エンタングルする認識
-- MIP*=REへ --

4/10 マルゼミ「楽しい哲学」

はじめに

先のセミナー「エンタングルする自然」では、21世紀の自然観の中核に「エンタングルする自然」という自然観が生まれていることを紹介しました。今回のセミナー「エンタングルする認識」は、こうした自然観を我々がどのように形成・獲得してきたかをみようとしたものです。

「自然の認識」は、「自然」と「認識」という二つの項からできています。ただ、その二つの項はまったく切り離された別々のものではありません。「自然」が新しい相貌の下に立ち現れ始めたということは、「認識」の飛躍が起きつつあるということに他なりません。それは、人間が新しい認識のスタイルを獲得しつつあることを意味します。

はじめに

筆者は、エンタングルメントの認識が、現時点での人間の認識能力の飛躍の中心舞台だと考えています。

小論は、こうした進行中の転換を、1964年のベルの定理（第一部）、1985-6年の対話型証明の登場（第二部）、そして2020年のMIP*＝RE定理（第四部）の三つのトピックを中心に概観したものです。

これらは、1930年代のアインシュタイン、チューリング、フォン・ノイマンの仕事に淵源するものです。

数学

1932年

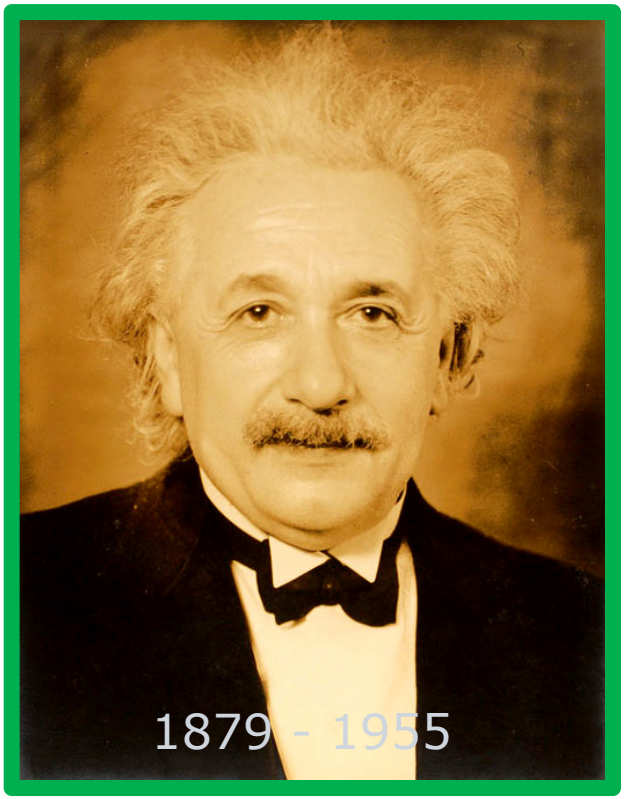
フォン・ノイマン

量子力学の
数学的形式化

量子力学

1935年

アインシュタイン



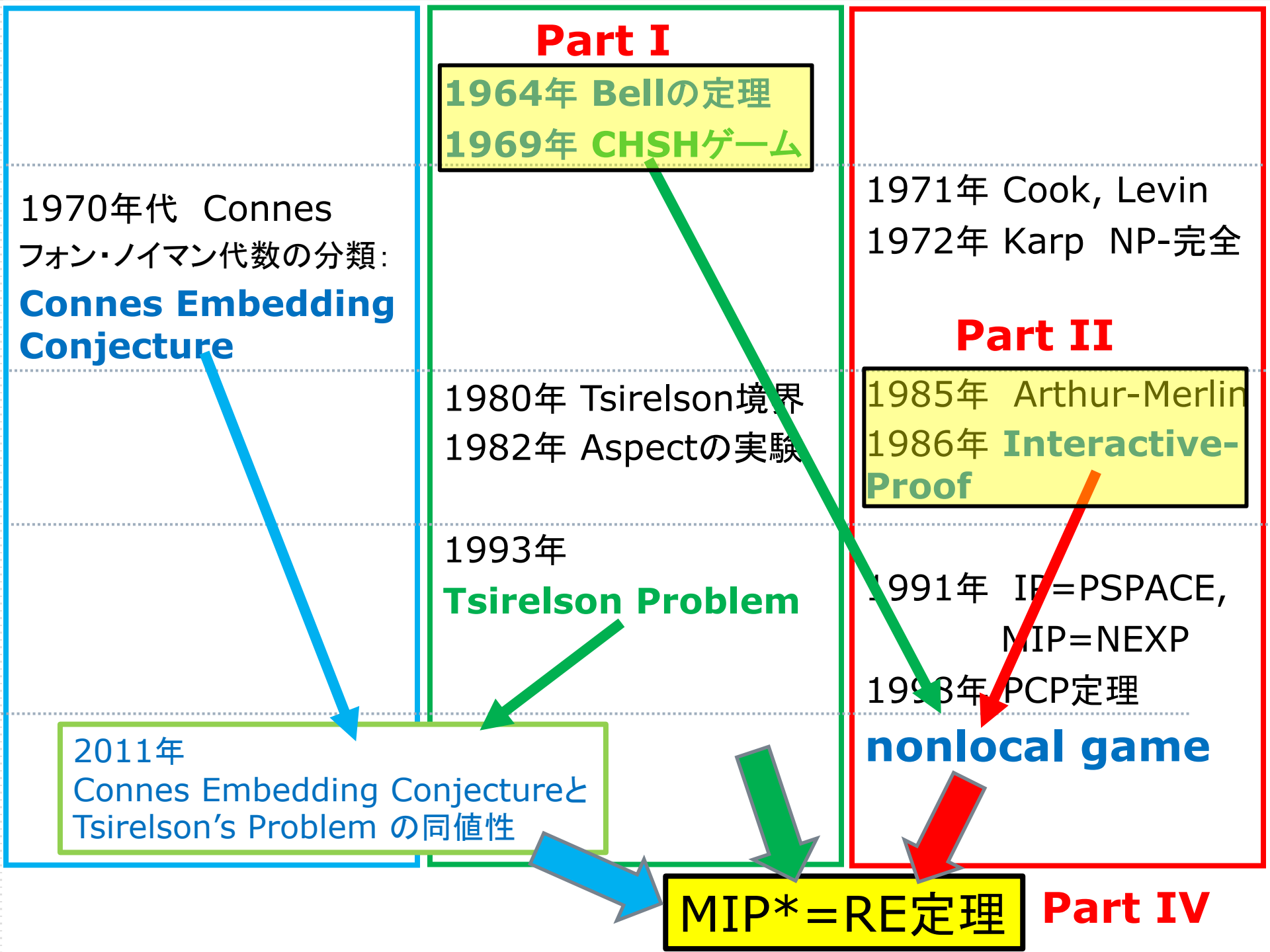
エンタングルメント
EPR状態の発見

計算科学

1936年

チューリング

「停止問題」の
決定不能性の証明


Part I
1964年 Bellの定理
1969年 CHSHゲーム
1970年代 Connes
フォン・ノイマン代数の分類:
Connes Embedding Conjecture
1980年 Tsirelson境界
1982年 Aspectの実験
1993年
Tsirelson Problem
1971年 Cook, Levin
1972年 Karp NP-完全
Part II
1985年 Arthur-Merlin
1986年 Interactive-Proof
1991年 IP=PSPACE,
MIP=NEXP
1998年 PCP定理
nonlocal game
2011年
Connes Embedding Conjectureと
Tsirelson's Problem の同値性
MIP*=RE定理
Part IV

はじめに

量子コンピュター（第三部）のトピックは、「自然」と「人間の認識」という二項のコンテキストからではなく、「自然と人間と機械」という三項の関係として捉えるのがいいと考えているのですが、あまり展開できていません。

（このあたりの問題については、機械の利用と認識能力の拡大を扱った次のショートムービーをご覧ください。
https://youtu.be/j8flZDzL6yA?list=PLQIrJ0f9gMcMlJbm6pdZKdXwrzWSGyeqL ）

はじめに

認識の「飛躍」と言いましたが、大きな飛躍には、歴史的に先行するやはり大きな飛躍があります。興味深いのは、歴史的飛躍を行った発見者自身（例えばアインシュタイン）でさえ、その飛躍がその後の歴史的飛躍の中で果たす役割を予見できないことがあるということです。その役割と意味は、現在から過去を見るときに、はっきりと浮かび上がります。

「ミネルバのフクロウは黄昏に飛び立つ」

自然科学は、自然の哲学から分離・発展したものですが、科学への「哲学的」アプローチも、少なくとも過去から現在の到達点をオーバービューするのには、意味があるのではと考えています。

Agenda

エンタングルする認識 — MIP*=REへ

Part I

エンタングルメントの実在の認識 -- CHSHゲーム

Part II

「全能者」との対話で得られる認識 -- Interactive Proof

Part III

量子コンピュータの能力の認識 -- BQPクラス

Part IV

「エンタングルする知性」の認識 -- MIP*=RE

Agenda Part I

エンタングルメントの実在の認識
-- CHSHゲーム --

- エンタングルメントをめぐるドラマ
- エンタングルメントの認識の難しさ --「局所性」について
- エンタングルメントの実在性の認識 -- Bellのアプローチ
- CHSHゲーム
  - CHSHゲームの概要
  - CHSHゲームの定式化
  - 古典論的相関と量子論的相関のもとでの CHSHゲームの最大勝率

Agenda Part II

「全能者」との対話で得られる認識
-- Interactive Proof --

- 数学的証明をめぐるいくつかのエピソード
  - 証明の難しさ
  - 数学の証明へのコンピューターの利用
  - Voevodskyの問題提起
- 新しい証明のスタイル -- 対話型証明の想定
- グラフの「同型問題」と「非同型問題」
  - グラフの「同じ」を考える
  - グラフの同型性チェックのために必要な場合の数
  - Graph Isomorphismの複雑性クラス
- 対話型証明の最初の成功
- 対話型証明の発展
- 新しい数学的証明観の登場

Agenda Part III

量子コンピュータの能力の認識
-- BQPクラス --

- 量子コンピュータ研究の始まりと量子複雑性理論の誕生
  - 量子コンピュータ研究の始まり
  - 量子複雑性理論の誕生
  - Shorの発見
- 基本的な複雑性クラスのまとめ
- 量子優越性とは何か
  - ファインマン
  - プレスキル
- Googleはどんな実験をしたのか？
- 実験の評価

Agenda Part IV

「エンタングルする知性」の認識

-- MIP*=RE --

- 量子の力を借りた人間の認識能力拡大への期待
  - 量子コンピュータとNP-完全問題
  - 量子の力を借りた人間の認識能力の拡大の試み
  - MP* = エンタングルした「全能者」
- MIP*=RE定理とは何か？
- nonlocal game と Interactive Proof
  - nonlocal ゲームは、Interactive Proofである
  - Interactive Proofは、nonlocal ゲームである
- MIP*はどのようなクラスか？
- MIP*=REの認識論的含意

Part I

エンタングルメントの実在の認識
-- CHSHゲーム --

4/10 マルゼミ「楽しい哲学」

Agenda Part I

エンタングルメントの実在の認識
-- CHSHゲーム --

- エンタングルメントをめぐるドラマ
- エンタングルメントの認識の難しさ --「局所性」について
- エンタングルメントの実在性の認識 -- Bellのアプローチ
- CHSHゲーム
  - CHSHゲームの概要
  - CHSHゲームの定式化
  - 古典論的相関と量子論的相関のもとでの CHSHゲームの最大勝率

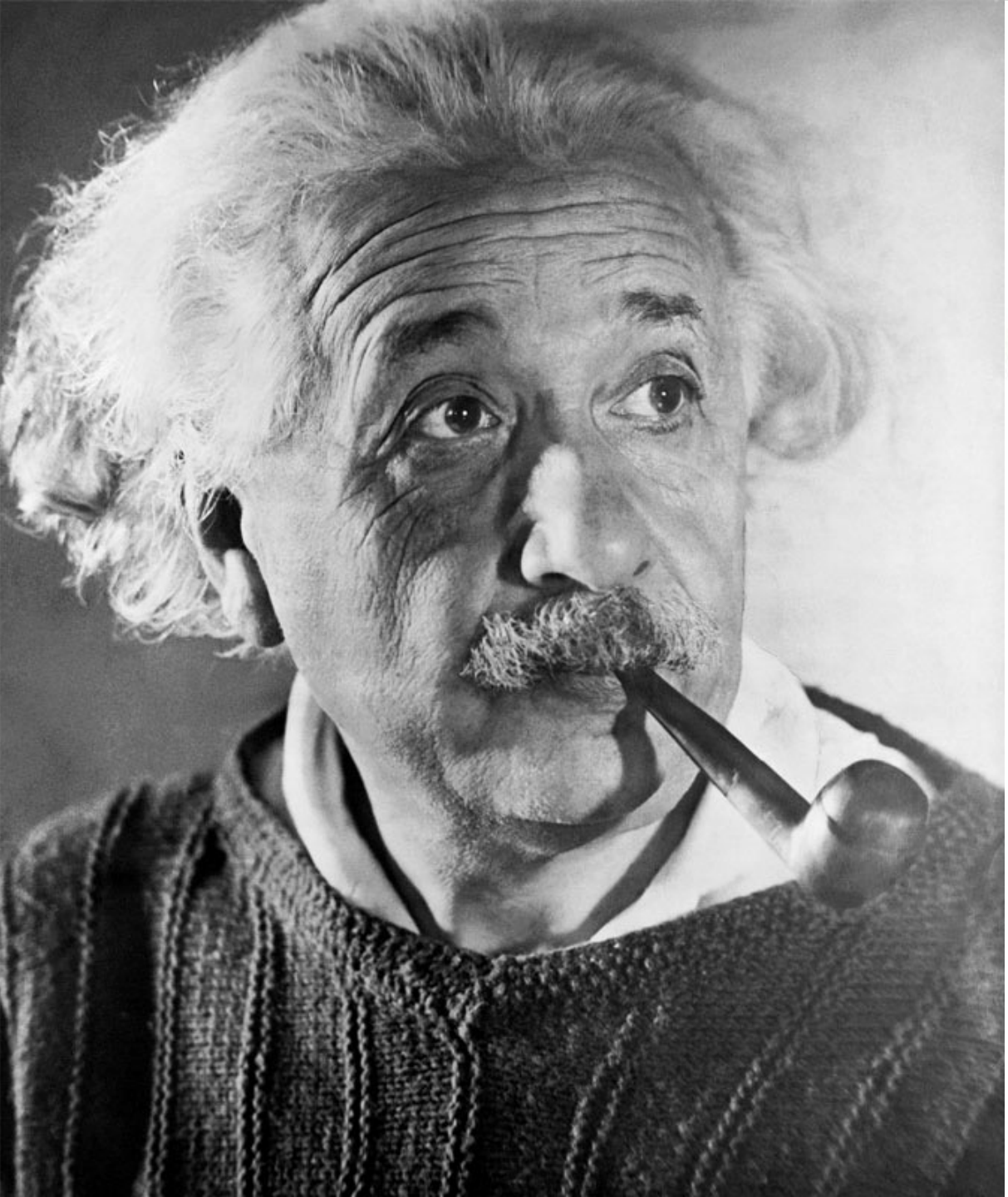
エンタングルメントをめぐるドラマ

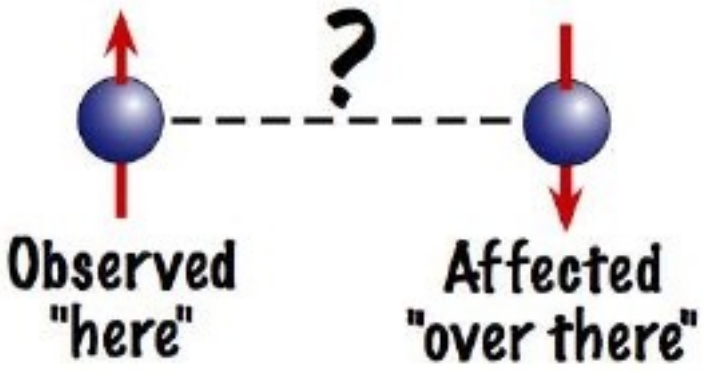
エンタングルメント
もつれあった二つの量子の状態の発見

1935年に、アインシュタインとポドルスキーとローゼンは、次の論文を発表します。（三人の著者の頭文字をとって、EPR論文と呼ばれます。）

"Can Quantum-Mechanical Description of Physical Reality Be Considered Complete ?"「物理的な実在の量子力学の記述は、完全なものと考えることができるか？」 https://goo.gl/qAWacP

この論文で、アインシュタインは、量子論では、二つの量子の「もつれあい」の状態が現れることを指摘します。





1935年

EPRの逆理

Einstein,
Podolsky,
Rosen

EPR論文を報ずる1935年のニューヨークタイムズ紙

EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

1964年：ベルによる「隠れた変数論」の否定と1982年：エンタングルメントの存在の確認

事態が動くのは、アインシュタインのエンタングルメントの発見から30年近くたった1964年のことでした。

彼は、アインシュタインらが量子論の不完全さを解決するものとして推進した「隠れた変数」理論を、理論的に否定することに成功します。

しかも、自然が、「隠れた変数」理論という古典論に従うか、あるいはエンタングルメントを含む量子論に従うかは、実験的に検証できると指摘します。

その後、Bellの主張は、1982年　Aspectによって実験的に実証されることになります。

ここに、量子論の正しさと、エンタングルメントの実在性は、理論的にも実験的にも確認されます。

1964年　Bellの定理
アインシュタインの「隠れた変数」の否定

ON THE EINSTEIN PODOLSKY ROSEN PARADOX*

J. S. BELL†
Department of Physics, University of Wisconsin, Madison, Wisconsin

(*Received* 4 *November* 1964)

I. Introduction

THE paradox of Einstein, Podolsky and Rosen [1] was advanced as an argument that quantum mechanics could not be a complete theory but should be supplemented by additional variables. These additional variables were to restore to the theory causality and locality [2]. In this note that idea will be formulated mathematically and shown to be incompatible with the statistical predictions of quantum mechanics. It is the requirement of locality, or more precisely that the result of a measurement on one system be unaffected by operations on a distant system with which it has interacted in the past, that creates the essential difficulty. There have been attempts [3] to show that even without such a separability or locality requirement no "hidden variable" interpretation of quantum mechanics is possible. These attempts have been examined elsewhere [4] and found wanting. Moreover, a hidden variable interpretation of elementary quantum theory [5] has been explicitly constructed. That particular interpretation has indeed a grossly nonlocal structure. This is characteristic, according to the result to be proved here, of any such theory which reproduces exactly the quantum mechanical predictions.

https://goo.gl/wyvd7B

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

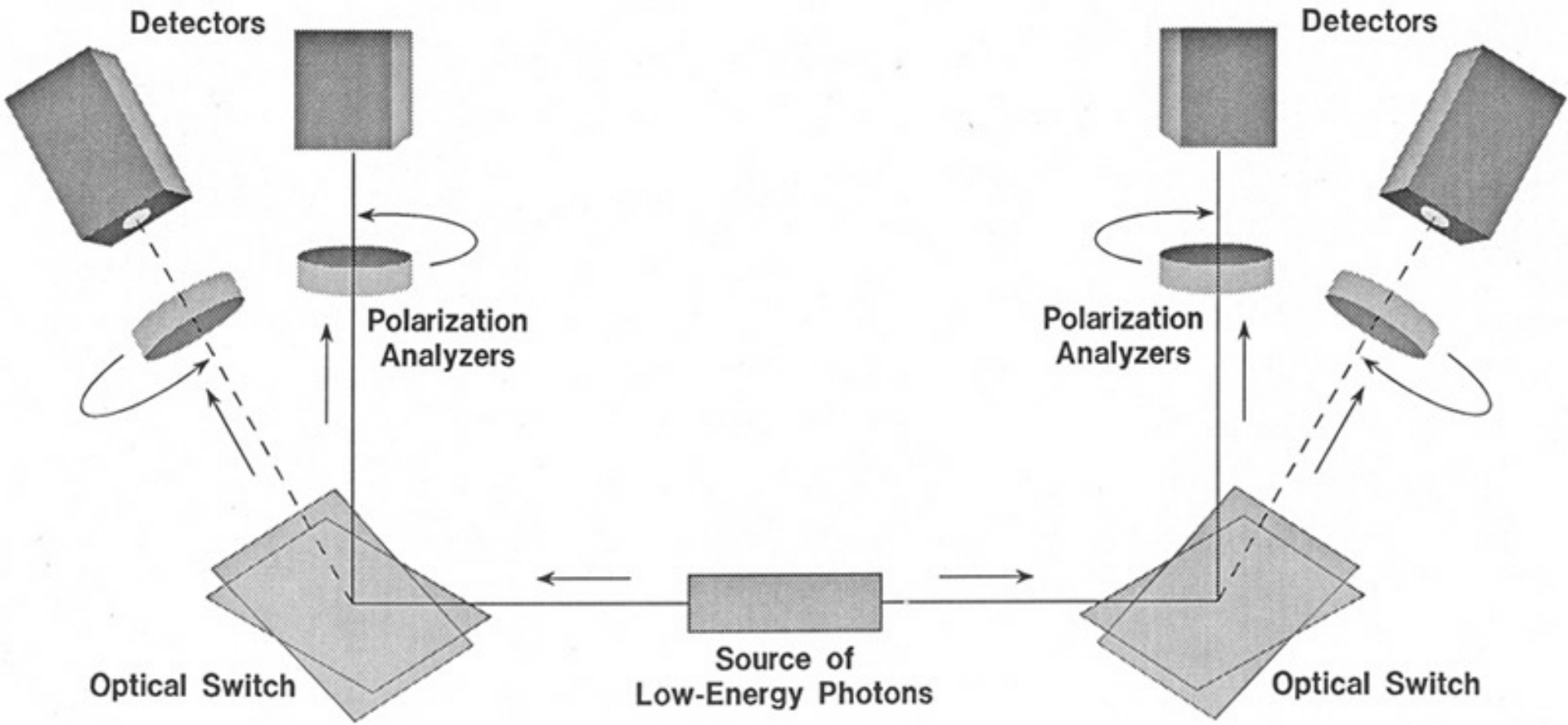
量子論的観測は、この不等式を破ることが、理論的に証明できる。

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。

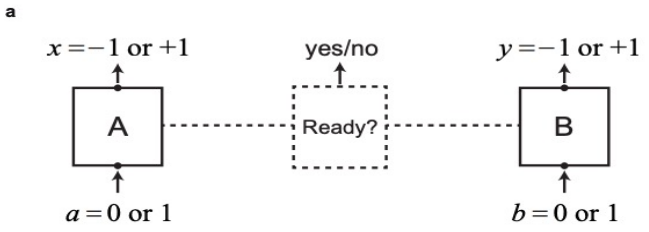
1964年
ベルの定理

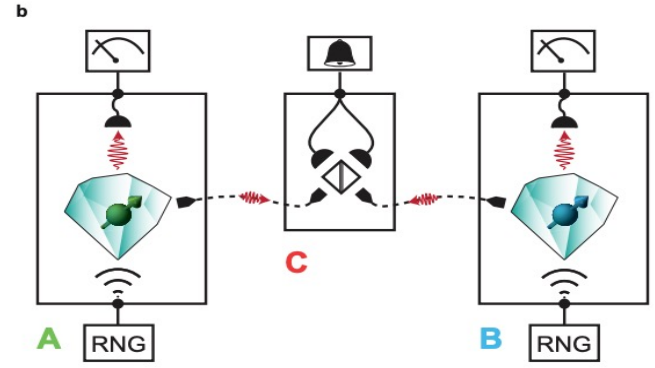
1982年　Aspectの実験

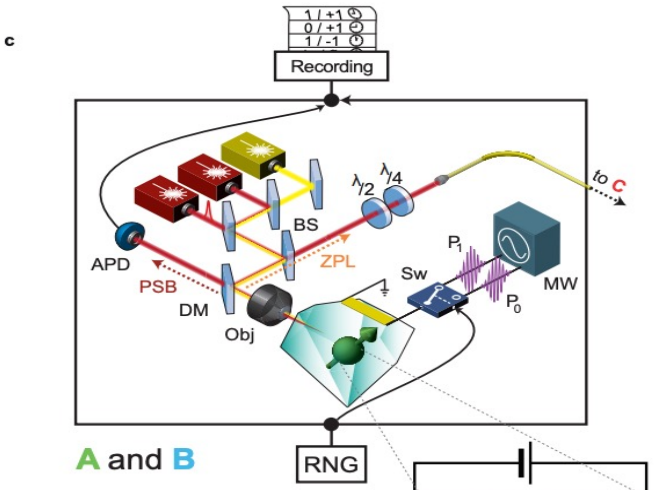


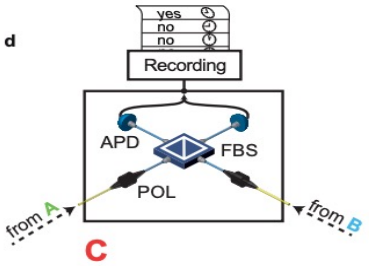
Bellの定理が成り立っていることの実験での確認

2015年 Delft University での実験









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

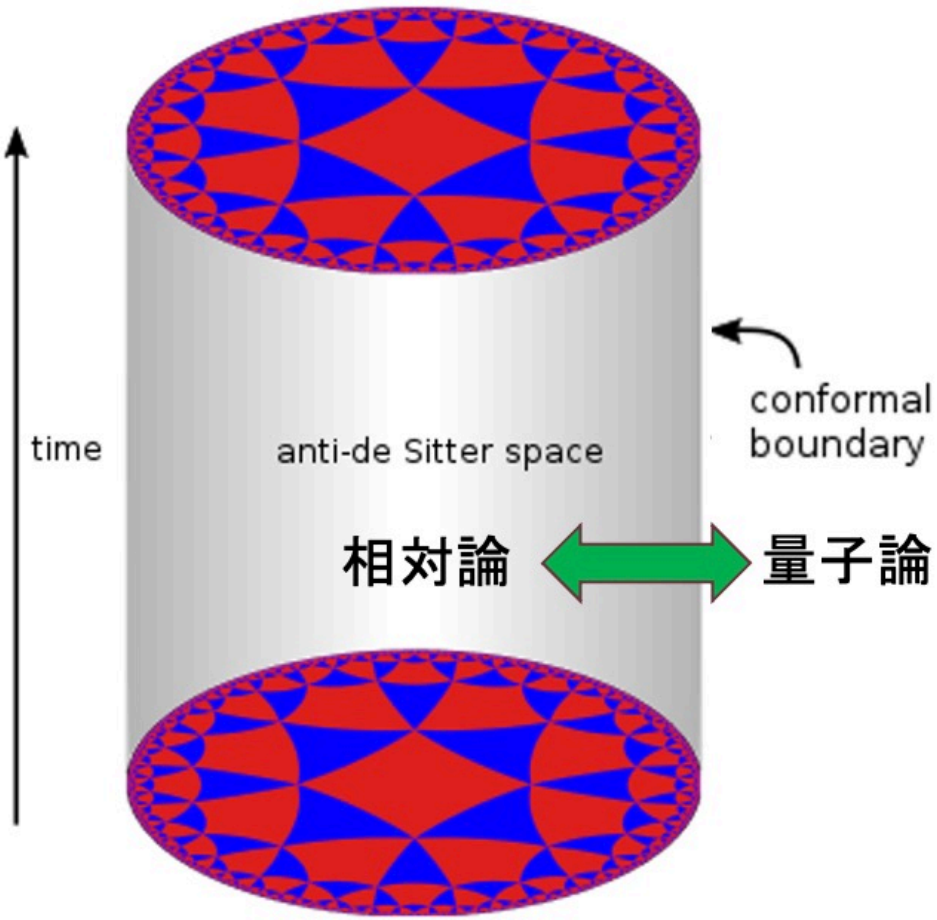
1997年 AdS/CFT対応

20世紀も終わりの1997年、マルデセーナは21世紀の物理学の扉を開く重要な発見をします。

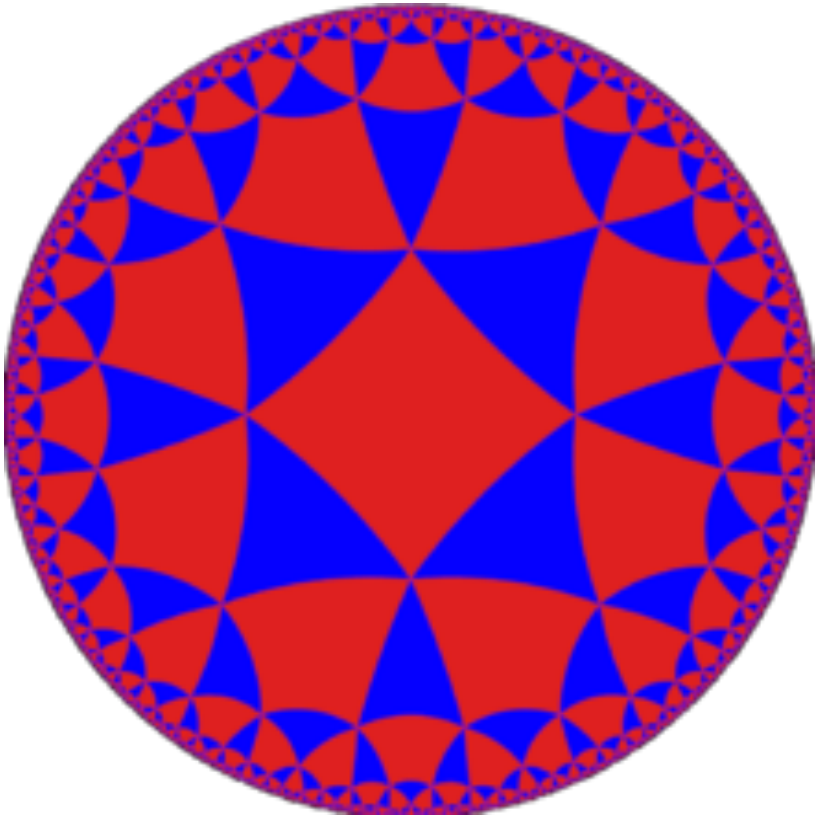
それは、d+1次元の時空を記述する重力理論AdS(Anti-de Sitter Space)と、d次元の場の量子理論CFT(Conformal Field Theory)が「対応」していることの発見です。この対応を「AdS/CFT対応」と言います。

この「対応」では、重力理論が d+1次元で量子論がd次元なので、相対論（重力理論）と量子論の次元が一つずれていることに注意してください。スープの入った缶詰で例えて言えば、相対論は缶のない中身のスープの理論で、量子論はスープのないスープをつつむ缶の理論だと言うことになります。

AdS/CFT対応


time
anti-de Sitter space
conformal
boundary
相対論
量子論


Campbell's
CONDENSED
TOMATO
SOUP



2006年　笠と高柳 エンタングルメントのエントロピー
“Holographic derivation of entanglement entropy from AdS/CFT”

マルデセーナの量子論と相対論（重力理論）の「対応」の発見をきっかけに、エンタングルメントの理解は、飛躍的に深まります。突破口を開いたのは、二人の日本人、笠真生と高柳匡でした。

「「時空」が、二つの部分 AとBに別れているとする。AとBの「境界部分」は、「時空」の「境界」なので、マルデセーナの理論にしたがって量子論で記述できるはず。」
「やってみたら、この「境界」は、なんと、量子論の「エンタングルメント」のエントロピーに対応するんだ！」

笠-高柳によるエンタングルメントがエントロピーを持つことの発見(2006年)は、先に見たベッケンシュタインのブラックホールがエントロピーを持つことの発見に匹敵する重要な発見でした。

2010年　Raamsdonk
“Building up spacetime with quantum entanglement”

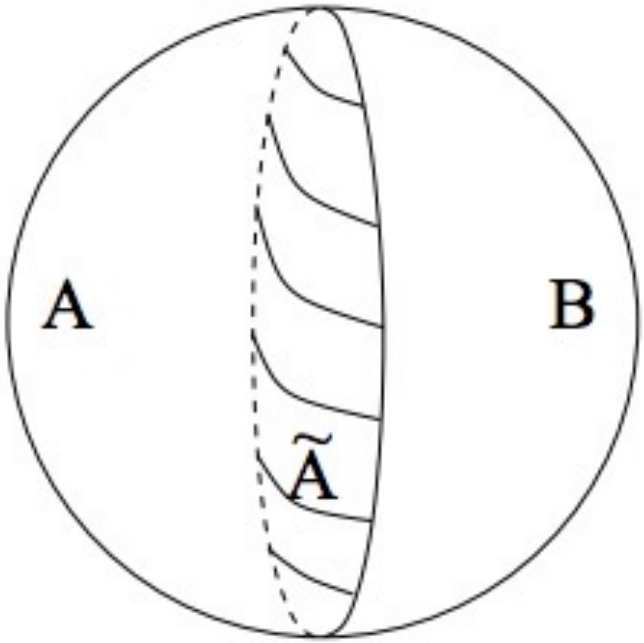
笠-高柳の発見に刺激されて、ラムズダンクが続きます。彼は、こう考えます。（2010年）

「二つの時空 A, B があったとする。二つの時空を、引き離してみる。そうすると、「境界面」の面積は減少する。これは、二つの時空が離れれば離れるほど、エンタングルメントのエントロピーが減ることを意味している。このエントロピーがゼロになった時、二つの時空は、引きちぎられる。」

「そうだ！　逆に考えればいいんだ。時空を結びつけているのは、エンタングルメントなんだ。エンタングルメントのエントロピーが、時空を縫い合わせているんだ！」

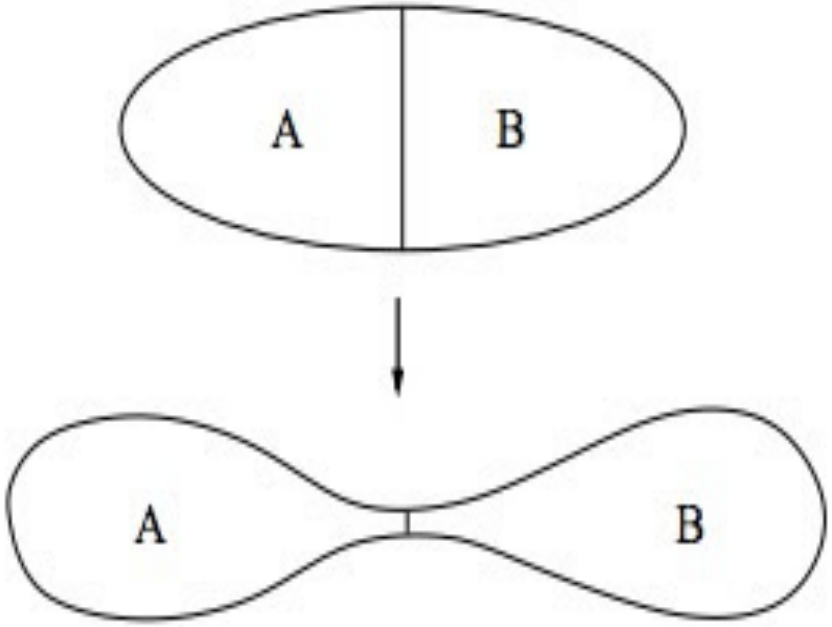
ここでは、二つの量子の奇妙なもつれあいとして発見されたエンタングルメントが、時空を結び合わせる「原理」として、見直されています。

笠-高柳



時空 A, Bの境界の量子論を考えるとエンタングルメントのエントロピーが出てくる

ラムズダンク



時空 A, Bを引き離すと、境界の面積、すなわち、エンタングルメントのエントロピーは減少する。

アインシュタインの1935年のもう一つの論文 “Einstein-Rosen Bridge”の存在

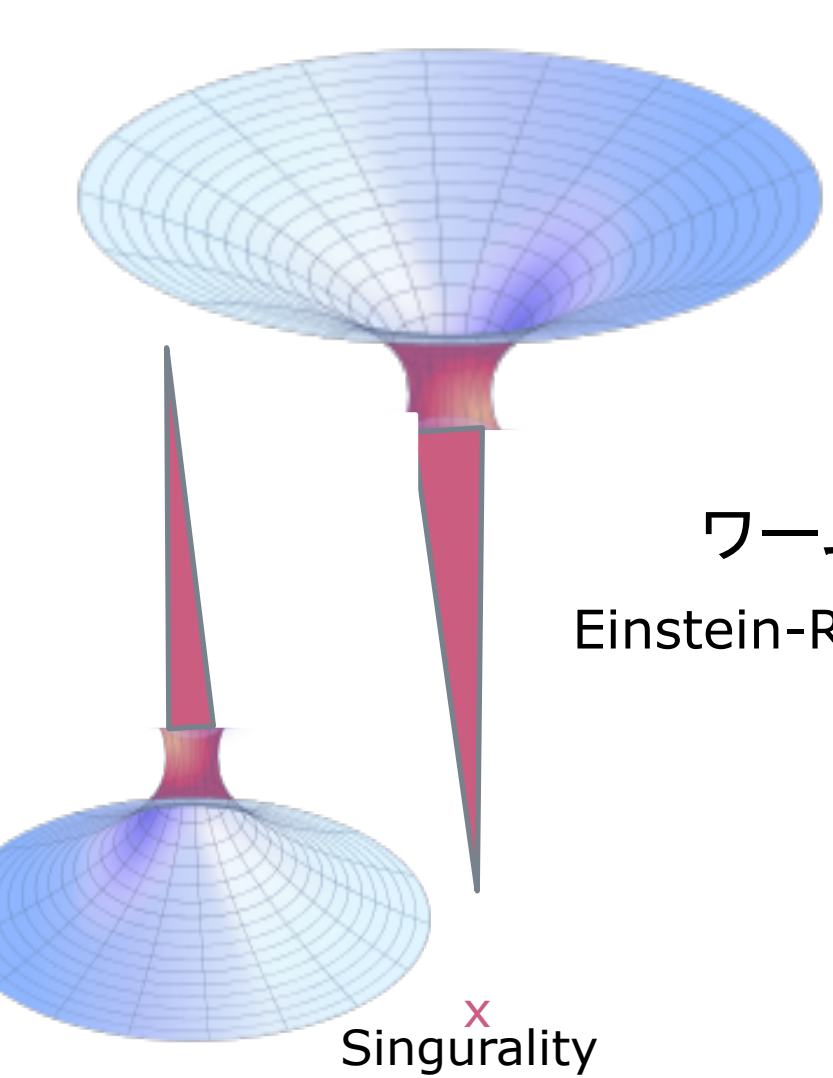
アインシュタインは、量子論の中に二つの量子の奇妙なもつれあった関係が存在することを発見して、それを「パラドックス」として提示しました。三人の著者 Einstein, Podolsky, Rosenの頭文字をとって、「EPR論文」と呼ばれます。1935年の5月のことです。

二ヶ月後の7月に、アインシュタインはローゼンとともに、"The Particle Problem in the General Theory of Relativity" 「相対性の一般理論における粒子の問題」という論文を公開します。この論文を「ER論文」と呼びます。

このER論文は、二つのブラックホールを結ぶ「橋」が存在しうることを指摘した論文です。この「橋」は、"Einstein-Rosen Bridge" と呼ばれ、別名「ワームホール」とも呼ばれます。

同時期にアインシュタインによってなされた、この二つの発見に何か関連があるのでしょうか？

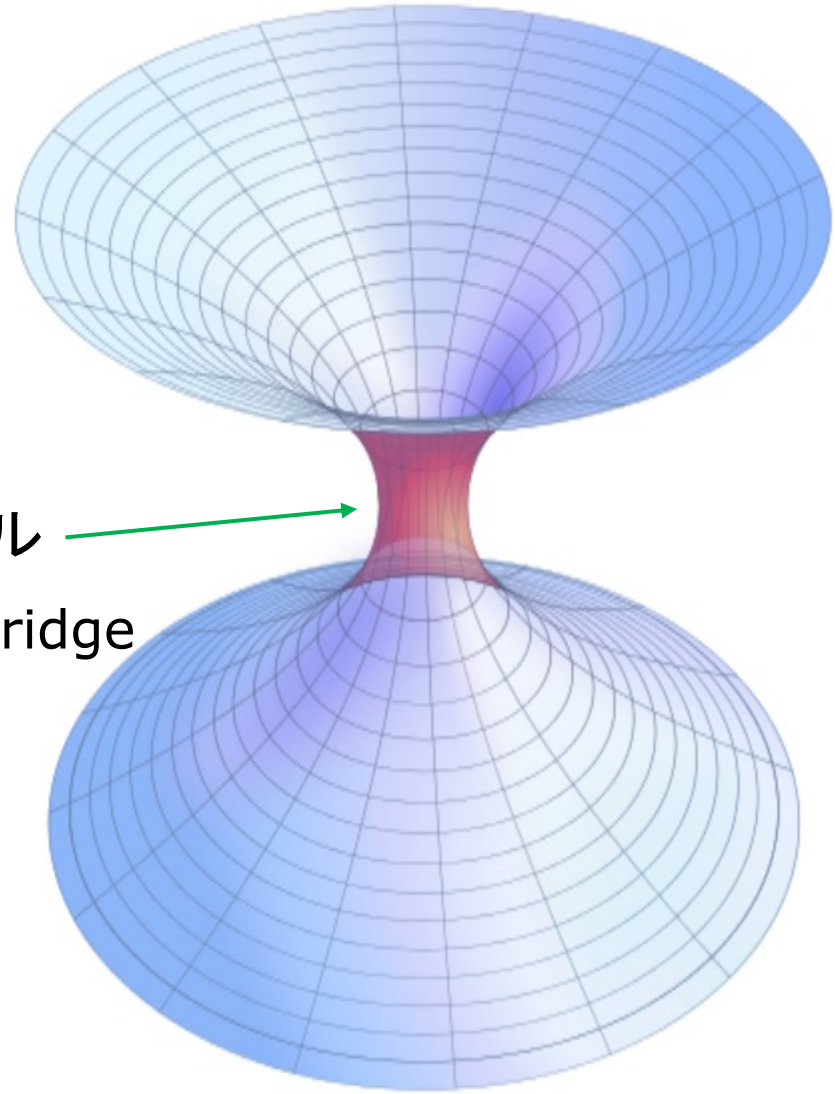
二つのブラックホールを結ぶ「ワームホール」



Singularity

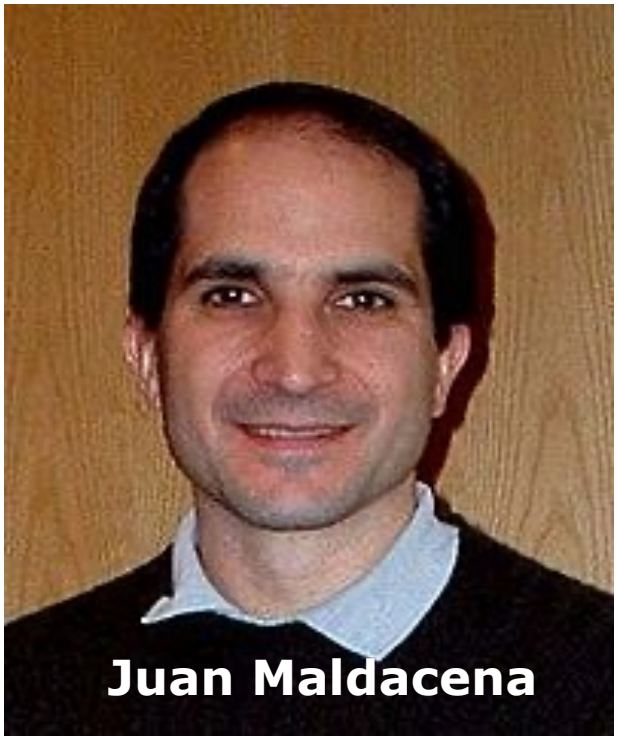
ワームホール

Einstein-Rosen Bridge

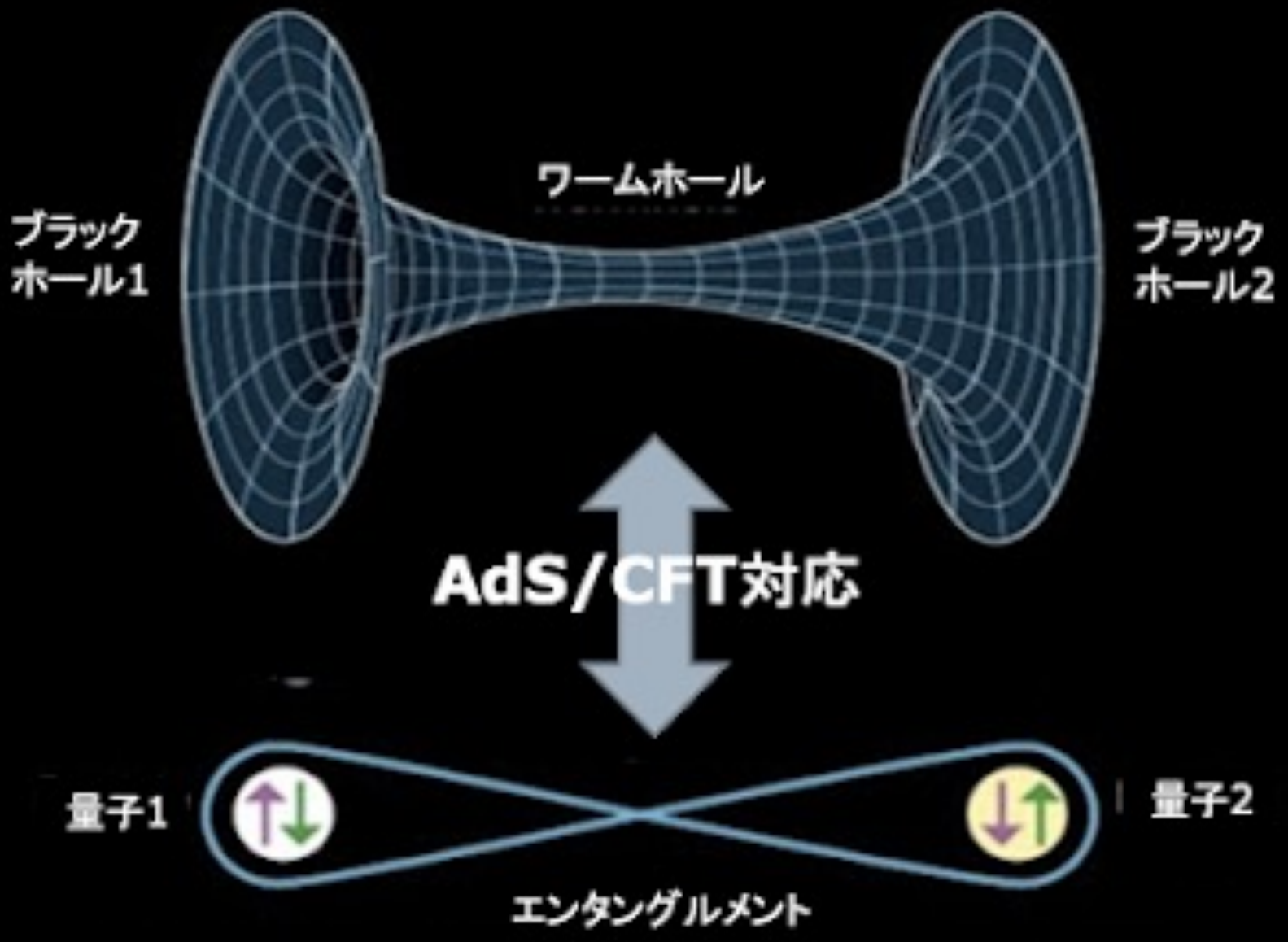


ER＝EPR仮説

2013年の論文で、マルデセーナとサスキンドは、1935年にアインシュタインが発見した「エンタングルメント」と二つのブラックホールを結ぶ「ワームホール」は、同じものだという大胆な仮説を提示します。「二つのブラックホールの間のワームホールは、二つのブラックホールのエンタングルメントによって生成される。」



ER=EPR 仮説



アインシュタインの洞察の深さの再評価

こうした経過は、1935年の二つの論文に見られるアインシュタインの洞察の深さの再評価という意味を持っています。「ER＝EPR仮説」の中心人物のサスキンドは、アインシュタインへの敬意をこめて、また当時の量子論サイドの対応を批判をしつつ次のように書いています。

「当時の量子論に対する最後の批判で、アインシュタインは、とても深く、とても直感に反していてとても人を困惑させるが、それでも人をとても興奮させる、何かを指摘していたのだ。だから、その何かは、21世紀の始まりと共に、多くの理論物理学者を魅了するものとして帰ってきているのだ。エンタングルメントの発見という、アインシュタインの最後の偉大な発見に対して、ボーアが行った唯一の回答は、それを無視することだった。」

