Efficient Generation of Clifford Circuits

信息科学技术学院　周书予

2021 年 12 月 17 日

outline

- Introduction: What is Clifford?
- Part A: Clifford circuit generating efficiency
- Part B: Canonical form
- Part C: Random sampling on Clifford group

Introduction

~~好像前一组同学做的内容也是围绕 Clifford 的，如果按照顺序讲的话我也许就不需要再介绍 Clifford 是什么了.~~

Pauli matrices

Pauli matrices

Single qubit

(一阶)Pauli matrices 的集合是 $\mathcal{P} = \{I, X, Y, Z\}$, 其中

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

在这里为了让 $\mathcal{P}$ 构成一个群, 我们给每个元素乘上 $\pm 1, \pm i$ 作为 global phase.

Pauli matrices

Single qubit

(一阶)Pauli matrices 的集合是 $\mathcal{P} = \{I, X, Y, Z\}$, 其中

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

在这里为了让 $\mathcal{P}$ 构成一个群, 我们给每个元素乘上 $\pm 1, \pm i$ 作为 global phase.

and for n qubits

$$\mathcal{P}_n = \{\sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n | \sigma_i \in \mathcal{P}\}$$

Pauli matrices

Single qubit

(一阶)Pauli matrices 的集合是 $\mathcal{P} = \{I, X, Y, Z\}$, 其中

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

在这里为了让 $\mathcal{P}$ 构成一个群, 我们给每个元素乘上 $\pm 1, \pm i$ 作为 global phase.

and for n qubits

$$\mathcal{P}_n = \{\sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n | \sigma_i \in \mathcal{P}\}$$

Property of Pauli group

群 $\mathcal{P}_n / U(1)$ 同构于向量空间 $\mathbb{F}_2^{2n}$

Pauli matrices

Single qubit

(一阶)Pauli matrices 的集合是 $\mathcal{P} = \{I, X, Y, Z\}$, 其中

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

在这里为了让 $\mathcal{P}$ 构成一个群, 我们给每个元素乘上 $\pm 1, \pm i$ 作为 global phase.

and for n qubits

$$\mathcal{P}_n = \{\sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n | \sigma_i \in \mathcal{P}\}$$

Property of Pauli group

群 $\mathcal{P}_n / U(1)$ 同构于向量空间 $\mathbb{F}_2^{2n}$

$$\begin{array}{ccc} Z & - & Y \\ | & & | \\ I & - & X \end{array} \quad \Leftrightarrow \quad \begin{array}{ccc} (0,1) & - & (1,1) \\ | & & | \\ (0,0) & - & (1,0) \end{array}$$

Clifford group

Definition

$$\mathcal{C}_n = \left\{ U \in U(2^n) | \sigma \in P_n \Rightarrow U \sigma U^\dagger \in P_n \right\} / U(1)$$

代数上称右侧 (没有商掉 $U(1)$ 的部分) 为 $\mathcal{P}_n$ 的 normalizer, 记作 $\mathcal{N}(\mathcal{P}_n)$.
可以发现 $\mathcal{C}_n$ 中 global phase 是不存在的, 因为被商掉了.

Clifford group

Definition

$$\mathcal{C}_n = \left\{ U \in U(2^n) | \sigma \in P_n \Rightarrow U\sigma U^\dagger \in P_n \right\} / U(1)$$

代数上称右侧 (没有商掉 $U(1)$ 的部分) 为 $\mathcal{P}_n$ 的 normalizer, 记作 $\mathcal{N}(\mathcal{P}_n)$.
可以发现 $\mathcal{C}_n$ 中 global phase 是不存在的, 因为被商掉了.

Size of $\mathcal{C}_1$

Clifford group

Definition

$$\mathcal{C}_n = \left\{ U \in U(2^n) | \sigma \in P_n \Rightarrow U\sigma U^\dagger \in P_n \right\} / U(1)$$

代数上称右侧 (没有商掉 $U(1)$ 的部分) 为 $\mathcal{P}_n$ 的 normalizer, 记作 $\mathcal{N}(\mathcal{P}_n)$.
可以发现 $\mathcal{C}_n$ 中 global phase 是不存在的, 因为被商掉了.

Size of $\mathcal{C}_1$

只需要决定 X, Z 分别被 U 共轭作用映到哪个 Pauli matrix.

Clifford group

Definition

$$\mathcal{C}_n = \left\{ U \in U(2^n) | \sigma \in P_n \Rightarrow U\sigma U^\dagger \in P_n \right\} / U(1)$$

代数上称右侧 (没有商掉 $U(1)$ 的部分) 为 $\mathcal{P}_n$ 的 normalizer, 记作 $\mathcal{N}(\mathcal{P}_n)$.
可以发现 $\mathcal{C}_n$ 中 global phase 是不存在的, 因为被商掉了.

Size of $\mathcal{C}_1$

只需要决定 X, Z 分别被 U 共轭作用映到哪个 Pauli matrix.
$UXU^\dagger$ 可以取 $\{\pm X, \pm Y, \pm Z\}$.

