2026-02-12 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?

Tatsuya Sakashita / 坂下 達哉

Department of Physics, The University of Tokyo / 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
- 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)

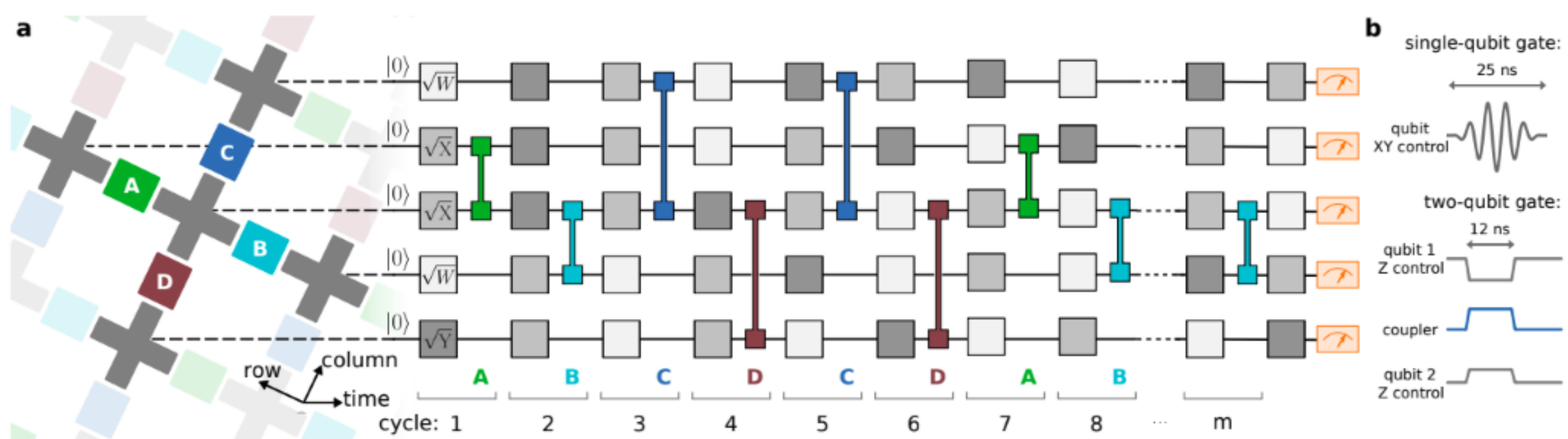
なぜ誤り訂正が必要なのか？

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は、様々な誤り検出・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、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

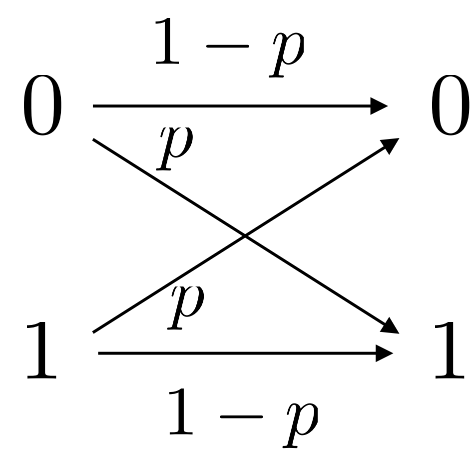
$$Z|0\rangle = |0\rangle$$
$$Z|1\rangle = -|1\rangle$$
$$Z(\alpha|0\rangle + \beta|1\rangle) = \alpha Z|0\rangle + \beta Z|1\rangle = \alpha|0\rangle - \beta|1\rangle$$

- 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 $(0 \leq p \leq 0.5)$



二元対称通信路

  - この古典通信路(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
  - 通信路を使用する度に、起きるエラーは独立とする。
  - →確率 pの独立同一分布
- 如何にして、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)」し送信する。
    - 受信側では「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：

元の情報		符号語
0	$\rightarrow$	000
1	$\rightarrow$	111

  - 000 と 111 をそれぞれ「論理 0 (logical 0)」と「論理 1 (logical 1)」と呼ぶ
- 通信路で誤りが起きるため、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：0が多い場合は0、1が多い場合は1と判定

