春の学校：Particles, Strings, and Quantum Information

量子情報・計算の基礎

藤井啓祐
京都大学白眉センター/大学院理学研究科

エンタングルメント・量子測定

量子情報・計算

量子暗号
の安全性

実現

量子重力
(Ads/CFT)
吉田紅さんのセミナー

トイモデル

量子誤り訂正

誤り耐性
量子計算

量子アルゴリズム

トポロジカル
量子計算

トイモデル

複雑性

TQFT
(Jones多項式)

復号化問題

可解模型

量子相
(トポロジカル秩序,エニオン)

統計力学
(スピングラス)

目次

第一部：量子計算

・量子計算の基礎

・量子アルゴリズム

-Hadamardテスト

-Shorの素因数分解アルゴリズム

-Jones多項式の近似

第二部：量子誤り訂正符号

参考資料：集中講義「量子コンピュータ概論」講義ノート
http://quantphys.org/keisukefujii/lecture.html

arXiv: 1504.01444 to be published from SpringerBriefs

量子計算の基礎

量子ビット

◆ 計算基底(computational basis)　$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$　$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

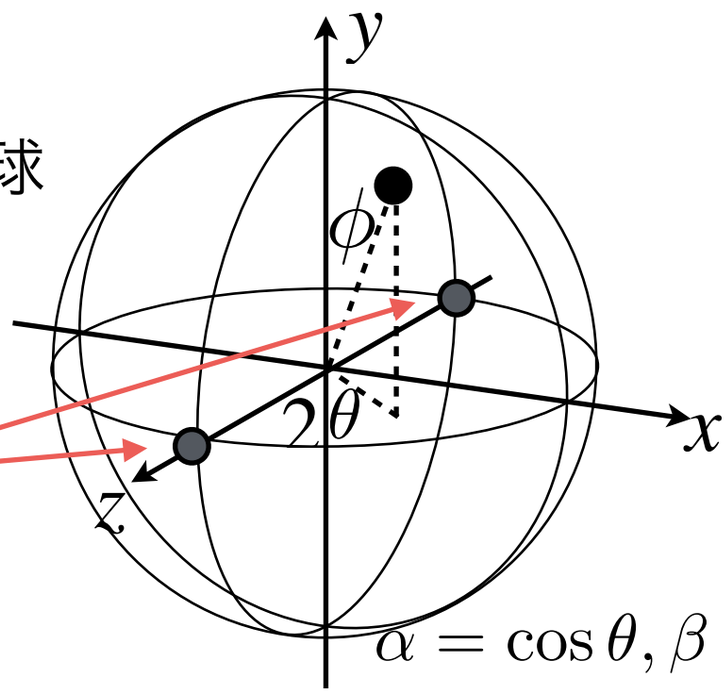
◆ 量子ビット

$$|\psi\rangle \doteq \alpha|0\rangle + \beta|1\rangle \qquad \alpha, \beta \in \mathbb{C} \quad |\alpha|^2 + |\beta|^2 = 1$$

◆射影測定 $\{|0\rangle, |1\rangle\}$

$$p_0 = |\langle 0|\psi\rangle|^2, \quad p_1 = |\langle 1|\psi\rangle|^2$$

Bloch球

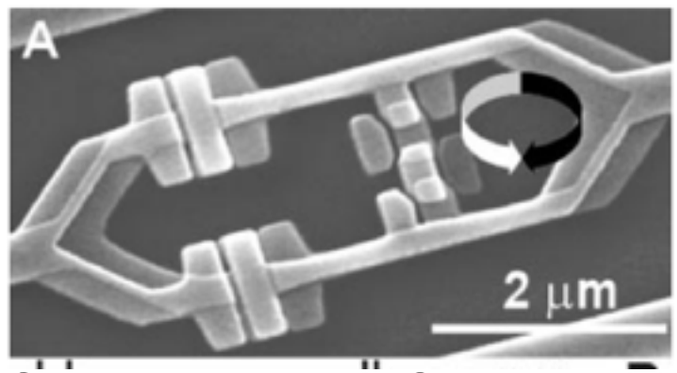


古典ビット

$\alpha = \cos\theta, \beta = e^{i\phi}\sin\theta$

単一光子,電子・核スピン,

イオン・中性原子, 超伝導回路



Chiorescu et al, Science 2003

Pauli演算子

◆ Pauli演算子

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- 反交換(anti-commute): $ZX = -XZ$
- $XZ = iY$

$$X|0\rangle = |1\rangle \quad X|1\rangle = |0\rangle \quad \text{(bit-flip)}$$

$$Z|0\rangle = |0\rangle \quad Z|1\rangle = -|1\rangle \quad \text{(phase-flip)}$$

$$Y|0\rangle = i|1\rangle \quad Y|1\rangle = -i|0\rangle \quad \text{(bit\&phase-flip + global phase)}$$

◆ Pauli演算子の固有状態（Pauli基底）

$$Z \to |0\rangle, |1\rangle \qquad X \to |+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$$

Z basis　　*X* basis

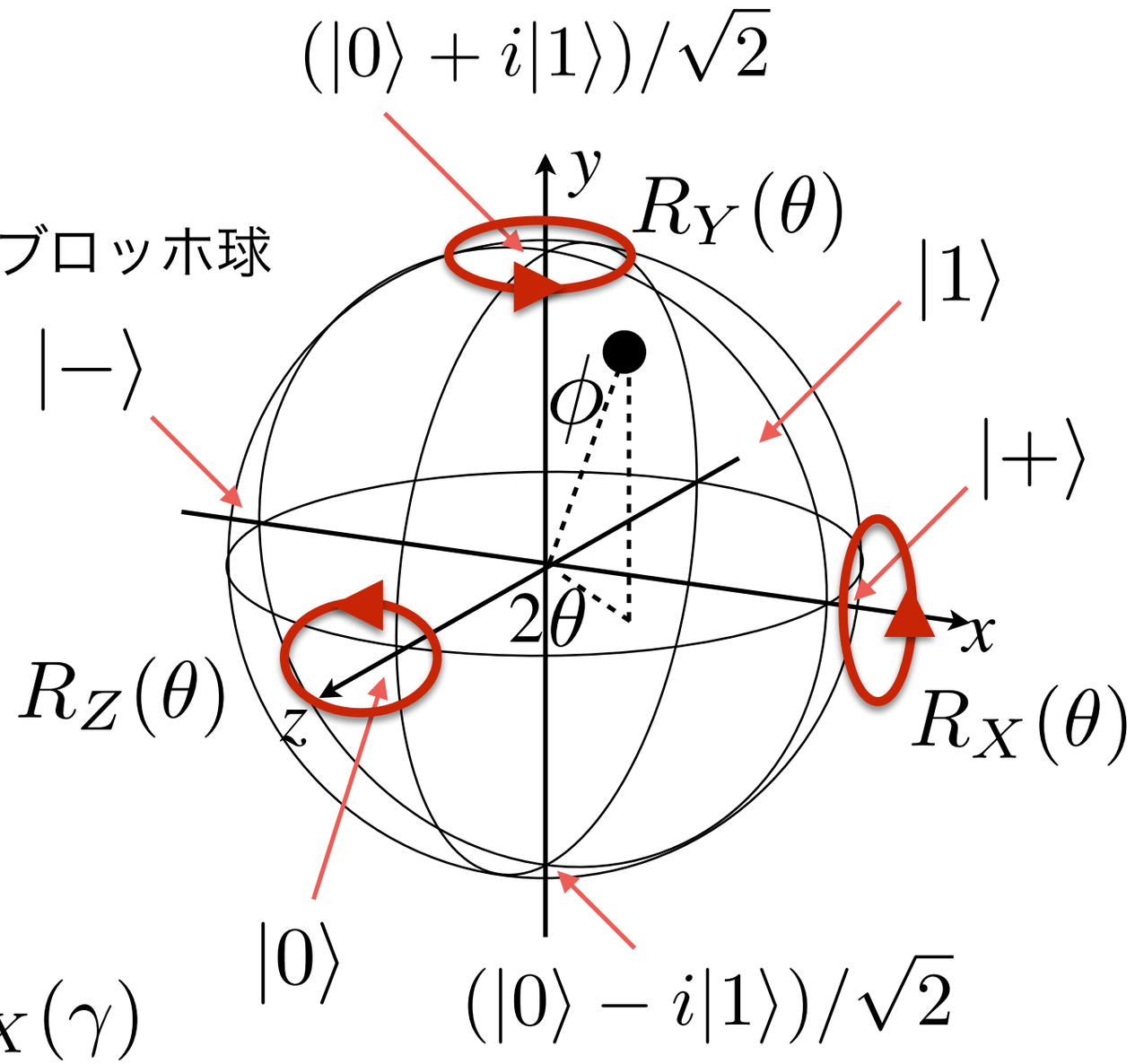
単一量子ビット演算

◆ x,y,z軸回転

$$R_A(\theta) = e^{-i\frac{\theta}{2}A}$$

$$A = X, Y, Z$$

例） $e^{-i\frac{\pi}{4}Y}|0\rangle = |+\rangle$

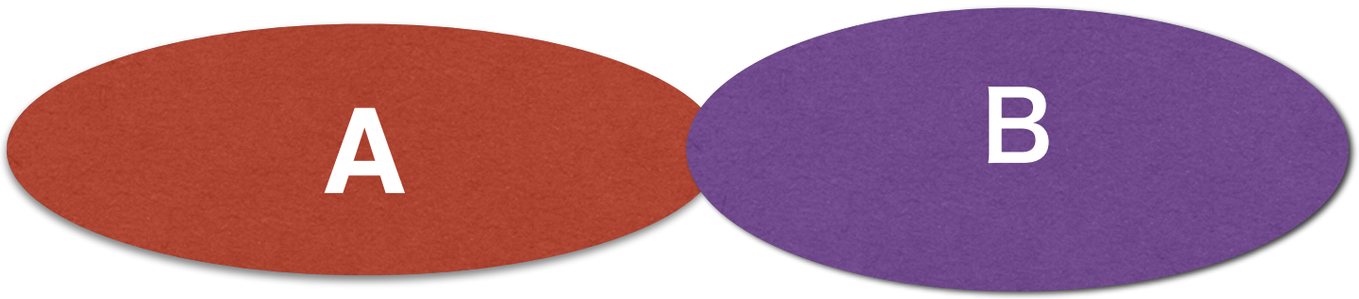


◆ SU(2)のEuler分解:

$$U = R_X(\alpha)R_Z(\beta)R_X(\gamma)$$

多量子ビット系

◆合成系 =テンソル積：



$$\mathcal{H}_A \otimes \mathcal{H}_B$$

◆テンソル積

$$|0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \begin{matrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{matrix}$$

