量子情報物理学　12月4-6日

量子計算と基礎物理

藤井啓祐

京都大学　白眉センター/ 情報学研究科

目次

- はじめに（なぜ量子計算？）
- ユニバーサル量子計算
- 測定型量子計算
- 古典シミュレート困難性

自己紹介

‘02-’06 京都大学 工学部 物理工学科

’06-’11 京都大学大学院 工学研究科 原子核工学専攻 (指導教員： 山本克治教授)

’11-’13 大阪大学大学院 基礎工学研究科 物質創成専攻 井元研究 博士研究員

’13- 京都大学 白眉センター・大学院情報学研究科

The goal of quantum information science is to understand the general high-level principles that govern complex quantum systems such as quantum computers. These principles relate to the laws of quantum mechanics in the way that heuristics for skillful play at chess relate to the game’s basic rules.

計算 = ダイナミクス

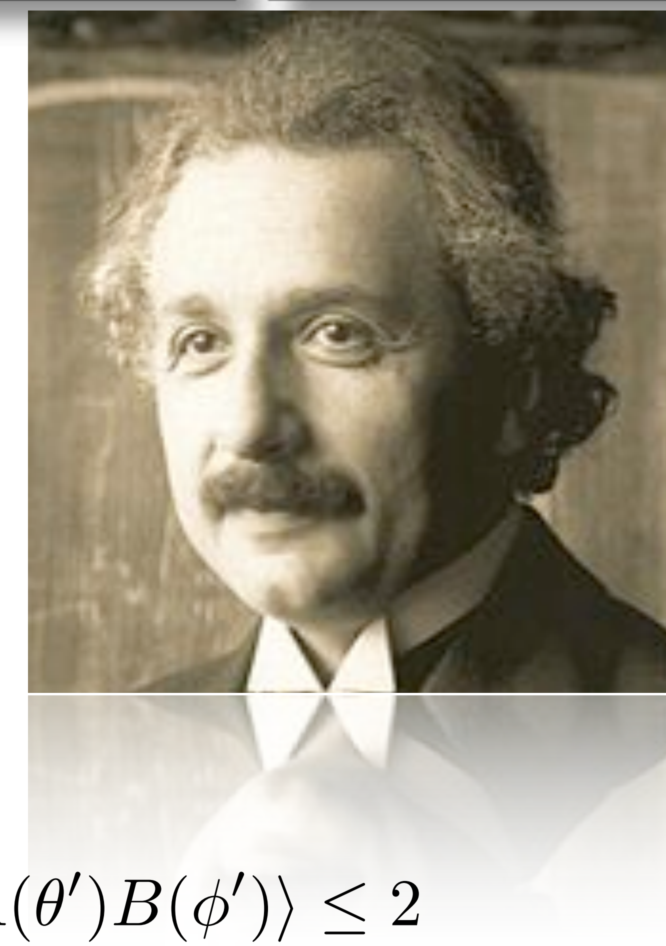
＋

最も基本的な物理 = 量子

= 量子計算

(物理を知りたければ、量子計算)

量子と古典の境界

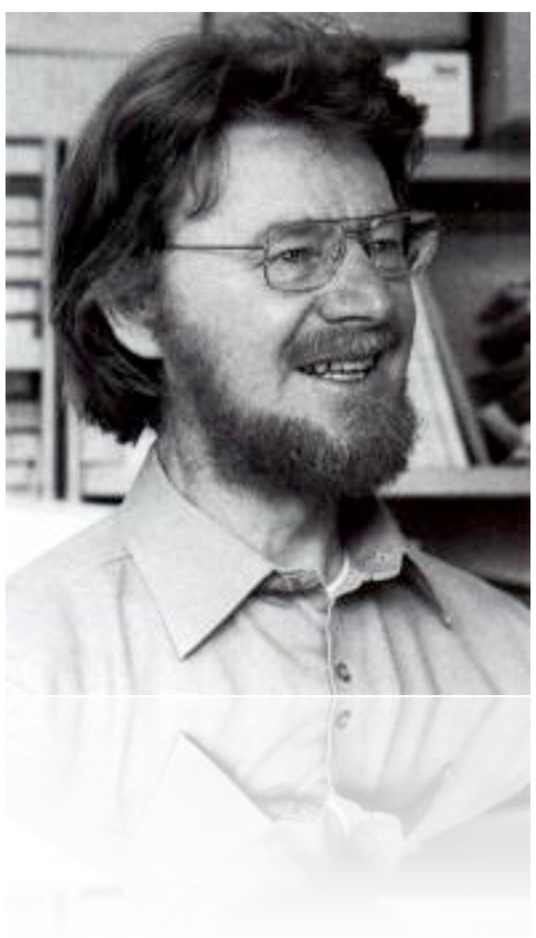


Einstein’s letter to M. Born (1926):
“I, at any rate, am convinced that He (God) does not throw dice”

$$\frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle) \quad \leftarrow \text{Z基底}$$

$$= \frac{1}{\sqrt{2}}(|+\rangle|+\rangle - |-\rangle|-\rangle) \quad \leftarrow \text{X基底}$$

EPR paradox, PR **47**, 777 (1935)



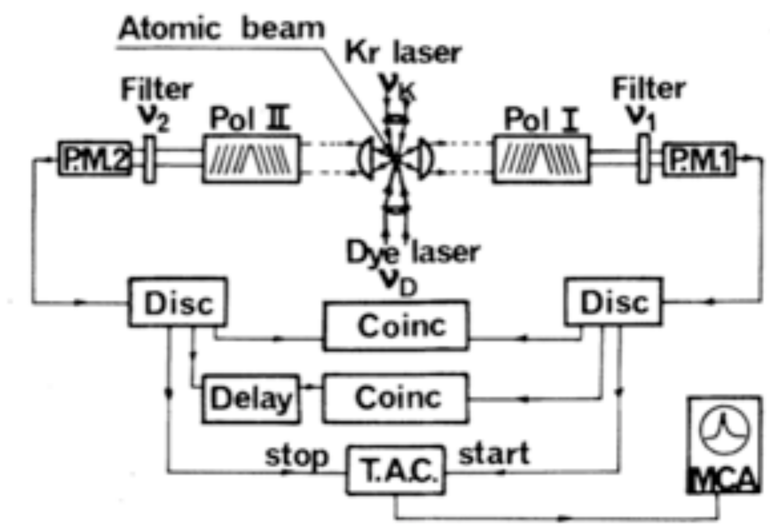
Bell不等式(CHSH不等式)

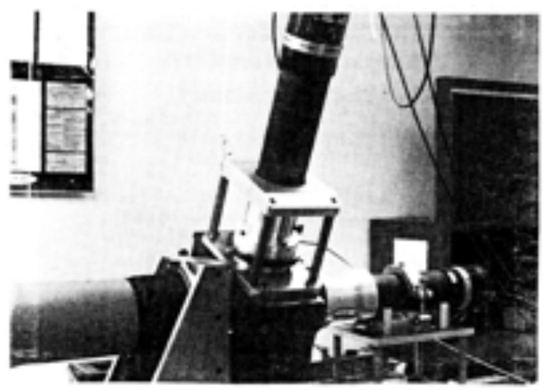
$$\langle A(\theta)B(\phi)\rangle + \langle A(\theta')B(\phi)\rangle - \langle A(\theta)B(\phi')\rangle + \langle A(\theta')B(\phi')\rangle \leq 2$$

→いかなる，局所実在論も否定.

量子と古典の境界

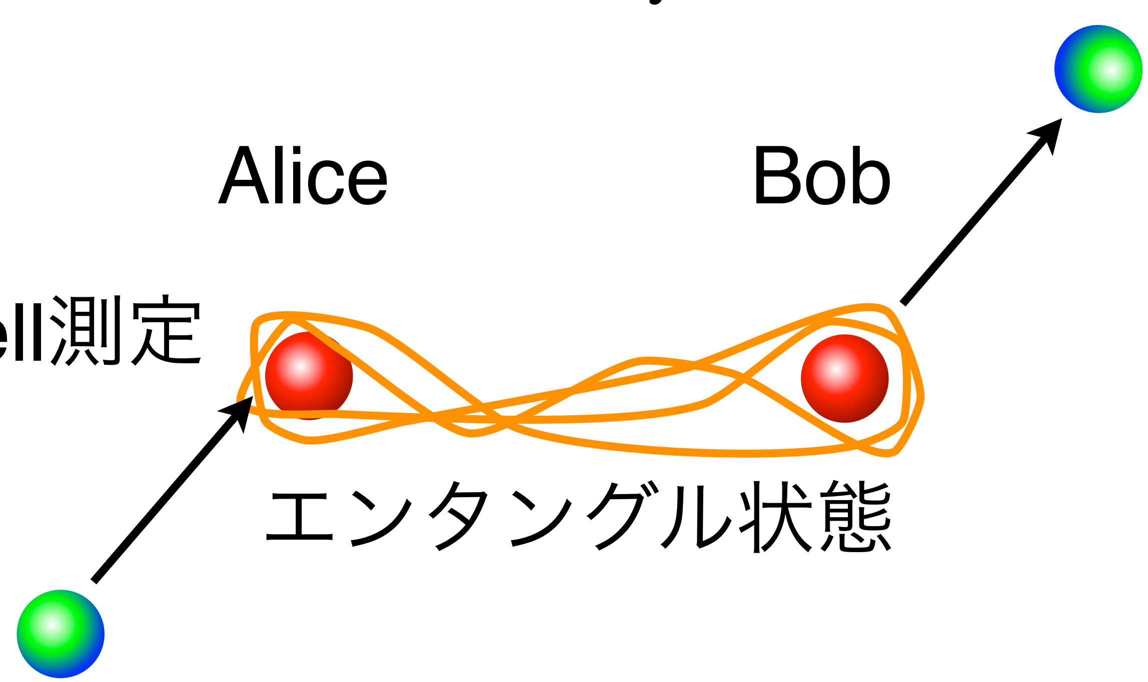
Aspect's の実験 (RPL 1981):

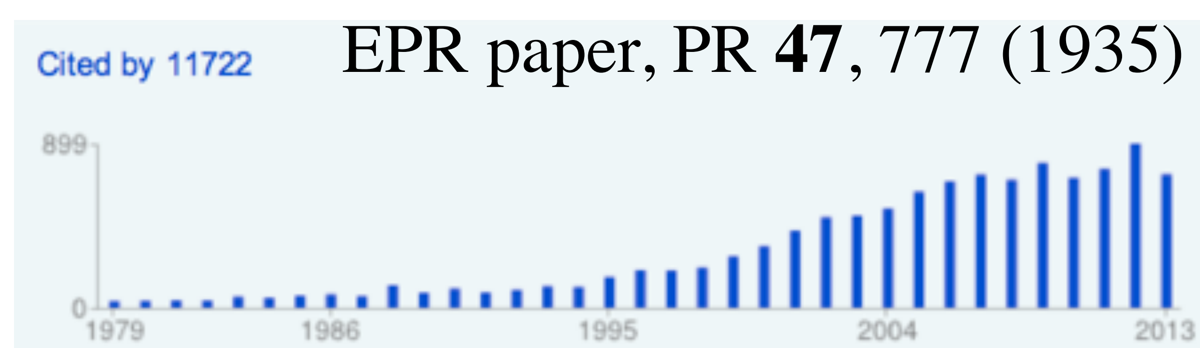





A. Aspect

量子テレポーテーション by Bennett *et al*., PRL **70** 1895 (1993)



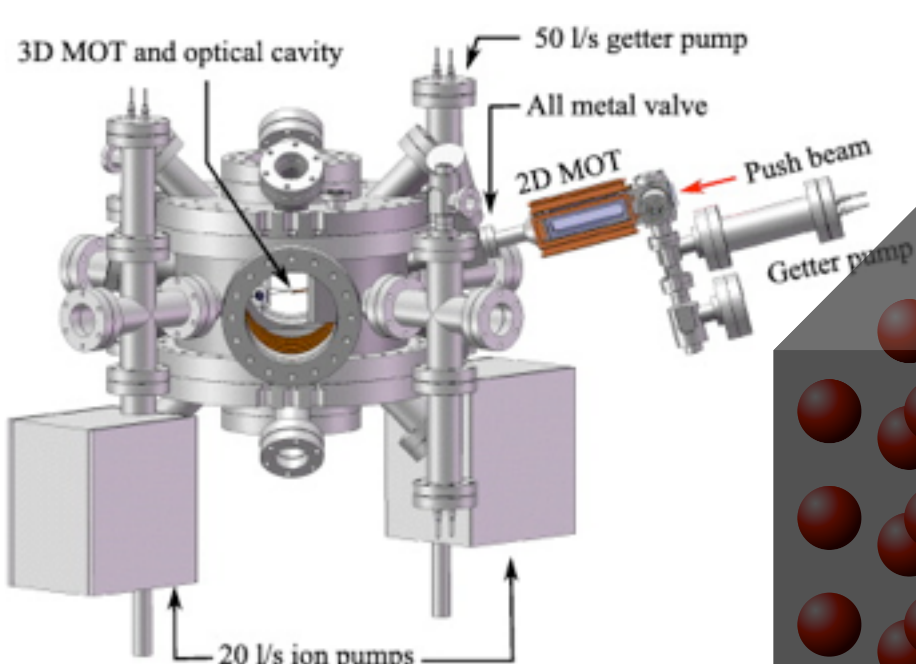


EPR paper, PR **47**, 777 (1935)

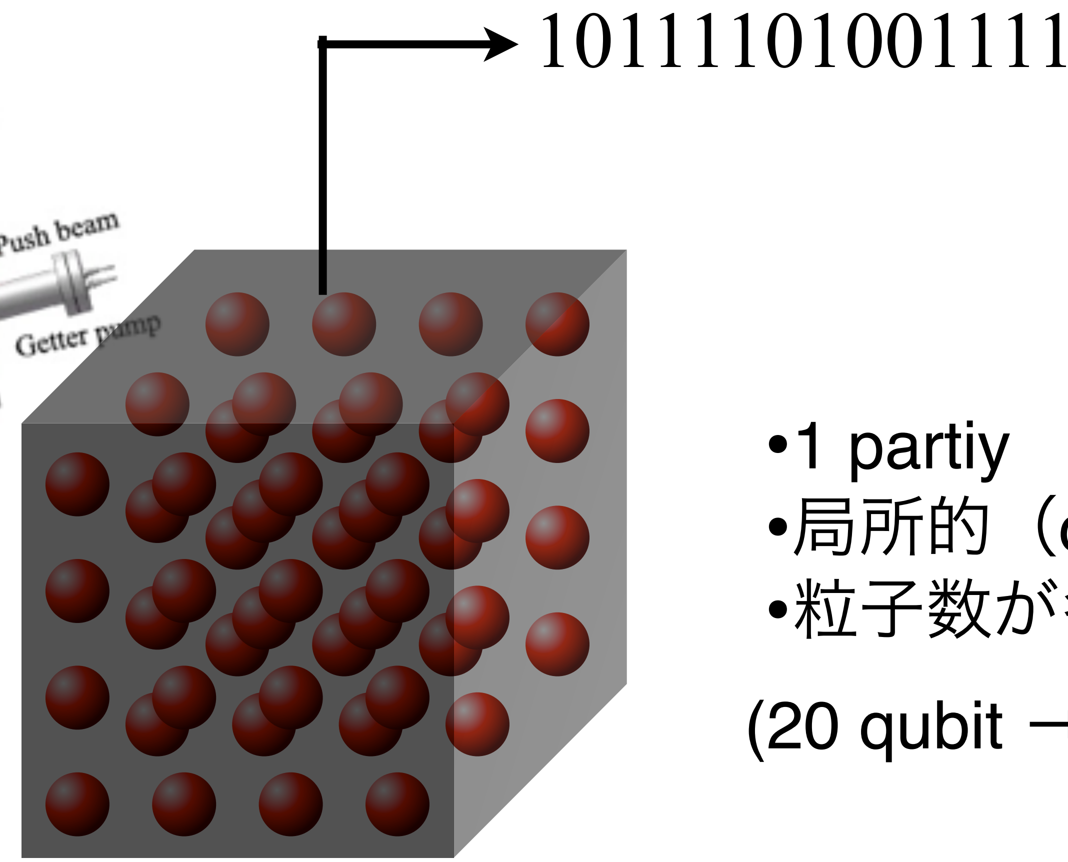
→量子情報通信、量子暗号へ

局所多体量子系の量子性

•2 partiy、
•非局所的



NJP 13 065021 (2011)



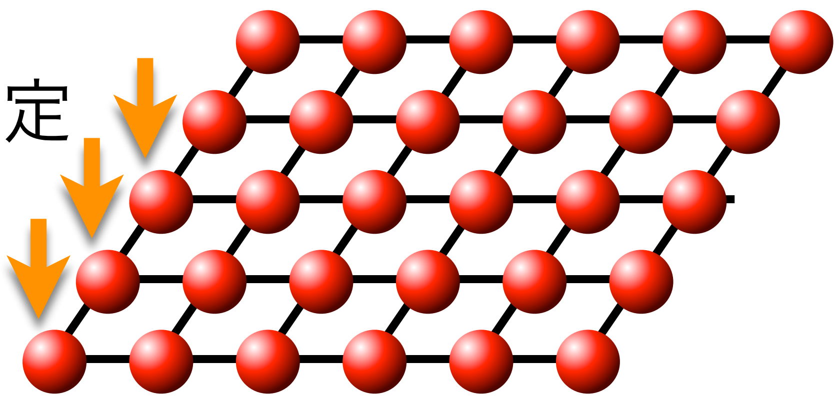
•1 partiy
•局所的（causal）
•粒子数が多い

(20 qubit → パラメータ $4^{20} \sim 10^{12}$)

Causal MBQC

measurement-based quantum computation

測定



多体エンタングル状態

(cluster状態, AKLT状態, VBS状態)

任意の量子計算が出来る.