Clifford group

Definition

$$\mathcal{C}_n = \left\{ U \in U(2^n) | \sigma \in P_n \Rightarrow U\sigma U^\dagger \in P_n \right\} / U(1)$$

代数上称右侧 (没有商掉 $U(1)$ 的部分) 为 $\mathcal{P}_n$ 的 normalizer, 记作 $\mathcal{N}(\mathcal{P}_n)$.
可以发现 $\mathcal{C}_n$ 中 global phase 是不存在的, 因为被商掉了.

Size of $\mathcal{C}_1$

只需要决定 X, Z 分别被 U 共轭作用映到哪个 Pauli matrix.
$UXU^\dagger$ 可以取 $\{\pm X, \pm Y, \pm Z\}$.
$UZU^\dagger$ 也可以取 $\{\pm X, \pm Y, \pm Z\}$, 但需要满足与 $UXU^\dagger$ anti-commute, 因此不能取 $\pm UXU^\dagger$. 剩下有恰好四种取法.

Clifford group

Definition

$$\mathcal{C}_n = \left\{ U \in U(2^n) | \sigma \in P_n \Rightarrow U\sigma U^\dagger \in P_n \right\} / U(1)$$

代数上称右侧 (没有商掉 $U(1)$ 的部分) 为 $\mathcal{P}_n$ 的 normalizer, 记作 $\mathcal{N}(\mathcal{P}_n)$.
可以发现 $\mathcal{C}_n$ 中 global phase 是不存在的, 因为被商掉了.

Size of $\mathcal{C}_1$

只需要决定 X, Z 分别被 U 共轭作用映到哪个 Pauli matrix.
$UXU^\dagger$ 可以取 $\{\pm X, \pm Y, \pm Z\}$.
$UZU^\dagger$ 也可以取 $\{\pm X, \pm Y, \pm Z\}$, 但需要满足与 $UXU^\dagger$ anti-commute, 因此不能取 $\pm UXU^\dagger$. 剩下有恰好四种取法.
$|\mathcal{C}_1| = 6 \cdot 4 = 24$.

Clifford group

Definition

$$\mathcal{C}_n = \left\{ U \in U(2^n) | \sigma \in P_n \Rightarrow U\sigma U^\dagger \in P_n \right\} / U(1)$$

代数上称右侧 (没有商掉 $U(1)$ 的部分) 为 $\mathcal{P}_n$ 的 normalizer, 记作 $\mathcal{N}(\mathcal{P}_n)$.
可以发现 $\mathcal{C}_n$ 中 global phase 是不存在的, 因为被商掉了.

Size of $\mathcal{C}_1$

只需要决定 X, Z 分别被 U 共轭作用映到哪个 Pauli matrix.
$UXU^\dagger$ 可以取 $\{\pm X, \pm Y, \pm Z\}$.
$UZU^\dagger$ 也可以取 $\{\pm X, \pm Y, \pm Z\}$, 但需要满足与 $UXU^\dagger$ anti-commute, 因此不能取 $\pm UXU^\dagger$. 剩下有恰好四种取法.
$|\mathcal{C}_1| = 6 \cdot 4 = 24$.

General Conclusion

$$|\mathcal{C}_n| = \prod_{i=1}^{n} 2(4^i - 1) \cdot 4^i = 2^{n^2+2n} \prod_{i=1}^{n} (4^i - 1)$$

Clifford group

上一页的结论与 A003956[1] 并不一致，这是为什么呢？

[1] http://oeis.org/A003956

Clifford group

上一页的结论与 A003956[1] 并不一致, 这是为什么呢?

Another Definition

$\mathcal{C}_n = \langle H, S, \mathrm{CNOT} \rangle$, 其中

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

[1] http://oeis.org/A003956

Clifford group

上一页的结论与 A003956[1] 并不一致, 这是为什么呢?

Another Definition

$\mathcal{C}_n = \langle H, S, \mathrm{CNOT} \rangle$, 其中

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

两种定义方式存在细微的区别. 后者定义的 $\mathcal{C}_n$ 中包含 $(SH)^3 = e^{\frac{i\pi}{4}} I$, 导致产生 8 种不同的 global phase, 从而使集合大小变成原来的 8 倍. OEIS 上的数列遵循的是后者 (所以多了 8 的系数).

我们会构造证明两种定义方式 (在忽略 gloal phase 时) 的等价性.

[1] http://oeis.org/A003956

Part A

先补充定义一些东西:
默认第二种对 $\mathcal{C}_n$ 的定义, 即暂时不承认 $\mathcal{C}_n/U(1) = \mathcal{N}(\mathcal{P}_n)/U(1)$, 称 H, S, CNOT 三个门为 Clifford gate, 称由这三个门组成的量子线路为 Clifford circuit, 称 Clifford circuit 实现的算符为 Clifford operator.

