2025-07-28 量子ソフトウェアハンズオン: 量子コンピュータの誤り訂正の基礎

量子誤り訂正とは？

What is Quantum Error Correction?

Synge Todo / 藤堂眞治

Department of Phys., UTokyo / 東京大学大学院理学系研究科

Outline

- なぜ誤り訂正が必要なのか？
  - 古典コンピュータにおけるエラー
  - 量子コンピュータにおけるエラー
- 古典誤り訂正
  - ビット反転エラー
  - 3ビット反復符号
  - エラーシンドローム
- 量子誤り訂正
  - 量子反復符号?
  - シンドローム測定
  - 9量子ビットショア符号
- スタビライザ形式
  - スタビライザ表現
  - スタビライザ符号
  - 7量子ビットスティーン符号
- 量子ゲートテレポーテーション
- 発展した話題
- 参考文献
  - M. A. Nielsen and I. L. Chuang, “Quantum Computation and Quantum Information”（Cambridge University Press, 2010）
  - S. J. Devitt et al, Rep. Prog. Phys. 76 076001 (2013)

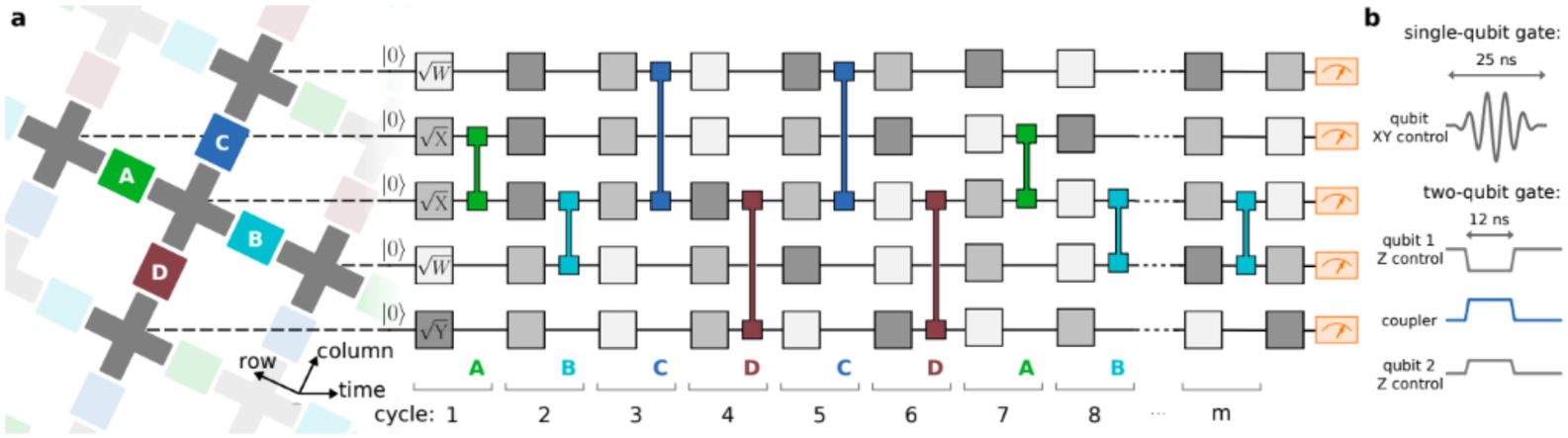
なぜ誤り訂正が必要なのか？

古典コンピュータにおけるエラー

- 我々が普段使っているPC（＝古典コンピュータ）の中でも多くのエラーが発生している
- エラーの原因
  - リーク電流、宇宙線など
- 古典コンピュータでにはさまざまな誤り検出・訂正の仕組みが実装されている
  - パリティーチェックビット
  - 反復符号
  - ECCメモリ
- 誤り訂正により、ユーザはあたかもエラーのない「理想的な」コンピュータかのようにPCを使うことができている

量子コンピュータにおけるエラー

- 量子コンピュータにおいてももさまざまなエラーの要因がある
  - 熱雑音、イオンや光子の消失...
  - 励起状態の効果（量子ビットは純粋な $|0\rangle$ と $|1\rangle$ の2準位系ではない）
  - 系統的なエラー（量子ビット操作におけるパルス長などの「本来あるべき値」からのズレ）
- 量子の重ね合わせ状態は「デジタル」ではなく連続的な状態を取りうる「アナログ」ビット
  - 古典コンピュータよりエラーに弱い？
- 量子コンピュータにおいて、誤り訂正は可能か？



Arute, Arya, Babbush, et al. Nature 574, 505 (2019)

量子コンピュータにおけるエラー

- ビット反転
  - 量子ビットが $|0\rangle$ から $|1\rangle$ へ、あるいは逆へ反転

$$X|0\rangle = |1\rangle$$
$$X|1\rangle = |0\rangle$$

$$X(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle$$

- 位相反転
  - 量子ビットの位相(符号)が反転

$$Z|0\rangle = |0\rangle$$
$$Z|1\rangle = -|1\rangle$$

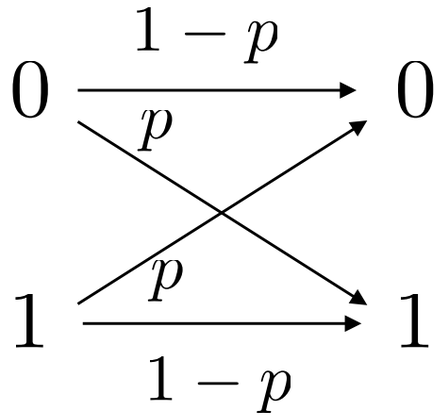
$$Z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$$

- 脱分極(Depolarization)
  - 量子ビットの状態が完全混合状態に置き換わる
- 振幅減衰(Amplitude Damping)
  - エネルギー散逸の効果

古典誤り訂正

ビット反転エラー

・ビット反転エラーが確率 p で発生するとする（$0 \leq p \leq 0.5$）



・このチャンネルを通して古典情報（ビット）を送信すると、受信者は確率 p で間違った（反転した）ビットを受け取る

・いかにして、エラーを検出し、エラーから情報を守るか？

・冗長化戦略: 複数のビットを用いて情報を「符号化（encode）」し、受け取った側で「復号化（decode）する

3ビット反復符号(Repetition Code)