(causalな測定に限定しても同じ)

→局所実在論で、説明できる?

→古典計算機？局所実在計算 = 量子計算

局所実在論で説明ができることと、そのシステムを古典計算機（既存の古典ダイナミクス）で効率よくシミュレートできることは異なる.

古典計算でシミュレートできない量子ダイナミクス
→計算複雑性に基づいた量子-古典の境界

DQC1

deterministic quantum computation with one clean qubit

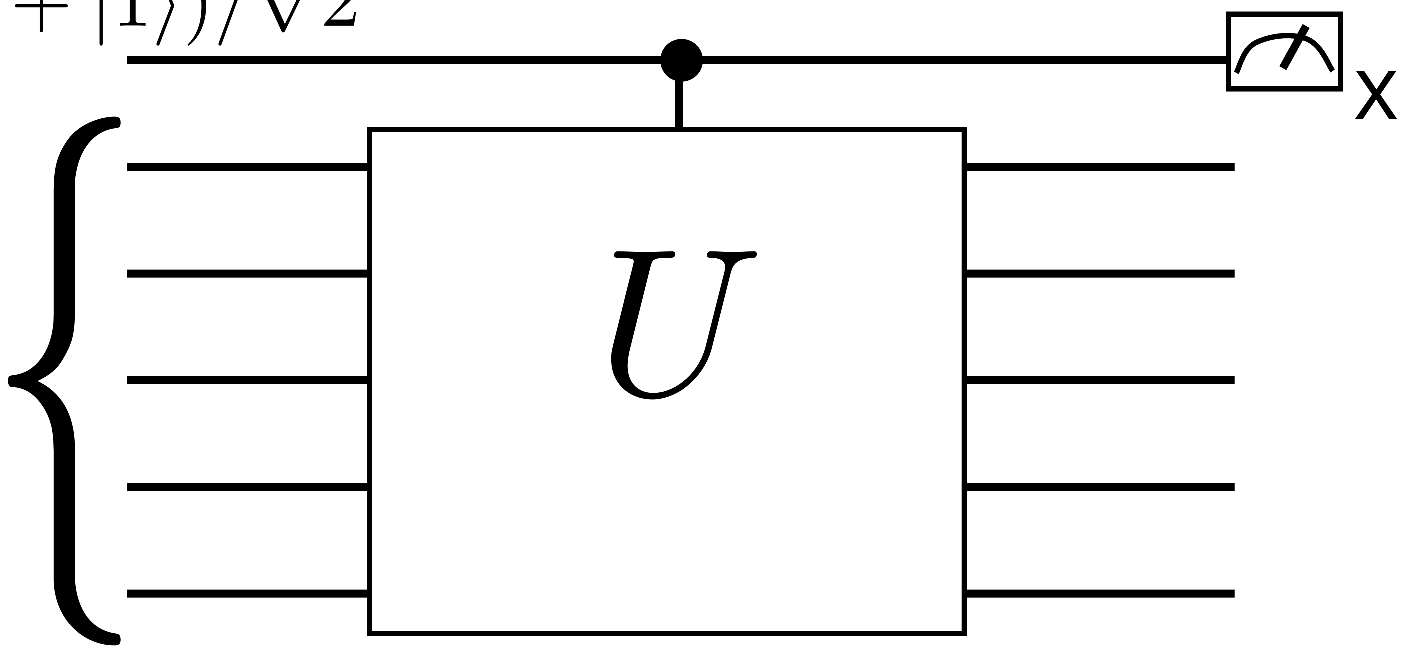
Deterministic quantum computation with one clean qubit: DQC1（NMR量子計算機）

Knill-Laflamme, PRL 81, 5672 (1998)

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

$I/2^n$

completely
mixed state



$$\longrightarrow \mathrm{Tr}[U]$$

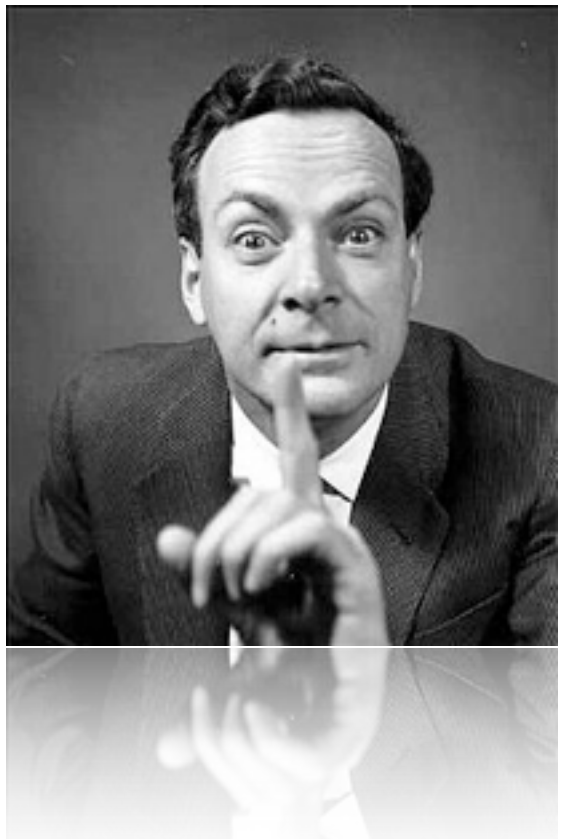
spectral density estimation,
Jones, HOMFLY polynomials

No entanglement,
but non-zero discord?

Datta *et al*., PRL **100**, 050502 (2008).

Poulin *et al*., PRL **92**, 177906 (2004). Shor-Jordan, QIC **8**, 681 (2008)

量子シミュレーション



量子系の自由度は粒子数に対して指数的に増える.
→古典コンピュータでは難しい.

"Let the computer itself be built of quantum mechanical elements which obey quantum mechanical laws."
R. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).

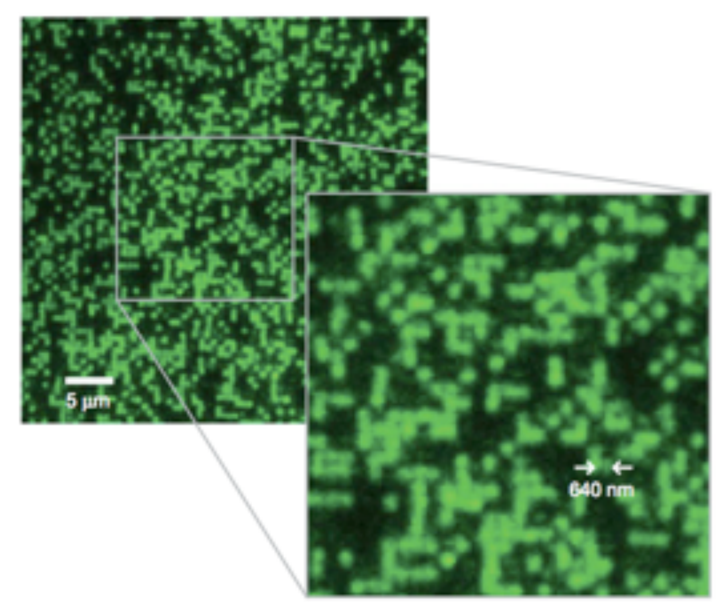
→Bose-Hubbard模型，non-Abelian gauge theory
D. Banerjee *et al*., PRL **110**, 125303 (2013)

今後より複雑に・正確に多体量子系の制御可能に．．．

古典コンピュータではシミュレーションが難しい領域に到達しているのか？

→そもそも古典シミュレーションができない対象物をどのように検証するのか？

→ダイナミクスにおける古典-量子の境界！



W. S. Bakr *et al*., Nature **462,** 74 (2009)

D-waveを例に
Boixo et al., arXiv:1304.4595

•100-500個の超伝導量子ビットを

•企業なので?デバイスの詳細は明

•古典では難しい問題に挑戦.

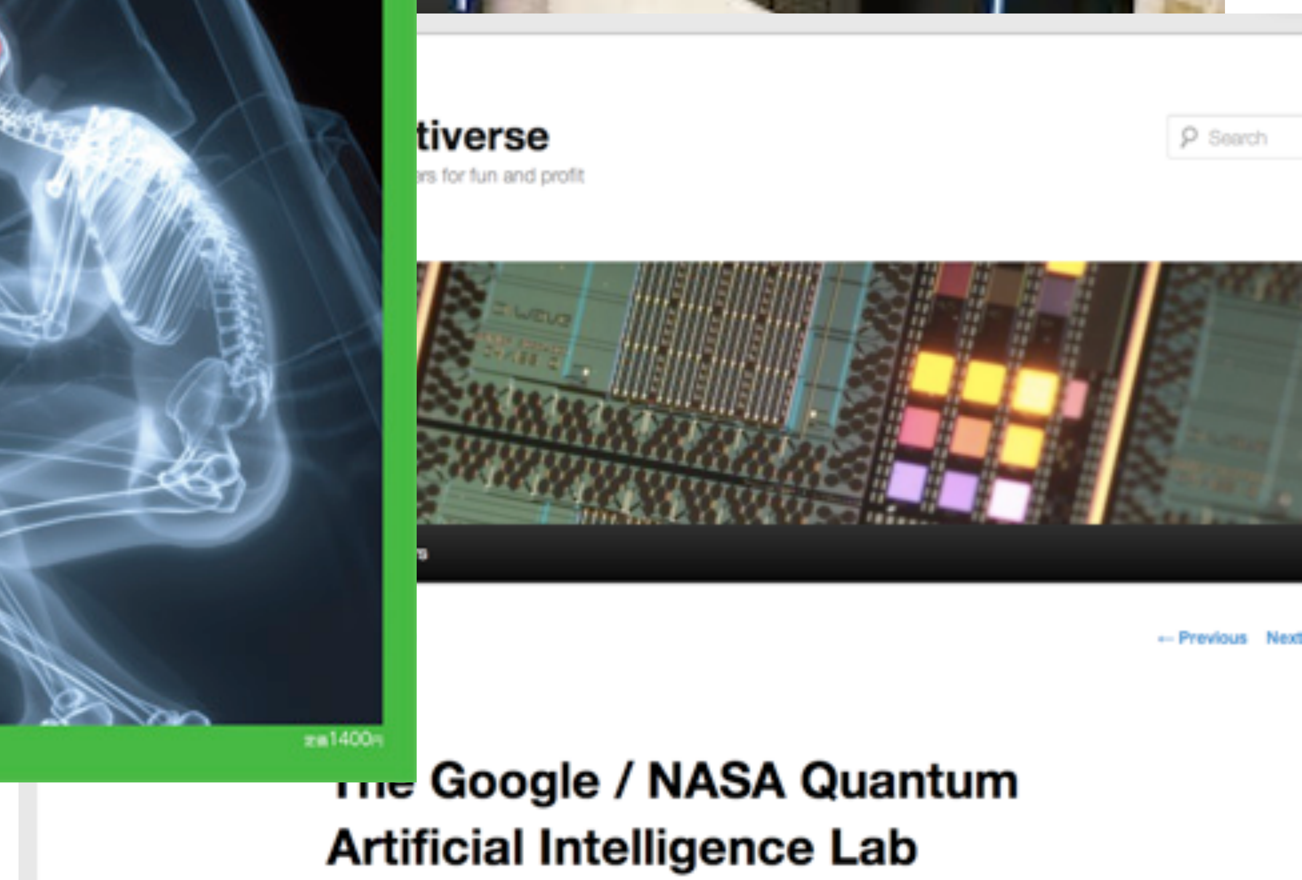
•多項式的ではないが，速く解ける
→非自明な量子ダイナミクス？

•いまのところ、古典の heuristic m
annealing)の方が圧倒的に速い.

•qubit数が増えれば、いつか勝てる

•真に量子だと判断する（古典だと

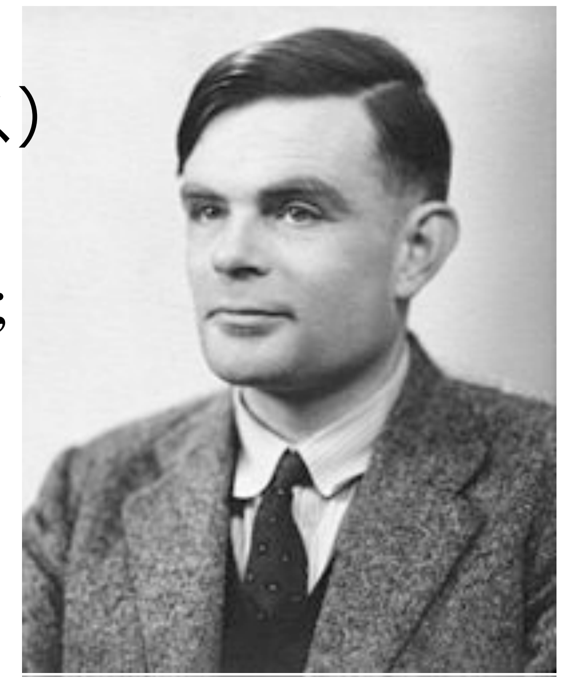
→ダイナミクスにおけ
境界を明確に.



Extended Church-Turing Thesis

すべての物理ダイナミクス（物理的な計算プロセス）
は、古典計算機で効率よくシミュレート出来る.

A. M. Turing, Proc. London Math. Soc. **42**, 230 (1937);
A. Church, Ann. Math. **33**, 346 (1932)



A. M. Turing

A. Church

P. W. Shor

素因数分解アルゴリズム
量子計算→多項式、古典計算→~~多項式~~
P. W. Shor, Proc. 35th FOCS, (1994).

（Groveアルゴリズム, Deutsch-Jozsaアルゴリズム）

→量子計算複雑性、extended quantum Church-Turing thesis

“Physical” computational model

物理的な計算

無限精度実数

計算モデルと

20 (1979).

Rolf Landauer @IBM

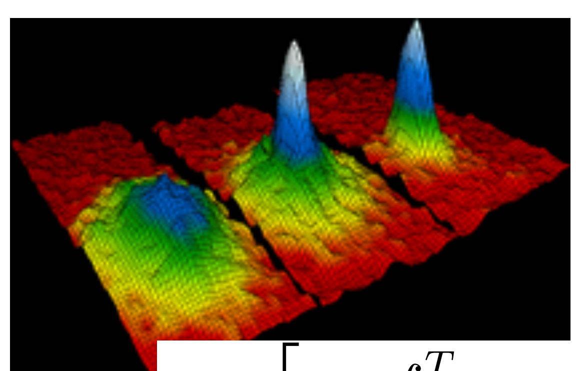
MIT Scientist Offers $100,000 to Anyone Who Can Prove Quantum Computing Is Impossible

“ The effort to build quantum computers, and to understand their capabilities and limitations, will lead us to a major conceptual advance in our understanding of QM.”

1000万円あげる

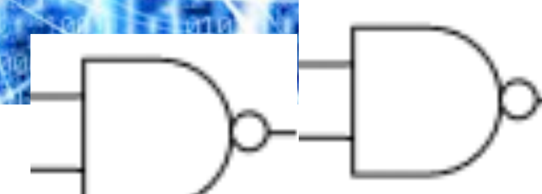
footnote: *“This proposal, like all*
eculative technology, does not in
rces of noise, unreliability and
probably will not work.” (S. Lloyd Nature 400 720 (1999))

量子状態は、実数値の複素振幅を含む.
計算モデルとして ill-defined?→量子誤り訂正と誤り耐性量子計算



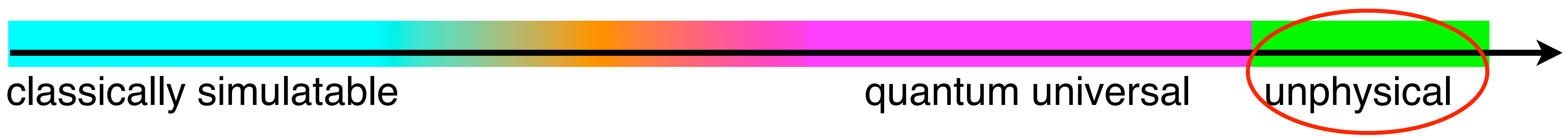
$$\exp\left[-i\int_0^T dtH(t)\right]$$

量子計算



Extended quantum Church-Turing Thesis

すべての物理ダイナミクスは、量子計算でシミュレート出来る.
→ 計算、ダイナミクスの自然限界を知りたければ,
量子計算を調べれば良い.



量子計算によってシミュレート可能：

- *k*-local Hamiltonian dynamics by S. Lloyed, Science **273**, 1073 (1996).
- *k*-local dissipative dynamics by M. Kliesch *et al*., PRL **107**, 120501 (2011).
- Adiabatic quantum computation by W. van Dam et al., FOCS ’01.