Part A

先补充定义一些东西:
默认第二种对 $\mathcal{C}_n$ 的定义, 即暂时不承认 $\mathcal{C}_n/U(1) = \mathcal{N}(\mathcal{P}_n)/U(1)$, 称 H, S, CNOT 三个门为 Clifford gate, 称由这三个门组成的量子线路为 Clifford circuit, 称 Clifford circuit 实现的算符为 Clifford operator.

Theorem 1

$\mathcal{C}_n \subseteq \mathcal{N}(\mathcal{P}_n)$, 即 Clifford operator 都是 $\mathcal{P}_n$ 的 normalizer.

Theorem 2

任意 $U \in \mathcal{N}(\mathcal{P}_n)$ 都可以通过 $O(n^2)$ 个 Clifford gates 实现, up to a global phase.

Part A

先补充定义一些东西:
默认第二种对 $\mathcal{C}_n$ 的定义, 即暂时不承认 $\mathcal{C}_n/U(1)=\mathcal{N}(\mathcal{P}_n)/U(1)$, 称 H, S, CNOT 三个门为 Clifford gate, 称由这三个门组成的量子线路为 Clifford circuit, 称 Clifford circuit 实现的算符为 Clifford operator.

Theorem 1

$\mathcal{C}_n \subseteq \mathcal{N}(\mathcal{P}_n)$, 即 Clifford operator 都是 $\mathcal{P}_n$ 的 normalizer.

Theorem 2

任意 $U \in \mathcal{N}(\mathcal{P}_n)$ 都可以通过 $O(n^2)$ 个 Clifford gates 实现, up to a global phase.

之后 “up to a global phase” 这样的状语可能会频繁地出现.

Proof of Theorem 1

只需要验证生成元 $\{H, S, \mathrm{CNOT}\}$ 就好了，而且也只要验证作用于 X, Z 这两个 Pauli matrices

U	σ	$U\sigma U^\dagger$
controlled-NOT CNOT	X_1	$X_1 X_2$
	X_2	X_2
	Z_1	Z_1
	Z_2	$Z_1 Z_2$
Hadamard H	X	Z
	Z	X
phase S	X	Y
	Z	Z

Proof of Theorem 2

考虑归纳.

- 证明: 任意 $U \in \mathcal{N}(\mathcal{P}_1)$ 可以通过 $O(1)$ 个 H, S 门实现.
- 证明: 如果结论对于 n 成立, 那么任意满足 $UZ_1U^\dagger = X_1 \otimes g$ 以及 $UX_1U^\dagger = Z_1 \otimes g'$ 的 $U \in \mathcal{N}(\mathcal{P}_{n+1})$ 可以通过 $O(n^2)$ 个 Clifford 门实现.
- 证明: 如果上一条成立, 那么任意 $U \in \mathcal{N}(\mathcal{P}_{n+1})$ 可以通过 $O(n^2)$ 个 Clifford 门实现.

(严谨地说, 每一步结论都需要加上一句 "up to a global phase" .)

Proof of Theorem 2

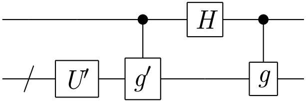
考虑归纳.

- 证明: 任意 $U \in \mathcal{N}(\mathcal{P}_1)$ 可以通过 $O(1)$ 个 H, S 门实现.
- 证明: 如果结论对于 n 成立, 那么任意满足 $UZ_1U^\dagger = X_1 \otimes g$ 以及 $UX_1U^\dagger = Z_1 \otimes g'$ 的 $U \in \mathcal{N}(\mathcal{P}_{n+1})$ 可以通过 $O(n^2)$ 个 Clifford 门实现.
- 证明: 如果上一条成立, 那么任意 $U \in \mathcal{N}(\mathcal{P}_{n+1})$ 可以通过 $O(n^2)$ 个 Clifford 门实现.

(严谨地说, 每一步结论都需要加上一句 “up to a global phase” .)
讲一下第二步怎么证明, 其中用到了一个比较巧妙的构造.

Proof of the Second Step

令 U' 满足 $U'|\psi\rangle = \sqrt{2}\langle 0|U(|0\rangle \otimes |\psi\rangle)$. 构造量子线路



假设线路实现了 $\tilde{U}$, 我们希望证明 $U = \tilde{U}$. 注意 $UZ_1U^\dagger = X_1 \otimes g$, $UX_1U^\dagger = Z_1 \otimes g'$, 可以写出 U 以及 $U'|\psi\rangle$ 的一些变式

$$
\begin{aligned}
U &= (X_1 \otimes g)UZ_1 \\
&= (Z_1 \otimes g')UX_1 \\
&= (Z_1X_1 \otimes g'g)U(Z_1X_1)
\end{aligned}
$$

$$
\begin{aligned}
U'|\psi\rangle &= \sqrt{2}\langle 0|U(|0\rangle \otimes |\psi\rangle) \\
&= \sqrt{2}\langle 1|gU(|0\rangle \otimes |\psi\rangle) \\
&= \sqrt{2}\langle 0|g'U(|1\rangle \otimes |\psi\rangle) \\
&= -\sqrt{2}\langle 1|g'gU(|1\rangle \otimes |\psi\rangle)
\end{aligned}
$$

Proof of the Second Step

想要证明 $U = \tilde{U}$, **可以验证对于** $\forall |\alpha\rangle, |\beta\rangle \in \{|0\rangle, |1\rangle\}$, **都有** $\langle\alpha|\, \tilde{U}(|\beta\rangle \otimes |\psi\rangle) = \langle\alpha|\, U(|\beta\rangle \otimes |\psi\rangle)$.