・情報(0 あるいは 1)を3ビットを用いて符号化する

$$0 \to 000$$

$$1 \to 111$$

・000 と 111 をそれぞれ「論理 0 (logical 0)」あるいは「論理 1 (logical 1)」と呼ぶ

・受信者は 000, 001, 010, 011, 100, 101, 110, あるいは 111 を受け取る

・多数決を使って復号

$$\begin{matrix} 000 \\ 001 \\ 010 \\ 100 \end{matrix} \to 0, \qquad \begin{matrix} 111 \\ 110 \\ 101 \\ 011 \end{matrix} \to 1$$

・注: 復号の前に全てのビットを「測定」している

3ビット反復符号の誤り率

$$\begin{matrix}000\\001\\010\\100\end{matrix} \rightarrow 0, \qquad \begin{matrix}111\\110\\101\\011\end{matrix} \rightarrow 1$$

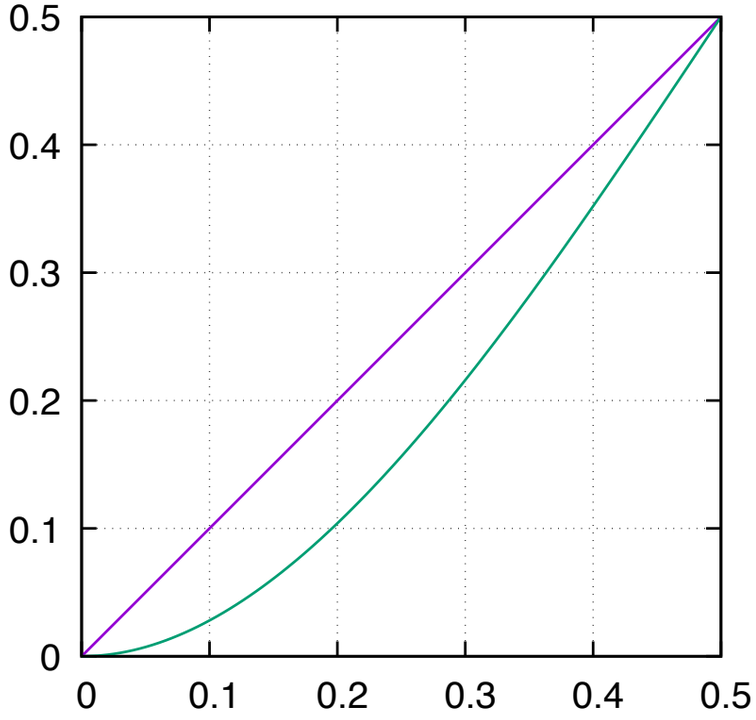
・1ビット反転の場合、必ず元の情報を復元できる

・2ビット以上の反転が起こる確率

$$p_3 = 3p^2(1-p) + p^3$$

- p_3 は p より小さくなる
- $p = 0.1 \rightarrow p_3 = 0.028 < p$

・複数のビットを使うことで誤り率を減らすことができる



5ビット反復符号

・1ビット反転あるいは2ビット反転の場合、元の情報を復元できる

・3ビット以上の反転が起こる確率

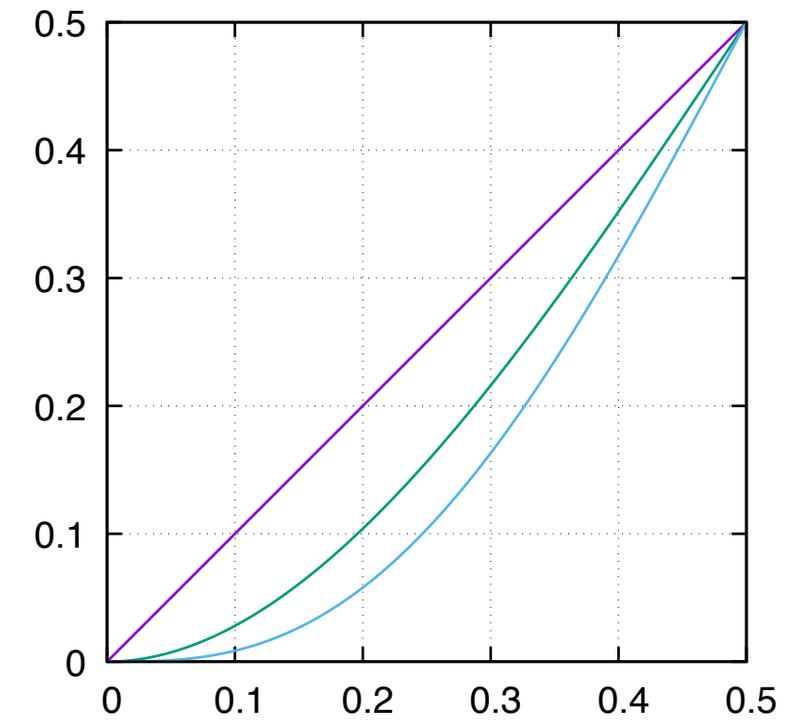
$$p_5 = 10p^3(1-p)^2 + 5p^4(1-p) + p^5$$

- p_5 はさらに小さくなる
- $p = 0.1 \rightarrow p_5 = 0.00856 < p_3 = 0.028 < p$

・d ビット反復符号の誤り率

- $\lfloor d/2 \rfloor$以下のビット反転の場合、元の情報を復元できる
- d を大きくするほど誤り率を減らすことができる

・論理0と論理1が何ビット離れているか(今の場合 d)を「符号距離」と呼ぶ



量子誤り訂正

量子反復符号？

- 古典誤り訂正と同じ戦略で誤り訂正は可能か？
- 古典の反復符号はそのままでは量子には使えない
  - 量子状態は複製できない
    - 任意の量子状態の複製を作る（$|\Psi\rangle \rightarrow |\Psi\rangle \otimes |\Psi\rangle \otimes |\Psi\rangle$）量子回路は存在しない
    - 「量子複製不可能定理（no-cloning theorem）」
  - 復号化の過程で量子ビットを測定すると「重ね合わせ」が破壊される
  - 量子状態や量子エラーは連続的

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

- → $|\Psi\rangle$ を複製するのではなく、基底（$|0\rangle$ と $|1\rangle$）に反復のアイデアを導入する

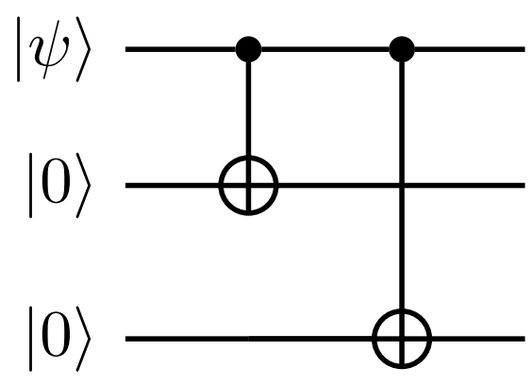
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle$$

