

量子計算モデル 参考資料

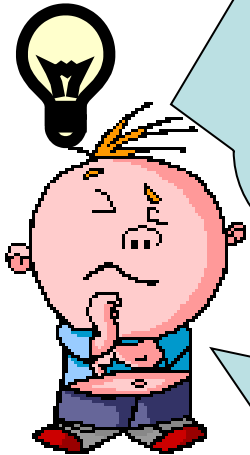
今井 浩

東京大学情報理工学系研究科コンピュータ科学専攻
JST ERATO-SORST量子情報システムアーキテクチャ

情報を処理する観点から

どうして量子計算・通信を研究するのか？

- 量子計算によって、古典計算・通信では現実的に解けない問題を、実際に解く
 - 今のコンピュータの高速化に量子力学が障害
 - その量子力学を肯定的に使って、今解けないものを解けるようにする



- 古典計算、確率計算の発展としての量子計算
 - 新計算モデルの開拓 — 限界の打破
 - 今のコンピュータ・情報処理方式への還元



- [Birch and Swinnerton-Dyer Conjecture](#)
- [Hodge Conjecture](#)
- [Navier-Stokes Equations](#)
- [P vs NP](#)
- [Poincaré Conjecture](#)
- [Riemann Hypothesis](#)
- [Yang-Mills Theory](#)

計算(情報処理;通信含む)とは何か

情報を

- まず何らかのルールで与え(入力)
- 何らかの物理状態で表現し(符号化)
- 所望の状態になるように操作し(計算)
- 所望の結果を得る(出力)

そして通信では

- その物理状態を伝送する(符号化・復号化)

計算モデル

1930年代

- Turing Machine
- Recursive Function Theory
- λ Calculus

1980年中ごろ:「計算は対話だ」!

- C. H. Papadimitriou: Games against Nature.
J. Computer & System Sciences, 1985.

現代:「Nature is computing」

- R. M. Karp (Turing賞(1985), 京都賞(2008))

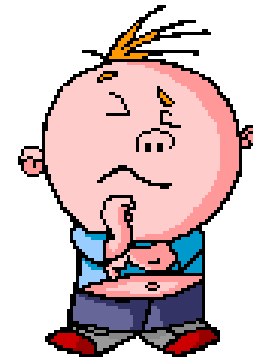
Nondeterministic Polynomial (NP)

- Two players: **prover**, **verifier**
 - **Prover** tries to convince verifier of her assertion by just given one certificate
 - **Verifier** must check validity of prover's assertion efficiently:
 - efficiently \Rightarrow in time polynomial to input length



Peggy (Prover)

Oracle
 $x = 1, y = 0, z = 1$
にして!



Victor (Verifier)

NP

$(x \vee y \vee z) \wedge (\bar{x} \vee \bar{y} \vee z) \wedge (x \vee \bar{y} \vee \bar{z})$ は satisfiable?

Computation Theory

undecidable

Halting problem of Turing Machine

decidable

Presburger arithmetic

$$2^{2^{2^{cn}}}$$

$$2^{2^{cn}}$$

**intractable=
exponential
time**

EXP
PSPACE
NP-complete

traveling salesman
graph isomorphism
integer factoring

$$\exp(O((\log n)^{1/3}(\log \log n)^{2/3}))$$

**tractable=
polynomial
time**

P
 $n^{3.5} L \log n$
 $\log \log n$

linear programming

$$n^{1.193}$$

$\sqrt{n} \times \sqrt{n}$ matrix multiplication

$$n \log n$$

sorting, FFT

$$n$$

median

n : input size

量子計算が現代計算を凌駕する点!?