Kronecker product

◆テンソル積空間の基底

$$\{|0\rangle, |1\rangle\} \otimes \{|0\rangle, |1\rangle\} \quad \rightarrow |00\rangle, |01\rangle, |10\rangle, |11\rangle$$

エンタングル状態: $(|00\rangle + |11\rangle)/\sqrt{2}$

多量子ビット系

◆ *n*量子ビット系（2^n次元）の記述

$$|\Psi\rangle = \sum_{i_1,i_2,\ldots,i_n} C_{i_1,i_2,\ldots,i_n} |i_1 i_2 \ldots i_n\rangle \quad (i_k = 0,1)$$

2^n 個の**複素パラメータ!!!**

http://www.nobelprize.org/nobel_prizes/physics/laureates/1965/feynman-bio.html

Richard Phillips Feynman
(1918-1988)

*"If a computer stimulates this …. require **an exponentially explosive growth in the size** of the simulating computer."*

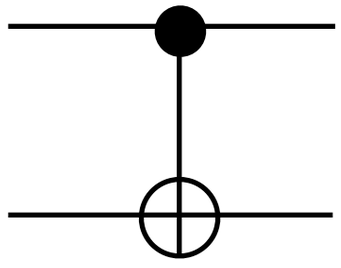
*"Let the computer itself be **built of quantum mechanical elements** which obey quantum mechanical laws."*

"Simulating Physics with Computers"
International Journal of Theoretical Physics (1982)

多量子ビット演算子

◆ CNOT (controlled NOT)

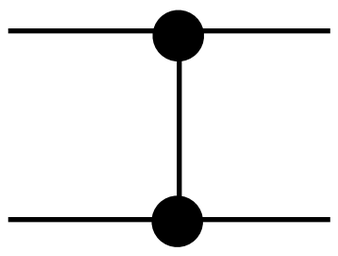
$\Lambda(X)$



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

◆ CZ (controlled Z)

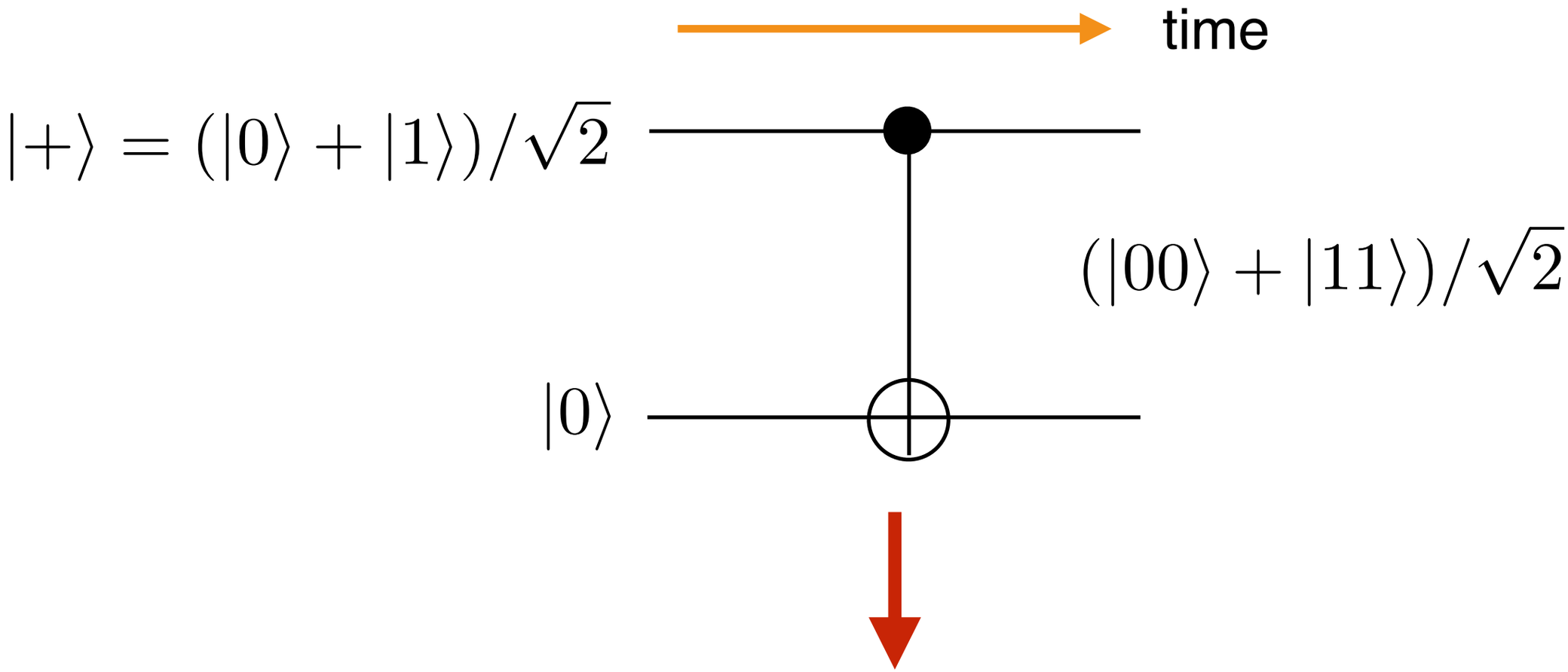
$\Lambda(Z)$



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

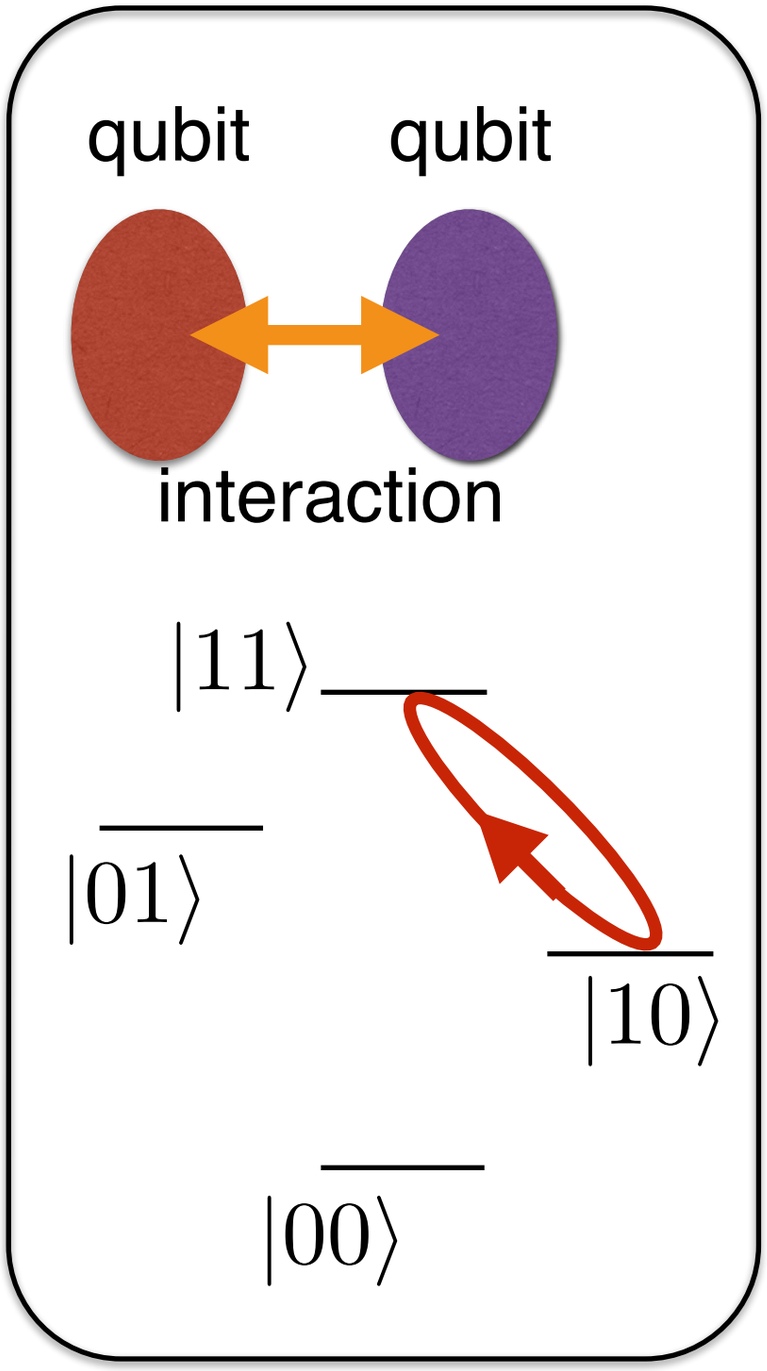
$$e^{-i\pi/4(Z_1 Z_2 - Z_1 - Z_2 - I)}$$