符号化のための量子回路

・量子重ね合わせ状態を3量子ビット状態に符号化

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle$$

・次の量子回路により符号化できる



・それぞれの基底が以下のように変換されることは明らか

$$|0\rangle \rightarrow |000\rangle$$
$$|1\rangle \rightarrow |111\rangle$$

・線形変換なので、重ね合わせ状態も重ね合わせ状態に変換される

量子反復符号？

- 古典誤り訂正と同じ戦略で誤り訂正は可能か？
- 古典の反復符号はそのままでは量子には使えない
  - 量子状態は複製できない
    - 任意の量子状態の複製を作る（$|\Psi\rangle \rightarrow |\Psi\rangle \otimes |\Psi\rangle \otimes |\Psi\rangle$）量子回路は存在しない
    - 「量子複製不可能定理（no-cloning theorem）」
  - 復号化の過程で量子ビットを測定すると「重ね合わせ」が破壊される
  - 量子状態や量子エラーは連続的

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

- $|\Psi\rangle$ を複製するのではなく、基底（$|0\rangle$ と $|1\rangle$）に反復のアイデアを導入する

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle$$

エラーシンドローム(Error Syndrome)

・全てのビットの状態を知らなくても、ビットペア(1,2)と(1,3)のビット積(パリティ)が分かればエラーの発生箇所は特定可能 (=エラーシンドローム)

	P_{12}	P_{13}	error
000	0	0	none
001	0	1	3
010	1	0	2
100	1	1	1

	P_{12}	P_{13}	error
111	0	0	none
110	0	1	3
101	1	0	2
011	1	1	1

・論理0、論理1の場合どちらも同じテーブルが使える！

・シンドロームの値さえわかれば、エラーの発生箇所の特定と修正が可能

ビット反転エラー

- 1番目の量子ビットに1量子ビット反転が起こった場合を考える

$$\alpha|000\rangle + \beta|111\rangle \rightarrow \alpha|100\rangle + \beta|011\rangle$$

- 復号化の過程で量子ビットを測定すると「重ね合わせ」が破壊される
  - 1番目の量子ビットを測定すると、確率 $|\alpha|^2$ で測定結果は 1、確率 $|\beta|^2$ で 0
  - 測定後の状態はそれぞれ $|100\rangle$ か $|011\rangle$ となる
  - 測定後はもはや重ね合わせではない！

- 1番目と2番目の量子ビットを同時に測定すると？ 「シンドローム測定」
  - 測定結果は常に 1
  - 測定後の状態は変化しない！

- 1番目と3番目の量子ビットを同時に測定するとこちらも結果は 1
  - 1番目の量子ビットにエラーが起こっていることが分かる → Xゲートを掛ければ修正できる

ビット反転エラー

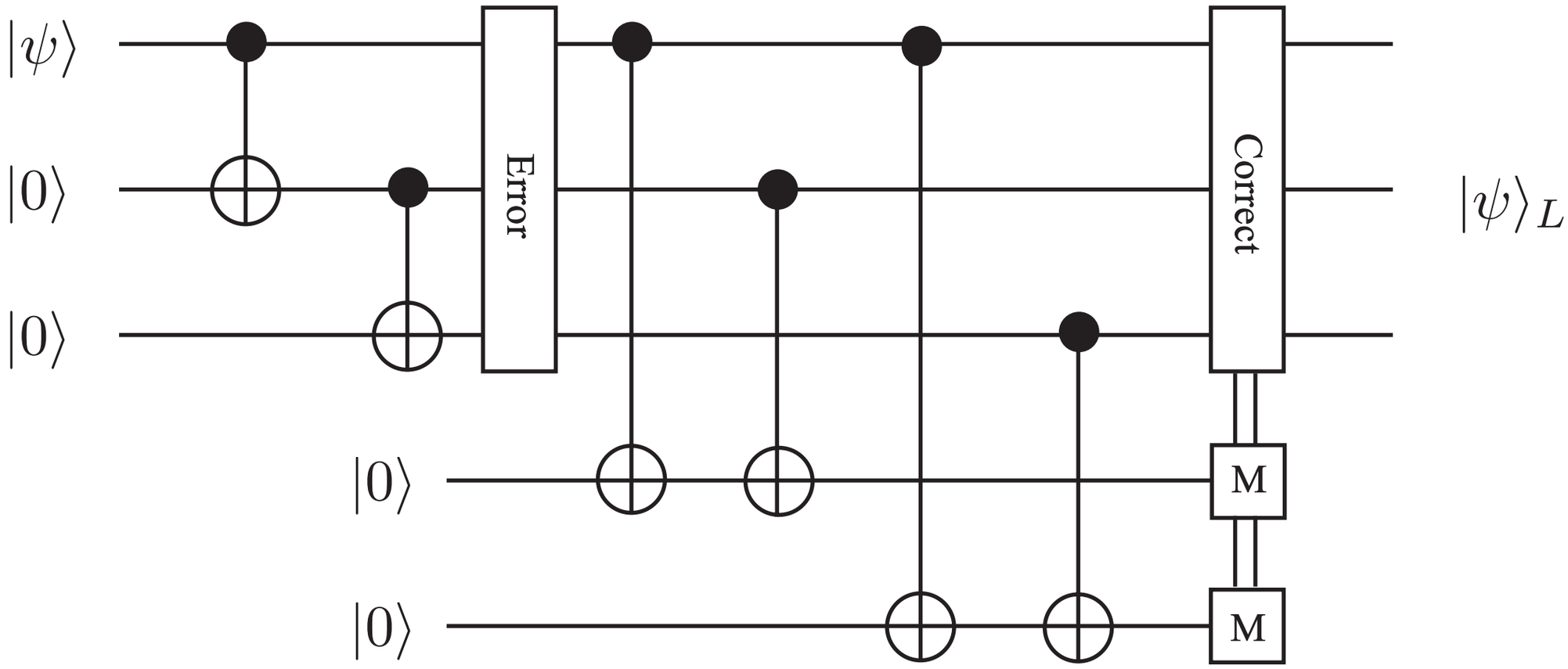
- 符号化された状態　$\alpha|000\rangle + \beta|111\rangle$　は $|000\rangle$ と $|111\rangle$ で張られる部分空間内にある（符号空間 Code Space）
- ビット反転エラー
  - ビット反転(X)が各量子ビットに確率 p で独立に起こるとする
- 1番目の量子ビットに1量子ビット反転が起こると？

$$\alpha|000\rangle + \beta|111\rangle \rightarrow \alpha|100\rangle + \beta|011\rangle$$