- **Deutsch-Jozsa algorithm**
 - Exponential gap, but for a partial function...
- **Shor's quantum polynomial factoring**
 - Classically, only subexponential factoring
 - Polynomial Las Vegas algorithm for primality testing
 - does not provide a rigorous proof...
- **Grover's search algorithm**
 - Practically important, but theoretical non-exponential

⇒ そして多数: 隠れ部分群問題、量子ウォーク/探索

量子力学の観点から

1927 Solvay Conference on Quantum Mechanics

http://commons.wikimedia.org/wiki/Image:Solvay_conference_1927.jpgより



A. Piccard, E. Henriot, P. Ehrenfest, Ed. Herzen, Th. De Donder, E. Schrödinger, E. Verschaffelt, W. Pauli, W. Heisenberg, R.H. Fowler, L. Brillouin,
P. Debye, M. Knudsen, W.L. Bragg, H.A. Kramers, P.A.M. Dirac, A.H. Compton, L. de Broglie, M. Born, N. Bohr,
I. Langmuir, M. Planck, M. Curie, H.A. Lorentz, A. Einstein, P. Langevin, Ch. E. Guye, C.T.R. Wilson, O.W. Richardson

EPR and Bohr

MAY 15, 1935

PHYSICAL REVIEW

VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in

quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

OCTOBER 15, 1935

PHYSICAL REVIEW

VOLUME 48

Can Quantum-Mechanical Description of Physical Reality be Considered Complete?

N. BOHR, *Institute for Theoretical Physics, University, Copenhagen*

(Received July 13, 1935)

It is shown that a certain "criterion of physical reality" formulated in a recent article with the above title by A. Einstein, B. Podolsky and N. Rosen contains an essential ambiguity when it is applied to quantum phenomena. In this connection a viewpoint termed "complementarity" is explained from which quantum-mechanical description of physical phenomena would seem to fulfill, within its scope, all rational demands of completeness.

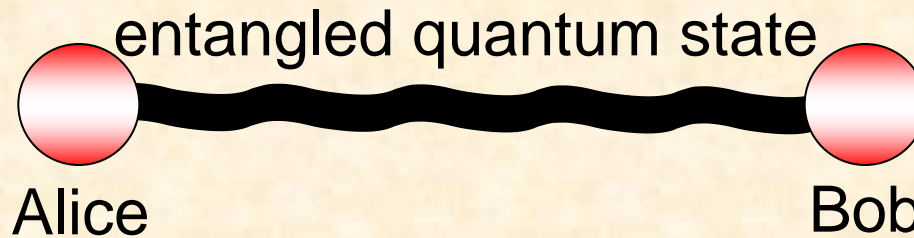
Bell-CHSH correlation experiment

two measurements
apply one

A_1



A_2



two measurements
apply one

B_1



B_2



Classical correlation:

$$-P(A_1) - P(B_1) + P(A_1B_1) + P(A_1B_2) + P(A_2B_1) - P(A_2B_2) \leq 0$$

Quantum correlation:

$$-P(A_1) - P(B_1) + P(A_1B_1) + P(A_1B_2) + P(A_2B_1) - P(A_2B_2) \leq \frac{1}{\sqrt{2}}$$