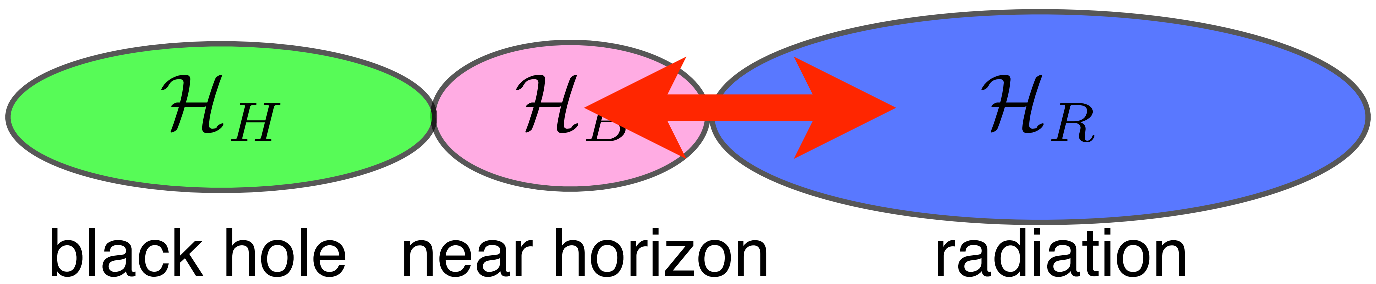
量子計算をシミュレート可能：

- Adiabatic quantum computation with 3-local Hamiltonian by D. Aharonov et al., FOCS ’04
- Additive approximation of Jones/ Tutte polynomials
by D. Aharonov *et al*., NJP **13**, 035019 (2011); QIP ’07
- Additive approximation of Ising partition functions
by G. De las Cuevas *et al*., NJP **13**, 093021 (2011); Matsuo-KF, in preparation

Quantum computation vs firewall

D. Harlow and P. Hayden, arXiv:1301.4504

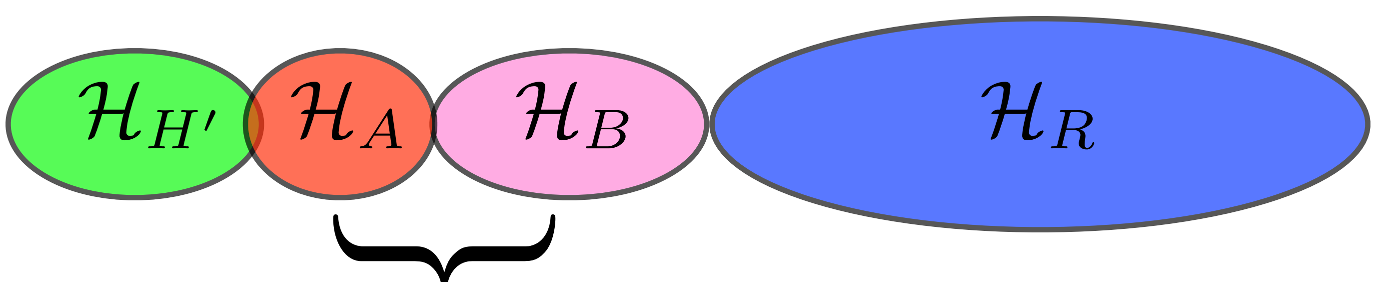
ブラックホールの外側の観測者：



Old black hole → Page's theorem:
maximally entangled with radiation fields

$$|\Psi\rangle = \left(\frac{1}{\sqrt{|H|}}\sum_h |h\rangle_H |h\rangle_{R_H}\right)\left(\frac{1}{\sqrt{|B|}}\sum_h |b\rangle_B |b\rangle_{R_B}\right)$$

ブラックホールの内側の観測者：



Rindler modes
Minkowski vacuum

$$|\text{vac}\rangle \sim \cancel{\sum_\omega e^{-\beta\omega/2}|\omega\rangle_A|\omega\rangle_B}$$

Strong subadditivity
→

$$I_{AB} \equiv S_A + S_B - S_{AB} = 0$$

Firewall annihilates any infalling observaer!

Almheiri-Marolf-Polchinski-Sully, arXiv:1207.3123

Quantum computation vs firewall

D. Harlow and P. Hayden, arXiv:1301.4504

Harlow-Hayden argument：

dynamics of black hole

$$U_{\mathrm{dyn}}|000\ldots 0\rangle_{\mathrm{int}} \sim \frac{1}{\sqrt{|B||H|}}\sum_{b,h}|b\rangle_B|h\rangle_H U_R|bh0\rangle_R$$

in order to extract entanglement, Alice have to undo U_R

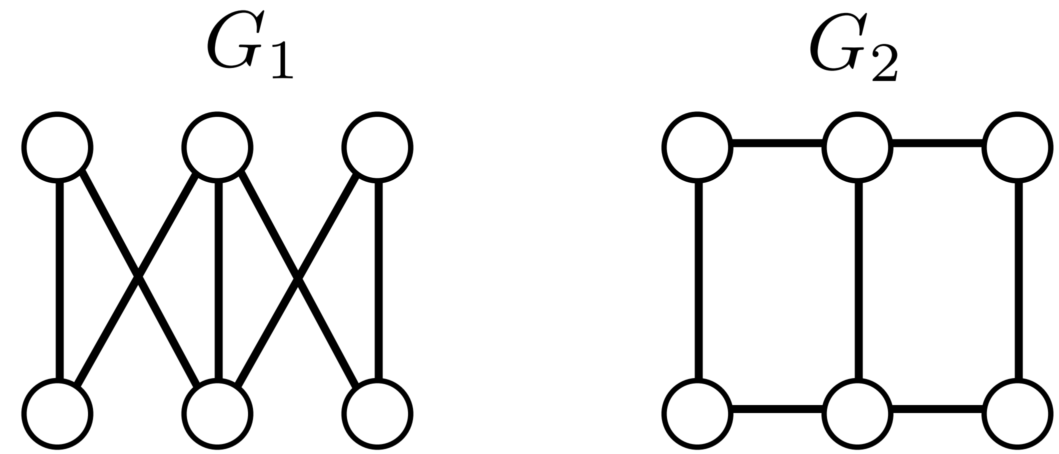
→ hard! QSZK-complete, which would be much harder than what quantum computer can do!

ゼロ知識証明

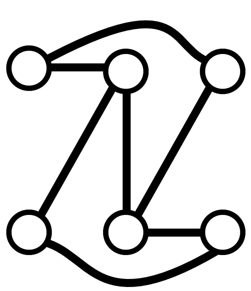
ゼロ知識証明, SZK (statistical zero knowledge proof)：
証拠を提示せずに命題が真であることを示す.

prover (証明者)

「グラフ同型問題を解く
アルゴリズムを持っているぞ．」



頂点の入れ替えで同じグラフになるか？
古典でも量子でもいまのところ効率よ
く解けない.



同型のグラフ G_3

verifier (検証者)
古典計算機
(多項式時間)

検証者はコインを投げて表なら, G_1 と G_3 の同型写像
裏なら, G_2 と G_3 の同型写像を proverに提出させる.

クラスSZKとは，このような証明ができる問題のクラス.

量子ゼロ知識証明

量子ゼロ知識証明, QSZK (quantum statistical zero knowledge proof)：
証拠を提示せずに命題が真であることを示す.

prover (証明者)

verifier (検証者)

量子計算機

クラスQSZKとは，量子計算機を用いて，
ゼロ知識証明できる問題のクラス.

量子計算機で解ける問題のクラス BQP
は，自明にQSZKに含まれる．なぜなら，
verifierは量子計算機を持っているので，
検証できる.

P≠NPほど試練を耐え抜いた訳ではない
が、QSZK≠BQPだと思われている.

ブラインド量子計算

実験装置（自然、宇宙）

prover (証明者)
量子サーバー
（量子計算機を持っている）
Qoogle, Q-wave, Quitter

verifier (検証者)

~~量子計算機~~
→ weak verifier, できるだけ古典デバイス
（single-qubit generator, measurement device）

実験者

“Is Quantum Mechanics Falsifiable? A computational perspective on the foundations of Quantum Mechanics”, Aharonov-Vazirani, arXiv:1206.3686

ブラインド量子計算：
（秘密委託量子計算）

Broadbent-Fitzsimons-Kashefi, FOCS ’09
Fitzsimons-Kashefi, arXiv:1203.5217
Morimae-KF, Nature Comm. **3** 1036 (2012)
Morimae-KF, PRA **87**, 050301 (2013)
Morimae-KF, PRL **111,** 020502 (2013)
Reichardt-Unger-Vazirani, Nature **496**, 456 (2013)

Quantum computation vs firewall

D. Harlow and P. Hayden, arXiv:1301.4504

Harlow-Hayden argument：

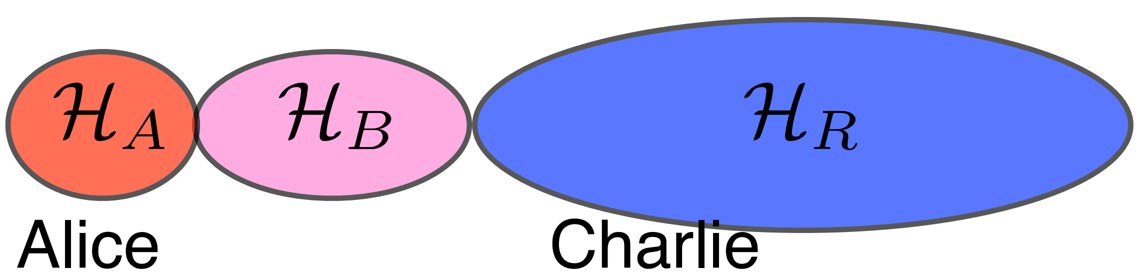
dynamics of black hole

$$U_{\rm dyn}|000\ldots 0\rangle_{\rm int} \sim \frac{1}{\sqrt{|B||H|}} \sum_{b,h} |b\rangle_B |h\rangle_H U_R |bh0\rangle_R$$

in order to extract entanglement, Alice have to undo U_R

→ hard, QSZK-complete, which would be much harder than what quantum computer can do!

“strong complementarity”:



$$\cancel{\rho_{BR}^{\rm Alice} = \rho_{BR}^{\rm Charlie}}$$

consistency conditions between different theories to ensure that observers agree on the experimental results visible to them.

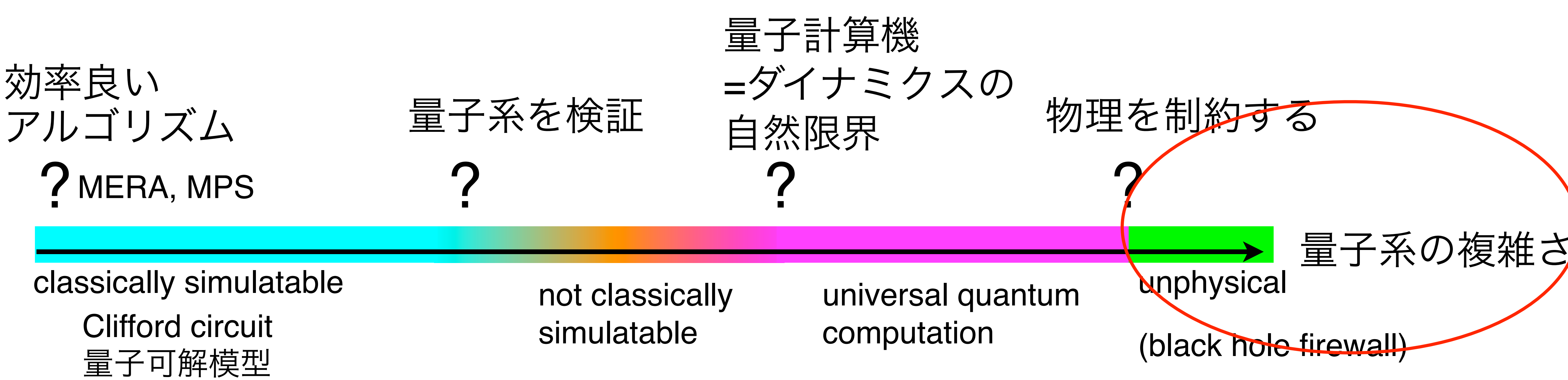
“standard complementarity”:

$$\text{“}A = R_B\text{”}$$

Embed Alice’s theory in Charlie’s.

目次

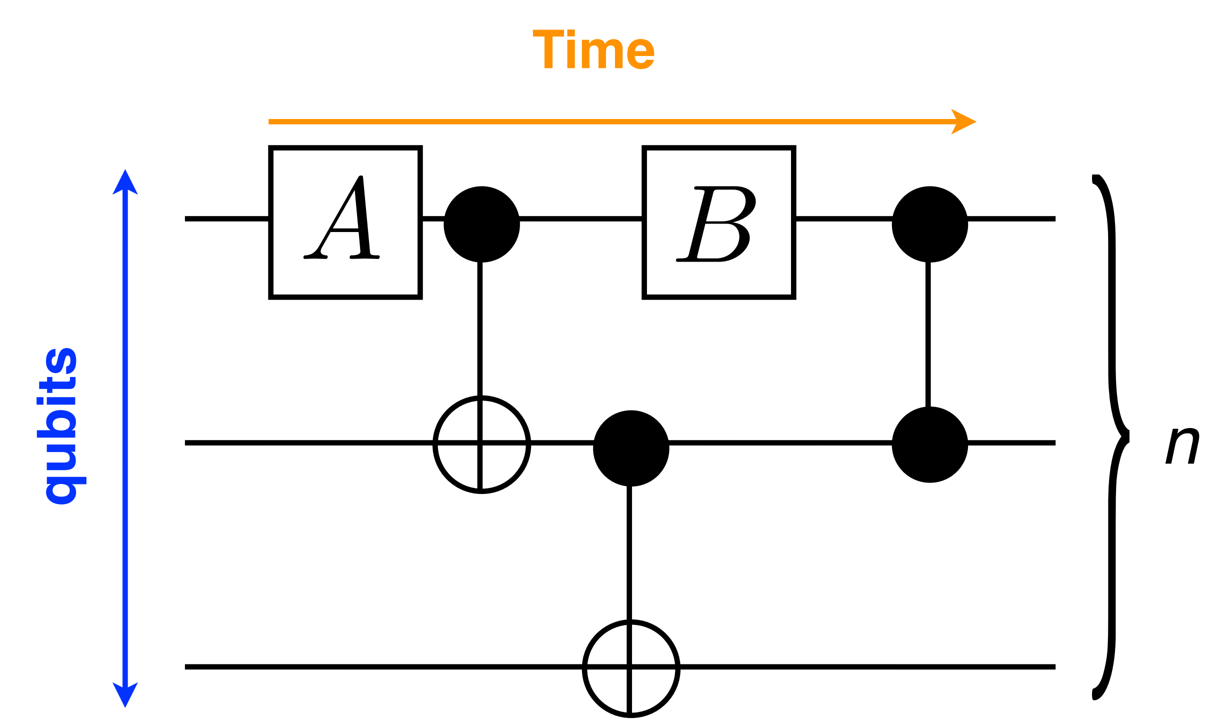
- はじめに（なぜ量子計算？）
- ユニバーサル量子計算
- 測定型量子計算
- 古典シミュレート困難性



量子計算（回路モデル）

量子回路モデル:

$$\langle 0|^{\otimes n} U |0\rangle^{\otimes n}$$



量子回路モデル

poly(n)個のユニタリ演算子（有限サイズ）の積

(任意の$2^n \times 2^n$ユニタリ演算子ではない！)

量子状態

- qubit = 量子２準位系: $\{|0\rangle, |1\rangle\}$ *Z*の固有状態

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

ただし $\alpha, \beta \in \mathbb{C}$, $\quad |\alpha|^2 + |\beta|^2 = 1$.

$(\,|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, \quad |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}\,)$

- *n*-qubit system:

$$|\psi_n\rangle = \sum_{s_1, s_2, \ldots, s_n} c_{s_1 s_2 \ldots s_n} \underbrace{|s_1 s_2 \ldots s_n\rangle}_{\downarrow\; |s_1\rangle \otimes |s_2\rangle \otimes \cdots \otimes |s_n\rangle}$$

→パラメータの数は指数的に増えてしまう.

量子状態を効率よく記述する必要がある.

→ Stabilizer 形式

D. Gottesman, Ph.D. thesis, California Institute of Technology (1997); arXiv:quant- ph/9705052.

Pauli群、Stabilizer群

- *n*-qubit Pauli積:

$$\{\pm 1, \pm i\} \times \{I, X, Y, Z\}^{\otimes n} \in \mathcal{P}_n$$

Pauli行列の積はPauli行列なので，Pauli 積は群をなす

→Pauli群

- Stabilizer群 $\mathcal{S} = \{S_i\}$: Pauli群の可換部分群

$$S_i \in \mathcal{P}, [S_i, S_j] = 0 \text{ for all } S_i, S_j \in \mathcal{S}$$

例) $\langle XX, ZZ \rangle = \{II, XX, ZZ, -YY\}$

生成元

$\longleftarrow$ even overlap **反可換×2=可換!**

→Stabilizer群は，その**生成元（独立な要素）**を指定すれば十分.