エンタングルメントの認識の難しさ
「局所性」について

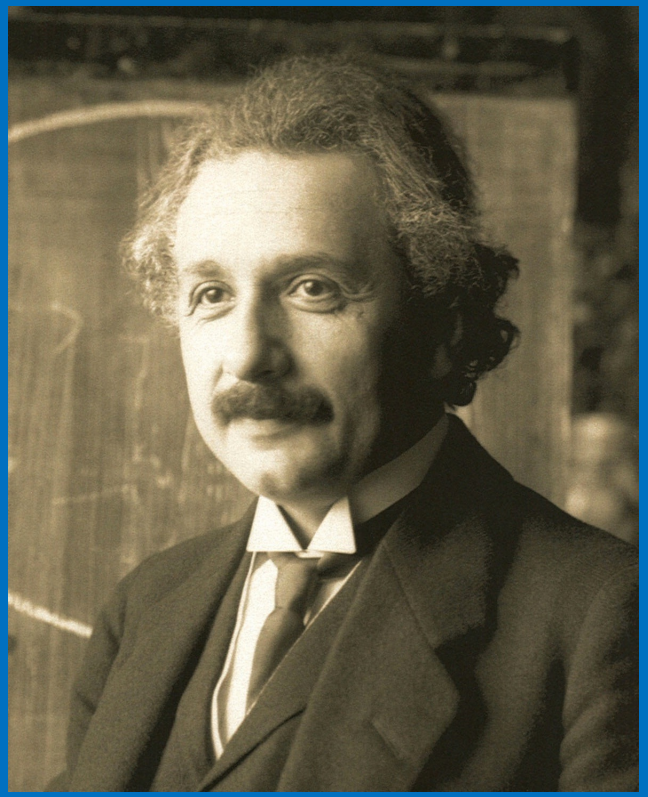
遠隔作用の否定と因果関係の局所性

「それは馬鹿げた遠隔作用だ。」

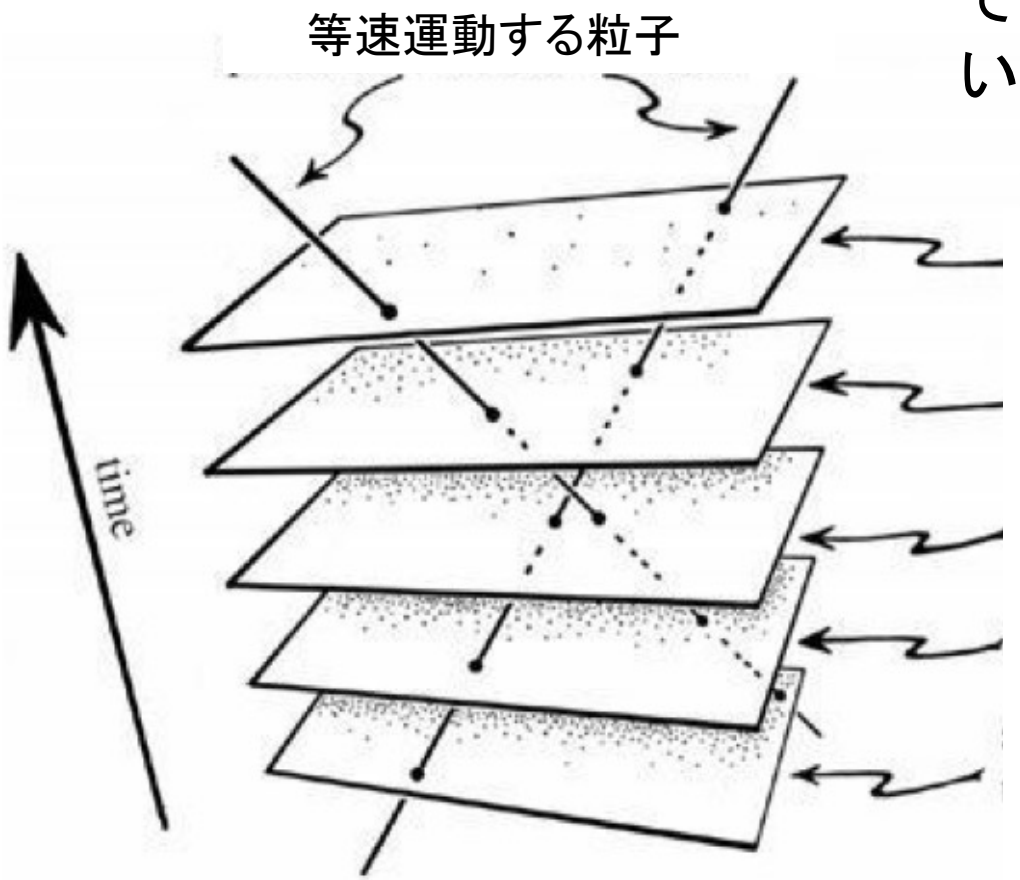
アインシュタインは、エンタングルメントのことをそう呼びました。確かにそれは、二つの量子がどんなに離れていても、片方の量子の状態を観測すると他方の量子の状態が瞬時に分かる現象のように見えます。

それは、アインシュタインが特殊相対論で確立した、ある事象の影響は光のスピードを上限としてしか他の事象に影響を及ぼさないという「事象の局所性」に反しているように見えます。物理的な「因果関係」は、局所的な性質を持ちます。

ミンコフスキーとアインシュタイン



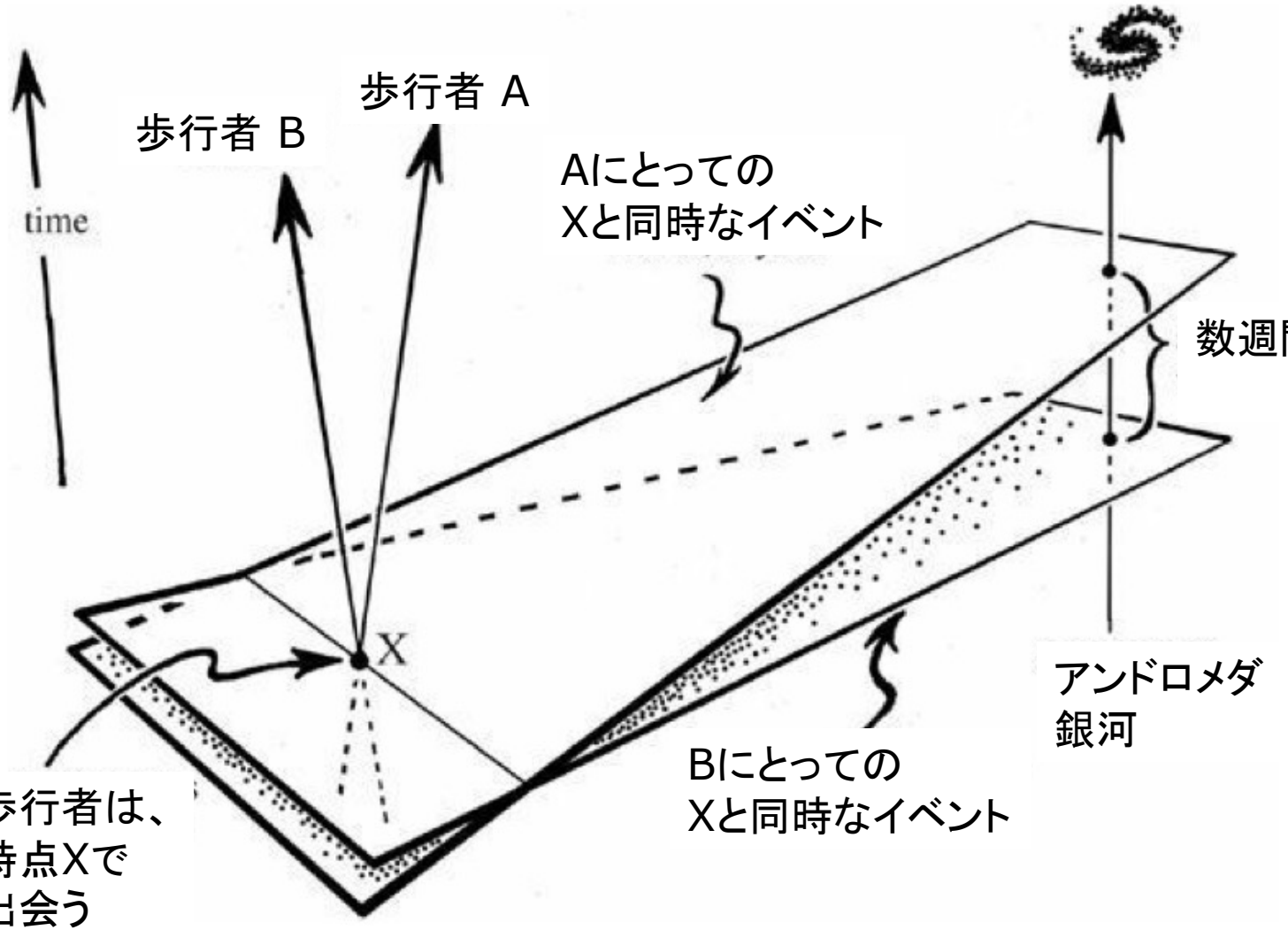
空間は、「同時刻の空間」で、平行にスライスされている。



ミンコフスキー以前の時空像

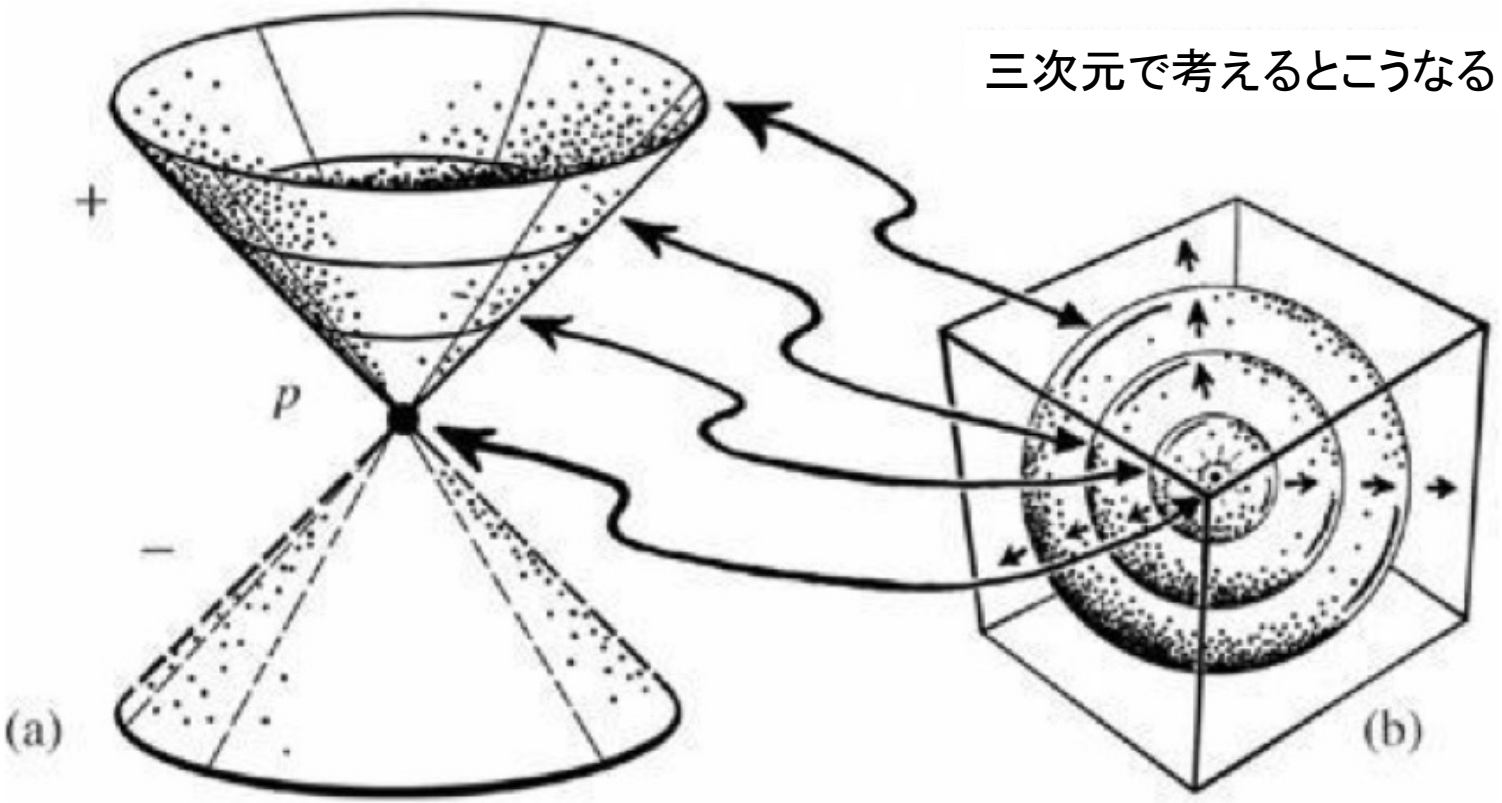
Penrose “Cycle of Time” https://goo.gl/RBYi5T

歩行者のスピードによって、「同時刻の空間」は、ことなる。



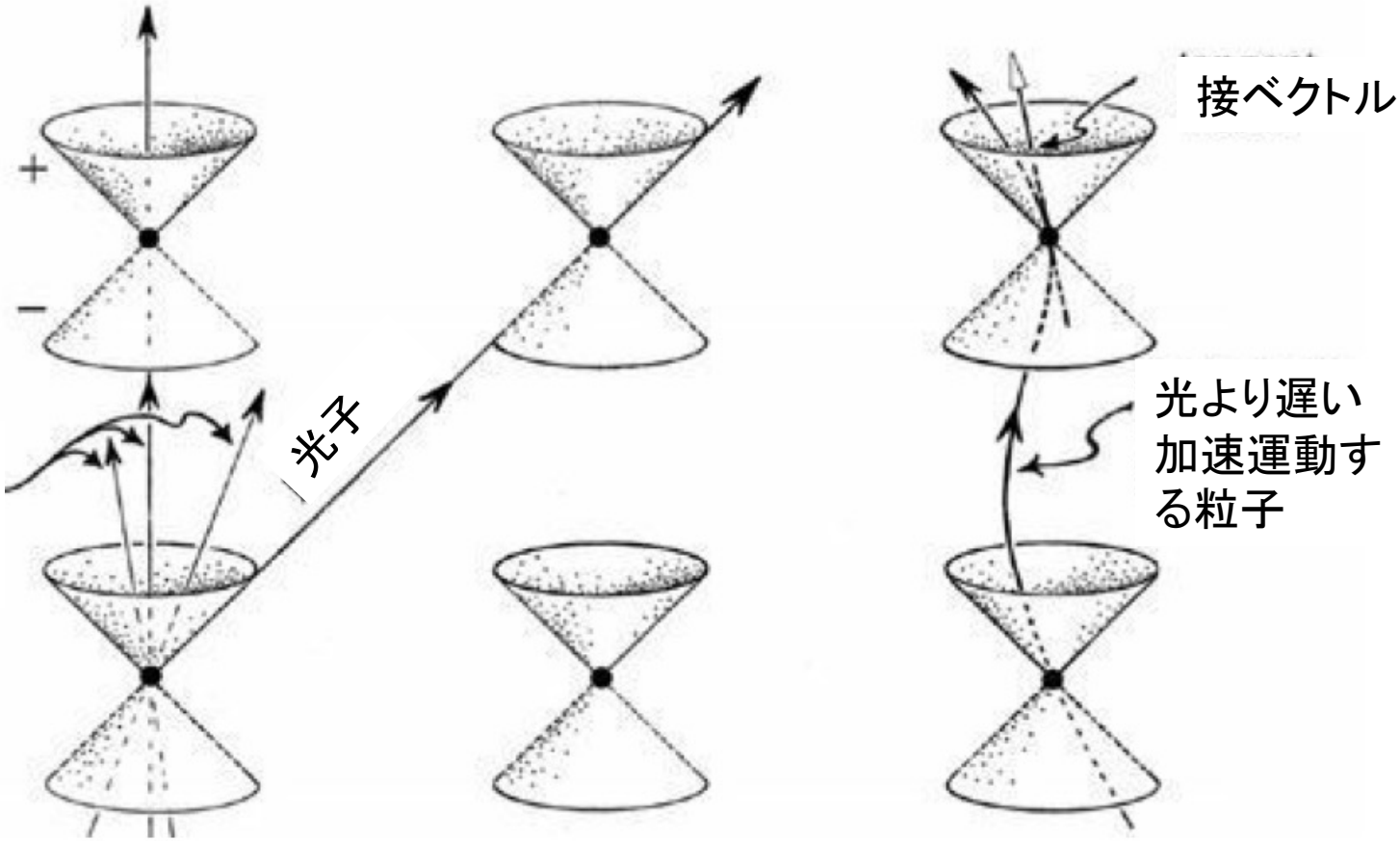
ミンコフスキー空間で二人の歩行者が出会う

Penrose “Cycle of Time” https://goo.gl/RBYi5T



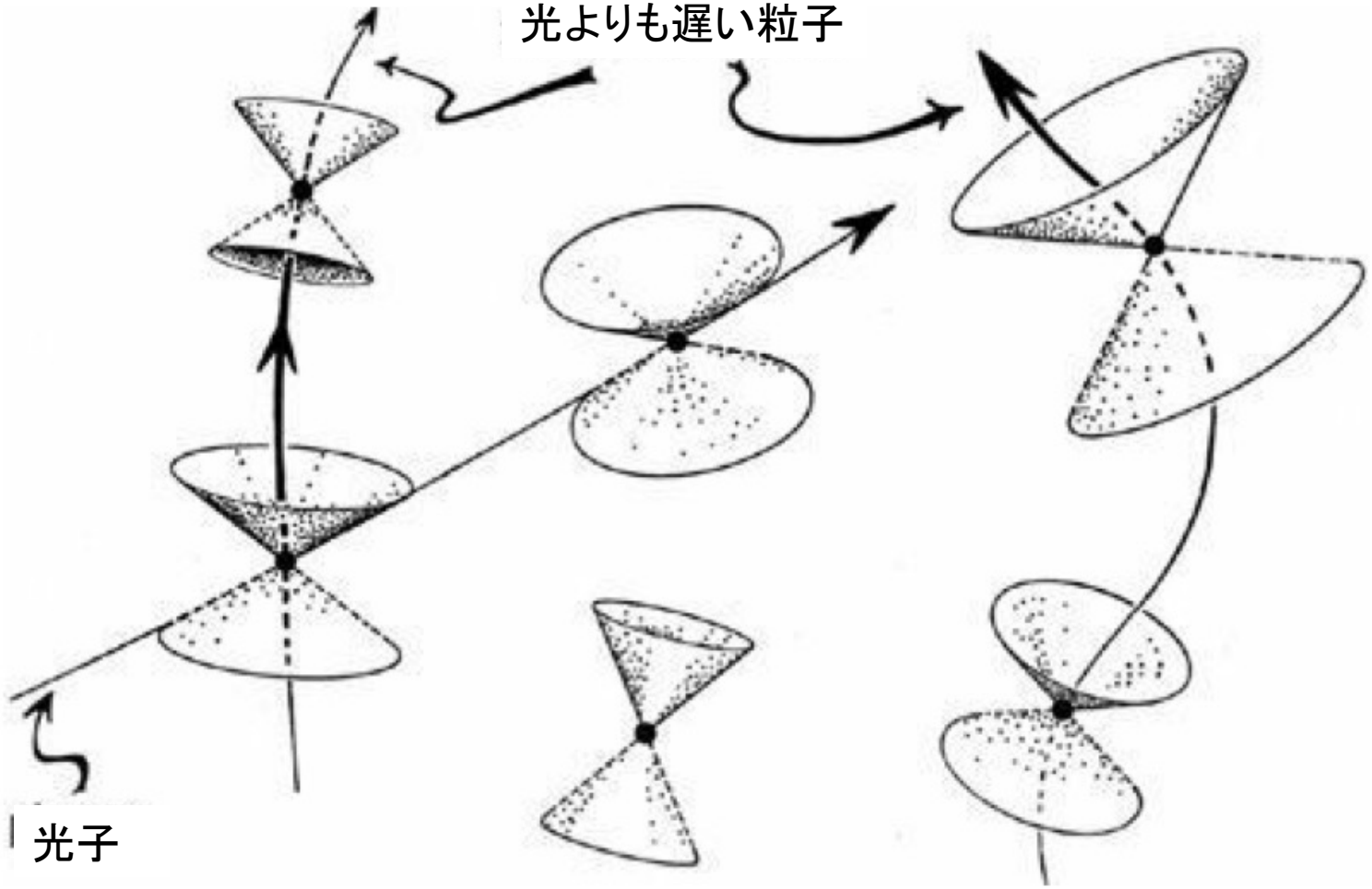
ミンコフスキー空間 pでの光円錐（Null cone）

Penrose “Cycle of Time” https://goo.gl/RBYi5T



ミンコフスキー空間の各点に
一様に置かれた光円錐（たいらな時空）
特殊相対論

アインシュタインは、時空の各点に時計を置いた



ミンコフスキー空間の各点に
非一様に置かれた光円錐（曲がった時空）
一般相対論

物理的な「実験」では、単純化していうと、実験の対象と観測機器と観測者の知覚が、すべて物理的な因果関係のチェーンで結ばれたされたシステムを構成しています。

それでは、そうした局所的な因果関係を破るエンタングルメントのような現象の実在は、どのような「実験的」手段で確かめることができるのでしょうか？　それは、物理的な因果関係に従わない「テレパシー」の存在を、物理的な因果関係に従う実験で証明しようというのに似ていないでしょうか？

エンタングルメントの実在性の認識
Bellのアプローチ

Bellのアプローチ

Bell は、エンタングルメントの分析を徹底して進めました。
彼は、もし、二方向に放たれたペアのそれぞれの粒子を独立に観測すれば、それぞれの粒子が独立に「隠れた変数」に従属するという仮定の下では、二つの粒子の観測の出力の相関は、ある「制約条件」を持つだろうと考えます。

そして、かれはその制約条件の定式化に成功します。Bellが見つけた「隠れた変数論」すなわち古典論が従うべき観測結果の相関の制約条件は、「Bellの不等式」と呼ばれます。

ついで、彼は、量子論での相関の予測が、この不等式を破ることを見出します。

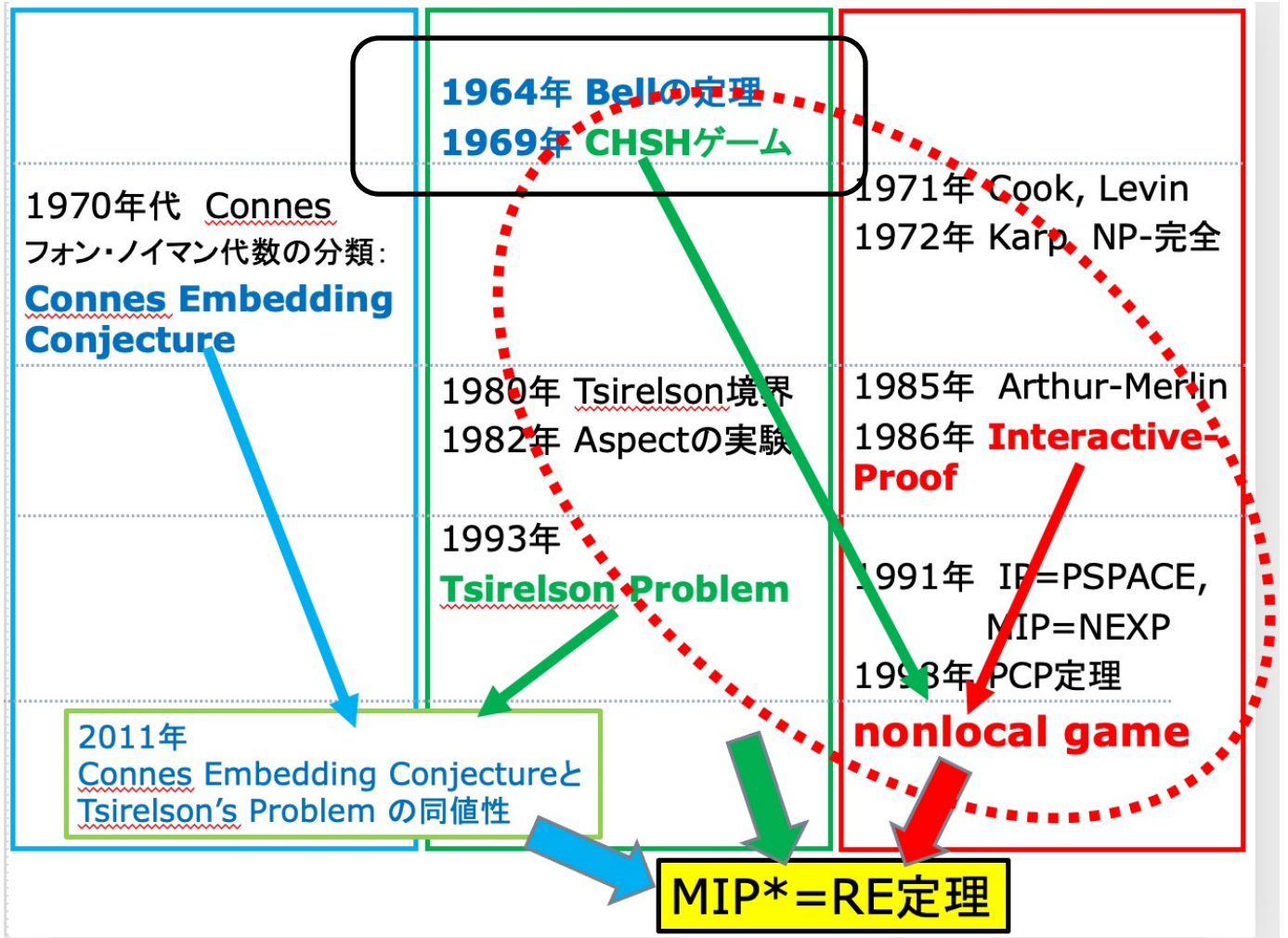
量子論の非局所性

結局のところ、「隠れた変数」論が量子論の予想を説明する唯一の方法は、量子論が「非局所的」だということでした。

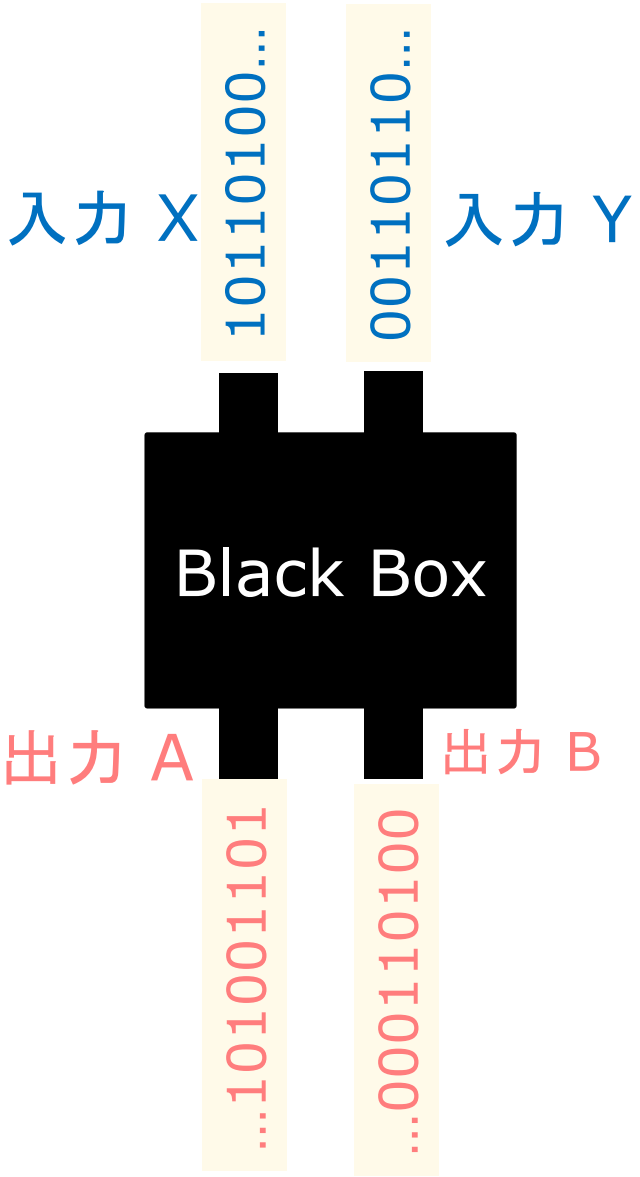
すなわち、ペアのそれぞれは独立に「隠れた変数」に従属しているのではなく、何らかの方法で関連していて、両者の距離がたとえどんなに遠くに離れていても、一方の影響を瞬時に他方に及ぼすことができるということでした。

Bellは、このことを次のように述べています。
「もしも、「隠れた変数」論が局所的であるなら、それは量子力学とは一致しないだろう。もし、それが一致するなら、それは局所的ではないであろう。」

ちなみに、こうしたアプローチの理論化は、1960年代になされたものですが、21世紀に入って、Interactive Proofの流れの中で、こうしたアプローチの再評価が行われ、次の認識の飛躍MIP*=RE を準備することになりました。

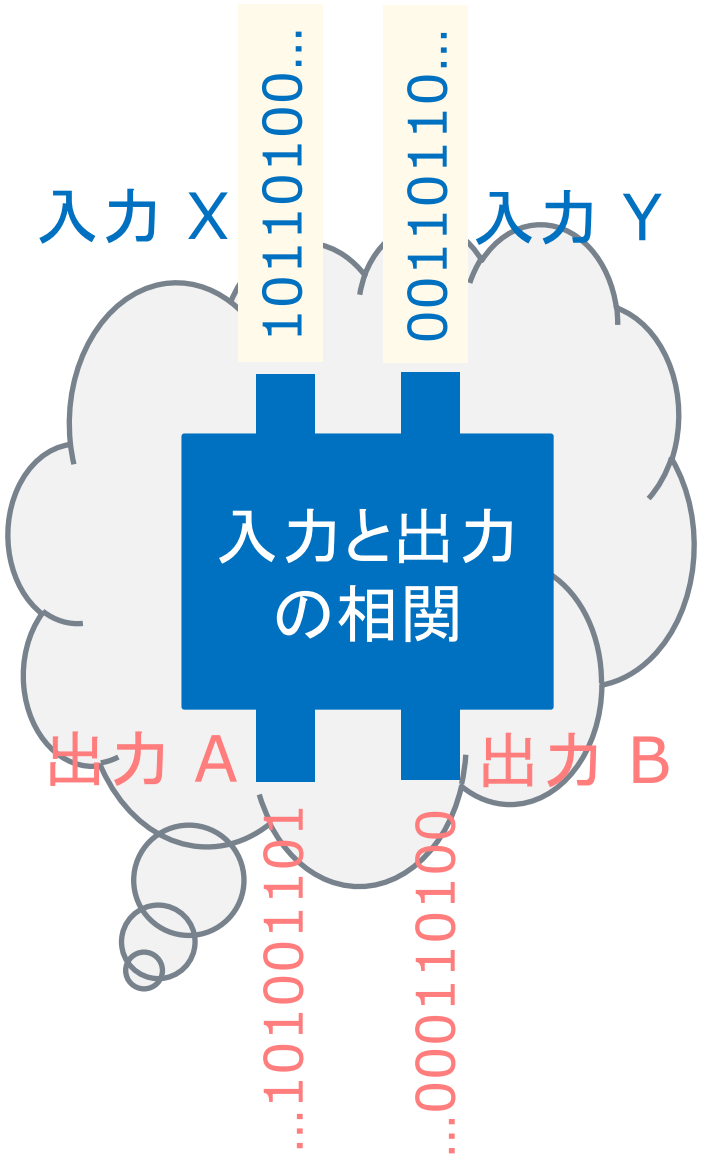


Bellのアプローチ



0または1を入力X,Yとして受け取り、0または1を出力A,Bとして吐き出す箱があるとしましょう。

内部の仕掛けはわからないブラックボックスです。

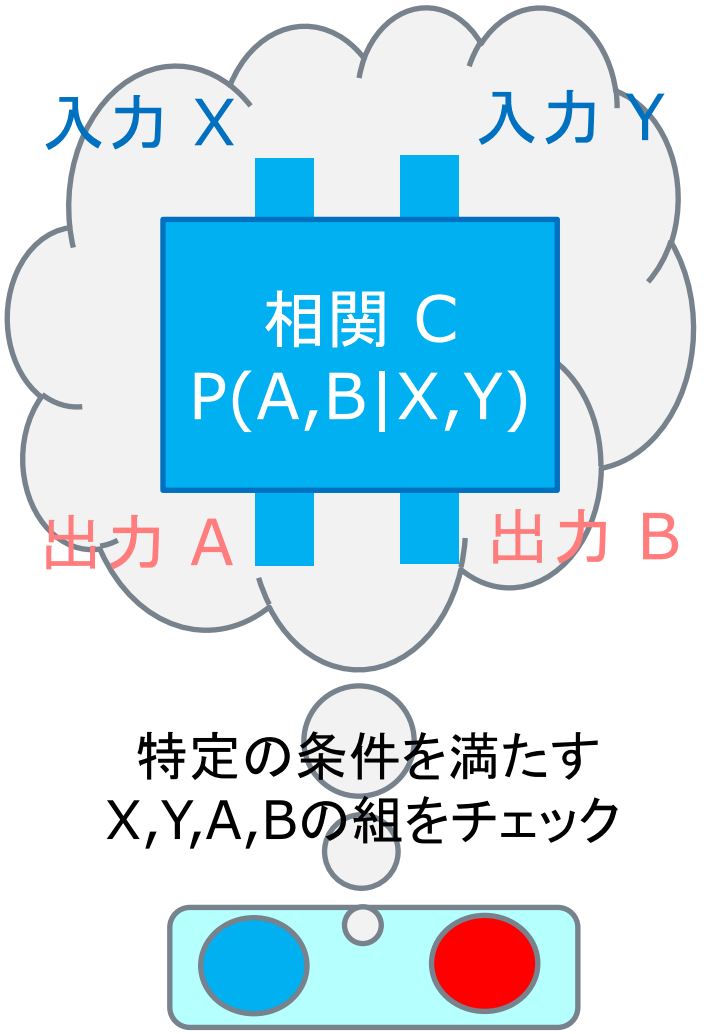


ブラックボックスだとしても、入力と出力を観察すれば、両者の「相関 C」は知ることができます。

入力と出力の「相関 C」は、入力X, Yが与えられた時の出力A, Bの条件付き確率で与えられます。

C = P(A, B | X, Y) です。

入力の分布：μ(X,Y)



今、ブラックボックスの入力 X, Yと出力 A, B が、ある関係 D(X,Y,A,B)＝1 を満たす時、青いランプがついて、そうでない時は赤いランプがつくとしましょう。

この時、入力の分布μ(X,Y) が与えられれば、相関Cのもとで、青いランプがつく確率を求めることができます。

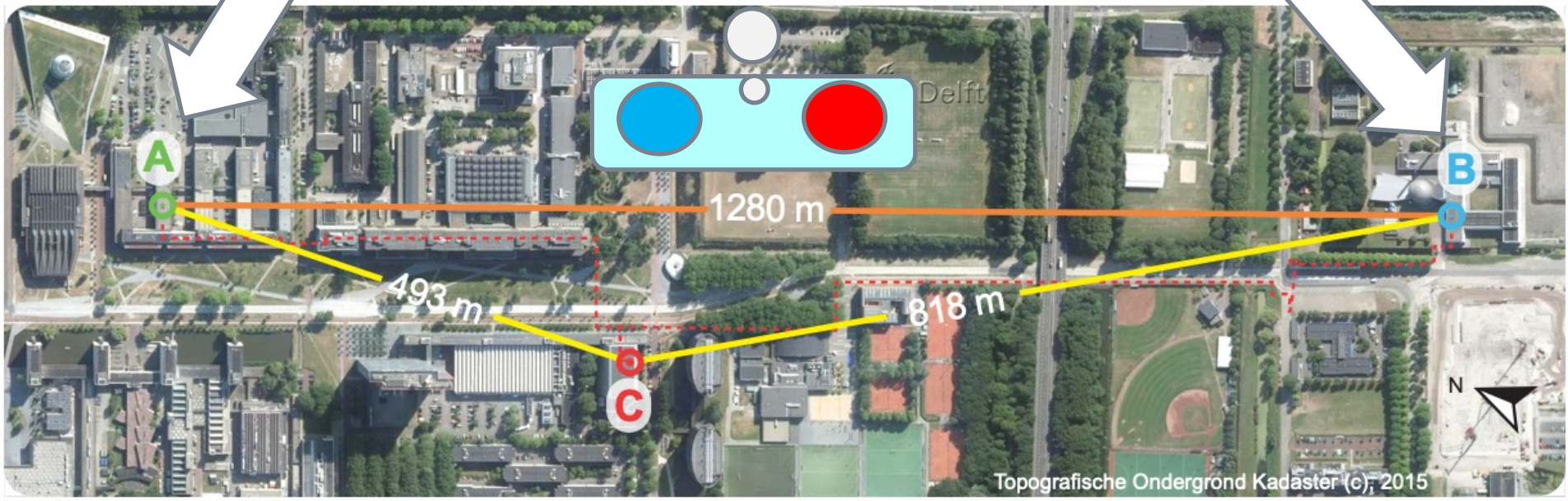
A地点での量子
入力 X

B地点での量子
入力 Y

相関 C
P(A,B|X,Y)

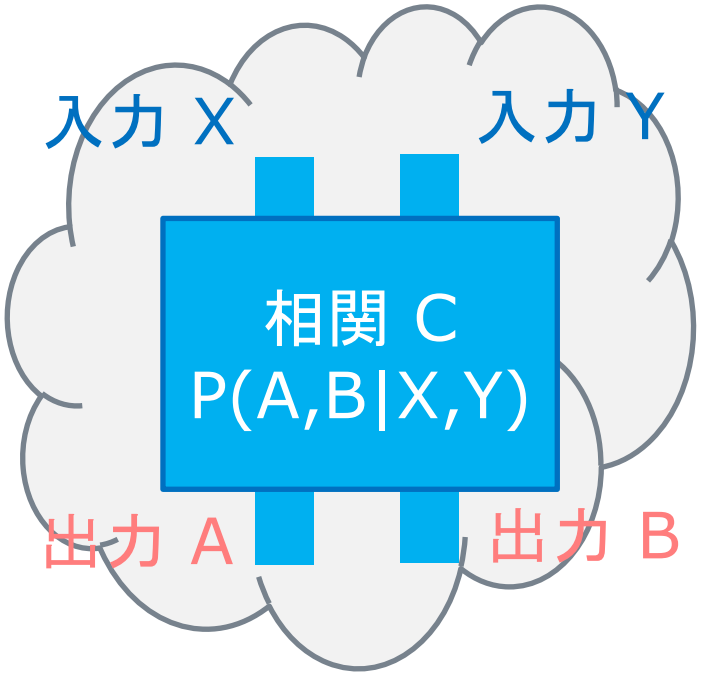
A地点での観測
出力A

B地点での観測
出力B

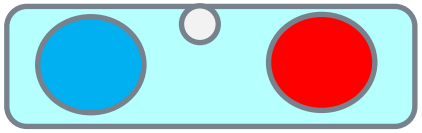


CHSHゲーム

入力の分布：μ(X,Y)



特定の条件を満たす
X,Y,A,Bの組をチェック



D(X,Y,A,B)=1
条件を満たす

D(X,Y,A,B)=0
満たさない

同じ状況を、出題者 vs. (Alice+Bobチーム)の対戦ゲームに読み替えたものが、CHSHゲームです。

出題者が、AliceとBobに問題を出して、AliceとBobはそれに答えます。問題 X, Y と回答 A, Bが、ある条件を満たすときに、Alice+Bobチームは、ゲームに勝ちます。

入力の分布：μ(X,Y)

入力 X

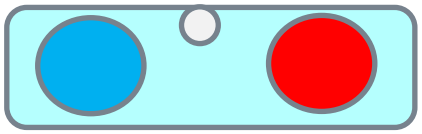
入力 Y

相関 C
P(A,B|X,Y)

出力 A

出力 B

特定の条件を満たす
X,Y,A,Bの組をチェック



D(X,Y,A,B)=1
条件を満たす

D(X,Y,A,B)=0
満たさない

CHSHゲーム

V:出題者(出題)

出題の分布：μ(X,Y)

出題 X

出題 Y

Alice

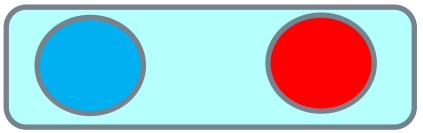
Bob

相関 C
P(A,B|X,Y)

