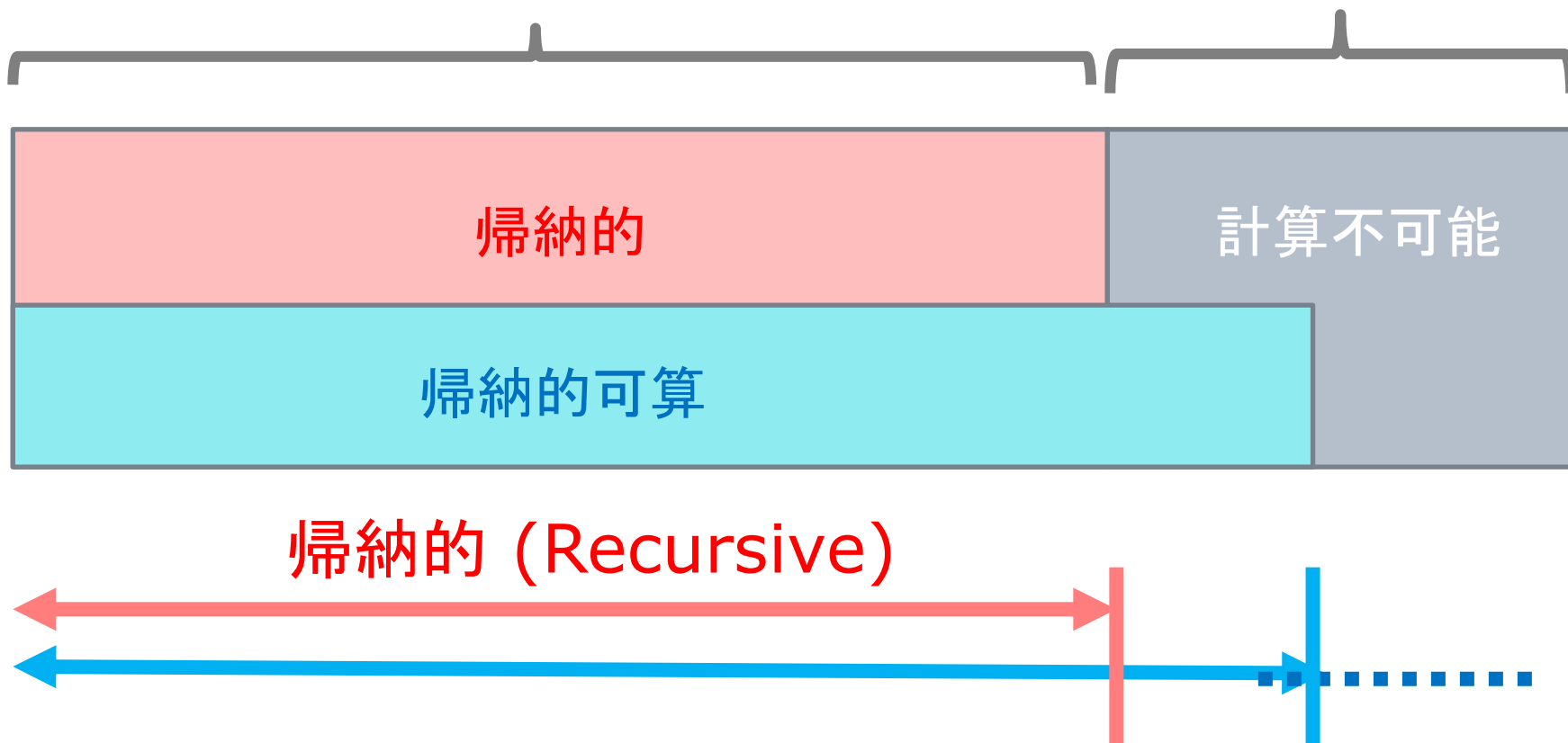
歸納的

計算不可能

歸納的可算

歸納的 (Recursive)

歸納的可算 (Recursively Enumerable)



計算複雑性理論の古典論

計算複雑性理論

ある数学的命題 S の真偽を決定する「純粹に機械的手続き」は存在しないにせよ、その S が、ある制限長さ n 以下の証明を持つかどうかを決定する手続きは存在する。單純に、長さ n 以下の証明を全て枚挙して、それが命題 S の証明になっているかをチェックすればいい。

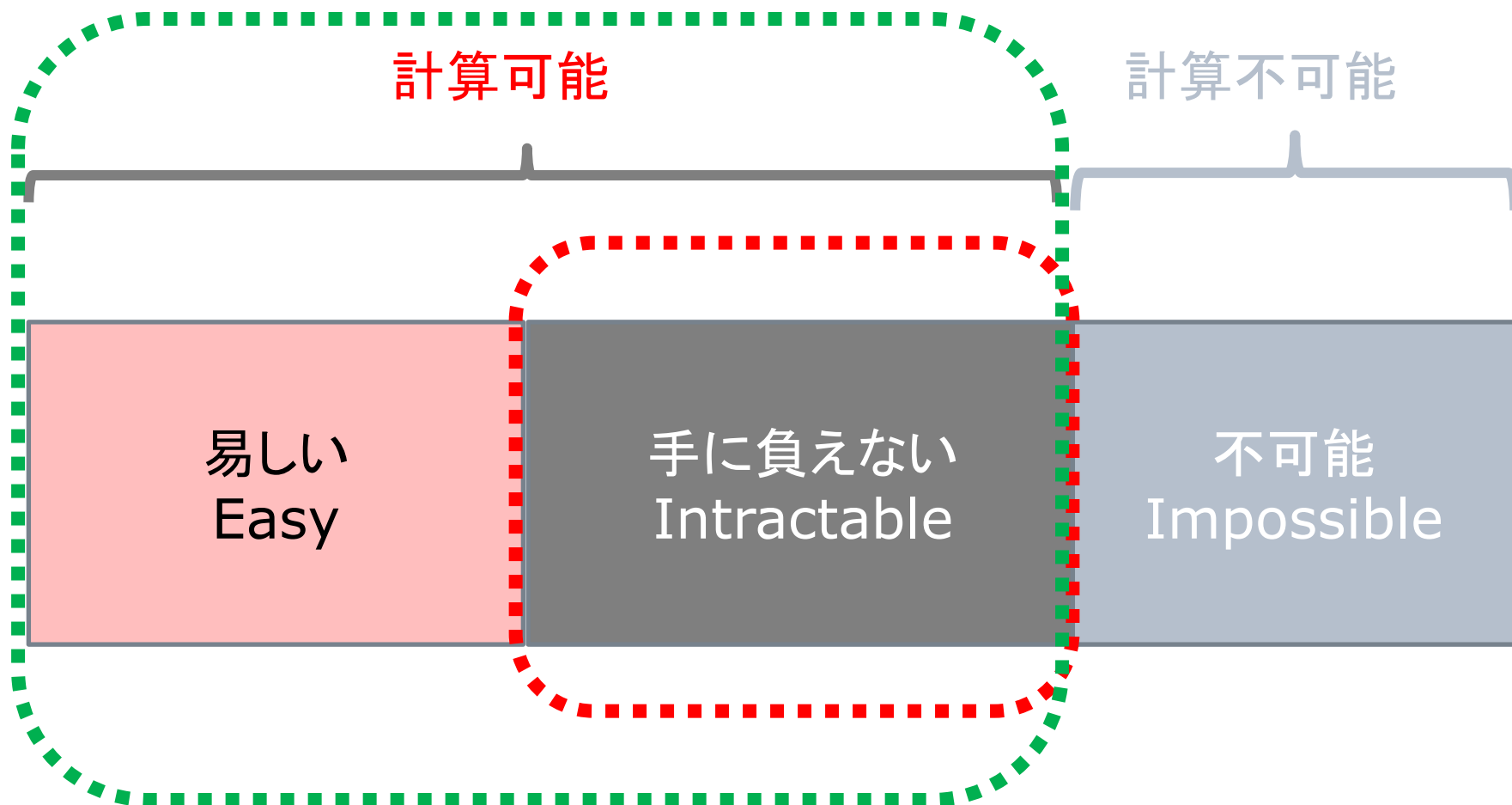
しかし、この方法は指数関数的な時間を必要とする。実際には手に負えない。 $P=NP?$ 問題は、こうした問題を解く「高速」なアルゴリズムがあるかを問うている。その意味では、 $P=NP?$ 問題は、ヒルベルトの問題提起の現代版だと考えることができる。

計算複雑性理論の始まり

この問題が、明確に提起されたのは、1970年代の初めのことで、CookとLevinの仕事である。現在のようなスタイルで、 $P = NP?$ 問題を最初に定式化したのは、バークレーのStephen Cookだ。1967年のことだ。計算複雑性理論の始まりである。