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

- 注: 復号の前に、全てのビットを個別に「測定」している

3ビット反復符号の誤り率

- 多数決を使って復号：0が多い場合は0、1が多い場合は1と判定

受信した符号語（誤りがあるかも）

$$\begin{matrix}000\\001\\010\\100\end{matrix} \to 0$$

推定した元の情報

受信した符号語（誤りがあるかも）

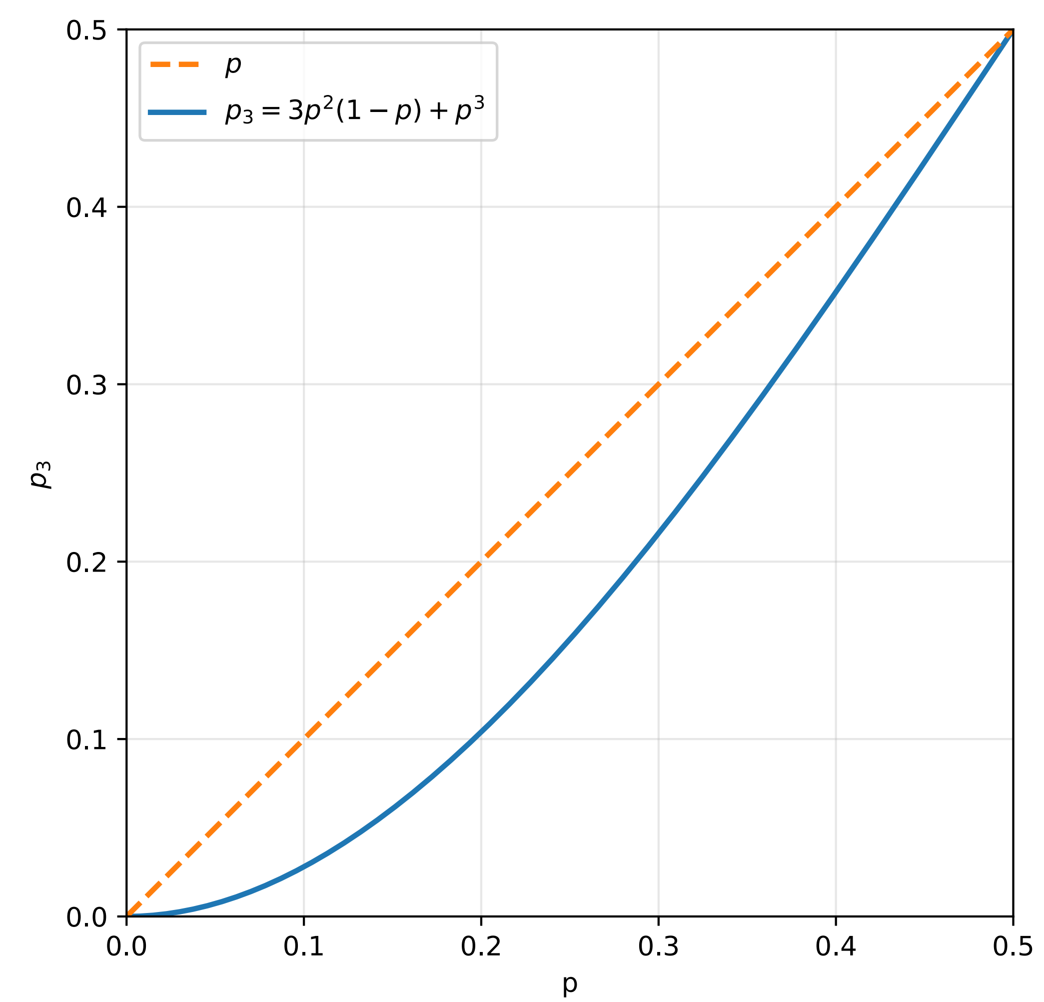
$$\begin{matrix}111\\110\\101\\011\end{matrix} \to 1$$

推定した元の情報

- 1ビット反転の場合、必ず元の情報を復元できる
- 正しく復元できない場合：
  - 誤り確率 ≈ 2ビット以上の反転が起こる確率

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

  - 常に$p_3 < p$ である。（図を参照）
  - 例えば、$p = 0.1$の時、$p_3 = 0.028 < p$
- 符号を用いない場合に比べて、誤り率を減らせる