Proof of the Second Step

想要证明 $U = \tilde{U}$, **可以验证对于** $\forall|\alpha\rangle, |\beta\rangle \in \{|0\rangle, |1\rangle\}$, **都有** $\langle\alpha|\tilde{U}(|\beta\rangle \otimes |\psi\rangle) = \langle\alpha|U(|\beta\rangle \otimes |\psi\rangle)$. **以** $|\alpha\rangle = |0\rangle, |\beta\rangle = |1\rangle$ **为例**

$$
\begin{aligned}
\langle 0|\tilde{U}(|1\rangle \otimes |\psi\rangle) &= \langle 0|(\frac{1}{\sqrt{2}}|0\rangle \otimes g' U'|\psi\rangle - \frac{1}{\sqrt{2}}|1\rangle \otimes gg' U'|\psi\rangle) \\
&= \frac{1}{\sqrt{2}} g' U'|\psi\rangle \\
&= \frac{1}{\sqrt{2}} g' \cdot \sqrt{2}\langle 0|g' U(|1\rangle \otimes |\psi\rangle) \\
&= \langle 0|U(|1\rangle \otimes |\psi\rangle)
\end{aligned}
$$

证明了 $U = \tilde{U}$ 之后, 由归纳假设 U' 可以被 $O(n^2)$ 个 Clifford 门实现. 剩下的部分可以被 $O(n)$ 个门实现 (考虑 Controlled-$\{X, Y, Z\}$), 因此结论得证. ■

Part A Conclusion

把两条结论连起来, 可以直接得到

Corollary

任意 Clifford operator 都可以通过 $O(n^2)$ 个 Clifford gates 实现.

本来是要 "up to a global phase" 的, 但 Clifford group 里的 global phase 都可以通过 $O(1)$ 个门实现, 因此就可以去掉了.
这个推论指出了 Clifford operator 的实现高效性.

Part B

在这一部分, 我们引入一个叫做 Canonical form 的记号, 并证明 $\mathcal{C}_n$ 与之的一一对应关系. 这有助于我们进一步掌握 Clifford group 内部的结构, 并最终实现随机采样.

[1] 中介绍的方法通过研究 $\mathcal{C}_n$ 的子群得到了一些有益的结论.

接下来我们均忽略 global phase.

Subset structure of $\mathcal{C}_n$

Notation	Name	Generating Set
$\mathcal{C}_n$	Clifford group	H, S, CNOT
$\mathcal{F}_n$	Hadamard-free group	$X, S, \mathrm{CNOT}, \mathrm{CZ}$
$\mathcal{B}_n$	Borel group	$X, S, \mathrm{CNOT}^{\downarrow}, \mathrm{CZ}$
$\mathcal{S}_n$	Symmetric group	SWAP
$\mathcal{P}_n$	Pauli group	X, Z

$\mathcal{C}_n$ 的 Generating Set 也可以写成 $\{X, Z, H, S, \mathrm{CNOT}, \mathrm{CZ}\}$, 从而显式地指出表中的所有群都是其子群.

Hadamard Free?

考虑这样一件事情: Hadamard gate 是 (在 computational basis 下) 唯一会产生叠加态的 Clifford gate, 这说明 Hadamard-free group $\mathcal{F}_n$ 中的任何算符都不能产生任何叠加, 只能把基矢映成基矢, 因而会有如下的形式:

Hadamard Free?

考虑这样一件事情: Hadamard gate 是 (在 computational basis 下) 唯一会产生叠加态的 Clifford gate, 这说明 Hadamard-free group $\mathcal{F}_n$ 中的任何算符都不能产生任何叠加, 只能把基矢映成基矢, 因而会有如下的形式:

$$F|x\rangle = i^{x^\intercal \Gamma x} O|\Delta x\rangle \tag{1}$$

其中 $x \in \mathbb{F}_2^n, \Gamma, \Delta \in \mathbb{F}_2^{n\times n}, O \in \mathcal{P}_n$. Δ 是可逆的, 它表示 n 个 qubit 之间的纠缠, 而 Γ 的作用是确定相位, 它是对称的.

Hadamard Free?

考虑这样一件事情: Hadamard gate 是 (在 computational basis 下) 唯一会产生叠加态的 Clifford gate, 这说明 Hadamard-free group $\mathcal{F}_n$ 中的任何算符都不能产生任何叠加, 只能把基矢映成基矢, 因而会有如下的形式:

$$F|x\rangle = i^{x^\intercal \Gamma x} O|\Delta x\rangle \tag{1}$$

其中 $x \in \mathbb{F}_2^n, \Gamma, \Delta \in \mathbb{F}_2^{n\times n}, O \in \mathcal{P}_n$. Δ 是可逆的, 它表示 n 个 qubit 之间的纠缠, 而 Γ 的作用是确定相位, 它是对称的.