ただ、こうした問題が存在することは、50年代に、ゲーデルもナッシュも気がついていていた。

計算可能だが計算が手に負えないものがある



計算可能性理論

計算複雑性理論

易しい
Easy

手に負えない
Intractable

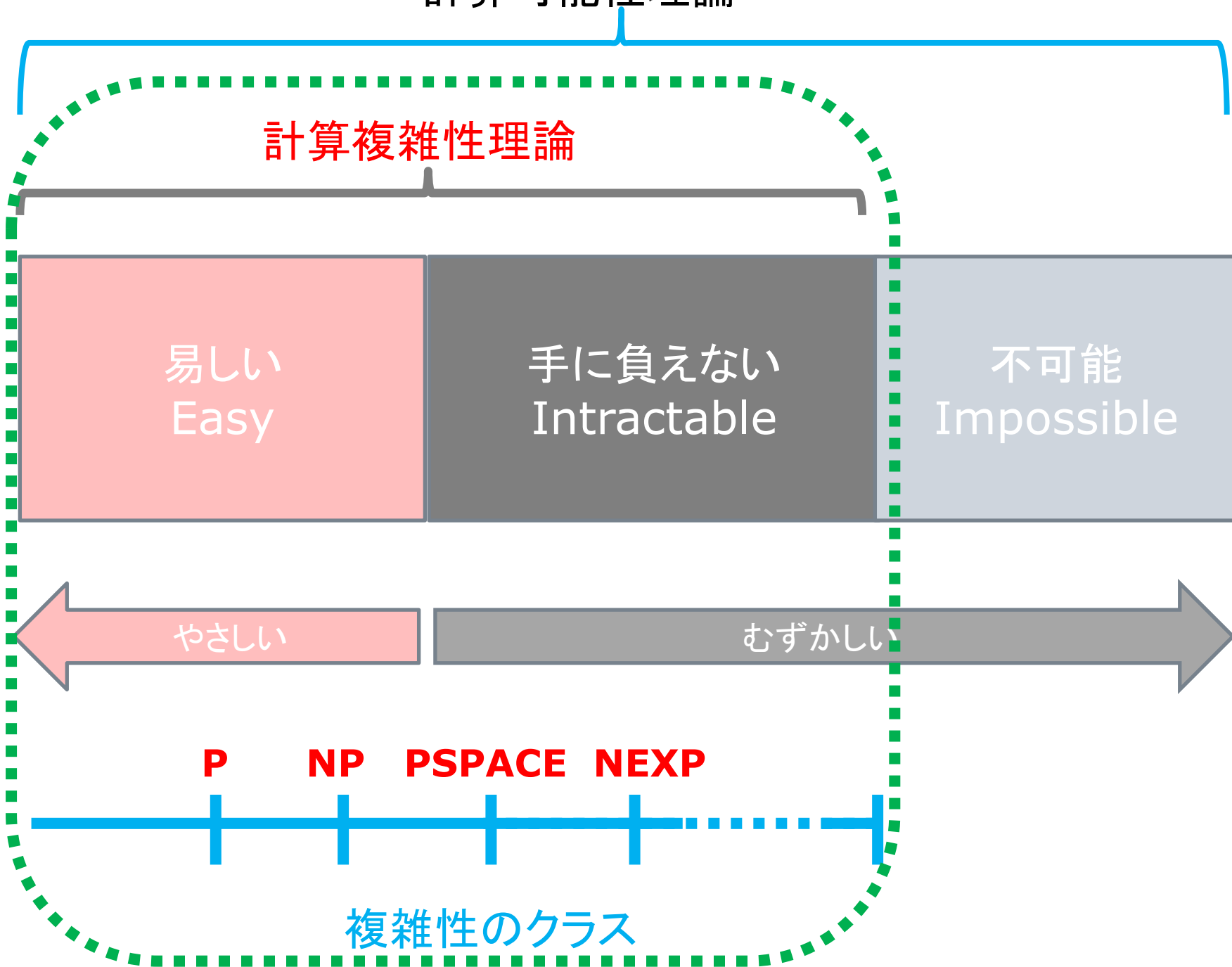
不可能
Impossible

やさしい

むずかしい

P **NP** **PSPACE** **NEXP**

複雑性のクラス

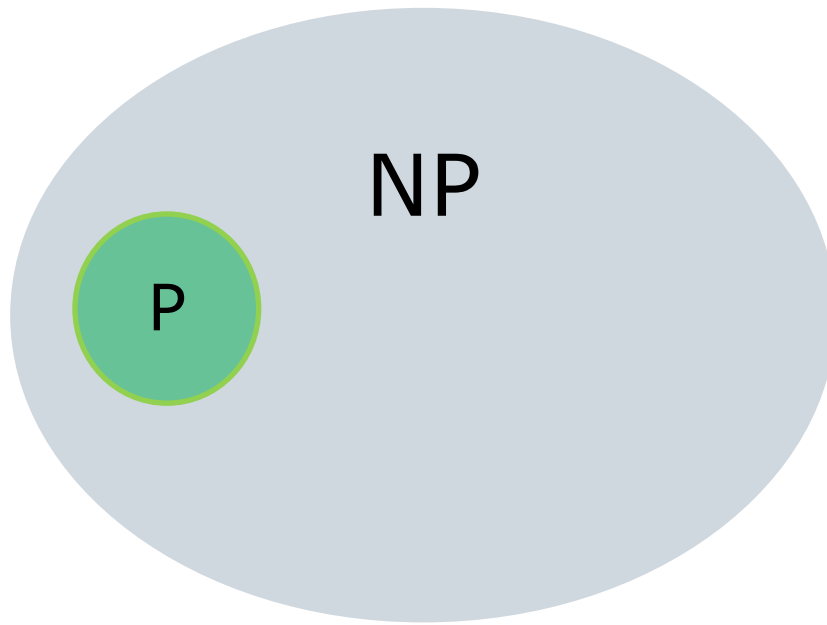


NP問題

その問題を解くのが「多項式時間」で終わるかどうかはわからなくても、具体的な値で与えられたその問題の「答え」と言われるものが、本当に「正しい答え」であるかどうかを「多項式時間」でチェックできる問題のクラスを、NPという。素因数分解問題は、NP問題である。

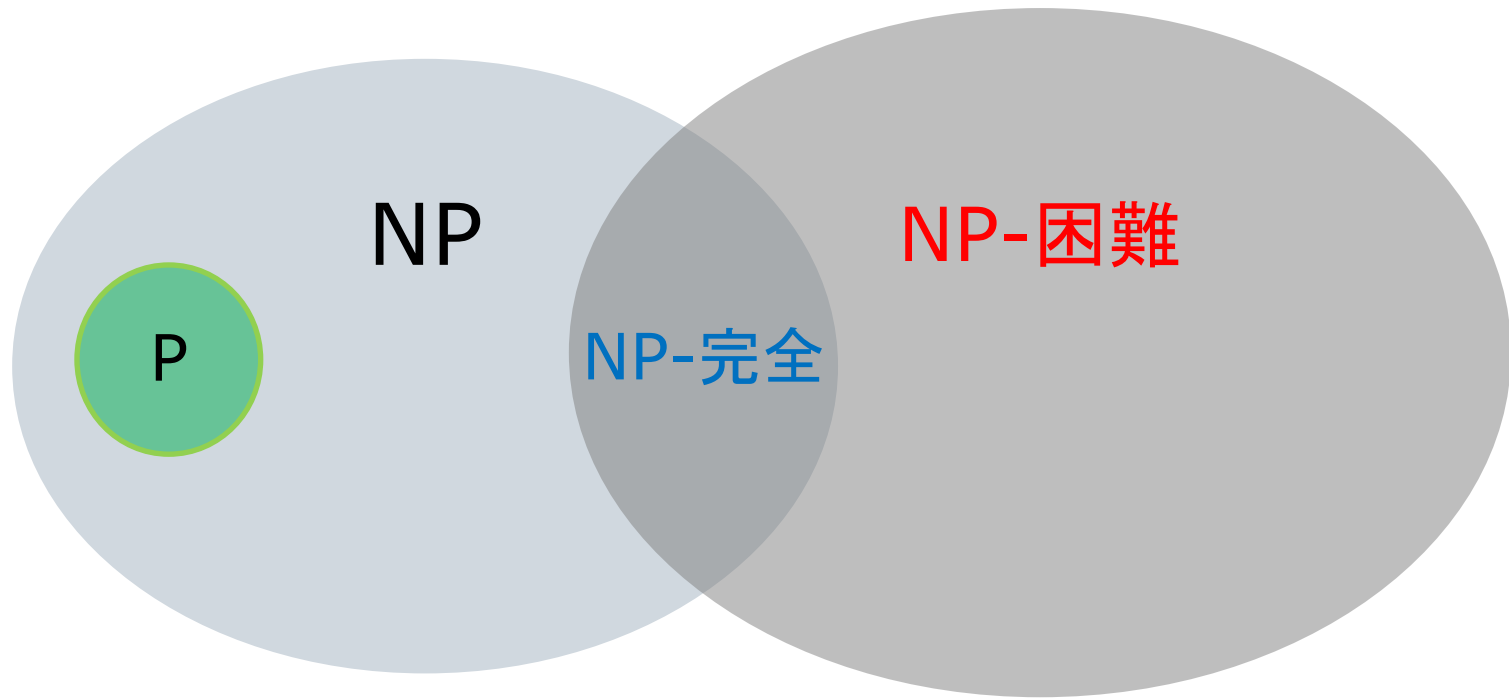
(ちなみに、「答え」(なるもの)が与えられた時、それが「間違った答え」であるかどうかを「多項式時間」でチェックできる問題のクラスを、co-NP問題という。素因数分解問題は、co-NP問題でもある。)

こうしたことや、NP問題である素因数分解問題に現れる「難しさ」と「易しさ」の「非対称性」が、現在の公開キー暗号の基礎になっていることは、多くの人が既に知っていることかもしれない。



P: 多項式時間で解ける問題

NP: 多項式時間で解けるとは限らないが、
答えが正しいかは多項式時間でチェックできる問題



P: 多項式時間で解ける問題

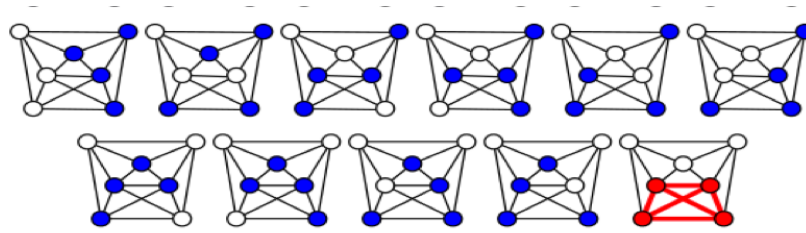
NP: 多項式時間で解けるとは限らないが、
答えが正しいかは多項式時間でチェックできる問題

NP-困難: 全てのNP問題が、このクラスの問題に帰着される問題
(この帰着は多項式時間で行われなければならない)

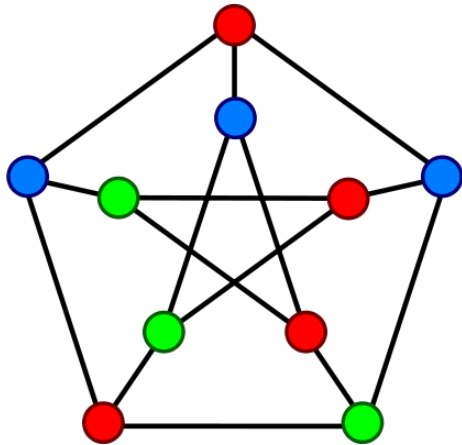
NP-完全: NP問題で、かつ、NP-困難な問題

NP-完全問題

- 1971年、Cookは、充足可能性問題が、NP-完全であることを証明した。ここに初めて、NP-完全というコンセプトが登場する。（同じ頃、ソヴィエトの数学者Levinも同じ結果を得ている）現代の複雑性理論は、この発見から始まる。
- 1972年、Karpは、ある問題がNP-完全であることを証明する標準的な「還元」の手法を開発し、多くの問題がNP-完全であることを示した（「Karpの21の問題」）。
- このNP-完全問題のリストは、現在では数百の問題をカバーして拡大している。（例えば、“List of NP-complete problems” <https://goo.gl/XUSvRz> ）
- これらの問題の「手に負えなさ: “Intractability ”」は、例外的なものではなく、一般的なものである。
- Cookは1982年、Karpは1985年、Turing賞を受賞した。



Clique



Graph Coloring

$$\begin{aligned}
 &(l_1 \vee l_2 \vee x_2) \wedge \\
 &(\neg x_2 \vee l_3 \vee x_3) \wedge \\
 &(\neg x_3 \vee l_4 \vee x_4) \wedge \cdots \wedge \\
 &(\neg x_{n-3} \vee l_{n-2} \vee x_{n-2}) \wedge \\
 &(\neg x_{n-2} \vee l_{n-1} \vee l_n)
 \end{aligned}$$

3-SAT



Hamilton Path

様々なNP-完全問題

轉換1: Interactive Proof の登場

Interactive Proofの登場

1990年代に入って、計算複雑性理論は、大きく発展する。その転機となったのは、László Babai, Shafi Goldwasser, Silvio Micali, Shlomo Moran, Charles Rackoff らによるInteractive Proof Systemである。Interactive Proofの登場は、計算複雑性理論を一変させた。

彼ら(彼女)らは、1993年、新設された「**ゲーデル賞**」の最初の受賞者となる。この手法とその拡張は、 $MIP^* = RE$ 定理の証明で本質的な役割を果たす。

こうした方向での研究の重要な達成としての、1996-98年の**PCP Theorem**も、 $MIP^* = RE$ 定理の証明で重要な役割を果たすことになる。

ゲーデル賞の女性たち



Shafi Goldwasser

Gödel Prize 1993, 2001

Interactive Proof



Irit Dinur

Gödel Prize 2019

PCP定理の新証明

「証明者」と「検証者」の分離と 両者の「対話」としての証明

- これまでも、数学的証明の特質については、様々な議論があった。証明が従うべき演繹規則、その出発点としての公理群、証明体系の無矛盾性 ... 等々、ただ、それは、主に証明を行う側から証明を考えたものだった。
- Interactive Proofの特徴は、「証明者」と「検証者」を分離し、証明を「証明者」と「検証者」の両者の「対話」の過程として捉え返すことである。