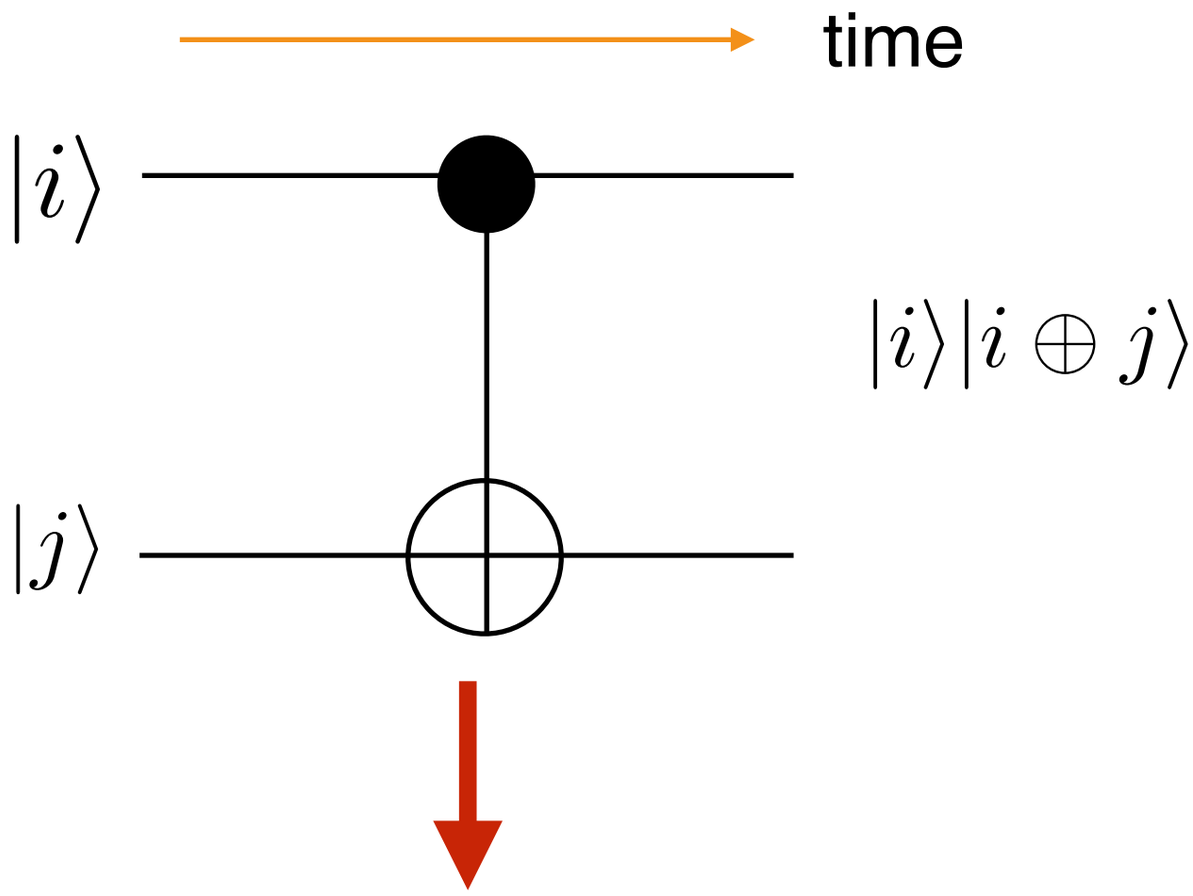
量子回路



$$\Lambda_{c,t}(X)|+\rangle_c|0\rangle_t = (|00\rangle + |11\rangle)/\sqrt{2}$$

量子回路





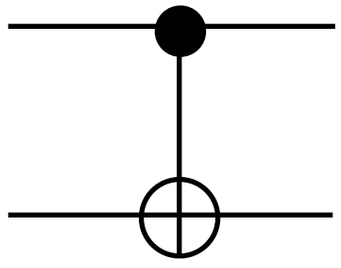
$$\Lambda_{c,t}(X)|ij\rangle = |i\ i \oplus j\rangle$$

XOR(排他的論理和)

多量子ビット演算子

◆ CNOT (controlled NOT)

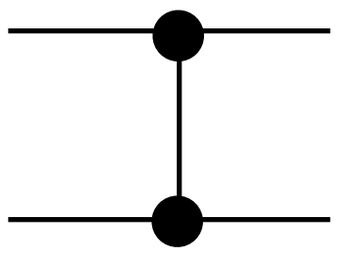
$\Lambda(X)$



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

◆ CZ (controlled Z)

$\Lambda(Z)$



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

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

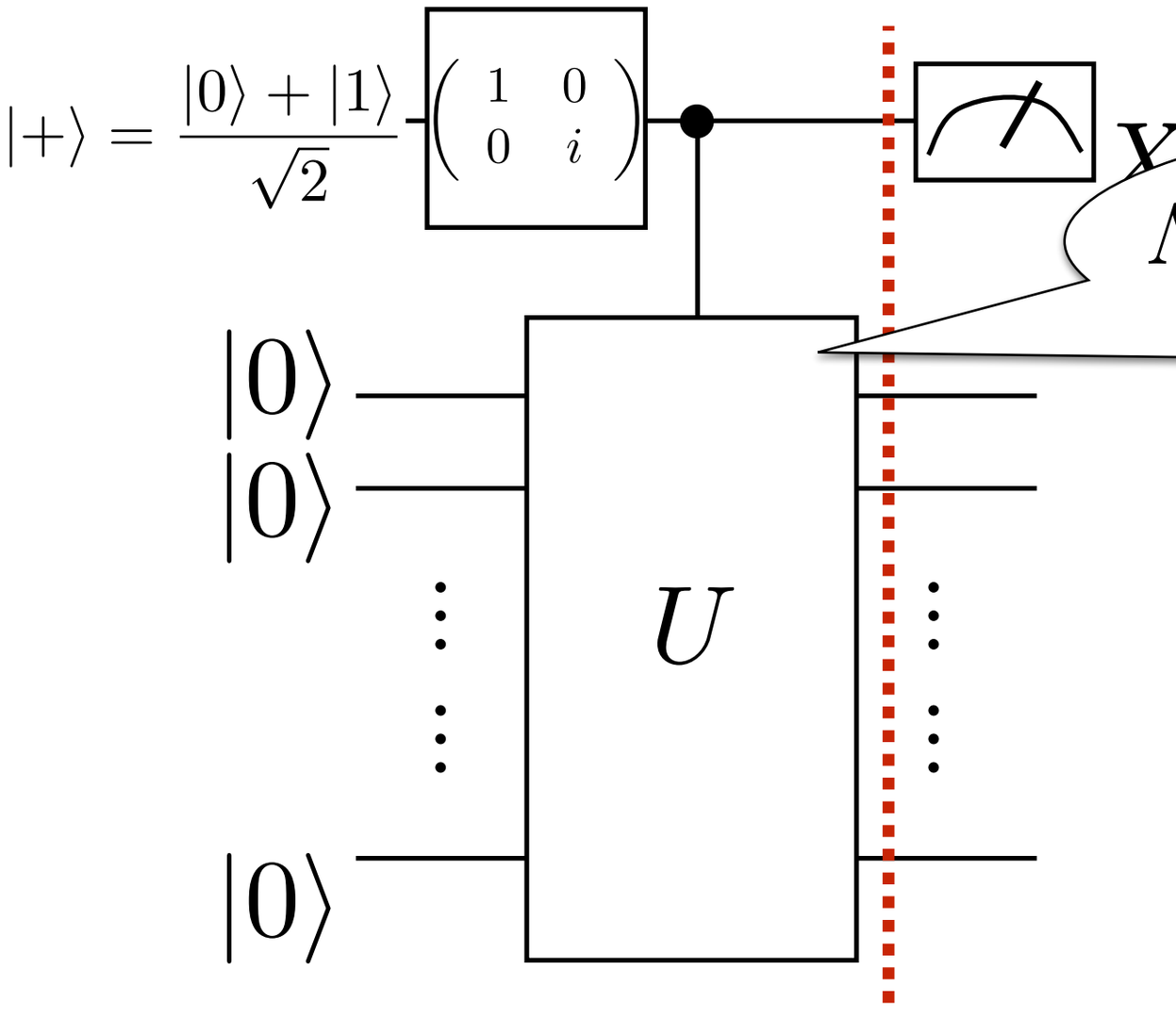
CNOT と **SU(2)** で任意の*n* 量子ビットユニタリ演算子を構成できる.　　→ **万能量子計算**

universal quantum computation

量子アルゴリズム

量子計算機で何が計算できるか？

Hadamardテスト



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

$$p_\pm = \|(\langle \pm| \otimes I)|\psi\rangle\|^2$$

$$\Lambda(U) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

$$p_- = \frac{1}{2}(1 - \mathrm{Re}\langle 00..0|U|00..0\rangle)$$

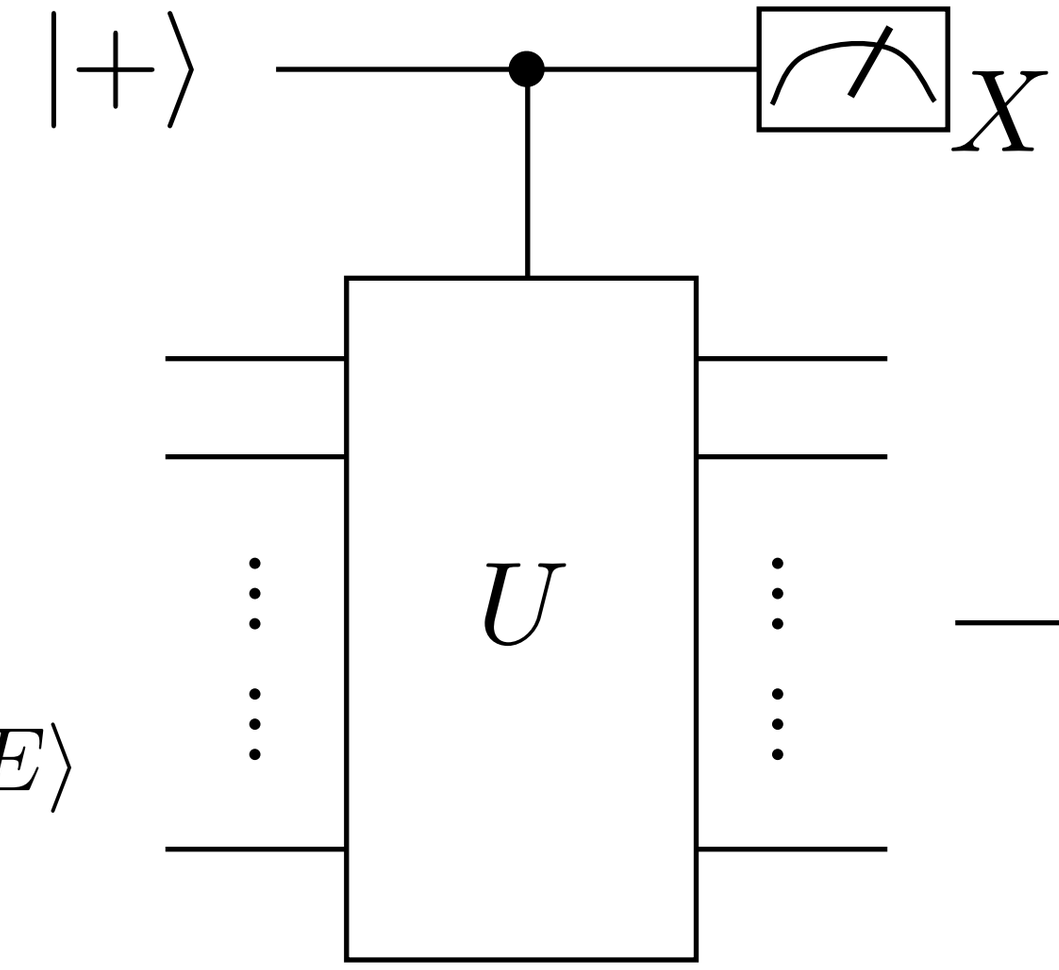
$$\longrightarrow \langle 00..0|U|00..0\rangle$$