量子非局所性

量子対話証明

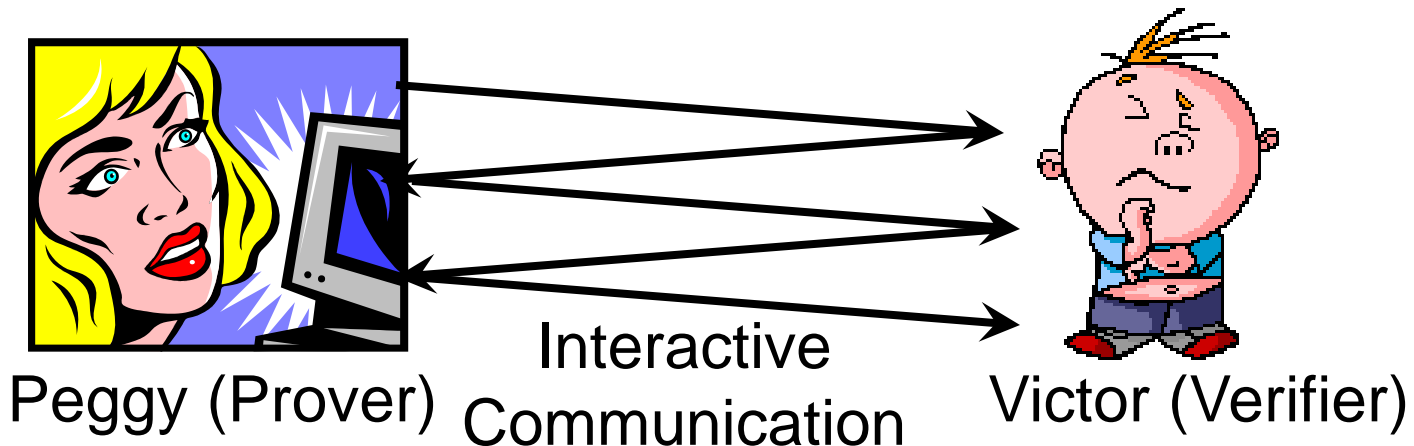
量子計算量理論

Interactive Proof System

[Babai 1985; Goldwasser, Micali, and Rackoff 1985]

- Two players: **prover**, **verifier**
 - **Prover** tries to convince verifier of her assertion with unbounded computational power
 - **Verifier** must check validity of prover's assertion probabilistically and efficiently:
 - probabilistically \Rightarrow with bounded error
 - efficiently \Rightarrow in time polynomial to input length

$IP=PSPACE$



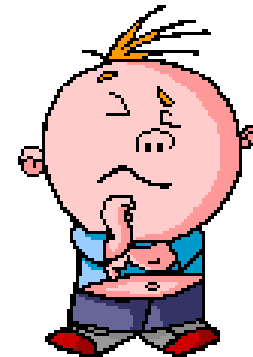
Nondeterministic Polynomial (NP)

- Two players: **prover**, **verifier**
 - **Prover** tries to convince verifier of her assertion by just given one certificate
 - **Verifier** must check validity of prover's assertion efficiently:
 - efficiently \Rightarrow in time polynomial to input length



Peggy (Prover)

Oracle
 $x = 1, y = 0, z = 1$
にして!



Victor (Verifier)

NP

$(x \vee y \vee z) \wedge (\bar{x} \vee \bar{y} \vee z) \wedge (x \vee \bar{y} \vee \bar{z})$ は satisfiable?

Example: Graph Non-Isomorphism

Graph Non-Isomorphism Problem (GNI)

INPUT: Two graphs G_1, G_2 of n vertices

QUESTION: For all permutation $\pi \in S_n$ on vertices,
 $\pi(G_1) \neq G_2$?

© Protocol of verifier V :

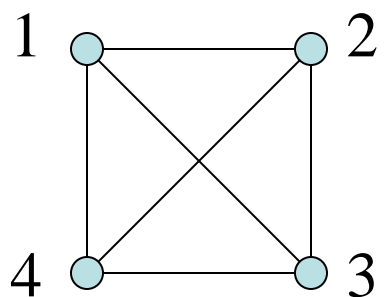
1. Choose an index $i \in \{1,2\}$ of graphs
and a permutation $\pi \in S_n$ at random.

Send a graph $\pi(G_i)$ to prover P

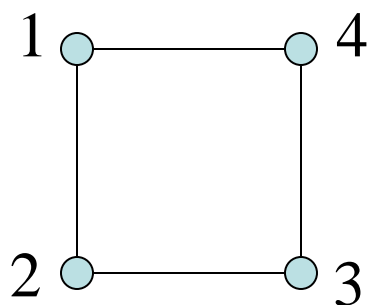
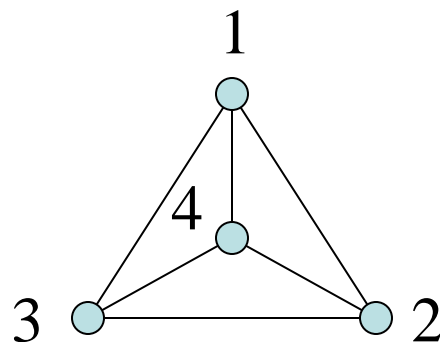
to ask which of the two is isomorphic to $\pi(G_i)$.