Stabilizer状態

◆ Stabilizer状態：すべてのstabilizer演算子$S_i \in \mathcal{S}$に対して

$$S_i|\Psi\rangle = |\Psi\rangle$$

を満たす状態$|\Psi\rangle$.

- stabilizer群は可換群なので，同時対角化できる.
- stabilizer生成元の固有状態であれば十分.

例1) $\mathcal{S}_1 = \langle XX, ZZ \rangle$

Bell state　$(|00\rangle + |11\rangle)/\sqrt{2}$

例2)　$\mathcal{S}_2 = \langle ZZ \rangle$

$\{|00\rangle, |11\rangle\}$ で張られる部分空間内の任意の状態.

→ 生成元の数がqubit数より少ないとき.

Clifford演算

U がPauli積をPauli積に写すユニタリ演算子，Clifford演算子であれば，stabilizer状態に.

$$\boxed{S'} = U S_i U^\dagger$$

新しい状態をstabilizeする演算子

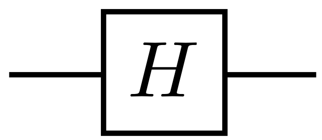
$$\begin{tikzcd}
\langle S_i \rangle \arrow[r, leftrightarrow] \arrow[d] & S_i|\Psi\rangle = |\Psi\rangle \arrow[d, "U"] \\
\langle S_i' \rangle \arrow[r, leftrightarrow] & S_i'|\Psi'\rangle = |\Psi'\rangle
\end{tikzcd}$$

Clifford演算子 U の作用は，stabilizer演算子への作用

$$S_i \to U S_i U^\dagger$$

によって記述される.

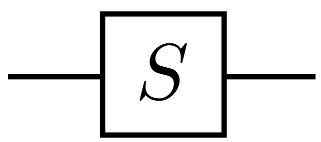
Clifford演算



Hadamard

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$HXH = Z$$

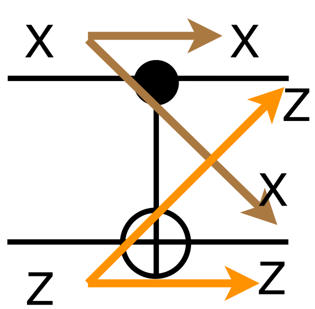


Phase

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$SXS^{\dagger} = Y$$

$\Lambda(X)$

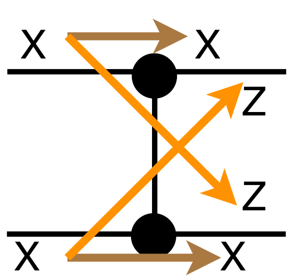


CNOT (controlled NOT)

$$\begin{array}{cc} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} & \begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \end{array} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

$$\Lambda(X)(X \otimes I)\Lambda(X) = X \otimes X$$
$$\Lambda(X)(I \otimes Z)\Lambda(X) = Z \otimes Z$$

$\Lambda(Z)$



CZ (controlled Z)

$$\begin{array}{cc} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} & \begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \end{array} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$$

$$e^{-i\pi/4(Z_1 Z_2 - Z_1 - Z_2 - I)}$$

$$\Lambda(Z)(X \otimes I)\Lambda(Z) = X \otimes Z$$
$$\Lambda(Z)(I \otimes X)\Lambda(Z) = Z \otimes X$$

Gottesman-Knillの定理

INPUT： Pauli演算子の固有状態.

OPERATION：Clifford回路

MEASUREMENT：Pauli基底

➡ Classically simulatable

n qubit stabilizer state → n個の演算子

$$\boxed{S'} = U S_i U^\dagger$$

新しい状態をstabilizeする演算子

$$\begin{tikzcd} \langle S_i \rangle \arrow[r, leftrightarrow] \arrow[d] & S_i|\Psi\rangle = |\Psi\rangle \arrow[d, "U"] \\ \langle S_i' \rangle \arrow[r, leftrightarrow] & S_i'|\Psi'\rangle = |\Psi'\rangle \end{tikzcd}$$

観測量（Pauli演算子）とstabilizer演算子との交換関係から,

確率分布を効率よく計算できる.

Kitaev-Solovayの定理

◆ Non-Clifford演算が一つでもあれば OK

•例えば π/8 演算

$$e^{i\pi Z/8}$$

$$e^{i\pi Z/8} X e^{-i\pi Z/8} = (X+Y)/\sqrt{2}$$

◆ Kitaev-Solovayの定理

ある基本演算（gate set）が$SU(2)$で稠密であれば,
すぐに（=polylog(1/ε)）$SU(2)$を覆い尽くす.

$$^{\forall}U \in SU(2) \text{ and } ^{\forall}\epsilon, \quad ^{\exists}S = g_1 \ldots g_n, \quad \text{s.t. } d(S,U) < \epsilon$$

•1-qubitの任意の回転は Hadamard演算とπ/8 演算で効率よく構成できる.
•1-qubitの任意の回転とCNOTがあれば任意のユニタリ演算子を構成できる.

→ universal set: $\{\Lambda(X), H, e^{-i\pi/8}\}$

Dawson-Nielsen, QIC **6**, 81 (2006)

Magic state

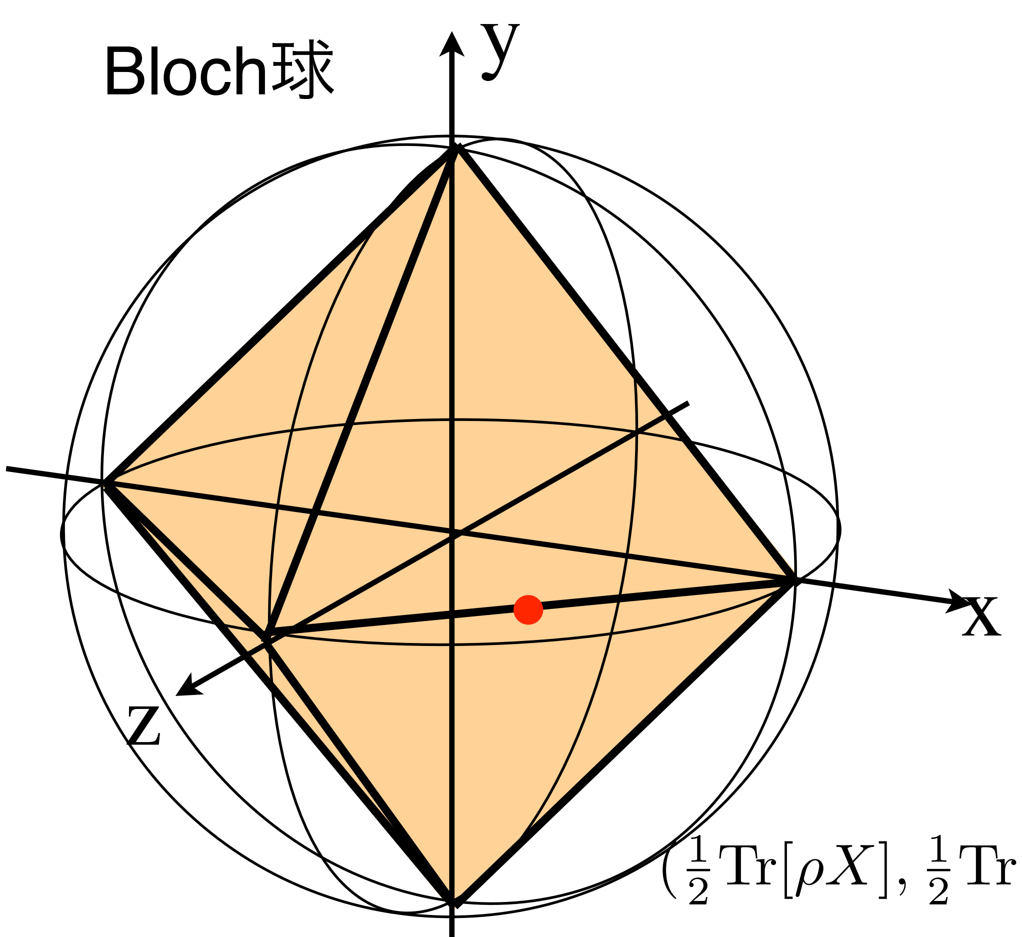
INPUT：~~Pauli演算子の固有状態~~→一般の状態

OPERATION：Clifford回路

MEASUREMENT：Pauli基底

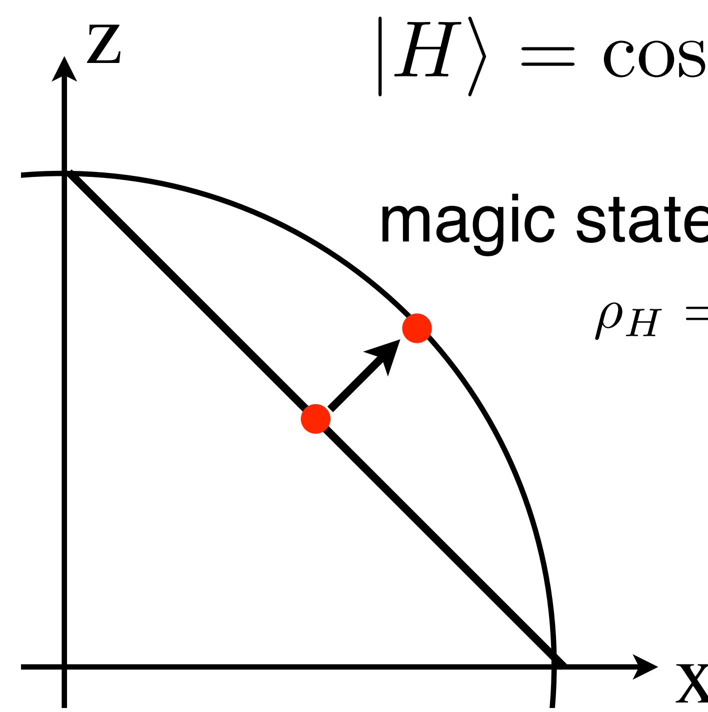
→Pauli演算子の固有状態の convex mixture は classically simulatable

Bloch球



$(\frac{1}{2}\mathrm{Tr}[\rho X], \frac{1}{2}\mathrm{Tr}[\rho Y], \frac{1}{2}\mathrm{Tr}[\rho Z])$

$$|H\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$$



$$\rho_H = (1-p)|H\rangle\langle H| + p|H^\perp\rangle\langle H^\perp|$$

$$p = \frac{1}{2}(1 - 1/\sqrt{2})$$

Clifford回路のみでpure magic stateをdistillできる.

Bravyi-Kitaev, PRA 71, 022316 (2005);
Reichardt, QIP 4, 251 (2005)

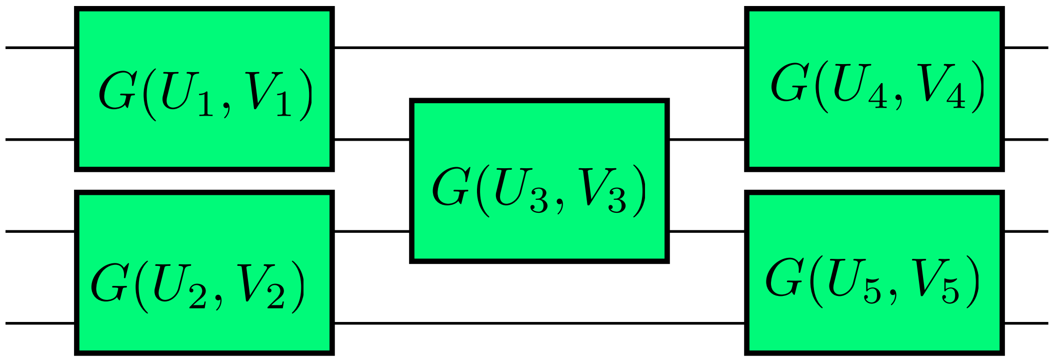
スタビライザー形式の応用

- 記述が非常に簡単
- +α で量子計算全体を記述できる.
- よく似た構造が他にもある.
  →Match gate (free-fermion),
  →Boson (gaussian operation)
- 量子誤り訂正符号を記述できる.
- トポロジカル秩序を持つ系のトイモデル.
- 測定型量子計算のリソースを記述できる.

Free-fermionic computation = Match gate

Match gate: two-qubit gate acting on nearest neighbors in one-dimension.

$$G(U,V) = \begin{pmatrix} U_{11} & 0 & 0 & U_{12} \\ 0 & V_{11} & V_{12} & 0 \\ 0 & V_{21} & V_{22} & 0 \\ U_{21} & 0 & 0 & U_{22} \end{pmatrix}$$



$$U, V \in SU(2)$$

$$G(U,V) = e^{iH}$$

$$H = H_1 + H_2 + H_3$$

$$\begin{aligned} H_1 &= \alpha_1 Z_i \otimes I_{i+1} + \beta_1 I_i \otimes Z_{i+1} \\ H_2 &= \alpha_2 X_i \otimes X_{i+1} + \beta_2 Y_i \otimes Y_{i+1} \\ H_3 &= \alpha_3 X_i \otimes Y_{i+1} + \beta_3 Y_i \otimes X_{i+1} \end{aligned}$$

Valiant (2002); Terhal-DiVincenzo (2002);Knill (2001); Jozsa-Miyake (2008);Jozsa *et al*., (2010)

Free-fermionic computation = Match gate

Fermion operators:

$$\{a_i, a_j\} = 0, \quad \{a_i^\dagger, a_j^\dagger\} = 0, \quad \{a_i, a_j^\dagger\} = \delta_{ij} I$$

Hermitian operators (Majorana fermions):

$$c_{2k-1} = a_k + a_k^\dagger, \quad c_{2k} = (a_k - a_k^\dagger)/i$$

$$\rightarrow \{c_\nu, c_\mu\} = 2\delta_{\nu\mu} I$$

Jordan-Wigner representation:

$$c_{2k-1} = Z_1 \ldots Z_{k-1} X_k I_{k+1} \ldots I_n$$
$$c_{2k} = Z_1 \ldots Z_{k-1} Y_k I_{k+1} \ldots I_n$$

$$\begin{array}{rcl} Z_k &=& -ic_{2k-1}c_{2k} \\ X_k X_{k+1} &=& -ic_{2k}c_{2k+1} \\ X_k Y_{k+1} &=& -ic_{2k}c_{2k+2} \end{array} \qquad \begin{array}{rcl} Z_{k+1} &=& -ic_{2k+1}c_{2k+2} \\ Y_k Y_{k+1} &=& ic_{2k-1}c_{2k+2} \\ Y_k X_{k+1} &=& ic_{2k-1}c_{2k+1} \end{array}$$

$G(U, V) = e^{iH}$ →quadratic form of fermion operators $H = \sum_{\mu\nu} h_{\mu\nu} c_\mu c_\nu$

Free-fermionic computation = Match gate

Time evolution in Heisenberg picture:

$$U^\dagger c_\nu U = \sum_{\mu=1}^{2n} R_{\nu\mu} c_\mu \qquad R_{\nu\mu} \in SO(2n)$$

Classical simulation of fermionic QC:

- Input as a product state: $|\Psi_{\rm in}\rangle \equiv |s_1\rangle|s_2\rangle\ldots|s_n\rangle$
- Observable, polynomial of degree at most *d*:

$$O_d = \sum_{\mu_1,\ldots,\mu_d} A_{\mu_1,\ldots,\mu_d} c_{\mu_1}\ldots c_{\mu_d}$$

- Match gates: $U = \prod_i^{\rm poly(n)} G(U_i, V_i)$

$$\begin{aligned}
\langle O_d\rangle_{\rm out} &= \sum_{\mu_1,\ldots,\mu_d} A_{\mu_1,\ldots,\mu_d}\langle c_{\mu_1}\ldots c_{\mu_d}\rangle_{\rm out} \\
&= \sum_{\mu_1,\ldots,\mu_d} A_{\mu_1,\ldots,\mu_d}\langle\Psi_{\rm in}|U^\dagger c_{\mu_1}\ldots c_{\mu_d} U|\Psi_{\rm in}\rangle \\
&= \sum_{\mu_1,\ldots,\mu_d} A_{\mu_1,\ldots,\mu_d}\sum_{\nu_1} R_{\mu_1\nu_1}\cdots\sum_{\nu_d} R_{\mu_d\nu_d}\langle\Psi_{\rm in}|c_{\nu}\ldots c_{\nu_d}|\Psi_{\rm in}\rangle \longrightarrow O(\mathrm{poly}(n))
\end{aligned}$$

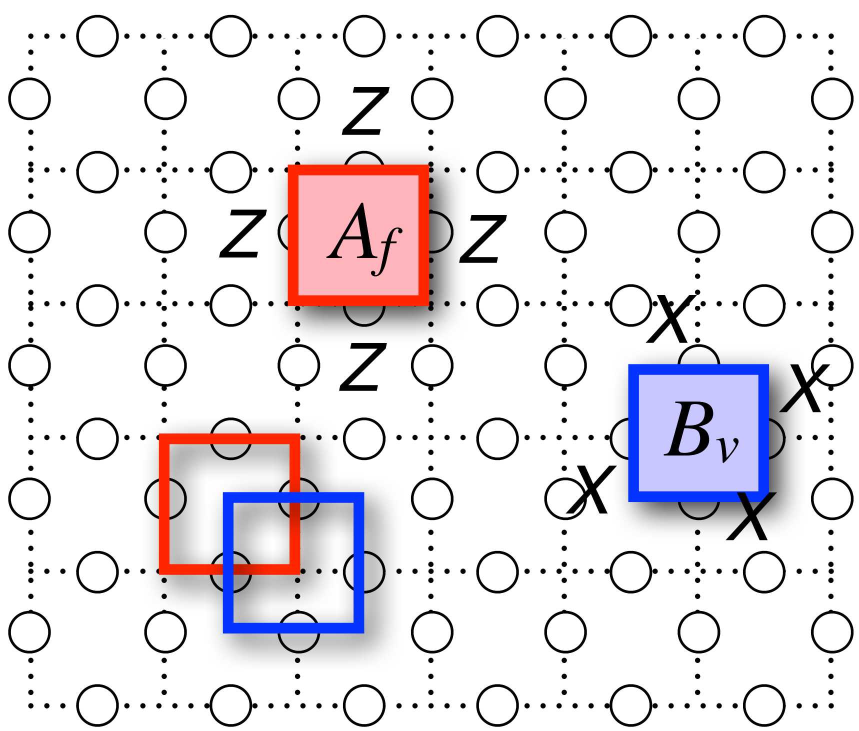
スタビライザー形式の応用

- 記述が非常に簡単
- +α で量子計算全体を記述できる.
- よく似た構造が他にもある.