回答 A

回答 B

V:出題者（判定）

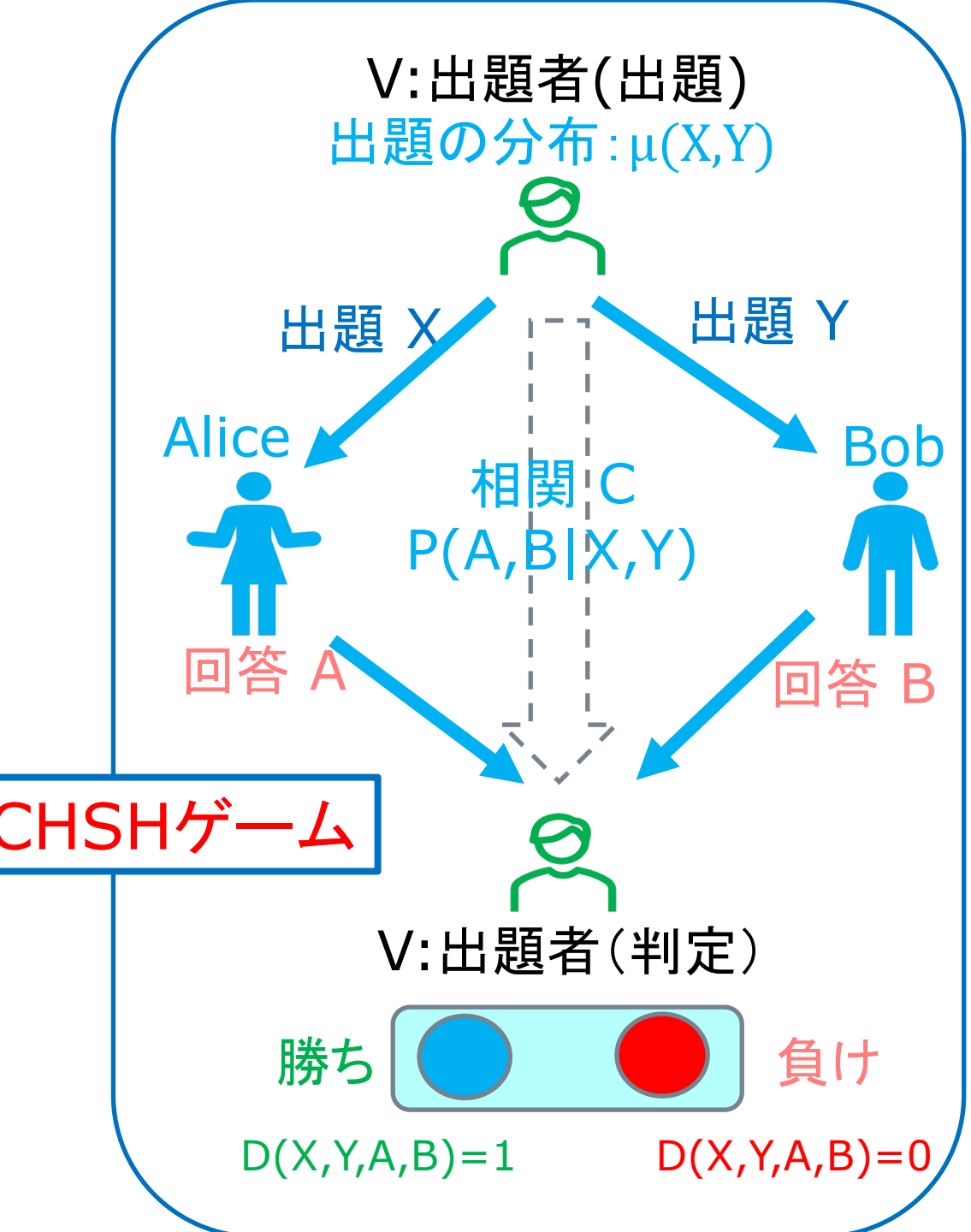


勝ち

負け

D(X,Y,A,B)=1

D(X,Y,A,B)=0



ブラックボックスの
入力 X, Y　出力 A, Bは、
CHSHゲームの
出題 X, Y　回答 A, Bに
対応しています。

先のブラックボックスで
青いランプがつく確率は、
CHSHゲームで
Alice+Bobチームが
勝つ確率に対応します。

CHSH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す。

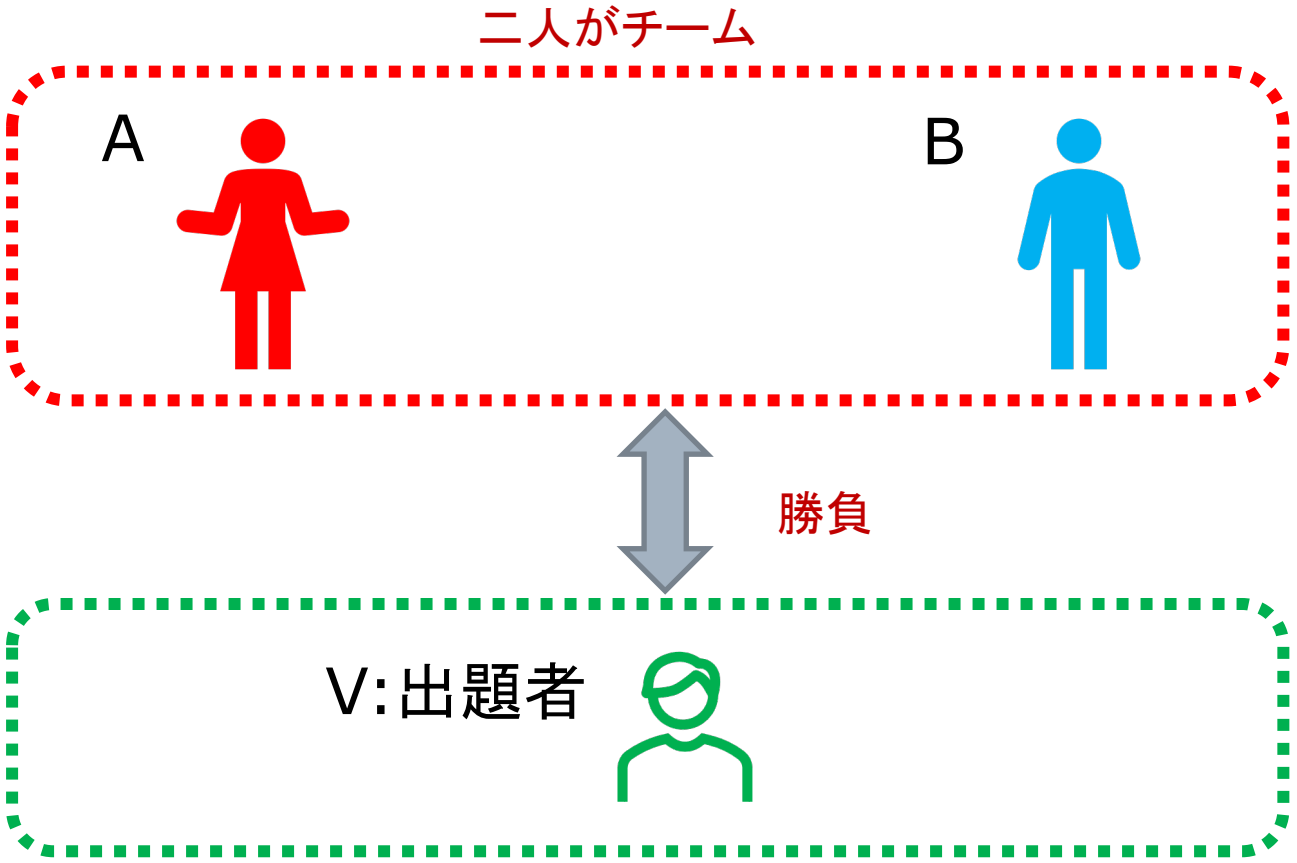
A 

B 

V:出題者 

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す。



ゲームの条件

ただし、AとBとの会話は禁じられています。
また、出題者はAとBに別々に問題 x, y を出すものとします。

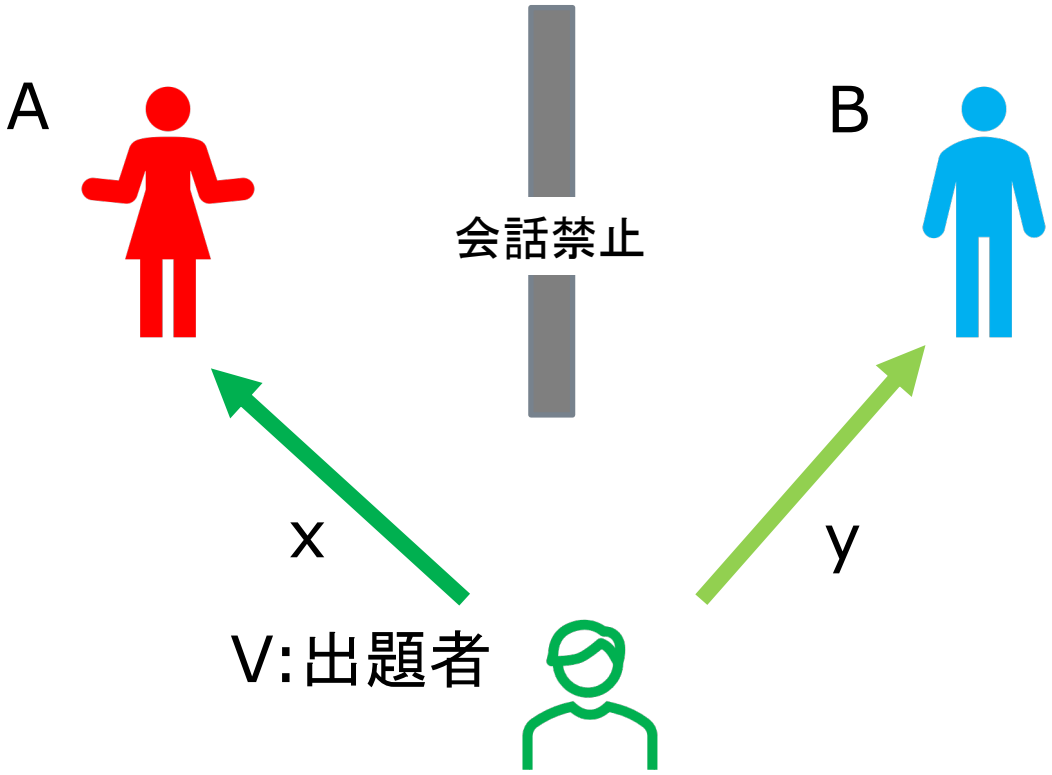
A

B

V:出題者

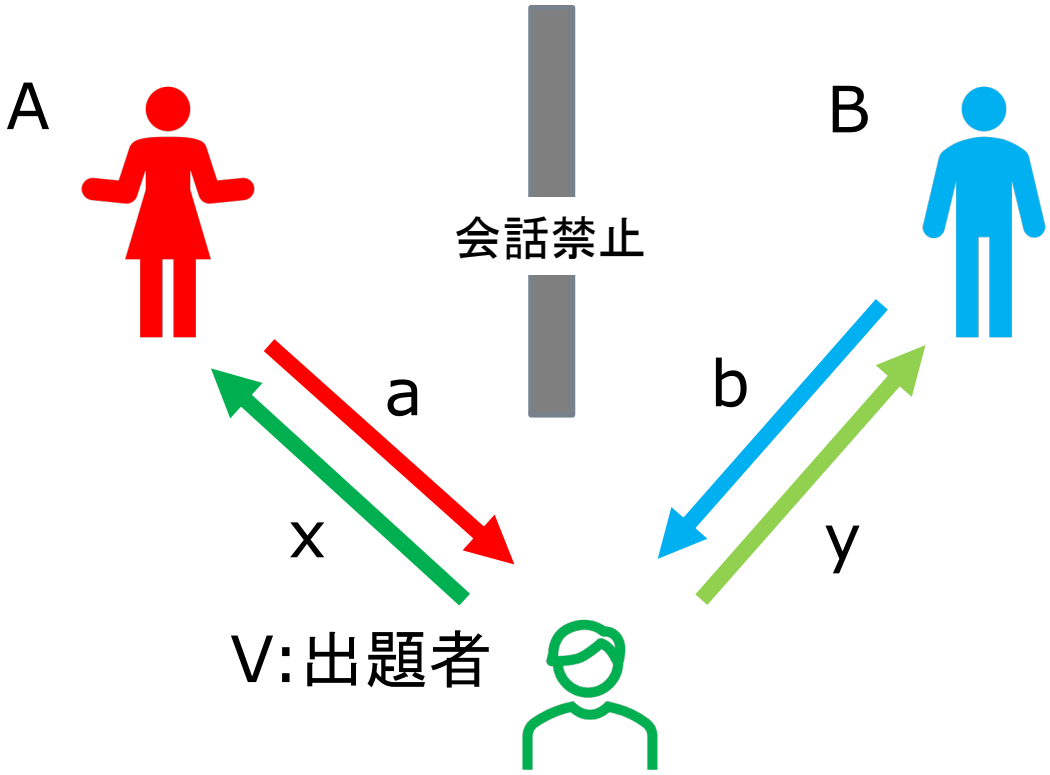
ゲームの条件

ただし、AとBとの会話は禁じられています。
また、出題者はAとBに別々に問題 x, y を出すものとします。



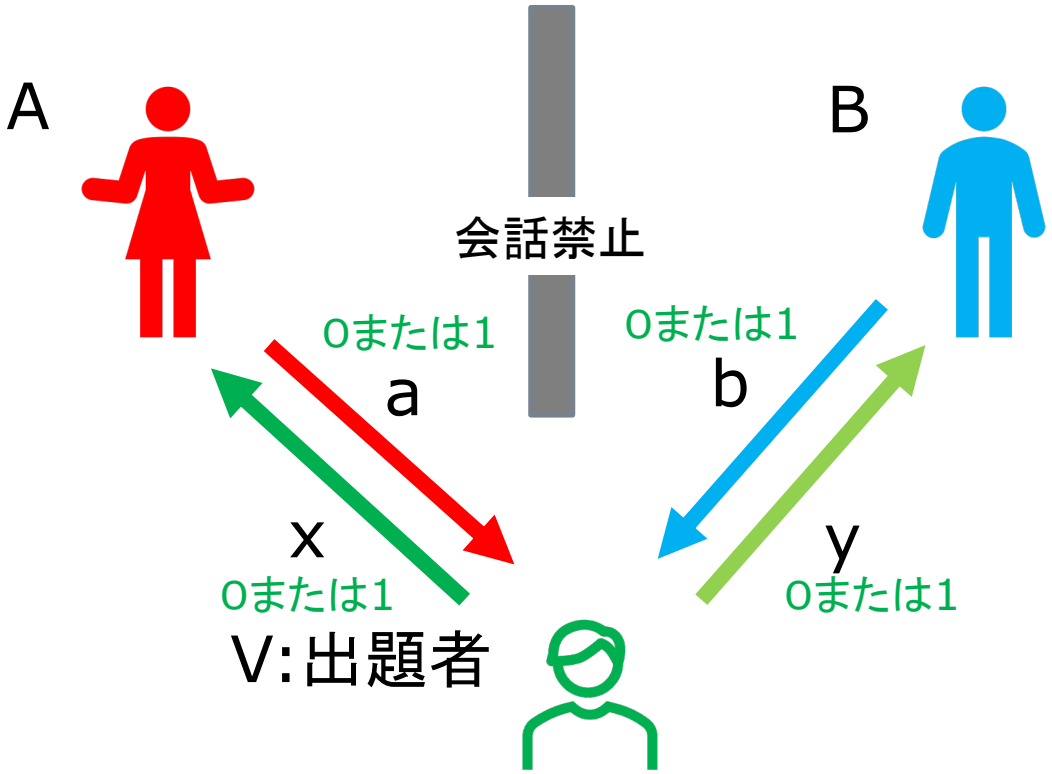
ゲームの条件

AとBは、Vの出した問題x, yに応じて答え a, bを返します。
AとBとの会話は禁じられているので、それぞれに答えを返します。



問題と答えのパターン

Vは A, Bに、問題として、0または1を送ります。
A, Bは Vに、答えとして、0または1を送ります。



ゲームのルール

次の条件を満たす時、A,Bチームの勝ちとします。
そうでない場合、A,Bチームは負けです。

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。

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、

x=0, y=0	x=0, y=1	x=1, y=0

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。

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

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、

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=1 b=1	a=1 b=1	a=1 b=1	

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

A,Bチームが勝つ条件は、
次のように書ける。

$$xy = a + b \pmod 2$$

あるいは

$$xy = a \oplus b$$

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

必勝法？

A,Bチームは、ゲームの勝敗のルールは知っているとする。

A,Bチームに必勝法はあるでしょうか？

もし、A,BがVからの問題を受け取った時点で、相談できれば、先の表を見て、勝つように答えを選ぶことができます。相談さえできれば、必勝法は存在します。

ただ、AとBの会話は禁じられています。

AはBがVから受け取ったyの値を知らないし、BはAがVから受け取ったxの値を知りません。これでは、必ず勝てるような答えを選ぶことはできません。このゲームの設定では、必勝法は存在しません。

A,Bがランダムに答えた場合の勝率

Vがランダムに問題を出し、A,Bがそれぞれランダムに答えた場合の勝率Pを計算しましょう。

P ＝ (x,yのいずれかが0である確率) x (a,b が等しい確率)
＋ (x=y=1である確率) x (a,b が等しくない確率)

$$\frac{3}{4}\times\frac{1}{2}+\frac{1}{4}\times\frac{1}{2}=\frac{4}{8}=\frac{1}{2}$$

このゲームは、双方がランダムに振舞えば、どちらかが有利なゲームとは言えないことがわかります。

A,Bチームの勝率を高める戦略

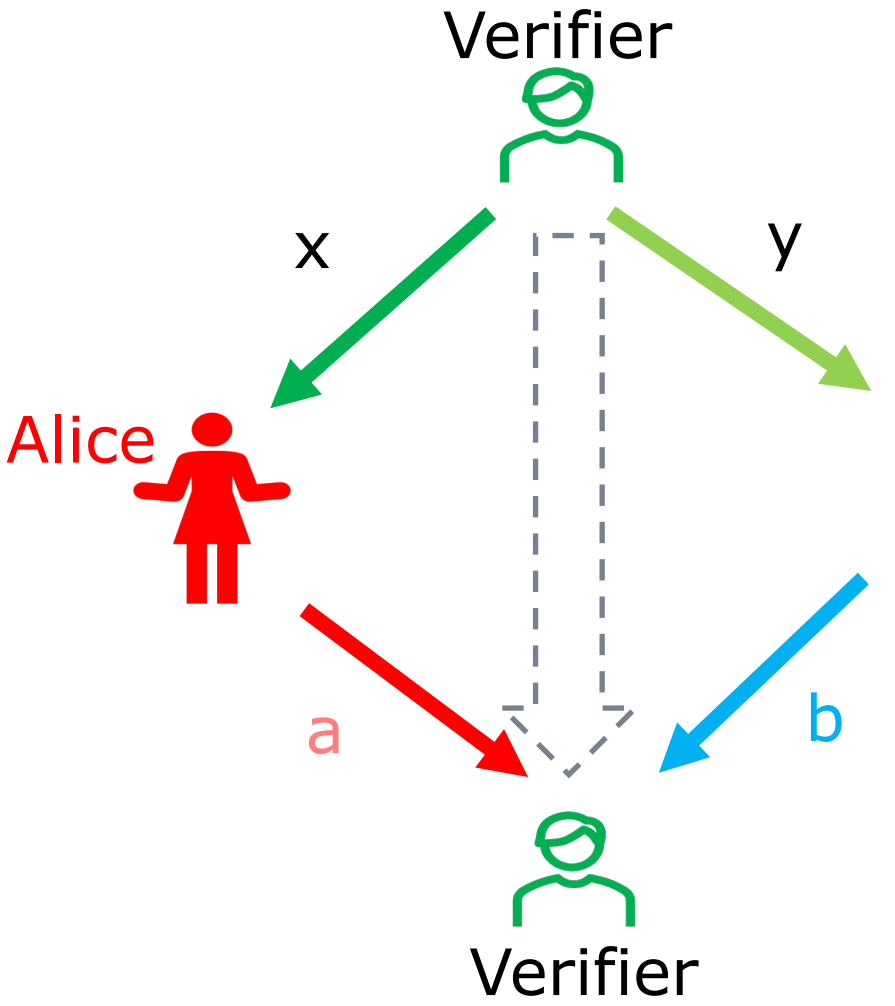
A,Bチームは、事前に打ち合わせをして、次の戦略を取ることができます。

A,Bは、x,yの値に関わらず、a=b=0と全て0を返す (Plan 0)。あるいは、a=b=1と全て1 を返す (Plan 1)。

いずれの場合でも、A,Bチームの勝率は、3/4 となり、ランダムに対応した場合の1/2より、勝率を高めることができます。

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=0	⇐ Plan 0
a=1 b=1	a=1 b=1	a=1 b=1	a=1 b=1	⇐ Plan 1

CHSHのゲームの定式化



①

質問の分布：

$\mu(x, y)$

②

質問と回答の相関：

$p(a, b \mid x, y)$

③

ゲームの勝敗を定義する関数：

$D(a, b, x, y) \rightarrow \{0, 1\}$

CHSHゲームの定式化

CHSHゲームは、次の三つの式で特徴付けられます。

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： $D(a, b, x, y) \to \{0, 1\}$

CHSHゲームの場合、

- $\mu(x, y)$は、0と1の一様にランダムな分布、
- $p(a, b \mid x, y)$
  $= p(a, b \mid 0, 0) + p(a, b \mid 0, 1) + p(a, b \mid 1, 0) + p(a, b \mid 1, 1)$、
- $D(a, b, x, y)$は、
  $a+b=xy \pmod 2$の時に1を、それ以外の時に0を返す関数。

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 $\omega(\mathrm{G},\mathrm{p})$は、次の式で与えられます。

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

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

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$p \in C_q$の違いに帰着します。

古典論的相関と量子論的相関のもとでのCHSHゲームの最大勝率

Bellの不等式に従う古典的相関のもとでは、CHSHゲームの最大勝率は、3/4 = 0.75 になります。

量子論的相関のもとでは、CHSHゲームの最大勝率は、$\cos^2(\pi/8) = 0.8125\ldots > 3/4$ になります。

物理実験に基づくCHSHゲームでは、その勝率は$\cos^2(\pi/8)$であることが確かめられました。

こうして、自然は、古典論的相関ではなく、量子論的相関に従うこと、エンタングルメントは実在することが、実験的に確かめられました。

Part II

「全能者」との対話で得られる認識
-- Interactive Proof --

4/10 マルゼミ「楽しい哲学」

Agenda Part II

「全能者」との対話で得られる認識
-- Interactive Proof --

- 数学的証明をめぐるいくつかのエピソード
  - 証明の難しさ
  - 数学の証明へのコンピューターの利用
  - Voevodskyの問題提起
- 新しい証明のスタイル -- 対話型証明の想定
- グラフの「同型問題」と「非同型問題」
  - グラフの「同じ」を考える
  - グラフの同型性チェックのために必要な場合の数
  - Graph Isomorphismの複雑性クラス
- 対話型証明の最初の成功
- 対話型証明の発展
- 新しい数学的証明観の登場


数学的証明をめぐる
いくつかのエピソード

証明の難しさ

誤っていた「証明」

「フェルマーの定理」は、最終的には、1995年のAndrew Wilesの論文によって証明されたのですが、フェルマー自身は、この定理を証明出来たと信じていました。それが、誤った「証明」であったのは確かです。

Wiles自身も、95年の論文以前に一度、「証明した」とする発表を行いましたが、誤りが見つかり、それを撤回しています。

世紀の難問である「リーマン予想」は、何度か「証明」が発表されています。今までのところ、それは誤って「証明」でした。

正しいことの判定が難しい証明

Grigory Perelmanは、2002年から2003年にかけて arXiv に投稿した論文で、「三次元のポアンカレ予想」を解いたと主張しました。

arXivは、学会の論文誌とは異なり、掲載の可否を決める査読が基本的にないので、発表の時点では、彼の論文以外に、彼の証明が正しいという裏付けはありませんでした。

彼の証明の検証は、複数の数学者のグループで取り組まれ、最終的に彼の証明の正しさが「検証」されたのは、2006年のことでした。

非常に膨大な証明

「有限単純群の分類問題」は、Daniel Gorensteinをリーダーとする数学者の集団によって解決され、20世紀の数学の大きな成果の一つと呼ばれています。

ただ、その「証明」は、100人以上の数学者が、50年のあいだに数百の論文誌に発表した、膨大な量の「証明」の総和です。そのページ数は一万ページを超えると言われています。

「証明を全部を読んでる数学者は、１人もいない。」というのがジョークなのか本当なのか、僕には分かりません。

数学の証明へのコンピューターの利用

なぜ、数学の証明にコンピュータが必要なのか？

フェルマーの定理を証明したワイルズが、謙遜して自分は「巨人の肩の上の小人だ」と言ったように、数学は、先行した無数の人たちの業績の蓄積の上に成り立っています。

ピタゴラスの「教団」は、いくつかの発見を「秘教」にしていたらしいのですが、もしも、ピタゴラスの子孫が生きていたとしても、ピタゴラスの定理を使うのに、彼らに著作権料を払う必要はありません。また、その「証明」を自分で繰り返す必要もありませんない。

少なくとも現代の数学では、情報の共有は、学問自体の前提でさえあります。

「四色問題」のコンピュータによる解決

1974年、イリノイ大学のKenneth AppelとWolfgang Hakenは、当時の最先端のコンピュータを使って、「四色問題」を解きました。

コンピュータの稼働時間は、1200時間に及び、夜間の空き時間しか利用が認められなかったので半年がかりの計算だったと言います。

コンピュータが人手にはあまる膨大な計算を行ったのは事実ですが、当時、その計算の正しさの検証しようのないことを理由に、こうした「証明」を疑問視する声も一部にはありました。

「四色問題」「Feit-Thompsonの定理」のCoqによる証明

2004年、Georges Gonthierは、Coqを使って「四色問題」を解きました。

Georges Gonthierは、また、2013年、有限群分類の重要な定理である、「Feit-Thompsonの定理」のCoqによる形式的証明を与えました。

15,000の定義、4,300の定理、17万行のソースからなるこの証明を、彼はチーム作業で、6年かけて完成させたといいます。

計算結果を印刷すると、
マンハッタン島ぐらいの
サイズになる

Mathematicians Map E_8

Mathematicians have mapped the inner workings of one of the most complicated structures ever studied: the object known as *the exceptional Lie group E_8*. This achievement is significant both as an advance in basic knowledge and because of the many connections between E_8 and other areas, including string theory and geometry. The magnitude of the calculation is staggering: the answer, if written out in tiny print, would cover an area the size of Manhattan. Mathematicians are known for their solitary work style, but the assault on E_8 is part of a large project bringing together 18 mathematicians from the U.S. and Europe for an intensive four-year collaboration.

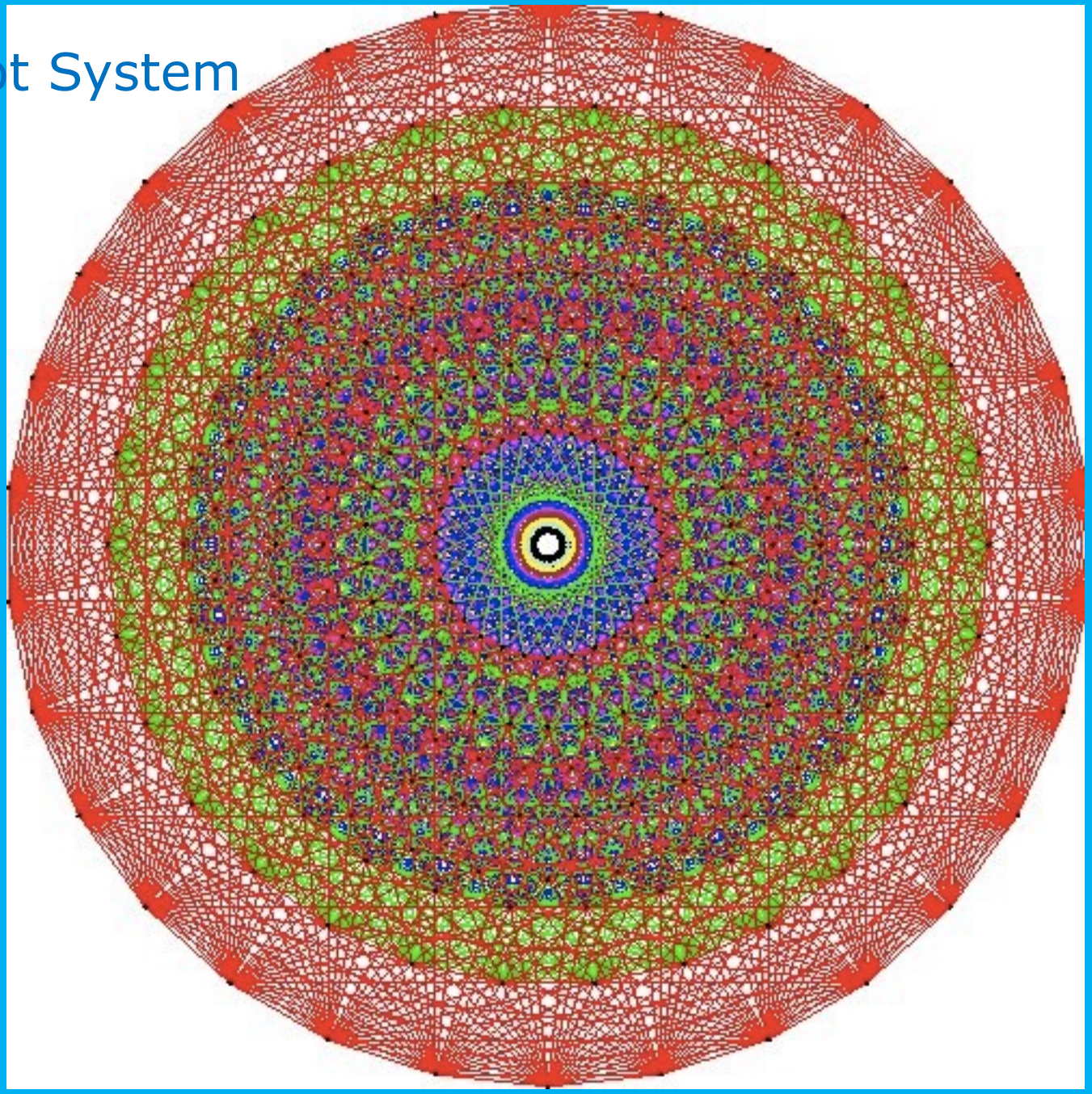
http://www.aimath.org/E8/

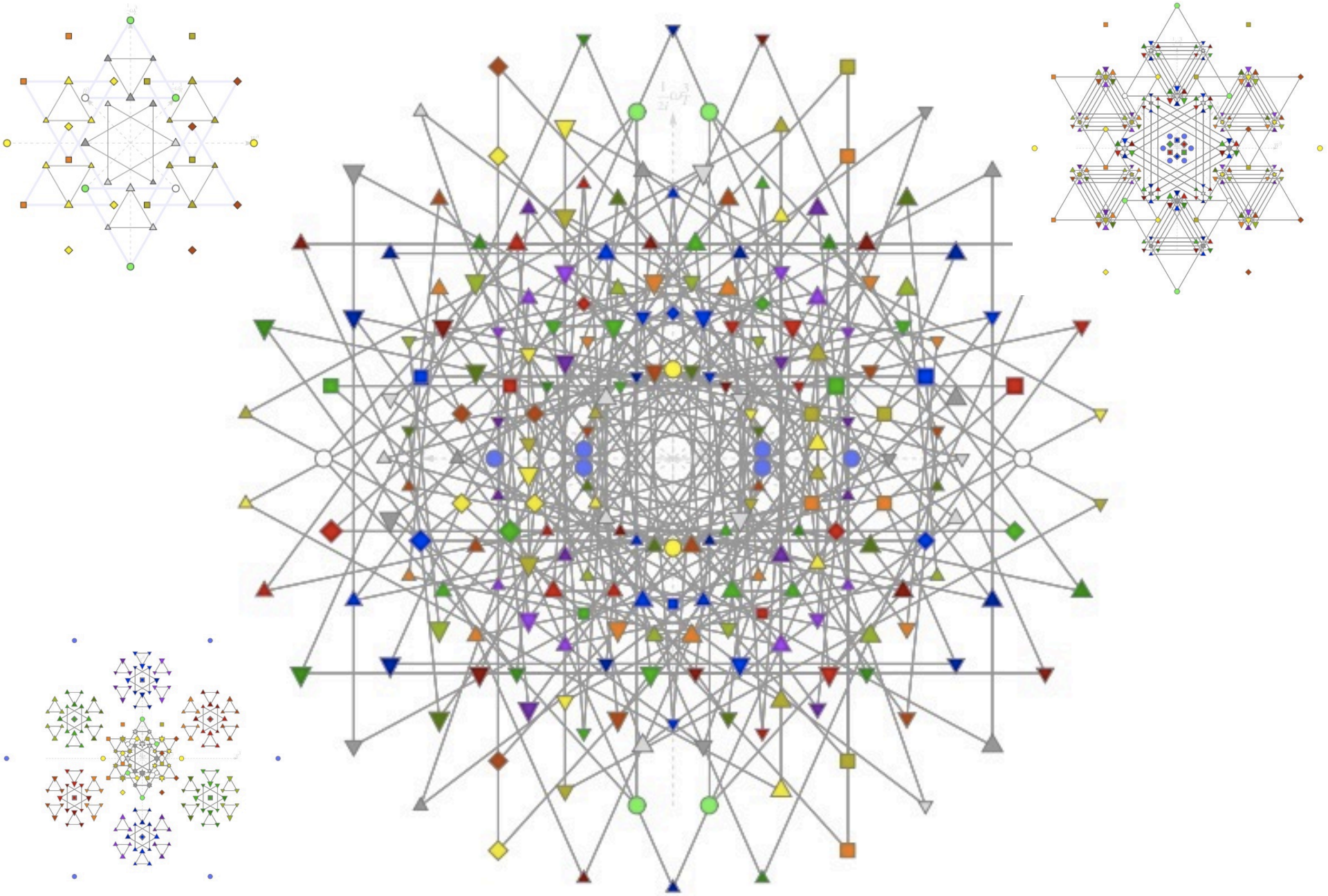
人間の遺伝子情報は、1ギガ以下。
E8の計算結果は60ギガ。

E_8 Map: Bigger than the Human Genome

The magnitude of the E_8 calculation invites comparison with the Human Genome Project. The human genome, which contains all the genetic information of a cell, is less than a gigabyte in size. The result of the E_8 calculation, which contains all the information about E_8 and its representations, is 60 gigabytes in size. That is enough space to store 45 days of continuous music in MP3 format. While many scientific projects involve processing large amounts of data, the E_8 calculation is very different: the size of the input is comparatively small, but the answer itself is enormous, and very dense.

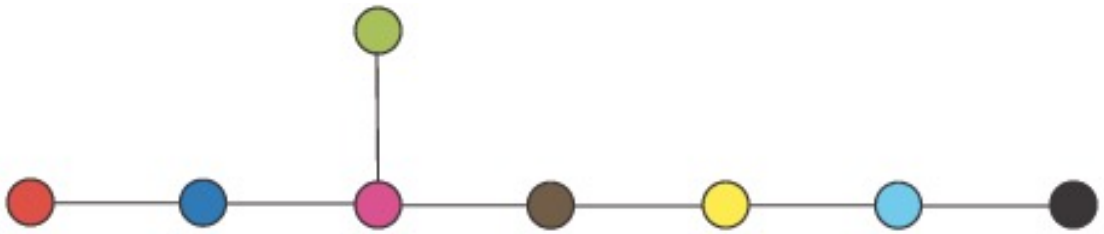
E_8 Root System



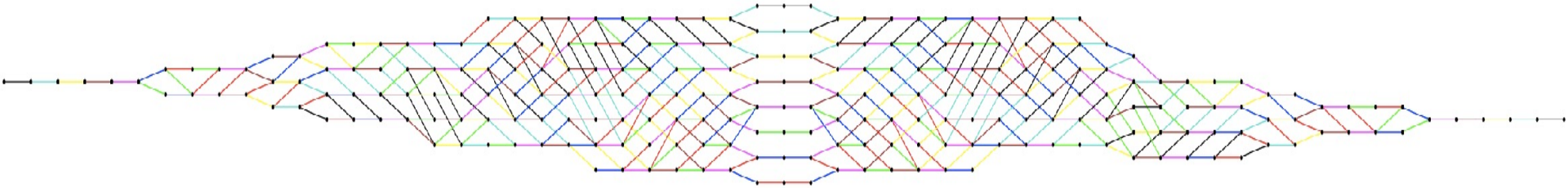


Garrett Lisi: An Exceptionally Simple Theory of Everything
https://goo.gl/bmfwxi

E_8 Dynkin diagram



picture of the 248-dimensional Lie algebra of E_8



The Lie algebra E_8 is generated by 16 elements X_{red}, Y_{red}, X_{blue}, Y_{blue},…, X_{black}, Y_{black} corresponding to the nodes in the Dynkin diagram.

Voevodsky

Voevodsky
1966年6月4日 - 2017年9月30日

Voevodsky

2017年に亡くなったVoevodskyは、Milner予想、Bloch-Kato予想を解くなど、代数幾何でグロタンディックが進もうとした道で、大きな業績を残しました。ヴョブドスキーの最後の仕事は、数学の基礎とコンピュータに関係していました。

彼は、数学の証明に、コンピュータを使うべきだと主張した最初の数学者の一人で、また、そのためのコンピュータによる証明支援システムのライブラリーUniMthを開発しました。

GitHub: https://github.com/UniMath/UniMath

2016年9月の講演 "UniMath - a library of mathematics formalized in the univalent style" https://goo.gl/3sJr1M

Voevodskyの経験

2000年頃、彼は1993年に自分が発表した論文の重要な補題が間違っていたことに気づきます。でも、その頃には、その論文は広く出回っていて、多くの数学者がその証明を「信じて」いました。彼が、その間違った補題なしでも、論文の結論が正しいことを証明できたのは、2006年になってからでした。

別のこともあった。1998年に共著で彼が発表した論文の証明に対して、「正しくない」という批判が出されます。結論的には、彼は、正しかったのですが、彼が、最終的に、自分が正しいことを確信できたのは、2013年になってからでした。

（このあたりの経緯は、"The Origins and Motivations of Univalent Foundations" https://goo.gl/LW2Wcq に、詳しく触れられています。）

ヴョブドスキーは、考えます。「数学が、累積的（accumulative）な性格を持つのなら、もしも、そこに誤りが紛れ込むと、それも、累積する可能性がある」と。

ワイルズのフェルマーの定理の1993年の証明には、誤りがあった。それが修正されたのは、1995年のことでした。どんどん複雑化して高度化する数学の「証明」の正しさをチェックするのは難しいのです。数学者の「証明」が正しいという保証はないのです！

ヴョブドスキーは、数学の証明は、コンピュータでチェックできるプログラムの形を取るべきだと主張し、実際に、それを実行してみせました。

この流れは、21世紀の数学の形式を、大きく変えていくだろうと、僕は考えています。

新しい証明のスタイル
対話型証明の想定

機械は全能になれるか？
「シンギュラリティ」論について

今から見ればだいぶ前になりますが、「AI＝人工知能」の大ブレイクが起きたとき、盛んに使われたのが「シンギュラリティ」という言葉です。機械の知能が人間の知能を超える時がいつか来る。それをこの言葉で呼んでいたように思います。ただ、この言葉やその意味に、僕はいささか「怪しさ」を感じていました。

なにが人間の知能の限界であるのか？　また、シンギュラリティの到来は、機械の知能が人間の知能をどのように超えることを意味しているのか？　当時流行した議論では、そうした基本的なことが、あまりよく考えられていないように感じました。

こうした問題を徹底的に考えるのは意味があることだと、僕は考えています。

対話型証明の「全能者」

タイトルの「全能者」は、いわば、機械の「シンギュラリティ」をはるかに超えた能力の持ち主です。ただし、「対話型証明 Interactive Proof」に登場する架空の存在です。

アーサー王伝説では、アーサーに仕えるマーリンという魔法使いが出てくるのですが、「対話型証明 Interactive Proof」では、「全能者」をマーリン、「全能者」と対話する普通の人間をアーサーと呼ぶことがあります。

アーサー王伝説のマーリンは、魔法使いですので、火を吹く竜を召喚したり、人間を豚に変えたり、文字通りなんでも出来るのですが、Interactive Proofのマーリンは、そういう魔法を使えるわけではありません。

「数学的全能者」＝「証明者」

ただ、理論的・数学的能力においては、彼は「全能」です。もし、リーマン予想が正しいのなら、彼はそれを瞬時に証明できます。もちろん、「全能」と言っても、数学的に証明不可能な 1＋1＝3 を証明できるわけではありません。彼は、「数学的全能者」なのです。

Interactive Proofの枠組みでは、「全能者 マーリン」を「証明者 Prover」と呼ぶことがあります。彼は、全知全能で、どんな問題も瞬時に答えを返す能力をもっています。

ただし、ここが重要なのですが、彼は誠実ではなく、時々、人を欺く嘘をつきます。

「証明者」と「検証者」

一方の「普通の人 アーサー」を、Interactive Proofの枠組みでは、「検証者 Verifier」と呼びます。彼の役割は「証明者」の「証明」を「検証」することです。

彼は、「証明者」のように全能ではないのですが、普通の数学者と同じ程度の数学的能力を持っていて、「証明者」の「証明」を「検証」することができます。彼は、数学的には全能の「証明者」の「証明」を盲信しません。

対話型証明の枠組み

「対話型証明 Interactive Proof」というのは、数学的能力の異なる「証明者」と「検証者」が対話をしたときに、何が分かるかを考えようという枠組みです。

基本的には、検証者が証明者の主張を受け入れた時、すなわち、証明者が証明者の主張が正しいと検証者を納得させることができた時、証明は終わります。

ただし、ある場合には、証明者の検証者の説得は失敗し、検証者は証明者の主張を拒否して、証明が終わります。

いずれの場合も、証明が正しいか否かの判断は、「証明者」の側ではなく、「検証者」が行うことに、注意してください。

対話型証明の想定

改めて、対話型証明の想定を確認しましょう。対話型証明では、次のような想定を行います。

- 証明における、「証明者」と「検証者」の役割の分離
- 「証明者」と「検証者」の「能力差」の存在を仮定する
- 両者の繰り返しの「対話」による証明の進行

こうした想定は、先に見た数学的証明をめぐる困惑するようなエピソードを整理する視点を提供しています。

Answer

Question

IP

Interactive Proof

対話型証明の最初の成功

問題は、こうしたアプローチが、現実の数学的問題の解決に、実際に役に立つのかということです。ここでは、それが、新しい認識を生み出した例を次に紹介したいと思います。

n個の頂点を持つ二つのグラフGとHがあったとします。この二つのグラフが同じものであることを証明する問題を「グラフの同型問題」といいます。この問題は、複雑性のクラスNPに属します。

ところが、二つのグラフが同じものではないことを証明する「グラフの非同型問題」は、実は、「グラフの同型問題」より難しい問題であること、すなわちその複雑性クラスはNPを超えるものであることが、Interactive Proofの手法を使って初めて証明されたのです。

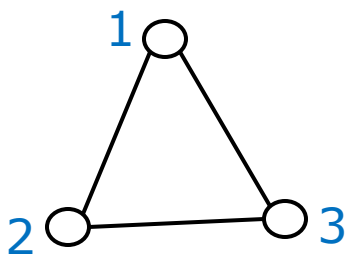
グラフの「同型問題」と「非同型問題」

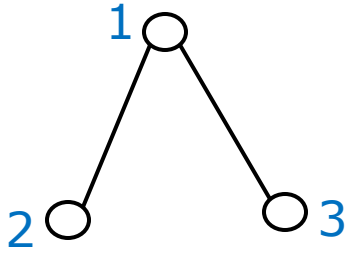
グラフの「同じ」を考える

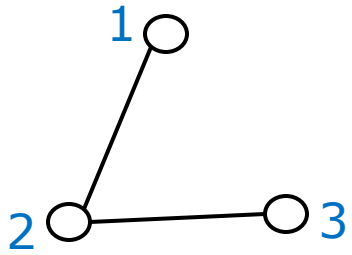
頂点と辺

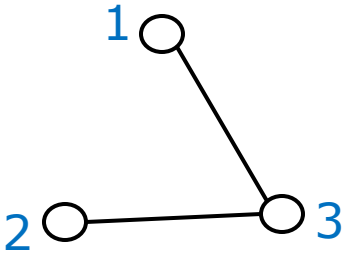
「頂点」と頂点を結んだ「辺」でできている図形を「グラフ」と言う。

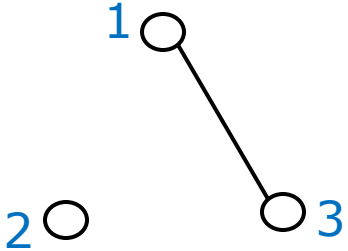
例えば、次の図形は、いずれも三つの頂点 1,2,3を持つグラフである。

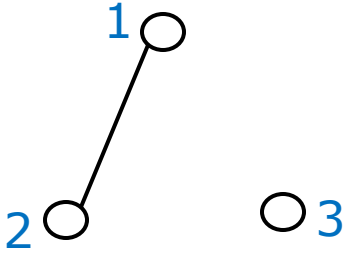






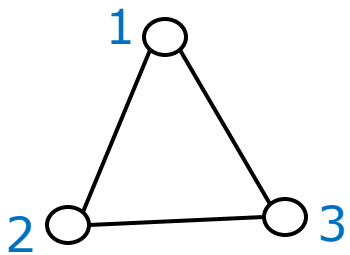


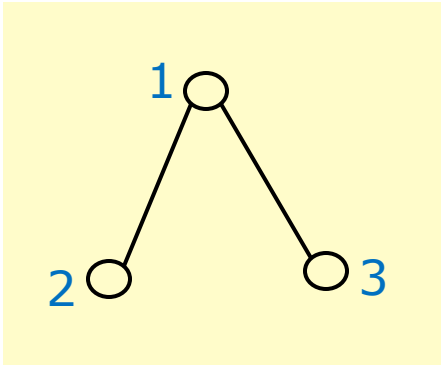


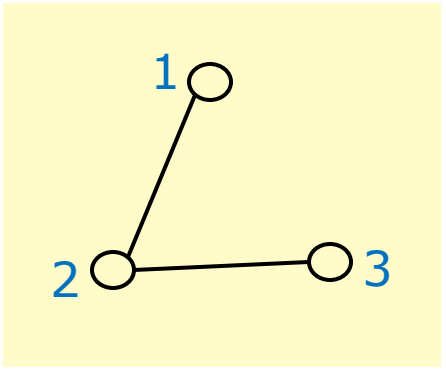


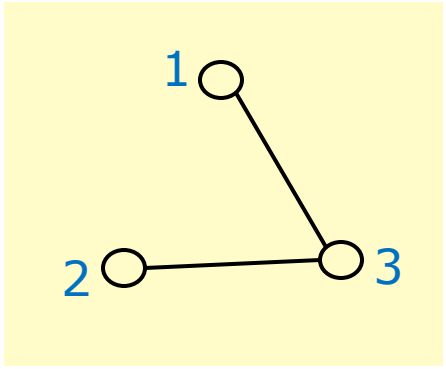
「似ている」グラフ

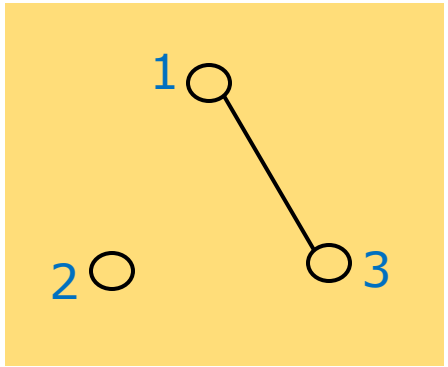
これらのグラフは、皆、見かけは違っているのだが、黄色の背景とオレンジの背景のグラフは、似ている。

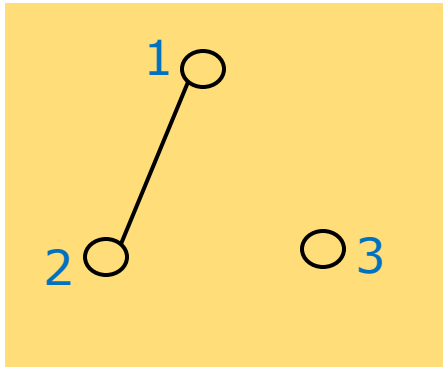






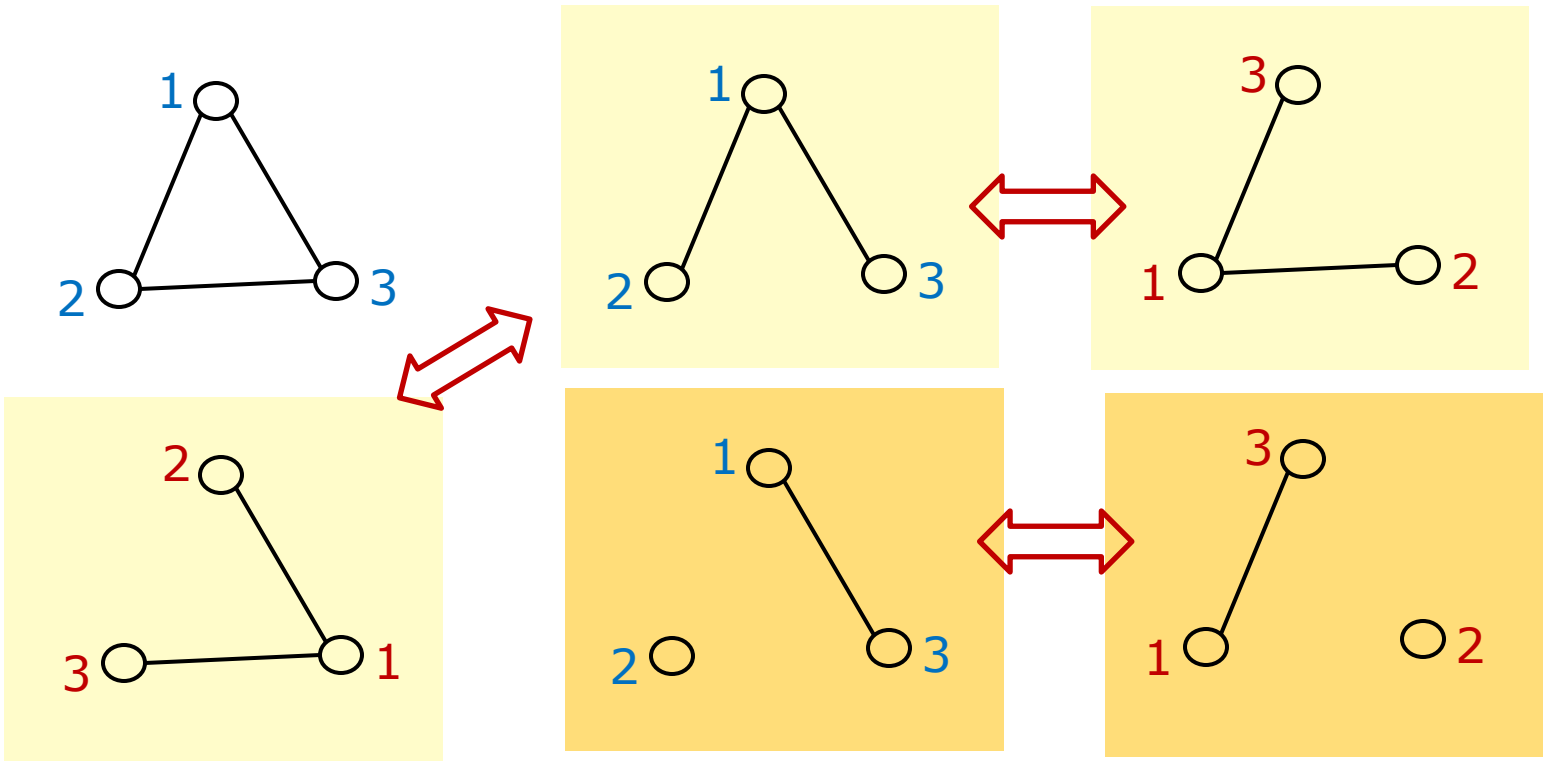






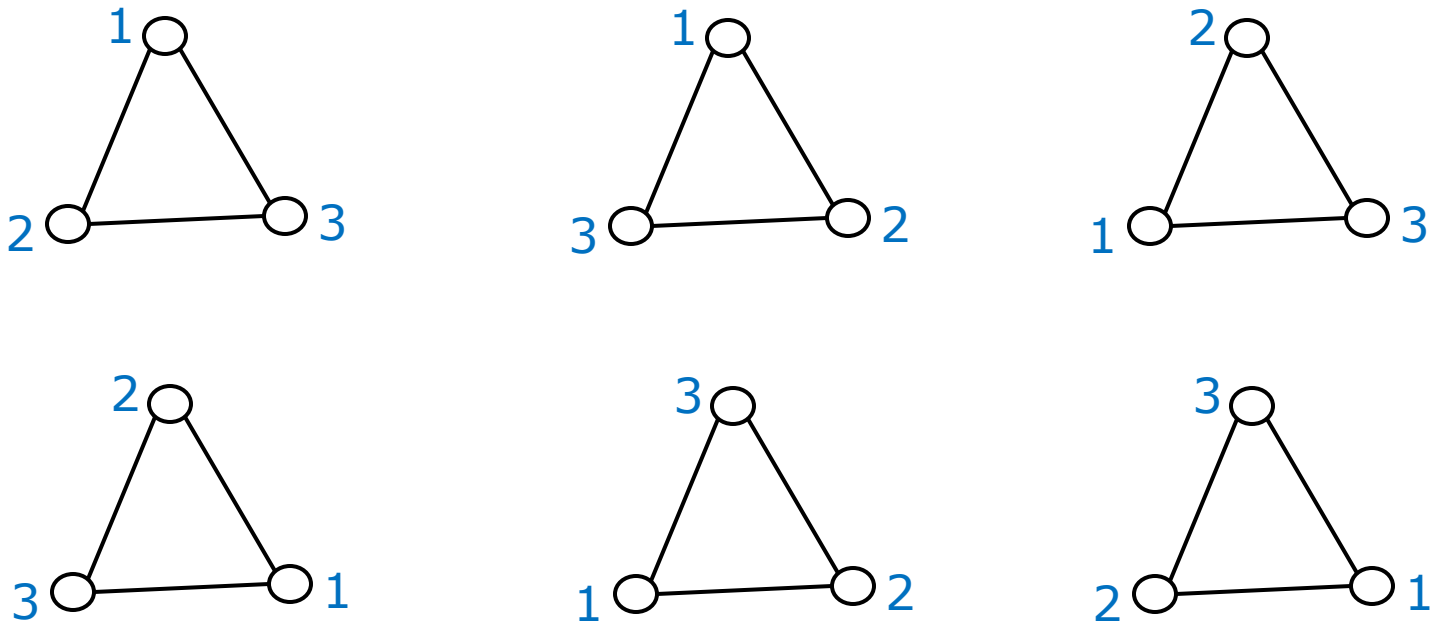
頂点の名前を付け替える

「似ている」と感じたのには理由がある。頂点の名前を付け替えると、同じグラフになるからだ。



名前を付け替えの自明な例

頂点の名前の付け替えが、グラフを「同じ」ままにすることは、次の自明な例を見ればわかる。



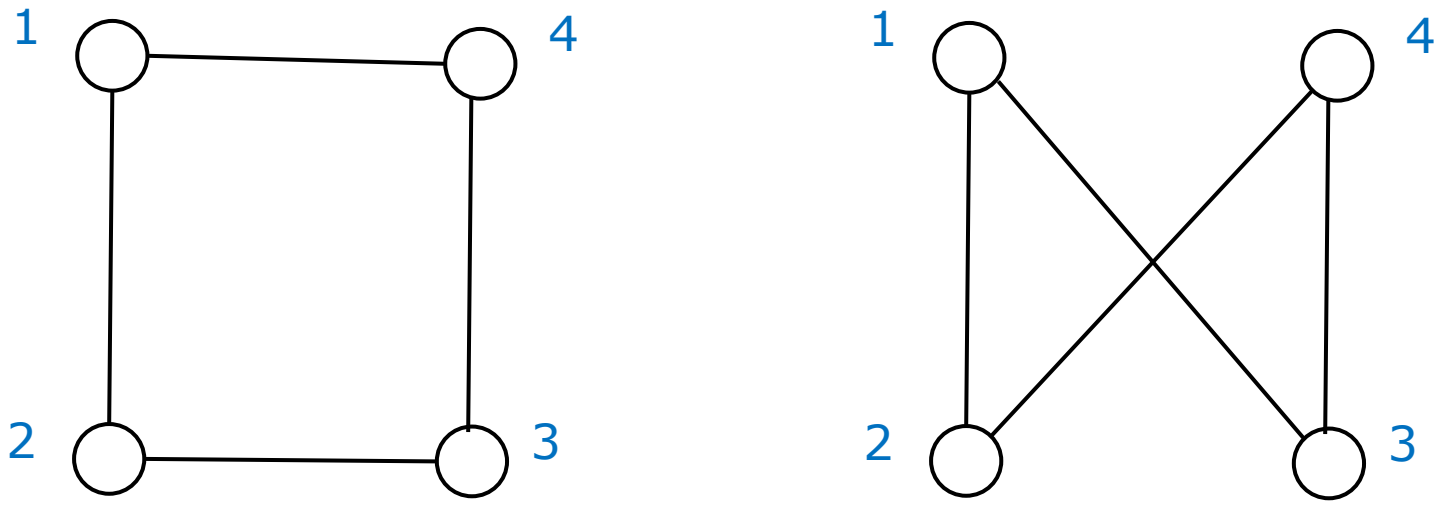
同じグラフの例 1

二つのグラフの「同じさ」にとって重要なことは、二つのグラフで頂点と頂点が一対一に対応する（これは名前の付け替えで保証される）だけでなく、一方のグラフである頂点とある頂点が結ばれていれば、他方のグラフでも対応する頂点が結ばれていることである。