2. Receive an index j from P .

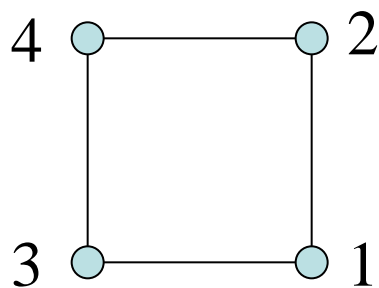
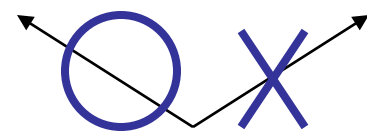
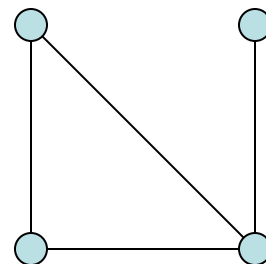
Accept iff $i = j$.



同型

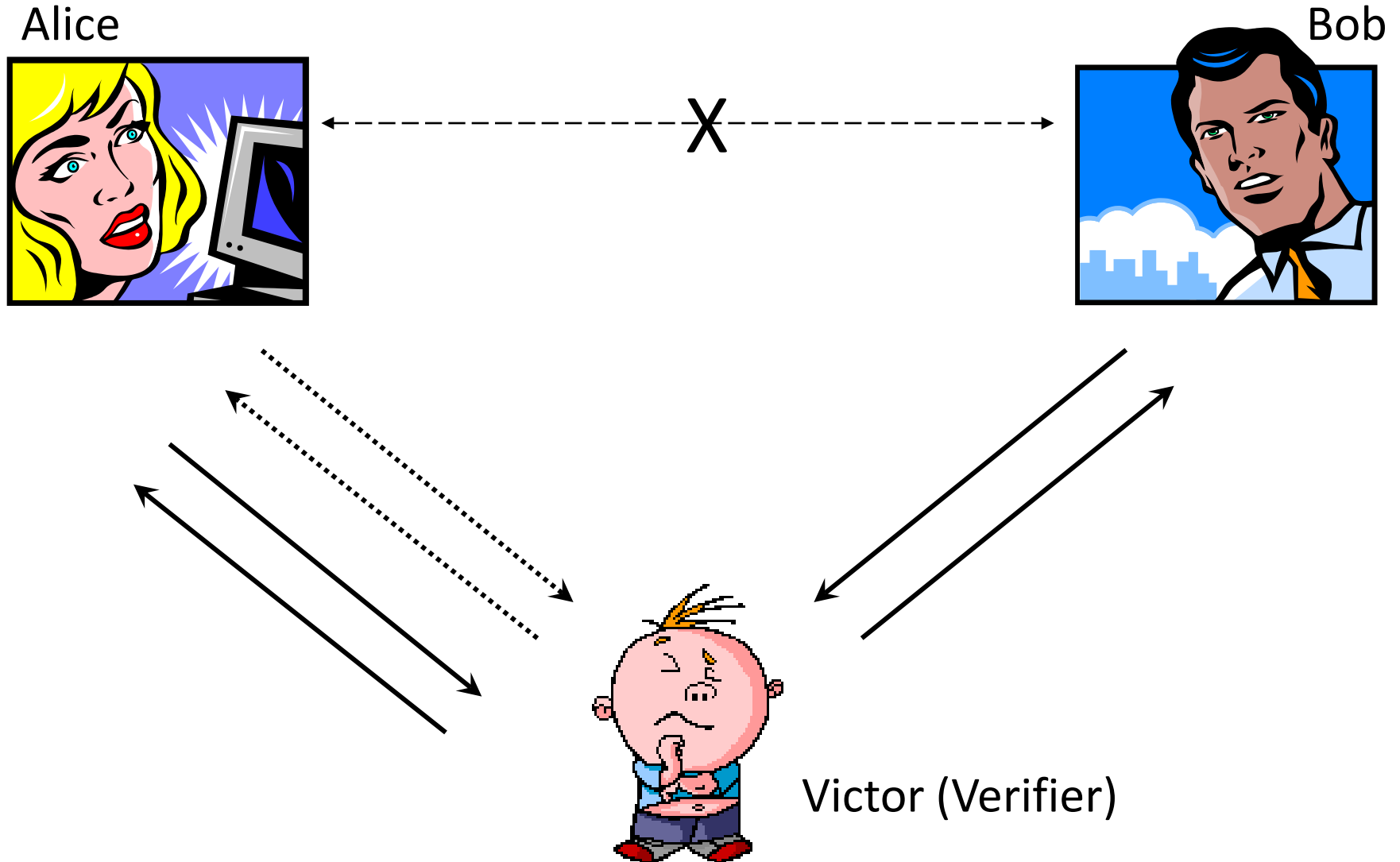


非同型

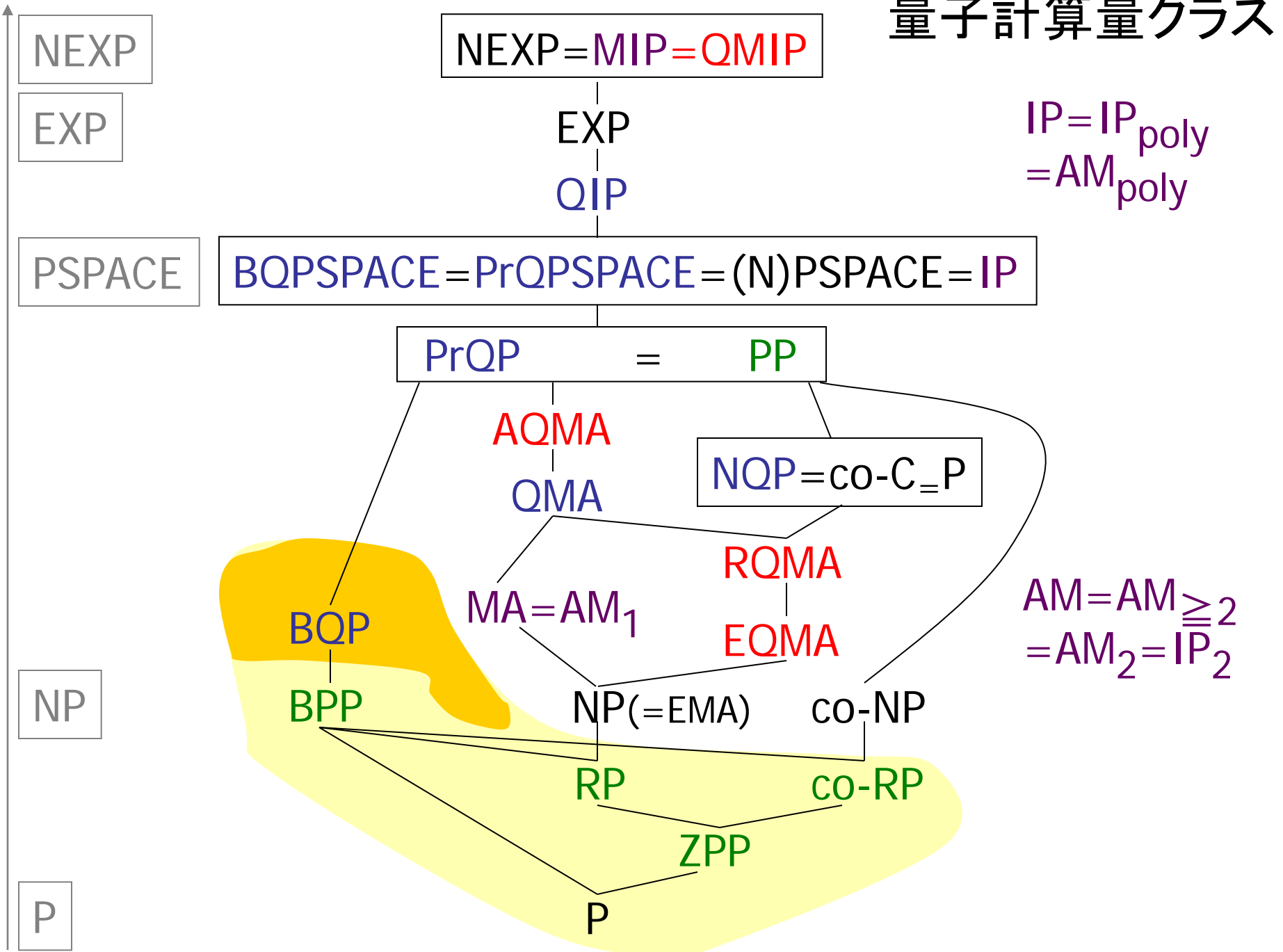


Multi-prover Interactive Proof

MIP=NEXPTIME



量子計算量クラス



$NEXP = MIP = QMIP$

EXP
 QIP

$IP = IP_{poly}$
 $= AM_{poly}$

NEXP

EXP

PSPACE