$2^n \times 2^n$ ユニタリ演算子の行列要素

Chernoff-Hoeffding 限界

$$\mathrm{Prob}\left(\left|\frac{N_+}{N} - p_+\right| > \delta\right) \leq 2e^{-2\delta^2 N}$$

Hadamardテスト



固有状態 $|E\rangle$

$U|E\rangle = e^{i\lambda}|E\rangle$

固有値

$\longrightarrow \langle E|U|E\rangle = e^{i\lambda}$

λをもっと精度よく推定できないか？

量子フーリエ変換 & Kitaevの位相推定

→ある性質をもったの U に対しては λ を多項式桁まで推定できる.

Shorの素因数分解アルゴリズム

N , *x* ：互いに素な整数.

r : 位数　$x^r = 1 \bmod N$

$$(x^{r/2} - 1)(x^{r/2} + 1) = 0 \bmod N$$

GCD → *N*の因数

Peter Shor

http://www-math.mit.edu/~shor/

$$U_x = \sum_y |xy \bmod N\rangle\langle y|$$

位相推定
(連分数展開)

$$U_x|u_s\rangle = e^{2\pi i(s/r)}|u_s\rangle$$

$$\left(|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i(s/r)k} |x^k \bmod N\rangle. \right)$$

Jones多項式の近似量子アルゴリズム

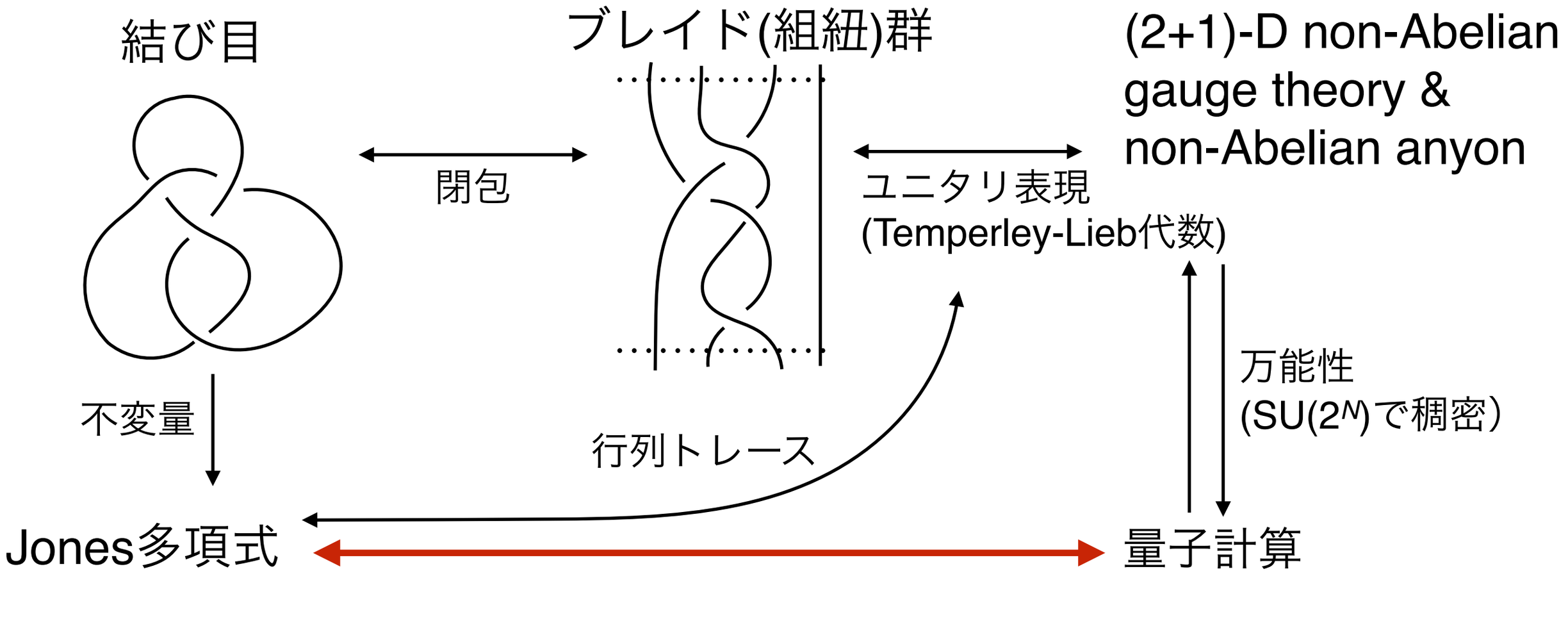
Jones多項式の近似と量子計算

Jones多項式：結び目(knot)不変量（多項式）

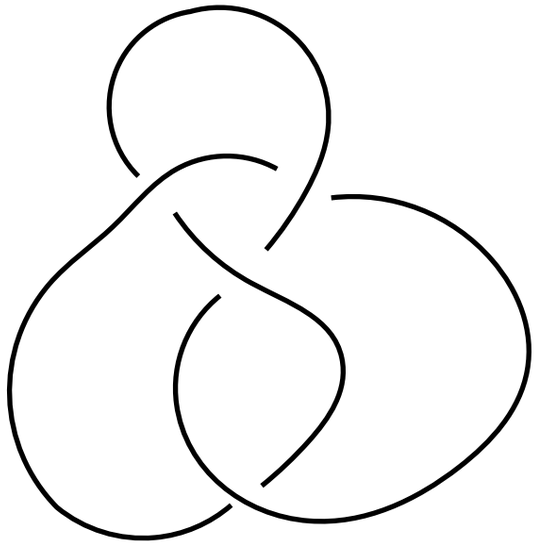
⇔TQFT/Chern-Simons theory [Witten89]

⇔TQFT⇔量子計算 [Freedman-Kitaev-Larsen-Wang03]

⇔量子計算 [Aharonov-Jones-Landau08]



結び目(knot)