  →Match gate (free-fermion),
  →Boson (gaussian operation)
- 量子誤り訂正符号を記述できる.
- トポロジカル秩序を持つ系のトイモデル.
- 測定型量子計算のリソースを記述できる.

Kitaev's toric code

A. Kitaev, Ann. Phys. 303, 2 (2003)



Stabilizer operators of *Z*-type, face operator:

$$A_f = \prod_{i \in \text{ face } f} Z_i$$

Stabilizer operators of *X*-type, vertex operator:

$$B_v = \prod_{i \in \text{ vertex } v} X_i$$

The code state is defined as an eigenstate with eigenvalue +1 for all stabilizers.

quantum error correction codes

stabilizer operators: A_f, B_v
(parity check operators)

code subspace

errors

correctability against errors

(*k*-error correction code)

topologically ordered system

stabilizers Hamiltonian: $H = -J \sum_f A_f - J \sum_v B_v$

degenerated ground states

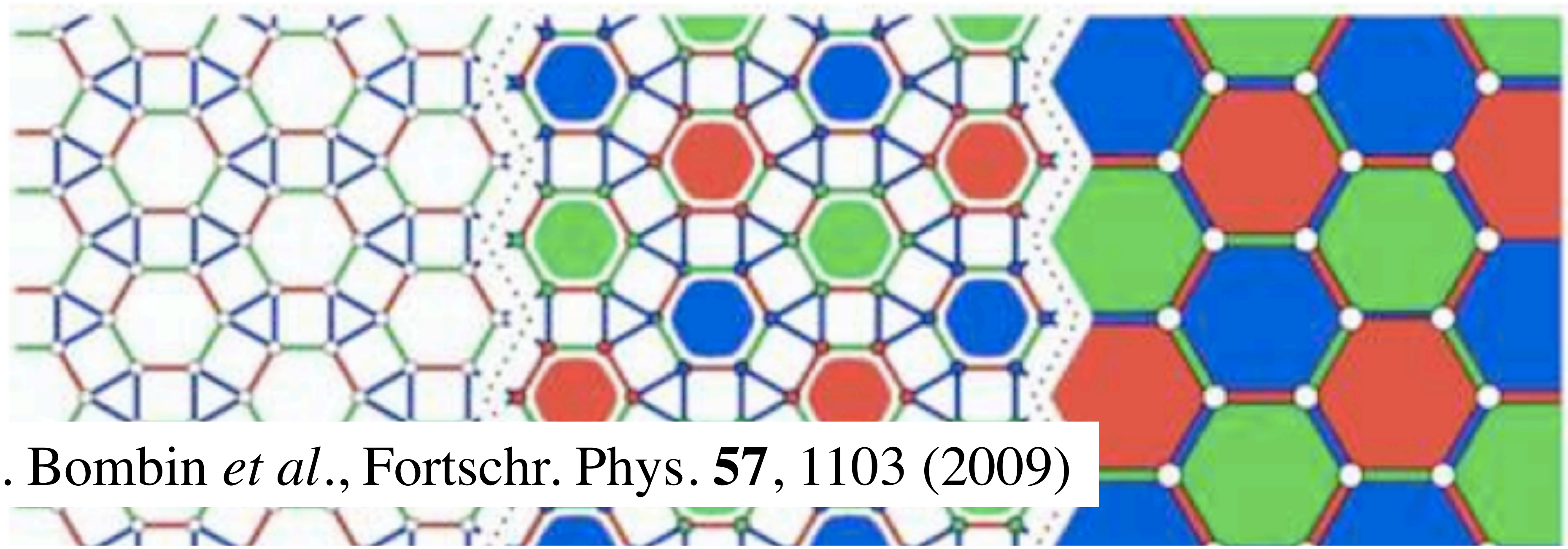
anyonic excitations

robustness against local perturbation

(robust up to (2k+1)-th order perturbation)

Kitaev's toric code

A. Kitaev, Ann. Phys. 303, 2 (2003)



H. Bombin *et al*., Fortschr. Phys. **57**, 1103 (2009)

Clasification:

B. Yoshida, Annals of Physics **326**, 15 (2011).

H. Bombin *et al*., New J. Phys. **14**, 073048 (2012).

Thermal stability of topological ordered system:

2D→ S. Bravyi and B. Terhal, New J Phys. **11**, 043029 (2009);

3D→ B. Yoshida, Ann. Phys. **326**, 2566 (2011).

Information capacity of discrete systems (coding rate):

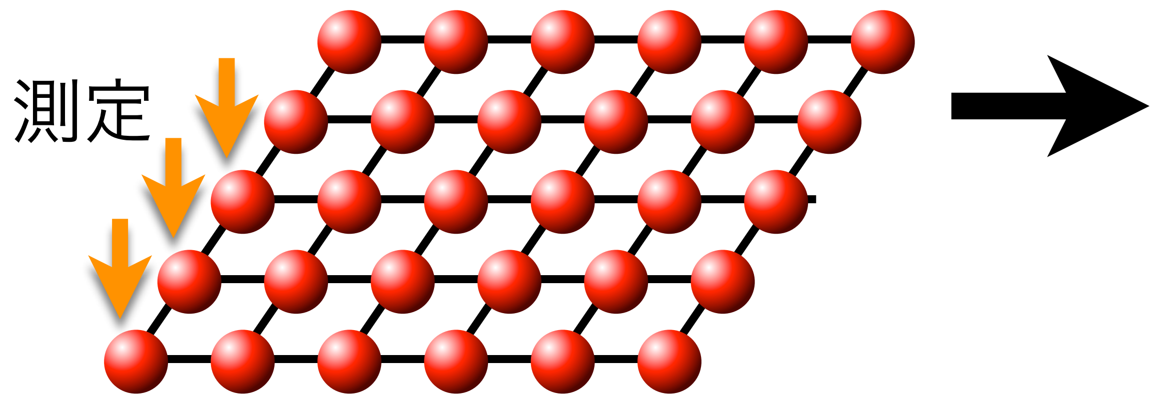
classical→ B. Yoshida, Annals of Physics 338, 134 (2013)

quantum→B. Yoshida, Phys. Rev. B 88, 125122 (2013)

スタビライザー形式の応用

- 記述が非常に簡単
- +α で量子計算全体を記述できる.
- よく似た構造が他にもある.
  →Match gate (free-fermion),
  →Boson (gaussian operation)
- 量子誤り訂正符号を記述できる.
- トポロジカル秩序を持つ系のトイモデル.
- $\boxed{\text{測定型量子計算のリソースを記述できる.}}$

MBQC
(measurement-based quantum computation)



任意の量子計算が出来る.

$$\langle \alpha_{nm} | \cdots \langle \alpha_i | \Psi \rangle$$

多体エンタングル状態（計算のリソース）
(cluster状態, AKLT状態, VBS状態)

- 量子力学特有の計算モデルである.
- ユニタリ行列よりも状態の変形のほうが分かりやすい.
- 多体量子系との対応を与える.
- リソース状態のエンタングルメントの評価から、計算能力がわかる.

Raussendorf-Briegel PRL **86** 910 (2001);
Raussendorf-Browne-Briegel PRA **68** 022312 (2003).

グラフ状態

◆ グラフ状態：グラフ G(V,E)を用いて定義される stabilizer 状態

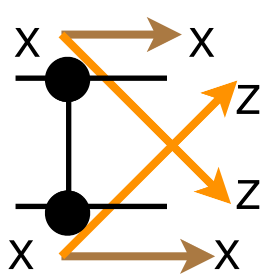
stabilizer演算子は各頂点に対して

$$K_i = X_i \prod_{j \in \boxed{V_i}} Z_j$$

点i と隣接する頂点の集合

と定義される.

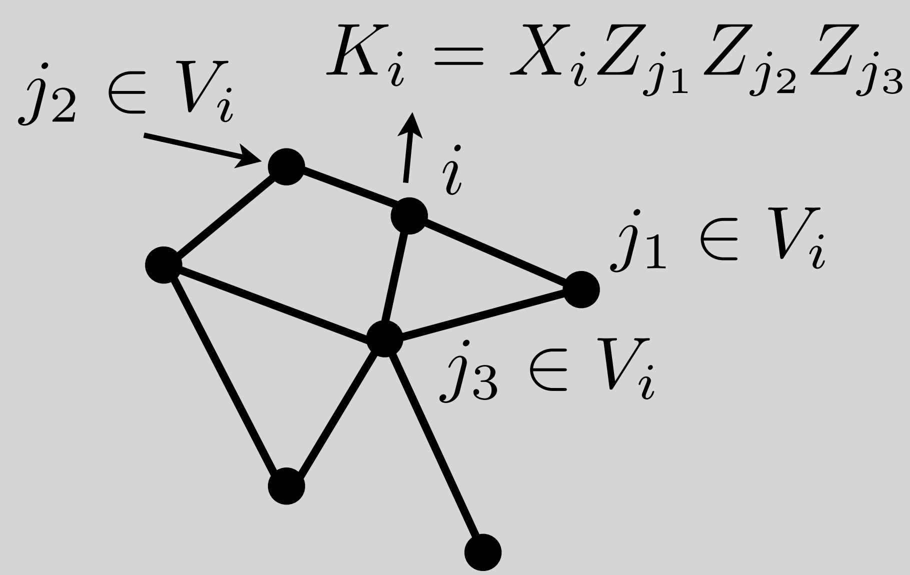
$$\rightarrow \ |\Psi_G\rangle = \prod_{e \in E} \Lambda(Z)_e |+\rangle^{\otimes |V|}$$



$$= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$$

$$e^{-i\pi/4(Z_1 Z_2 - Z_1 - Z_2 - I)}$$

CZ (controlled Z)



グラフ G(V,E)

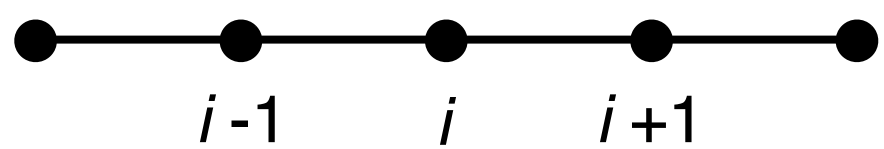
V:頂点の集合，E:辺の集合

グラフ状態

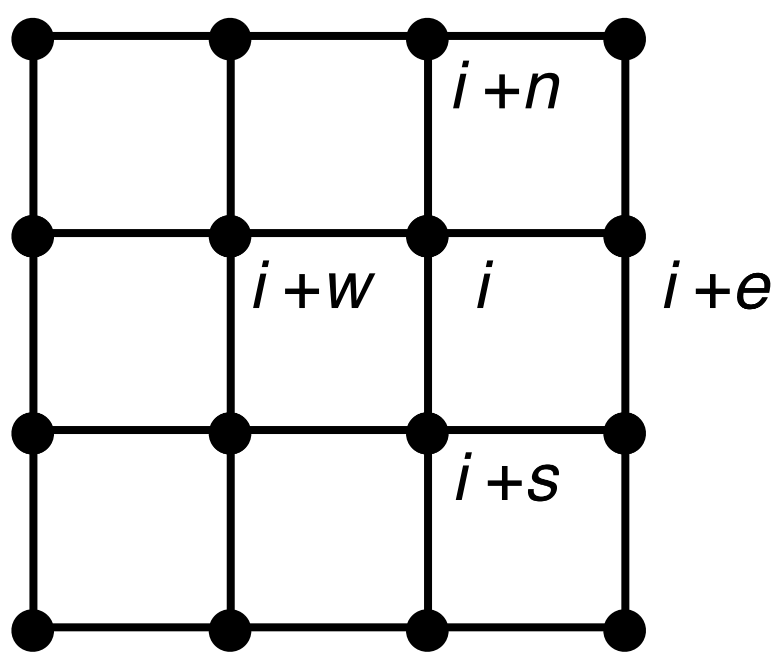
特に，並進対称性のあるグラフ（直線上，正方格子，六角格子など）上で定義される場合，cluster stateと呼ばれる．

◆ 1D cluster state

$$K_i = Z_{i-1} X_i Z_{i+1}$$



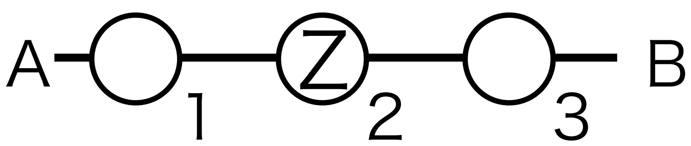
◆ 2D cluster state



$$K_i = X_i Z_{i+n} Z_{i+e} Z_{i+s} Z_{i+w}$$

グラフ状態の変形

◆ *Z* 基底の測定



測定前の stabilizer

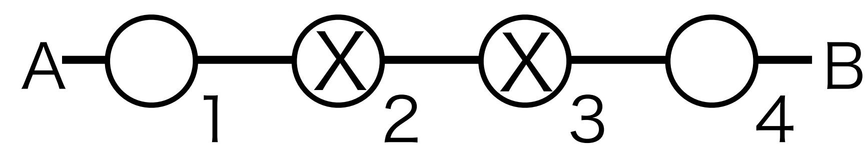
$$\begin{cases} S_1 &= A_z X_1 Z_2 \\ S_2 &= Z_1 X_2 Z_3 \\ S_3 &= Z_2 X_3 B_Z \end{cases}$$

測定後の stabilizer

$$\begin{cases} S_1 = A_z X_1 (Z_2) \\ S_3 = (Z_2) X_3 B_z \end{cases}$$

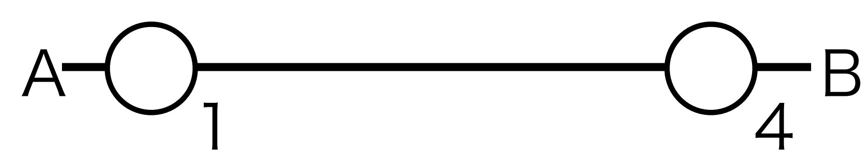
Z 測定された状態がグラフ状態から消える.

◆ *X* 基底の測定



$$\begin{aligned} S_1 &= A_z X_1 Z_2 \\ S_2 &= Z_1 X_2 Z_3 \\ S_3 &= Z_2 X_3 Z_4 \\ S_4 &= Z_3 X_4 B_Z \end{aligned}$$

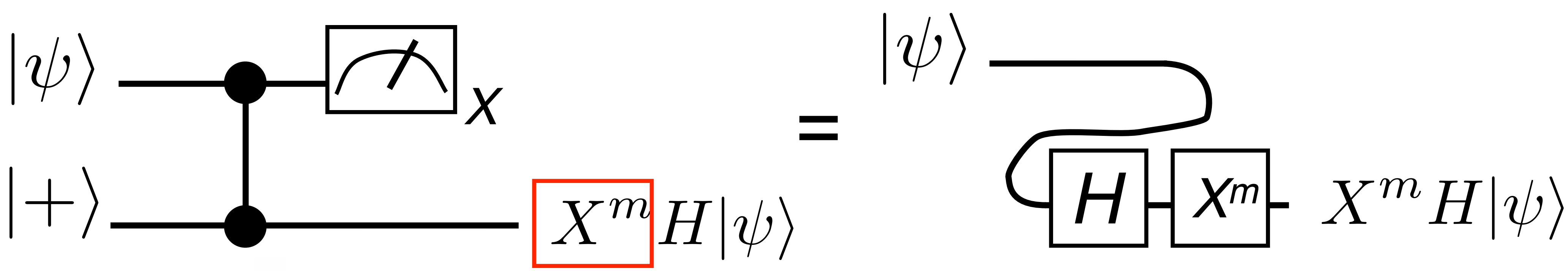
$$S_1 S_3 = A_z X_1 (X_3) Z_4$$
$$S_2 S_4 = Z_1 (X_2) X_4 B_z$$



2個連続で*X*基底で測定すると直接繋がる.