- 状態は符号空間から飛び出す
- エラーの発生位置により異なった部分空間(それぞれ互いに直交)に移る

$$\begin{aligned}
\text{No bit flips:} &\quad \text{Span}\{|000\rangle, |111\rangle\} \\
\text{Bit flip on qubit 1:} &\quad \text{Span}\{|100\rangle, |011\rangle\} \\
\text{Bit flip on qubit 2:} &\quad \text{Span}\{|010\rangle, |101\rangle\} \\
\text{Bit flip on qubit 3:} &\quad \text{Span}\{|001\rangle, |110\rangle\}
\end{aligned}$$

シンドローム測定によるビット反転誤り訂正

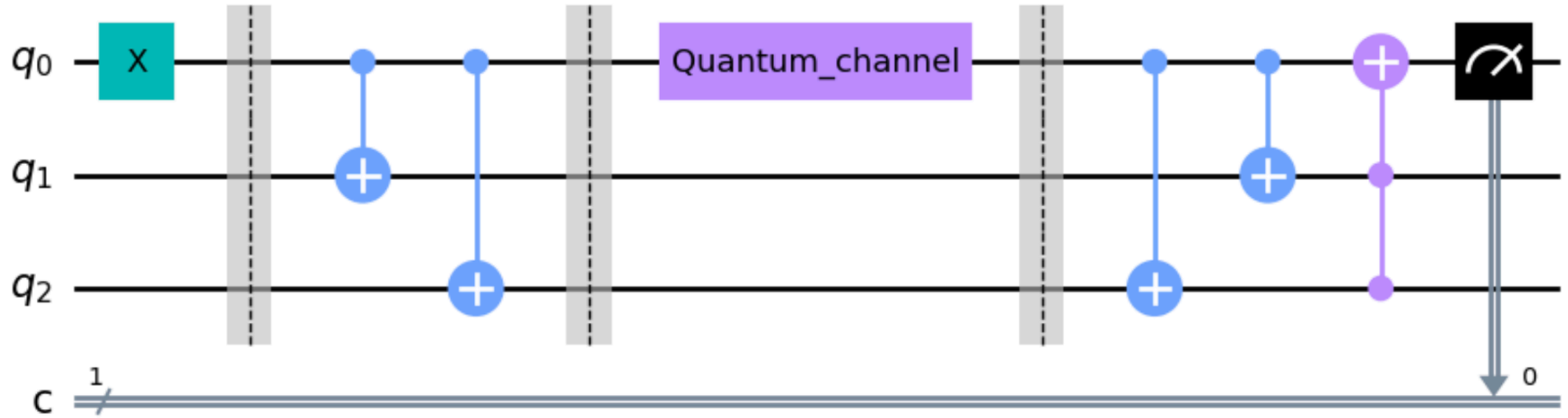


- アンシラの測定結果が
  - (0,0) → エラーなし
  - (1,0) → qubit 2にエラー
  - (0,1) → qubit 3にエラー
  - (1,1) → qubit 1にエラー

$$\alpha|0\rangle+\beta|1\rangle \rightarrow \alpha|000\rangle|00\rangle+\beta|111\rangle|00\rangle$$
$$\rightarrow \alpha|100\rangle|00\rangle+\beta|011\rangle|00\rangle$$
$$\rightarrow \alpha|100\rangle|11\rangle+\beta|011\rangle|11\rangle$$

シンドローム測定によるビット反転誤り訂正

- 誤り訂正直後に最終結果の測定(or 復号)を行うのであれば、アンシラを使う代わりにqubit 2と3を使ってもよい
  - → 演習での例



$$\alpha|0\rangle+\beta|1\rangle \rightarrow \alpha|000\rangle+\beta|111\rangle$$
$$\rightarrow \alpha|100\rangle+\beta|011\rangle$$
$$\rightarrow \alpha|011\rangle+\beta|111\rangle$$

位相反転

- ビット反転は古典エラーと類似
  - それ以外のエラーを訂正できるか？
- 位相反転
  - 位相反転(Z)がそれぞれのビットに確率 p で独立に生じる

$$Z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$$

- 位相反転エラーは、|+> と |-> の状態に対するビット反転エラーと等価であることに着目すると、ビット反転の場合と同様にエラー訂正可能

$$Z|+\rangle = |-\rangle$$
$$Z|-\rangle = |+\rangle$$

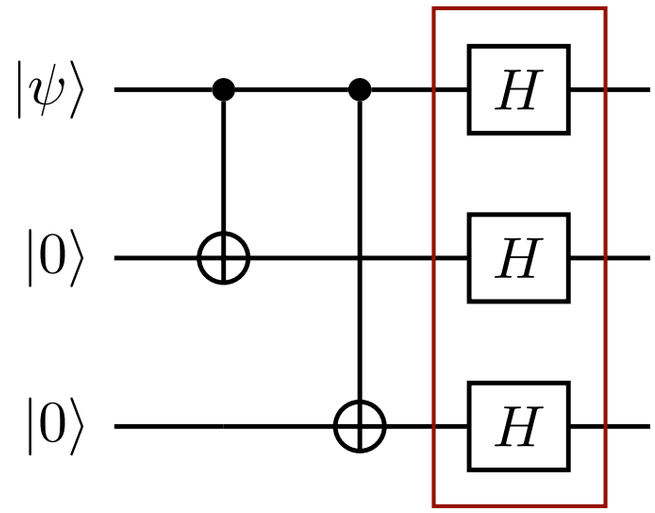
$$|+\rangle \equiv \frac{|0\rangle + |1\rangle}{\sqrt{2}}, |-\rangle \equiv \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