$\mathcal{B}_n$ 生成元集合中的 $\mathrm{CNOT}^{\downarrow}$ 记号表示 control qubit 比 target qubit 标号小的 CNOT 门, 这使得 eq. (1) 式中的 Δ 变成了下三角, 且对角元全是 1。这样的简化也使得我们可以直接地写出算符 F 的量子线路表示:

Hadamard Free?

考虑这样一件事情: Hadamard gate 是 (在 computational basis 下) 唯一会产生叠加态的 Clifford gate, 这说明 Hadamard-free group $\mathcal{F}_n$ 中的任何算符都不能产生任何叠加, 只能把基矢映成基矢, 因而会有如下的形式:

$$F|x\rangle = i^{x^{\mathsf{T}}\Gamma x} O|\Delta x\rangle \tag{1}$$

其中 $x \in \mathbb{F}_2^n, \Gamma, \Delta \in \mathbb{F}_2^{n\times n}, O \in \mathcal{P}_n$. Δ 是可逆的, 它表示 n 个 qubit 之间的纠缠, 而 Γ 的作用是确定相位, 它是对称的.
$\mathcal{B}_n$ 生成元集合中的 $\mathrm{CNOT}^{\downarrow}$ 记号表示 control qubit 比 target qubit 标号小的 CNOT 门, 这使得 eq. (1) 式中的 Δ 变成了下三角, 且对角元全是 1。这样的简化也使得我们可以直接地写出算符 F 的量子线路表示:

$$F = O\prod_{i=1}^{n} S_i^{\Gamma_{i,i}} \prod_{1\le i<j\le n} \mathrm{CZ}_{i,j}^{\Gamma_{i,j}} \prod_{1\le i<j\le n} \mathrm{CNOT}_{i,j}^{\Delta_{j,i}} \tag{2}$$

接下来会用 $F(O,\Gamma,\Delta)$ 来表示 eq. (2) 中的 F. 称算符 $F(O,\Gamma,\Delta)$ 的 Pauli 部分是平凡的, 当且仅当 $O = I$.

Canonical Form

Theorem(Canonical Form)

任意 $U \in \mathcal{C}_n$ 都可以被唯一地写成

$$U = F(I, \Gamma, \Delta) \cdot \left(\prod_{i=1}^{n} H_i^{h_i} \right) \sigma \cdot F(O', \Gamma', \Delta') \tag{3}$$

其中 $h \in \{0,1\}^n, \sigma \in \mathcal{S}_n$ 是 n 阶排列，$F(I, \Gamma, \Delta), F(O', \Gamma', \Delta') \in \mathcal{B}_n$，其中 Γ, Δ 需要满足条件：对于 $\forall 1 \leq i, j \leq n$:

1. 若 $h_i = 0, h_j = 0$，则 $\Gamma_{i,j} = 0$.
2. 若 $h_i = 1, h_j = 0, \sigma(i) > \sigma(j)$，则 $\Gamma_{i,j} = 0$.
3. 若 $h_i = 0, h_j = 0, \sigma(i) > \sigma(j)$，则 $\Delta_{i,j} = 0$.
4. 若 $h_i = 1, h_j = 1, \sigma(i) < \sigma(j)$，则 $\Delta_{i,j} = 0$.
5. 若 $h_i = 1, h_j = 0$，则 $\Delta_{i,j} = 0$.

Why Canonical?

Bruhat Decomposition[2]

Clifford group $\mathcal{C}_n$ 可以写成如下不交并的形式

$$\mathcal{C}_n = \bigsqcup_{h\in\{0,1\}^n} \bigsqcup_{\sigma\in\mathcal{S}_n} \mathcal{B}_n \left(\prod_{i=1}^{n} H_i^{h_i}\right) \sigma \mathcal{B}_n$$

Definition

对于 $h \in \{0,1\}^n, \sigma \in \mathcal{S}_n$, 定义 $\mathcal{B}_n$ 的子群

$$\mathcal{B}_n(h,\sigma) = \{F \in \mathcal{B}_n : W^{-1}FW \in \mathcal{B}_n\}$$

(可以验证这是一个子群) 其中 $W = \left(\prod_{i=1}^{n} H_i^{h_i}\right)\sigma$, 以下会始终沿用这个记号.