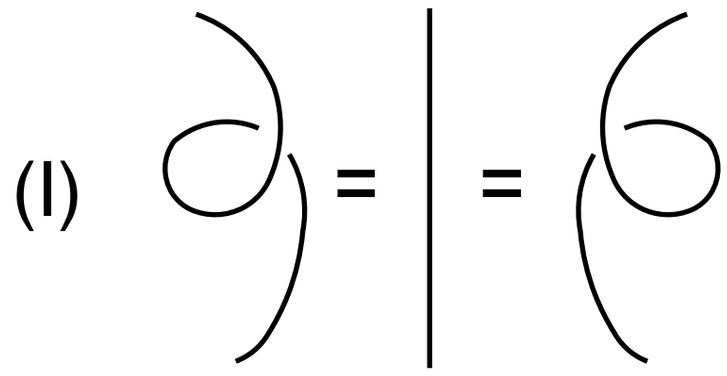


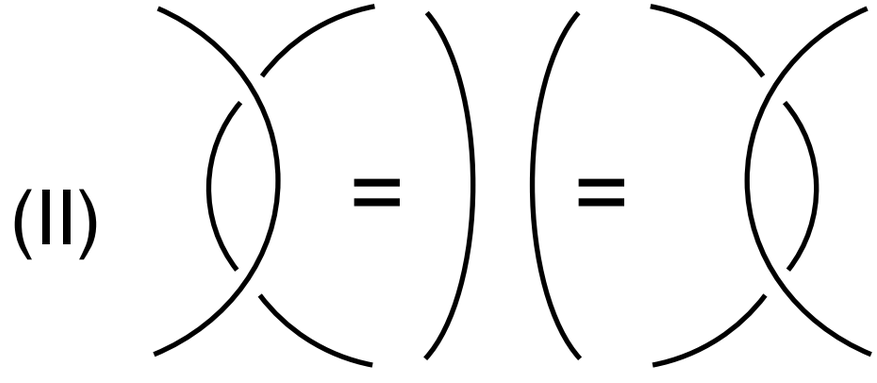
2次元での射影図

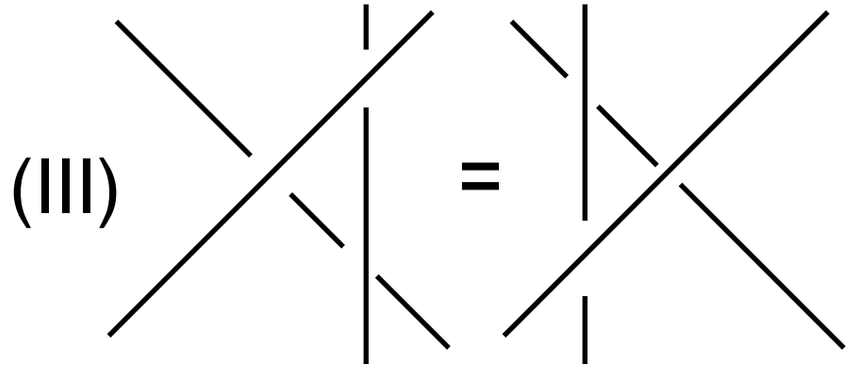
結び目の変形：

連続変形

Reidemeister変形





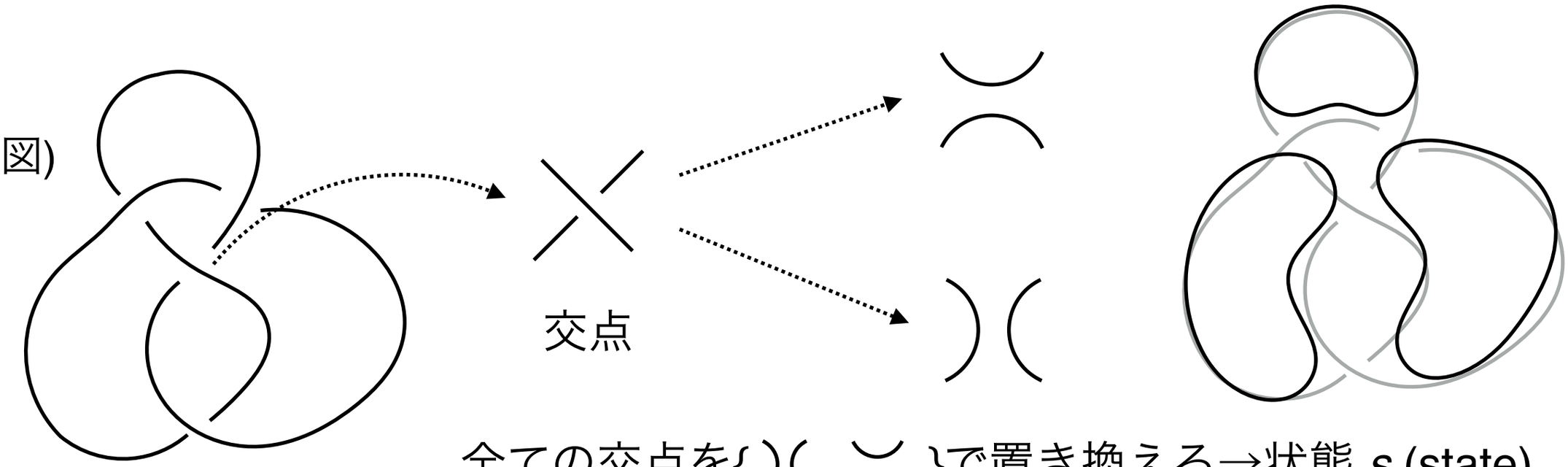


これらの変形に対して不変な量は？

Jones多項式

結び目L

(2次元射影図)



全ての交点を{)(, ⌒ }で置き換える→状態 s (state)

Kauffman多項式： $\langle L \rangle = \sum_s A^{s^+ - s^-} d^{|s|-1}$

s^+≡ ⌒ の数,　s^-≡)(の数,　|s|≡ループの数,　$d = -(A^2 + A^{-2})$

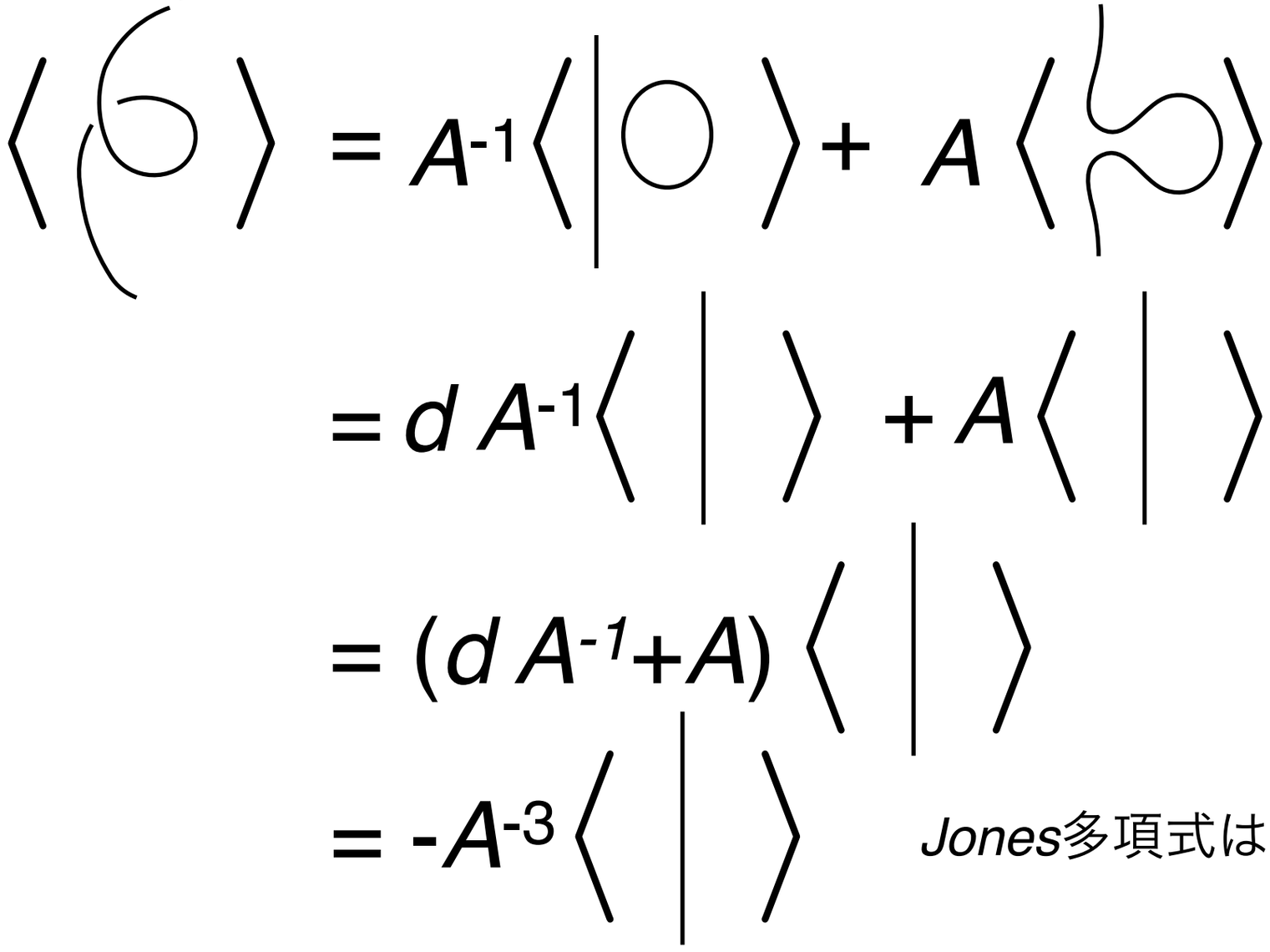
Jones多項式： $V_L(t) = (-A)^{3w(L)} \langle L \rangle \qquad t = A^{-4}$

$w(L)$≡(↗↘ の数) − (↘↗ の数)

ひねり数(writhe)

Jones多項式

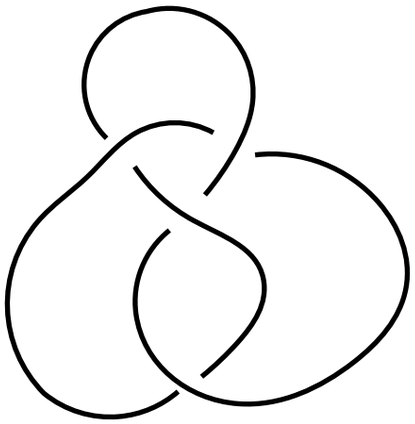
Kauffman多項式



*Jones*多項式は不変！

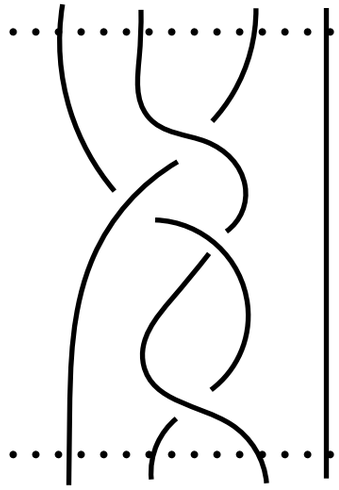
Reidemeister変形(II), (III)に対しても同様に不変である事が示せる.

結び目



閉包

ブレイド(組紐)群



ユニタリ表現
(Temperley-Lieb代数)

(2+1)-D non-Abelian
gauge theory &
non-Abelian anyon

万能性
(SU(2^N)で稠密)

不変量

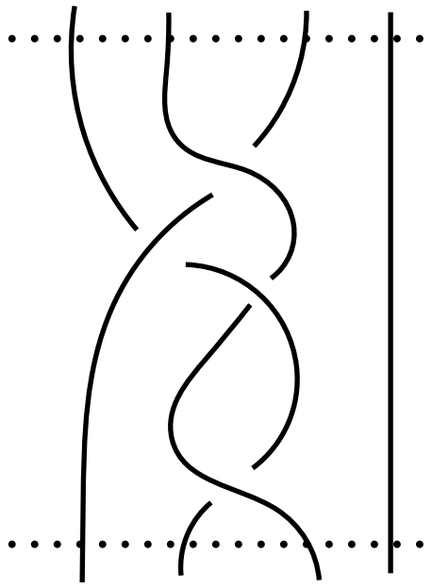
行列トレース

Jones多項式

量子計算

ブレイド群 B_n

ブレイド
（組紐）

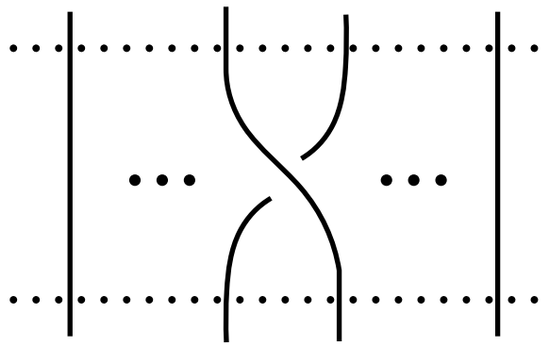


生成元 $\{\sigma_i\}$:

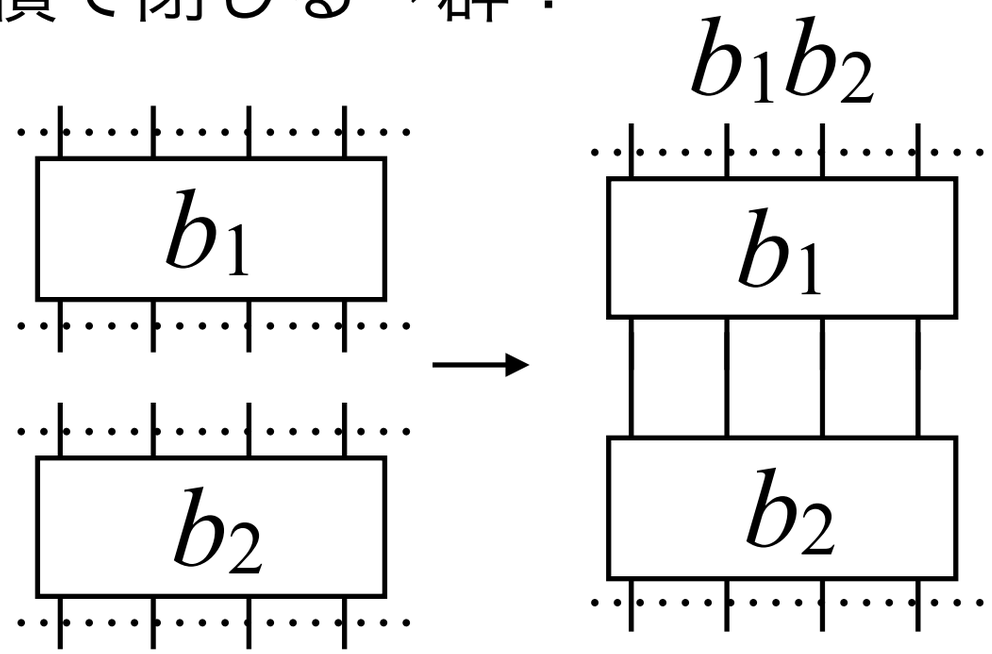
$$\sigma_i\sigma_j = \sigma_j\sigma_i \text{ for } |i-j| \geq 2$$

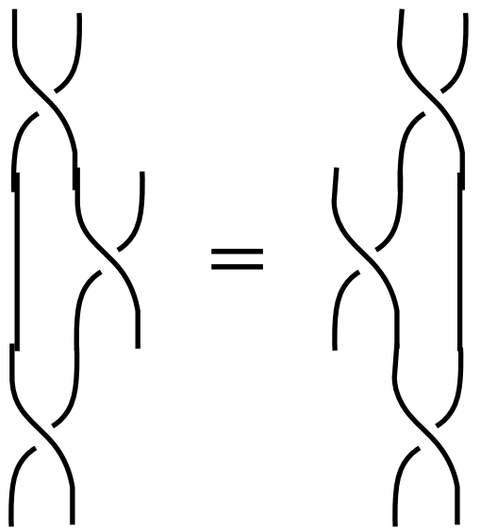
$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}.$$

$\sigma_i =$



積で閉じる→群：

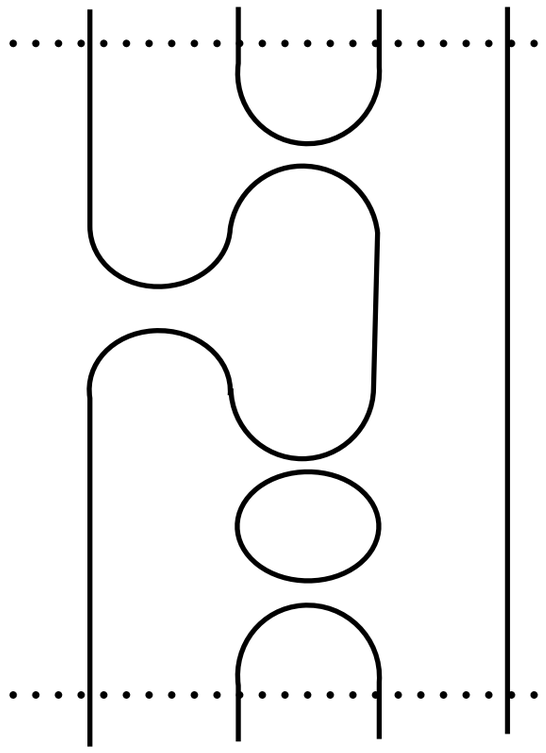




＝

変形(III)

Temperley-Lieb代数 $TL_n(d)$



タングル図

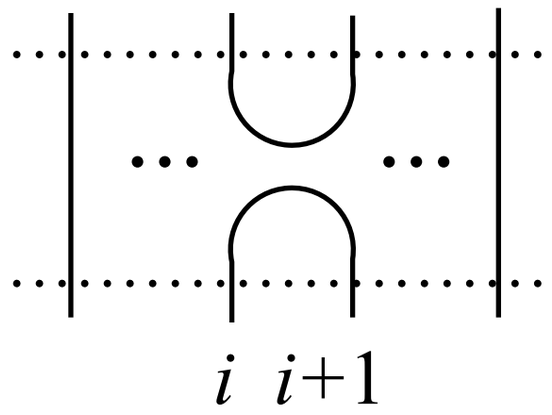
生成元$\{E_i\}$:

$$E_i E_j = E_j E_i \text{ for } |i-j| \geq 2,$$

$$E_i E_{i\pm 1} E_i = E_i,$$

$$E_i^2 = dE_i.$$

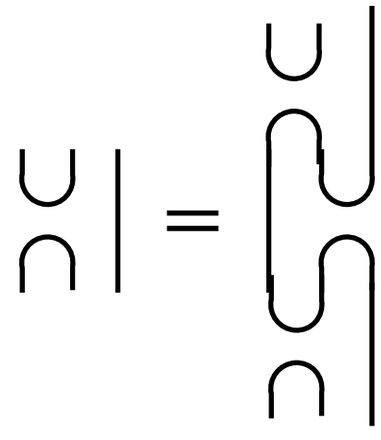
$E_i =$

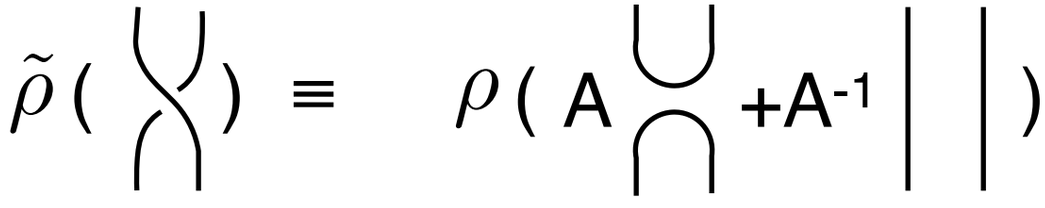


$$\tilde{\rho}(\sigma_i) \equiv A\rho(E_i) + A^{-1}I$$

↑

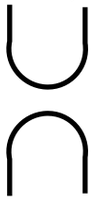
TL代数の表現



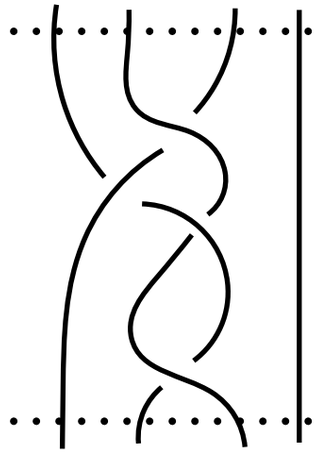
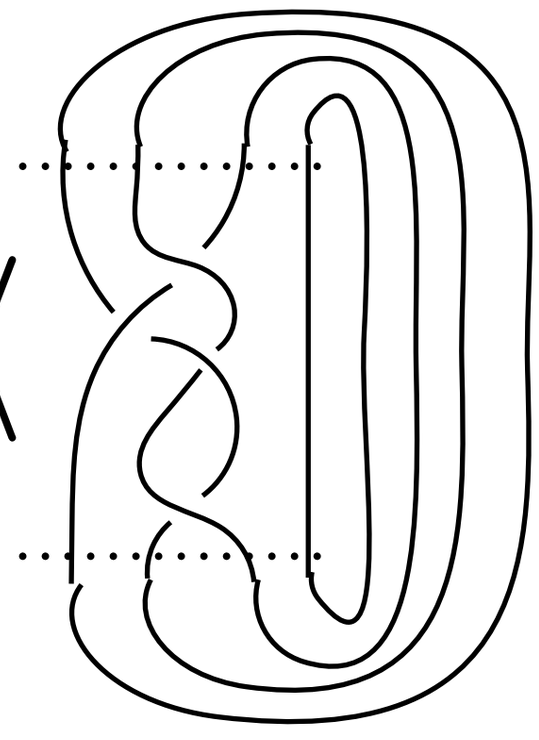