$BQPSPACE = PrQPSPACE = (N)PSPACE = IP$

$PrQP = PP$

AQMA

$NQP = co-C=P$

QMA

RQMA

$MA = AM_1$

EQMA

$AM = AM_{\geq 2}$
 $= AM_2 = IP_2$

NP

BQP

$NP(=EMA)$

co-NP

BPP

RP

co-RP

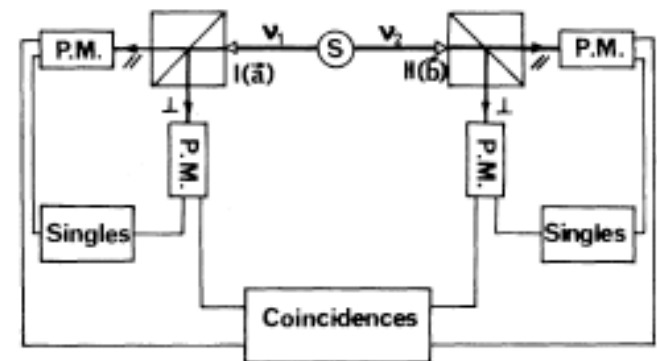
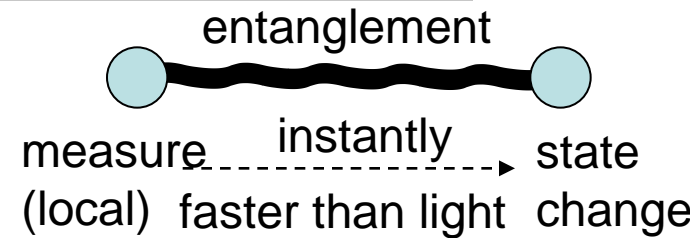
P

ZPP

P

EPR paradox and Bell inequalities

- Einstein, Podolsky, Rosen (1935)
 - quantum entanglement vs. relativity theory
- Bell inequality (1964)
 - Entanglement/Nonlocality \Rightarrow violation
- CHSH inequality (Clauser, Horne, Shimony, Holt 1969)
 - applicable to a bipartite system
- Aspect et al. (1982)
 - Experimental verification of violation of CHSH inequality
- Tsirelson (1980): max. violation value \Rightarrow Semidefinite Programming (Avis, Imai, Ito 2006)



A Two-Party One-Round Interactive Proof System [Cleve, Høyer, Toner, Watrous CCC 2004]