証明を、検証の側から捉え直す 検証されたものが正しい証明である

- それはまた、証明を証明の世界に閉じたものと考えることをやめて、証明を検証との関係で、検証の側から捉え返すことでもあった。
- 証明は、もともとが正しい推論によって導かれているから、正しいと検証されるのだと考えることと、正しいと検証されるから正しい証明だと考えることは別のことである。
- Interactive Proofのアプローチは、証明の正しさについて後者の考え方をとる。正しいと検証されたものが正しい証明なのである。

「確率的に検証可能な証明」 というコンセプト

- 「正しいものから正しいものを演繹する」という証明観では、証明の世界と確率の世界を結びつけるのは難しい。演繹のルールは確率論的性質を持たず、厳密に決定論的に振る舞うからである。
- ただ、検証の世界は、確率論的な性質を持つ。証明者が、正しい証明を持っていない場合には、検証者に返す答がランダムなものになるのは明らかだし、正しい証明を持っている場合には、証明者が提示するサンプルの全てを検証する必要はない。
- 検証から証明を捉え返した時、証明の世界と確率の世界は結びつき、「確率的に検証可能な証明」という重要なコンセプトが現れてくる。

証明概念の転換としての Interactive Proof

- こうした、「証明観」の大きな転換は、証明が可能とするものの領域を大きく広げることとなった。
- Interactive Proofの基本的な想定と、それによる証明の射程の拡大を見る前に、我々が、これまで考えてきた、いわば「古典」的な「証明論」が、複雑性クラスのNP-完全のクラスにすっぽりと含まれることを見ておこう。

古典的な証明のイメージ

命題: T

証明: $\pi_1, \pi_2, \pi_3, \dots, \pi_n = T$

- π_i は、公理であるか、予め定義された論理的な演繹規則から導かれた命題である。(ここでは、ZFCの公理系を取ろう)
- 論理的な演繹規則は、一階の述語論理を利用することにしよう。
- π_i が、 $\pi_1, \pi_2, \pi_3, \dots, \pi_{i-1}$ から導かれることは、簡単にチェックされなければならない。それが、我々が証明を理解できるということである。

チェックのアルゴリズムと数学的導出

命題: T

証明: $\pi_1, \pi_2, \pi_3, \dots, \pi_n = T$

- 数学的証明のシステムを形式化するには、
 $\pi_1, \pi_2, \pi_3, \dots, \pi_{i-1} \rightarrow \pi_i$ なる数学的導出の各ステップを形式化すれば十分である。それは、チェックのアルゴリズムを形式化することに等しい。
- 数学的導出のルール、すなわち、それぞれのチェック・アルゴリズムが、証明の中に現れる命題と証明全体を規定している。
- また、証明が有限の時間のうちに検証可能であるなら、それを構成する、それぞれのチェック・アルゴリズム、すなわち、数学的導出のルールは、時間的な制約条件を満たさなければならない。

数学的証明問題はNP完全問題である

数学の問題を解くことは難しいが、その証明を理解することは証明を行うより容易である。かつその証明の理解は、多項式時間で行われる。数学的証明は、NP問題である。

証明可能な数学的な命題が、NP-困難のクラスに属することは自明である。なぜなら、数学的に記述された全てのNP問題は、証明可能な数学的命題のクラスに還元できるからである。

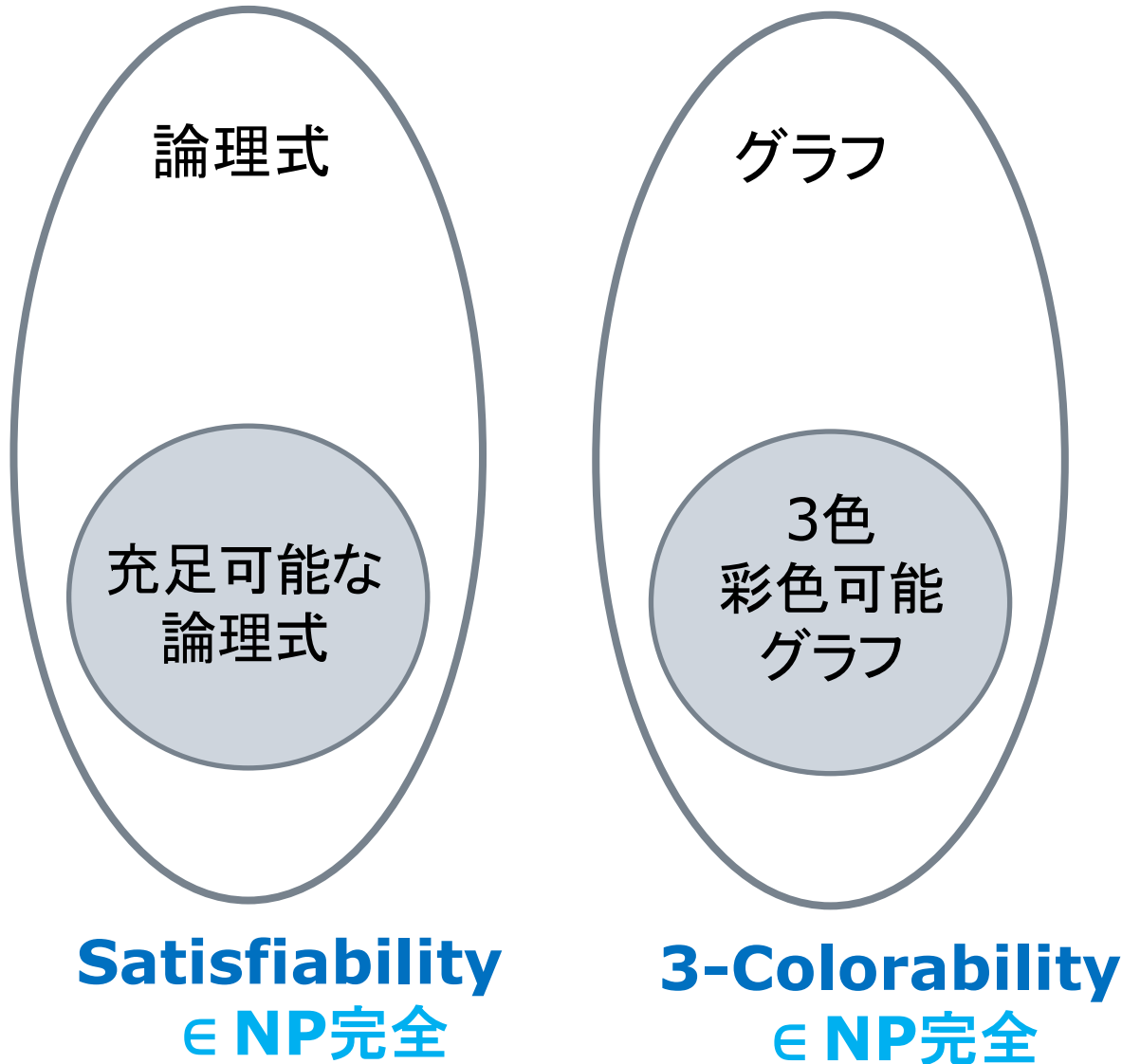
よって、(実効的に)証明可能な数学的な命題のクラスは、NP完全である。

代表的なNP完全のクラス



Satisfiability
∈ NP完全

代表的なNP完全のクラス



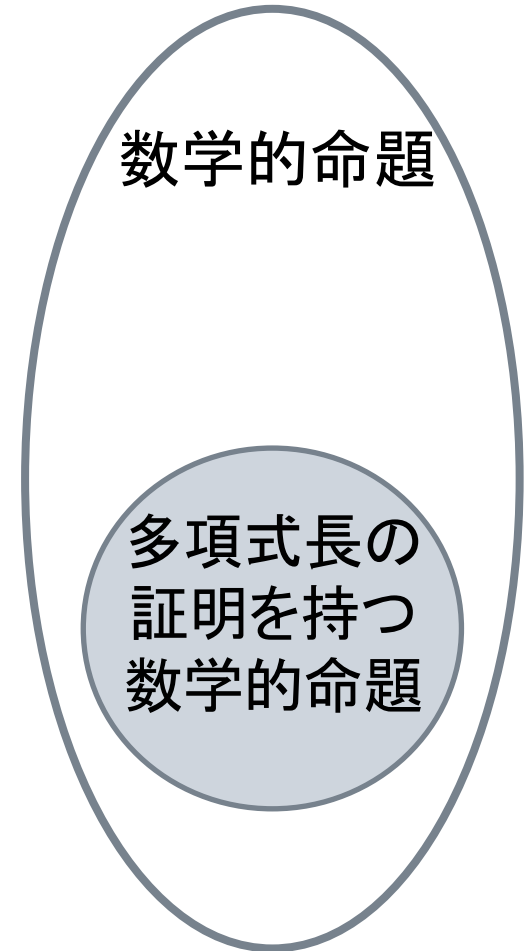
代表的なNP完全のクラス



Satisfiability
∈ NP完全



3-Colorability
∈ NP完全



Efficient ZFC
∈ NP完全

代表的なNP完全のクラス

論理式

充足可能な
論理式

Satisfiability
∈ NP完全

グラフ

3色
彩色可能
グラフ

3-Colorability
∈ NP完全

数学的命題

多項式長の
証明を持つ
数学的命題

Efficient ZFC
∈ NP完全

Interactive Proofの基本的な想定

ProverとVerifierの役割

Interactive Proofでは、Prover(「証明者」)、Verifier(「検証者」)について、次のような役割を想定をする。

1. 「証明者」は、「検証者」に「証明」を提示し、「検証者」は、その「証明」を「検証」する。
2. ただし、「証明者」は、常に正しいことをいうとは限らない。
3. 「検証者」は、何度でも「証明者」に質問をすることができる。「証明者」は、必ずそれに答えなければならない。「検証者」は、その答えを「検証」する
4. 「証明者」が「検証者」に、その「証明」が正しいと確信させるのに成功した時、その証明は終わる。

Interactive Proofの基本的な想定

ProverとVerifierの計算能力

Interactive Proofでは、Prover(「証明者」)、Verifier(「検証者」)の計算能力について、次のような想定をする。

1. 「証明者」の方が、「計算者」より高い計算能力を持つ。
2. 「証明者」は無限の計算能力を持つと想定する。複雑性理論での「オラクル」と似た役割を果たす。
3. 「検証者」は、人間がモデルと置いていい。その計算能力は多項式時間で制限され有限である。複雑性のクラスとしては、PまたはBPPのクラスで特徴付けられる。

Interactive Proofの基本的なパターン

Interactive Proofには、次のようなパターンがある。

1. IP(Interactive Proof):

証明者一人と検証者との対話型証明。

2. MIP(Multi Prover Interactive Proof):

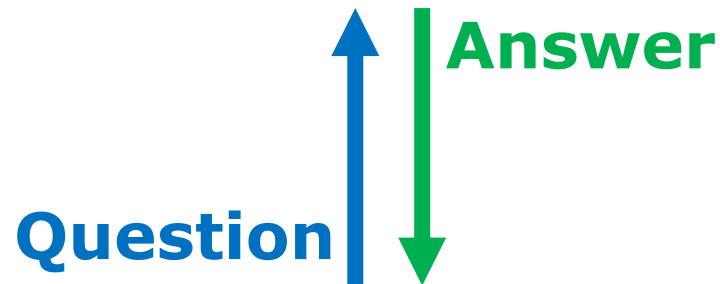
複数の証明者と検証者との対話型証明。

3. MIP*(Multi Prover Interactive Proof with Entanglement):

エンタングルした量子を共有する複数の証明者と検証者との対話型証明。



Prover



IP



Verifier

Interactive Proof



Prover A



Prover B

Answer a

Answer b

Question x

Question y

MIP



Verifier

**Multi Prover
Interactive Proof**

2004年、コンピュータ・サイエンティストのRichard Cleve, Peter Hoyer, Ben Toner, John Watrousらは、Bellの思考実験がInteractive Proofと極めて似ていることに気づく。