同じグラフの例 1

二つのグラフの「同じさ」にとって重要なことは、二つのグラフで頂点と頂点が一対一に対応する（これは名前の付け替えで保証される）だけでなく、一方のグラフである頂点とある頂点が結ばれていれば、他方のグラフでも対応する頂点が結ばれていることである。

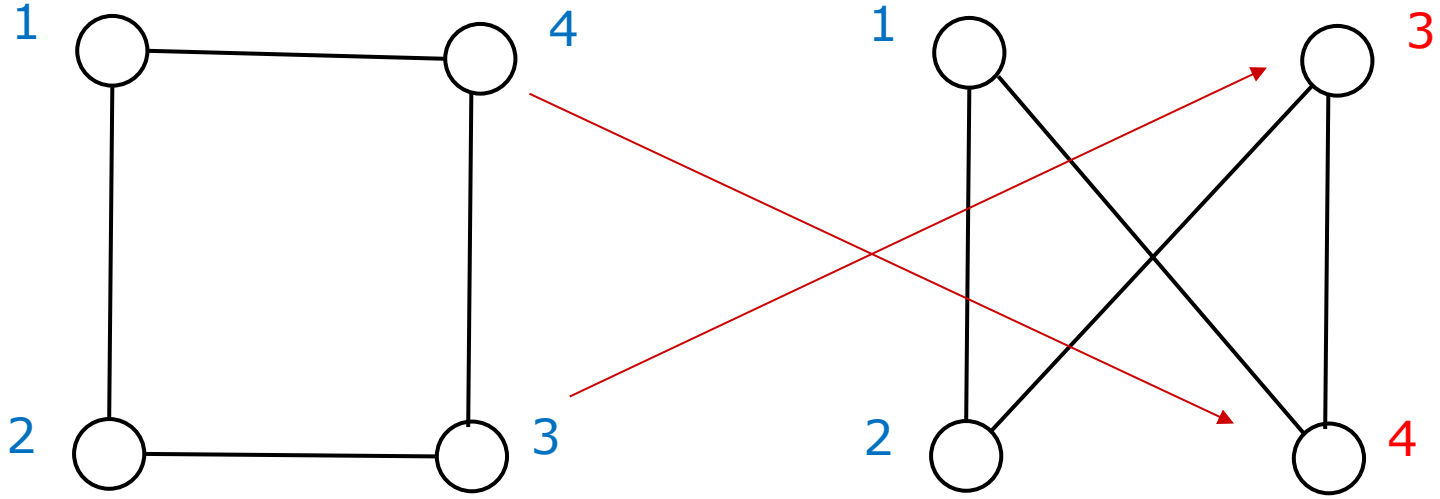
次の二つのグラフで考えてみよう。



同じグラフの例 1

左のグラフと右のグラフは、見かけは異なっているが、頂点3,4の名前を置き換えれば、左右いずれのグラフも次の条件を満たしていることがわかる。（確かめよ）

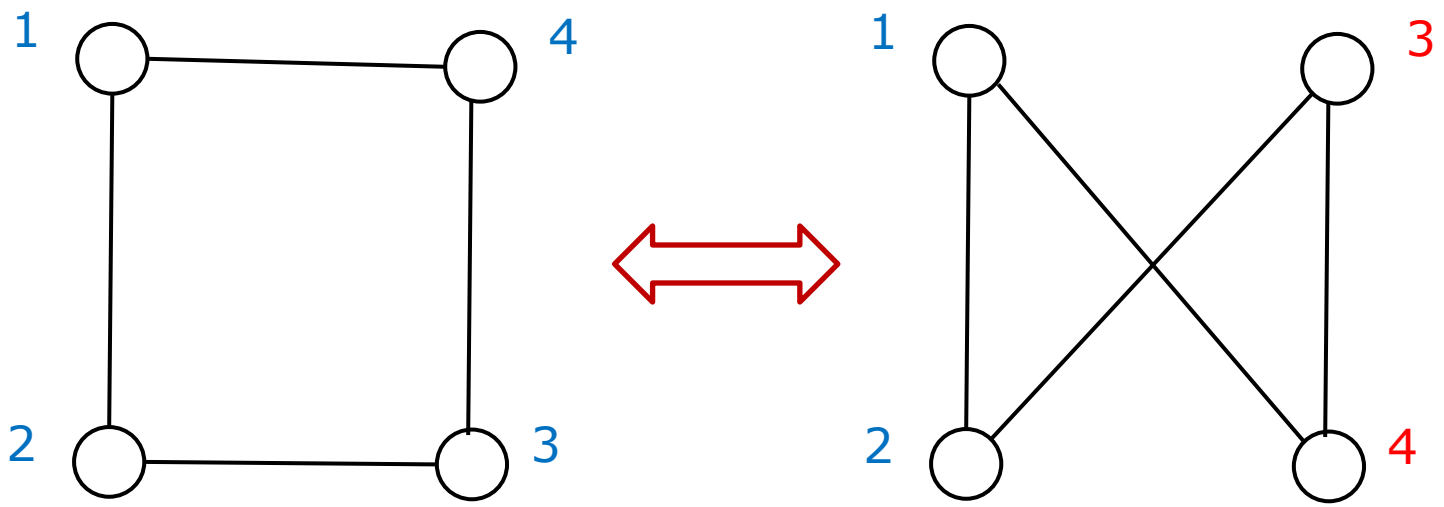
- 頂点1,2 はつながっている。
- 頂点2,3 はつながっている。
- 頂点3,4 はつながっている。
- 頂点4,1 はつながっている。



同じグラフの例 1

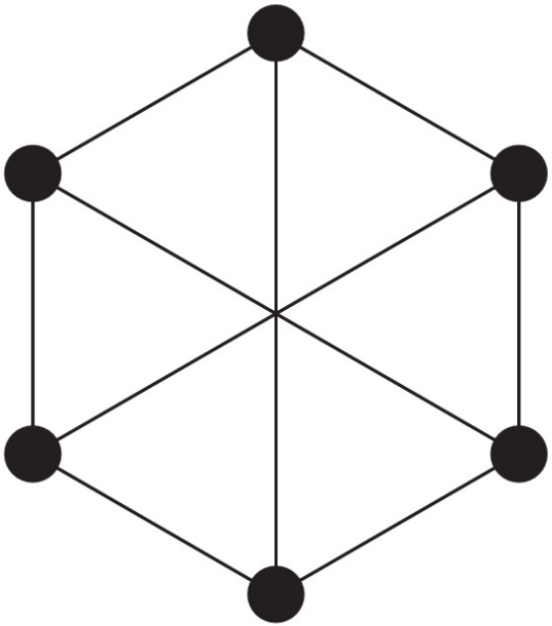
- 頂点1,2 はつながっている。
- 頂点2,3 はつながっている。
- 頂点3,4 はつながっている。
- 頂点4,1 はつながっている。

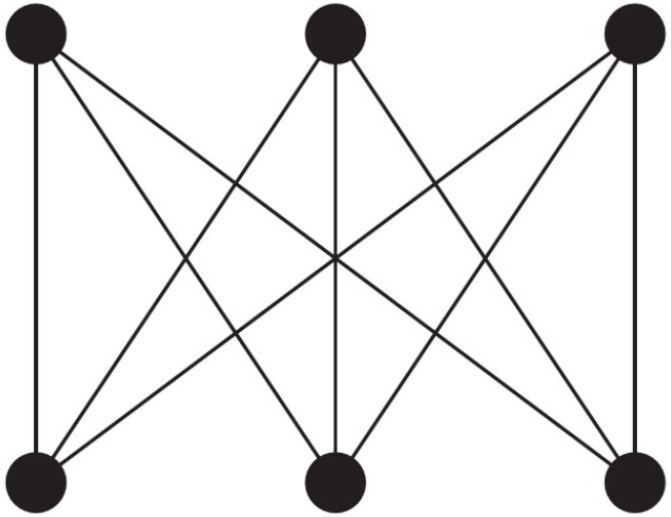
よって二つのグラフは「同じ」ものである。



同じグラフの例　2

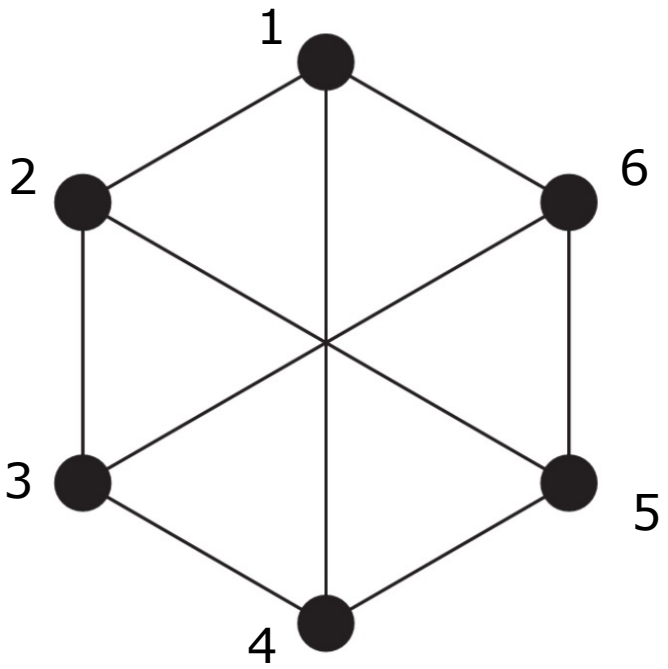
次の二つのグラフを考えてみよう。見かけは違うのだが、この二つのグラフは、「同じ」ものである。

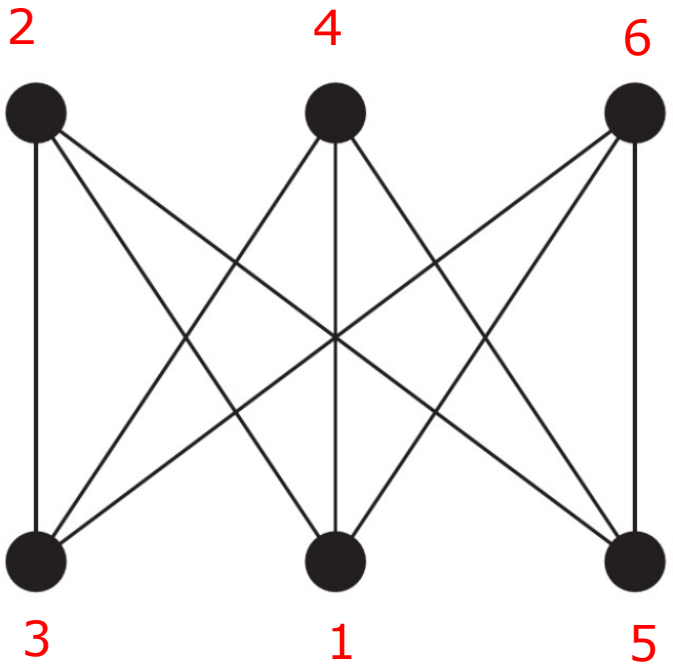




同じグラフの例　2

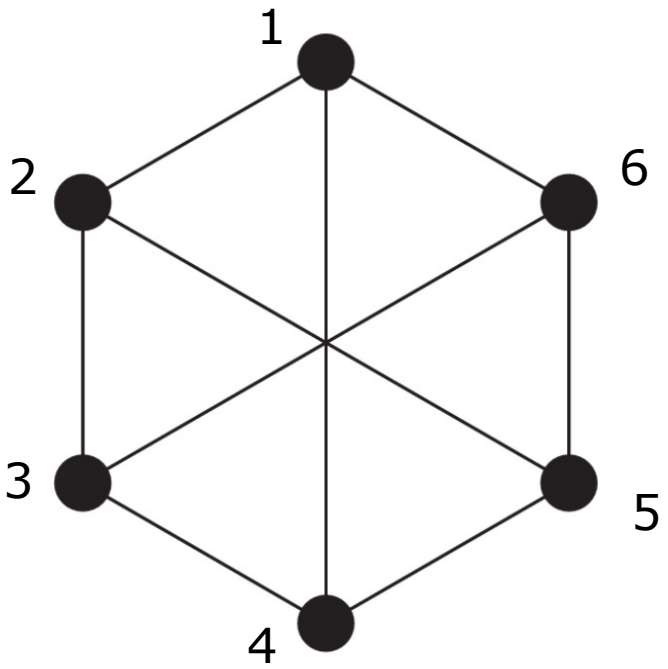
次のように6つの頂点に名前をつけよう。

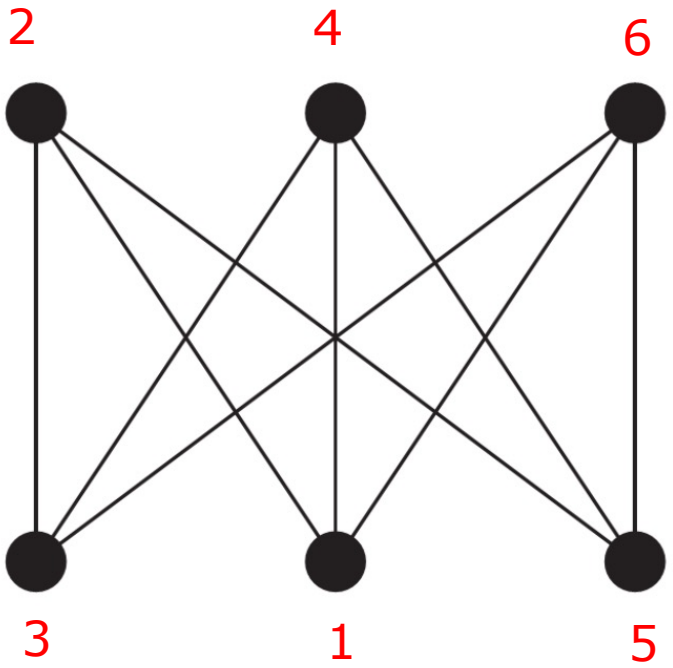




同じグラフの例　2

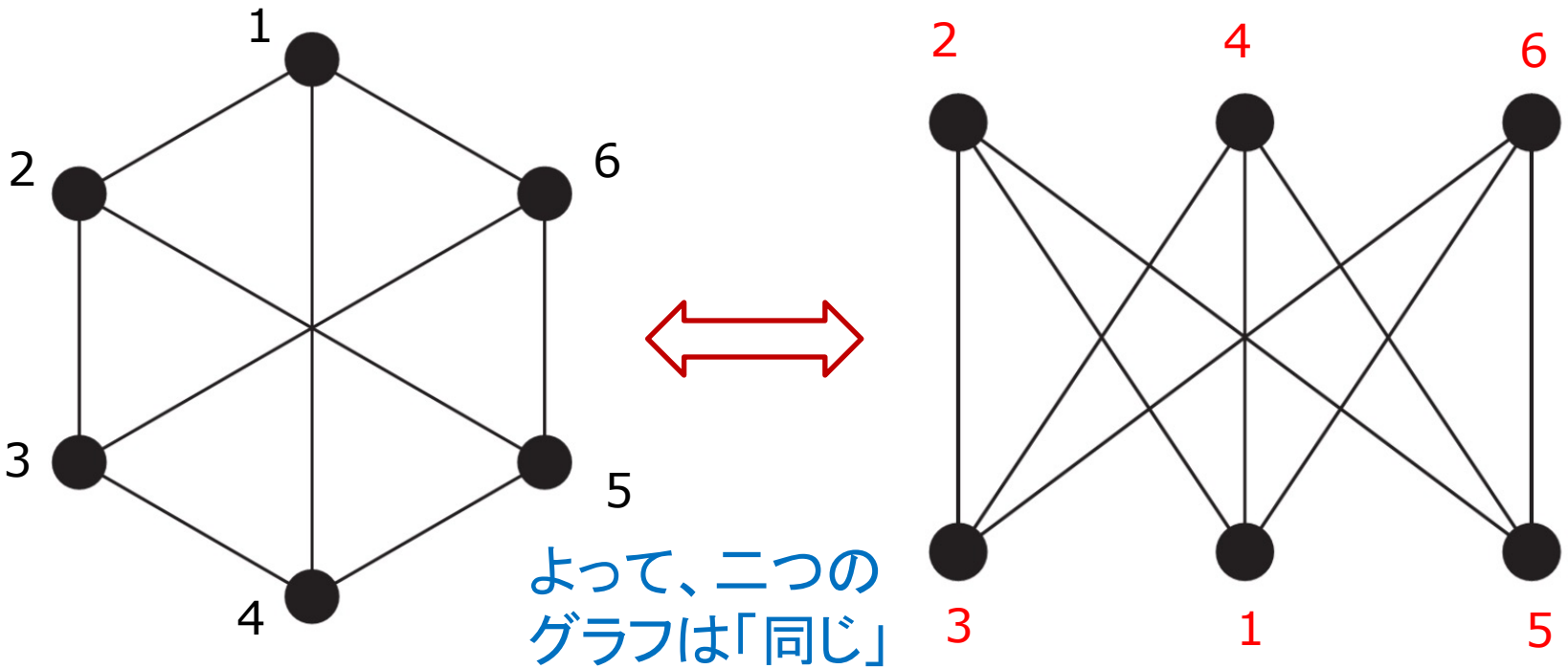
次のように6つの頂点に名前をつけよう。
この時、左右のグラフとも、頂点(1,2), (2,3), (3,4), (4,5), (5,6), (6,1), (1,4), (2,5), (3,6) はつながっている。





同じグラフの例　2

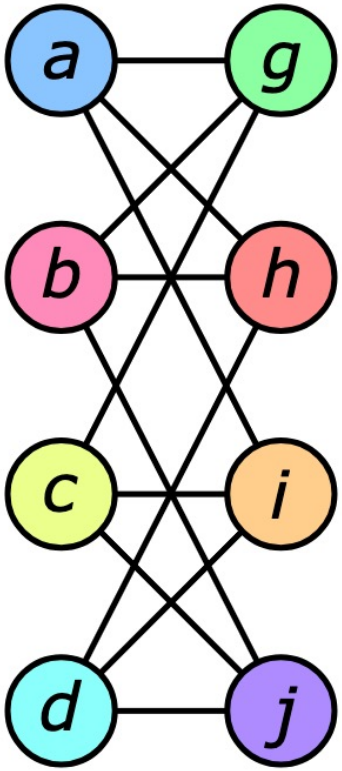
次のように6つの頂点に名前をつけよう。
この時、左右のグラフとも、頂点(1,2), (2,3), (3,4), (4,5), (5,6), (6,1), (1,4), (2,5), (3,6) はつながっている。

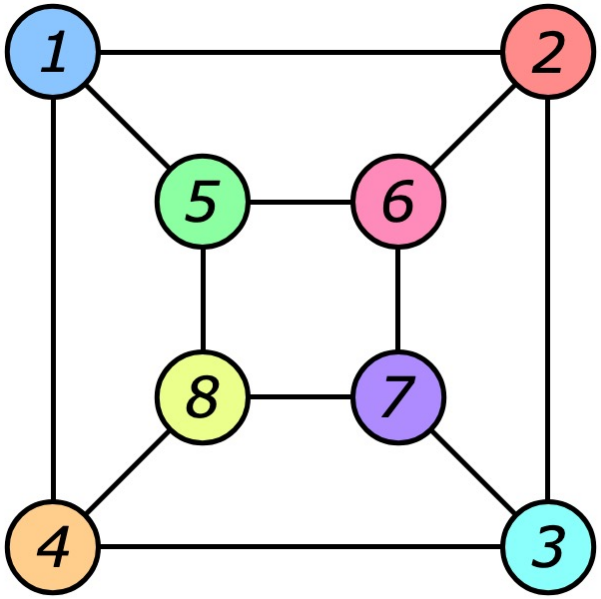


よって、二つのグラフは「同じ」である。

同じグラフの例　3

次の二つのグラフを考えてみよう。見かけは違うのだが、この二つのグラフは、「同じ」ものである。

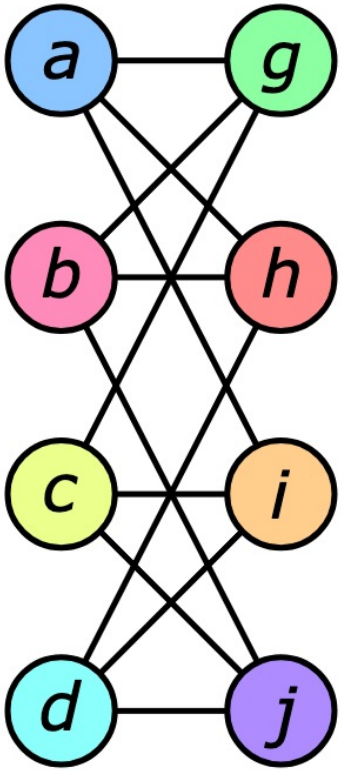


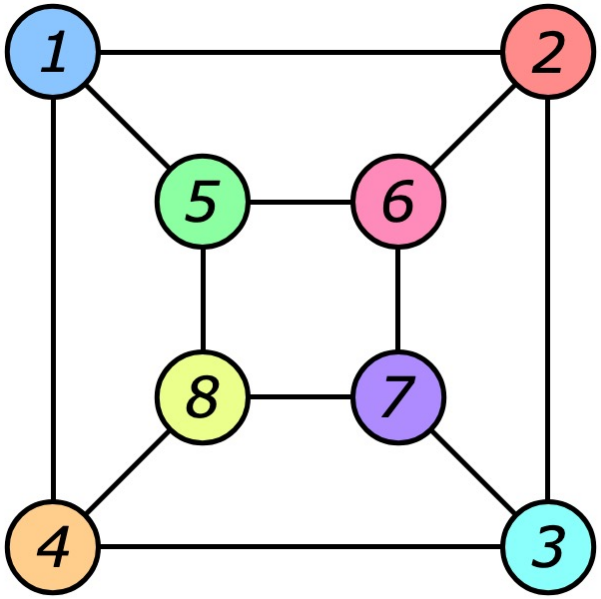


https://en.wikipedia.org/wiki/Graph_isomorphism

同じグラフの例　3

次のような名前の対応を考える





$f(a) = 1$

$f(b) = 6$

$f(c) = 8$

$f(d) = 3$

$f(g) = 5$

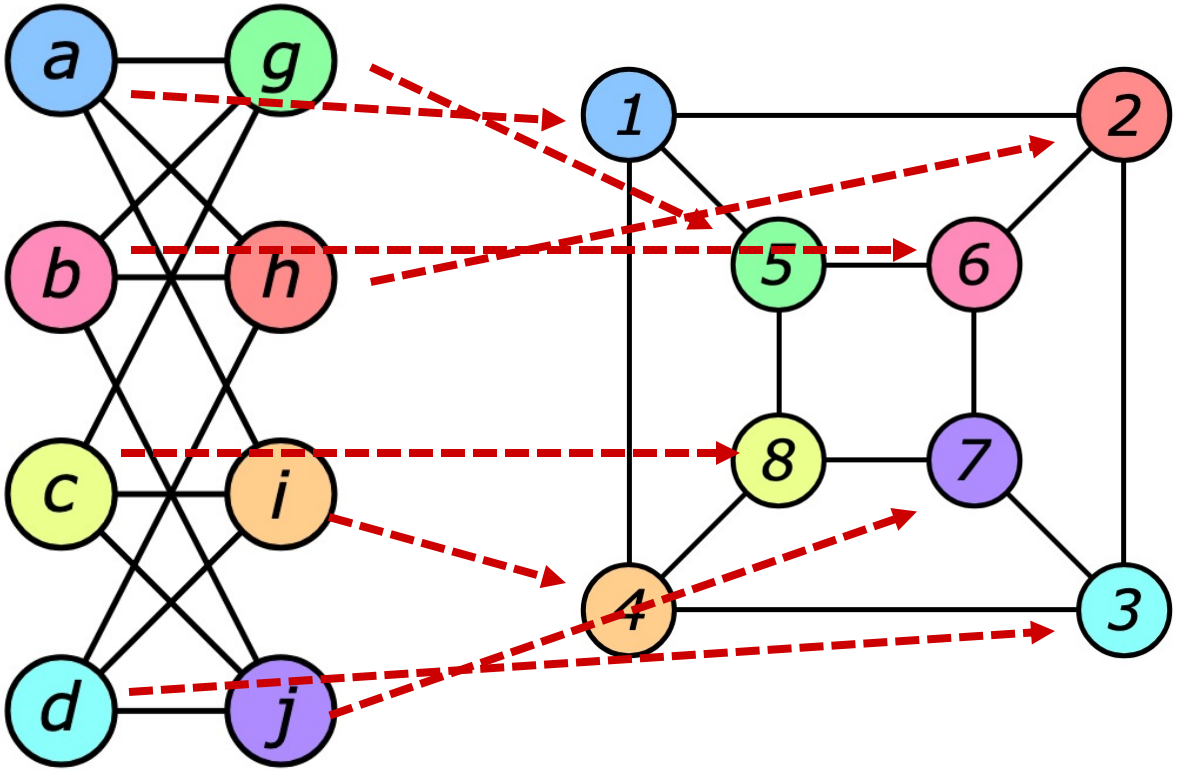
$f(h) = 2$

$f(i) = 4$

$f(j) = 7$

同じグラフの例　3

次のような名前の対応を考える



$f(a) = 1$

$f(b) = 6$

$f(c) = 8$

$f(d) = 3$

$f(g) = 5$

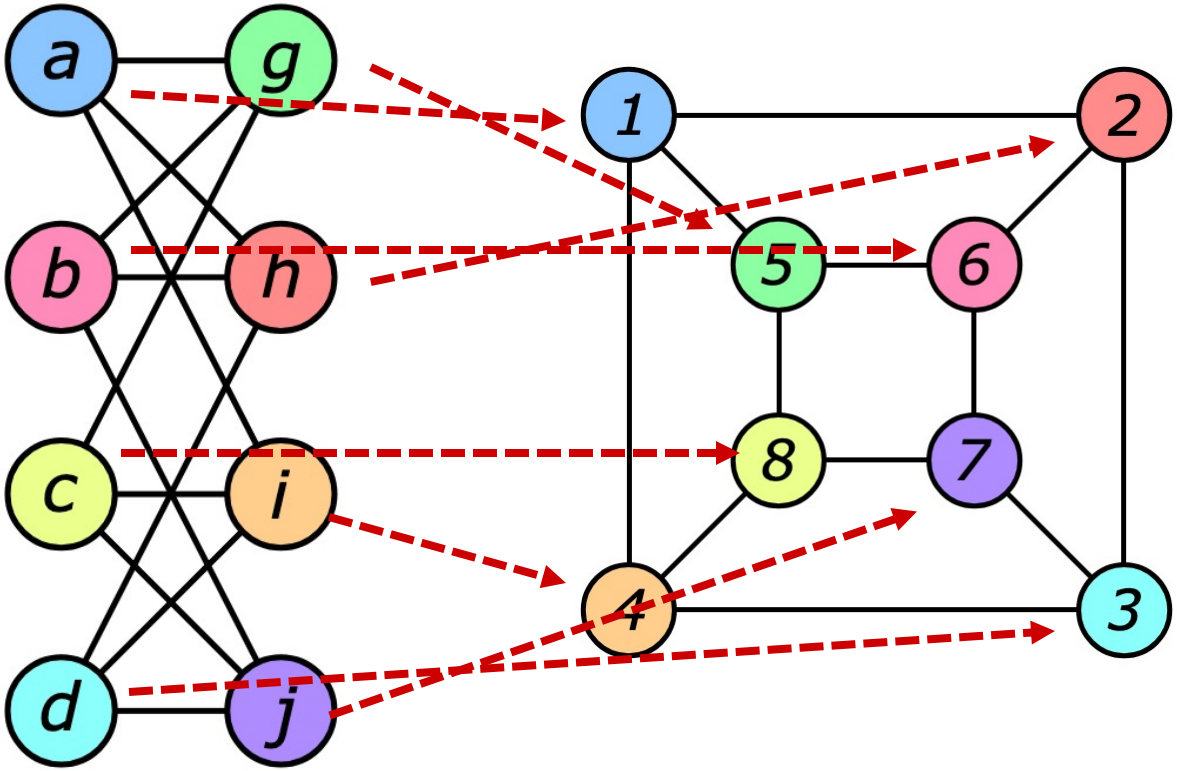
$f(h) = 2$

$f(i) = 4$

$f(j) = 7$

同じグラフの例　3

次のような名前の対応を考える



$f(a) = 1$

$f(b) = 6$

$f(c) = 8$

$f(d) = 3$

$f(g) = 5$

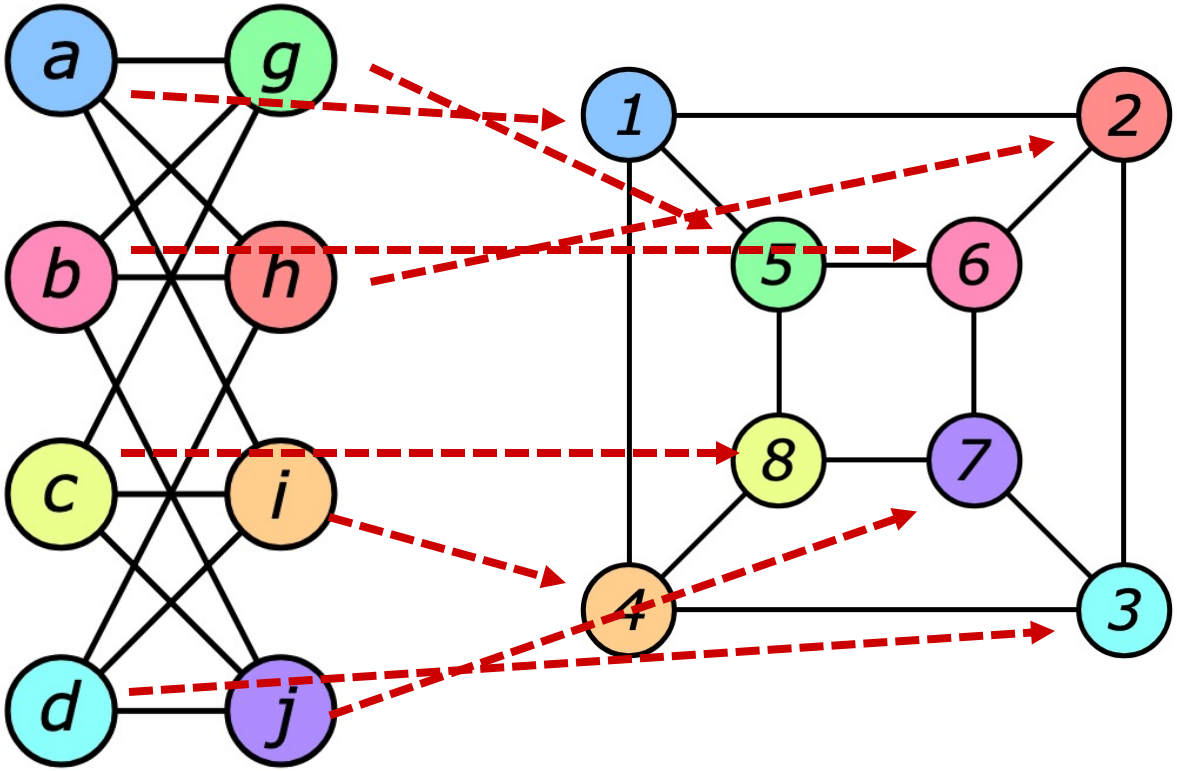
$f(h) = 2$

$f(i) = 4$

$f(j) = 7$

同じグラフの例　3

接続の対応は、(a,g)=(f(a),f(g))=(1,5)。同様に、
(a,h)=(1,2);(a,i)=(1,4);(b,g)=(6,5);(b,h)=(6,2);
(b,j)=(6,7);(c,g)=(8,5);(c,i)=(8,4);(c,j)=(8,7);
(d,h)=(3,2);(d,i)=(3,4);(d,h)=(3,4)



$f(a) = 1$

$f(b) = 6$

$f(c) = 8$

$f(d) = 3$

$f(g) = 5$

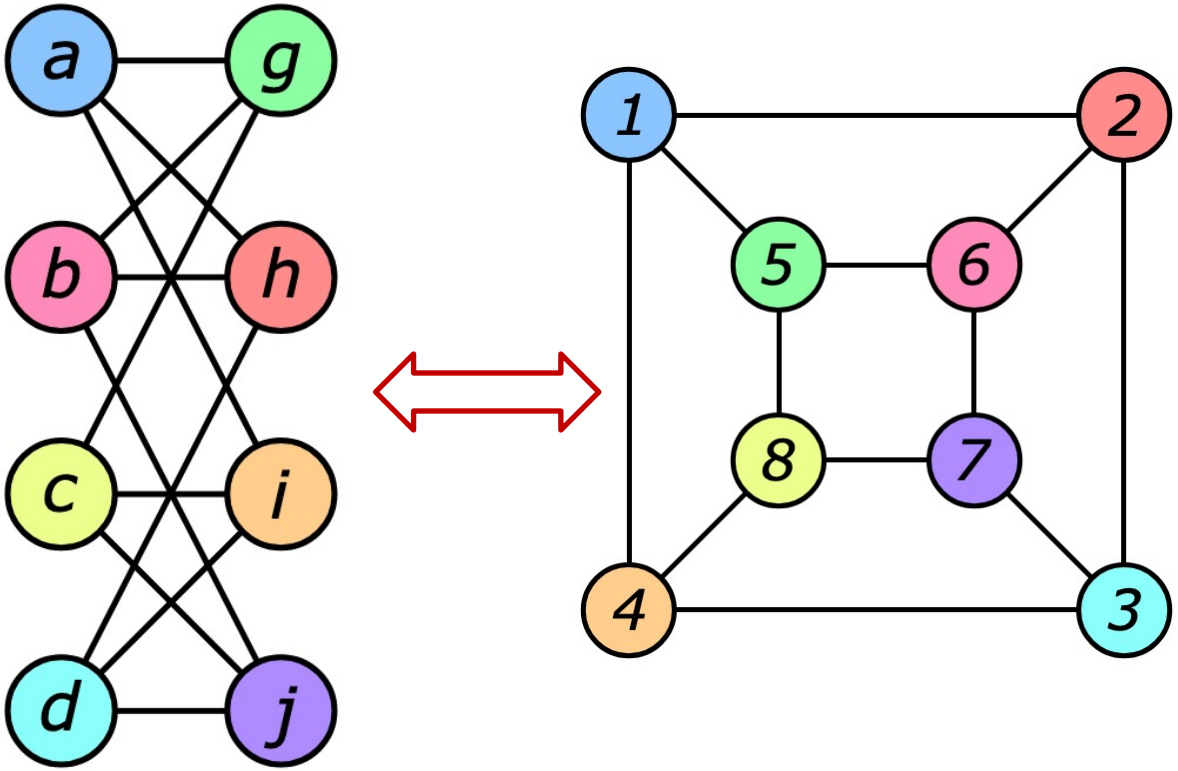
$f(h) = 2$

$f(i) = 4$

$f(j) = 7$

同じグラフの例　3

左右のグラフの頂点のつながりは一致する。
左右のグラフは、「同じ」ものである。



$f(a) = 1$

$f(b) = 6$

$f(c) = 8$

$f(d) = 3$

$f(g) = 5$

$f(h) = 2$

$f(i) = 4$

$f(j) = 7$

グラフの同型性の定義
Graph isomorphism

グラフの同型性の定義

次の条件を全て満たす時、グラフGとグラフHは同型であると言う。

1. グラフGとグラフHの頂点の数は等しい。
2. グラフGの頂点V_GとグラフHの頂点V_Hを一対一に対応させる関数 f が存在する。
3. グラフGの頂点 i, j がつながっているならば（頂点iと頂点jをつなぐ辺があると言うこと）、これらのグラフGの頂点に対応するグラフHの頂点も(f(i), f(j)とあらわすことが出来る)、つながっている。

グラフの同型性チェックのために必要な場合の数

次の条件を全て満たす時、グラフGとグラフHは同型であると言う。
どれくらいの場合の数のチェックが必要か見ておこう。

1. グラフGとグラフHの頂点の数を nとする。
2. グラフGの頂点V_GとグラフHの頂点V_Hを一対一に対応させる関数 f が存在する。こうした fは、n! 個存在する。
3. グラフの頂点 i, j がつながっている c(i,j) = 1、つながっていないならば、c(i,j)=0 という関数を考える。先の条件は、c(i,j)=c(f(i),f(j)) と表せる。
   0,1に値をとる関数cは、何個存在するだろうか？
   c(i,j) の引数部分 i,j の可能な組み合わせは、n^2 個ある。
   よって、0,1 二つの値に値をとる 関数c(i,j) ->{0.1}は、2^{n^2}個だけ存在する。

Graph Isomorphismの複雑性クラス

グラフGとグラフHの間で、頂点の対応を表す f: $V_G \vdash V_H$ と、辺の対応を表す c(i,j)→{0,1}が与えられれば、グラフGとグラフHの同型性は、多項式時間でチェックできる。

だから、Graph Isomorphizmの複雑性クラスは NPに属することは明らかである。

ただ、それがPに属するのかは不明だし、NP-完全かもよくわかっていない。

cf. László Babai "Graph Isomorphism"
January 9, 2017
https://people.cs.uchicago.edu/~laci/update.html

頂点の置換とグラフの同型性

前回見た、グラフの同型性の定義

前回は、グラフの同型性の定義として次のような定義を考えた。
ただ、この定義は、少し冗長である。
例えば、明らかに、1. の条件は、2. の条件に含まれている。

1. グラフGとグラフHの頂点の数は等しい。
2. グラフGの頂点V_GとグラフHの頂点V_Hを一対一に対応させる関数 f が存在する。
3. グラフGの頂点 i, j がつながっているならば（頂点iと頂点jをつなぐ辺があると言うこと）、これらのグラフGの頂点に対応するグラフHの頂点も(f(i), f(j)とあらわすことが出来る)、つながっている。

改めて、グラフの同型性を定義する

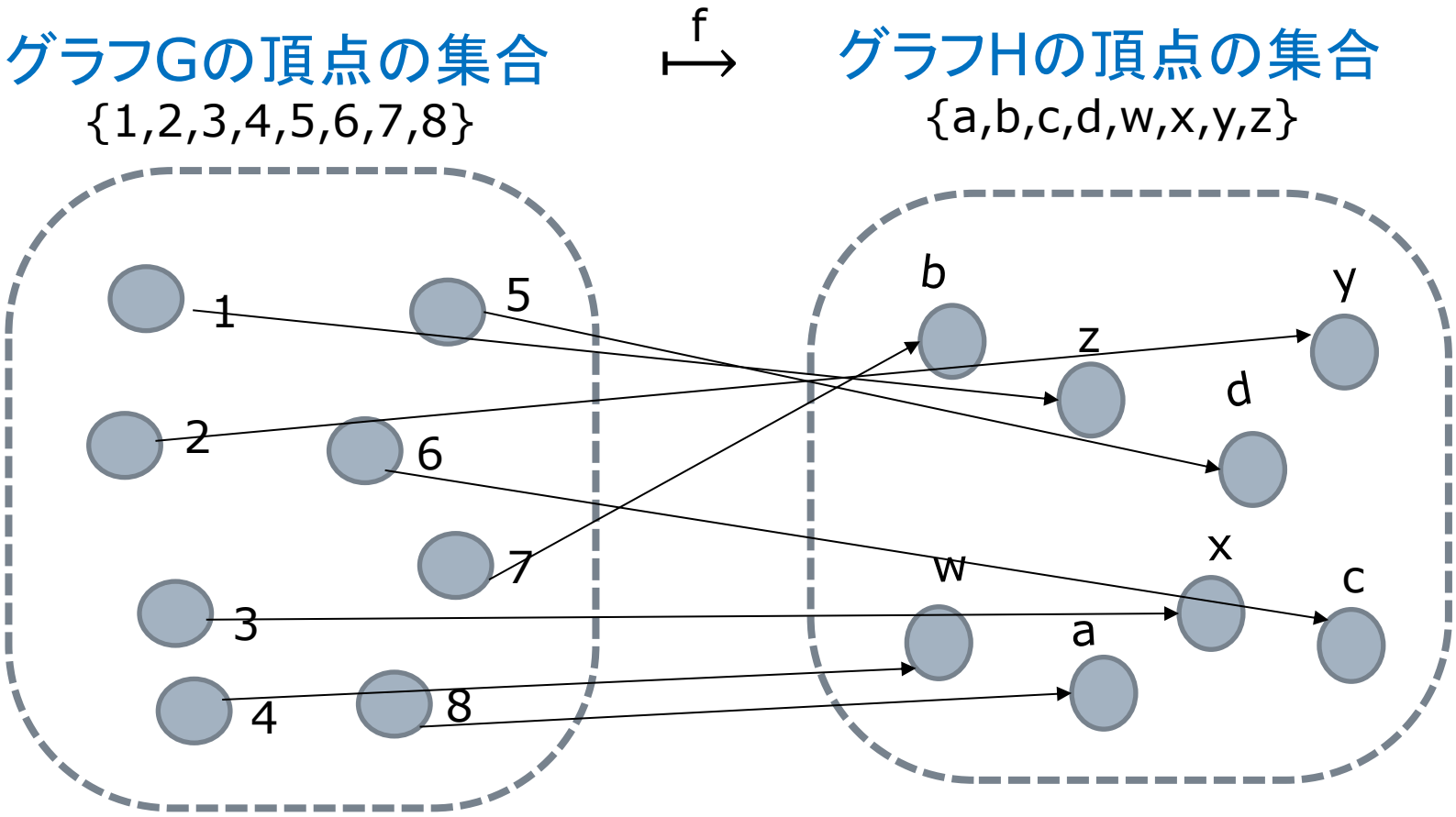
先の条件 2. はグラフの頂点についての条件で、条件 3. はグラフの辺についての条件である。もう少し整理しよう。

辺については、グラフの頂点 i, j をつなぐ辺があることを c(i,j)＝1、辺がないことを c(i,j)＝0 で表すことにしよう。

グラフG,Hが同型である条件は、

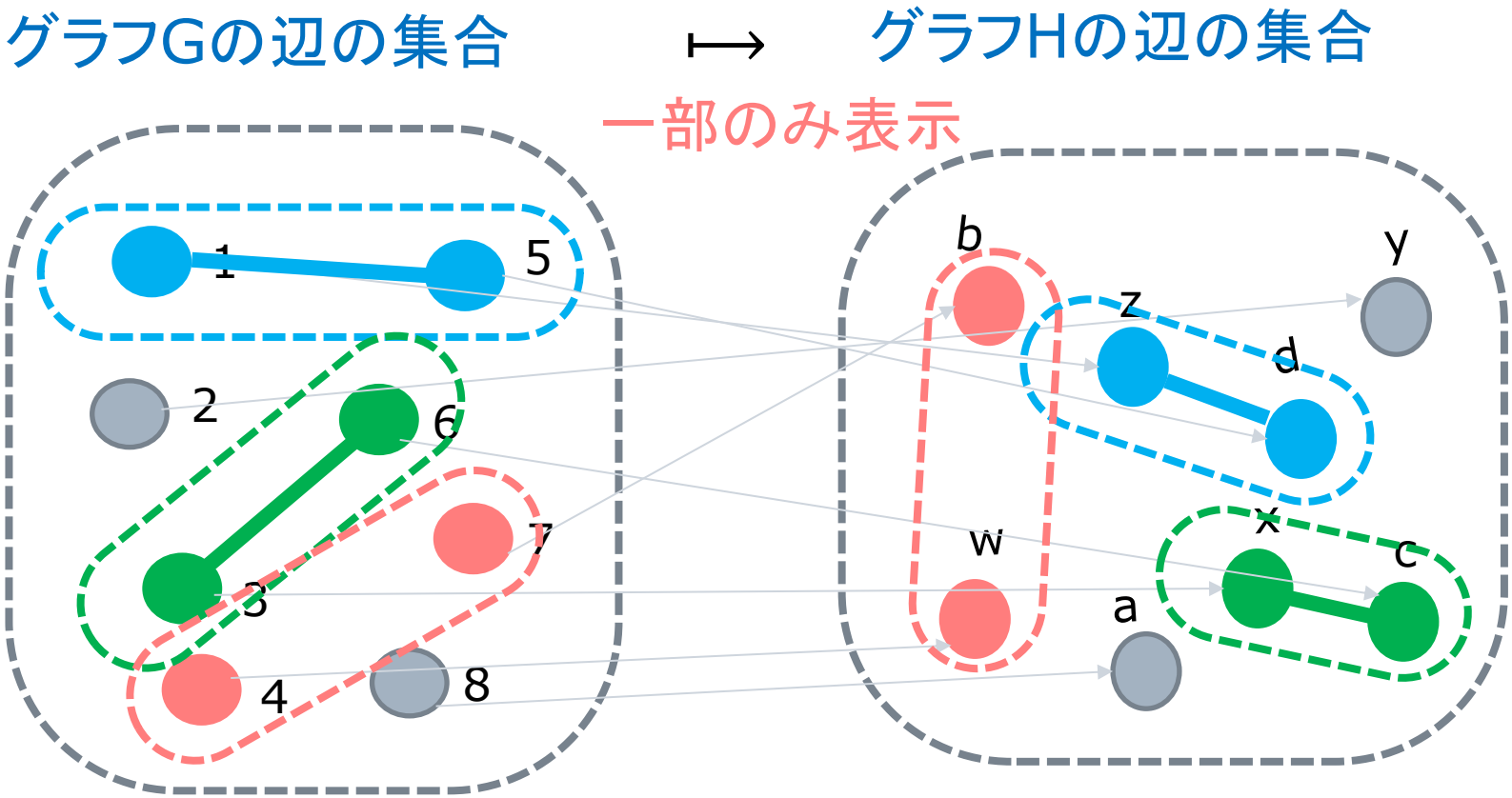
1. グラフGの頂点をグラフHの頂点に一対一に対応させる関数 f が存在する。
2. 頂点の対応 fが与えられれば、グラフGの辺はグラフHの辺に次の式で、一対一で対応する。　c(i,j)＝c(f(i),f(j))
   こうした時、対応 fは、グラフの辺を保存するという。

グラフGの頂点をグラフHの頂点に一対一に対応させる関数 f が存在する。



f(1)=z, f(2)=y, f(3)=x, f(4)=w
f(5)=d, f(6)=c, f(7)=b, f(8)=a

頂点の対応 fが与えられれば、グラフGの辺はグラフHの辺に次の式で、一対一で対応する。　c(i,j)=c(f(i),f(j))



c(1,5)=c(f(1),f(5))=c(d,z)=1 ;辺あり
c(3,6)=c(f(3),f(6))=c(x,c)=1 ;辺あり
c(4,7)=c(f(4),f(7))=c(w,b)=0 ;辺なし

グラフの頂点に自然数 1,2,…,n で名前をつける

グラフGのn個の頂点に自然数 1,2,…,n で名前をつけることにしよう。グラフHのn個の頂点も、同様に自然数 1,2,…,n で名前をつけることにしよう。

頂点の置換

グラフGのn個の頂点に自然数 1,2,…,n で名前をつけることにしよう。グラフHのn個の頂点も、同様に自然数 1,2,…,n で名前をつけることにしよう。

この時、グラフGの頂点をグラフHの頂点に一対一に対応させる関数 f は、{1,2,..,n}上で定義され{1,2,..,n}に値を持つ関数である。こうした関数を{1,2,..,n}の「置換」と呼ぶ。
（「置換 permutation」である）

頂点の置換

グラフGのn個の頂点に自然数 1,2,…,n で名前をつけることにしよう。グラフHのn個の頂点も、同様に自然数 1,2,…,n で名前をつけることにしよう。

この時、グラフGの頂点をグラフHの頂点に一対一に対応させる関数 f は、{1,2,..,n}上で定義され{1,2,..,n}に値を持つ関数である。こうした関数を{1,2,..,n}の「置換」と呼ぶ。
(「置換 permutation」である)