5ビット反復符号

- 情報(0 あるいは 1)を5ビットを用いて符号化する：

元の情報　　符号語

$$
\begin{aligned}
0 &\rightarrow 00000 \\
1 &\rightarrow 11111
\end{aligned}
$$

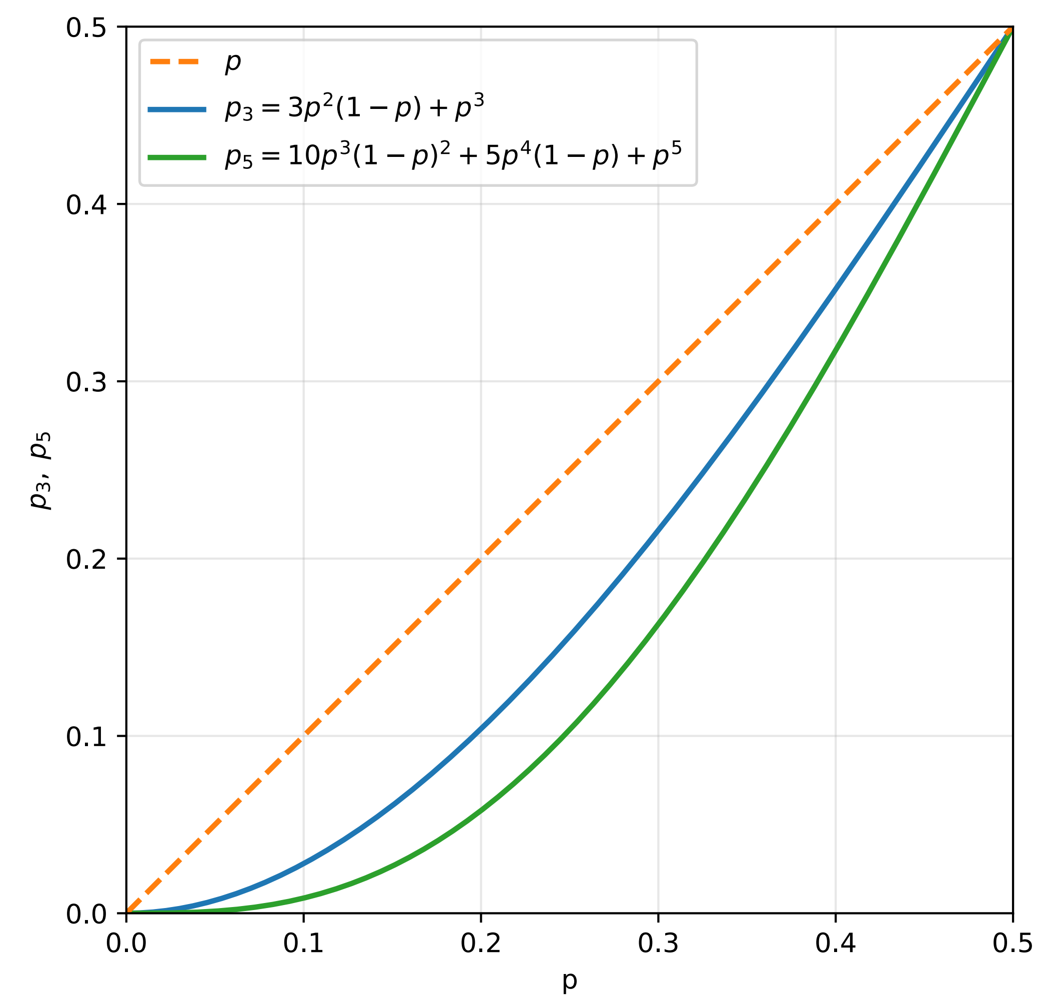
- 1ビット反転あるいは2ビット反転の場合、元の情報を復元できる
- 正しく復元できない場合
  - 誤り確率 ≈ 3ビット以上の反転が起こる確率

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

  - p_5 はさらに小さい：$p_5 < p_3 < p$　（図を参照）
  - 例えば、$p = 0.1$ のとき、

$$p_5 = 0.00856 < p_3 = 0.028 < p = 0.1$$

- ビット数を多くするほど、誤り率を減らせる



dビット反復符号

- $\lfloor d/2 \rfloor$ 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、誤り率を減らせる

- 論理0と論理1のハミング距離（合計で何ビット離れているか）を「符号距離」と呼ぶ
- dビット反復符号の場合、符号距離 = $0\cdots0$と$1\cdots1$のハミング距離 = d である。

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操作 $|\Psi\rangle \to |\Psi\rangle \otimes |\Psi\rangle \otimes |\Psi\rangle$ を行う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

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \to \quad \alpha'|000\rangle + \beta'|111\rangle$$

- → $|\psi\rangle$ を複製するのではなく、基底 $\{|0\rangle, |1\rangle\}$ に反復のアイデアを導入する

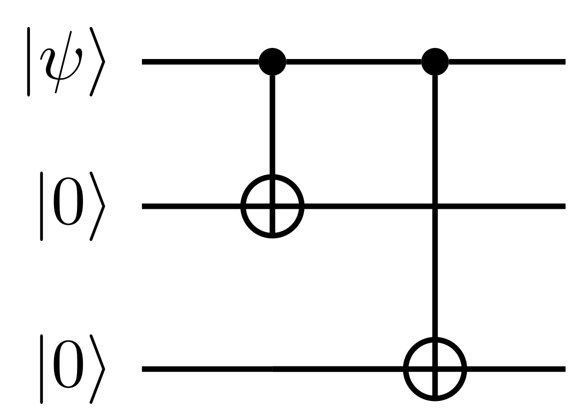
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \to \quad \alpha|000\rangle + \beta|111\rangle$$

符号化を行う量子回路

- 量子重ね合わせ状態を3量子ビット状態に符号化

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

- 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操作$|\Psi\rangle \to |\Psi\rangle \otimes |\Psi\rangle \otimes |\Psi\rangle$を行う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

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

- $|\psi\rangle$ を複製するのではなく、基底$\{|0\rangle, |1\rangle\}$に反復のアイデアを導入する

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

エラーシンドローム(Error Syndrome)

- 実際に起きたエラー（ビット反転）を直接観測することはできない。
- エラーが乗ったビット列に対して、以下の情報を観測する。
  - $P_{12} := b_1 \oplus b_2$ ビットペア(1,2)のパリティ
  - $P_{13} := b_1 \oplus b_3$ ビットペア(1,3)のパリティ
- このパリティP_{12}, P_{13}から、エラーの発生箇所を特定可能 (=エラーシンドローム)

論理0状態

受信語	P_{12}	P_{13}	エラー箇所
000	0	0	none
001	0	1	3
010	1	0	2
100	1	1	1

論理1状態

受信語	P_{12}	P_{13}	エラー箇所
111	0	0	none
110	0	1	3
101	1	0	2
011	1	1	1

- 論理0、論理1の場合の双方において、パリティとエラー箇所の対応は同一

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個別に測定すると、「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！