彼らは、量子的なMulti-Prover Interactive Proof MIP*を研究することを提案する。彼らが提起した問題は、次のようなものだった。

$\omega_q(G)$ を近似的に求めるアルゴリズムは存在するだろうか？



Entanglement



Answer a

Answer b

Question x

Question y

*MIP**



Verifier

Multi Prover
Interactive Proof
with Entanglement



Entanglement

複数のエンタ
ングルした量子の
共有を許す



Answer a

Answer b

Question x

Question y

*MIP**



Verifier

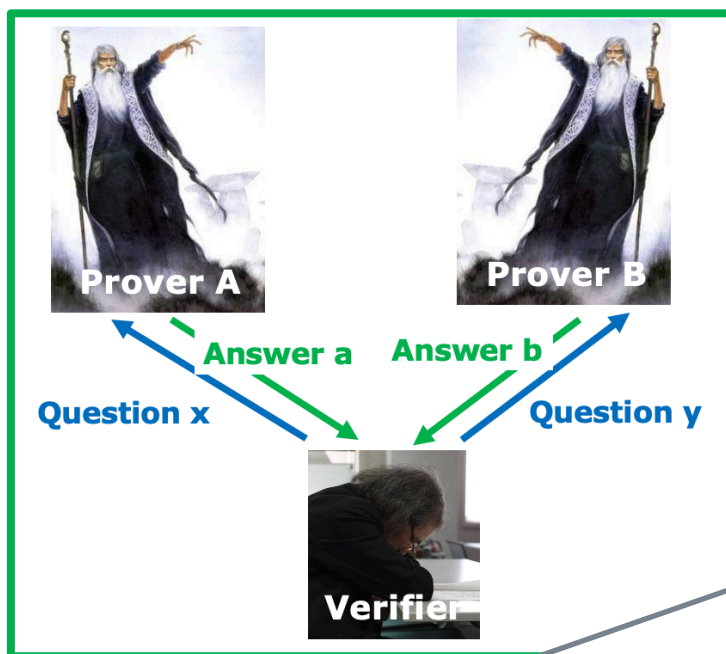
Multi Prover
Interactive Proof
with Entanglement

Interactive Proof の いくつかのパターン

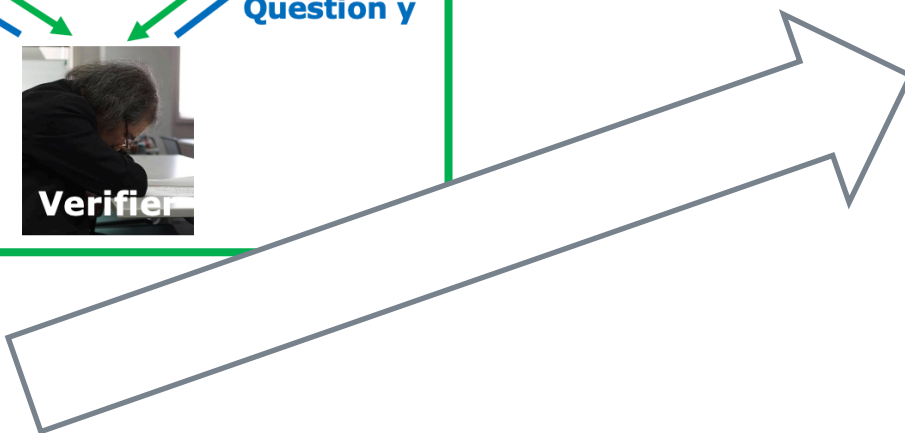
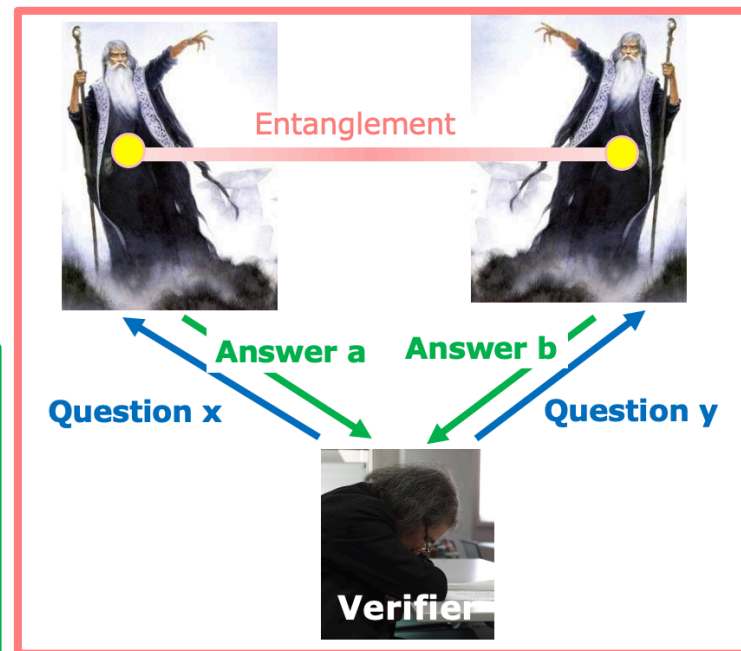
IP



MIP



MIP*



Interactive Proofの基本的達成

MIP*へ

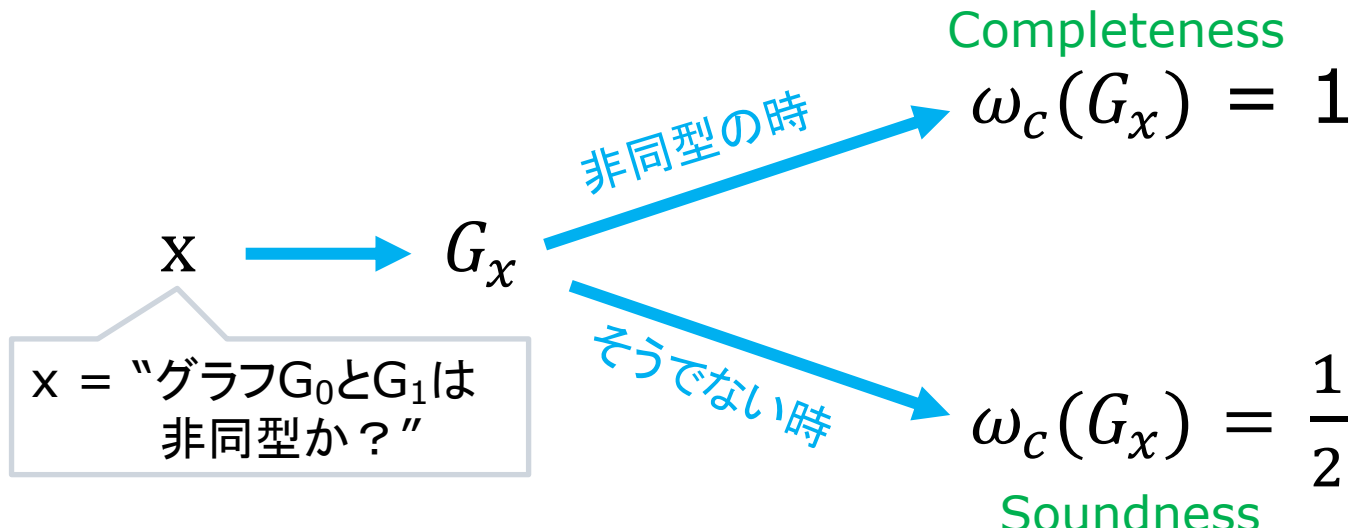
グラフの非同型問題

- 同じ頂点数 n を持つグラフ G_0 と G_1 ある時、この二つのグラフ G_0 と G_1 が同型でないことを決定する問題を考える。
- この問題が、NPに属するかは、非同型であることを多項式時間でチェックするアルゴリズムが与えられない限り、よくわからない。ここでは、次のようなIPのスタイルで、グラフの非同型問題を考えよう。
 1. グラフ G_0 と G_1 は、ProverにもVerifierにも与えられている。
 2. Verifierは、ランダムに0,1の値 i を選んで、 G_0 と G_1 のいずれかの G_i (i は、0または1)の頂点をスクランブルしたグラフ H をProverに送る。 G_i と H は同型である。
 3. Proverは、送られた H が、 G_0 から作られたものなら0を、 G_1 から作られたものなら1を、 j として返す。
 4. Verifierは、 $i=j$ なら受理し、そうでないならrejectする。

グラフの非同型問題

1986年 Goldreich, Micali, and Wigerson

- グラフ G_0 と G_1 が同型でないなら、Proverは、確実に、 H から j を導くことができる。Proverのパワーで、 H が G_0 と G_1 のどちらかに同型かを調べればいい。
- ただ、グラフ G_0 と G_1 が同型の場合、Proverは、確実に、 H から j を導くことができない。 H は G_0 とも G_1 とも同型だから。この時、ProverはVerifierに、ランダムに0か1を送ることになる。 $i=j$ である確率は $1/2$ になる。



IP=PSPACE

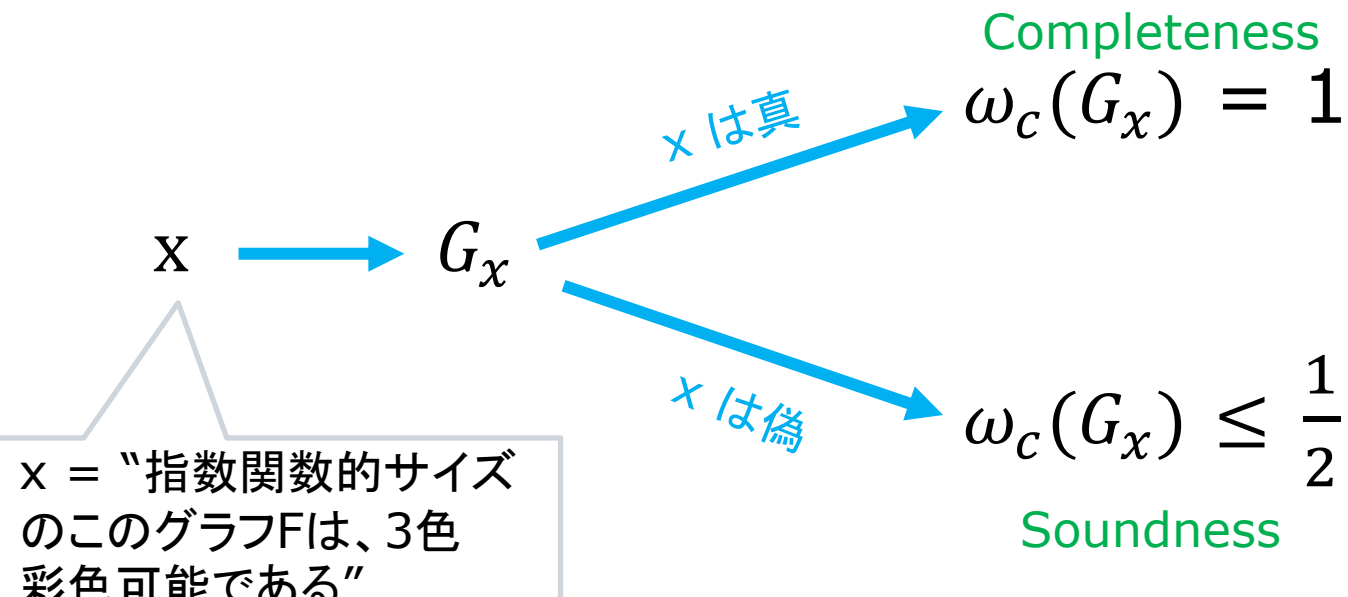
- IPの複雑性は、NPより大きい複雑性のクラス PSPACE に等しいことが、1990年 Shamir によって証明されている。**IP=PSPACE**である。