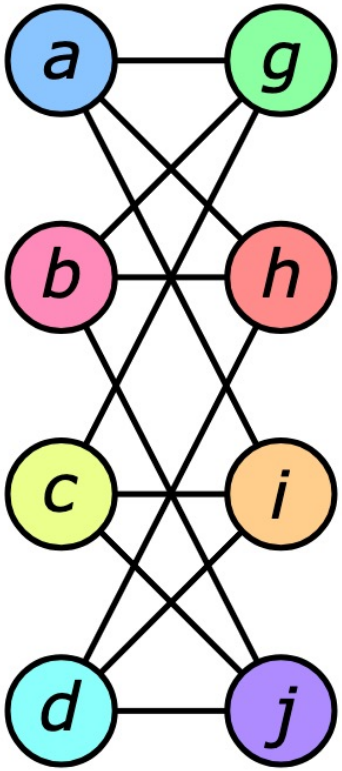
次は、{1,2,3} の置換の例である。
{1,2,3},{1,3,2},{2,3,1},{2,1,3},{3,1,2},{3,2,1}

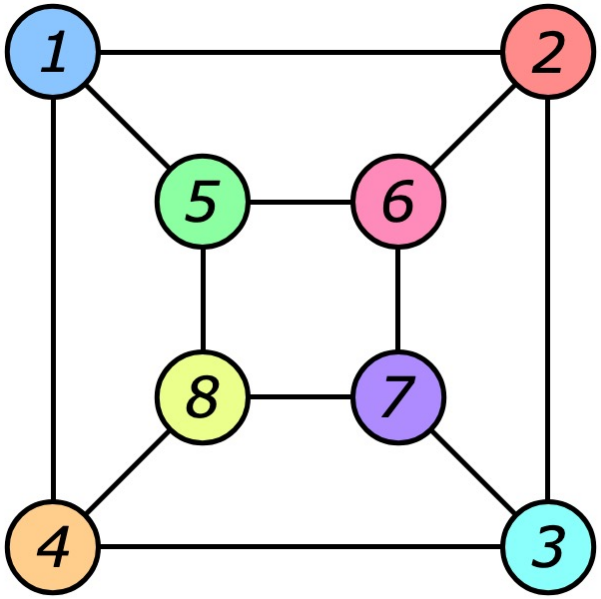
{1,2,3}->{1,3,2}->{2,3,1}->

{2,1,3}->{3,1,2}->{3,2,1}->{1,2,3}

前回見た例

前回このような名前をを持つ二つのグラフをみたが、左のグラフの名前を自然数に付け替えよう。





$f(a) = 1$

$f(b) = 6$

$f(c) = 8$

$f(d) = 3$

$f(g) = 5$

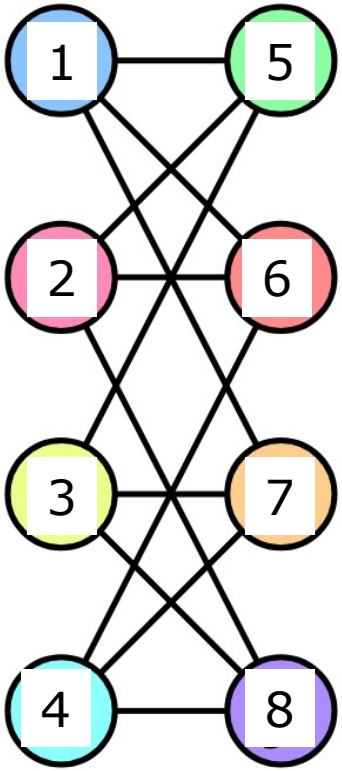
$f(h) = 2$

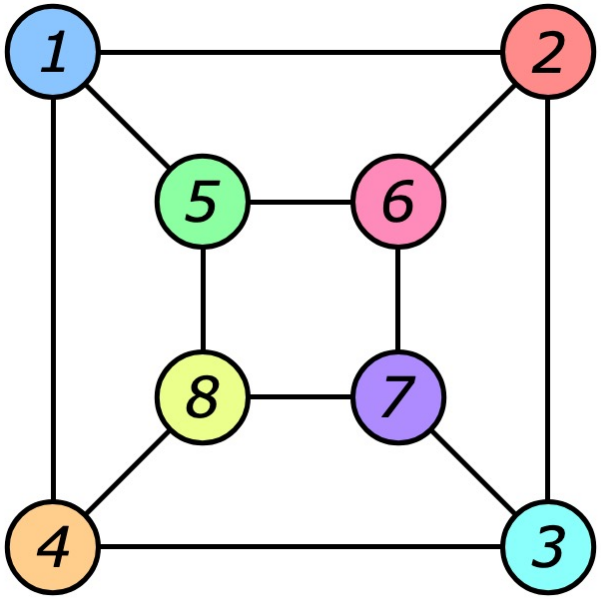
$f(i) = 4$

$f(j) = 7$

前回見た例の名前の付け替え

左のグラフ頂点の名前を{1,2,3,4,5,6}に付け替えよう。
fの定義も、このように変更される。





f(1) = 1

f(2) = 6

f(3) = 8

f(4) = 3

f(5) = 5

f(6) = 2

f(7) = 4

f(8) = 7

置換の表現

右のような、{1,2,3,4,5,6,7,8}の置換 fが与えられた時、置換fを、次のように表す。

f(1) = 1

f(2) = 6

f(3) = 8

f(4) = 3

f(5) = 5

f(6) = 2

f(7) = 4

f(8) = 7

置換の表現

右のような、{1,2,3,4,5,6,7,8}の置換 fが与えられた時、置換fを、次のように表す。

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 6 & 8 & 3 & 5 & 2 & 4 & 7 \end{bmatrix}$$

f(1) = 1
f(2) = 6
f(3) = 8
f(4) = 3
f(5) = 5
f(6) = 2
f(7) = 4
f(8) = 7

これは、f が次のような関数であることを表している。

1 2 3 4 5 6 7 8
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
1 6 8 3 5 2 4 7

まぎれがなければ、置換 fを次のように表しても構わない。

(1 6 8 3 5 2 4 7)

頂点の置換とグラフの同型性

グラフGの頂点{1,2,..n}と辺の情報を与えるc(i,j)が与えられているとする。頂点の置換の一つを fとすると、fを頂点として、c(f(i),f(j))で定義される辺を持つグラフHは、Gと同型である。

グラフHの頂点がGの頂点の置換 fであり、この置換fが辺を保存するなら(c(i,j)=c(f(i),f(j))なら)、グラフGとグラフHは同型である。

グラフGとグラフHが同型なら、GとHの間に辺を保存する頂点の置換が存在する。

グラフGの頂点を置換して、Gと同型のグラフHを作ることが出来る。辺の保存の条件は自然に導入できる。

対話型証明の最初の成功

Interactive Proofから見る
グラフの非同型性

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が与えられた時、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。これを「グラフの非同型問題」という。

グラフの「同型問題」は、「グラフG_0とG_1は同型である」という証明が与えられた時、その証明が正しいことの検証は簡単にできる。証明が与える「頂点と頂点の対応、辺と辺の対応」をチェックすればよい。グラフの「同型問題」は、NP問題である。

ところが、「グラフの非同型問題」については、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、この問題が、NPに属するかは、よくわからない。

Interactive Proofのスタイルで グラフの非同型問題を考える

ここでは、次のようなInteractive Proofのプロトコルで、グラフの非同型問題を考える。

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

グラフG_0とG_1が与えられた時、
G_0とG_1が同型でないことを
証明せよ

Question

Answer

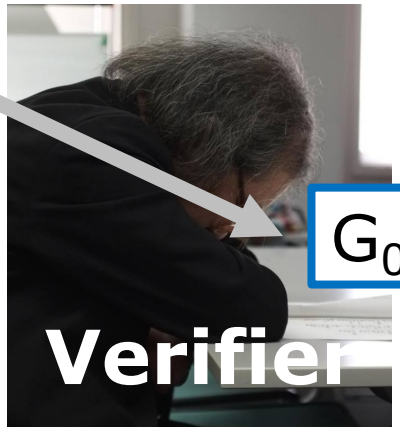
グラフの非同型問題

STEP 0

グラフG_0とG_1を、Proverと
Verifierの双方に送る。

G_0, G_1

G_0, G_1



G_0, G_1

グラフの非同型問題

STEP 1

Verifierは、G_0, G_1の頂点をランダムに置換してG_0, G_1と同型のH_0, H_1を生成する。

G_0, G_1

$G_0 \Rightarrow H_0$

$G_1 \Rightarrow H_1$

$H_0 \cong G_0$

$H_1 \cong G_1$

G_0, G_1

グラフの非同型問題

STEP 2

Verifierは、H_0, H_1のいづれか一方を選んで、それをHとしてProver に送る。
$H_0 \cong G_0$, $H_1 \cong G_1$ である。

G_0, G_1

H

$H_0 \cong G_0$
$H_1 \cong G_1$

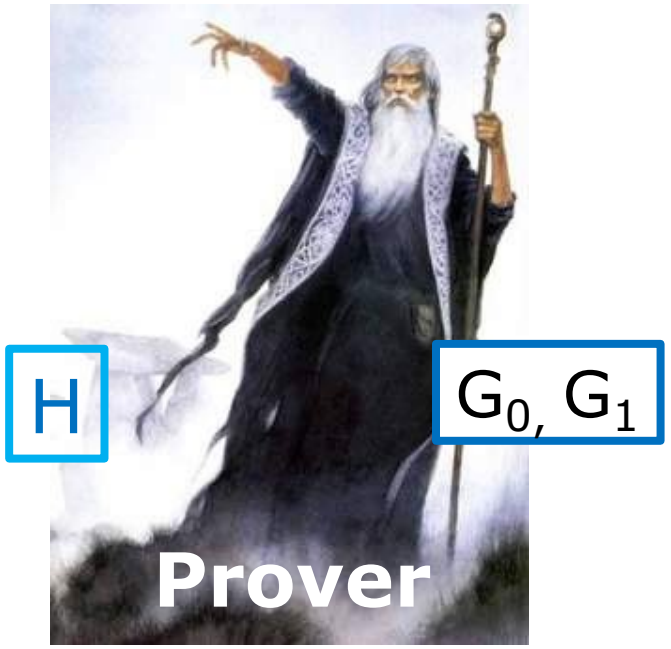
G_0, G_1

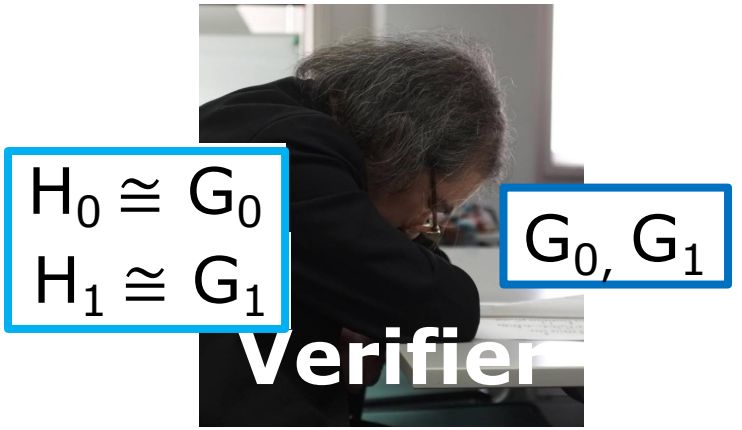
グラフの非同型問題

STEP 2

Verifierは、H_0, H_1のいづれか
一方を選んで、それをHとして
Prover に送る。
$H_0 \cong G_0$, $H_1 \cong G_1$ である。

Verifierは、どのH_iをHとして
送ったのか i を記憶しておく。





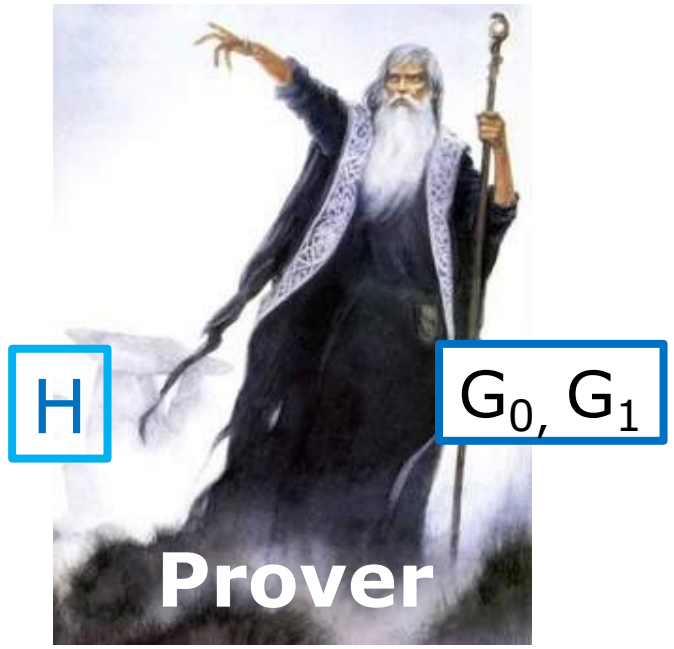
グラフの非同型問題

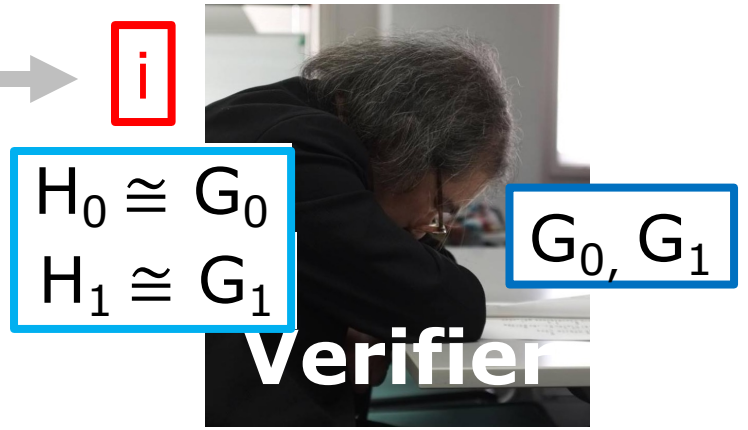
STEP 2

Verifierは、H_0, H_1のいづれか
一方を選んで、それをHとして
Prover に送る。
$H_0 \cong G_0$, $H_1 \cong G_1$ である。

Verifierは、どのH_iをHとして
送ったのか i を記憶しておく。

H=H_0なら i=0 を、
H=H_1なら i=1 を記憶する。

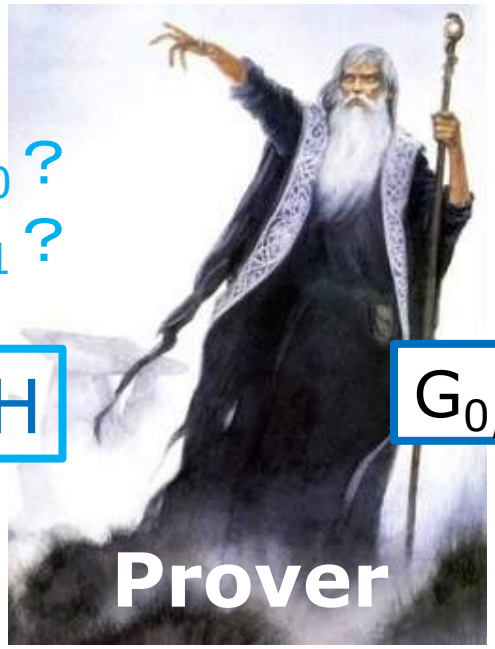


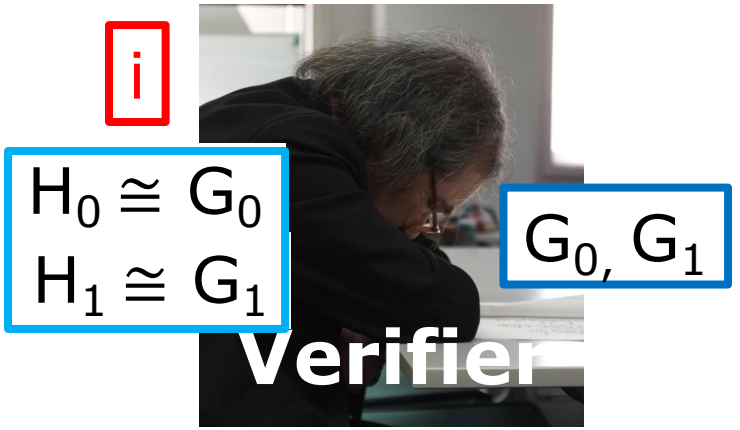


グラフの非同型問題

STEP 3

Proverは、送られたHについて、
$H \cong G_0$ であるか、あるいは、
$H \cong G_1$ であるかを判断する。

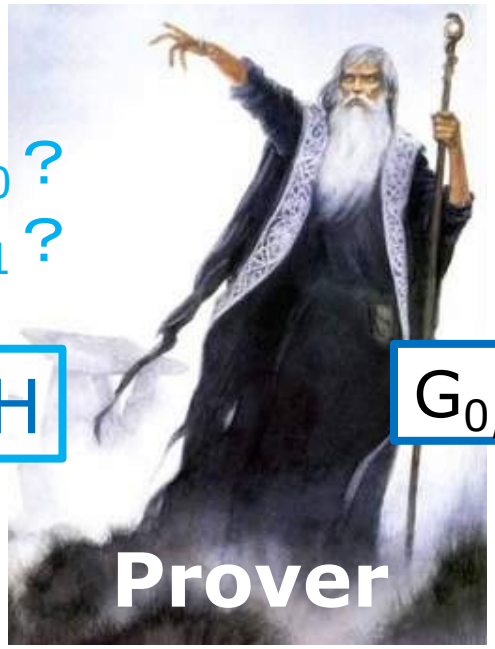


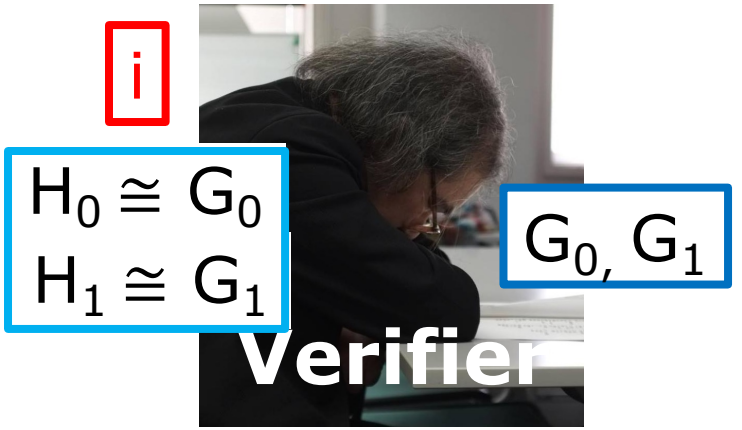


グラフの非同型問題

STEP 3

Proverは、送られたHについて、
$H \cong G_0$ であるか、あるいは、
$H \cong G_1$ であるかを判断する。



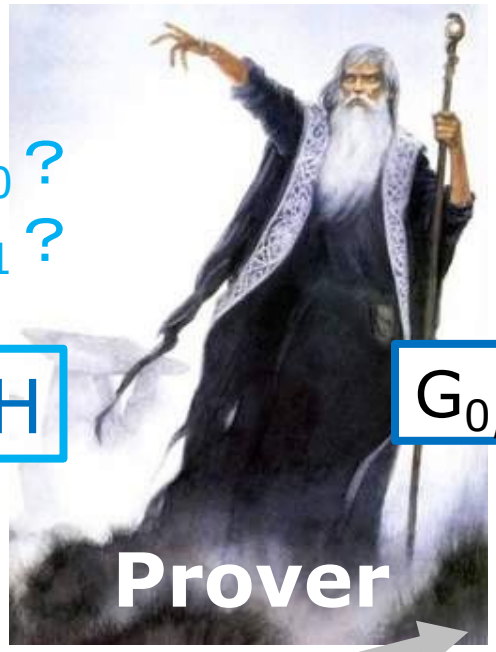


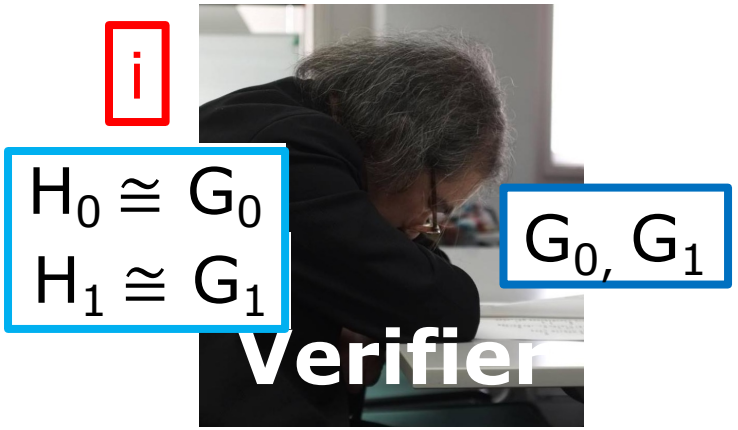
グラフの非同型問題

STEP 3

Proverは、送られたHについて、
$H \cong G_0$ であるか、あるいは、
$H \cong G_1$ であるかを判断する。

$H \cong G_0$ であれば $j=0$、
$H \cong G_1$ であれば $j=1$ とする。

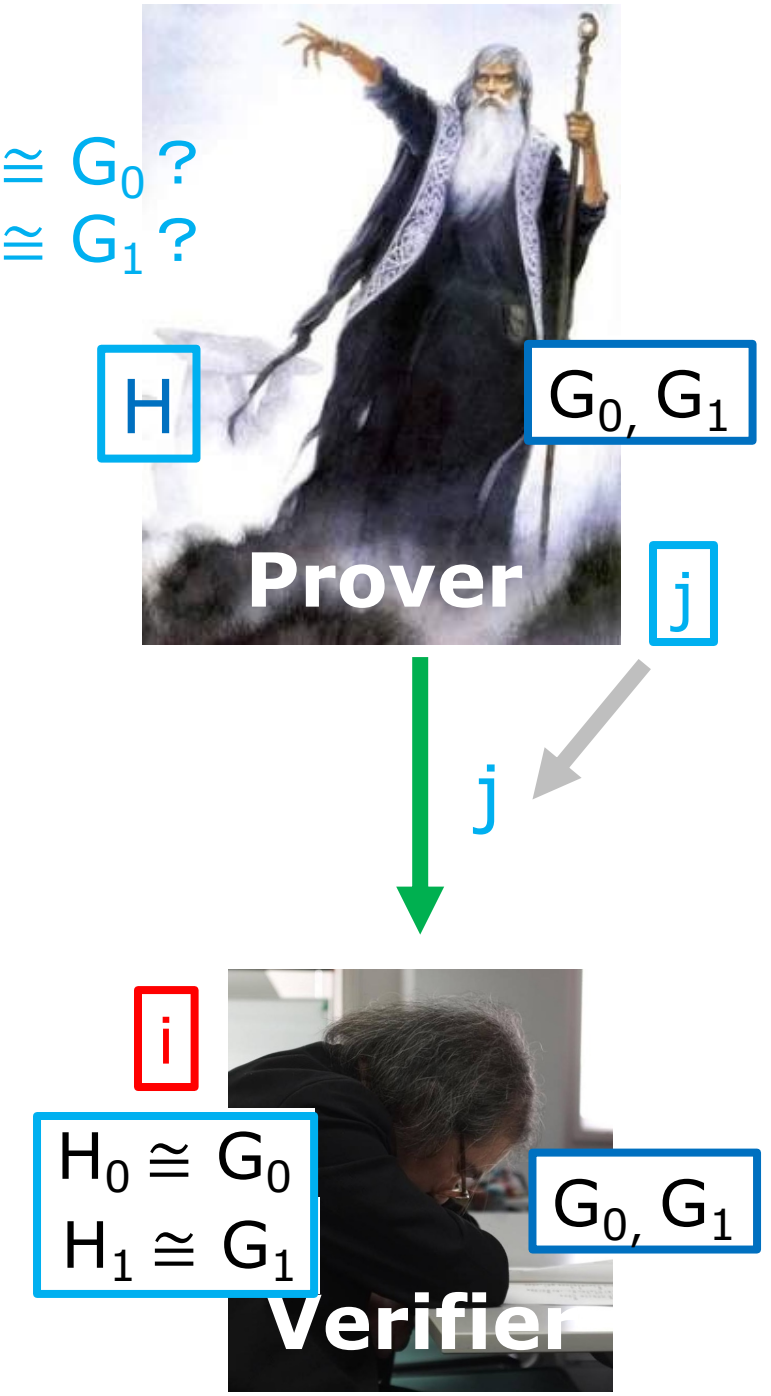




グラフの非同型問題

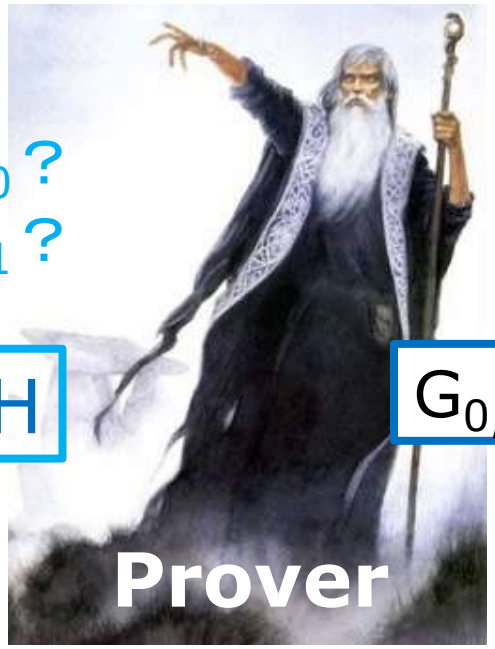
STEP 4

Prover は、j を Verifierに送る。



グラフの非同型問題

$H \cong G_0$?
$H \cong G_1$?



H

G_0, G_1

j

STEP 5

Verifierは、Proverから送られたjを記憶したiと比較する。

i ＝ j ?
i ≠ j ?

i

$H_0 \cong G_0$
$H_1 \cong G_1$

j

G_0, G_1

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、確実には、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。

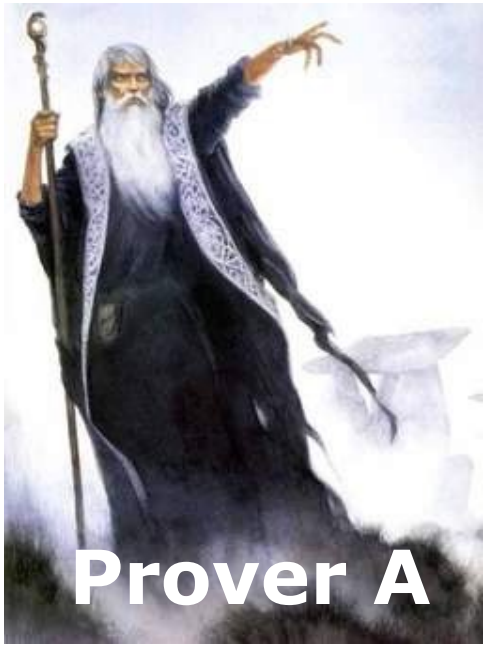
対話型証明の発展

Answer

Question

IP

Interactive Proof



Answer a

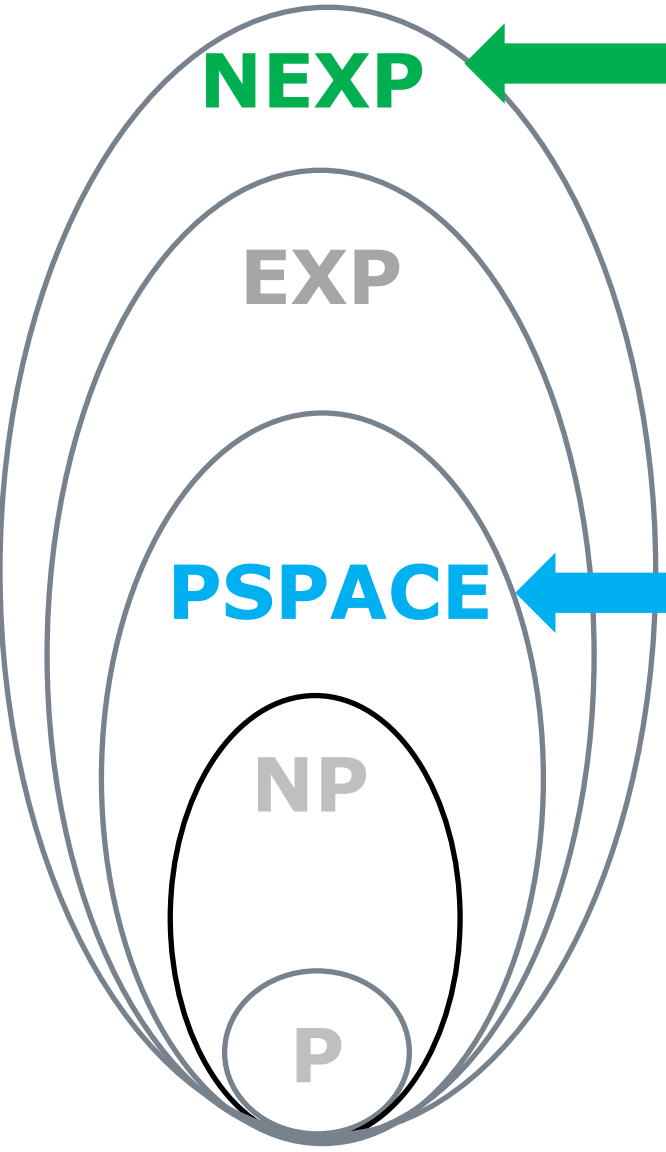
Answer b

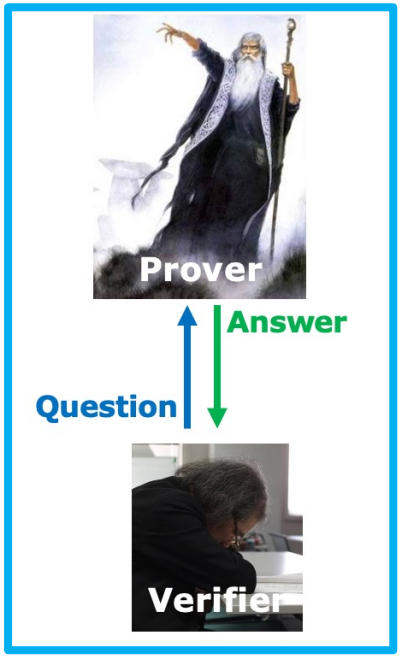
Question x

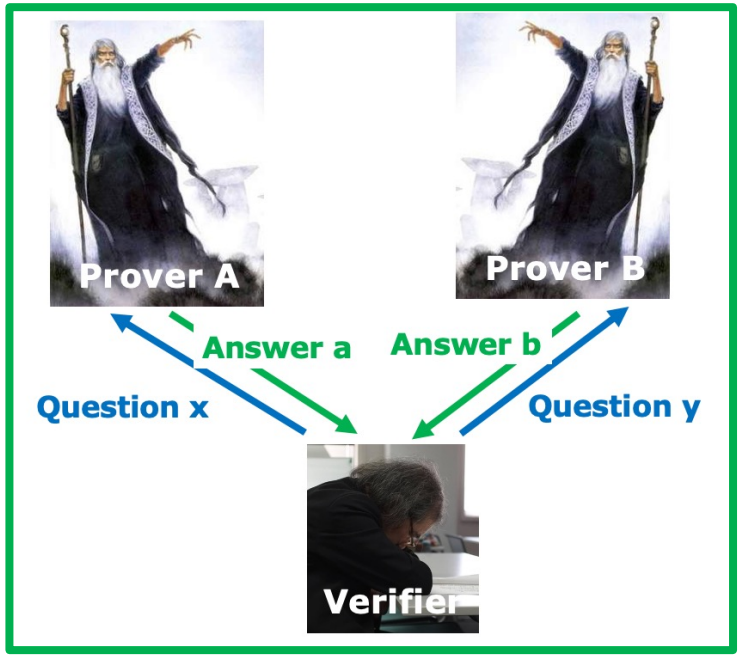
Question y

MIP

Multi Prover
Interactive Proof







MIP=NEXP
IP=PSPACE

Interactive Proof と nonlocal ゲーム

Interactive Proof とnonlocalゲーム

ProverとVerifierとの間の対話を通じたInteractive Proofは、ProverとVerifierとの間の対話型のゲームと考えることが出来る。

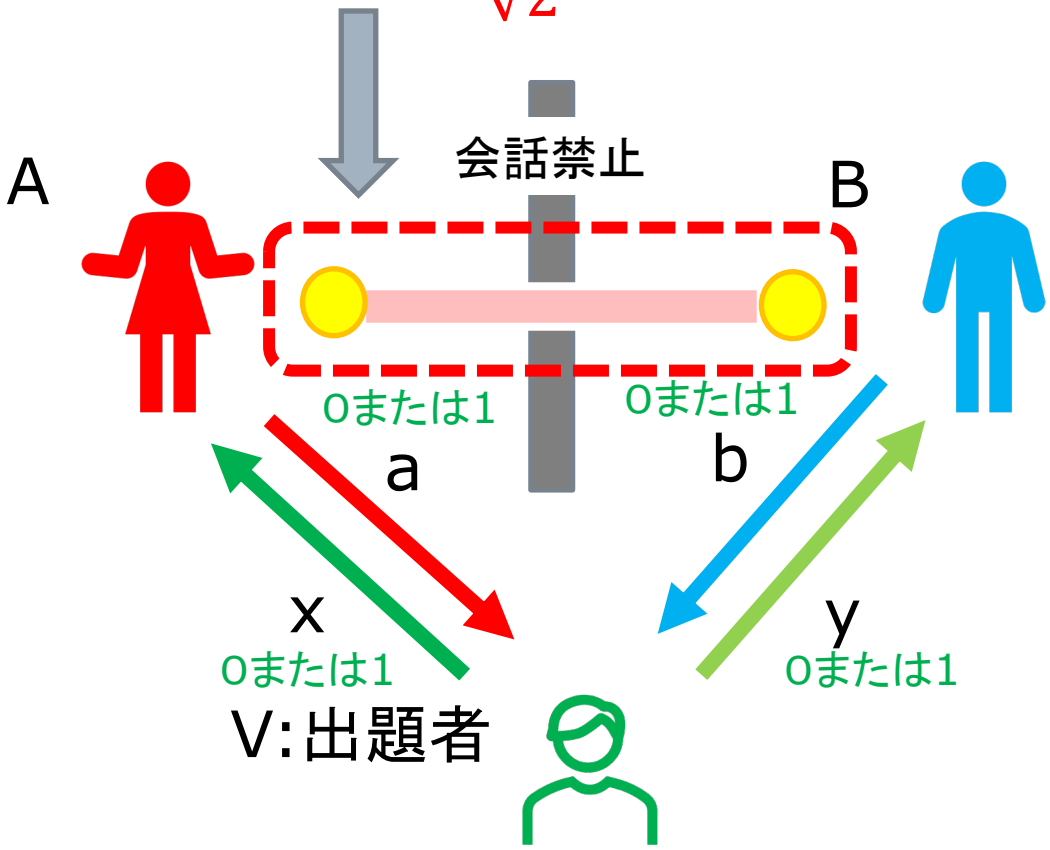
ゲームには勝ち負けのルールがある。Verifierは、そのルールに従って、自分が出した問題とそれに対するProverの答えをチェックして、勝ち負けを判定する。

Proverが、エンタングルした量子を共有している時、そのゲームをnonlocal ゲームと呼ぶ。

CHSHゲームは、nonlocalゲームである。「nonlocalゲーム」の名は、古典論の「局所実在論」に対して、量子論の「非局所性(non-locality)」を実証した、CHSHゲームに由来する。

CHSHゲームは
nonlocalゲームである

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



Answer a

Answer b

Question x

Question y

MIP^*

Multi Prover
Interactive Proof
with Entanglement

Entanglement

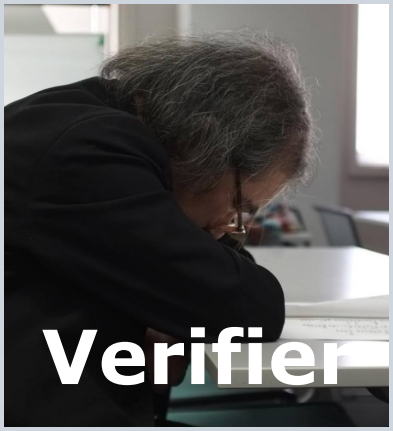
複数のエンタングルした量子の共有を許す

Answer a

Answer b

Question x

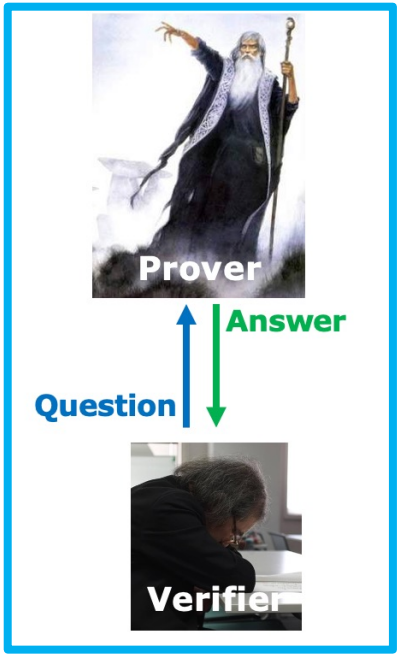
Question y

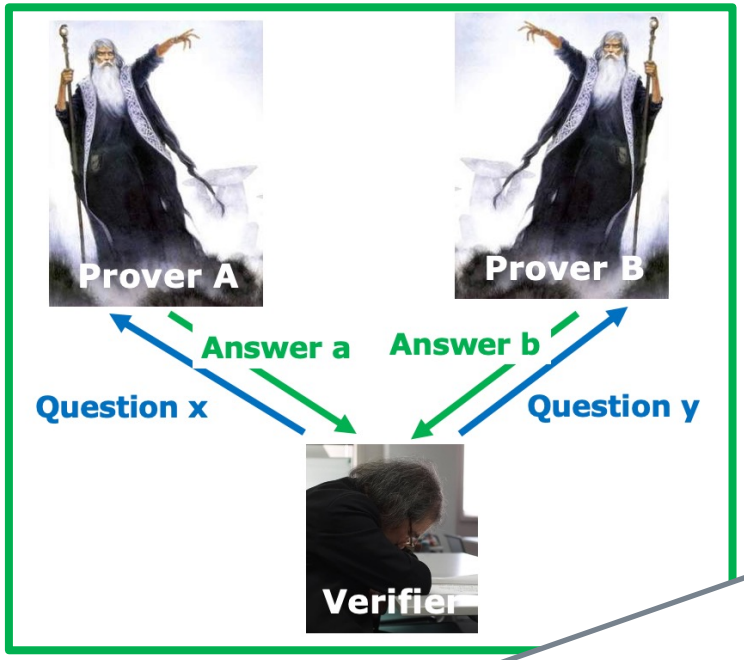


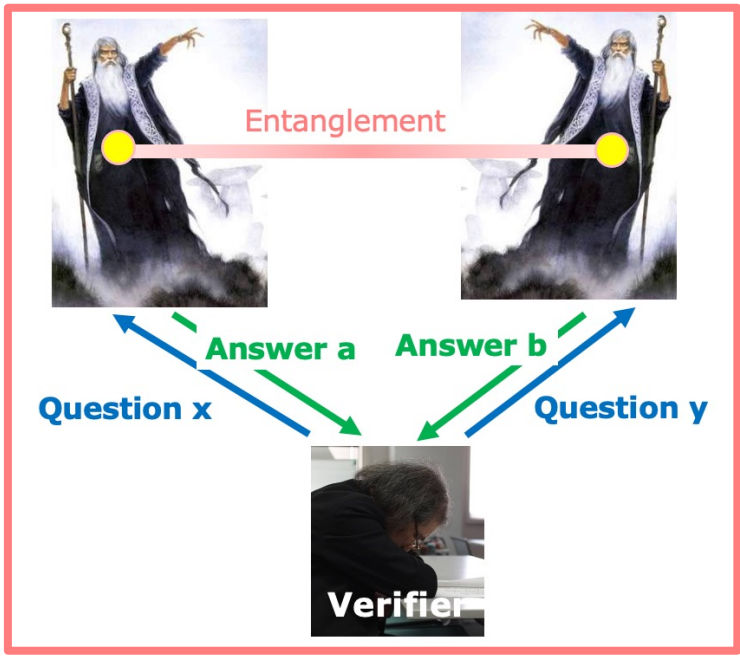
MIP^*

Multi Prover
Interactive Proof
with Entanglement

Interactive Proof のいくつかのタイプ

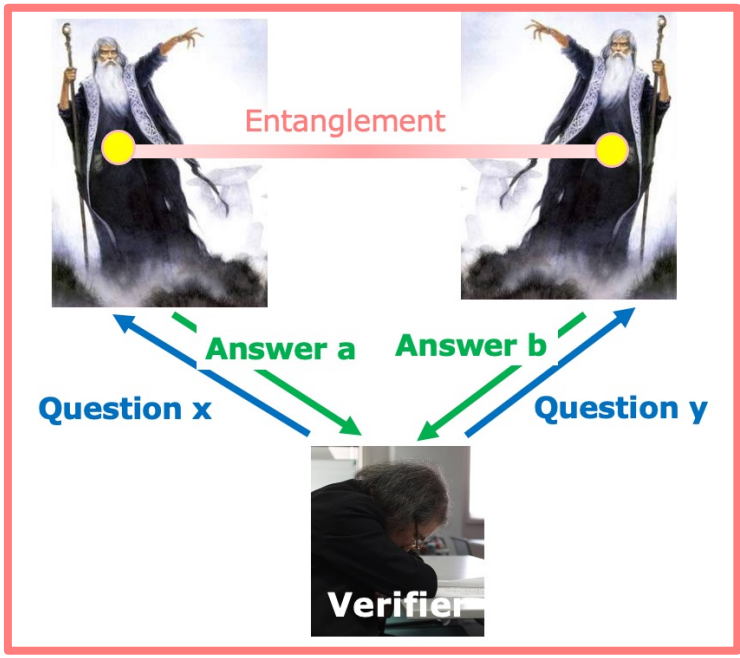




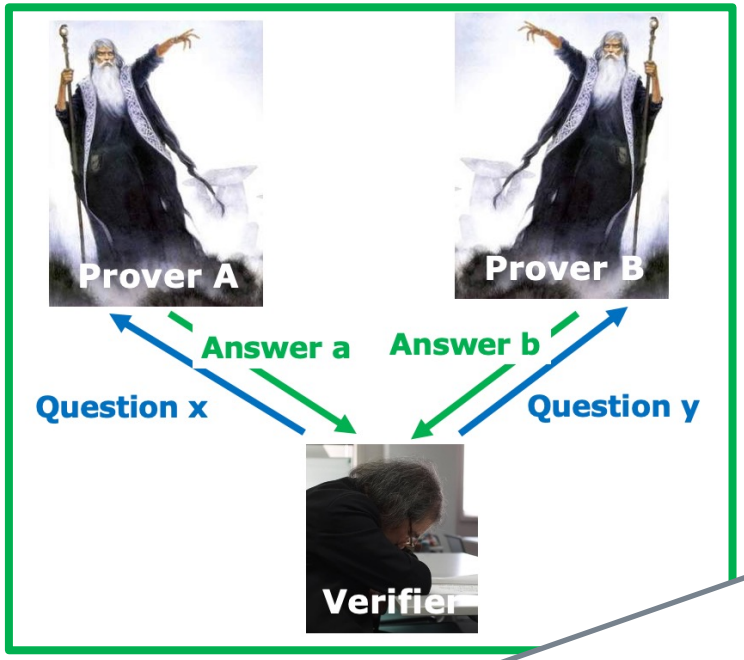


Interactive Proof のいくつかのタイプ

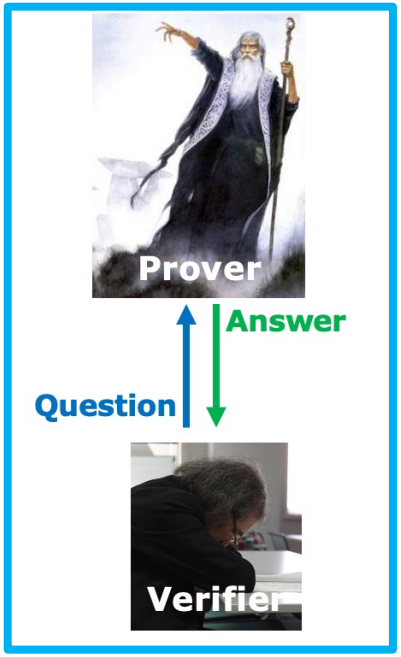
MIP*= RE



MIP= NEXP



IP = PSPACE



対応する複雑性のクラス

新しい数学的証明観の登場

「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、様々な議論がありました。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、主要に証明を行う側から証明を考えたものでした。

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す。

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りました。

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す。

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ります。正しいと検証されたものが正しい証明なのだと。

「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くなります。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す。

ただ、検証の世界は、確率論的な性質を持ちます。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ですし、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ありません。

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きます。

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りました。

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きましょう。

古典的な証明のイメージ

命題：T

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

- 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、$\pi_1, \pi_2, \pi_3, \ldots, \pi_{i-1}$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：$\pi_1, \pi_2, \pi_3, \ldots, \pi_n = T$

- 数学的証明のシステムを形式化するには、$\pi_1, \pi_2, \pi_3, \ldots, \pi_{i-1} \rightarrow \pi_i$ 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。

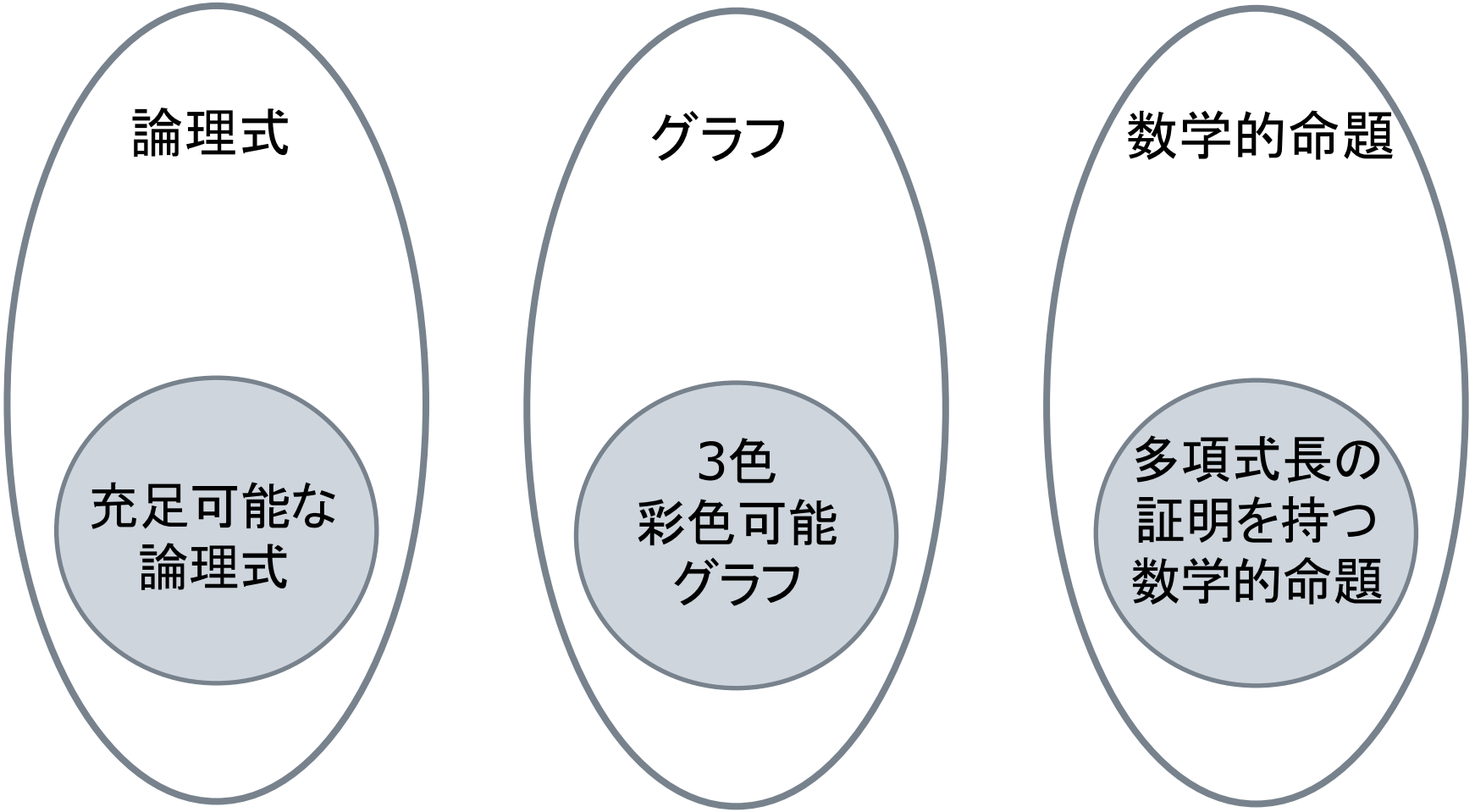
数学的証明問題はNP完全問題である

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

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す。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す。