受信語	P_{12}	P_{13}	エラー箇所
111	0	0	none
110	0	1	3
101	1	0	2
011	1	1	1

- シンドローム測定
  - 1番目と2番目の量子ビットを同時に測定すると、結果は常に 1
  - 1番目と3番目の量子ビットを同時に測定すると、結果は常に 1
  - 測定後の状態は変化しない！

- 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 ゲートを掛けて訂正

ビット反転エラー

- 符号化された状態 $\alpha|000\rangle + \beta|111\rangle$ からなる集合を、符号空間(code space)と呼ぶ。

$$\mathrm{Span}\{|000\rangle, |111\rangle\} := \{\alpha|000\rangle + \beta|111\rangle : \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1\}$$

$|000\rangle$ と $|111\rangle$ で張られる部分空間

- ビット反転エラー
  - ビット反転(X演算子)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、状態は符号空間から飛び出す：

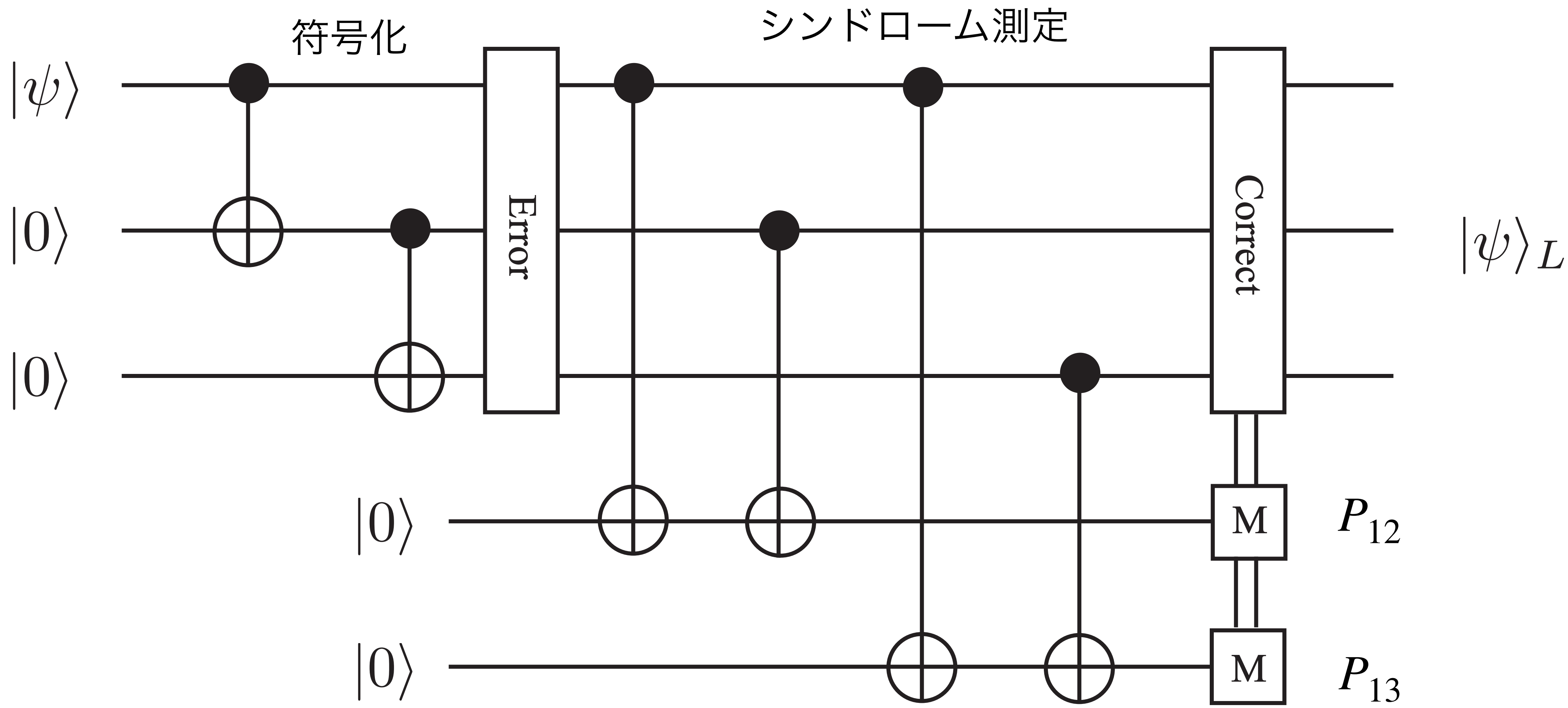
$$\alpha|000\rangle + \beta|111\rangle \quad \xrightarrow[XII]{} \quad \alpha|{\color{red}1}00\rangle + \beta|{\color{red}0}11\rangle$$

$$\notin$$

$$\mathrm{Span}\{|000\rangle, |111\rangle\}$$

- 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：
  - ビット反転なし（III）： $\mathrm{Span}\{|000\rangle, |111\rangle\}$ （符号空間に留まる）
  - 1番目の量子ビットにビット反転（XII）が起きる： $\mathrm{Span}\{|100\rangle, |011\rangle\}$
  - 2番目の量子ビットにビット反転（IXI）が起きる： $\mathrm{Span}\{|010\rangle, |101\rangle\}$
  - 3番目の量子ビットにビット反転（IIX）が起きる： $\mathrm{Span}\{|001\rangle, |110\rangle\}$