Provers

- 事前に回答戦略を協力して練ってよい
- 質問が始まったら通信できない

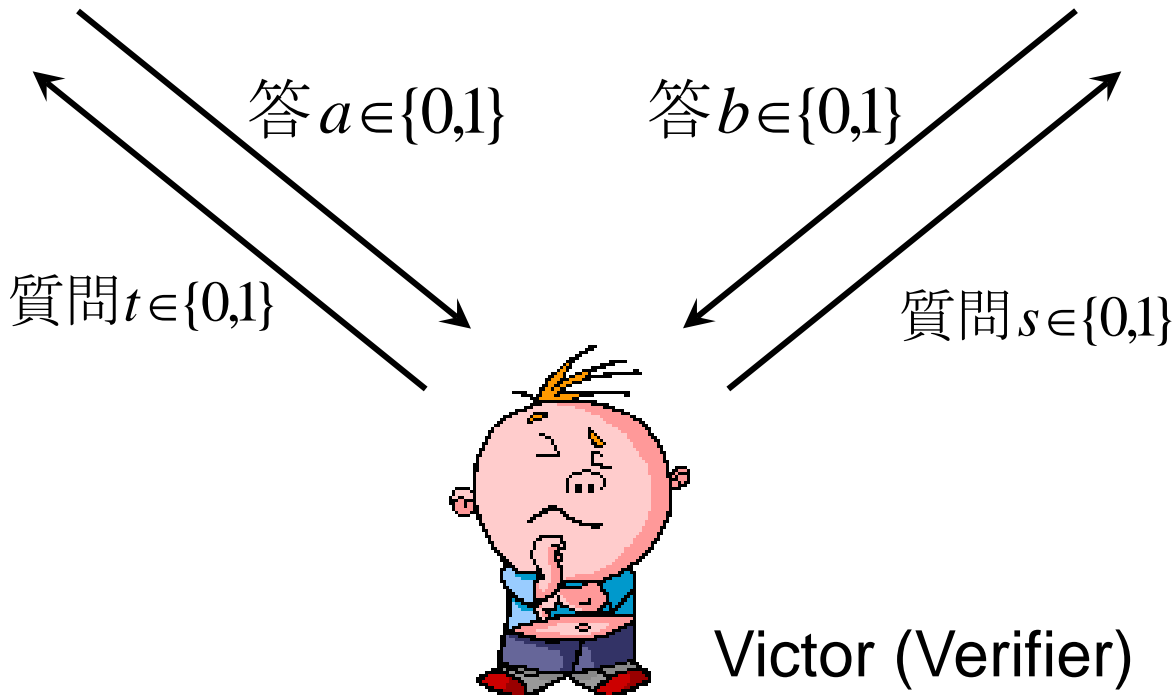
Alice



Bob



$$V(a,b;s,t) = \begin{cases} 1 & \text{Provers win} \\ 0 \leq < 1 & \text{Provers lose} \end{cases}$$



A Two-Party One-Round Interactive Proof System

[Cleve, Høyer, Toner, Watrous CCC 2004]

Provers

- 事前に回答戦略を協力して練ってよい
 - 関数 $a:S \rightarrow A$, $b:T \rightarrow B$ を確定
- 質問が始まったら通信できない

Alice



Bob



ゲームの値

$$V(a,b;s,t) = \begin{cases} 1 & \text{Provers win} \\ 0 \leq < 1 & \text{Provers lose} \end{cases}$$

答 $a \in A$

$$= \{0, 1, \dots, |A| - 1\}$$

答 $b \in B$

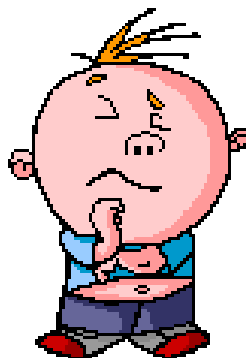
$$= \{0, 1, \dots, |B| - 1\}$$

質問 $s \in S$

$$= \{0, 1, \dots, |S| - 1\}$$

質問 $t \in T$

$$= \{0, 1, \dots, |T| - 1\}$$



Victor (Verifier)

CHSH Game

$$V(a,b;s,t) = \begin{cases} 1 & a \oplus b = s \wedge t \\ 0 & \text{otherwise} \end{cases}$$