よって、(実効的に)証明可能な数学的な命題のクラスは、NP完全です。

代表的なNP完全のクラス

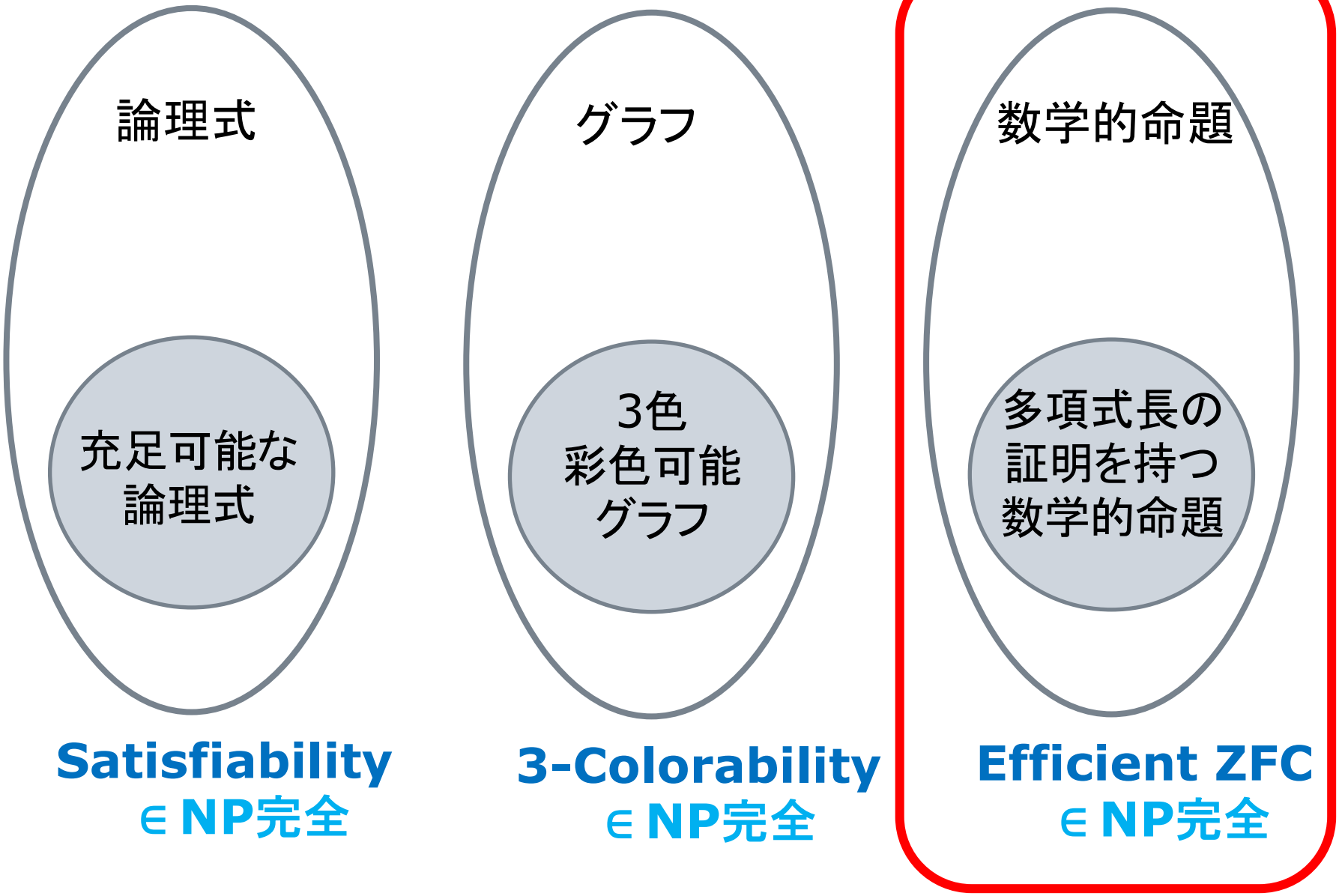


Satisfiability
∈ NP完全

3-Colorability
∈ NP完全

Efficient ZFC
∈ NP完全

代表的なNP完全のクラス



Satisfiability
∈ NP完全

3-Colorability
∈ NP完全

Efficient ZFC
∈ NP完全

Part III

量子コンピュータの能力の認識
-- BQPクラス --

4/10 マルゼミ「楽しい哲学」

Agenda Part III

量子コンピュータの能力の認識
-- BQPクラス --

- 量子コンピュータ研究の始まりと量子複雑性理論の誕生
  - 量子コンピュータ研究の始まり
  - 量子複雑性理論の誕生
  - Shorの発見
- 基本的な複雑性クラスのまとめ
- 量子優越性とは何か
  - ファインマン
  - プレスキル
- Googleはどんな実験をしたのか？
- 実験の評価

量子コンピュータ研究の始まりと
量子複雑性理論の誕生

量子コンピュータ研究の始まり

「計算可能性理論」が、大きな転機を迎えるのは、1980年代に入ってからです。

ファインマンが、コンピュータでは量子力学の法則に従う自然のシミュレートができないことに気づきます。彼は、自然のシミュレートが可能なコンピュータは、量子力学の法則に従ったコンピュータでなければならないと主張します。

この指摘が、「量子コンピュータ」研究の始まりです。

数学的体系と同様に、自然もまた、我々の認識の対象です。数学だけでなく、物理学もまた、我々の認識の可能性と限界について、強い関心を持っているのです。

ドイッチェは、ファインマンの考えを受けて、チューリングマシンの量子版を構成し、こうしたチューリング・マシンで計算可能なものが計算可能であるとします。これを、計算可能性についての「チャーチ＝チューリング＝ドイッチェのテーゼ」といいます。

一見すると、同じような定式化に思えるのだが、本質的な違いがあります。

「チャーチ＝チューリングのテーゼ」は、抽象的・形式的・数学的な「計算可能性」の定義についての提言なのですが、「チャーチ＝チューリング＝ドイッチェのテーゼ」は、「計算可能性」が、実在的・物理的に定義されねばならないと主張しています。

Church-Turing-Deutsch Thesis

Church-Turing-Deutsch Thesis:
物理システムによって実行されるすべての計算可能な計算は、あるTuringマシンによって実行される。

ここでの計算は、抽象化された数学的な計算ではなく、物理的システムによって実行される物理的なものである。

この命題を言い換えれば、
Turingマシンによって実行できない計算は、物理的システムでは実行できない
ということになるのだが、この命題は物理的な法則の限界として計算可能性について語っている。
Turingマシンによって実行できない計算は、物理法則を破らない限り実行できない

「チャーチ＝チューリングのテーゼ」は、いわば、遠くの雲の上に抽象的に存在する原理だったのですが、「チャーチ＝チューリング＝ドイッチェのテーゼ」は、地上に降りた現実の物理的原理です。

重要なことは、こうした「計算可能性」概念の「物理化」の背景にある思想でし。それは、情報過程が、けっして抽象的なものではなく、物理的なものに支えられた物理過程に他ならないという考えです。

ただ、80年代は、まだ、量子コンピュータは概念としてしか存在していませんでした。「計算可能性」の物理化という画期的な変化も、まだまだ、抽象的な議論でした。

量子複雑性理論の誕生

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ました。

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」と呼びます。量子複雑性理論は、現在の複雑性理論の中心分野です。

Umesh Vazirani

BQP

量子複雑性理論で最も基本的なクラスは、BQPです。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 に相当するものです。

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ます。

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)によく似ています。

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 $\subset \{0,1\}^*$ 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 $C_n(|x> |0>^{\otimes q(n)})$ accepts with probability > 2/3
  - if $x \notin L$ then $C_n(|x> |0>^{\otimes q(n)})$ 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 ecient algorithm to produce C_n given n.

Shorの発見

“Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”

1997年

https://goo.gl/kf4ScC

1994年、ショアは驚くべき発見をする。（論文は、1997年）

量子コンピュータでは、古典的なコンピュータでは指数関数的時間を要する素因数分解が、多項式時間で解けるという発見である。

現代のセキュリティ技術の根幹部分が、RSA暗号のように素因数分解の困難性に基礎を置いている事情から、この「ショアのアルゴリズム」の発見は、コンピュータ・サイエンスの枠を超えた、社会的と言っていい大きな反響を呼び起こした。

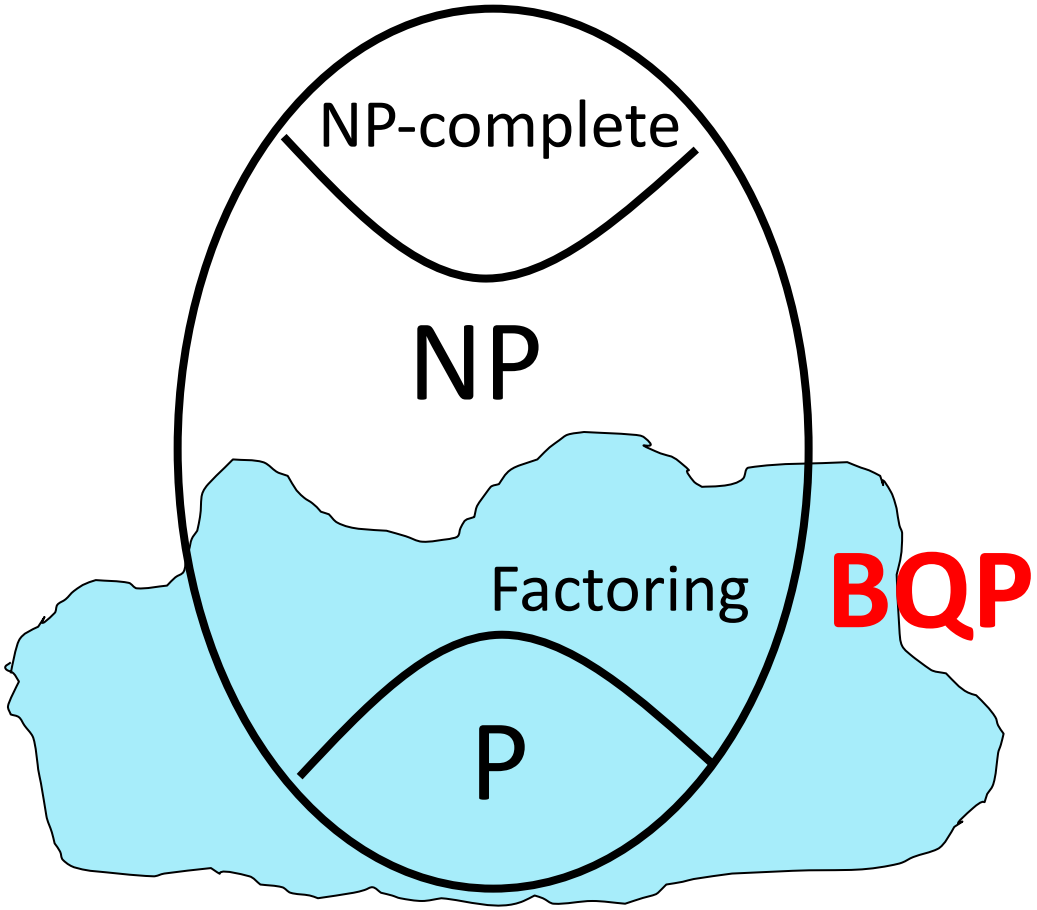
If computers that you build are quantum,
Then spies everywhere will all want 'em.
Our codes will all fail,
And they'll read our email,
Till we get crypto that's quantum, and daunt 'em.

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time of at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

BQP (Bounded-Error Quantum Polynomial-Time): The class of problems solvable efficiently by a quantum computer, defined by Bernstein and Vazirani in 1993

Shor 1994: Factoring integers is in **BQP**



複雑性クラスと問題の例

より難しい

n x *n* チェス

n x *n* 碁

箱詰め問題

地図の塗り分け

トラベリング・セールスマン

n x *n* 数独

グラフ同型問題

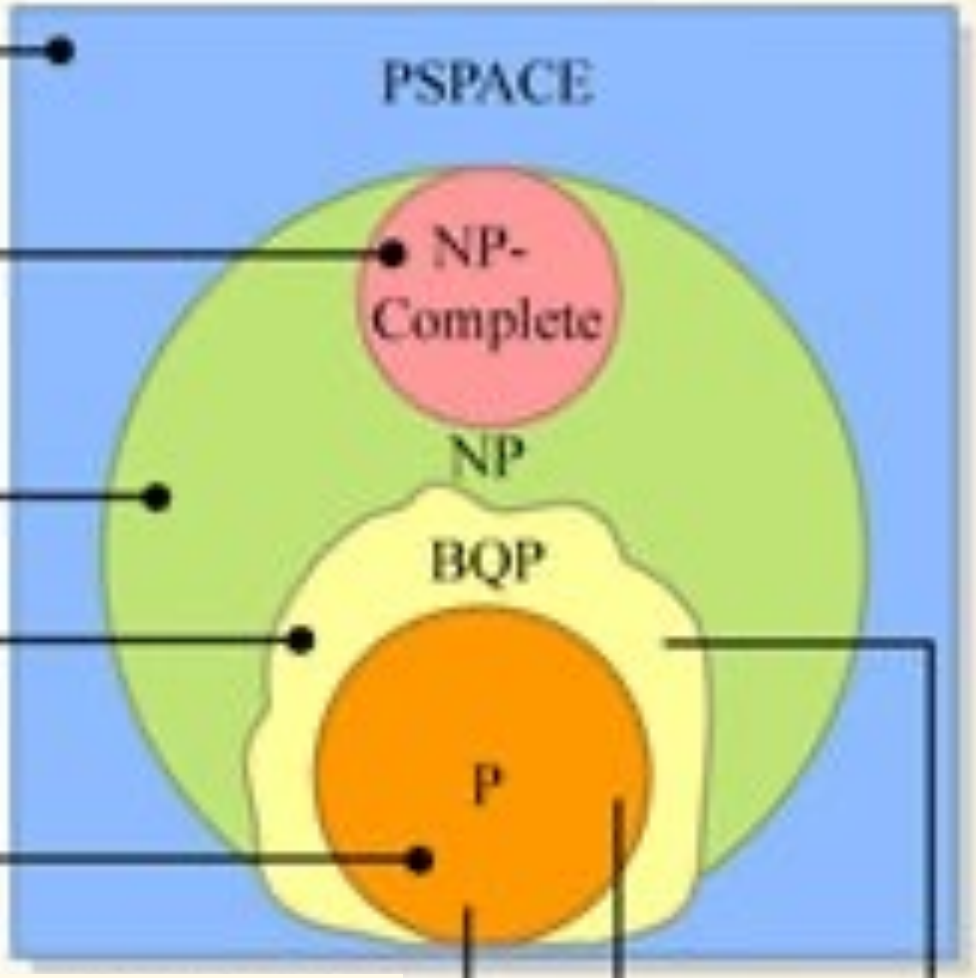
素因数分解

離散対数

グラフの接続性

素数判定

マッチ・メーキング



古典コンピュータで
効率的に解ける問題

量子コンピュータで
効率的に解ける
問題

複雑性クラスと問題の例

より難しい

n x *n* チェス

n x *n* 碁

箱詰め問題

地図の塗り分け

トラベリング・セールスマン

n x *n* 数独

グラフ同型問題

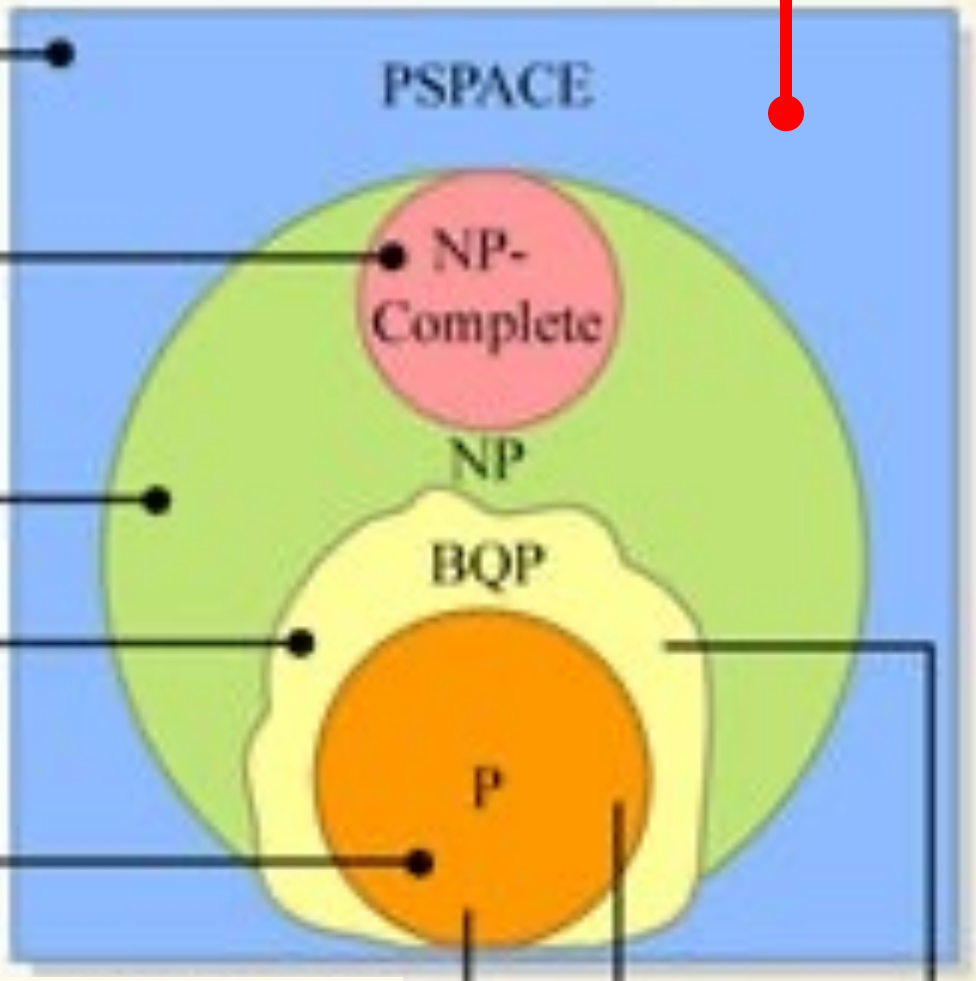
素因数分解

離散対数

グラフの接続性

素数判定

マッチ・メーキング



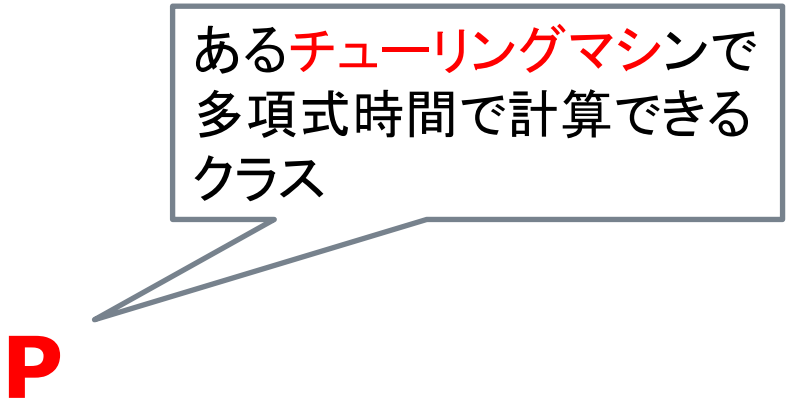
Interactive Proof

古典コンピュータで
効率的に解ける問題

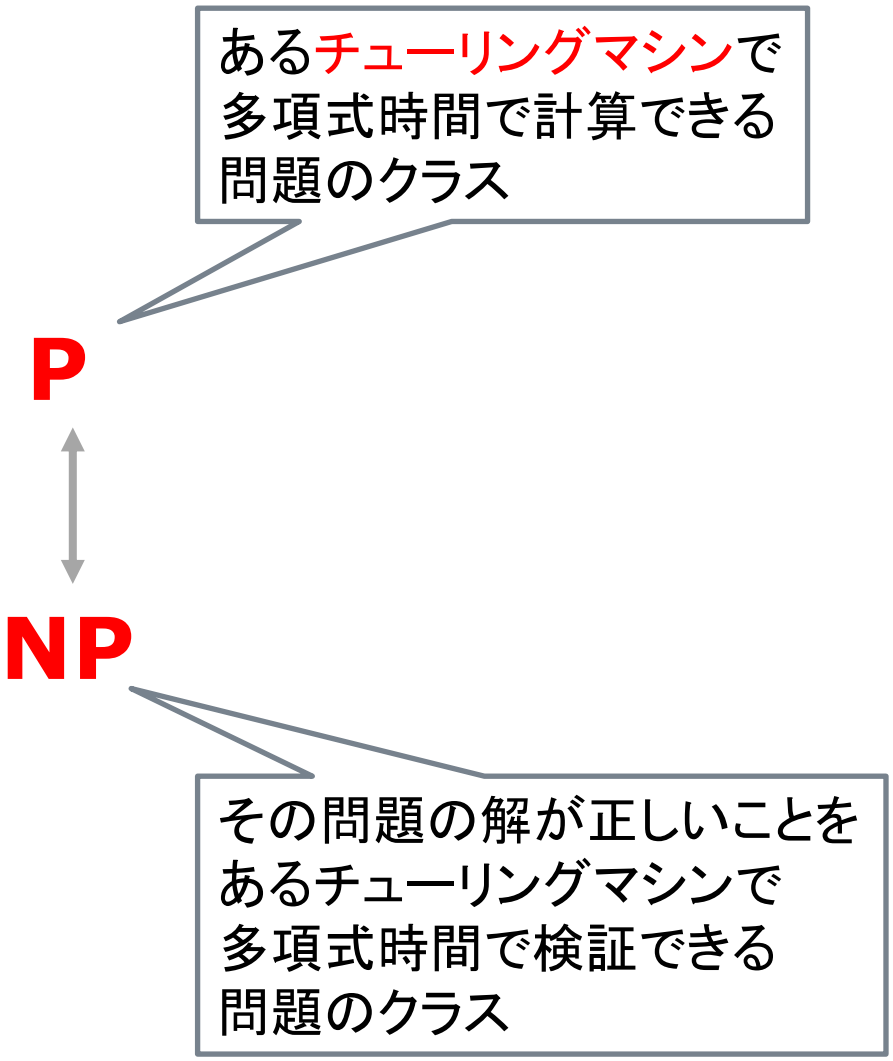
量子コンピュータで
効率的に解ける
問題

基本的な複雑性クラスのまとめ

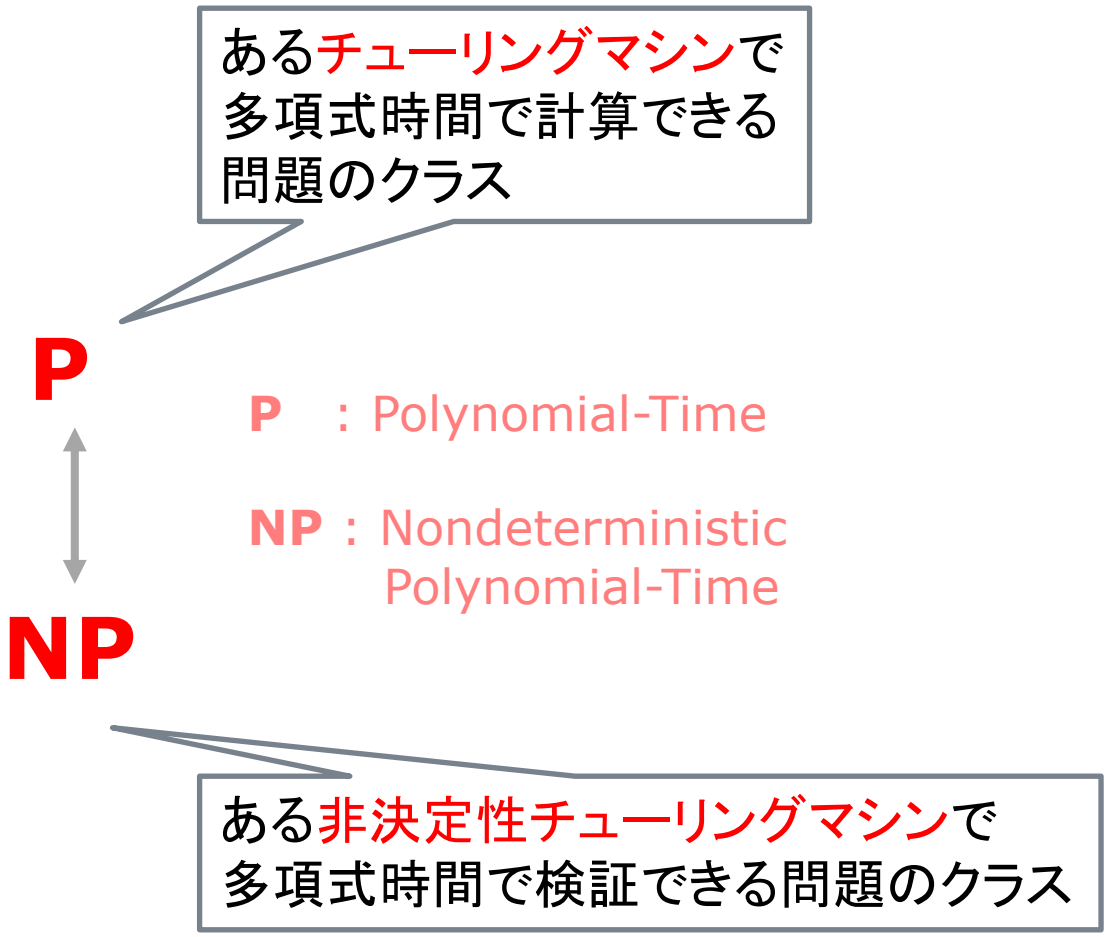
Pクラス



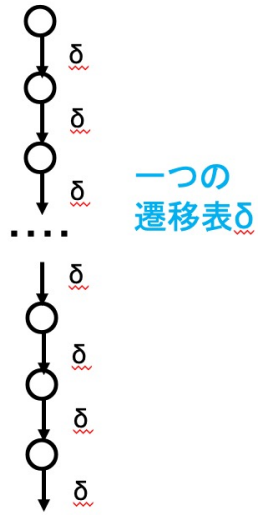
PクラスとNPクラス


あるチューリングマシンで
多項式時間で計算できる
問題のクラス
P
NP
その問題の解が正しいことを
あるチューリングマシンで
多項式時間で検証できる
問題のクラス

NPクラスの別の定義


あるチューリングマシンで
多項式時間で計算できる
問題のクラス
P
P ：Polynomial-Time
NP：Nondeterministic
Polynomial-Time
NP
ある非決定性チューリングマシンで
多項式時間で検証できる問題のクラス

NPクラスの別の定義



一つの
遷移表δ

決定性チューリングマシン

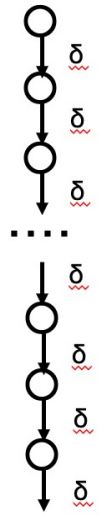
ある決定性チューリングマシンで
多項式時間で計算できる問題のクラス

P

NP

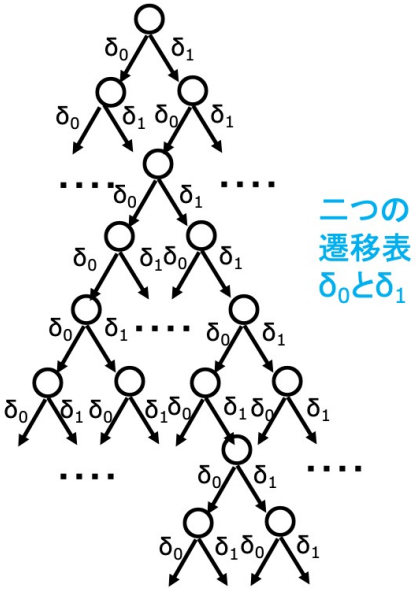
ある非決定性チューリングマシンで
多項式時間で検証できる問題のクラス

NPクラスの別の定義



一つの
遷移表δ

決定性チューリングマシン



二つの
遷移表
δ_0とδ_1

非決定性チューリングマシン

P

ある**チューリングマシン**で
多項式時間で計算できる
問題のクラス

NP

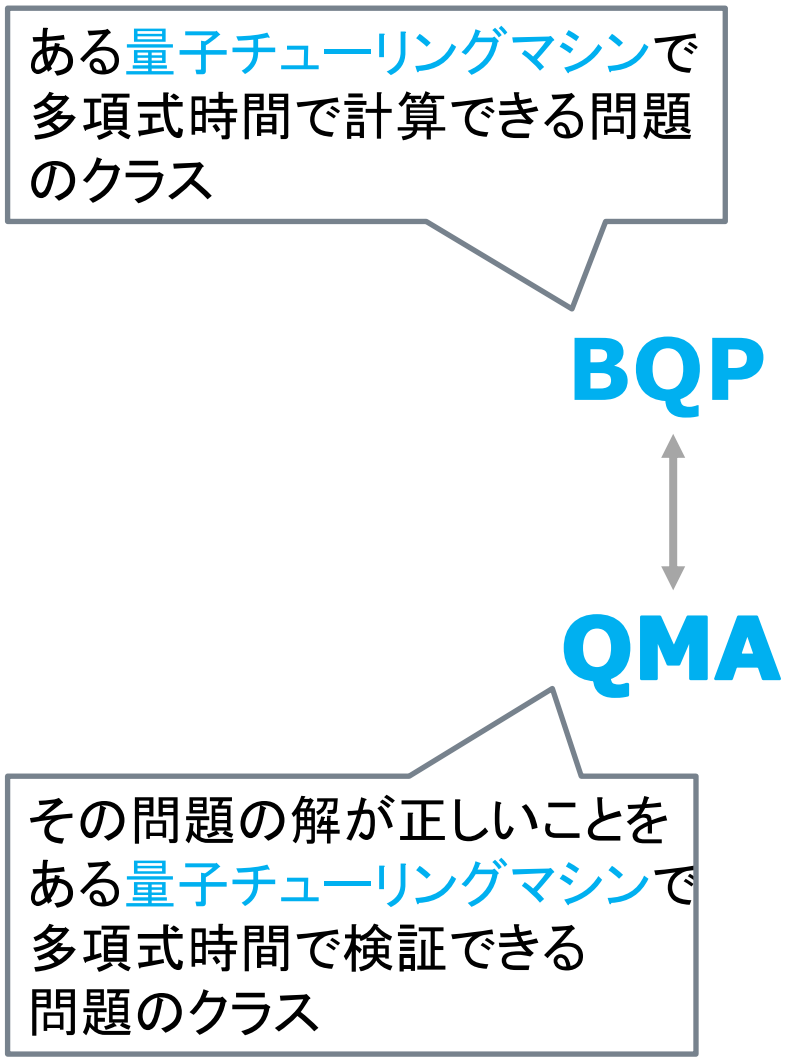
ある**非決定性チューリングマシン**で
多項式時間で検証できる問題のクラス

BQPクラス

ある量子チューリングマシンで多項式時間で計算できる問題のクラス

BQP

BQPクラスとQMAクラス



BQPクラスとQMAクラス

ある量子チューリングマシンで
多項式時間で計算できる問題
のクラス

BQP

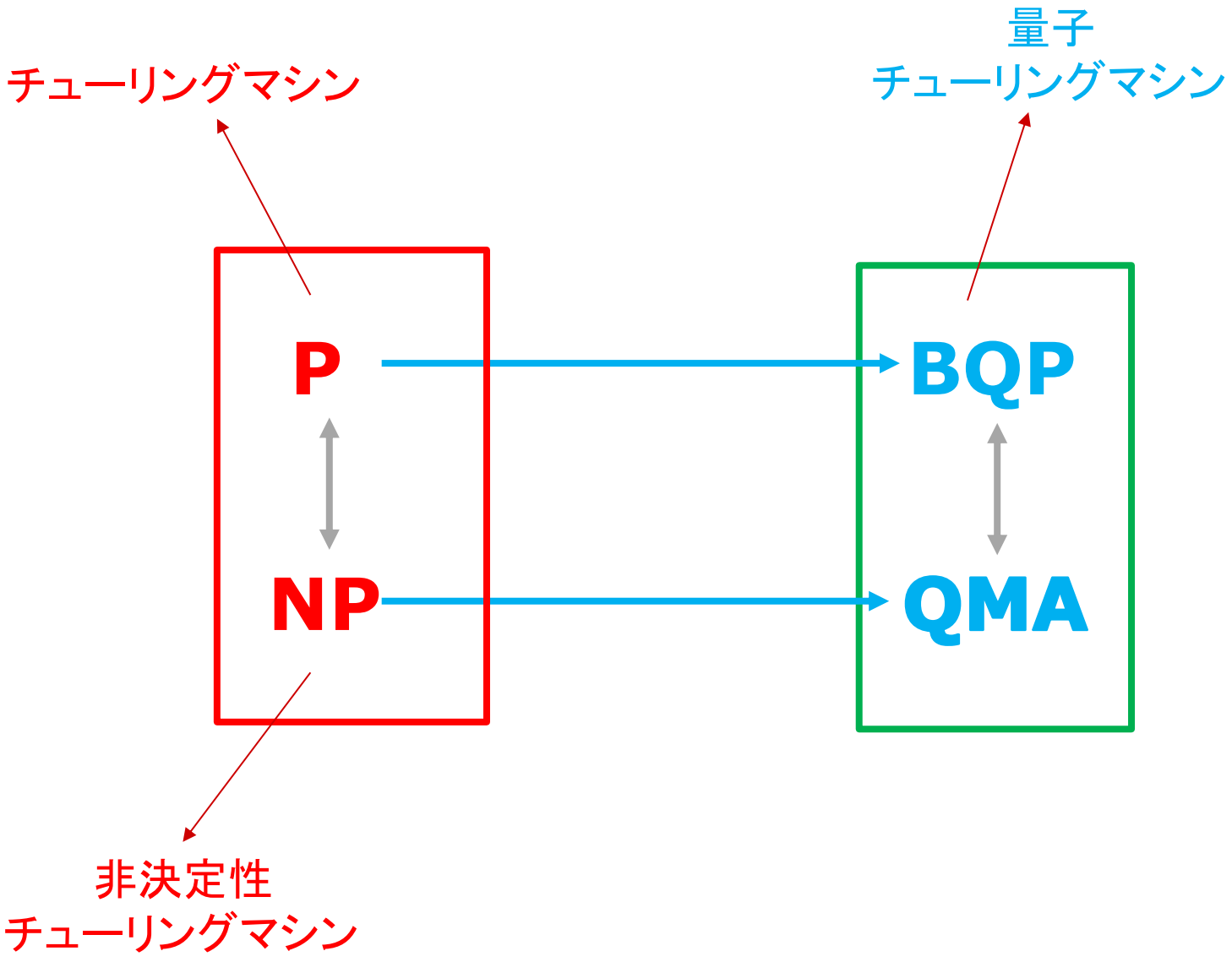
BQP：Bounded-Error Quantum
Polynomial-Time