Important Lemmas

Lemma 1

记 $\overline{h} = h \oplus 1^n$ 表示 h 的按位取反，那么任意算符 $F(O, \Gamma, \Delta) \in \mathcal{B}_n$ 是 $\mathcal{B}_n(\overline{h}, \sigma)$ 中的元素，当且仅当 Γ, Δ 对于 h, σ 满足 Canonical form 中的五条限制，此外还存在关系

$$\mathcal{B}_n(\overline{h}, \sigma) \cap \mathcal{B}_n(h, \sigma) = \mathcal{P}_n$$

Lemma 2

任意算符 $F \in \mathcal{B}_n$ 都可以被唯一写成 $F = F_L F_R$，其中 $F_R \in \mathcal{B}_n(h, \sigma)$，$F_L \in \mathcal{B}_n(\overline{h}, \sigma)$ 且 Pauli 部分是平凡的。

Proof of One-to-one Correspondence

Bruhat Decomposition 和两个引理的证明篇幅太长了我们直接跳过, 考虑利用它们来证明 Canonical form 的存在与唯一性.

Proof of One-to-one Correspondence

Bruhat Decomposition 和两个引理的证明篇幅太长了我们直接跳过, **考虑利用它们来证明 Canonical form 的存在与唯一性.**

首先由 Bruhat Decomposition **知任意** $U \in \mathcal{C}_n$ **可以写成** $U = LWR$, **其中** $L, R \in \mathcal{B}_n$, **且** W **唯一确定. 根据** Lemma 2, L **可以被进一步分解为** $L = BC$, **其中** $C \in \mathcal{B}_n(h, \sigma), B \in \mathcal{B}_n(\overline{h}, \sigma)$ **且** Pauli **部分平凡, 因此有**

$$U = LWR = BCWR = BWW^{-1}CWR = BWC'R$$

根据 $\mathcal{B}_n(h, \sigma)$ **的定义, 有** $C' \triangleq W^{-1}CW \in \mathcal{B}_n$, **因而** $C'R \in \mathcal{B}_n$, **这证明了** Canonical form **的存在性.**

Proof of One-to-one Correspondence

Bruhat Decomposition 和两个引理的证明篇幅太长了我们直接跳过, 考虑利用它们来证明 Canonical form 的存在与唯一性.

首先由 Bruhat Decomposition 知任意 $U \in \mathcal{C}_n$ 可以写成 $U = LWR$, 其中 $L, R \in \mathcal{B}_n$, 且 W 唯一确定. 根据 Lemma 2, L 可以被进一步分解为 $L = BC$, 其中 $C \in \mathcal{B}_n(h, \sigma), B \in \mathcal{B}_n(\overline{h}, \sigma)$ 且 Pauli 部分平凡, 因此有

$$U = LWR = BCWR = BWW^{-1}CWR = BWC'R$$

根据 $\mathcal{B}_n(h, \sigma)$ 的定义, 有 $C' \triangleq W^{-1}CW \in \mathcal{B}_n$, 因而 $C'R \in \mathcal{B}_n$, 这证明了 Canonical form 的存在性.

至于唯一性, 考虑 $F_1 W F_1' = F_2 W F_2'$ 均满足条件, 由于

$$W^{-1}(F_2^{-1}F_1)W = F_2'(F_1')^{-1} \in \mathcal{B}_n$$

这说明了 $F_2^{-1}F_1 \in \mathcal{B}_n(\overline{h}, \sigma) \cap \mathcal{B}_n(h, \sigma) = \mathcal{P}_n$, 注意到两者 Pauli 部分平凡, 导致 $F_2^{-1}F_1 = I$ 从而 $F_1 = F_2, F_1' = F_2'$, 唯一性得证.

High Level Proof of Lemma 1

Lemma 1

记 $\overline{h} = h \oplus 1^n$ 表示 h 的按位取反，那么任意算符 $F(O, \Gamma, \Delta) \in \mathcal{B}_n$ 是 $\mathcal{B}_n(\overline{h}, \sigma)$ 中的元素，当且仅当 Γ, Δ 对于 h, σ 满足 Canonical form 中的五条限制，此外还存在关系

$$\mathcal{B}_n(\overline{h}, \sigma) \cap \mathcal{B}_n(h, \sigma) = \mathcal{P}_n$$

High Level Proof of Lemma 1

Lemma 1

记 $\overline{h} = h \oplus 1^n$ 表示 h 的按位取反，那么任意算符 $F(O, \Gamma, \Delta) \in \mathcal{B}_n$ 是 $\mathcal{B}_n(\overline{h}, \sigma)$ 中的元素，当且仅当 Γ, Δ 对于 h, σ 满足 Canonical form 中的五条限制，此外还存在关系

$$\mathcal{B}_n(\overline{h}, \sigma) \cap \mathcal{B}_n(h, \sigma) = \mathcal{P}_n$$

充分性 ($\Leftarrow$)：即证明只要 Γ, Δ 满足五条限制就可以使 $F(O, \Gamma, \Delta) \in \mathcal{B}(\overline{h}, \sigma)$，考虑对满足条件的生成元验证.