MIP = NEXP

Classical Multi Prover Interactive Proof

MIPでの重要な成果は、1991年のBabai, Fortnow, Lundによる、**MIP = NEXP** という認識である。

MIPは、C-GAP問題 古典値 $\omega_c(G)$ の近似問題に還元される。



PCP定理

- PCPは、Probabilistically checkable proof の意である。この定理は、NP問題は、「確率的に検証可能な証明」を持つことを主張している。もちろん、Interactive Proofのスタイルを使う。
- さまざまな定式化がある。1992年の、Arora-Lund-Motwani-Sudan-Szegedyの定式化では、
 $NP \subseteq PCP[\log n, 1]$ の形で述べられている。
- すなわち、 $\log n$ ビットの情報のやり取りで、固定数の箇所の証明をチェックするだけで証明の検証が可能だという、驚くべき内容の定理である。
- $MIP^* = RE$ の証明でも、この定理は大活躍する。

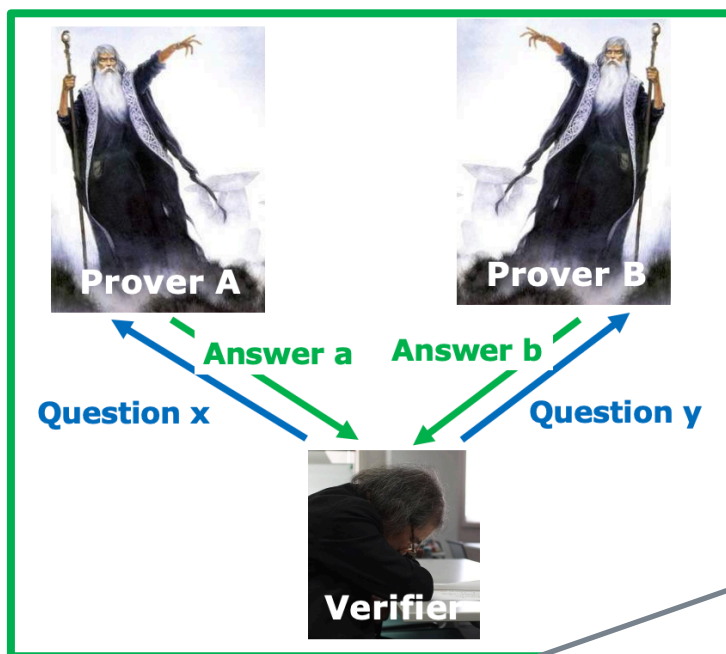
Interactive Proof の 基本的達成

1991年 Babai, Fortnow, Lund

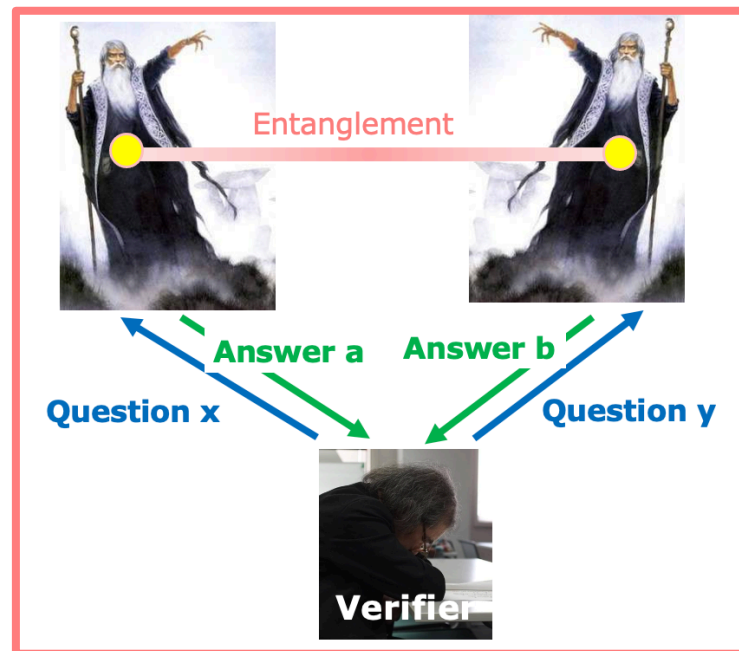
$$\text{MIP} = \text{NEXP}$$

1990年 Shamir

$$\text{IP} = \text{PSPACE}$$



$$\text{MIP}^* = \text{RE}$$



2020年 JNVWY

対応する複雑性のクラス

轉換2: 量子複雑性理論 確率と複雑性クラス

量子複雑性理論

- 1993年に、Bernstein と Vazirani は、これまでのTuringマシンの拡大である「量子Turingマシン」を新しく定義して、その上で複雑性理論を展開した。
- ここから始まったこの複雑性理論の新しい分野を「量子複雑性理論」と呼ぶ。量子複雑性理論は、現在の複雑性理論の中心分野である。



Umesh Vazirani

BQP

- ❑ 量子複雑性理論で最も基本的なクラスは、BQPである。それは、従来の複雑性理論での多項式時間で決定可能な複雑性のクラス P に相当するものである。
- ❑ ただし、量子Turingマシンの特性として、その出力は古典的なTuringマシンのように常に確定した値を返すのではなく、確率分布として与えられる。
- ❑ BQPは、“Bounded error, Quantum, Polynomial time”の略である。この Bounded error は、このマシンの出力の「誤り」が一定の確率（一般には $1/3$ を使う）以下であることを表している。
- ❑ その点では、BQPは古典的な複雑性理論でのBPP (bounded-error probabilistic polynomial time)によく似ている。

BPPの定義

□ **Denition. BPP** is the class of languages $L \subset \{0, 1\}^*$ for which there exists a Turing machine M and a polynomial q so that for inputs $x \in \{0, 1\}^n$, M terminate in at most $q(n)$ steps and

- if $x \in L$ then M accepts with probability $> 2/3$
- if $x \notin L$ then M accepts with probability $< 1/3$

The constants $1/3$ and $2/3$ aren't important; we can amplify to make the success probability as high as we want by running the program a bunch of times and taking the majority result.

BQPの定義

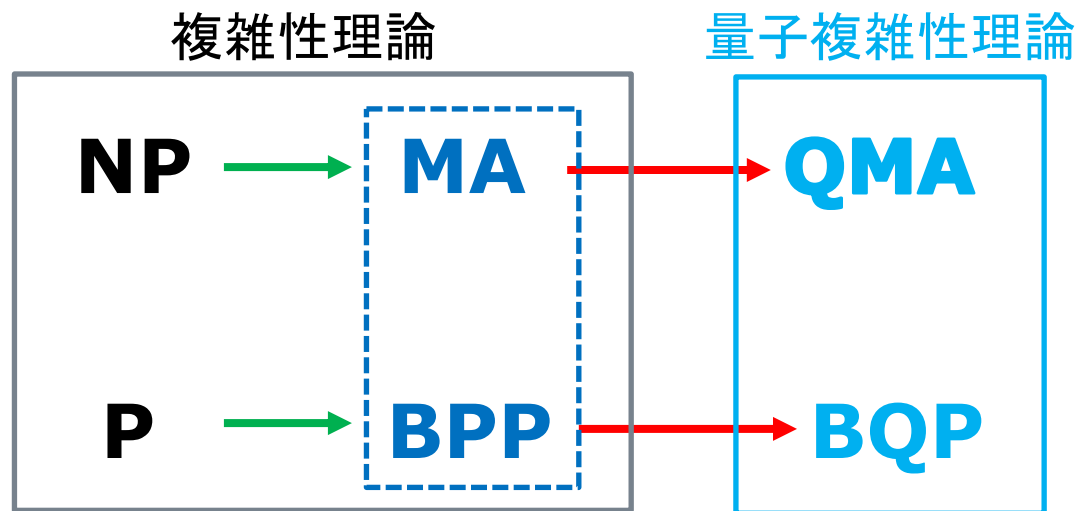
□ **Definition. BQP** is the class of languages $L \subseteq \{0,1\}^*$ for which there exists a uniform family of polynomial-size quantum circuits $\{C_n\}$ over some basis of universal gates and a polynomial q so that for all n and inputs $x \in \{0,1\}^n$

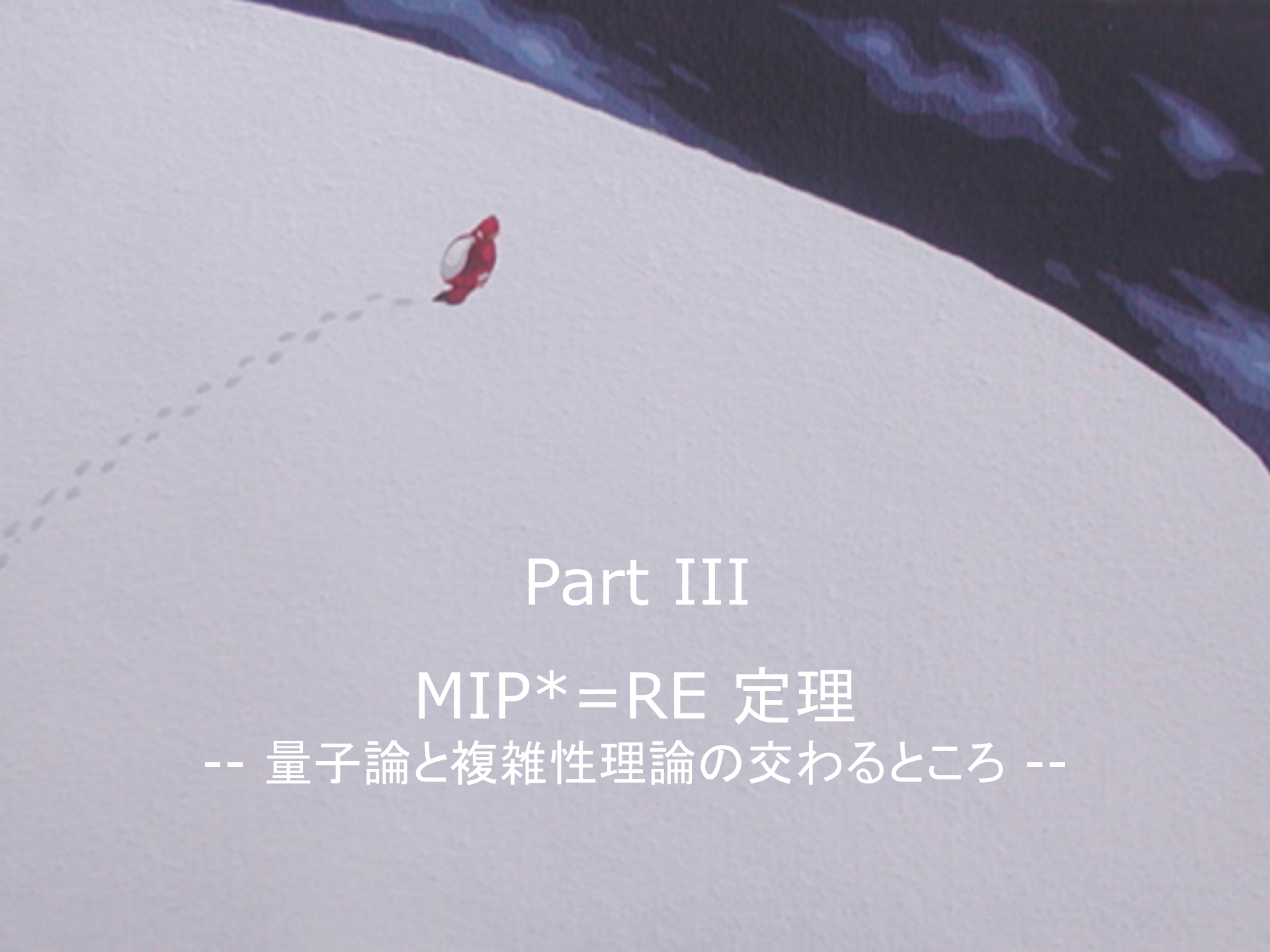
- if $x \in L$ then $C_n(|x\rangle |0\rangle^{\otimes q(n)})$ accepts with probability $> 2/3$
- if $x \notin L$ then $C_n(|x\rangle |0\rangle^{\otimes q(n)})$ accepts with probability $< 1/3$

Since circuits have to pre-specify the input size, so we need a circuit for each input size n . By uniform, we mean that there is a classically efficient algorithm to produce C_n given n .