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(P_{12}, P_{13})を用いて、エラーが起きた量子ビットを同定：
  - (0,0) → エラーなし
  - (1,0) → qubit 2にエラー
  - (0,1) → qubit 3にエラー
  - $\boxed{(1,1)}$ → qubit 1にエラー

アンシラ　　アンシラ

$$\alpha|0\rangle + \beta|1\rangle \to \alpha|000\rangle|00\rangle + \beta|111\rangle|00\rangle$$

符号化

$$\to \alpha|100\rangle|00\rangle + \beta|011\rangle|00\rangle$$

エラーXIIが発生

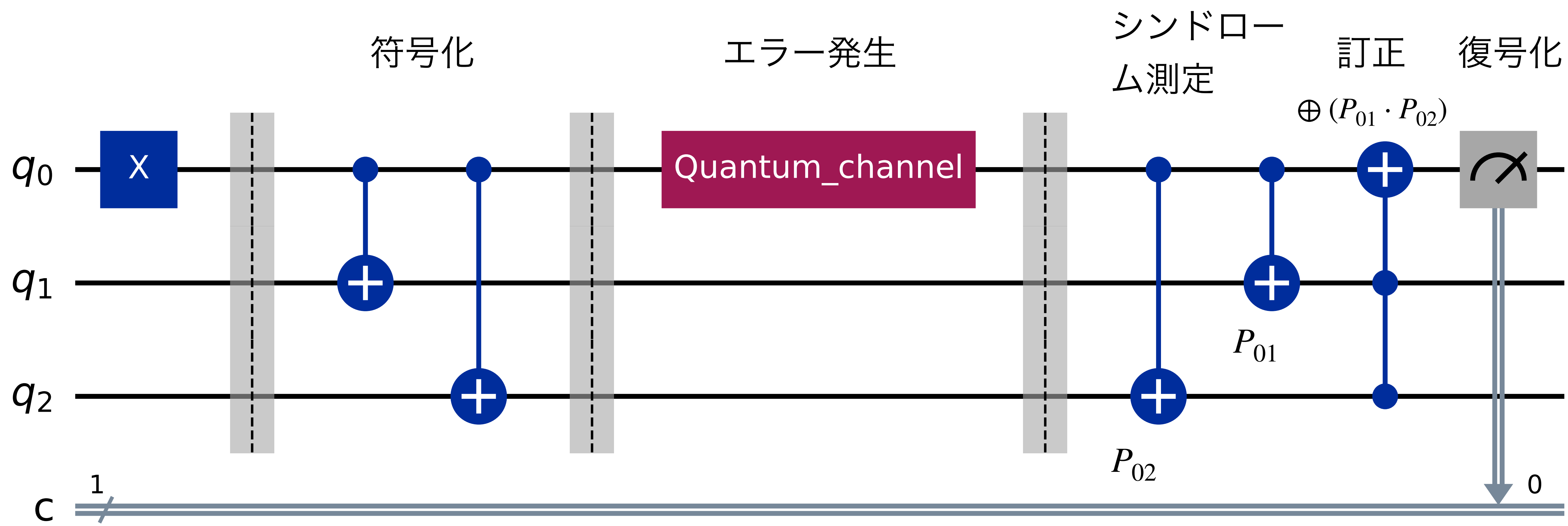
$$\to \alpha|100\rangle\boxed{|11\rangle} + \beta|011\rangle\boxed{|11\rangle}$$

シンドローム測定

シンドローム測定結果

シンドローム測定によるビット反転誤り訂正

- ハンズオンでは、以降q1, q2の結果は不要なため、直にq1とq2においてシンドローム測定を行う。
- この方針では、アンシラは不要



$$\alpha|0\rangle + \beta|1\rangle \xrightarrow[\text{符号化}]{} \alpha|000\rangle + \beta|111\rangle$$

$$\xrightarrow[\text{エラー}XII\text{が発生}]{} \alpha|100\rangle + \beta|011\rangle$$

$$\xrightarrow[\text{シンドローム測定}]{} \alpha|0\boxed{11}\rangle + \beta|1\boxed{11}\rangle$$

訂正

シンドローム測定結果

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演算子)がそれぞれのビットに確率 p で独立に生じる

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

  - 位相反転エラーは、$|+\rangle$と$|-\rangle$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