Jones多項式とブレイド群

$$\tilde{\rho}(\sigma_i) \equiv A\rho(E_i) + A^{-1}I$$

$\tilde{\rho}($  $) \equiv \rho($ A  +A^{-1} $)$

トレース閉包

$d^{n-1}\mathrm{Tr}[\tilde{\rho}($  $)] =$ $\langle$  $\rangle$

行列トレース

Kauffman
多項式

Jones多項式

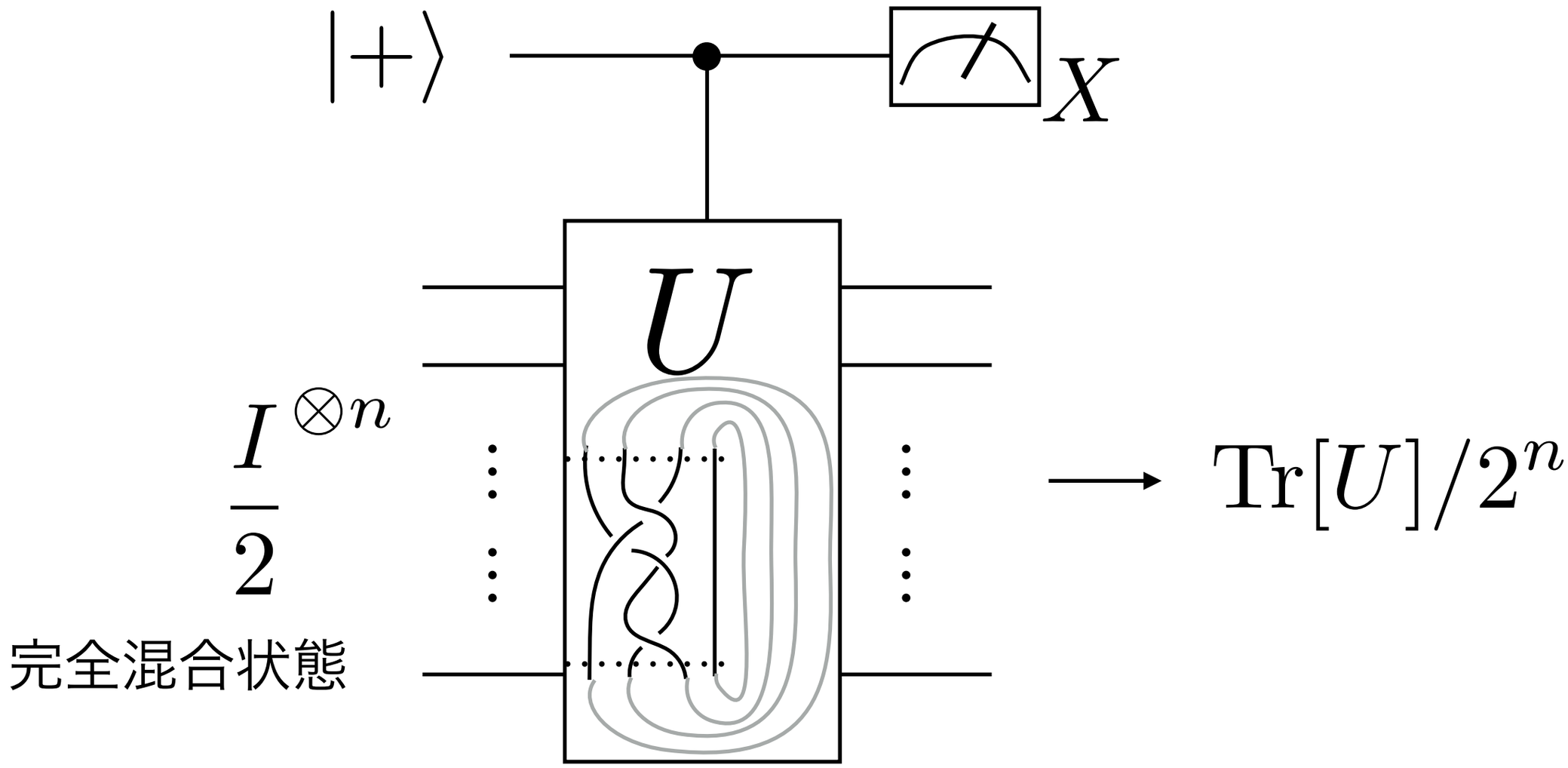
ブレイド群の表現のトレース

$$V_{b^{\mathrm{tr}}}(t) = (-A)^{3w(b^{tr})} d^{n-1}\mathrm{Tr}[\tilde{\rho}(b)]$$

Jones多項式と量子計算

Jones多項式　　ブレイド群の表現のトレース

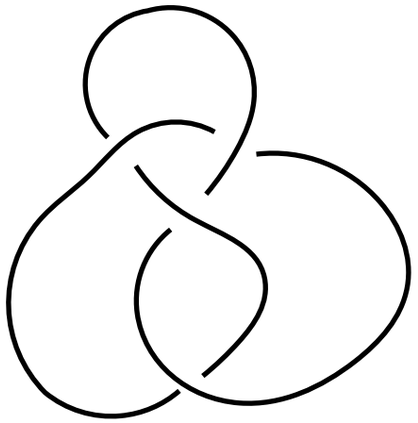
$$V_{b^{\mathrm{tr}}}(t) = (-A)^{3w(b^{tr})} d^{n-1} \mathrm{Tr}[\tilde{\rho}(b)]$$



完全混合状態

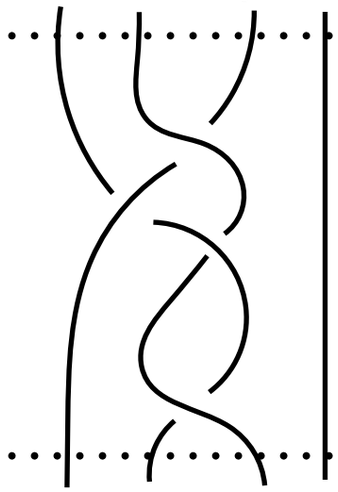
ブレイド群のユニタリ表現

結び目



閉包

ブレイド(組紐)群



(2+1)-D non-Abelian
gauge theory &
non-Abelian anyon

ユニタリ表現
(Temperley-Lieb代数)

path-model表現

万能性
(SU(2^N)で稠密)

不変量

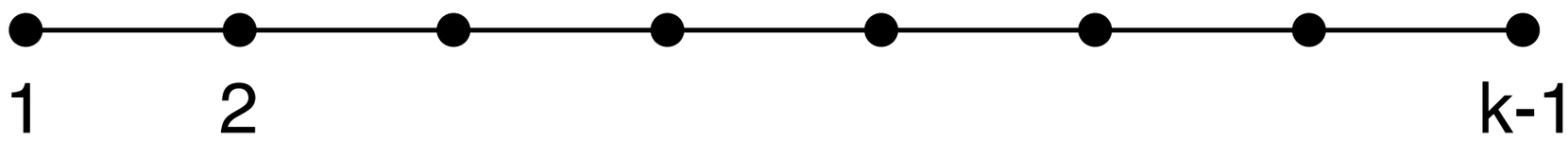
行列トレース

Jones多項式

量子計算

Path-model表現

1次元グラフ（*k*-1頂点）上の *n* ステップウォークを考える



path: *p*=1→2→1→2→3…..

左、右への移動によって0,1表示

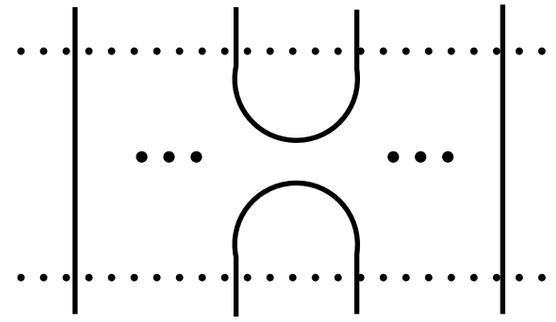
p= 1 0 1 1 …..

pathを基底として空間を構成→ $|p\rangle \in \mathcal{H}_{n,k}$

Path-model表現

$z_i \in \{1, ..., k-1\}$:ステップiの前にいた頂点

$$E_i =$$



$i \;\; i{+}1$

$$\rho(E_i)|...v_{i-1}00v_{i+2}...\rangle = 0,$$

$$\rho(E_i)|...v_{i-1}01v_{i+2}...\rangle = \frac{\lambda_{z_i-1}}{\lambda_{z_i}}|...v_{i-1}01v_{i+2}...\rangle + \frac{\sqrt{\lambda_{z_i+1}\lambda_{z_i-1}}}{\lambda_{z_i}}|...v_{i-1}10v_{i+2}...\rangle,$$

$$\rho(E_i)|...v_{i-1}10v_{i+2}...\rangle = \frac{\lambda_{z_i+1}}{\lambda_{z_i}}|...v_{i-1}10v_{i+2}...\rangle + \frac{\sqrt{\lambda_{z_i+1}\lambda_{z_i-1}}}{\lambda_{z_i}}|...v_{i-1}01v_{i+2}...\rangle,$$

$$\rho(E_i)|...v_{i-1}11v_{i+2}...\rangle = 0,$$

$$\lambda_j = \sin(j\pi/k) \quad A = ie^{-i\pi/(2k)} \quad d = 2\cos(\pi/k)$$

$(j = 1, ..., k-1)$

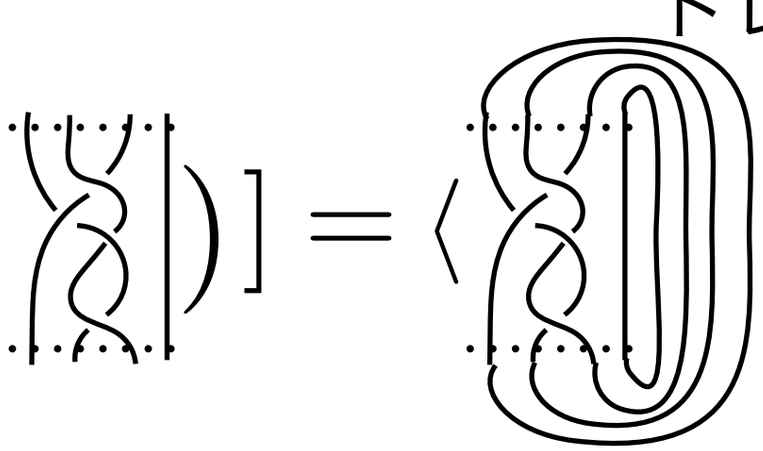
→ $\rho(E_i)$はエルミート、$\tilde{\rho}(\sigma_i)$ はユニタリ演算子

(SU(2) Chern-Simons level-(k-2) theory [Witten89])