One-bit teleportation

◆ 1-bit teleportation： Zhou-Leung-Chuang, Phys. Rev. A 62,052316 (2000).

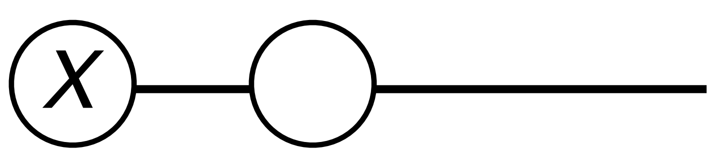


測定結果に依存してつく

“Pauli byproduct”

グラフ状態で書くと

input state

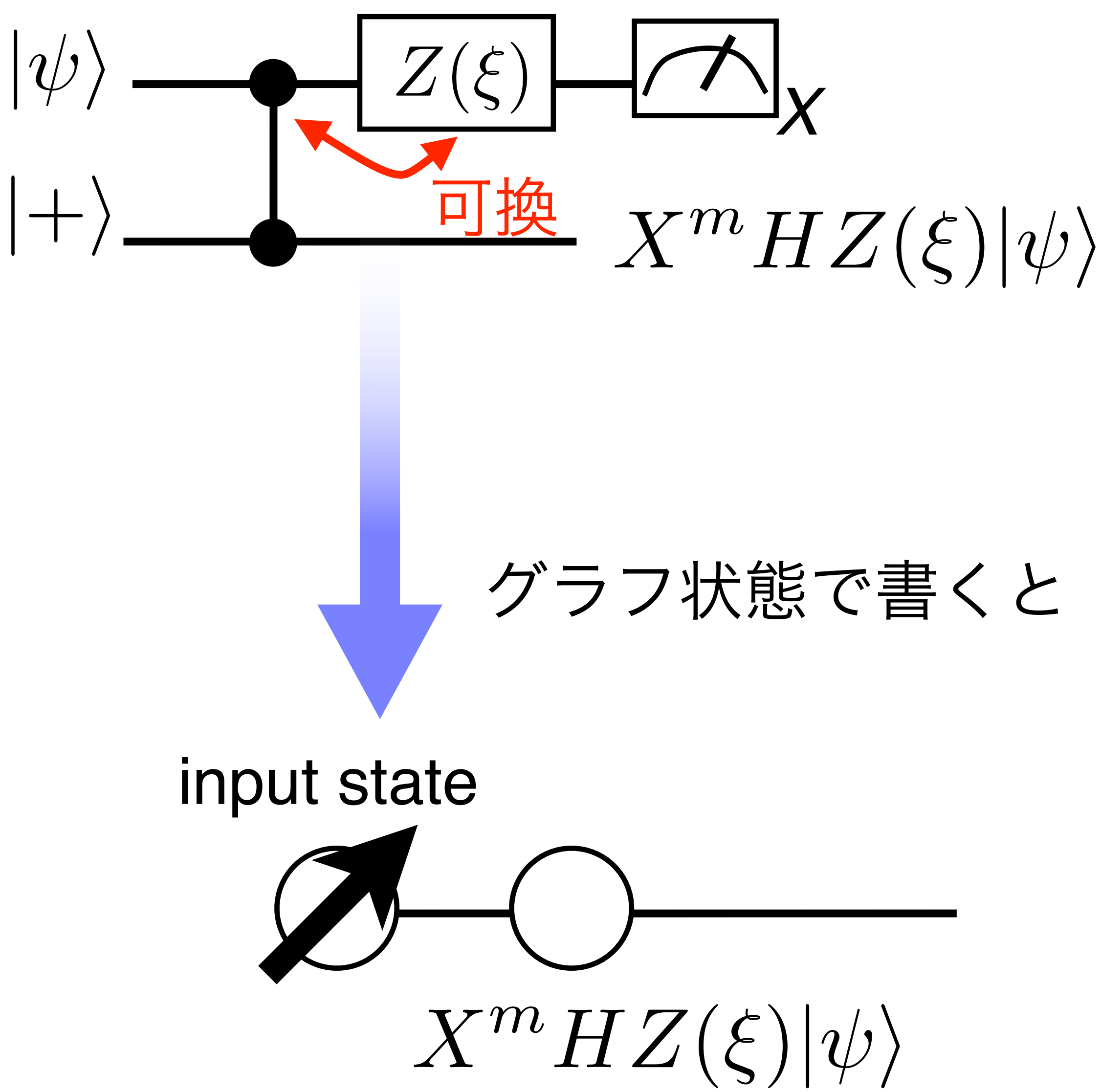


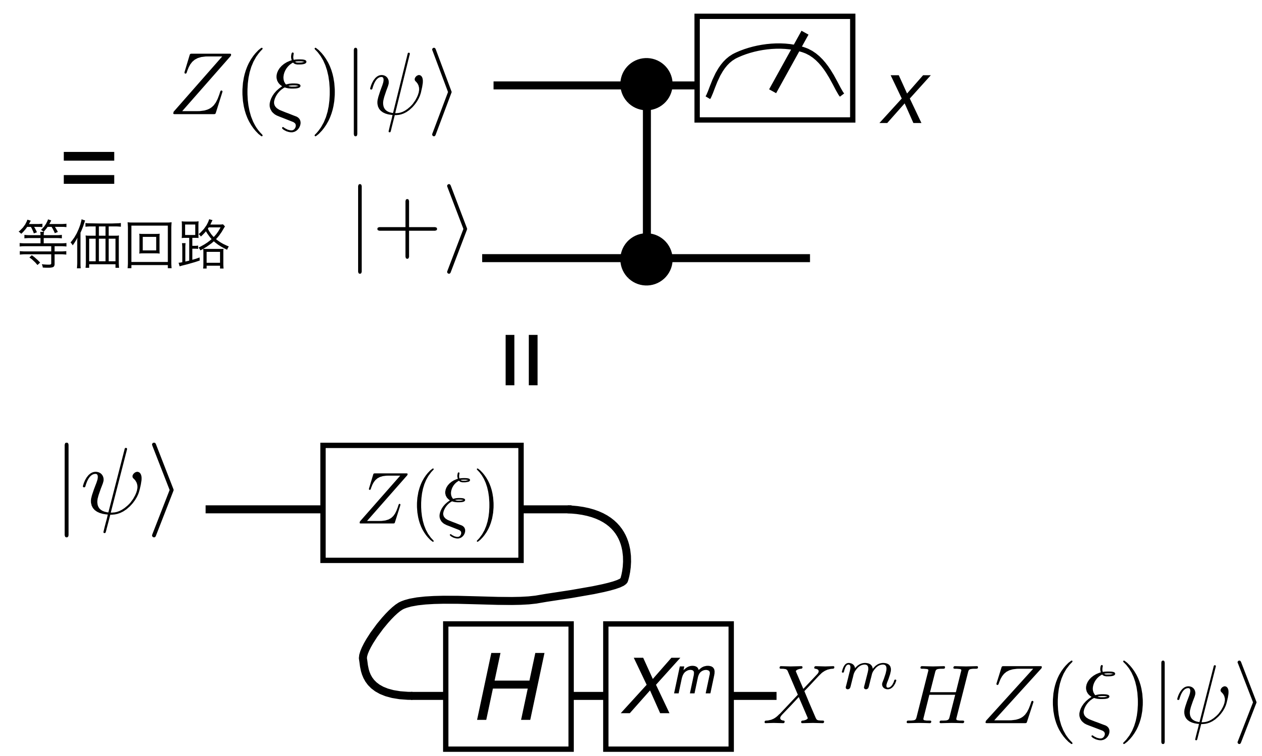
$X^m H|\psi\rangle$

One-bit teleportation

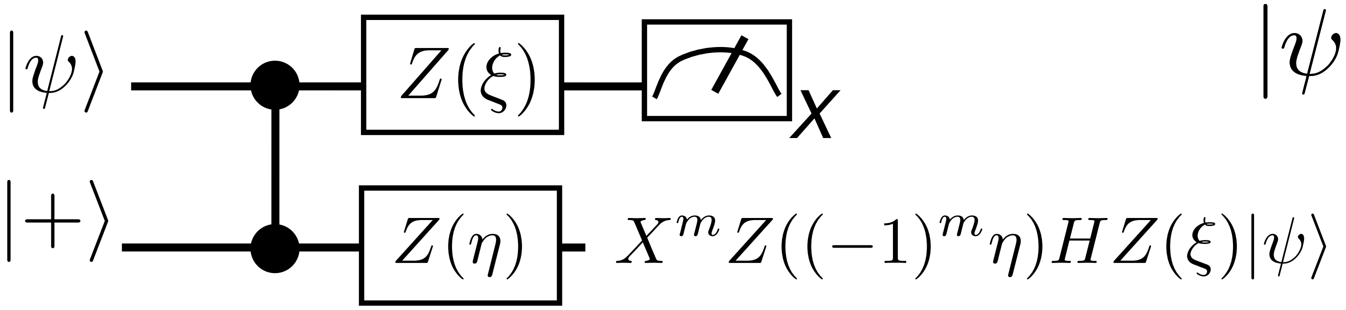
一次元cluster状態に対して $Z(\xi) = e^{-i\xi Z/2}$ を作用させて

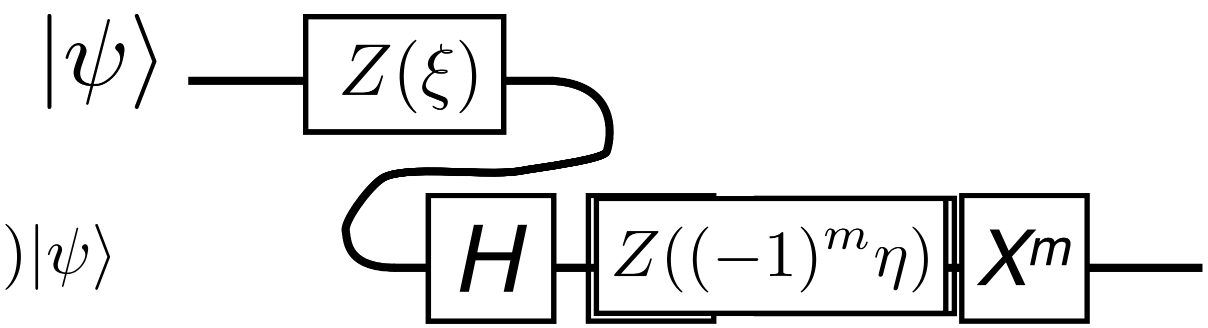
X 基底で測定→ $\{|0\rangle \pm e^{i\xi}|1\rangle\}$基底での測定 .

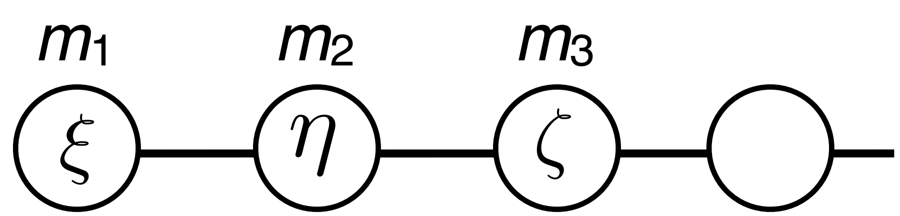




Feedforward







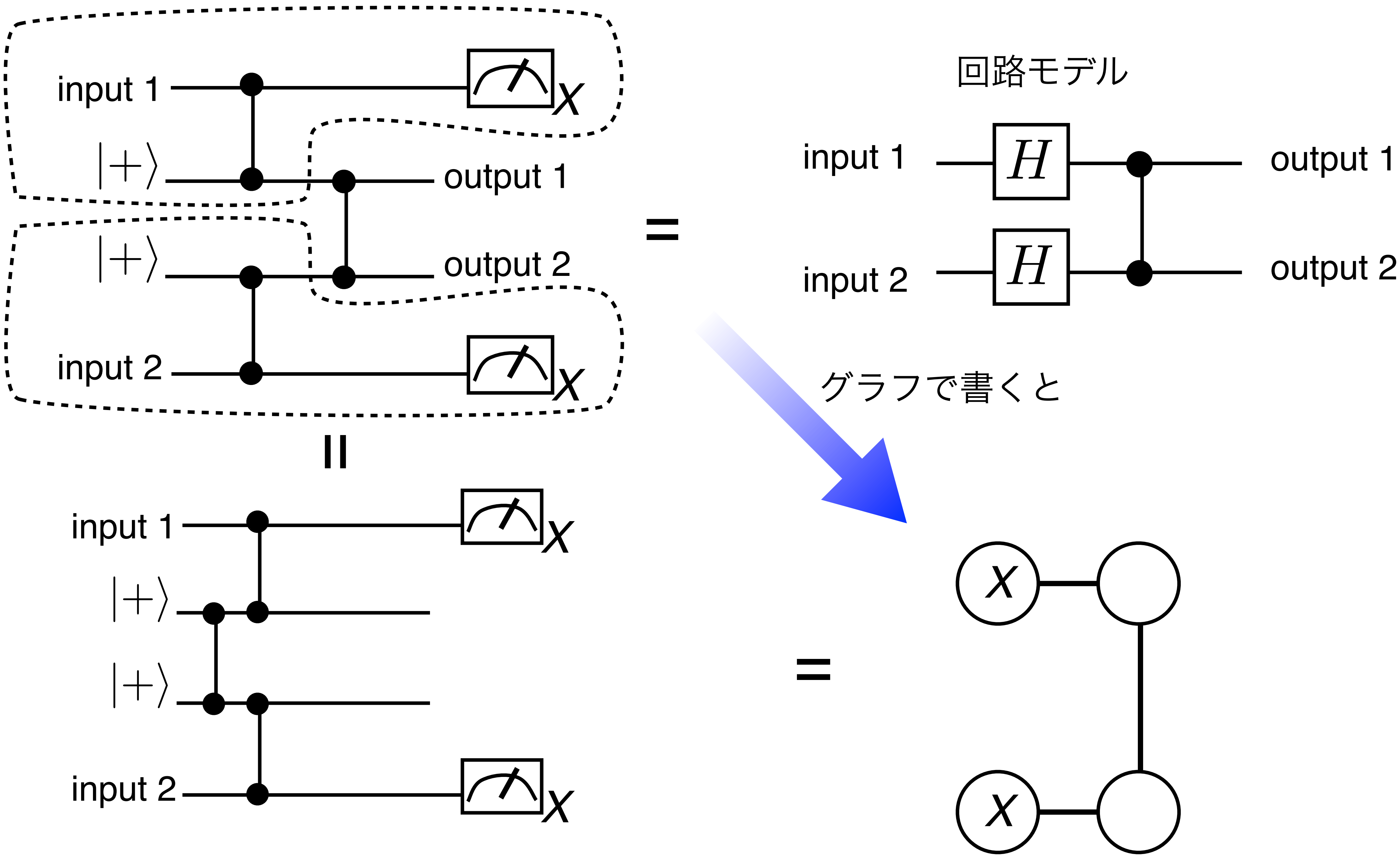
$$
\begin{aligned}
&X^{m_3} HZ(\zeta) X^{m_2} HZ(\eta) X^{m_1} HZ(\xi)|\psi\rangle \\
&= X^{m_3+m_1} Z^{m_2} HZ\big((-1)^{m_2}\zeta\big) HZ\big((-1)^{m_1}\eta\big) HZ(\xi)|\psi\rangle
\end{aligned}
$$

測定結果に従って，$\eta = (-1)^{m_1}\tilde{\eta}, \zeta = (-1)^{m_2}\tilde{\zeta}$, とすれば,

測定結果によらず $HZ(\tilde{\zeta})\underbrace{HZ(\tilde{\eta})H}_{= X(\tilde{\eta})}Z(\xi)|\psi\rangle$ を作用させれる.

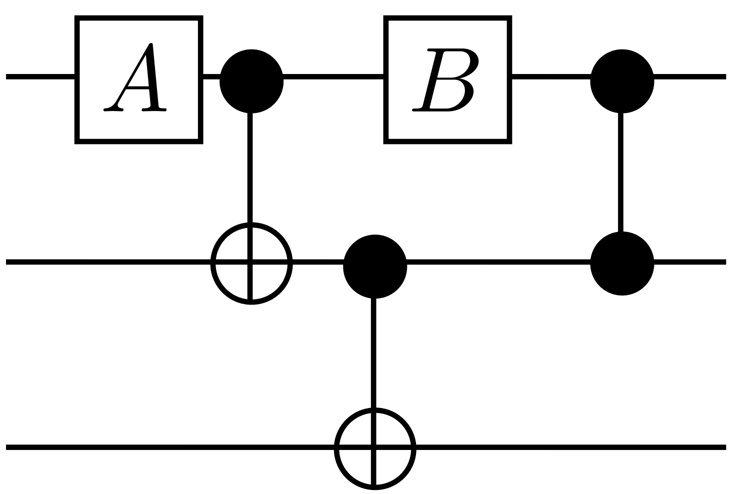
Gate teleportation

- Gate teleportation：D. Gottesman and I. L. Chuang, Nature (London) **402**, 390 (1999).