BQPとQMA

- BQPとならんで、量子複雑性理論で基本的なクラスは、QMA (Quantum Merlin Arthur)である。それは、古典的な複雑性理論のNPクラスの量子版である。(正確にいうと、NPクラスの確率版であるMAクラスの量子版である)





Part III

$\text{MIP}^* = \text{RE}$ 定理

-- 量子論と複雑性理論の交わるところ --

Agenda Part III

MIP*=RE 定理 -- 量子論と複雑性理論の交わるところ

□ MIP*はどのようなクラスか？

- MIP*の複雑性=Q-GAPの複雑性
- $\text{MIP} \subseteq \text{MIP}^*$
- $\text{NEEXP} \subseteq \text{MIP}^*$

□ 量子的な相関の階層

- $\mathcal{C}_c \subseteq \mathcal{C}_q \subseteq \mathcal{C}_{qs} \subseteq \mathcal{C}_{qa} \subseteq \mathcal{C}_{qc}$
- Tsirelsonの問題: $\mathcal{C}_{qa} = \mathcal{C}_{qc}$
- Connes Embedding Conjecture = Tsirelsonの問題

□ Q-GAP計算のアルゴリズムとMIP*=RE の証明

MIP*はどのようなクラスか？

MIP*はどのようなクラスか？

- ある命題 X が、エンタングルした二人のProverとのInteractive Proofで検証されるというのは、次のような条件を満たすときである。
 1. X が真であるなら、Proverは高い確率で、Verifierに確信を与えることができないといけない。
この条件を **Completeness** と呼ぶ。
 2. X が偽であるなら、Verifierは高い確率で、それを拒否できないといけない。
この条件を **Soundness** と呼ぶ。
- MIP*は、エンタングルした二人のProverとのInteractive Proofで検証される解を持つ問題のクラスである。

MIP*の複雑性=Q-GAPの複雑性

「MIP*の複雑性とは何か？」という問題は、次の問題に関連している。「nonlocalゲームで、最適の戦略をとった時の勝率の最大値の近似を求めるアルゴリズムは存在するか？」

それは、第一部で見た nonlocalゲームGの $\omega_q(G)$ の近似を求めるアルゴリズムが存在するかという問題である。

Quantum Game Approximation Problem(**Q-GAP**)は、ゲームGが与えられた時、次のような α を求める問題である。

$$|\alpha - \omega_q(G)| \leq \frac{1}{10}$$

MIP*の複雑性は、Q-GAPに還元されることが知られている。

NP $\subseteq$ MP*

3SAT: ϕ は充足可能か？

Prover

a: 変数への値の割り当て

- Proverは、変数への値の割り当て aを送る
- Verifierは、aが ϕ を充足する時にかぎり受理する



Verifier

SATをエンコードした
nonlocal ゲーム

3SAT式

ϕ

G_ϕ

ϕ は充足される

$$\omega_q(G_\phi) = 1$$

ϕ は充足されない

$$\omega_q(G_\phi) = 0$$

Soundness

Q-GAP問題は、単純な問題ではない

3SATの場合のQ-GAPは、SATをエンコードしたnonlocalゲーム G_φ が与えられた時、次のような α を求める問題である。

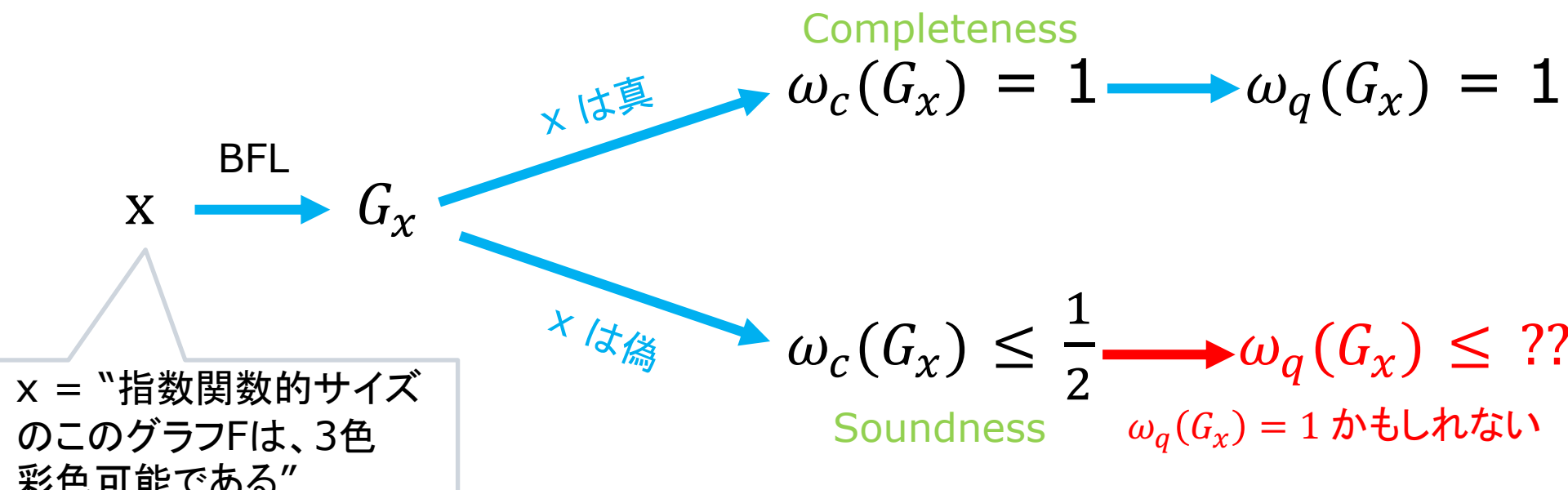
$$|\alpha - \omega_q(G_\varphi)| \leq \frac{1}{10}$$

この問題は、 φ が充足可能かを決定する問題に帰着する。

MIP $\subseteq$ MIP* ?

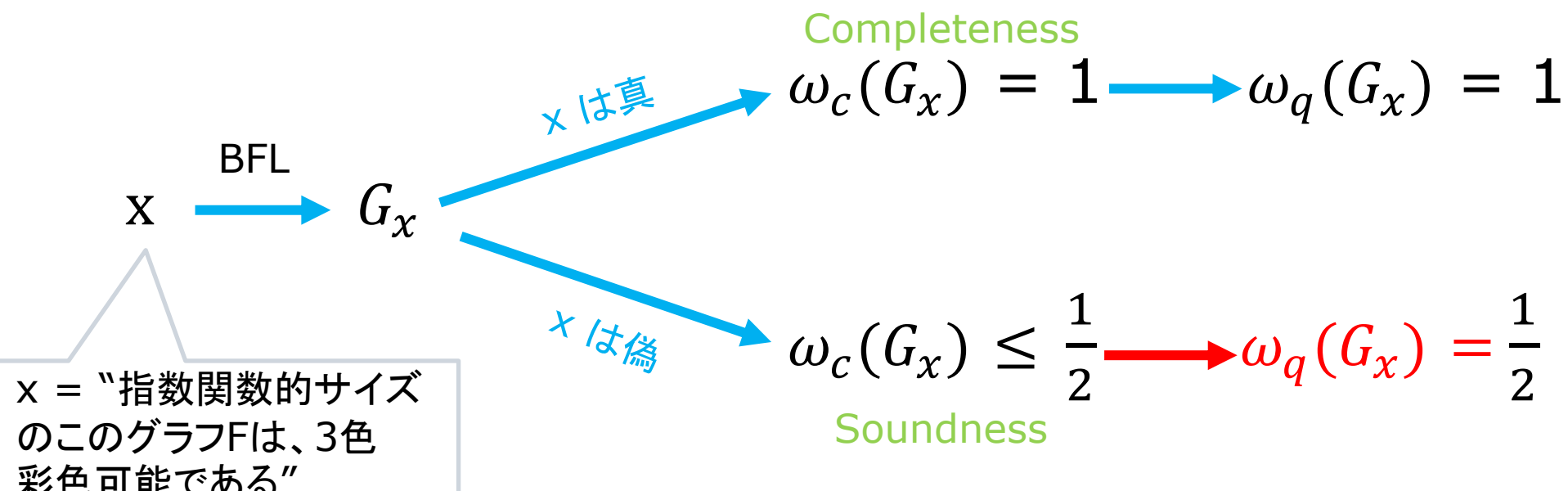
MIP $\subseteq$ MIP* かどうかは自明ではない。

エンタングルしてパワーアップしたProverは、その力をVerifierを欺くために利用する可能性がある。その場合、MIP*の証明能力は MIPより低くなるかもしれない。Soundnessは、保存されないかもしれない。



$$\text{MIP} \subseteq \text{MIP}^*$$

幸いこの問題は、2012年に Ito, Vidickによって解決された。彼らは、Babai, Fortnow, Lundが、 $\text{MIP} = \text{NEXP}$ を証明したのと同じ構成を用いて、 $\omega_q(G_x) \approx \omega_c(G_x)$ であることを示した。エンタングルメントは、MIPの複雑性を低下させないのである。