位相反転エラーに対する3量子ビット符号

・量子状態を次のように符号化する

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

・次のような回路で符号化できる



・シンドローム測定と誤り訂正

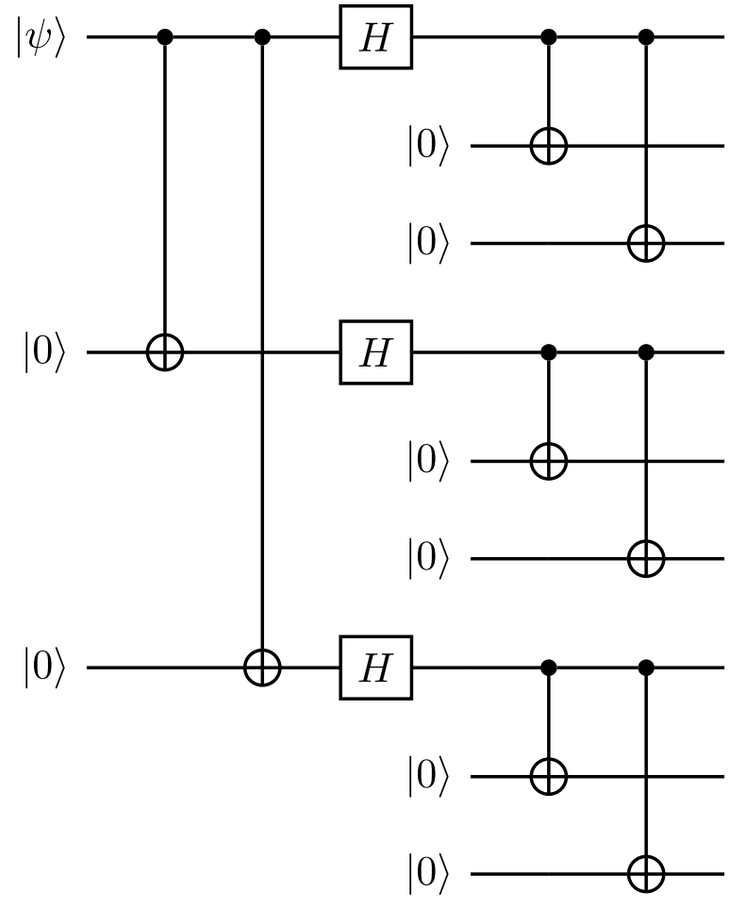
・ビット反転の場合の $|0\rangle$, $|1\rangle$, X を $|+\rangle$, $|-\rangle$, Z で置き換えればOK

9量子ビットショア符号（9-qubit Shor Code）

- 任意の1量子ビットエラーを訂正できる
  - ビット反転のための3量子ビット符号と位相反転のための3量子ビット符号を組み合わせる

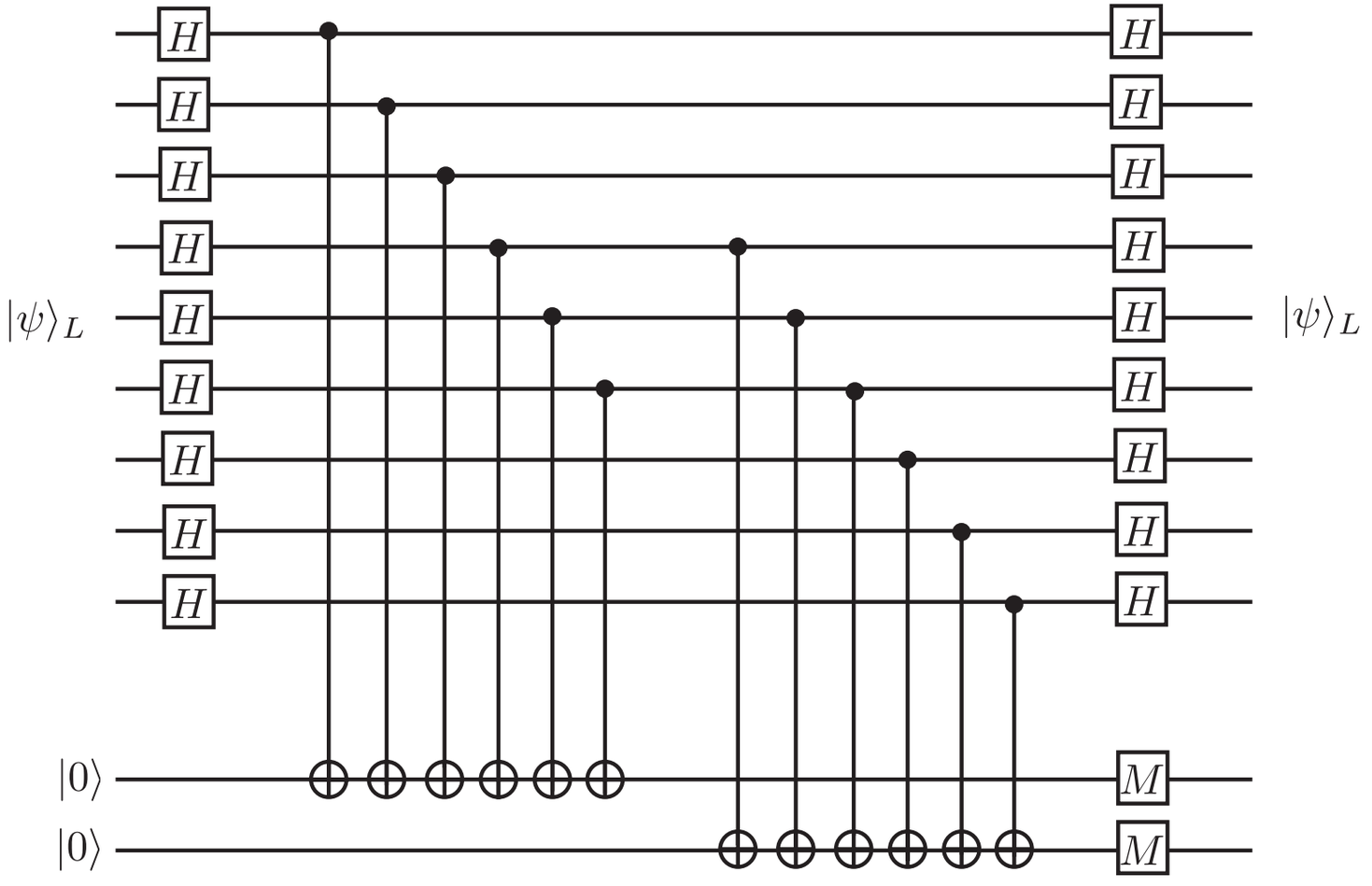
$$|0\rangle \to |+++\rangle \quad \to \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$|1\rangle \to |---\rangle \quad \to \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$$