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

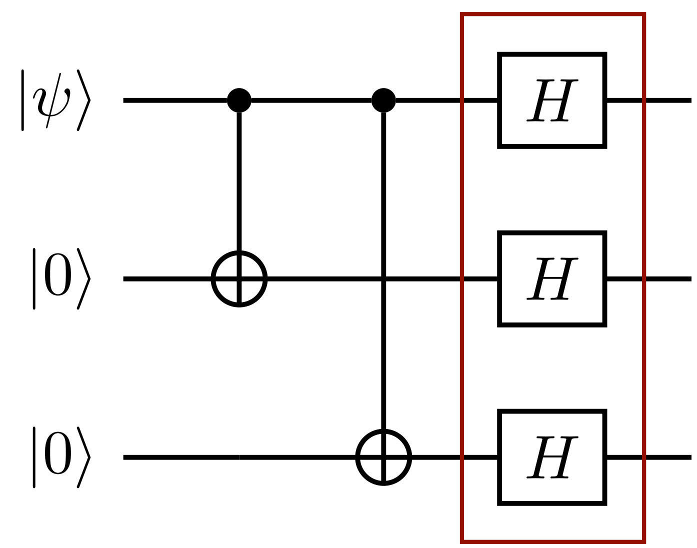
$$|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

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

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

  - 次のような回路で符号化できる



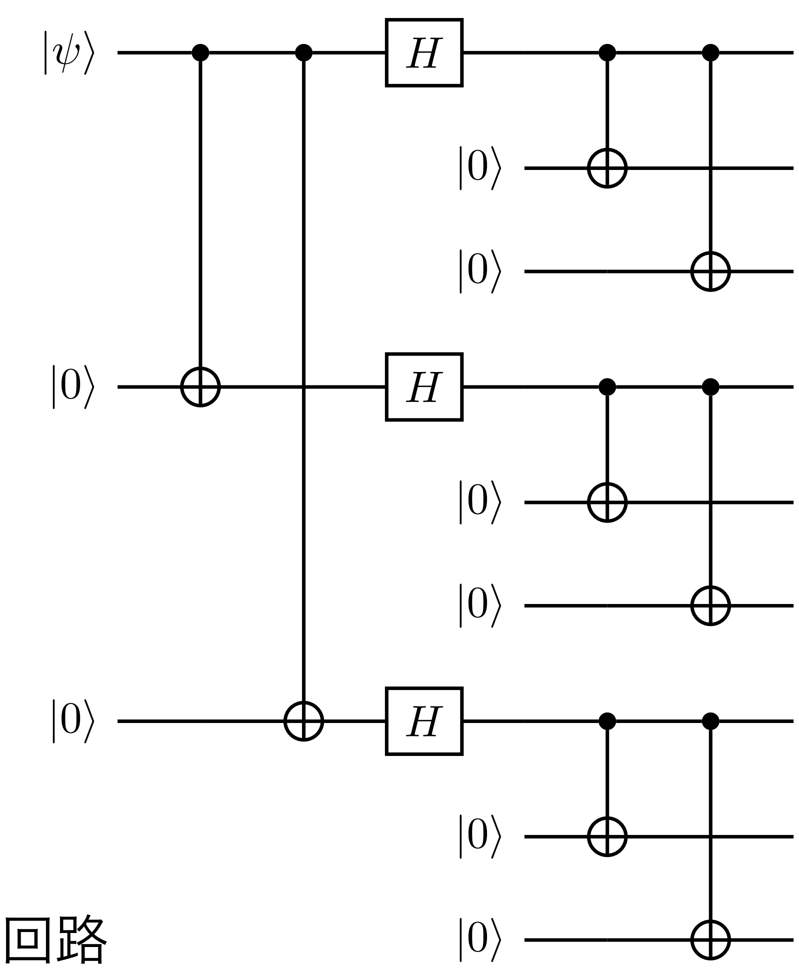
- シンドローム測定と誤り訂正
  - ビット反転の場合の$|0\rangle, |1\rangle, X$を、それぞれ$|+\rangle, |-\rangle, Z$で置き換えればOK