QMA：Quantum MA

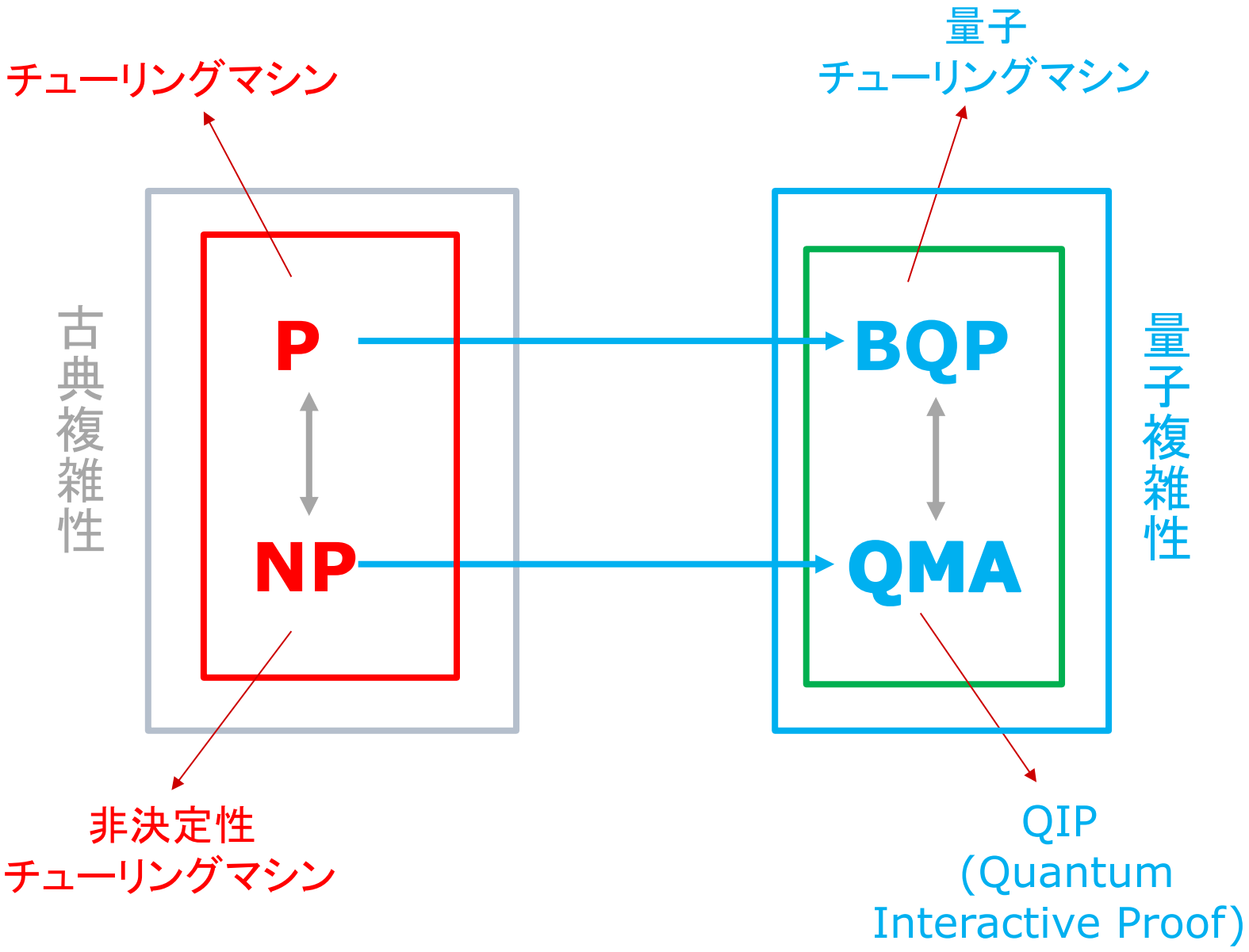
QMA

その問題の解が正しいことを
ある量子チューリングマシンで
多項式時間で検証できる
問題のクラス

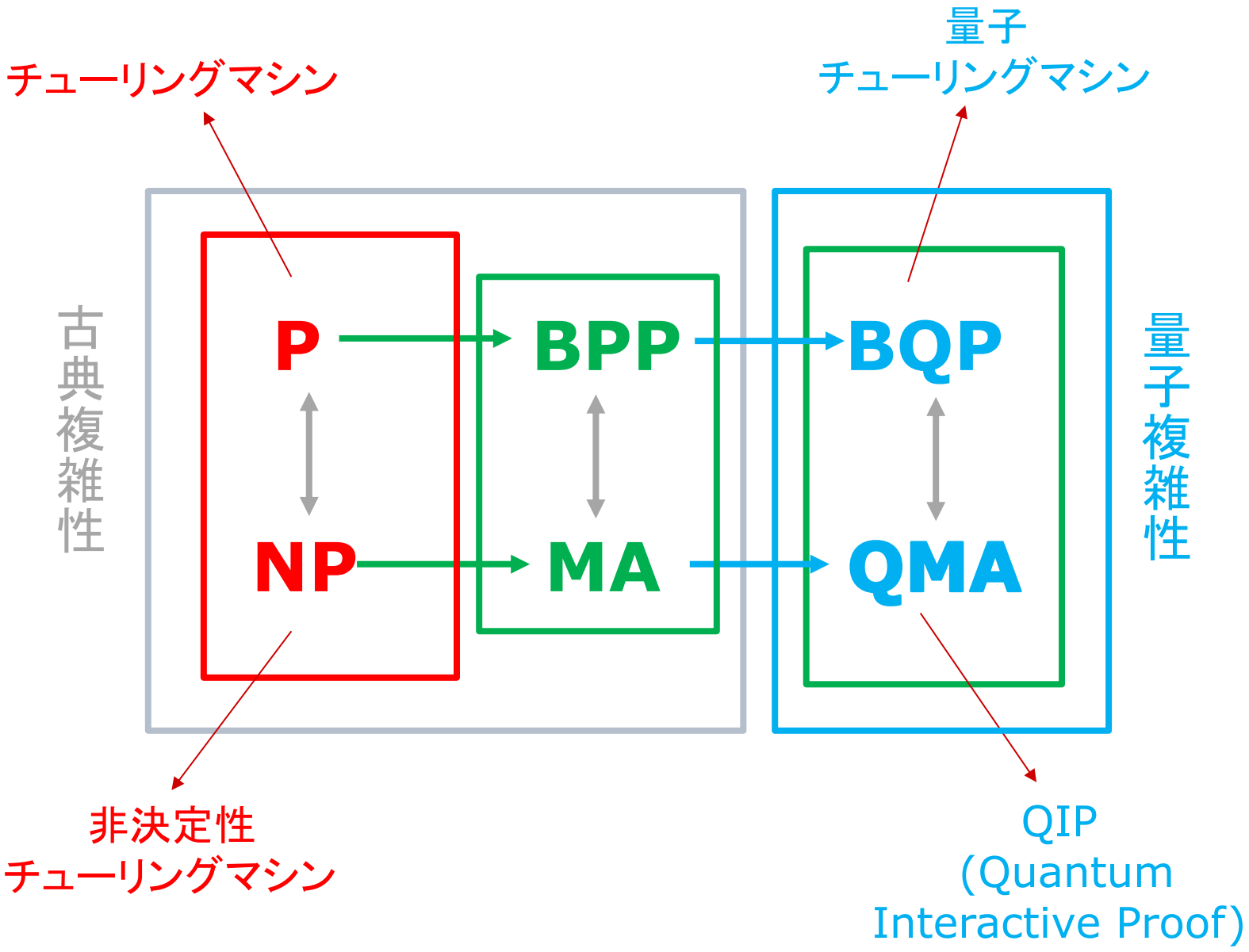
チューリングマシンと量子チューリングマシン



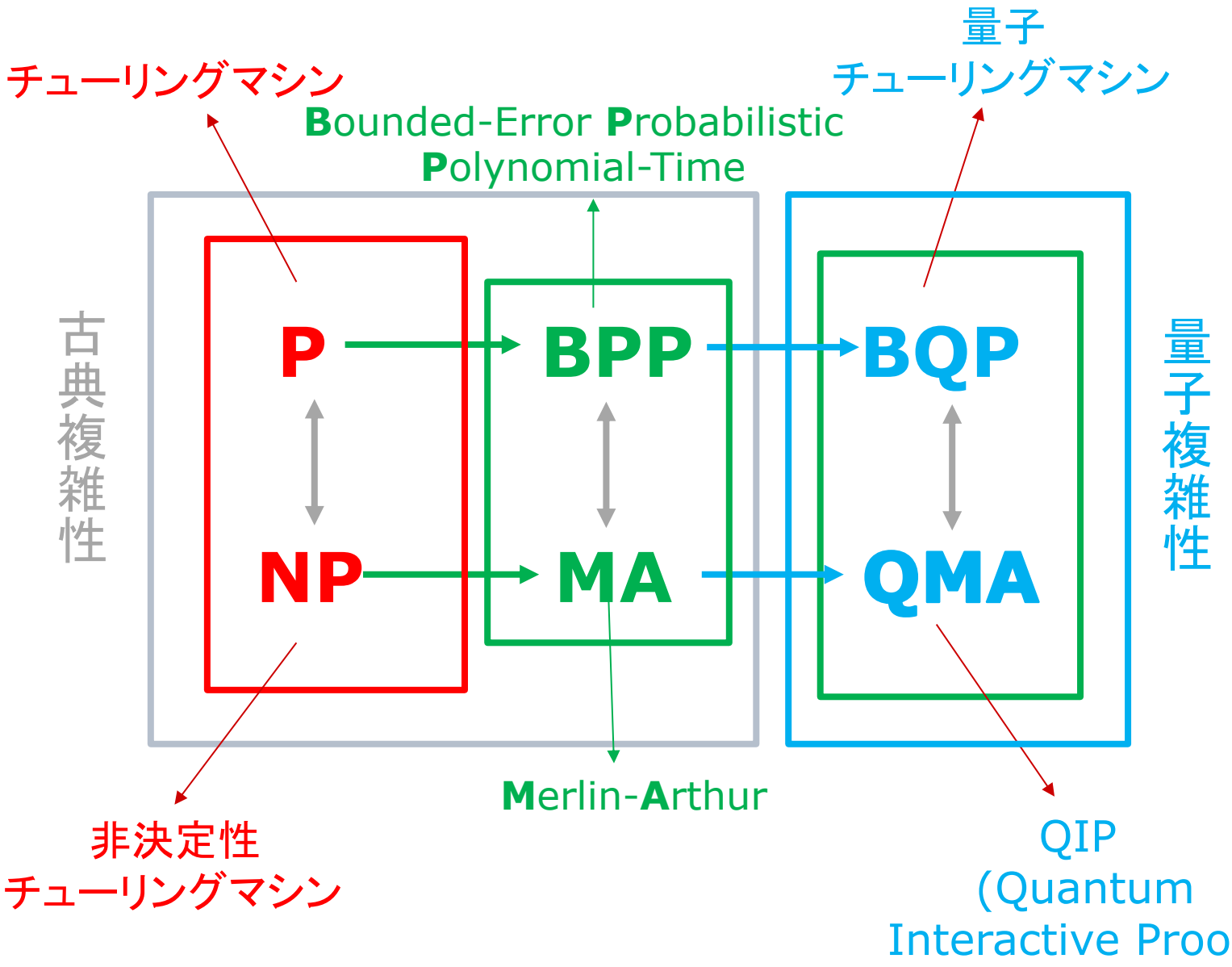
古典複雑性と量子複雑性



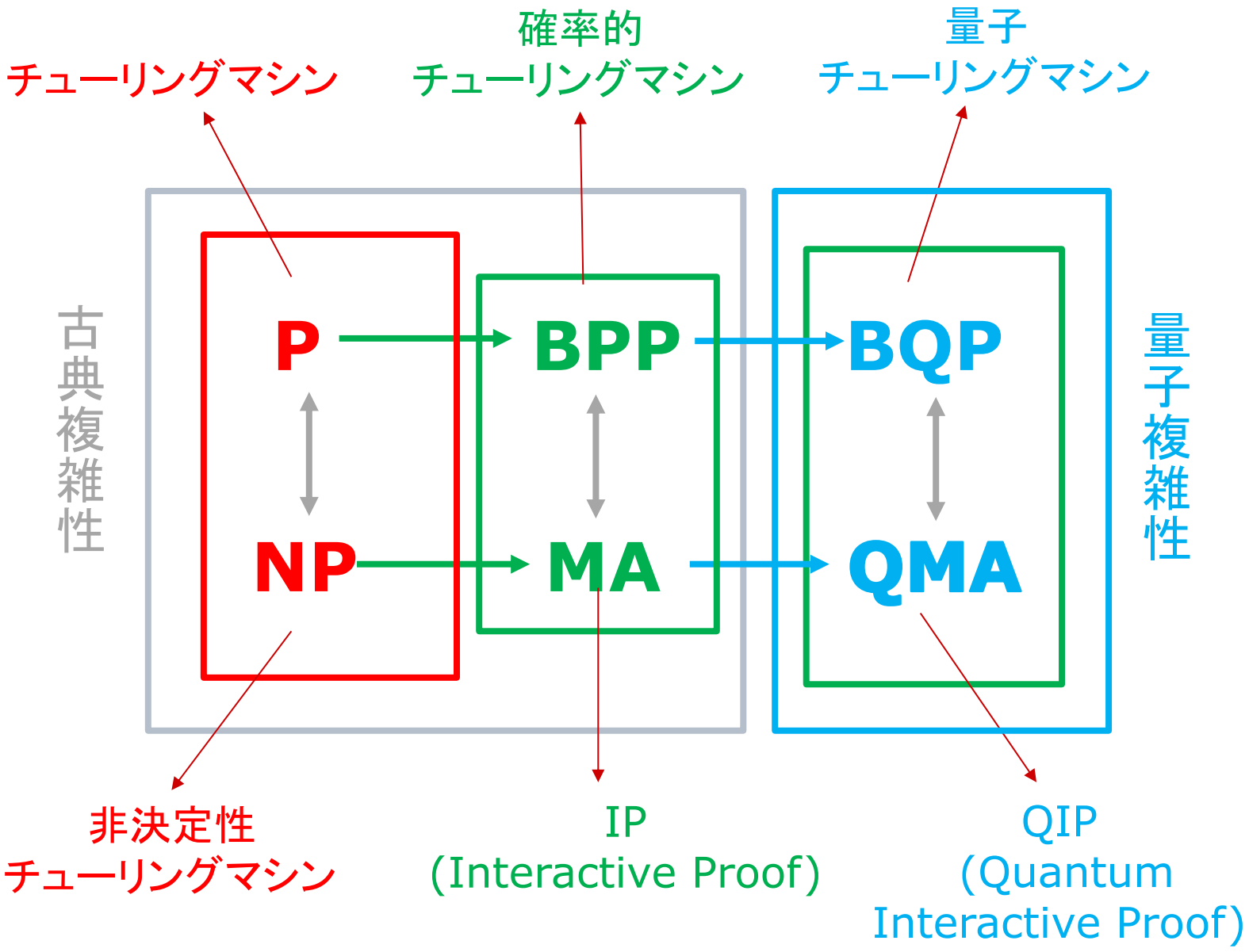
BPPクラスとMAクラス



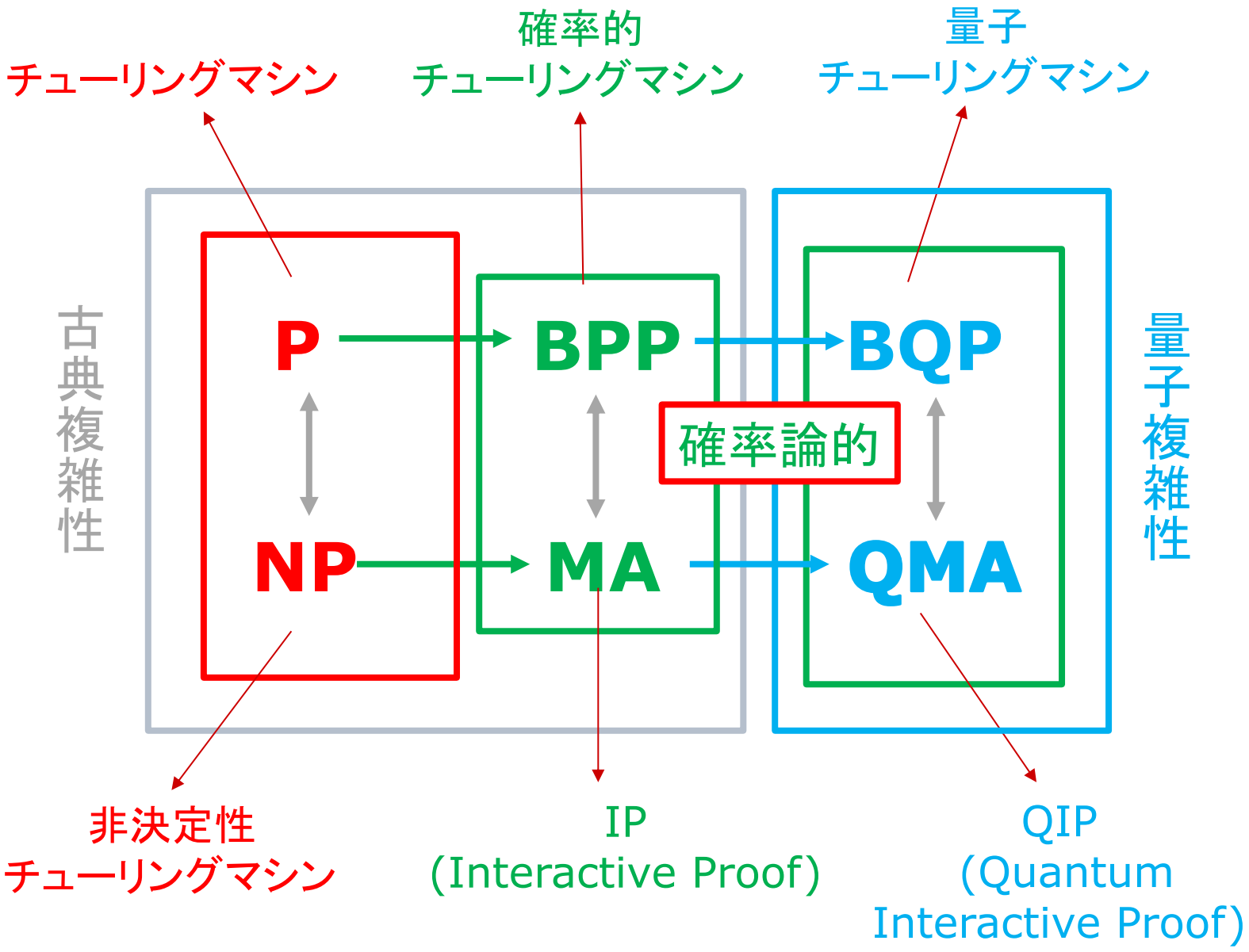
BPPクラスとMAクラス

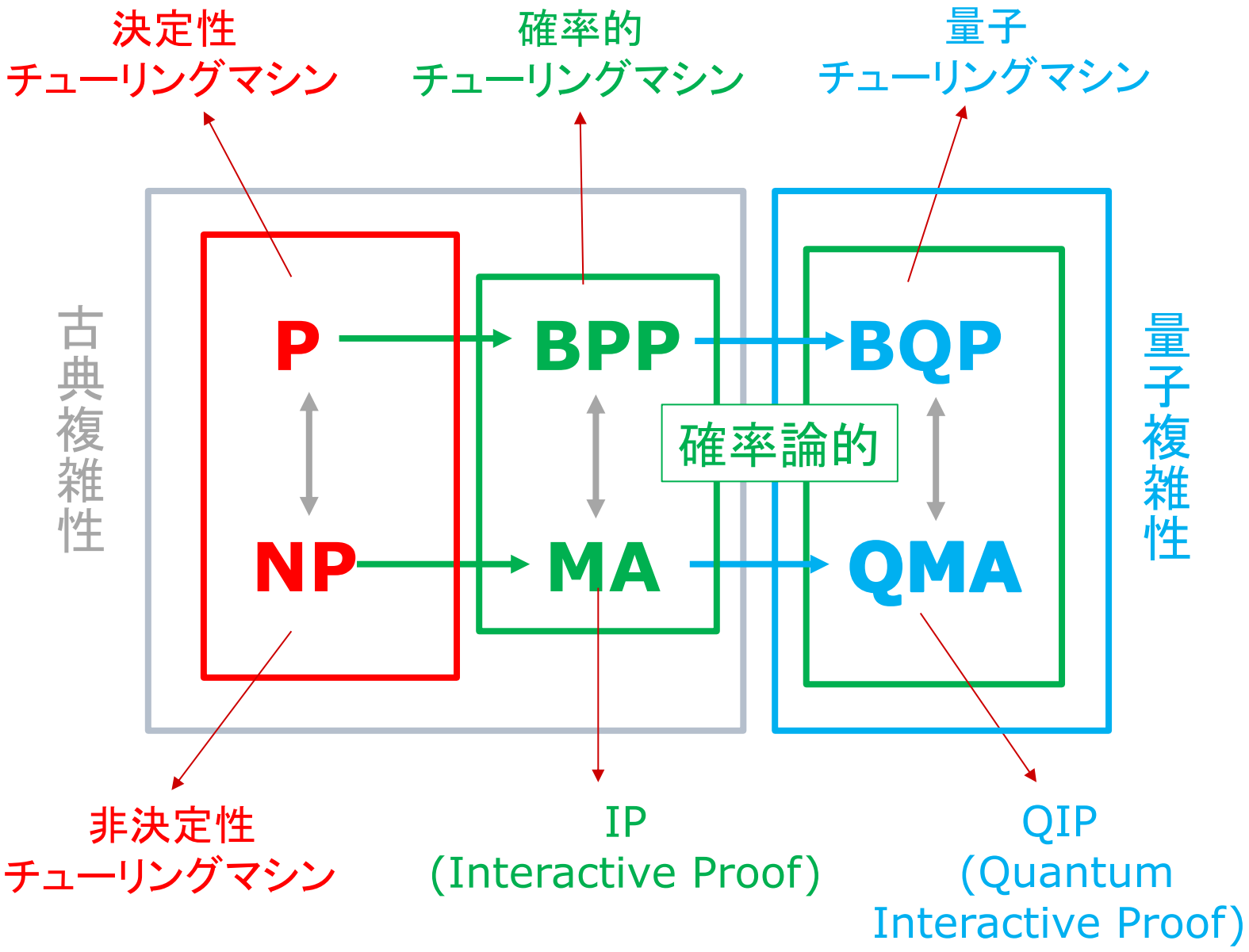


確率的チューリングマシンとInteractive Proof



確率と証明の結びつき


チューリングマシン
確率的
チューリングマシン
量子
チューリングマシン
古典複雑性
P
BPP
BQP
確率論的
NP
MA
QMA
量子複雑性
非決定性
チューリングマシン
IP
(Interactive Proof)
QIP
(Quantum
Interactive Proof)


決定性
チューリングマシン
確率的
チューリングマシン
量子
チューリングマシン
古典複雑性
量子複雑性
P
BPP
BQP
確率論的
NP
MA
QMA
非決定性
チューリングマシン
IP
(Interactive Proof)
QIP
(Quantum
Interactive Proof)

量子優越性とは何か

量子優越性とは何か？

1982年　ファインマン

2012年　プレスキル

量子優越性とは何か？

「量子優越性」という言葉は、2012年にプレスキルが論文 ”Quantum computing and the entanglement frontier” で提唱した造語です。

彼はこう言っています。

Classical systems cannot in general simulate quantum systems efficiently.

（古典システムは、一般には、量子システムを効率的にはシミレートできない）

Quantum computing and the entanglement frontier

John Preskill 2012年

https://arxiv.org/pdf/1203.5813.pdf

量子優越性の考え方は、ファインマンの量子コンピューターのアイデアにさかのぼります

あるシステムをシミレートするためには、一定の計算能力が必要です。これは、量子コンピュータは、古典コンピューターより、計算能力で優っていることを意味します。

古典システムと量子システムの複雑さを対比する、こうした考え方は、量子コンピュータのアイデアを初めて提案したファインマンの考えに遡るものです。彼は、1982年の論文”Simulating Physics with Computers” で、次のように述べていました。

自然をシミュレートするコンピュータ

コンピューターが、正確に自然と同じように振る舞う、正確なシミュレーションが存在する可能性について話そうと思う。

それが証明されて、そのコンピュータのタイプが先に説明したようなものであるなら、必然的に、有限の大きさの時空の中で起きる全てのものは、有限な数の論理的な操作で正確に分析可能でなければならないことになるだろう。

量子論的システムは、古典的なコンピューターでシミュレートされるか？

量子論的なシステムは、古典的な万能計算機で、確率論的にシミュレートされるだろうか？　別の言い方をすれば、コンピューターは、量子論的なシステムが行うのと、同じ確率を与えるだろうか？

コンピューターを今まで述べてきたような古典的なものだとすれば（前節で述べたような量子論的なものではないとすれば）、また法則はすべて変更されないままで、ごまかしもないとすれば、答えは明らかにノーである。

量子コンピュータ -- 万能量子シミュレーター

それは、新しいタイプのコンピューター、量子コンピューター？で可能になるだろう。

私が理解する限りでは、それは量子論的なシステムによって、量子コンピューターの要素によって、シミュレート出来るようになることは、いまや、明らかになった。

それはチューリング・マシンではない。別のタイプのマシンである。

Simulating Physics with Computers

Richard P. Feynman, 1982年
http://www.cs.berkeley.edu/~christos/classics/Feynman.pdf

こうしたファインマンの考えは、そのままプレスキルに受け継がれています。

classical systems cannot simulate highly entangled quantum systems efficiently, and we hope to hasten the day when well controlled quantum systems can perform tasks surpassing what can be done in the classical world.

彼は、この考えをさらに具体的に進めます。

One way to achieve such "quantum supremacy" would be to run an algorithm on a quantum computer which solves a problem with a super-polynomial speedup relative to classical computers,

この時点では、プレスキルは、量子コンピュータを実際に作り上げることが、とてもとても難しいことをよく理解していました。あるいは、「とんでもないほど、笑えるほど難しいいのかも」

To operate a large scale quantum computer reliably we will need to overcome the debilitating effects of decoherence, which might be done using "standard" quantum hardware protected by quantum error-correcting codes, or by exploiting the nonabelian quantum statistics of anyons realized in solid state systems, or by combining both methods.

Classical systems cannot in general simulate quantum systems efficiently.

Is controlling large-scale quantum systems merely really, really hard, or is it ridiculously hard?

実験前夜
NISQ 時代の課題

2018年　プレスキル

Quantum Computing in the NISQ era and beyond

John Preskill　2018/01/27

https://arxiv.org/abs/1801.00862v2

こうした時代を「NISQ 時代」と名付け、その課題を整理したのは、プレスキルの論文 “Quantum Computing in the NISQ era and beyond” だった。

彼は、「50～100qubitの量子コンピュータは、今日の古典的なデジタルコンピュータの能力を上回るタスクを実行する可能性を持つ」ことを指摘し、「量子複雑性」と「量子誤り訂正」の二つを、この時代の課題として提示した。

Quantum Computing in the NISQ era and beyond

John Preskill 2018/01/27

https://arxiv.org/abs/1801.00862v2

論文概要

近い将来、ノイズの下での中規模程度の量子技術NISQ (Noisy Intermediate-Scale Quantum)が利用可能になるだろう。50～100qubitの量子コンピュータは、今日の古典的なデジタルコンピュータの能力を上回るタスクを実行する可能性を持つのだが、量子ゲートのノイズは、信頼性をもって実行できる量子回路のサイズを制限する。NISQデバイスは、多体量子物理学の研究の有用なツールとなるだろう。その他の有用な応用もあるのだが、100qubitの量子コンピュータは、すぐには世界を変えないだろう。我々は、それを、将来のより強力な量子技術に向けた重要なステップとみなすべきである。量子技術者は、完全にフォールト・トレラントな量子コンピューティングを結果的に可能とする、より正確な量子ゲートの実現に向けて努力しなければならない。

エンタングルメントのフロンティア

私は粒子物理学と宇宙論をバックグラウンドとした理論物理学者なのが、20年以上にわたり、私の研究の努力の多くは量子情報科学に向けられていた。私がこの分野にひきつけられたのは、我々が物理科学の新しいフロンティア -複雑性のフロンティアあるいはエンタングルメントのフロンティアとでもよぶべきものの探求の初期段階にいると感じていたからである。この新しいフロンティアは、素粒子論や宇宙論のフロンティアとは異なっているのだが、非常に基本的でエキサイティングである。我々は人類史上初めて、多くの粒子、非常に複雑で高度にもつれあった量子状態を構築し、それを正確にコントロールするためのツールを手に入れて完成させつつある。その状態は非常に複雑で、現在我々が持つ最良のディジタル・コンピュータでもシミュレートできず、既存の理論的道具では、それをうまく特徴付けることもできない。

現在のコンピュータでは
自然のシミュレートはできない

私のような物理学者が、量子コンピューティングについて本当に興奮しているのは、量子コンピュータが自然界で起こる全てのプロセスを効率的にシミュレートできると信じる十分な理由があるからである。これは、古典的（すなわち非量子）デジタルコンピュータでは当てはまらないことだ。古典的コンピュータは、高度にもつれあった量子システムをシミュレートすることができないのだ。

量子コンピュータがあれば、きっと複雑な分子やエキゾチックな材料の特性をより深く探求することが可能になるだろう。それだけでなく、例えば、基本粒子の性質やブラックホールの量子的挙動やビッグバン直後の宇宙の進化をシミュレートすることで、新しいやり方で、基本的な物理学を切り開いていくだろう。

「量子複雑性」と「量子誤り訂正」という二つの原理基礎はエンタングルメント

エンタングルメント（量子もつれ）の最前線の開拓が実り多いものであるという我々の確信は、次の二つの原理に基づいている。

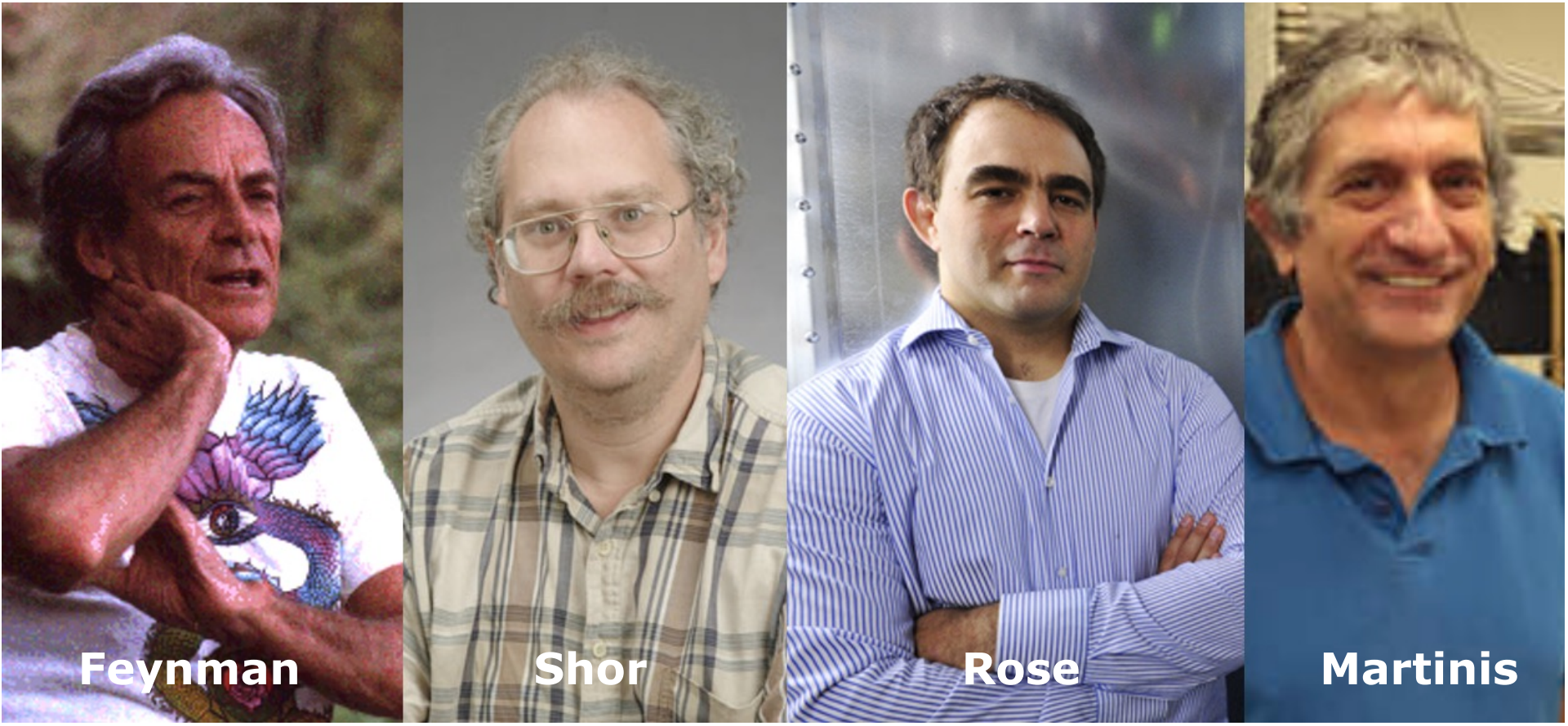
(1) 量子複雑性（量子コンピューティングが強力であると考える我々の考えの基礎）

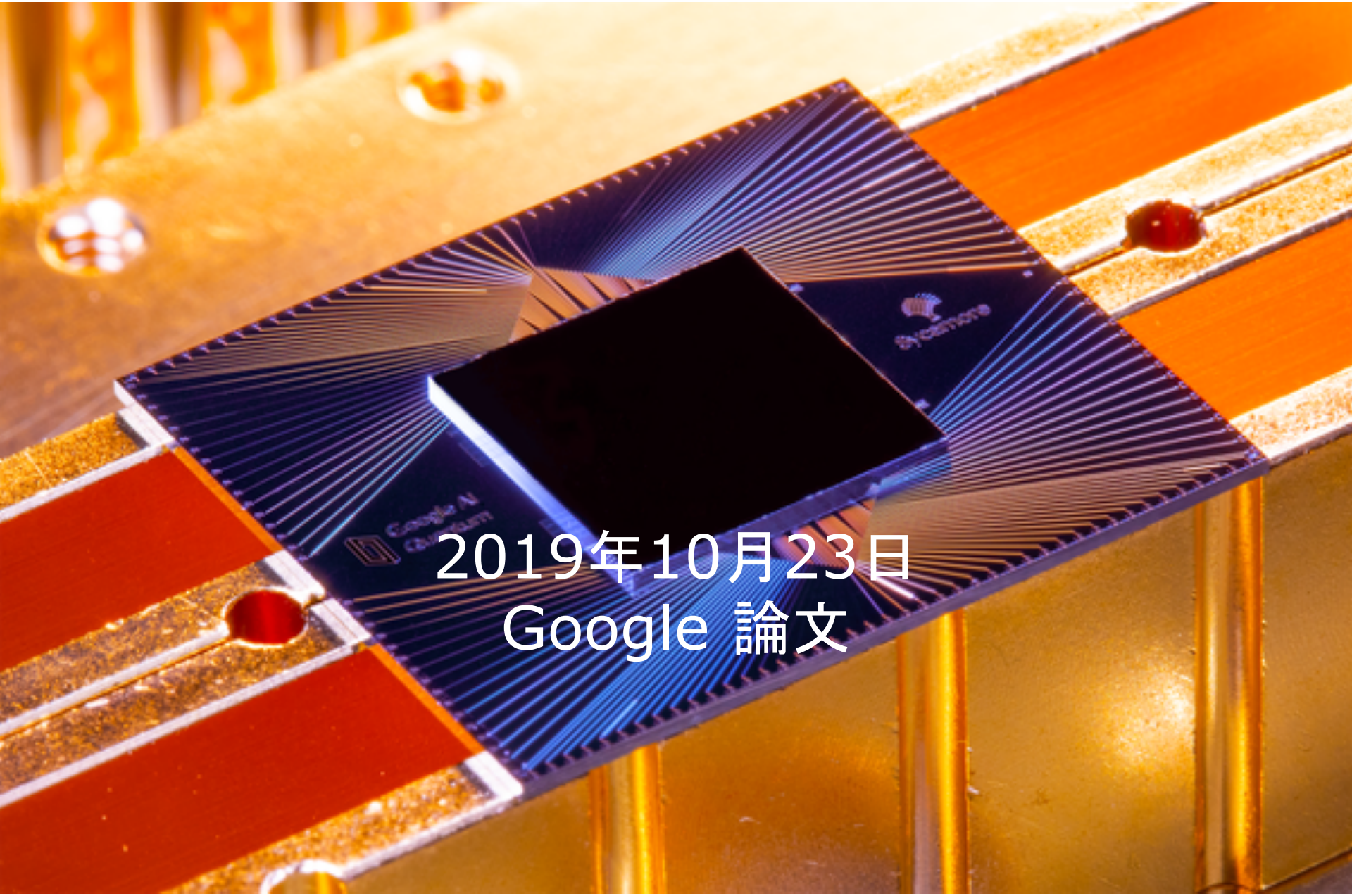
（2）量子誤り訂正（量子コンピュータは、難しい問題を解決する大規模なデバイスに拡張可能であると考える私たちの基礎）

これらの二つの原理の基礎となるのは、量子エンタングルメントの考え方である。エンタングルメントは、私たちが日常生活でであう相関とは全く異なる、量子システムの部分の間の特徴的な相関のために使用する言葉である。


Googleはどんな実験をしたのか？

量子コンピュータの実現に貢献した人々




2019年10月23日
Google 論文

Article | Published: 23 October 2019

Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, [...] John M. Martinis

Nature **574**, 505–510(2019) | Cite this article

Abstract

The promise of quantum computers is that certain computational tasks might be executed exponentially faster on a quantum processor than on a classical processor[1]. A fundamental challenge is to build a high-fidelity processor capable of running quantum algorithms in an exponentially large computational space. Here we report the use of a processor with programmable superconducting qubits[2,3,4,5,6,7] to create quantum states on 53 qubits, corresponding to a computational state-space of

2019年10月23日
Natureに論文発表

circuit a million times—our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years. This dramatic increase in speed compared to all known classical algorithms is an experimental realization of quantum supremacy[8,9,10,11,12,13,14] for this specific computational task, heralding a much-anticipated computing paradigm.

Quantum supremacy using a programmable superconducting processor

2019/10/23

https://www.nature.com/articles/s41586-019-1666-5

Google 論文は、多くの著者の連名で書かれている

Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando G. S. L. Brandao, David A. Buell, Brian Burkett, Yu Chen, Zijun Chen, Ben Chiaro, Roberto Collins, William Courtney, Andrew Dunsworth, **Edward Farhi**, Brooks Foxen, Austin Fowler, Craig Gidney, Marissa Giustina, Rob Graff, Keith Guerin, Steve Habegger, Matthew P. Harrigan, Michael J.Hartmann, Alan Ho, Markus Hoffmann, Trent Huang, Travis S. Humble, Sergei V. Isakov, Evan Jeffrey, Zhang Jiang, Dvir Kafri, Kostyantyn Kechedzhi, Julian Kelly, Paul V. Klimov, Sergey Knysh, Alexander Korotkov, Fedor Kostritsa, David Landhuis, Mike Lindmark, Erik Lucero, Dmitry Lyakh, Salvatore Mandrà, Jarrod R. McClean, Matthew McEwen, Anthony Megrant, Xiao Mi, Kristel Michielsen, Masoud Mohseni, Josh Mutus, Ofer Naaman, Matthew Neeley, Charles Neill, Murphy Yuezhen Niu, Eric Ostby, Andre Petukhov, John C. Platt, Chris Quintana, Eleanor G. Rieffel, Pedram Roushan, Nicholas C. Rubin, Daniel Sank, Kevin J. Satzinger, Vadim Smelyanskiy, Kevin J. Sung, Matthew D. Trevithick, Amit Vainsencher, Benjamin Villalonga, Theodore White, Z. Jamie Yao, Ping Yeh, Adam Zalcman, Hartmut Neven & **John M. Martinis**

論文の概要

量子コンピューターが約束していることは、特定の計算タスクが古典プロセッサーよりも量子プロセッサー上では、指数関数的に高速に実行される可能性があることである。

基本的な挑戦は、指数関数的に大きな計算空間上で量子アルゴリズムを実行できる高い信頼性を持つプロセッサを構築することである。

この論文では、プログラム可能な超伝導量子ビットを備えたプロセッサを使用して、53量子ビットの量子状態を作成したことを報告する。この量子状態は、次元2^{53}（約10^{16}）の計算状態空間に対応する。

繰り返される実験からの測定は、結果の確率分布をサンプリングすることで行われる。この結果は、古典的なシミュレーションを使用して検証する。

論文の概要

我々のSycamoreプロセッサでは、量子回路の1つのインスタンスを100万回サンプリングするのに約200秒を要した。

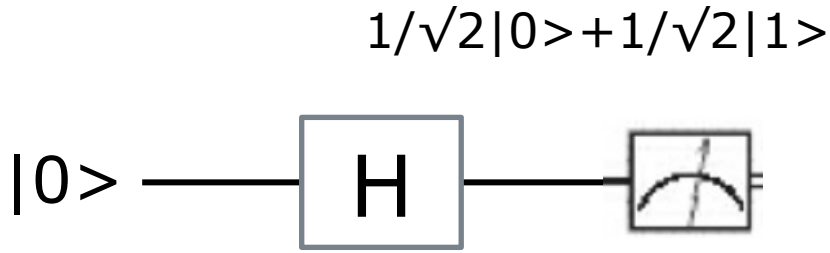
現在のベンチマークでは、最先端の古典的なスーパーコンピューターで同等のタスクを実行するには、約10,000年かかる。

すべての既知の古典的なアルゴリズムと比較して、この劇的な速度の向上は、この特定の計算タスクに対して量子優位性を実験的に実現したものとなる。この実験は、待望のコンピューティングパラダイムの先駆けである。

ランダム量子回路

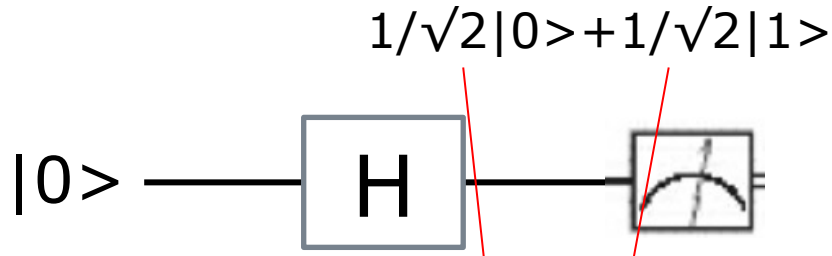
今回のGoogleの実験の一つのポイントは、量子優越性を実証するのに、「ランダム量子回路」という手法をとったことである。ここでは、それがどういうアイデアかを説明する。

つぎのように、アダマール・ゲートH 一つに、
初期値として |0>を与えた時、サンプリングで得られる分布を考えよう



Hは、|0>を
1/√2|0>+1/√2|1>
に変える

つぎのように、アダマール・ゲートH 一つに、
初期値として |0>を与えた時、サンプリングで得られる分布を考えよう

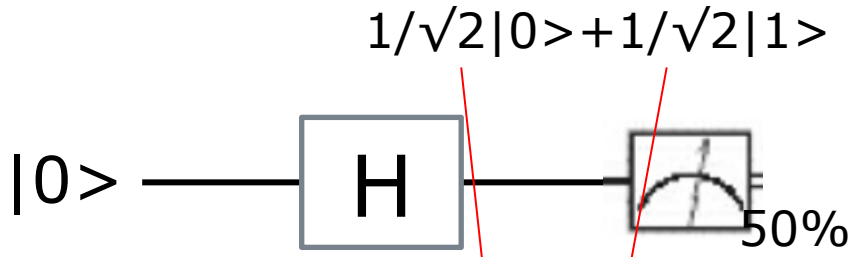


Hは、|0>を
1/√2|0>+1/√2|1>
に変える

この時、|0>が観測される確率は
$|1/\sqrt{2}|^2 = 1/2$
この時、|1>が観測される確率は
$|1/\sqrt{2}|^2 = 1/2$

よって、分布は次のようになる

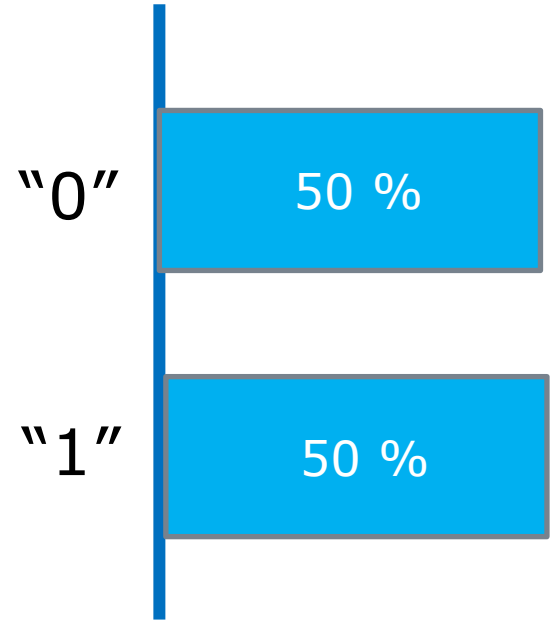
つぎのように、アダマール・ゲートH 一つに、
初期値として |0>を与えた時、サンプリングで得られる分布を考えよう



Hは、|0>を
1/√2|0>+1/√2|1>
に変える

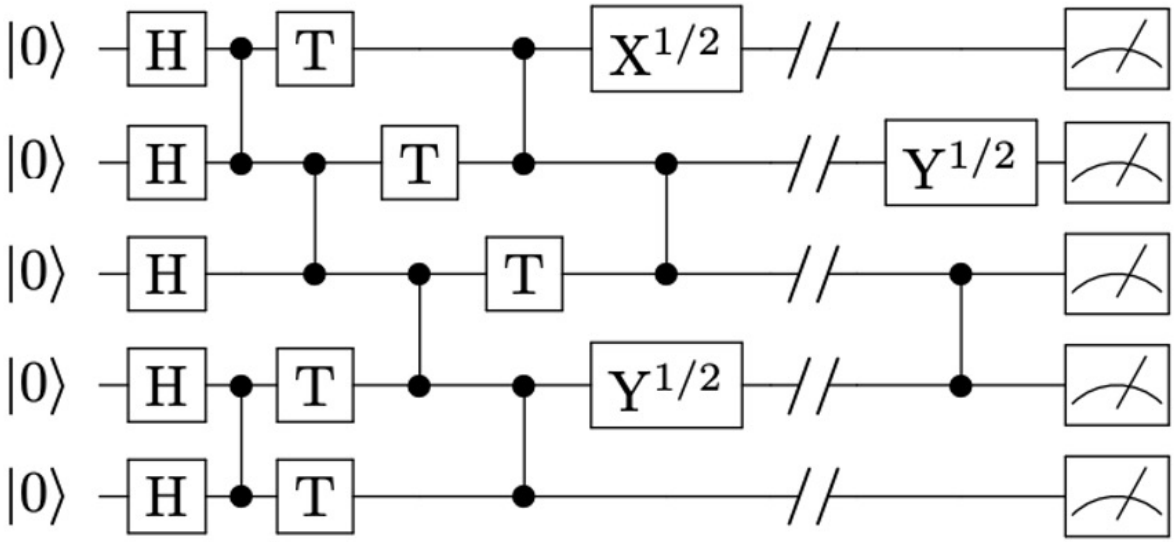
この時、|0>が観測される確率は
$|1/\sqrt{2}|^2 = 1/2$
この時、|1>が観測される確率は
$|1/\sqrt{2}|^2 = 1/2$

よって、分布は次のようになる



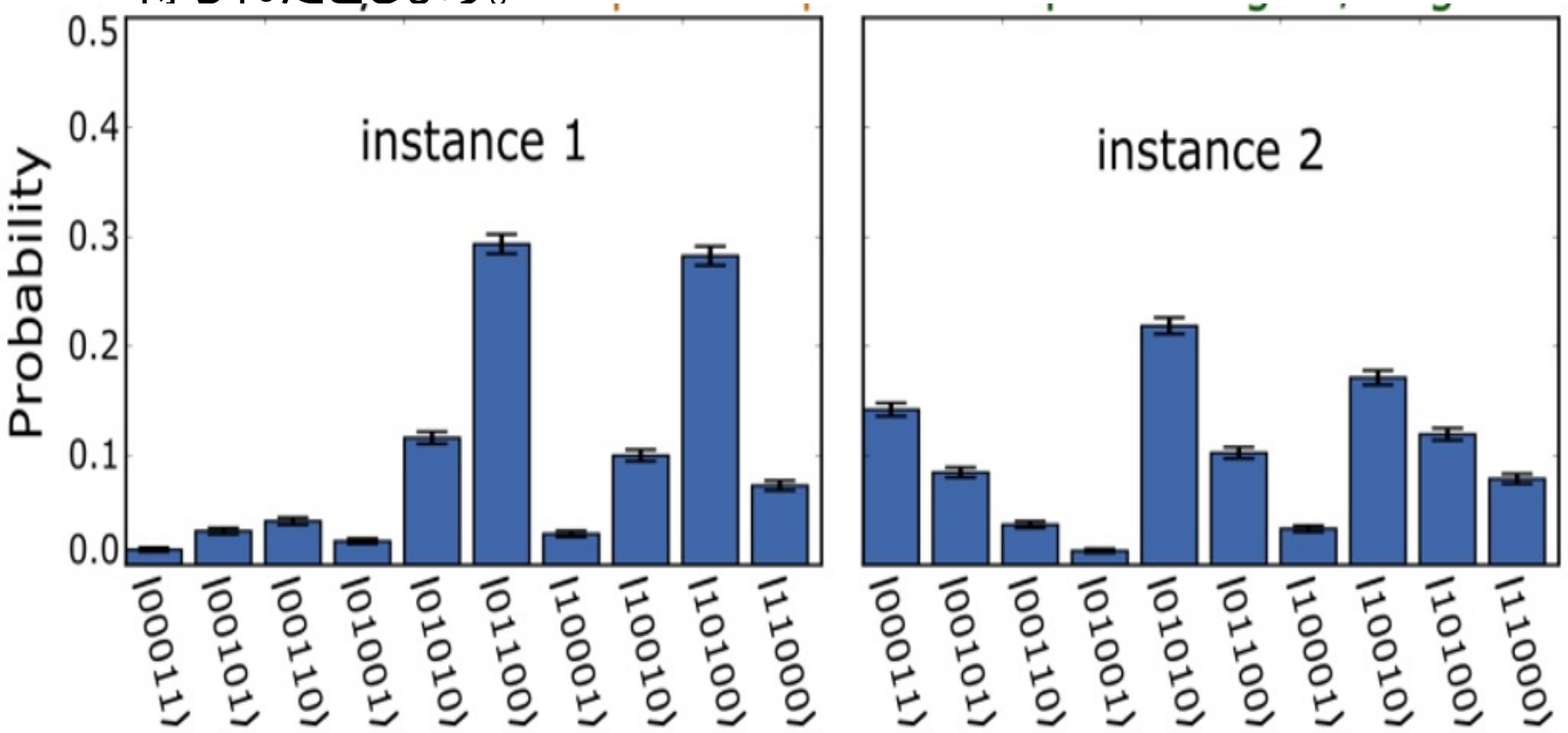
ランダムに量子回路を生成する

- ランダムに量子回路を生成する。この回路が何を計算しているかは考えない。
- 二つの別のランダム量子回路を、インスタンス1とインスタンス2としよう。



ランダム量子回路の出力をサンプリングし、出力の分布をチェックする

- 二つの量子回路の出力をサンプリングして、次のような分布が得られたとしよう。



得られた分布は、回路の特徴を反映している

- インスタンス1の回路と、インスタンス2の回路は、どちらもランダムに作られたものだが、それぞれ異なった回路である。その回路の違いが、分布の違いに反映している。
- サンプリングの数を増やしていけば、それぞれの回路に固有な分布の特徴は、いっそうはっきりしたものになってゆくだろう。

回路図が与えられれば、コンピュータを使って出力をシミレートできる

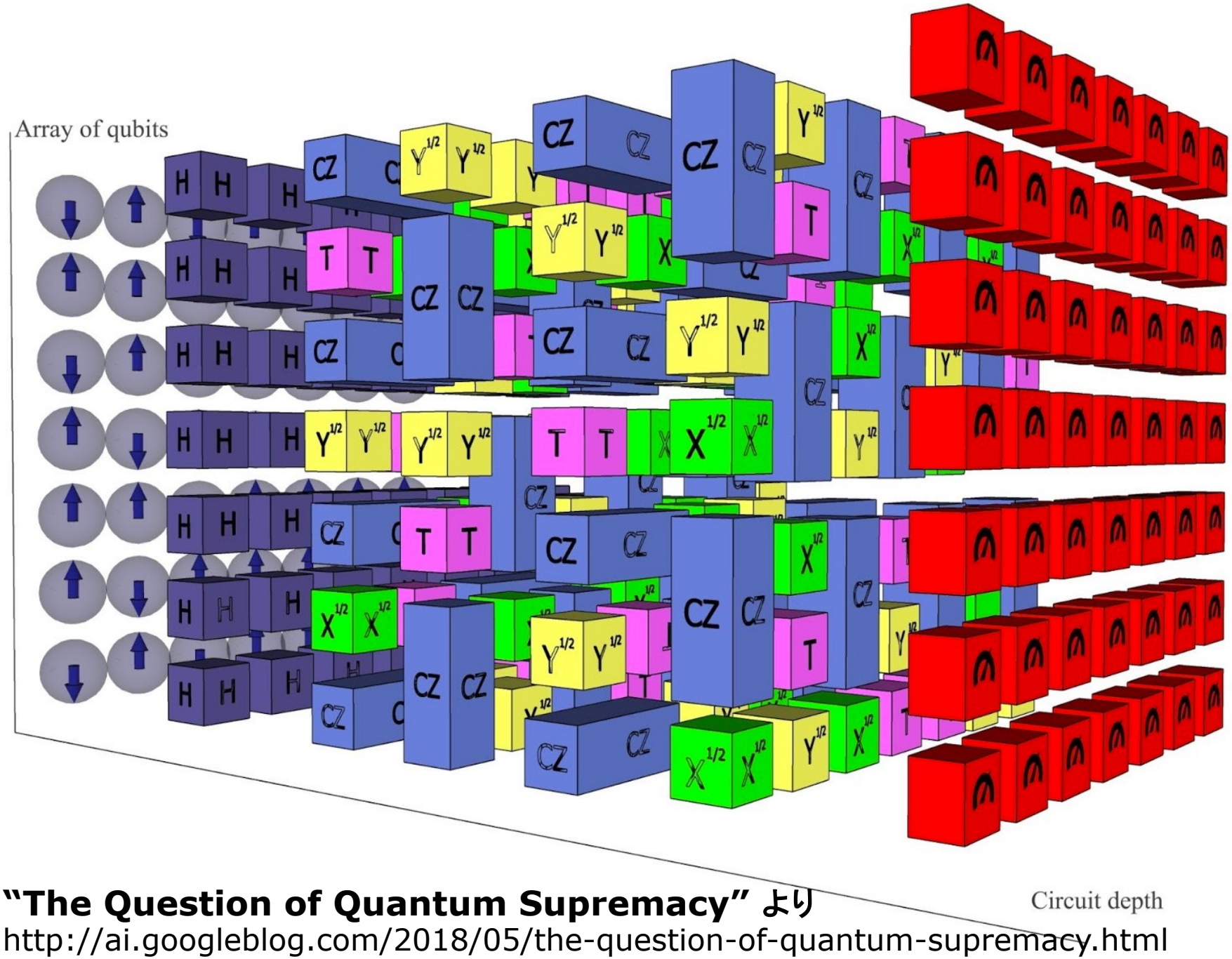
- もしも、インスタンス1とインスタンス2の回路図が与えられれば、コンピュータを使って、その出力をシミレートでき、サンプリングの数を増やせば、量子回路を使わなくても、正確な分布を得ることができるだろう。

- 問題は、これからである。
  量子回路の出力のサンプリングで作られた分布と、コンピュータの回路シミレートのサンプリングで作られた分布は、サンプル数を増やせば、基本的に同じものになるはずである。
- 量子回路もコンピュータでのシミレーションも、基本的には、「同じ仕事」をしたと考えることができる。それでは、この同じ仕事に要した時間は、それぞれ、どれくらいかかるのだろう？

ランダム量子回路を使った、量子優越性の実証

- 今回のGoogleの実験は、ランダム量子回路の出力を直接サンプリングする方が、コンピュータを使ってシミレートするよりも、圧倒的に速いことを示そうとしたものである。

- 実際、実験では、53qubit x 20段（これを「深さ」という）上の量子回路の100万回のサンプリングを 200秒で終えた。
- スーパーコンピュータが、この回路のシミレーションを行おうとすると、膨大な時間がかかる。論文では、それを「1万年」と見積もったが、そこは違っていたようだ。IBMの見積もりによると、「2.5日」だという。



“The Question of Quantum Supremacy” より
http://ai.googleblog.com/2018/05/the-question-of-quantum-supremacy.html

実験の評価

私はなぜそれを
量子優越性と呼んだのか？

Why I Called It ‘Quantum Supremacy’

Preskill **2019/10/02**

https://www.quantamagazine.org/john-preskill-explains-quantum-supremacy-20191002/

なぜ、この言葉を提案したか？

私は、この新しい言葉で、現在が我々の惑星の歴史の中で、特別の時期だと言うことを強調したかったのだ。すなわち、現在は、量子物理学の原理に基づく情報技術が登場し隆盛になる時期なのだと。

他の言葉の可能性も考えたのだけど、それらは退けて、私が伝えたいポイントをもっとも捉えている言葉として、この言葉に決めた。

この言葉の代わりの一つは、今でも広く使われている「量子アドバンテージ」なのだが、それは、私には「優越性」の持つパンチが欠けている。競馬で、鼻の差で勝っても、それはアドバンテージだ。

それとは対照的に、ある計算について、量子コンピュータのスピードは、古典コンピュータのスピードを、遥かに超えている。少なくとも、原理的には、それが正しいのだ。

反対論と擁護論

「量子優越性」という言葉は、その概念が問題ではないにしても、2つの理由で議論の余地があることが明らかになった。一つは、「白人の優越性」という言葉との連想を通じて、忌まわしい政治的スタンスを呼び起こすということである。もう一つの理由は、この言葉が、量子テクノロジーの状況に関する既に誇張された報道をさらに悪化させるということである。

第二の反対論は、予期していたものであったが、第一の反対論は予見することができなかった。

いずれにしろ、この言葉は人の心を捉え、GoogleのAI量子チームは、特別の熱意を持ってこの言葉を擁護してきた。

Googleの実験について

最近のGoogleの論文は、それが正しいものなら、それは実験物理学における驚くべき成果であり、量子コンピューティングハードウェアの急速な進歩のあかしである。関係者全員に心からのお祝いを申し上げたい。

実験結果自体は、意味のある情報を持たないにしても、しかしながら、このデモが示したことは、依然として重要である。量子コンピューターの出力が従来のスーパーコンピューターの出力と一致することを確認することにより（計算に数千年もかからない場合だが）、チームはデバイスを理解し、それが予想した通りに振る舞うことを確認したのだ。ハードウェアが機能していることがわかったので、さらに有用なアプリケーションの研究を開始できる。

NISQ時代の先駆けとしての Googleの実験

Googleによって達成されたと伝えられる量子優越性のマイルストーンは、実用的な量子コンピューターの研究における極めて重要なステップである。私は、今、明けつつある時代について一つの言葉があった方がいいと 考えて、最近、NISQという言葉を作った。（riskと同じ韻を踏んでいる。）

Googleチームは、以前は解決できなかった問題を解決する為の、十分な大きさで正確な量子マシンを構築できるようになったことを明らかにした。それは、先駆けとして、NISQ時代の始まりを告げるものだ。

Part IV

「エンタングルする知性」の認識
-- MIP*=RE --

4/10 マルゼミ「楽しい哲学」

Agenda Part IV

「エンタングルする知性」の認識

-- MIP*=RE --

- 量子の力を借りた人間の認識能力拡大への期待
  - 量子コンピュータとNP-完全問題
  - 量子の力を借りた人間の認識能力の拡大の試み
  - MP* = エンタングルした「全能者」
- MIP*=RE定理とは何か？
- nonlocal game と Interactive Proof
  - nonlocal ゲームは、Interactive Proofである
  - Interactive Proofは、nonlocal ゲームである
- MIP*はどのようなクラスか？
- MIP*=REの認識論的含意


量子の力を借りた
人間の認識能力拡大への期待

量子コンピュータとNP-完全問題

量子コンピュータの計算能力は、素晴らしいものです。それは、ある問題群（例えば、素因数分解のような）に対しては、古典コンピュータの計算能力の指数関数的高速化を可能にします。

量子コンピュータのアイデアの登場とともに、量子コンピュータが古典コンピュータで解くには指数関数的時間のかかる「NP-完全問題」を多項式時間で解くのではという期待がうまれました。ただ、それは不可能です。

先日の複雑性クラスの関係図を、改めて見て欲しいのですが、「NP-完全」のクラスは、量子コンピュータが多項式時間で解くことができる BQP クラスのはるか外側に存在しています。