9量子ビットショア符号（9-qubit Shor Code）

- ビット反転エラー
  - それぞれの3量子ビットブロック内で訂正可能
- 位相反転エラー
  - ブロック間の位相差を測定して訂正
  - 位相反転エラーのためのシンドローム測定



スタビライザ形式

スタビライザ表現

- 量子状態を基底の「線型結合の係数」で表すかわりに、「演算子の組」で表す
- N 量子ビット系について
  - ビット毎のパウリ演算子(I, X, Y, Z)と符号±の積を考える（エルミートでユニタリーなパウリ群の元）
  - 例: $IIXX, XYZZ, -YIZZ$
  - 全てエルミートかつユニタリー → 固有値は±1のみ
- これらの演算子は互いに交換、あるいは反交換
  - 全部で 2×4^N 種類の演算子の中から、可換で独立なものを N 個選ぶことができる(スタビライザ生成元、スタビライザ)
  - 全ての固有値が+1の同時固有状態 → 状態が一つ定まる(スタビライザ状態)
- 例
  - $|0\rangle$: Zのスタビライザ状態
  - $\mathrm{GHZ}_3 = \dfrac{|000\rangle + |111\rangle}{\sqrt{2}}$: $K_1 = XXX, K_2 = ZZI, K_3 = IZZ$のスタビライザ状態
- シュレディンガー形式 ⇔ ハイゼンベルグ形式

スタビライザ符号

- N 量子ビットに対して、$N-1$ 個のスタビライザを考える
  - $2^{N-(N-1)}$ = 2次元のスタビライザ部分空間(=符号空間)を定めることができる
- 例(3量子ビット):
  - 2つのスタビライザ(ZZIとIZZ)を考えると
  - スタビライザ部分空間: $\alpha|000\rangle + \beta|111\rangle$
- 全てのスタビライザと可換で独立なもう一つのパウリ群の演算子を考えると、その±1の固有状態として論理0と論理1が定義できる → 論理Z演算子($\bar{Z}$)
- 例(3量子ビット):
  - $\bar{Z} = ZZZ \Rightarrow |0\rangle_{\mathrm{L}} \equiv |000\rangle, |1\rangle_{\mathrm{L}} \equiv |111\rangle$
  - $\bar{Z}|0\rangle_{\mathrm{L}} = |0\rangle_{\mathrm{L}}$
  - $\bar{Z}|1\rangle_{\mathrm{L}} = -|1\rangle_{\mathrm{L}}$

スタビライザ符号

- $\bar{Z}$ (論理Z)と反可換で、他のスタビライザ生成元と交換する、もう一つのパウリ群の演算子を導入 → 論理X演算子($\bar{X}$)
  - $\bar{Z}\bar{X}|0\rangle_{\mathrm{L}} = -\bar{X}\bar{Z}|0\rangle_{\mathrm{L}} = -\bar{X}|0\rangle_{\mathrm{L}} \equiv |1\rangle_{\mathrm{L}}$
- 例(3量子ビット):
  - $\bar{X} = XXX$
  - $\bar{X}|0\rangle_{\mathrm{L}} = XXX|000\rangle = |111\rangle = |1\rangle_{\mathrm{L}}$
  - $\bar{X}|1\rangle_{\mathrm{L}} = XXX|111\rangle = |000\rangle = |0\rangle_{\mathrm{L}}$

- 誤り検出・訂正もスタビライザに関する射影測定(=シンドローム測定)で行える

9量子ビットショア符号（9-qubit Shor Code）

- 9量子ビットで1つの論理量子ビットを符号化
  - 9-1 = 8個のスタビライザ

K^1	Z	Z	I	I	I	I	I	I	I
K^2	Z	I	Z	I	I	I	I	I	I
K^3	I	I	I	Z	Z	I	I	I	I
K^4	I	I	I	Z	I	Z	I	I	I
K^5	I	I	I	I	I	I	Z	Z	I
K^6	I	I	I	I	I	I	Z	I	Z
K^7	X	X	X	X	X	X	I	I	I
K^8	X	X	X	I	I	I	X	X	X

- 論理 Z と論理 X
  - $\bar{Z} = XXXXXXXXX$
  - $\bar{X} = ZZZZZZZZZ$

7量子ビットスティーン符号（7-qubit Steane Code）

- 7量子ビットで1つの論理量子ビットを符号化
  - 7-1 = 6個のスタビライザ

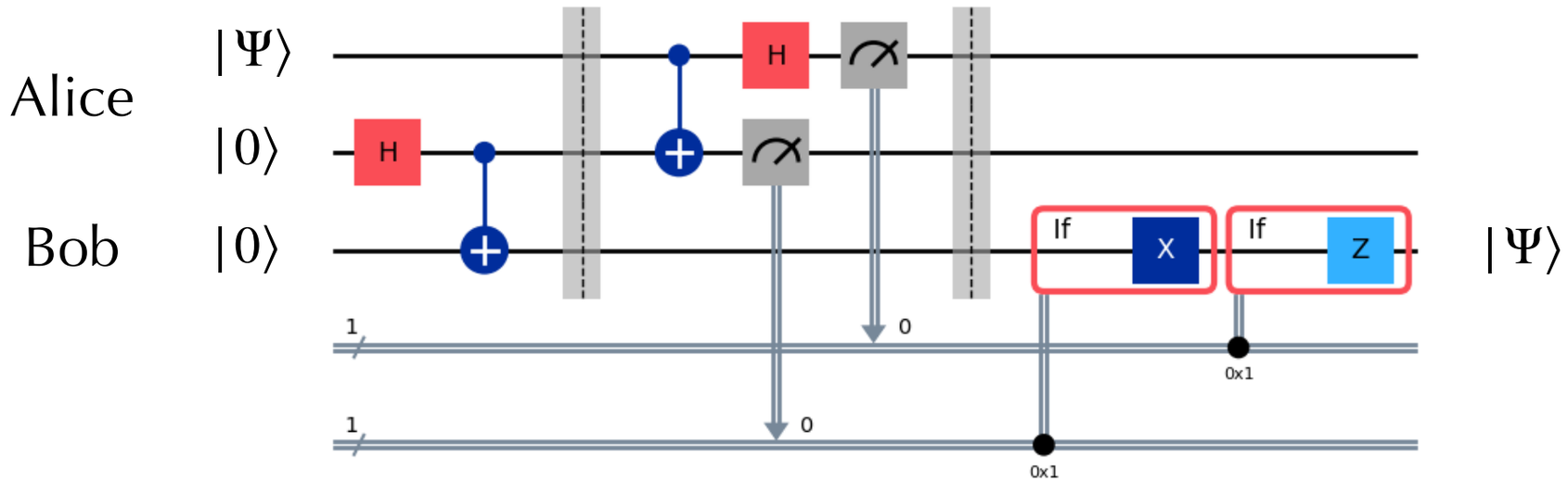
$$K^1 = IIIXXXX, \qquad K^2 = XIXIXIX,$$
$$K^3 = IXXIIXX, \qquad K^4 = IIIZZZZ,$$
$$K^5 = ZIZIZIZ, \qquad K^6 = IZZIIZZ.$$