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

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

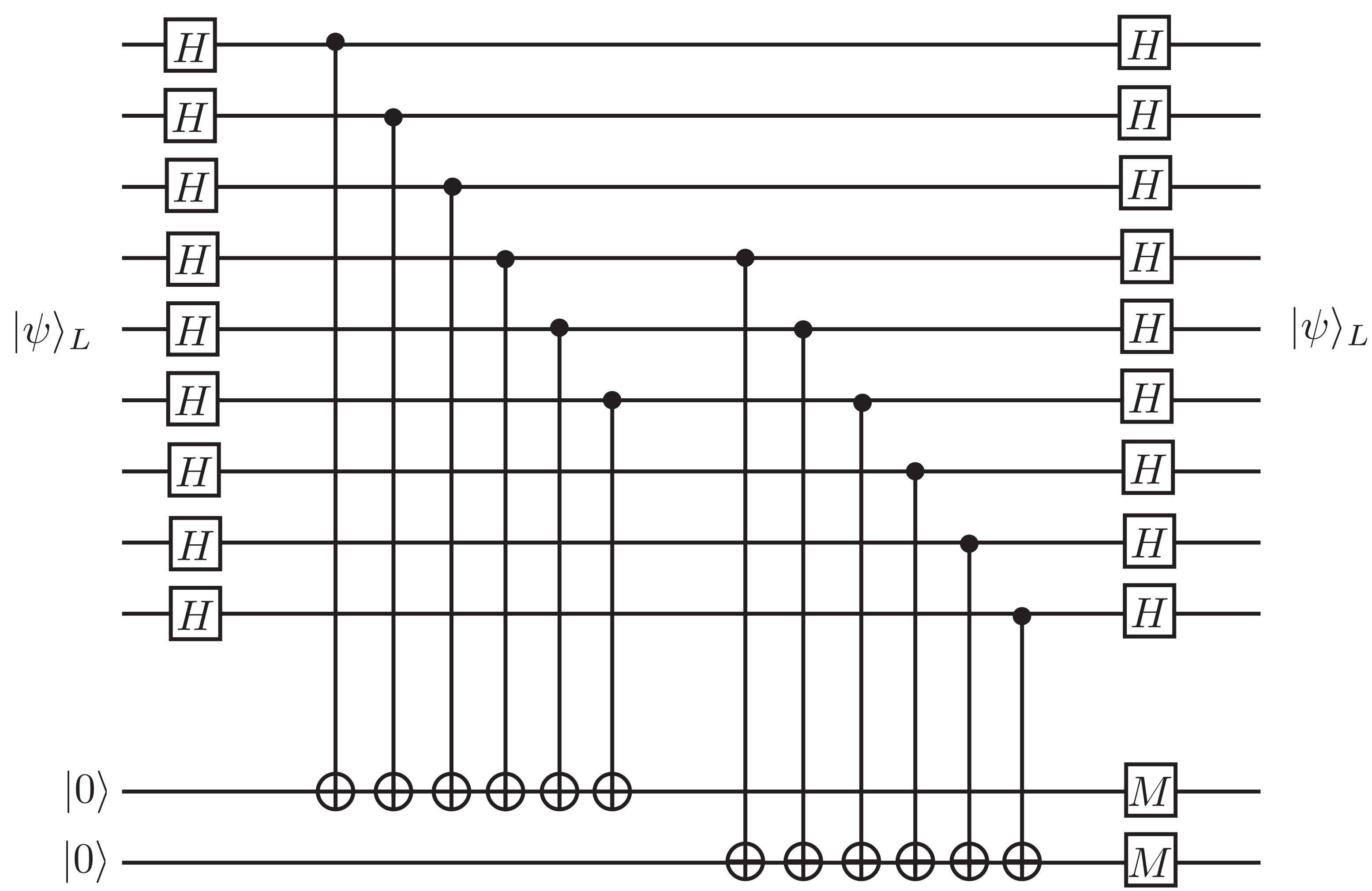
$$|1\rangle \rightarrow |---\rangle \rightarrow \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$$



符号化を行う量子回路

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（以下の量子回路）



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」で表す代わりに、「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$\pm 1, \pm i$の積を考える。これは、エルミートでユニタリなパウリ群（4×4^N個）の元
  - 例: $IIXX, XYZZ, -YIZZ$
  - 全てエルミートかつユニタリ → 固有値は± 1のみ
- パウリ群の演算子は互いに可換、あるいは反交換
  - パウリ群の$-I^{\otimes N}$を除いた中から、可換で独立な元を 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)

    反交換なパウリ演算子が２組あれば、可換であることに注意
  - 全てのスタビライザ生成元の固有値が$+1$の同時固有状態 → 状態が一つ定まる(スタビライザ状態)
- 例
  - $|0\rangle$は、Zのスタビライザ状態
  - $\mathrm{GHZ}_3 = \dfrac{|000\rangle + |111\rangle}{\sqrt{2}}$は、$K_1 = XXX, K_2 = ZZI, K_3 = IZZ$のスタビライザ状態

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):
  - $\bar{Z}:=ZZZ \quad \Rightarrow \quad |0\rangle_{\mathrm{L}}:=|000\rangle,\ |1\rangle_{\mathrm{L}}:=|111\rangle$
  - $\bar{Z}|0\rangle_{\mathrm{L}}=|0\rangle_{\mathrm{L}}$
  - $\bar{Z}|1\rangle_{\mathrm{L}}=-|1\rangle_{\mathrm{L}}$

元のパウリ演算子Zと同じ性質を満たす

スタビライザ符号

- $\bar{Z}$ (論理Z)と反交換で、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($\bar{X}$)
    - $\bar{Z}\bar{X}|0\rangle_\mathrm{L} = -\bar{X}\bar{Z}|0\rangle_\mathrm{L} = -\bar{X}|0\rangle_\mathrm{L}$より、$\bar{X}|0\rangle_\mathrm{L}$は$\bar{Z}$の固有値$-1$に対応する固有ベクトルである。したがって、$\bar{Z}|1\rangle_\mathrm{L} = -|1\rangle_\mathrm{L}$より、$\bar{X}|0\rangle_\mathrm{L} = |1\rangle_\mathrm{L}$である。

- 例(3量子ビット):
    - $\bar{X} := XXX$
    - $\bar{X}|0\rangle_\mathrm{L} = XXX|000\rangle = |111\rangle = |1\rangle_\mathrm{L}$
    - $\bar{X}|1\rangle_\mathrm{L} = XXX|111\rangle = |000\rangle = |0\rangle_\mathrm{L}$