MIP*の上限は？

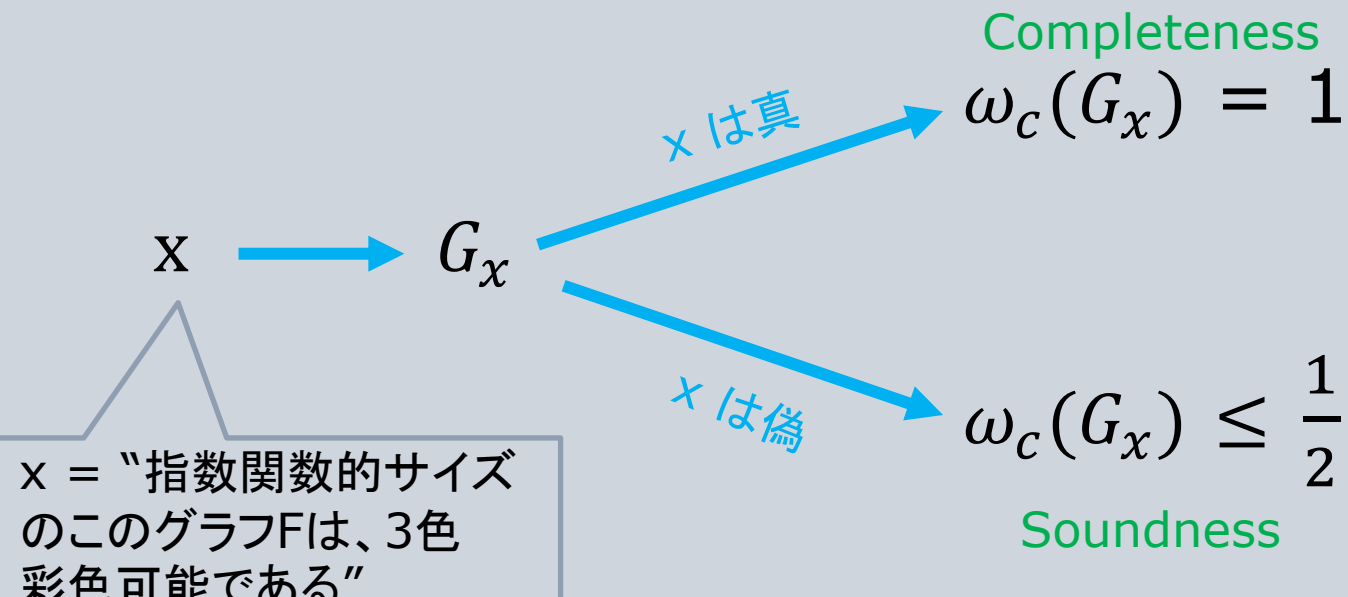
- Q-GAPを解くアルゴリズムは存在するか？
- C-GAPの場合の、トリビアルなアルゴリズムは、可能なProverの戦略を全て数え上げることである。
 - それは、Double-Exponential 2^{2^n} な時間で解ける。
だから、 $\text{MIP} \subseteq \text{DOUBLE-EXP}$ である。
- Q-GAPの場合には、可能な戦略の数え上げは難しい。
というのも、Proverの戦略は、利用するエンタングルする量子の数ごとに無限個あるから。
- 基本的な障害は、最適な戦略を選ぶためのエンタングルした量子の数の上限がわからないことである。

MIP = NEXP

Classical Multi Prover Interactive Proof

MIP*が、Q-GAP問題に還元されるように、
MIPは、C-GAP問題 古典値 $\omega_c(G)$ の近似問題に還元される。

MIPでの重要な成果は、1991年のBabai, Fortnow, Lund
による、**MIP = NEXP** という認識である。



NEEXP $\subseteq$ MIP*

- 2019年、Anand Natarajan と John Wrightは、**NEEXP $\subseteq$ MIP*** を証明した。
NEEXPは、nondeterministic doubly exponential time の意で、ある命題が正しいことの検証に、 2^{2^n} 時間を必要とする複雑性のクラスである。
- これは、古典的なInteractive Proofでの、Babai, Fortnow, Lundによる、**MIP = NEXP** に対応した成果で、エンタングルしたProverは、古典的なProverより、指数関数的に大きなパワーを持つことを示している。
- 彼らが、この証明で用いた手法 **Introspection**は、翌2020年のMIP* = REの証明に直接、引き継がれていく。

NEEXP $\subseteq$ MIP* からみる MIP* = RE 証明

Introspection とゲームの圧縮(**compression**)の手法を、繰り返し利用すると、次のような関係を証明できる。

RE $\subseteq$ MIP* ?

NP $\subseteq$ MIP* (自明)

NEXP $\subseteq$ MIP* ('91 BFL)

NEEXP $\subseteq$ MIP* ('19 Anand , Vidick)

NEEEXP $\subseteq$ MIP*

NEEEEXP $\subseteq$ MIP*

NEEEEEEXP $\subseteq$ MIP*

NEEEEEEEEXP $\subseteq$ MIP*

...

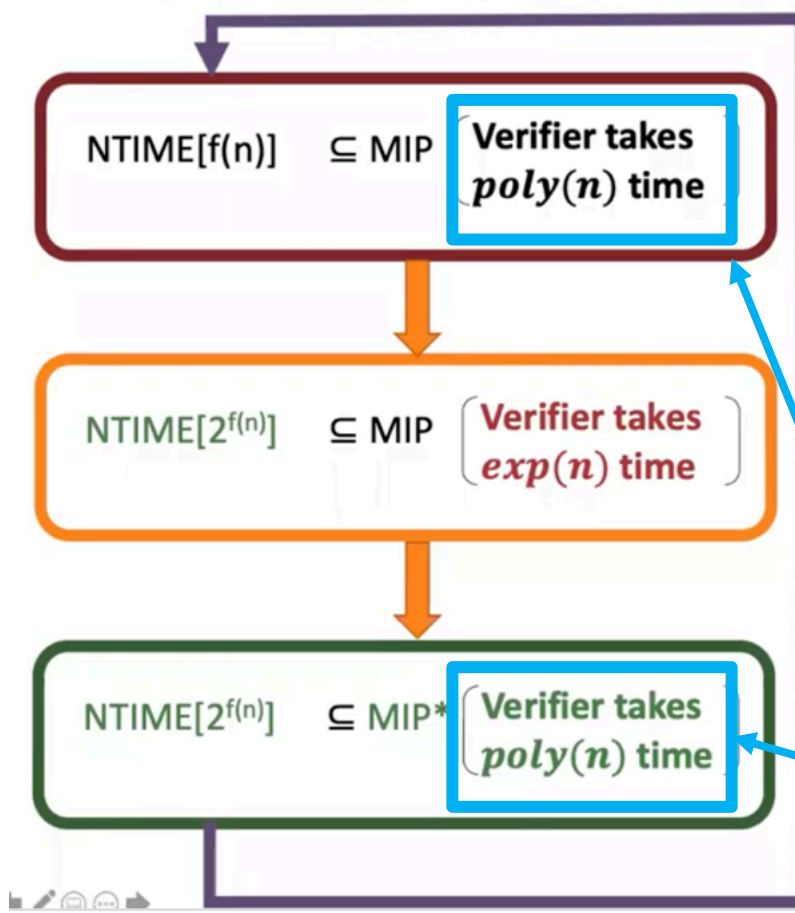
RE $\subseteq$ MIP*

$2^{2^{2^{\dots}}}$

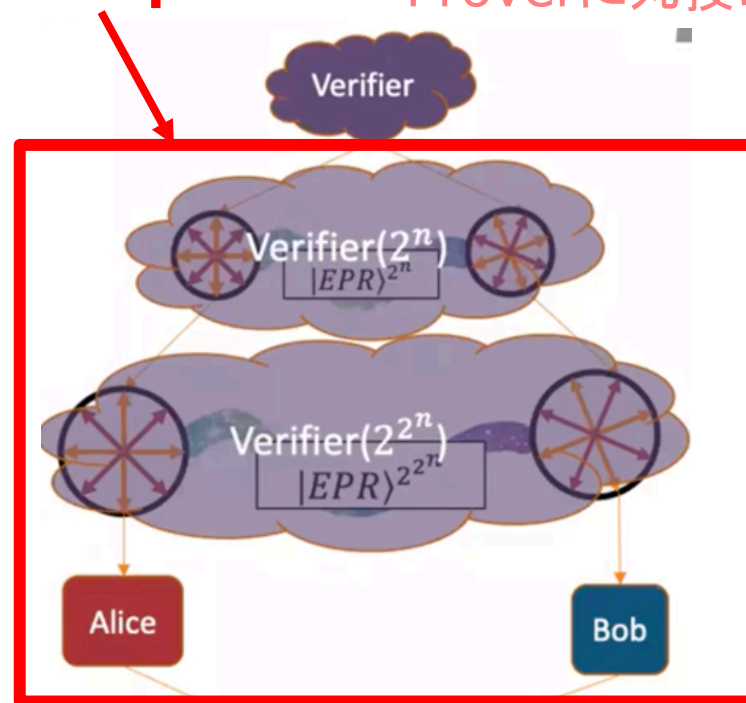
IntrospectionとCompressionのイメージ

NEEEXP $\subseteq$ MIP* の場合

圧縮を繰り返す



Introspection Verifierの仕事を Proverに丸投げ



多項式時間に
圧縮されている

NEEEXP $\subseteq$ MIP*

量子的な相関の階層

ゲームの定式化

それぞれのゲームは、次の三つの式で特徴付けられる。

1. 質問の分布: $\mu(x, y)$
2. 質問と回答の相関: $p(a, b \mid x, y)$
入力 x, y が与えられた時 a, b を出力する、条件付き確率である
3. ゲームの勝敗を定義する関数: $D(a, b, x, y) \rightarrow \{0, 1\}$

CHSHゲームの場合、

- $\mu(x, y)$ は、0と1の一樣にランダムな分布、
- $p(a, b \mid x, y)$
 $= p(a, b \mid 0, 0) + p(a, b \mid 0, 1) + p(a, b \mid 1, 0) + p(a, b \mid 1, 1)$ 、
- $D(a, b, x, y)$ は、
 $a + b = xy \pmod{2}$ の時に1を、それ以外の時に0を返す関数である。

相関 p が与えられた時のゲームの勝率

相関 p が与えられたときのゲーム G の勝率 $\omega(G, p)$ は、次の式で与えられる。

$$\omega(G, p) = \sum_{x,y,a,b} \mu(x, y) \cdot D(x, y, a, b) \cdot p(a, b|x, y)$$

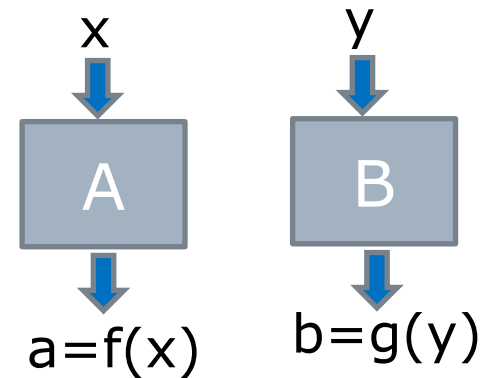
古典論的なCHSHと、エンタングルメントを利用したCHSHとの違いは、相関 p が古典論的相関に属するか $p \in C_c$ 、量子論的相関に属するか $p \in C_q$ の違いに帰着する。

どのような相関を選択するかで勝率は変わる。こうして選択された相関をゲームの「戦略」という。

古典論的相関 C_c

古典論では、相関 $p(a, b|x, y)$ は、0か1の値しか取らない。

すなわち、 n bitの入力に対して k bitの出力を返す関数 $f, g: [n] \rightarrow [k]$ が存在して、 $a=f(x)$, $b=g(y)$ である時、



$p(a, b|x, y) = 1$, それ以外の場合には $p(a, b|x, y) = 0$ となる。

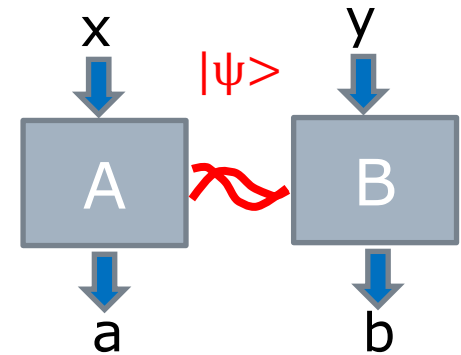
古典論的相関 $C_c: p(a, b|x, y)$ は、 $a=f(x)$, $b=g(y)$ である関数 f, g によって決定論的に特徴付けられる。

量子論的相関 C_q

量子論では、相関 $p(a, b|x, y)$ は、確率を返す。

A, Bの状態を表す有限次元のヒルベルト空間を $\mathcal{H}_A, \mathcal{H}_B$ とし、それぞれに作用して観測を行う演算子を $\{A_a^x\}_{\mathcal{H}_A}, \{B_b^y\}_{\mathcal{H}_B}$ とする。