- 論理 Z と論理 X
  - $\bar{Z} = ZZZZZZZ$
  - $\bar{X} = XXXXXXX$
- 論理0と論理1
  - $|0\rangle_{\mathrm{L}} \sim (I+\bar{Z})\prod_i (I+K^i)\,|0000000\rangle \sim \frac{1}{\sqrt{8}}(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle),$
  - $|1\rangle_{\mathrm{L}} \sim (I-\bar{Z})\prod_i (I+K^i)\,|0000000\rangle \sim \frac{1}{\sqrt{8}}(|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle).$

量子ゲートテレポーテーション

量子ゲートテレポーテーション

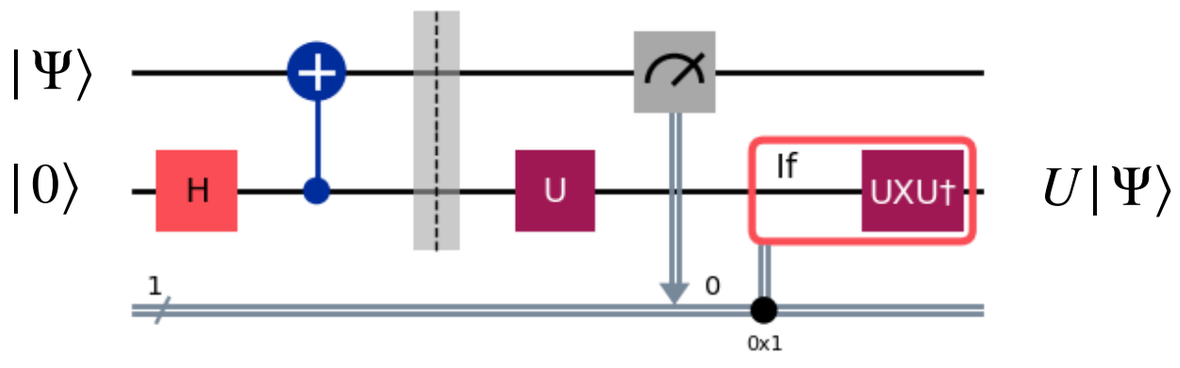
- 量子テレポーテーション（Quantum Teleportation）
  - 量子もつれ(ベル状態)と古典通信を組み合わせて、量子ビットの状態を転送する技術



- 量子ゲートテレポーテーション（Quatum Gate Teleportation）
  - 量子状態そのものを転送するのではなく、ある量子ゲート(操作)を、間接的に別の量子ビットに作用
  - 直接作用させるのが困難な操作も、間接的に実行可能

量子ゲートテレポーテーション

- 量子ゲートテレポーテーション（Quatum Gate Teleportation）
  - 量子状態そのものを転送するのではなく、ある量子ゲート（操作）を、間接的に別の量子ビットに作用



- $|0\rangle \otimes |0\rangle$ ではなく $|\Psi\rangle \otimes |0\rangle$ にベル回路を適用すると

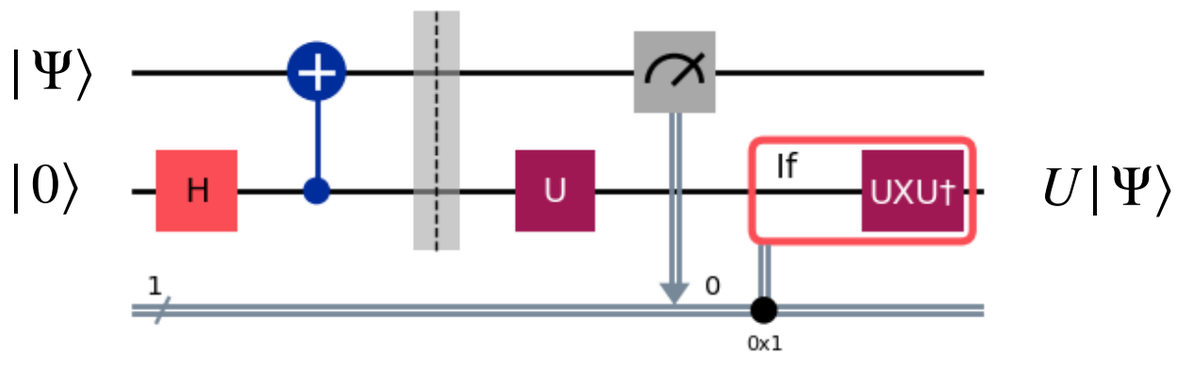
$$|\Psi\rangle \otimes |0\rangle \rightarrow |\Psi\rangle \otimes (\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = (a|0\rangle + b|1\rangle) \otimes (\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$= \frac{1}{\sqrt{2}}(a|00\rangle + a|01\rangle + b|10\rangle + b|11\rangle)$$

$$\rightarrow \frac{1}{\sqrt{2}}(a|00\rangle + a|11\rangle + b|10\rangle + b|01\rangle) = \frac{1}{\sqrt{2}}(|0\rangle \otimes |\Psi\rangle + |1\rangle \otimes X|\Psi\rangle)$$

量子ゲートテレポーテーション

- 量子ゲートテレポーテーション（Quatum Gate Teleportation）
  - 量子状態そのものを転送するのではなく、ある量子ゲート（操作）を、間接的に別の量子ビットに作用