Alice

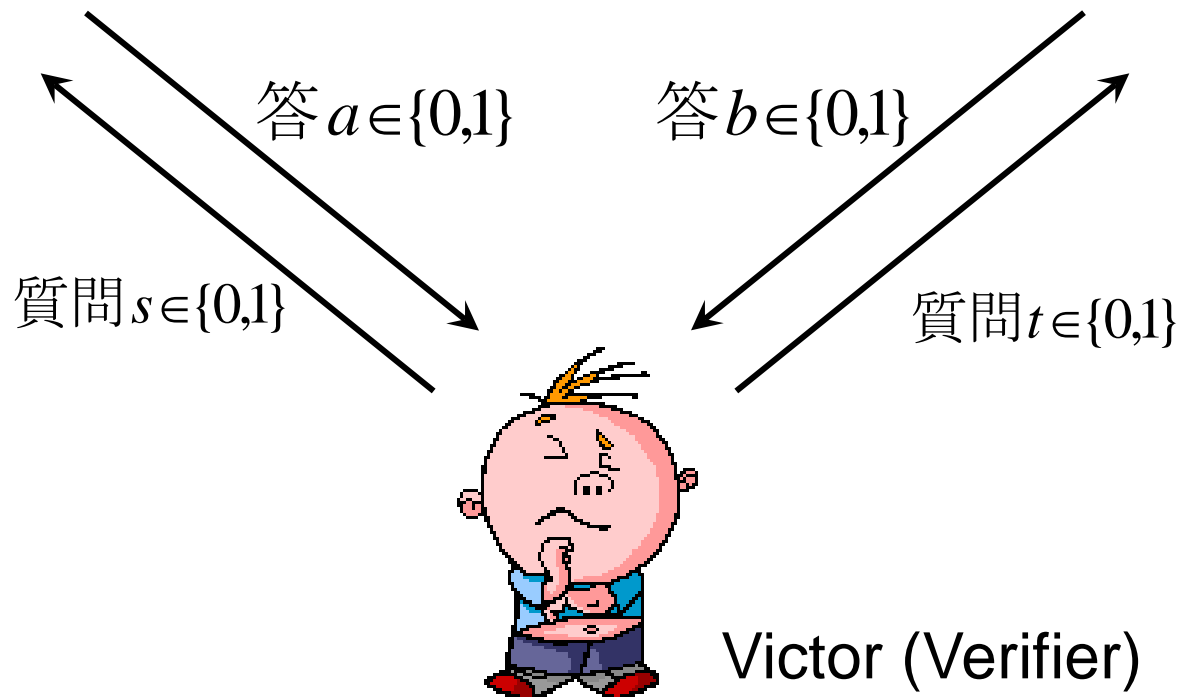


Bob



ゲームの値: 等確率質問に対して
証明者が勝つ確率の最大値

$$a(0)=0, a(1)=1; b(0)=1, b(1)=0 \\ \Rightarrow \text{ゲームの値 } 3/4$$



CHSH Gameの解析

- 古典の場合：ゲームの値 $3/4$
- 量子の場合：
 - 事前にAliceとBobがエンタングル状態 $(|00\rangle + |11\rangle)/\sqrt{2}$ を共有
 - それぞれ自分のところで部分測定できる

$$|\phi_0(\theta)\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$$

$$|\phi_1(\theta)\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle$$

として

$$X_0^a = |\phi_a(0)\rangle\langle\phi_a(0)|$$

$$X_1^a = |\phi_a(\pi/4)\rangle\langle\phi_a(\pi/4)|$$

$$Y_0^b = |\phi_b(\pi/8)\rangle\langle\phi_b(\pi/8)|$$

$$Y_1^b = |\phi_b(-\pi/8)\rangle\langle\phi_b(-\pi/8)|$$

で測定、
結果を回答

⇒ ゲームの値 $\cos^2(\pi/8) \approx 0.85 > 0.75$

まさしくCHSH不等式として知られるBell不等式の話そのもの

他にKochen-Specker定理、擬似テレパシー、量子グラフ彩色など種々の展開