二つの異なる空間を一つの空間とみなすには、そのテンソル積を考えればいい。 $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ なる状態 $|\psi\rangle$ を観測した時に得られる相関 量子論的相関 C_q は、次の式で表される。



$$C_q: p(a, b|x, y) = \langle \psi | A_a^x \otimes B_b^y | \psi \rangle$$

射影演算子 $P_k = |k\rangle\langle k|$ と観測の確率

$P_k = |k\rangle\langle k|$ の時、 $\langle\psi|P_k|\psi\rangle$ を計算する。

$$|\psi\rangle = \sum_i c_i |i\rangle, \langle\psi| = \sum_j \langle j| c_j^*$$

$$\begin{aligned}\langle\psi|P_k|\psi\rangle &= \langle\psi|k\rangle\langle k|\psi\rangle \\ &= \sum_j \langle j| c_j^* |k\rangle\langle k| \sum_i c_i |i\rangle \\ &= \sum_{i,j} c_j^* c_i \boxed{\langle j|k\rangle\langle k|i\rangle} \\ &= c_k^* c_k = |c_k|^2\end{aligned}$$

よって、 $|\psi\rangle$ を観測して、状態 $|k\rangle$ が観測される確率は、
 $\langle\psi|P_k|\psi\rangle$ である。

量子論的相関 C_{qs} と C_{qa}

量子論的相関 C_q は、有限次元のヒルベルト空間のテンソル積で構成される空間上の相関である。

これを無限次元にまで拡張したものを C_{qs} で表す。ここでのqsのsは、**spatial** の意味を持つ。空間的には別々の空間をテンソル積で一つにまとめた空間を考えているからである。

さらに、すべての C_q をあわせたもののクロージャを考え、それを C_{qa} で表す。有限次元のテンソル積のクロージャである。

定義から、 $C_q \subseteq C_{qs} \subseteq C_{qa}$ である。

もう一つの量子論的相関 C_{qc}

場の量子論では、一つのヒルベルト空間 $\mathcal{H}$ しか扱わない。
状態 $|\psi\rangle \in \mathcal{H}$ を二人の観測者A, Bが行った観測 $\{A_a^x\}_{\mathcal{H}}, \{B_b^y\}_{\mathcal{H}}$ が
産み出す相関を C_{qc} で表す。この時、この相関は、次の式で表される。

$$C_{qc}: p(a, b|x, y) = \langle \psi | A_a^x \cdot B_b^y | \psi \rangle$$

この時、 $[A_a^x, B_b^y] = 0$ である。

すなわち、 A_a^x, B_b^y は可換で、どちらの観測が先に行われても、
同じ相関が産み出される。添字のqcは、quantum commuting
の意味である。

$$C_q \subseteq C_{qs} \subseteq C_{qa} \subseteq C_{qc}$$

Tsirelsonの問題

$$C_{qa} = C_{qc} ?$$

Tsirelsonの問題とは C_{qa} が C_{qc} と等しいか否かという問題である。

$$C_c \subseteq C_q \subseteq C_{qs} \subseteq C_{qa} \subseteq C_{qc}$$

という階層の中で、次の結果は既に知られていた。

$$C_c \subsetneq C_q \subsetneq C_{qs} \subsetneq C_{qa} \subseteq C_{qc}$$

$C_c \neq C_q$: 1964年 Bell

$C_{qs} \neq C_{qa}$: 2017年 Slofstra

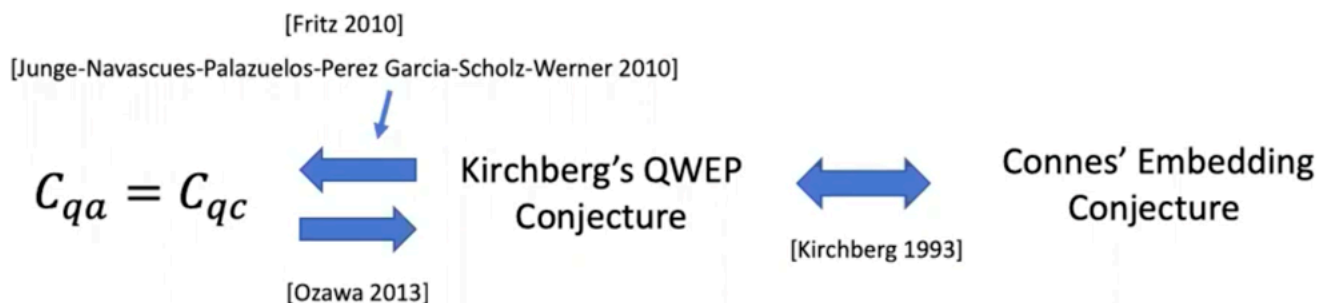
$C_q \neq C_{qs}$: 2018年 Coladangelo and Stark

$$C_c \subseteq C_q \subseteq C_{qs} \subseteq C_{qa} \subseteq C_{qc}$$

Connes Embedding Conjecture (CEC) と Tsirelson 問題

1976年 Alain Connes

“We now construct an embedding of N into R . Apparently such an embedding ought to exist for all II_1 factors.”



2013年 Tsirelson問題の $C_{qa} = C_{qc}$ は、CECと同値であることが証明された。

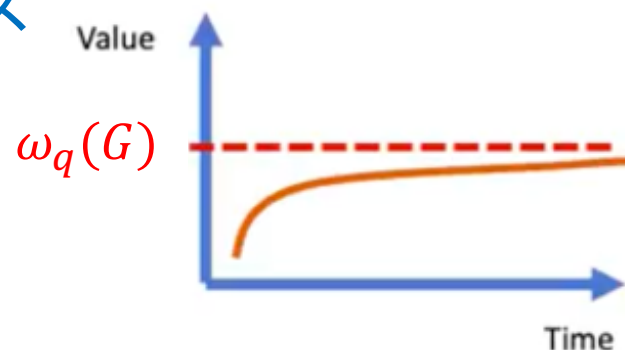
Q-GAP計算のアルゴリズムと $MIP^* = RE$ の証明

$C_{qa} = C_{qc}$ (あるいはCEC)を仮定すると、
Q-GAP を計算するアルゴリズムが見つかる

下から $\omega_q(G)$ に近づく次のようなシーケンス
を計算するアルゴリズムが存在する。

$$\alpha_1 \leq \alpha_2 \leq \alpha_3 \leq \cdots \leq \omega_q(G)$$

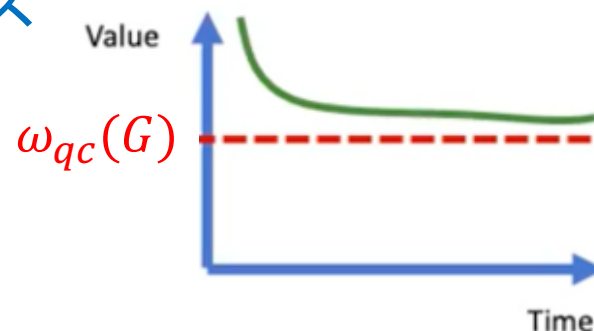
$d \rightarrow \infty$ の時、 $\alpha_d \rightarrow \omega_q(G)$



上から $\omega_{qc}(G)$ に近づく次のようなシーケンス
を計算するアルゴリズムが存在する。

$$\beta_1 \geq \beta_2 \geq \beta_3 \geq \cdots \geq \omega_{qc}(G)$$

$d \rightarrow \infty$ の時、 $\beta_d \rightarrow \omega_{qc}(G)$

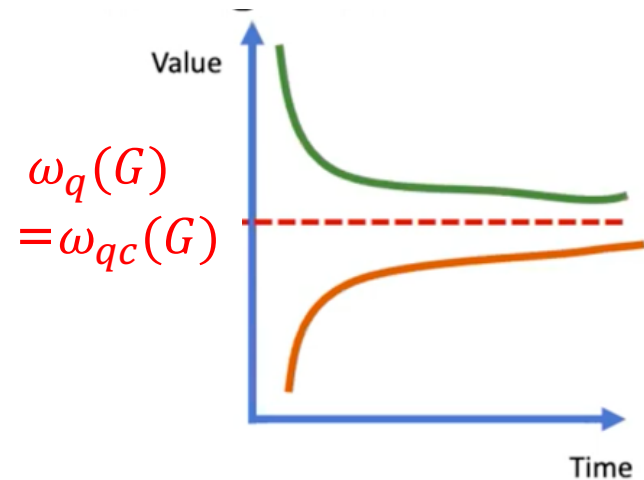


$C_{qa} = C_{qc}$ (あるいはCEC)を仮定すると、
Q-GAP を計算するアルゴリズムが見つかる

$C_{qa} = C_{qc}$ (あるいはCEC)を仮定すると、
二つの曲線は、 $\omega_q(G)$ に収束するので、
次のようなアルゴリズムで、Q-GAPを計算
することができる。

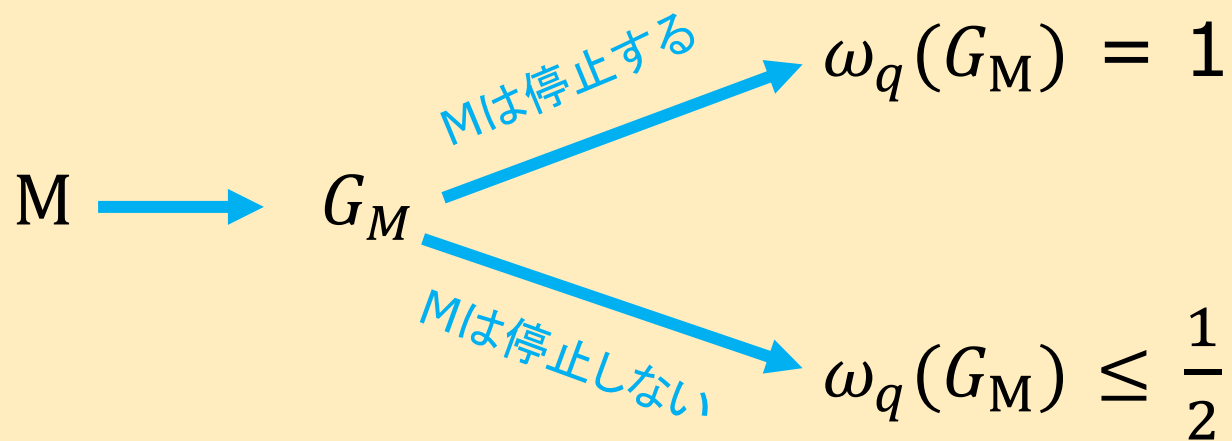
$d = 1, 2, 3, \dots$ について

1. α_d を計算する
2. β_d を計算する
3. $\beta_d - \alpha_d < \varepsilon$ なら β_d を出力する。



$$\text{MIP}^* = \text{RE}$$

チューリングマシン M に対して、 M から次のような nonlocal ゲーム G_M への変換が存在する。



この証明の含意

- 我々は $C_{qa} = C_{qc}$ を仮定して、チューリングマシンをnonlocal ゲーム G_M に変換したのだが、この G_M はチューリングマシンの「停止問題」が、MIP*では解けることを主張している。これは不可能である。
- 任意の ε について、 $\omega_q(G)$ の近似解 $\omega_q(G) \pm \varepsilon$ である Q-GAP を求めるアルゴリズムは存在しない。
- 特に、上からの近似/下からの近似のアルゴリズムは、全ての G については収束しない。こうして、 $\omega_q(G) \neq \omega_{qc}(G)$ である G が存在する。
- このことは、 $C_{qa} \neq C_{qc}$ と、Tsirelsonの問題の否定を意味する。
- よって、Connes予想は、否定される。