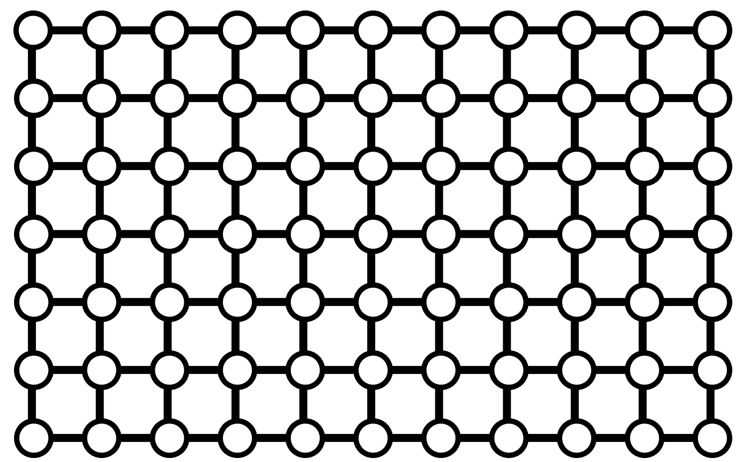
MBQC

実行したい量子計算



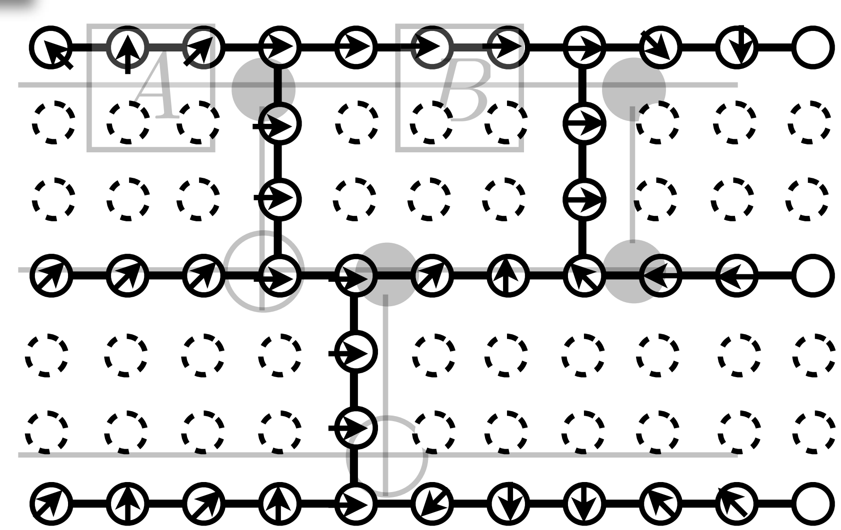
$$\langle 0|^{\otimes n} U |0\rangle^{\otimes n}$$

2Dグラフ状態



MBQC！

$$\langle \alpha_{nm}| \cdots \langle \alpha_i|\Psi\rangle$$



任意の量子計算

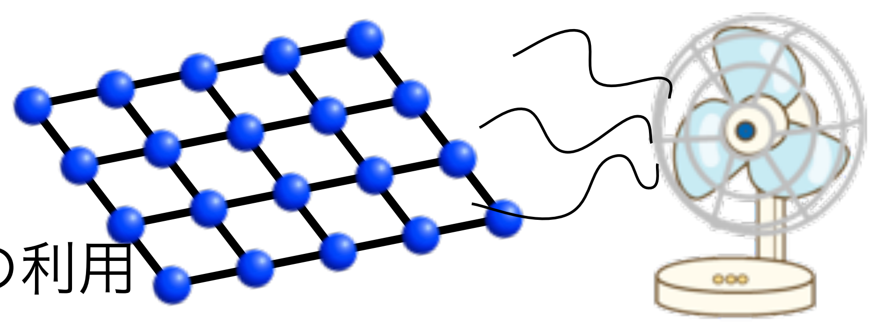
測定

MBQC on general resources

◆２体相互作用ハミルトニアン

クラスター状態は局所２体ハミルトニアンの基底状態になり得ない.

Nielsen, Rep. Math. Phys. **57,** 147 (2006);
Van den Nest *et al*., PRA **77,** 012301 (2008):
Chen *et al*., PRA **83,** 050301 (2011).



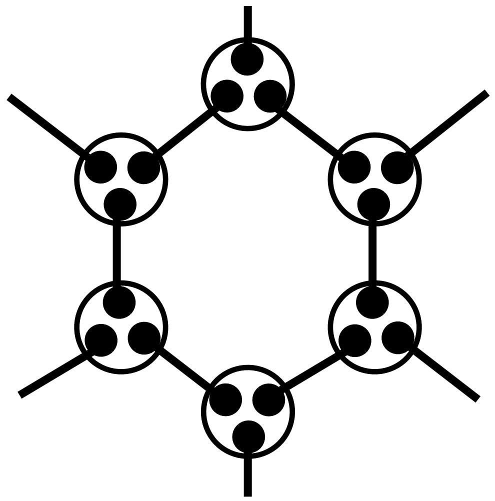
→**高次元粒子（qudit）**多体エンタングル状態の利用

Gross-Eisert, PRL **98,** 220503 (2007); Gross *et al*. PRA **76,** 052315 (2007).

dimension (spin)	model	resource	
d=6 (spin-5/2)	Tri-cluster by Chen *et al*., PRL ‘09	ground state	
d=4 (spin-3/2)	quasi 1D AKLT by Cai *et al*., PRA ‘10	ground state	
d=4 (spin-3/2)	2D AKLT by Miyake, Ann. Phys. ‘11	ground state	
d=4 (spin-3/2)	2D AKLT by Wei *et al*., PRL ‘11	ground state	
d=4 (spin-3/2)	2D honeycomb by Li *et al*., PRL ‘11	ground state	
d=5 (spin-2)	3D lattice by Li *et al*., PRL ‘11	thermal state	(T=0.21Δ)
d=4 (spin-3/2)	3D lattice by Fujii-Morimae, PRA ’12	thermal state	(T=0.18Δ)

MBQC on general resources

- **2D AKLT (VBS) model with spin-3/2 particles:**



$$H = J\sum_{\langle ij\rangle}\left[\mathbf{S}_i\cdot\mathbf{S}_j + \frac{116}{243}(\mathbf{S}_i\cdot\mathbf{S}_j)^2 + \frac{16}{243}(\mathbf{S}_i\cdot\mathbf{S}_j)^3\right]$$

A. Miyake, Ann. Phys. **326**, 1656 (2011)
T.-C. Wei, I. Affleck, R. Raussendorf, PRL **106,** 070501 (2011)

- **3D AKLT-like (VBS) model with spin-3/2 particles:**

K.F. and T. Morimae, PRA **85,** 010304R (2012).

Hamiltonian:

$$\begin{aligned} H &= \Delta\sum_{\mathbf{r}} \underbrace{\boxed{\vec{S}_{\mathbf{r}}}}_{\text{spin-3/2}}\cdot\underbrace{\boxed{(\vec{I}_{\mathbf{r+1}}+\vec{I}_{\mathbf{r+2}}+\vec{I}_{\mathbf{r+3}})}}_{\text{spin-1/2}} \\ &= \Delta/2\sum_{\mathbf{r}}(\vec{T}_{\mathbf{r}}^2-\vec{S}_{\mathbf{r}}^2-\vec{I}_{\mathbf{r}}^2) = \Delta/2\sum_{\mathbf{r}}[T(T-1)-S(S-1)-I(I-1)] \end{aligned}$$

→ ground state: T=0, S=3/2, I=3/2.

Local filtering operation:

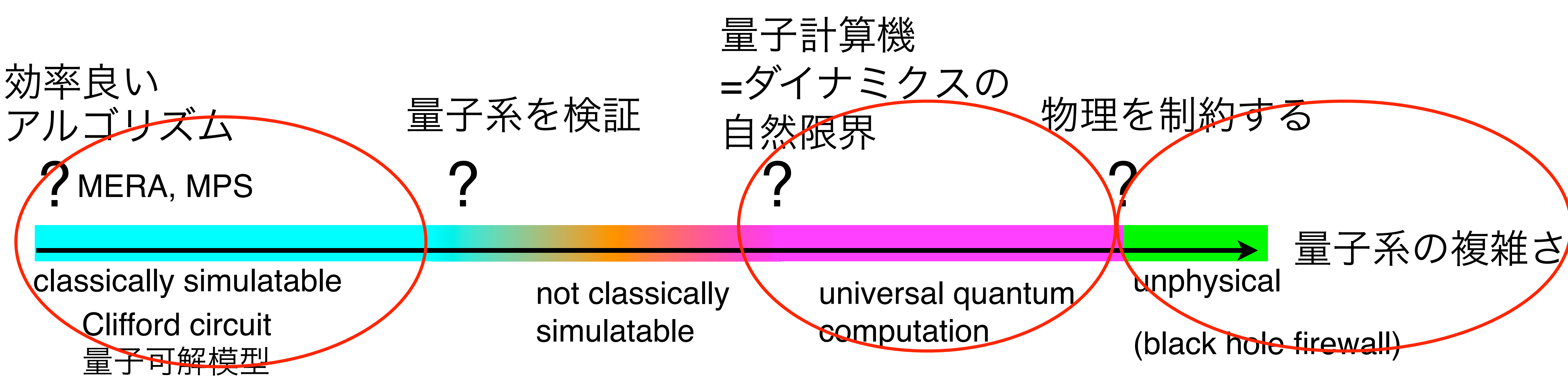
$$F^\alpha = (S_{\mathbf{r}}^{\alpha\,2}-1/4)/\sqrt{6} \text{ where } \alpha = x, y, z$$

→ **3D cluster state**

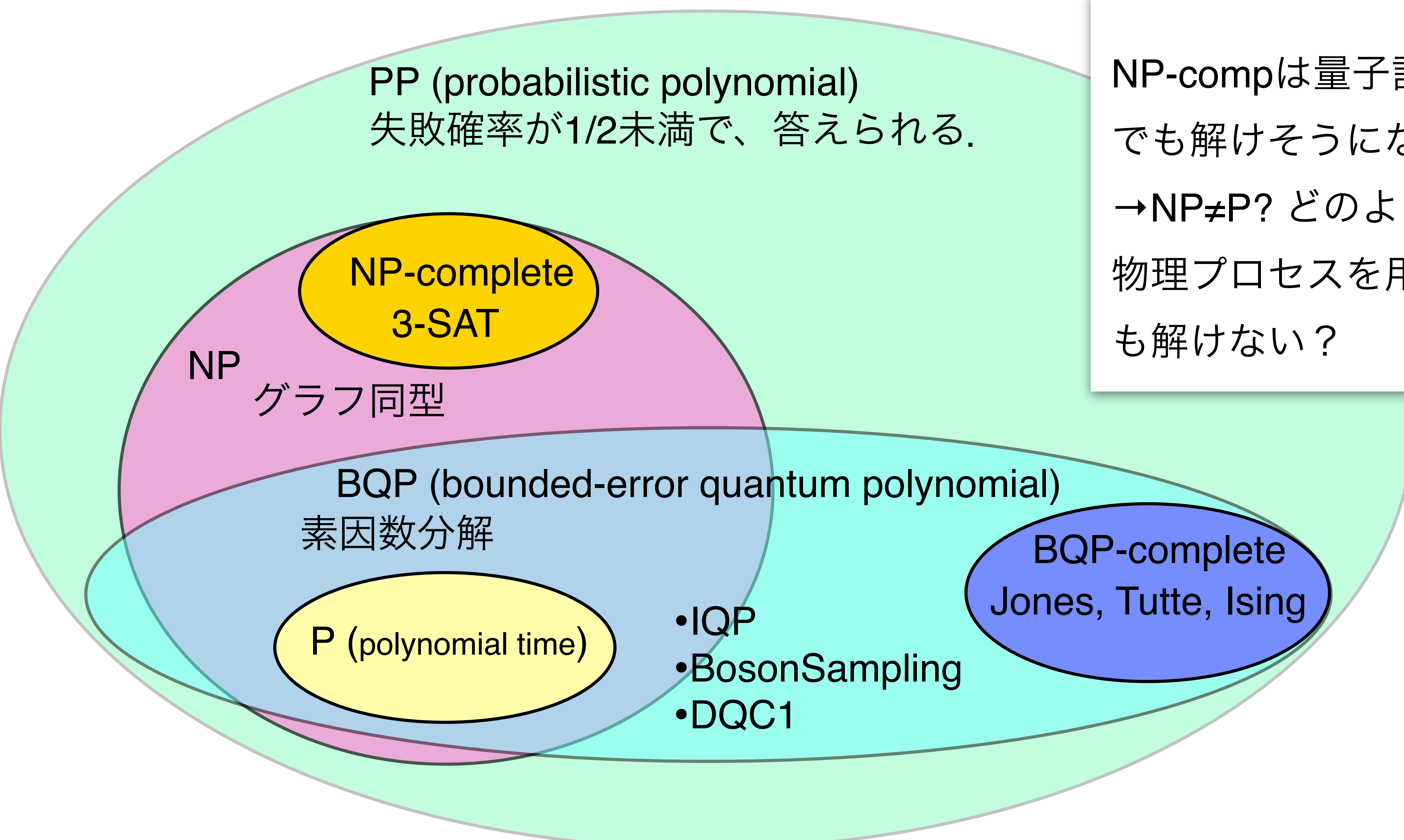
threshold temperature: $T_c = 0.18\Delta$

目次

- はじめに（なぜ量子計算？）
- ユニバーサル量子計算
- 測定型量子計算
- 古典シミュレート困難性



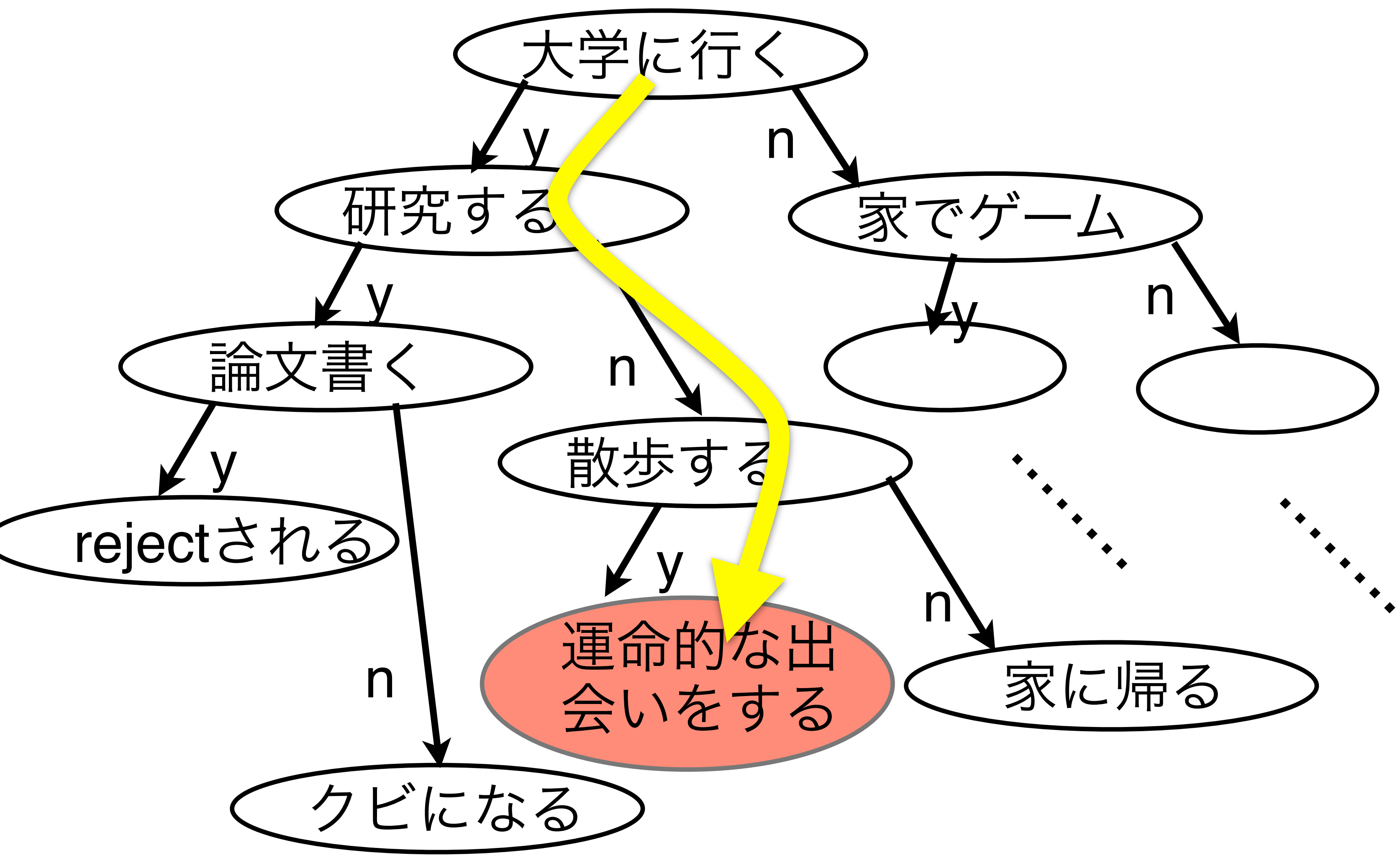
計算複雑性



NP-compは量子計算でも解けそうにない.
→NP≠P? どのような物理プロセスを用いても解けない？

非決定性マシン
nondeterministic machine

非決定性マシン = 最も幸運な経路を選択できるマシン
luckiest possible guesser



NP≠P

→こんなラッキーなことは起こらない.