High Level Proof of Lemma 1

Lemma 1

记 $\overline{h} = h \oplus 1^n$ 表示 h 的按位取反，那么任意算符 $F(O, \Gamma, \Delta) \in \mathcal{B}_n$ 是 $\mathcal{B}_n(\overline{h}, \sigma)$ 中的元素，当且仅当 Γ, Δ 对于 h, σ 满足 Canonical form 中的五条限制，此外还存在关系

$$\mathcal{B}_n(\overline{h}, \sigma) \cap \mathcal{B}_n(h, \sigma) = \mathcal{P}_n$$

充分性 ($\Leftarrow$)：即证明只要 Γ, Δ 满足五条限制就可以使 $F(O, \Gamma, \Delta) \in \mathcal{B}(\overline{h}, \sigma)$，考虑对满足条件的生成元验证.

必要性 ($\Rightarrow$)：记 $\mathcal{B}'_n(h, \sigma)$ 表示对于 $\overline{h}, \sigma$ 满足五条限制的算符集合，充分性指出了 $\mathcal{B}'_n(h, \sigma) \subseteq \mathcal{B}_n(h, \sigma)$，于是

$$|\mathcal{C}_n| \leq \sum_{h \in \{0,1\}^n} \sum_{\sigma \in \mathcal{S}_n} \frac{|\mathcal{B}_n|^2}{|\mathcal{B}_n(h, \sigma)|} \leq \sum_{h \in \{0,1\}^n} \sum_{\sigma \in \mathcal{S}_n} \frac{|\mathcal{B}_n|^2}{|\mathcal{B}'_n(h, \sigma)|}$$

High Level Proof of Lemma 1

$$|\mathcal{C}_n| \leq \sum_{h\in\{0,1\}^n} \sum_{\sigma\in\mathcal{S}_n} \frac{|\mathcal{B}_n|^2}{|\mathcal{B}_n(h,\sigma)|} \leq \sum_{h\in\{0,1\}^n} \sum_{\sigma\in\mathcal{S}_n} \frac{|\mathcal{B}_n|^2}{|\mathcal{B}'_n(h,\sigma)|}$$

High Level Proof of Lemma 1

$$|\mathcal{C}_n| \leq \sum_{h\in\{0,1\}^n}\sum_{\sigma\in\mathcal{S}_n}\frac{|\mathcal{B}_n|^2}{|\mathcal{B}_n(h,\sigma)|} \leq \sum_{h\in\{0,1\}^n}\sum_{\sigma\in\mathcal{S}_n}\frac{|\mathcal{B}_n|^2}{|\mathcal{B}'_n(h,\sigma)|}$$

考虑证明右侧等于左侧. 定义 $I_n(h,\sigma)$ 表示 $\overline{h},\sigma$ 给 Γ,Δ 的限制条数, 那么有 $|\mathcal{B}'_n(h,\sigma)| = |\mathcal{B}_n|2^{-I_n(h,\sigma)}$.
可以验证 $I_n(h,\sigma) = \frac{n(n-1)}{2} + |h| + \sum_{1\leq i<j\leq n:\sigma(i)<\sigma(j)}(-1)^{h_i+1}$, 回忆 $|\mathcal{C}_n| = 2^{n^2+2n}\prod_{i=1}^{n}(4^i-1)$ 的, 只需要证明

$$\sum_{h\in\{0,1\}^n}\sum_{\sigma\in\mathcal{S}_n}2^{I_n(h,\sigma)} = \prod_{i=1}^{n}(4^i-1)$$

就可以了, 手段是归纳.

High Level Proof of Lemma 1

$$|\mathcal{C}_n| \le \sum_{h\in\{0,1\}^n} \sum_{\sigma\in\mathcal{S}_n} \frac{|\mathcal{B}_n|^2}{|\mathcal{B}_n(h,\sigma)|} \le \sum_{h\in\{0,1\}^n} \sum_{\sigma\in\mathcal{S}_n} \frac{|\mathcal{B}_n|^2}{|\mathcal{B}'_n(h,\sigma)|}$$

考虑证明右侧等于左侧. 定义 $I_n(h,\sigma)$ 表示 $\overline{h},\sigma$ 给 Γ,Δ 的限制条数, 那么有 $|\mathcal{B}'_n(h,\sigma)| = |\mathcal{B}_n|2^{-I_n(h,\sigma)}$.
可以验证 $I_n(h,\sigma) = \frac{n(n-1)}{2} + |h| + \sum_{1\le i<j\le n:\sigma(i)<\sigma(j)}(-1)^{h_i+1}$, 回忆 $|\mathcal{C}_n| = 2^{n^2+2n}\prod_{i=1}^n(4^i-1)$ 的, 只需要证明

$$\sum_{h\in\{0,1\}^n} \sum_{\sigma\in\mathcal{S}_n} 2^{I_n(h,\sigma)} = \prod_{i=1}^n (4^i-1)$$

就可以了, 手段是归纳. 至于证明 $\mathcal{B}_n(\overline{h},\sigma)\cap\mathcal{B}_n(h,\sigma) = \mathcal{P}_n$, 根据以上等价条件可知 Γ,Δ 需要同时对 (h,σ) 和 $(\overline{h},\sigma)$ 满足限制, 验证这样会使 $\Gamma=\Delta=0^{n\times n}$, 从而使 $F\in\mathcal{P}_n$.