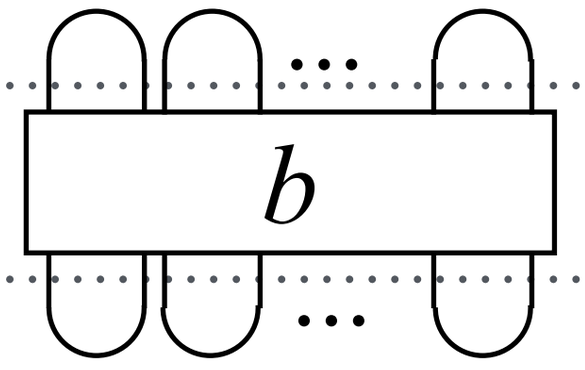
プラット閉包

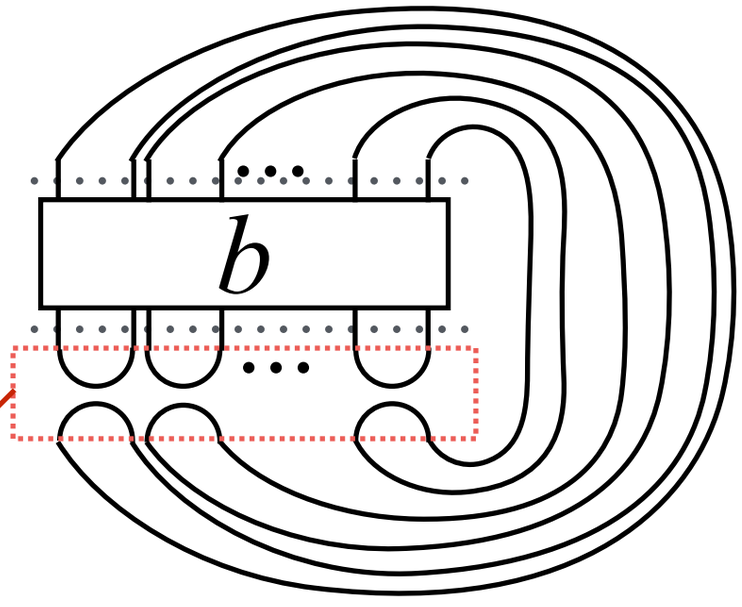
トレース閉包

$$d^{n-1}\,\mathrm{Tr}[\tilde{\rho}\,(\quad)\,] =$$



プラット閉包

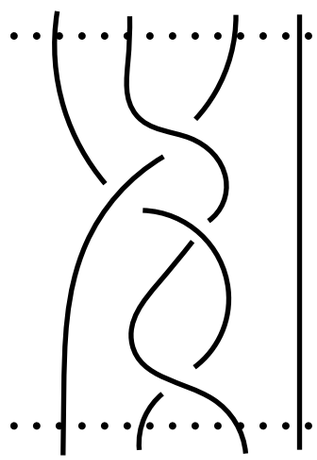
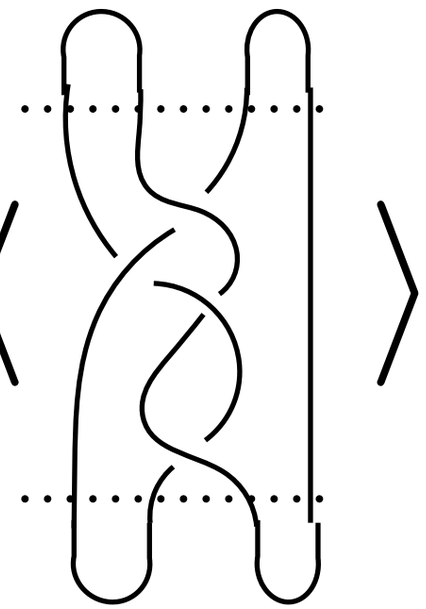




path $|p_0\rangle \equiv |1010\ldots10\rangle$ への射影演算子(定数倍)

Jones多項式と量子計算

プラット閉包

$$d^{n/2-1}\langle p_0|\tilde{\rho}($$  $$)|p_0\rangle =$$ 

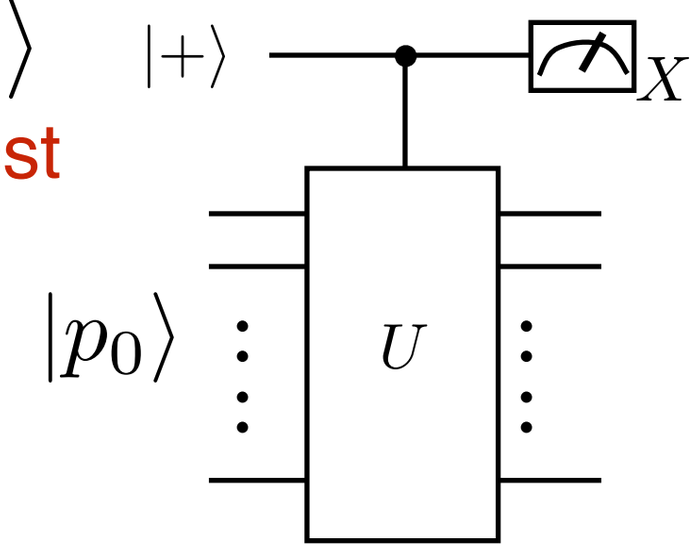
$$V_{b^{\mathrm{pr}}}(t) = (-A)^{3w(b^{\mathrm{pr}})} d^{n/2-1} \langle p_0|\tilde{\rho}(b)|p_0\rangle$$

Jones多項式　　Hadamard test

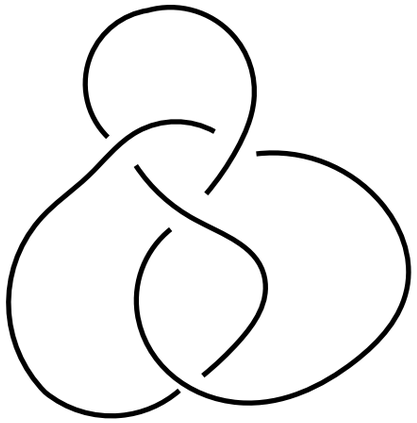
Jones多項式の$A = ie^{-i\pi/(2k)}$　(k>4, k≠6)

量子計算機をシミュレートできることも示せる.

（←4stepエンコーディング）

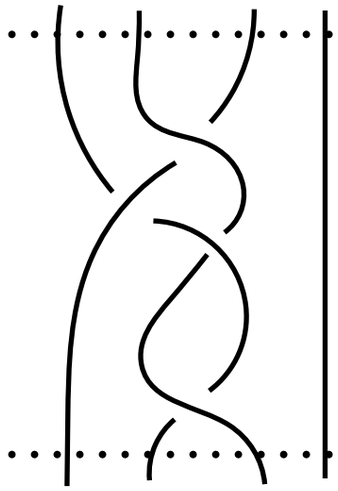


結び目



不変量

ブレイド(組紐)群



閉包

ユニタリ表現
(Temperley-Lieb代数)

path-model表現

行列トレース

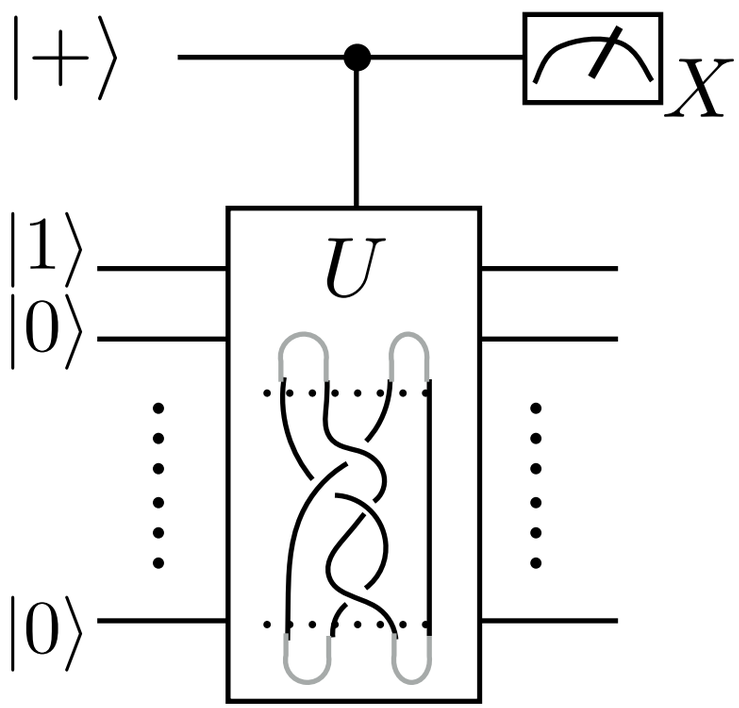
(2+1)-D non-Abelian
gauge theory &
non-Abelian anyon

$k>4,\ k\neq 6$

万能性
(SU(2^N)で稠密)

Jones多項式

量子計算



エンタングルメント・量子測定

量子情報・計算

量子誤り訂正

実現

量子暗号
の安全性

誤り耐性
量子計算

量子重力
(Ads/CFT)
吉田紅さんのセミナー

トイモデル

量子アルゴリズム

トポロジカル
量子計算

TQFT
(Jones多項式)

量子相
(トポロジカル秩序)

トイモデル

復号化問題

複雑性

統計力学
(スピングラス)

可解模型

レポート： Path-model表現

$z_i \in \{1, ..., k-1\}$:ステップiの前にいた頂点

↓ブレイド群の表現になっていることを示せ.

$$\tilde{\rho}(\sigma_i) \equiv A\rho(E_i) + A^{-1}I$$

↓TL代数の表現になっていることを示せ.

$$E_i = \quad i \;\; i{+}1$$

$$\begin{aligned}
\rho(E_i)|...v_{i-1}00v_{i+2}...\rangle &= 0, \\
\rho(E_i)|...v_{i-1}01v_{i+2}...\rangle &= \frac{\lambda_{z_i-1}}{\lambda_{z_i}}|...v_{i-1}01v_{i+2}...\rangle + \frac{\sqrt{\lambda_{z_i+1}\lambda_{z_i-1}}}{\lambda_{z_i}}|...v_{i-1}10v_{i+2}...\rangle, \\
\rho(E_i)|...v_{i-1}10v_{i+2}...\rangle &= \frac{\lambda_{z_i+1}}{\lambda_{z_i}}|...v_{i-1}10v_{i+2}...\rangle + \frac{\sqrt{\lambda_{z_i+1}\lambda_{z_i-1}}}{\lambda_{z_i}}|...v_{i-1}01v_{i+2}...\rangle, \\
\rho(E_i)|...v_{i-1}11v_{i+2}...\rangle &= 0,
\end{aligned}$$

$$\lambda_j = \sin(j\pi/k) \quad A = ie^{-i\pi/(2k)} \quad d = 2\cos(\pi/k)$$

$$(\, j = 1, ..., k-1 \,)$$

→ $\rho(E_i)$はエルミート、$\tilde{\rho}(\sigma_i)$はユニタリ演算子←示せ.