「NP完全問題が，どんな物理ダイナミクスを用いても解けない.」

→たとえ量子を用いても，こんなラッキーなことは起きない.

NP問題：非決定性マシンで多項式的に解ける問題
（解が正しいことを効率よく検証できる問題）

多項式階層

polynomial hierarcy

オラクル（神託機械）：ある種の問題を1ステップで解いてくれる.

A^B ：計算機 A に クラスBの問題を 1 ステップで解けるオラクルを授けたもの.

多項式階層（polynomial hierarchy)：

$$\Delta_1 = P, \quad \Delta_{k+1} = P^{N\Delta_k}$$

$$PH = \cup_k \Delta_k$$

多項式階層がレベル k でつぶれる→ $\Delta_k = \Delta_{k+1} = \ldots\ldots = PH$

もし，P=NPなら，階層が完全につぶれる.

階層がつぶれることはあり得ないとされ，しばしば議論の仮定として用いられる.
→ PH が level-3で崩壊しない限り，命題が正しい etc.

P^{PP} は PH に含まれる問題をすべて解けるほどパワフル （戸田の定理）

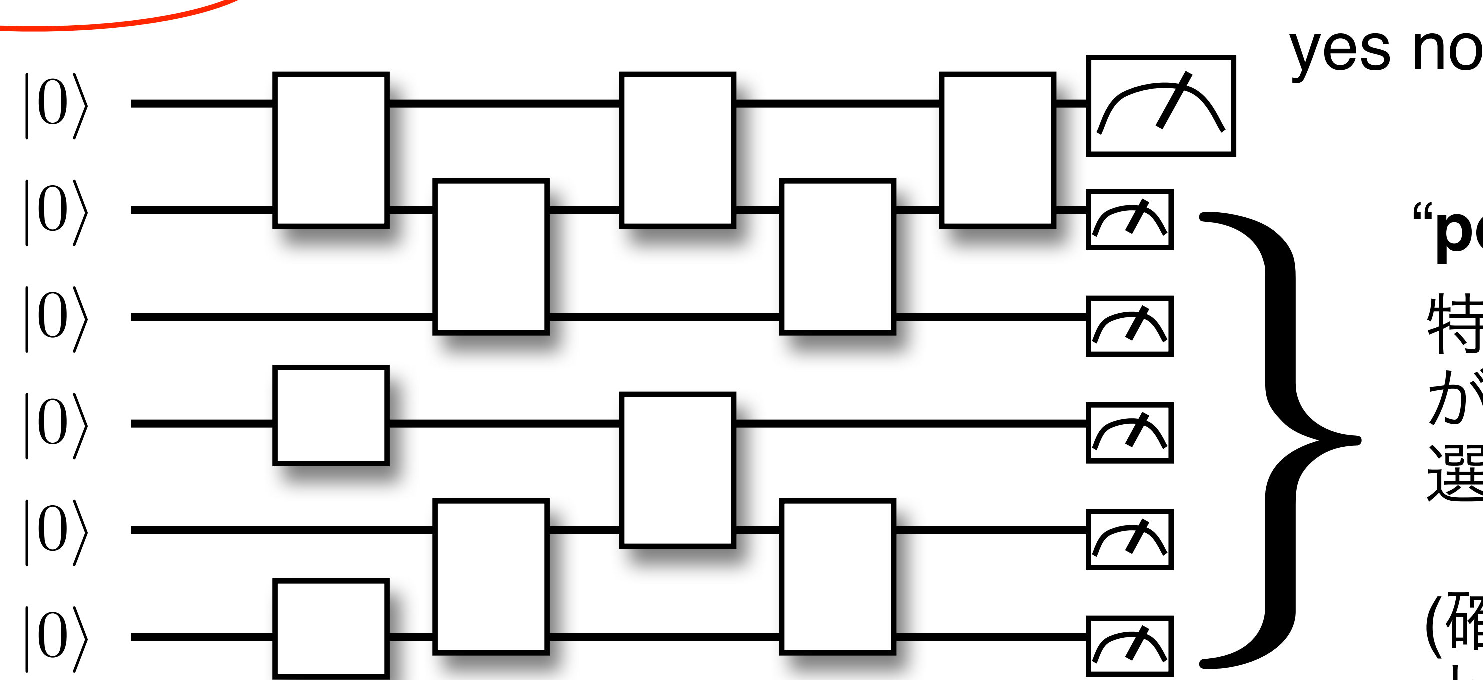
Postselected quantum computation

◆ 量子計算で解ける(Yes or No)問題のクラス

→Bounded-error Quantum Polynomial (BQP)

成功確率が$1/2+\delta$

δ は問題サイズに依存しない.



“postselection”

特定の測定結果が出る場合のみ選択する.

(確率は指数的に小さくていい)

“post”BQP

postBQP = PP

(量子計算+postselection) (probabilistic polynomial)

量子計算にpostselectionを許すとものすごくパワフルになる！

S. Aaronson, Proc. Royal Soc. A: Math., Phys. and Eng. Sci. 461.2063 (2005)

Born規則と計算量

◆ 測定結果が $|\alpha|^p, |\beta|^p$ で得られる量子力学を考えてみる.

量子計算 → $\mathrm{BQP_p}$

$$\mathrm{postBQP} = \mathrm{PP} \subseteq \mathrm{BQP_p}$$

$\sum_z \alpha_z |z\rangle$ のうち, $z \in \mathcal{S}$ を postselect したい. . .

もし, $p < 2$ ならば, K qubitのアンシラに対して, $z \in \mathcal{S}$ 関する controled-Hadamard変換を作用させる($|0\rangle \to (|0\rangle + |1\rangle)/\sqrt{2}$)

$$|\alpha_z|^p \to 2^K |2^{-K/2}\alpha_z|^p = 2^{K(2-p)/2}|\alpha_z|^p$$ (増幅できる！)

もし $p > 2$ ならば, $z \notin \mathcal{S}$ に対して同様のことをする.

いかなる物理プロセスも NP完全問題を解けないならば, *p*=2（Born rule）

S. Aaronson, Proc. Royal Soc. A: Math., Phys. and Eng. Sci. 461.2063 (2005)

postBQP=PPの応用

postselectionして量子計算をシミュレートできるものは,

古典計算機でシミュレートできない（量子性を含む）.

$$\text{post-}\boxed{\text{A}} = \text{postBQP} = \text{PP}$$

一見ほとんど量子性がない

ように思われるもの。

もしAを古典でシミュレートできたとすると、

$$\text{PP} = \text{post-A} \subseteq \text{postBPP}$$ (古典+postselection)

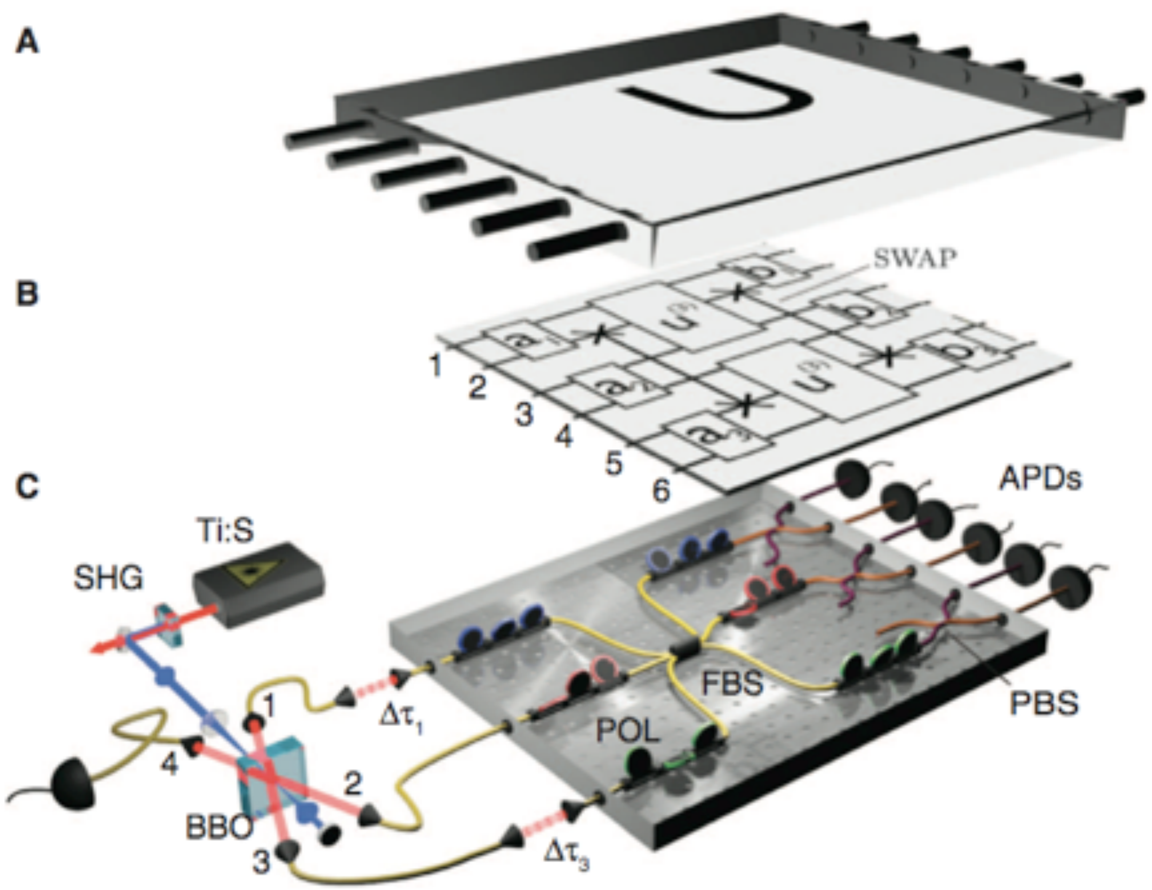
→PHがレベル３で崩壊.

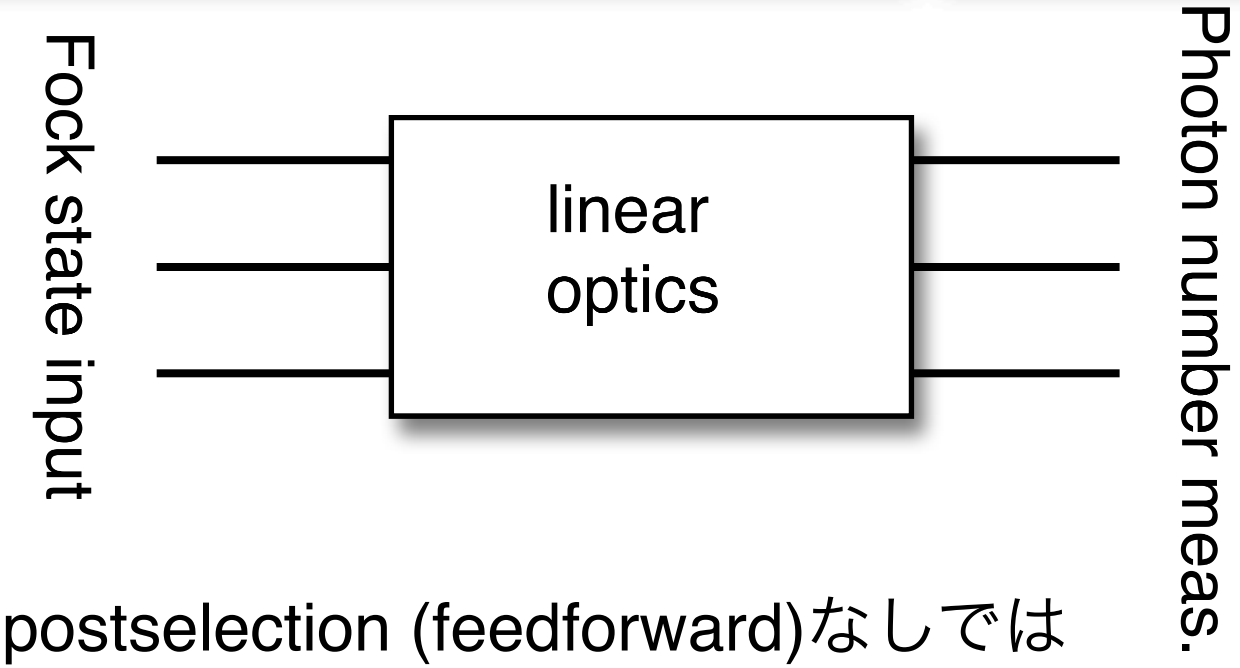
→PHが崩壊しない限り，Aは古典ではシミュレートできない.

Bremner-Jozsa-Shepherd, Proc. Royal Soc. A: Math. Phys. and Eng. Sic. 467, 2126 (2011)

BosonSampling

Aaronson-Arkhipov, STOC '11, arXiv:1011.3245





postselection (feedforward)なしでは universal QCは出来ない.

Knill-Laflamme-Milburn, Nature 409, 46 (2001)
Knill, arXiv:0307015.

Postselection (feedforward)のない linear opticsを，古典でシミュレートするのは PHが崩壊しない限り，難しい.

boson → 行列のpermanent，fermion → 行列のdeterminant

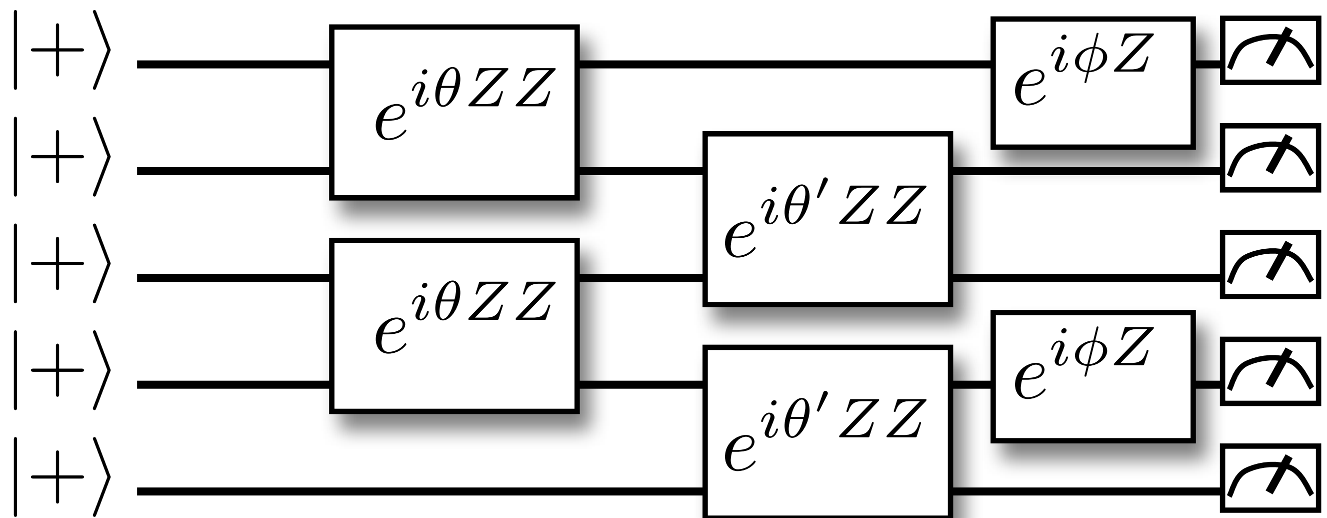
実証実験：J. B. Spring *et al*. Science **339**, 798 (2013); M. A. Broome, Science **339**, 794 (2013); M. Tillmann *et al*., Nature Photo. **7**, 540 (2013); A. Crespi *et al*., Nature Photo. **7**, 545 (2013)

IQP (Instantaneous Quantum Polynomial)

Bremner-Jozsa-Shepherd, Proc. Royal Soc. A: Math. Phys. and Eng. Sic. 467, 2126 (2011)

可換量子回路（順序は関係なし）

Xの
固有状態



X基底での測定

可換回路でも、エンタングルメントは生成できる.
→graph 状態を作れる.

測定結果による feedforward が許されていないので，MBQCはできない.
→postselectionを許せば，feedforwardなしで量子計算できる.
→IQPは古典ではシミュレートできない.

イジング模型分配関数の計算複雑性との対応：KF-Morimae, arXiv:1311.2128

- 可解模型→classically simulatable (かなりエンタングルはします)
- 特定のイジング分配関数の計算→ 量子計算機の出力と同等に難しい

まとめると．．．．

効率良い
アルゴリズム

量子系を検証

量子計算機

物理を制約する

? MERA, MPS

?

?

?

classically simulatable

not classically
simulatable

quantum universal

unphysical

Clifford circuit
free-fermion
量子可解模型

BosonSampling
IQP

MBQC
(AKLTなど）
Ising分配関数、
Jones多項式
Tutte多項式

QSZK
(Black hole firewall)

量子計算の研究 ＝ 物理に複雑さの尺度を提供する!