元のパウリ演算子Xと同じ性質を満たす

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

以下を確かめてください。

- スタビライザー生成元どうしが可換、スタビライザー生成元と論理演算子が可換
- 論理 Z 演算子と論理 X 演算子が反交換

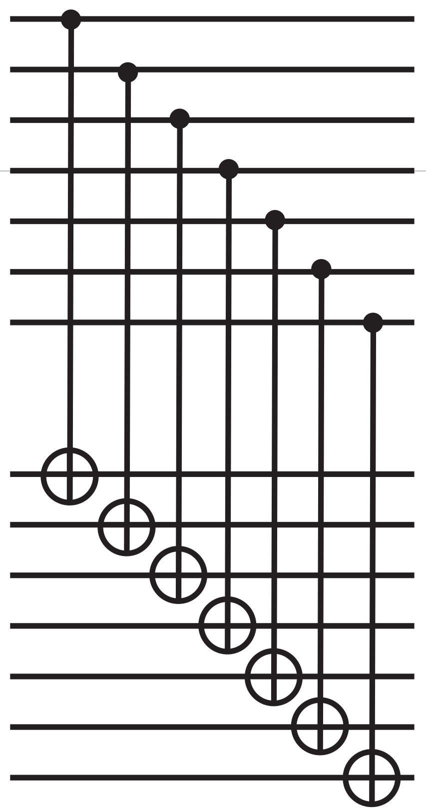
7量子ビットスティーン符号 (7-qubit Steane Code)

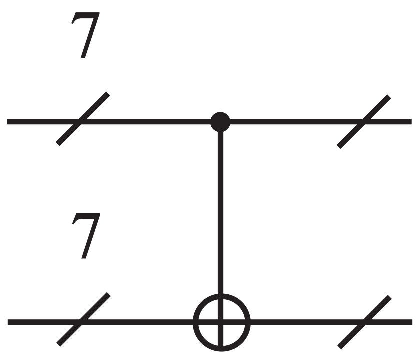
- 7量子ビットで1つの論理量子ビットを符号化
  - $7-1=6$個のスタビライザ

$$
\begin{aligned}
K^1 &= IIIXXXX, & K^2 &= XIXIXIX \\
K^3 &= IXXIIXX, & K^4 &= IIIZZZZ \\
K^5 &= ZIZIZIZ, & K^6 &= IZZIIZZ
\end{aligned}
$$

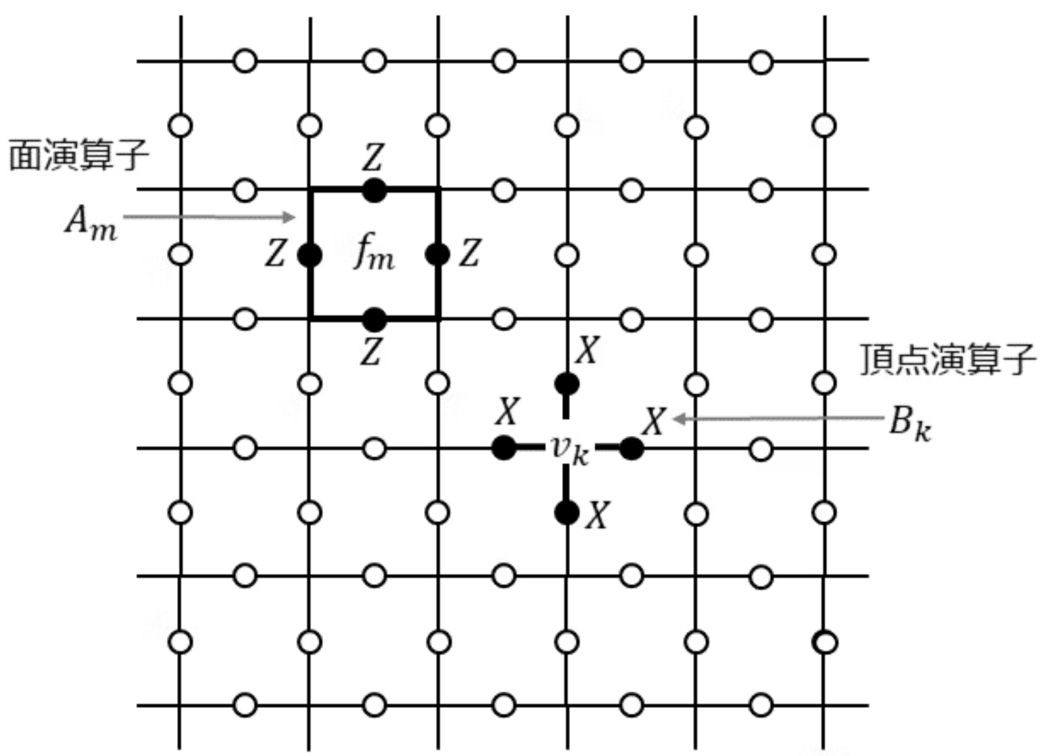
- 論理Z演算子と論理X演算子
  - $\bar{Z} = ZZZZZZZ$
  - $\bar{X} = XXXXXXX$
- 論理0状態と論理1状態
  - $$|0\rangle_{\mathrm{L}} \sim (I+\bar{Z})\prod_i (I+K^i)|0000000\rangle \sim \frac{1}{\sqrt{8}}(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle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

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