複雑性クラスと問題の例

より難しい

n x *n* チェス

n x *n* 碁

箱詰め問題

地図の塗り分け

トラベリング・セールスマン

n x *n* 数独

グラフ同型問題

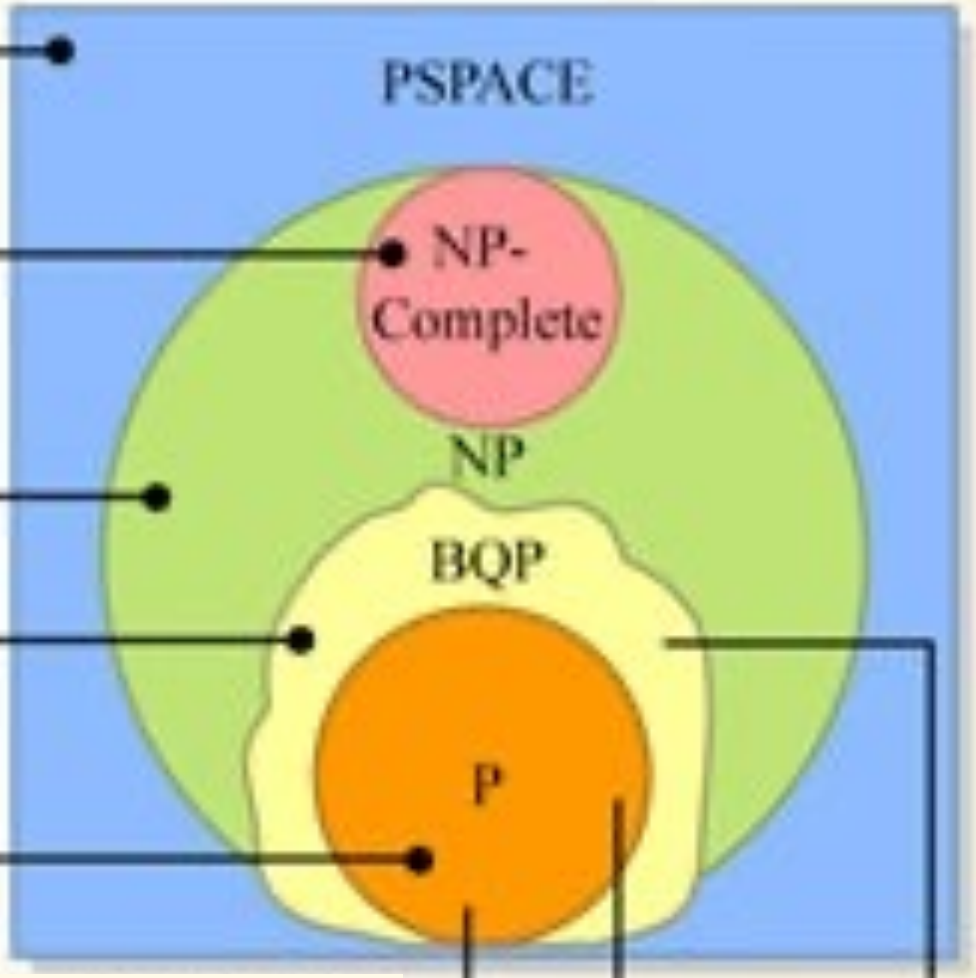
素因数分解

離散対数

グラフの接続性

素数判定

マッチ・メーキング



古典コンピュータで
効率的に解ける問題

量子コンピュータで
効率的に解ける
問題

量子の力を借りた
人間の認識能力の拡大の試み

それでは、量子の力を借りた人間の計算能力拡大の試み、それは人間の認識能力の拡大の試みを意味するのですが、それは現在のスタイルの量子コンピュータの進化の延長上の限界 BQPで頭打ちなのでしょうか？

もっとも、こうした問題意識自体が、そもそも混乱していることは、次のように考えればわかります。チューリングマシンが多項式時間で計算可能な能力の限界 P は、人間＝機械の双方の計算能力の限界と見做せるのですが、BQPは機械のみが持ちうる能力です。人間は機械の助けなしには単独ではその能力を持つことは出来ません。

「人間」の認識能力の拡大？

量子の力を借りた人間の認識能力の拡大というのは、量子機械の力を借りた人間の認識能力の拡大に他なりません。

人間の認識能力の未来を考えるのなら、裸の人間の生まれ持った能力だけで、人間の認識能力を語ることは出来ないのです。宇宙のどこかには、古典チューリングマシンではなく量子チューリングマシンと同じ計算能力を、単独で生得的に持つ知的生命が存在するかもしれないのですが。

話がSFみたいになってきたのですが、2020年に証明された「MIP*＝RE定理」も、それが想定していることを考えれば、SFみたいな話に聞こえるかもしれません。

MP* ＝ エンタングルした「全能者」

先に、「数学的全能者」と「人間」の対話によって認識を拡大する枠組みとして「対話型証明　Interactive Proof」を紹介しました。MIP*　(Multi Prover Interactive Proof with Entanglement)というのは、この対話型証明の発展形です。

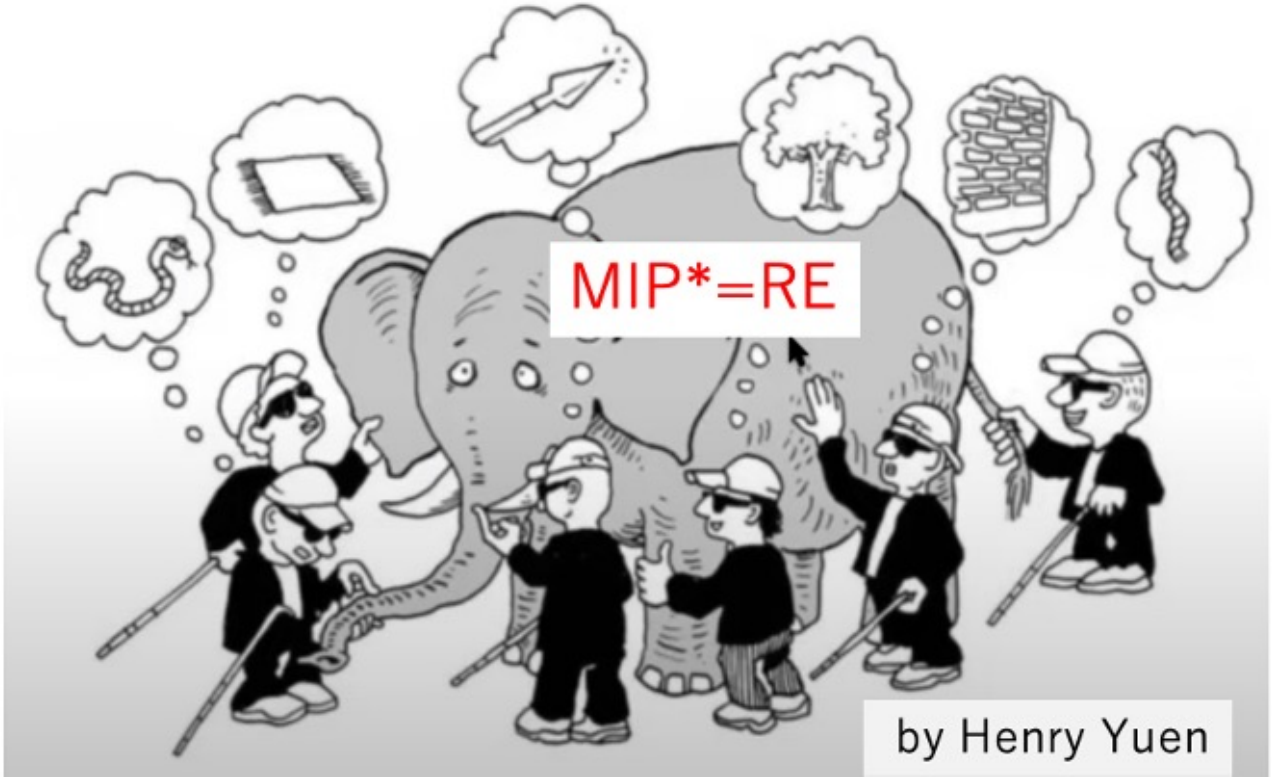
ここでは、人間が対話する「全能者」が一人から二人に増えています。さらに、この二人の「全能者」は、エンタングルした量子を共有しています。二人の「全能者」は、直接にはコミュニケーションすることはないのですが、そもそも、エンタングルしているのです。

エンタングルしている全能者！

「MIP*＝RE定理」は、この「エンタングルしている全能者」二人と、人間が対話を繰り返したら、何が分かるかを考えたものです。

MIP*＝RE定理の解釈

「MIP*＝RE定理」は、何を意味しているのでしょう？　様々な解釈が可能です。「MIP*＝RE定理」の証明者の一人 Henry Yuenは、それを「群盲、象を撫でる」に喩えています。



MIP*=RE定理とは何か？

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の値を持つかどちら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の値を持つかどちら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。

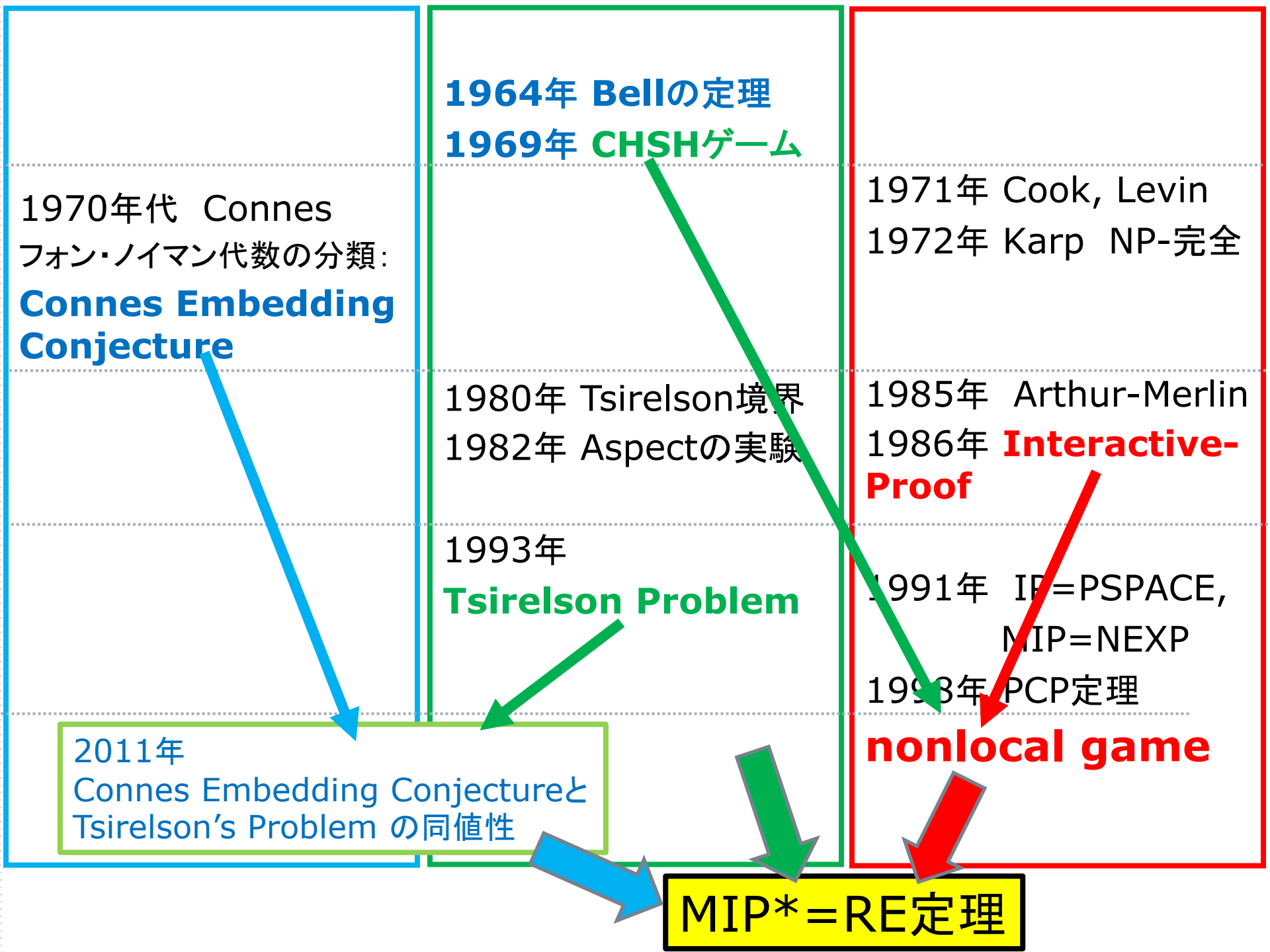
論文 “MIP*=RE” の概要

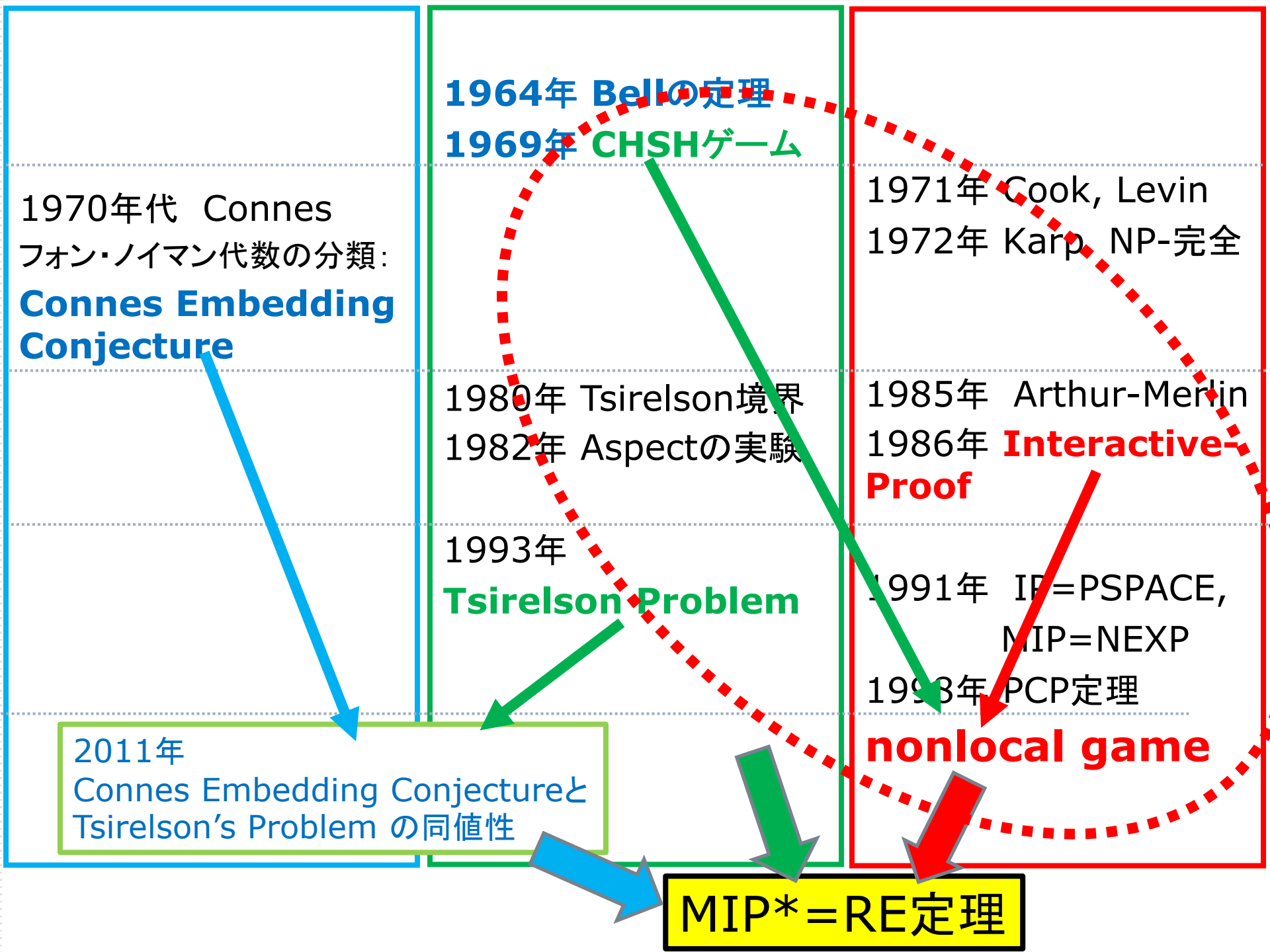
1. **MIP*=RE :**
   我々は、古典論的検証者が、エンタングルメントを共有する全能の量子論的証明者と相互作用して、決定することが出来るMIP* 言語のクラスが、帰納的可算な言語 REのクラスに等しいことを示した。
2. **Halting Problem :**
   我々の結果の直接の副産物は、「停止問題」から、二人のプレーヤーによるnonlocalゲームがエンタングルした値1を持つかあるいは最大でも1/2の値を持つかどちらかなのかを決定する問題への、実効的な還元が存在するということである。
3. **Tsirelson’s problem :**
   エンタングルした値の決定不可能性は、「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の値を持つかどちら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。

nonlocal game と Interactive Proof


1964年 Bellの定理
1969年 CHSHゲーム
1970年代 Connes
フォン・ノイマン代数の分類:
Connes Embedding Conjecture
1971年 Cook, Levin
1972年 Karp NP-完全
1980年 Tsirelson境界
1982年 Aspectの実験
1985年 Arthur-Merlin
1986年 Interactive-Proof
1993年
Tsirelson Problem
1991年 IP=PSPACE,
MIP=NEXP
1998年 PCP定理
nonlocal game
2011年
Connes Embedding Conjectureと
Tsirelson's Problem の同値性
MIP*=RE定理


1964年 Bellの定理
1969年 CHSHゲーム
1970年代 Connes
フォン・ノイマン代数の分類:
Connes Embedding Conjecture
1971年 Cook, Levin
1972年 Karp, NP-完全
1980年 Tsirelson境界
1982年 Aspectの実験
1985年 Arthur-Merlin
1986年 Interactive-Proof
1993年
Tsirelson Problem
1991年 IP=PSPACE,
MIP=NEXP
1998年 PCP定理
nonlocal game
2011年
Connes Embedding Conjectureと
Tsirelson's Problem の同値性
MIP*=RE定理

nonlocal game と Interactive Proof

- CHSHゲームやMagic Squareゲーム等をnonlocal gameと呼びます。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す。
- 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すが、それは次に見るように、Interactive Proofと、同じ構造をしています。
- 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です。

21世紀になって気づかれたこと

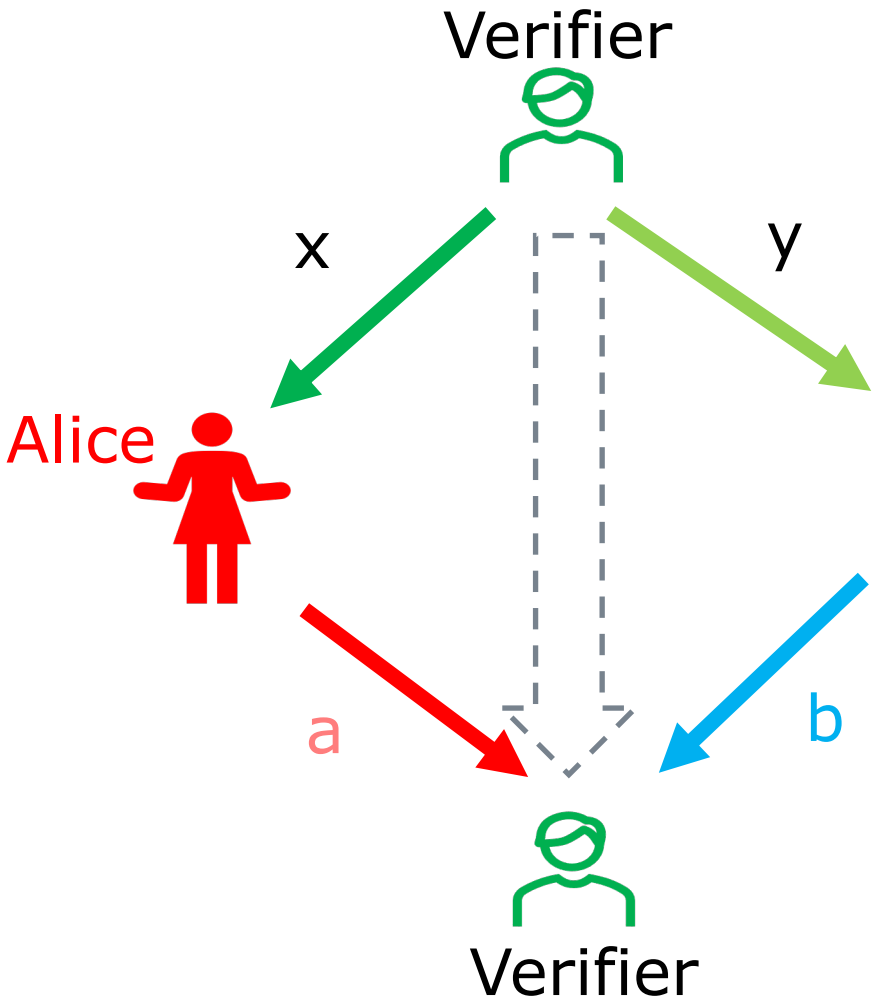
2004年、コンピュータ・サイエンティストのRichard Cleve, Peter Hoyer, Ben Toner, John Watrousらは、Bellの思考実験がInteractive Proofと極めて似ていることに気づきます。

彼らは、量子的なMulti-Prover Interactive Proof MIP*を研究することを提案します。

Bellの論文から、40年後のことでした。

アインシュタインが「パラドックス」としてエンタングルメントを発見した時からは 70年が経っています。

nonlocalのゲームの定式化



①

質問の分布：

$\mu(x, y)$

②

質問と回答の相関：

$p(a, b \mid x, y)$

③

ゲームの勝敗を定義する関数：

$D(a, b, x, y) \rightarrow \{0, 1\}$

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の一様にランダムな分布、
- $p(a, b \mid x, y)$
  $= p(a, b \mid 0, 0) + p(a, b \mid 0, 1) + p(a, b \mid 1, 0) + p(a, b \mid 1, 1)$、
- $D(a, b, x, y)$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の一様にランダムな分布、
- $p(a, b \mid x, y)$
  $= p(a, b \mid 0, 0) + p(a, b \mid 0, 1) + p(a, b \mid 1, 0) + p(a, b \mid 1, 1)$、
- $D(a, b, x, y)$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 $\omega(\mathrm{G},\mathrm{p})$は、次の式で与えられる。

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

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ω(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

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

- $\omega_c(\mathrm{CHSH}) = 3/4$
- $\omega_q(\mathrm{CHSH}) = \cos^2(\pi/8)$

- $\omega_c(\mathrm{Magic\ Square}) = 8/9$
- $\omega_q(\mathrm{Magic\ Square}) = 1$

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$\mathcal{E}$ (G, p)で表す。

- $\mathcal{E}$ (CHSH, 3/4) = 0
- $\mathcal{E}$ (CHSH, $\cos^2(\pi/8)$) = 2

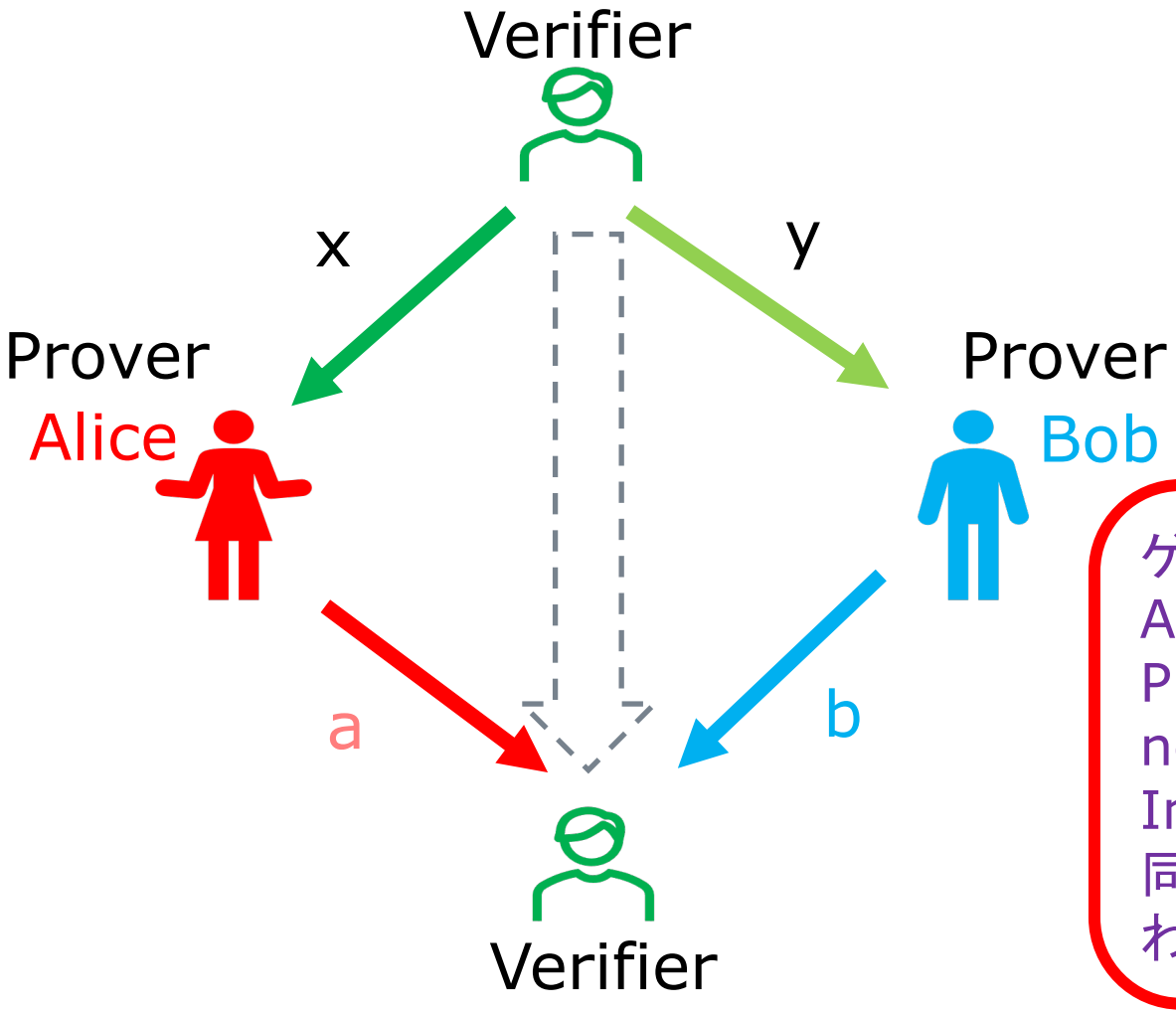
- $\mathcal{E}$ (Magic Square, 8/9) = 0
- $\mathcal{E}$ (Magic Square, 1) = 4

MIP*研究の課題

Bellの思考実験がInteractive Proofと極めて似ていることに気づき、量子的なMulti-Prover Interactive Proof MIP*を研究することを提案したCleveらが提起した問題は、次のようなものでした。

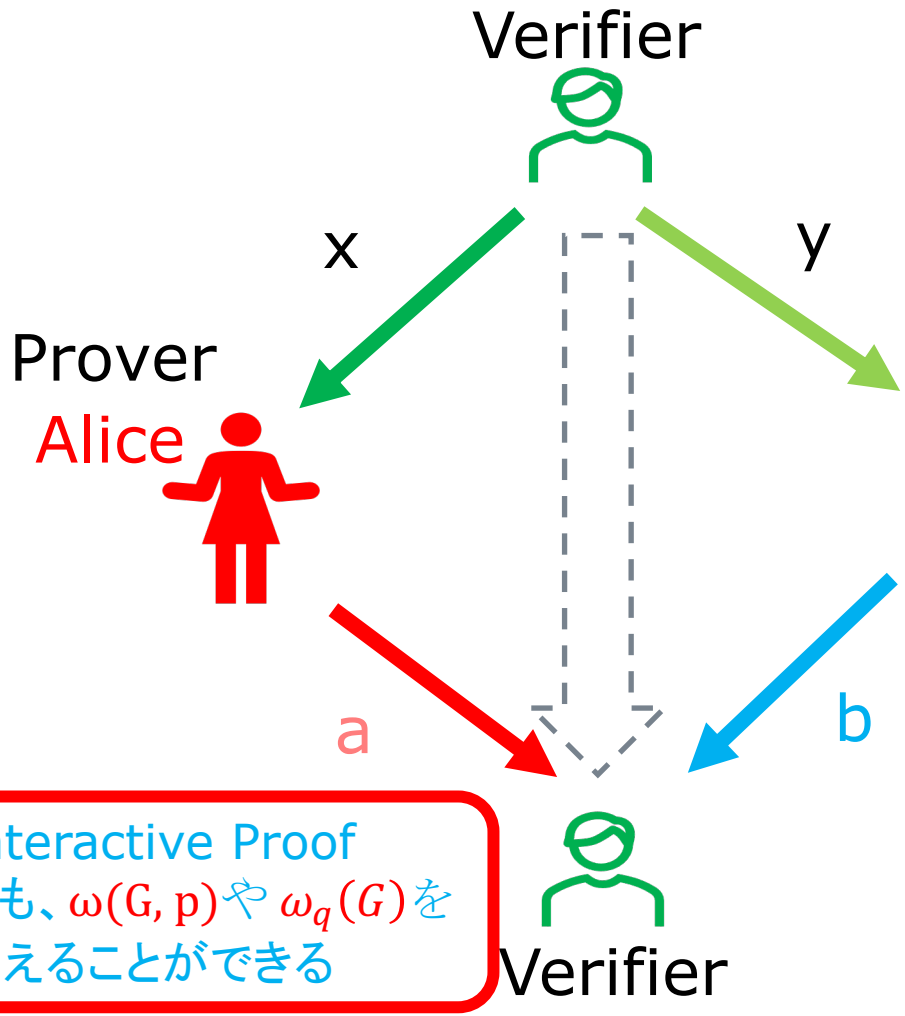
$\omega_q(G)$を近似的に求めるアルゴリズムは存在するだろうか？

nonlocal ゲームは、Interactive Proofである



ゲームのプレーヤーの
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



質問の分布：
$\mu(x, y)$

質問と回答の相関・戦略：
$p(a, b \mid x, y)$

ゲームの勝敗を定義する関数：
$D(a, b, x, y) \rightarrow \{0, 1\}$

Interactive Proof
でも、$\omega(G, p)$や $\omega_q(G)$を
考えることができる

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す。

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ければならない。
   この条件を Completeness と呼びます。
2. Xが偽であるなら、Verifierは高い確率で、それを拒否できなければならない。
   この条件を Soundness と呼びます。

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す。

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、次の問題に関連します。「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、先に見た 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す。

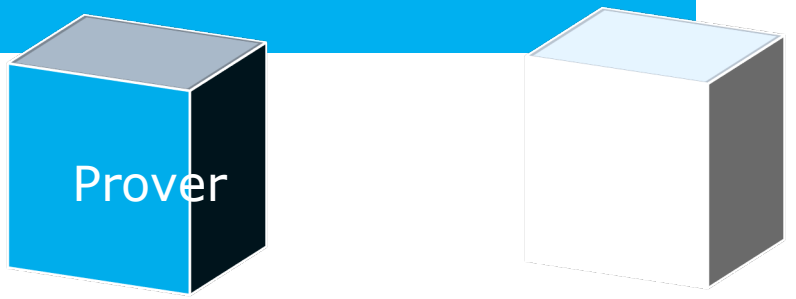
Quantum Game Approximation Problem(**Q-GAP**)は、ゲームGが与えられた時、次のようなαを求める問題です。

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

MIP*の複雑性は、Q-GAPに還元されることが知られています。

NP ⊆ MP*

3SAT: φは充足可能か？



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

SATをエンコードした
nonlocal ゲーム

3SAT式

$\varphi \rightarrow G_\varphi$

φ は充足される → $\omega_q(G_\varphi) = 1$ Completeness

φ は充足されない → $\omega_q(G_\varphi) = 0$ Soundness

Q-GAP問題は、単純な問題ではない

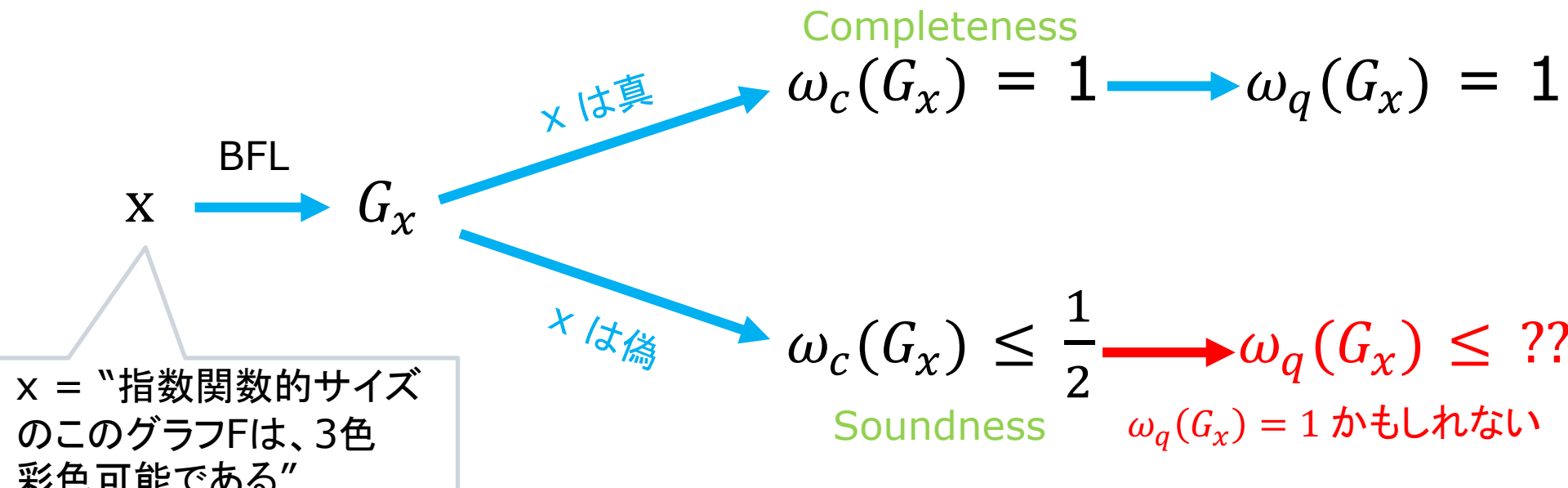
3SATの場合のQ-GAPは、SATをエンコードしたnonlocal ゲームG_φが与えられた時、次のようなαを求める問題です。

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

この問題は、φが充足可能かを決定する問題に帰着します。

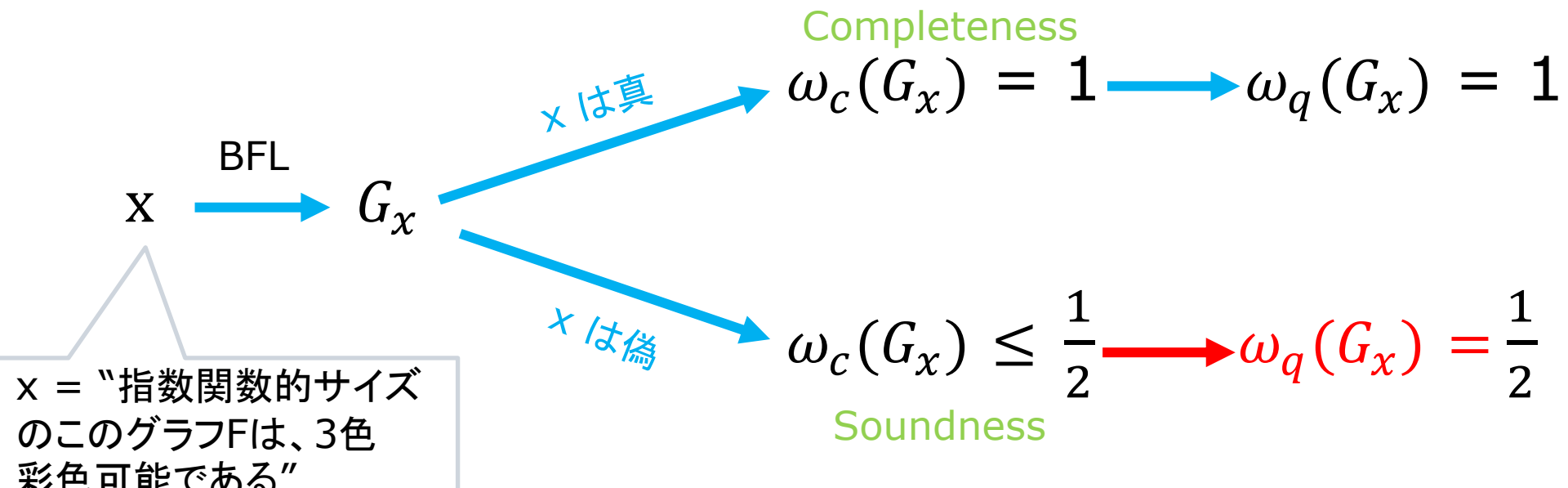
MIP ⊆ MIP* ?

MIP ⊆ MIP* かどうかは自明ではありません。
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ります。その場合、MIP*の証明能力は MIPより低くなるかもしれません。Soundnessは、保存されないかもしれないのです。



MIP ⊆ MIP*

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



MIP*の上限は？

Q-GAPを解くアルゴリズムは存在するのでしょうか？

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す。

- それは、Double-Exponential 2^{2^n}な時間で解ける。
  だから、MIP $\subseteq$ DOUBLE-EXP である。

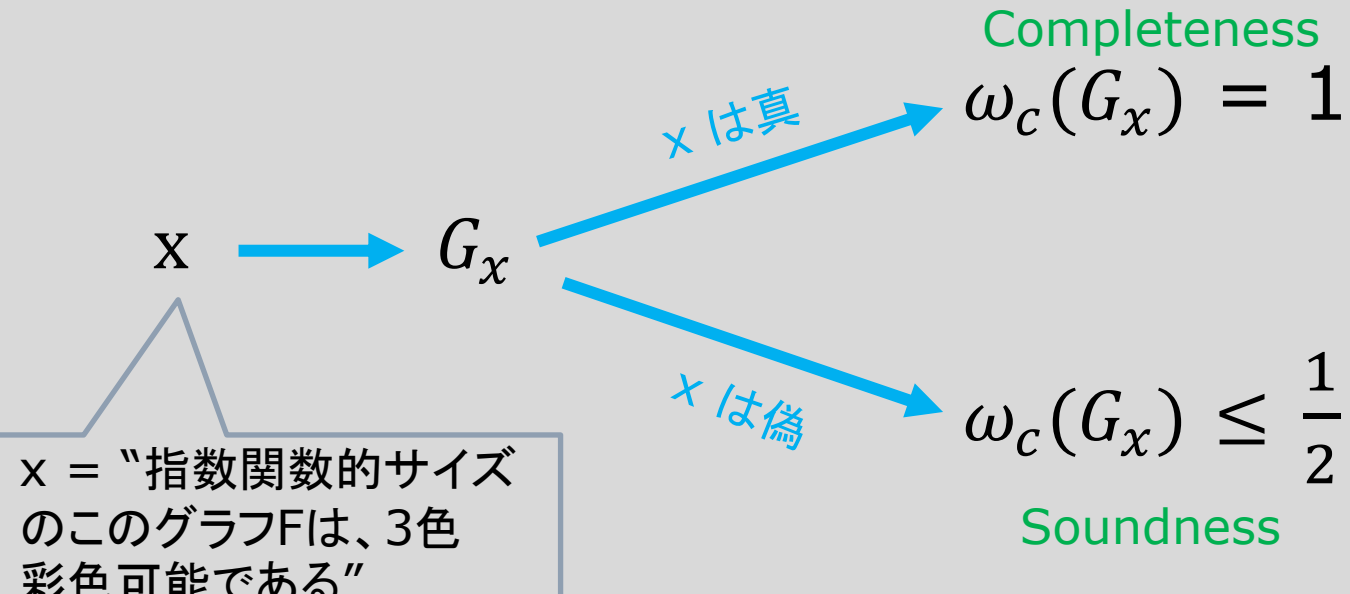
Q−GAPの場合には、可能な戦略の数え上げは難しいです。
というのも、Proverの戦略は、利用するエンタングルする量子の数ごとに無限個ありうるからです。

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す。

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ます。

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



NEEXP ⊆ MIP*

- 2019年、Anand Natarajan と John Wrightは、**NEEXP ⊆ MIP*** を証明しました。
  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す。
- 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ます。
- 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、引き継がれていきます。

NEEXP ⊆ MIP* から MIP* = RE 証明へ

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ます。

RE ⊆ MIP*

NP ⊆ MIP*　　（自明）

NEXP ⊆ MIP*　　(1991 BFL)

NEEXP ⊆ MIP*　　（2019 Anand , Vidick)

NEEEXP ⊆ MIP*

NEEEEXP ⊆ MIP*

NEEEEEXP ⊆ MIP*

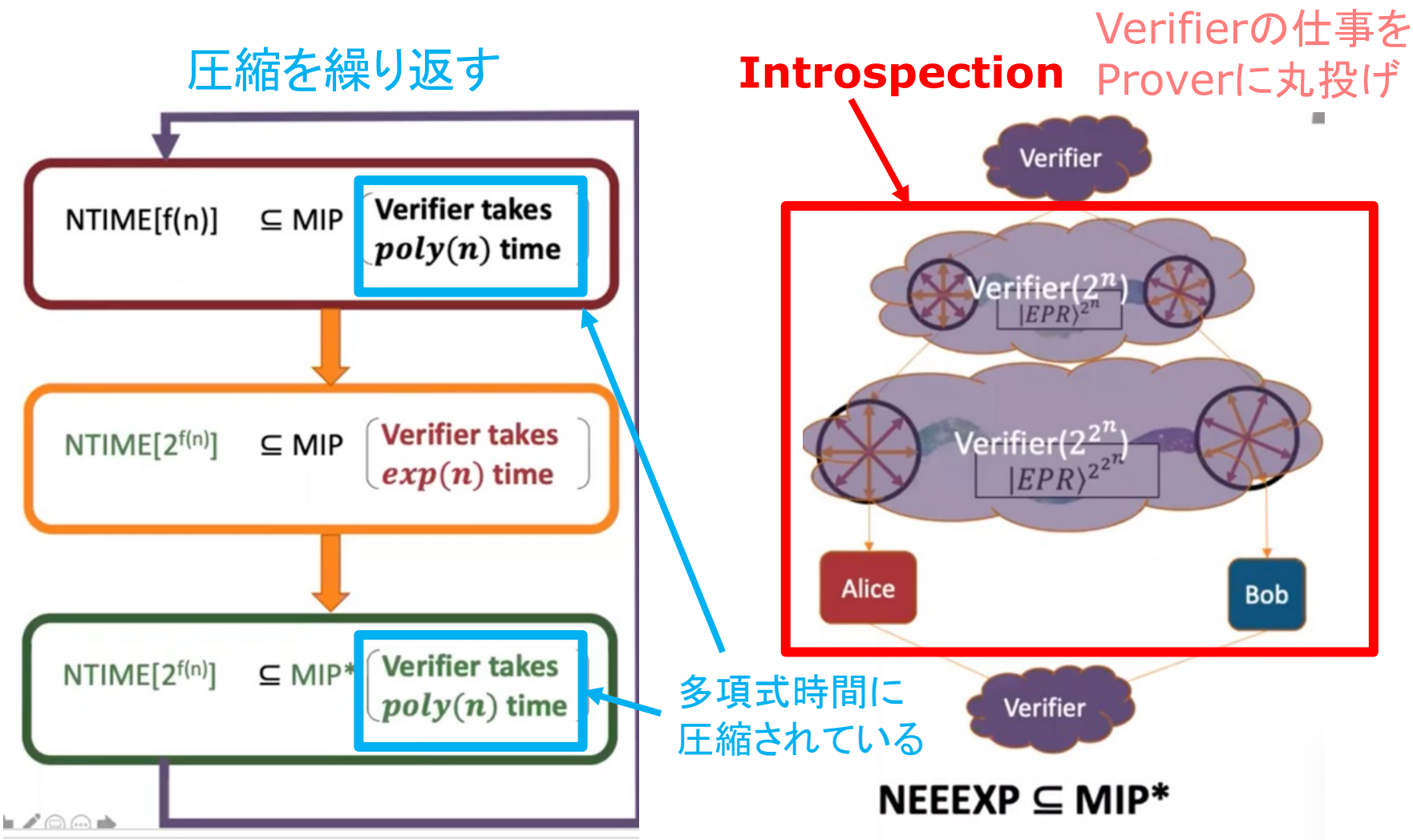
NEEEEEEXP ⊆ MIP*

$2^{2^{2^{\cdot^{\cdot^{\cdot}}}}}$

...

RE ⊆ MIP*　　（2020 JNVWY MIP*=RE)

IntrospectionとCompressionのイメージ
NEEEXP ⊆ MIP* の場合



MIP*=REの認識論的含意

ゲーデルの不完全性定理と MIP*＝RE定理

「MIP*＝RE定理」というのは、MIP*という複雑性のクラスが、「決定不能」だということを述べている定理です。

それは、ゲーデルの「不完全性定理」に端を発する、一連の「決定不能」型定理の一つと考えることが出来ます。

ゲーデルの結果は、人間の認識可能性の一つの限界を示すものとして、多くの人にいわば認識論的・哲学的なレベルで衝撃を与えました。

ただ、その方法の適用は、数学の基礎の理論の内側にとどまっていて、科学の方法論そのものに影響を与えることはなかったし、ゲーデルの定理が、他の数理科学の分野の問題解決に応用されたことはなかったように思います。

21世紀の「不完全性定理」とも呼ぶべき「MIP*＝RE定理」は、この点では、明らかに様相が異なります。

それは、新興科学としての「コンピュータ・サイエンス」の「決定不能」型定理として登場したのですが、その定理は、狭い意味での「コンピュータ・サイエンス」の枠を超え、純粋数学や物理学の基礎理論に、重要な応用を持つのです。

エンタングルしたnonlocalゲームの値の「決定不能」性は、量子力学の基礎の「ティレルソンの問題」に対する否定的な答えを導きます。また、この結果は、数学の作用素環論の長年の難問だった「コンヌの埋め込み予想」否定的に解決しました。

計算可能性理論と計算複雑性理論の接するところ「拡大されたCHテーゼ」の誤り

計算複雑性理論は、計算可能性理論の達成を受けて、決定可能なもの（計算可能なもの）にフォーカスを合わせて、その現実的な計算の「手に負えなさ」の階層を研究することを課題としてきました。

MIP*＝RE の左辺MIP*は複雑性のクラスで、右辺はREは、計算可能性理論の基本的カテゴリーです。

理論的には、計算可能性理論の枠組みの中でも、原理的には計算可能でも、いくらでも計算リソースを必要とする計算が存在することはよく知られていました。だからこそ計算複雑性理論が生まれたのですが。

ただ、計算可能性を「多項式時間」での計算可能性に制限することが当たり前のようになっていきます。これを「拡大されたチャーチ・チューリングのテーゼ」というのですが、それは間違ったものだと、思います。

決定論的な認識と確率論的な認識

証明へのInteractive Proofの手法の導入は、それまで決定論的なものと思われていた証明過程に、確率や近似の概念を導入することを可能にしました。

そのことは、確率的なアプローチに基づく、量子論的な自然認識のスタイルに適合的です。おそらく、あまりに複雑なものに対しては、我々は確率論的にアプローチするしかないのだと、僕は考えています。

そして「情報」というものは、もともとそういう性質を持ったものです。

エンタングルした
「全能」の「証明者」たちは何者か？

第一に考えるべきことは、この定理の証明で中心的な役割をはたす、可能的には無限個のエンタングルメントを共有し、時には人間を欺く「不実」で、しかしながら「全能」の「証明者」たちは何者かということです。

それは、我々が認識の対象とする「自然」あるいは「宇宙」の「人格化」だと理解すればいいと僕は思います。

我々は、我々の「有限」な認識を組み合わせて、「近似的」に対象に迫ろうとします。しかし、「宇宙」は、あくまでも「無限」で、そうした「有限」の「近似」では、覆い尽くせないのです。

ただ、それにもかかわらず重要なことは、我々は、そうした「関係性」自体を正確に認識できるだけでなく、その「有限」な認識への実効的な「還元」プロセスを、ある場合には数学的に定式化できるということです。これは大きな希望です。

機械と人間の関係

第二に考えたいのは、もっと問題を身近なものに引き付けて、「宇宙」ではなく「機械」と人間の関係、人工知能論の課題としてこの定理の含意を考えることです。

確かに、現実の量子コンピュータによる近年の「量子優越性」の実証は、かつて我々が、機械の知能と人間の知能の同一性の根拠に、両者の計算能力の同一性においた枠組みの見直しを迫るものです。

たとえ、エンタングルメントで結合されていなくても、量子機械は、古典的チューリング・マシンに等しい我々人間より、高い計算能力を持ちうるのです。

それでは、多数のエンタングルメントで結合された複数の量子機械のグループは、我々人間にとってどのような「知能」の持ち主に見えるのでしょうか？　さらに、こうした量子機械たちとの「対話」は、我々の認識をどのように拡大してくれるのでしょうか？

こうした問題に応えるいくつかのヒントは、「MIP*＝RE定理」の中に含まれていると僕は考えています。答えは、もちろん、まだありません。

ただ、我々は、新しい問題を新しく提起することができる段階の戸口に立ち始めています。適切に問題が提起されれば、答えはいずれ見つかるだろうと思います。

新しい科学へ

すこし、空想的だったかもしれません。ただ、空想は楽しいものです。

いずれにしても、現在の「コンピュータ・サイエンス」のただ中から、その経験主義的外皮を脱ぎ捨てて、情報と計算の科学が、新しい数理科学として誕生するのだと思っています。

それは、空想ではなく、いつか現実になるでしょう。