- 補助ビットに U を作用

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

- 1ビット目を測定して、結果が 1 なら補助ビットに $UXU^{\dagger}$ を作用させる

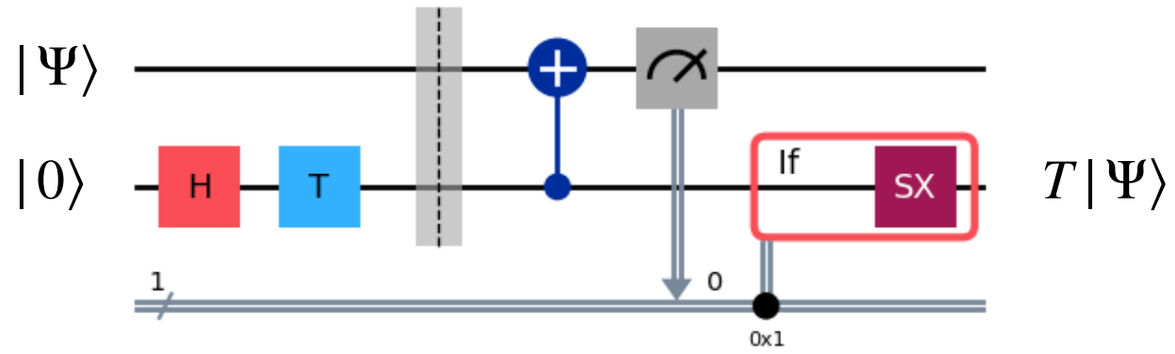
$$UXU^{\dagger}UX = U$$

量子ゲートテレポーテーション

- Tゲートの量子ゲートテレポーテーション
  - Tゲートの場合

$$TXT^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\pi/4} \end{bmatrix} = e^{-i\pi/4} \begin{bmatrix} 0 & 1 \\ e^{i\pi/2} & 0 \end{bmatrix} = e^{-i\pi/4} SX$$

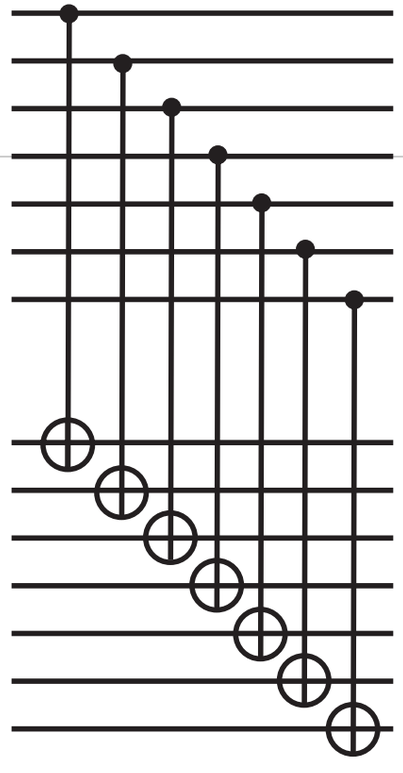
  - さらに、TゲートとCXゲートは交換するので

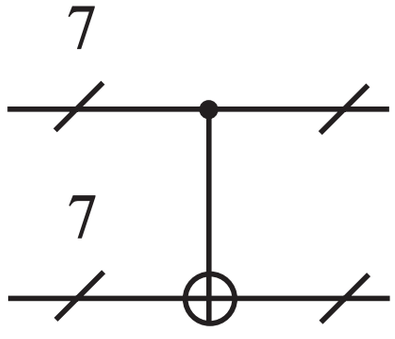


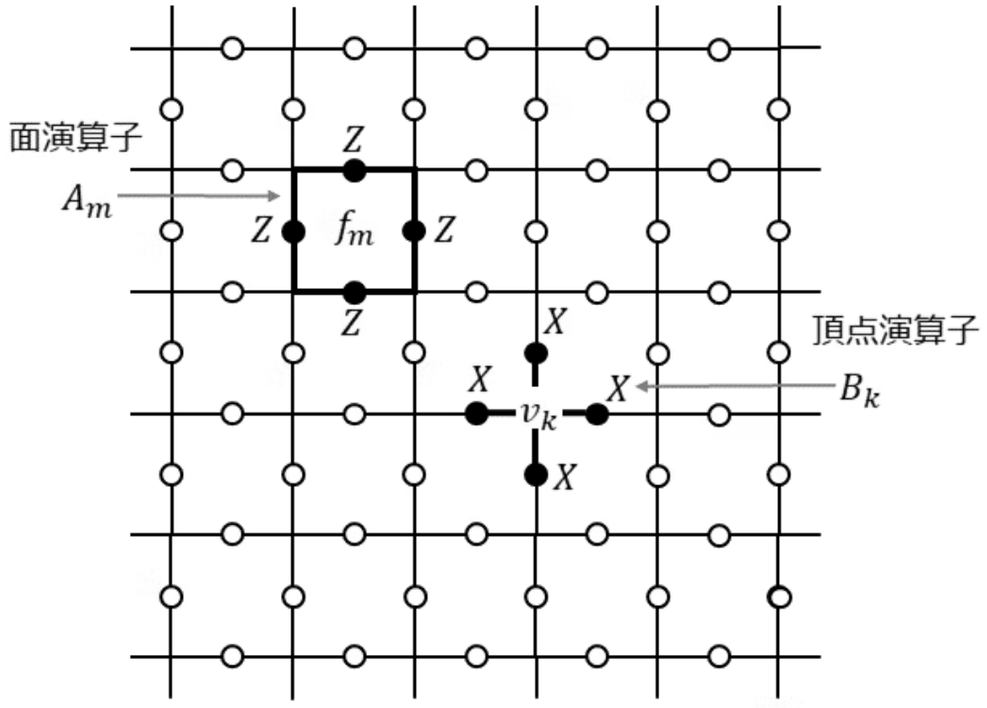
- Tゲートを直接作用させるのは難しくても、$T|+\rangle$（魔法状態）が準備できれば、クリフォード演算（CX, X, S）のみで $|\Psi\rangle$ にTゲートを作用させることができる！
- FTQC（誤り耐性量子演算）で特に有用

発展した話題

- 多量子量子ビット論理演算
  - 論理CNOT、論理トフォリゲート、etc
- ユニバーサル量子演算
  - 論理位相シフト(T)ゲート
- 誤り耐性量子計算(Fault-Tolerant Quantum Computation: FTQC)
  - 連結符号(Concatenated Code)
    - 階層的に符号化を構成
  - 表面符号(Surface Code)
    - 二次元格子上のスタビライザ符号
    - スタビライザは局所的な演算子の積
    - 系統的に符号距離を増やすことが可能







https://qiita.com/SamN