High Level Proof of Lemma 2

Lemma 2

任意算符 $F \in \mathcal{B}_n$ 都可以被唯一写成 $F = F_L F_R$，其中 $F_R \in \mathcal{B}_n(h, \sigma)$，$F_L \in \mathcal{B}_n(\overline{h}, \sigma)$ 且 Pauli 部分是平凡的。

High Level Proof of Lemma 2

Lemma 2

任意算符 $F \in \mathcal{B}_n$ 都可以被唯一写成 $F = F_L F_R$，其中 $F_R \in \mathcal{B}_n(h, \sigma)$，$F_L \in \mathcal{B}_n(\overline{h}, \sigma)$ 且 Pauli 部分是平凡的。

令 $F_1, \cdots, F_m \in \mathcal{B}_n(\overline{h}, \sigma)$ 且 Pauli 部分平凡的全部元素, 验证左陪集 $F_j \mathcal{B}_n(\overline{h}, \sigma)$ 两两不交, 从而说明分解的唯一性.

High Level Proof of Lemma 2

Lemma 2

任意算符 $F \in \mathcal{B}_n$ 都可以被唯一写成 $F = F_L F_R$，其中 $F_R \in \mathcal{B}_n(h, \sigma)$，$F_L \in \mathcal{B}_n(\overline{h}, \sigma)$ 且 Pauli 部分是平凡的。

令 $F_1, \cdots, F_m \in \mathcal{B}_n(\overline{h}, \sigma)$ 且 Pauli 部分平凡的全部元素，验证左陪集 $F_j\mathcal{B}_n(\overline{h}, \sigma)$ 两两不交，从而说明分解的唯一性.

存在性又是考虑对元素计数，想要验证

$$|\mathcal{B}_n(h, \sigma)| \cdot |\mathcal{B}_n(\overline{h}, \sigma)| = |\mathcal{P}_n| \cdot |\mathcal{B}_n| = 4^n|\mathcal{B}_n|$$

注意到 $|\mathcal{B}_n(h, \sigma)| = |\mathcal{B}_n|2^{-I_n(h,\sigma)}$，$I_n(h, \sigma) + I_n(\overline{h}, \sigma) = n^2$ 以及 $|\mathcal{B}_n| = 2^{n^2+2n}$，代入即可直接得到结论.

Part C

利用前面证明的一一对应关系, 现在我们可以通过对 Canonical form 的随机采样来实现对 Clifford group 的随机采样了.

Part C

利用前面证明的一一对应关系, 现在我们可以通过对 Canonical form 的随机采样来实现对 Clifford group 的随机采样了.

采样的过程分为两步, 第一步是采样 $W=\left(\prod_{i=1}^{n} H_i^{h_i}\right)\sigma$, 需要遵循概率分布

$$P_n(h,\sigma)=\frac{|\mathcal{B}_n W\mathcal{B}_n|}{|\mathcal{C}_n|}=\frac{|\mathcal{B}_n|^2}{|\mathcal{B}_n(h,\sigma)|\cdot|\mathcal{C}_n|}=\frac{2^{I_n(h,\sigma)}}{\sum_{h,\sigma}2^{I_n(h,\sigma)}}$$

这个概率分布被称为 quantum Mallows distribution, (可以证明) 对其进行的采样可以被下一页中的算法实现.

Sampling on Quantum Mallows Distribution

$A \leftarrow [1 \ldots n]$
for $i = 1$ to n **do**
    $m \leftarrow |A|$
    Sample $h_i \in \{0, 1\}$ and $k \in [1 \ldots m]$ from the probability distribution

$$p(h_i, k) = \frac{2^{m-1+h_i+(m-k)(-1)^{1+h_i}}}{4^m - 1}$$

    Let j be the k-th largest element of A
    $\sigma(i) \leftarrow j$
    $A \leftarrow A \setminus \{j\}$
end for
return (h, σ)

Clifford Random Sampling

采样的第二步就是根据第一步中得到 h, σ 来采样 Canonical form 中的 $\Gamma, \Delta, \Gamma', \Delta', O$, 其中 Γ, Δ 受到了一定的限制.

[2] 准确来说限制在了 $\mathcal{B}_n/\mathcal{B}_n(h,\sigma) \cong \mathcal{B}_n(\overline{h},\sigma)/\mathcal{P}_n$ 里.

Clifford Random Sampling

采样的第二步就是根据第一步中得到 h, σ 来采样 Canonical form 中的 $\Gamma, \Delta, \Gamma', \Delta', O$, 其中 Γ, Δ 受到了一定的限制.

其实也可以不管这些限制. 通过前面的证明我们可以知道限制本质上是把 $\mathcal{B}_n W \mathcal{B}_n$ 形式中的前一个 $\mathcal{B}_n$ 限制在了一个更小的子群[2], 而 Lagrange 定理 [3] 指出了子群的每个陪集大小都是相同的, 即说明对大群的均匀随机采样也是对子群的均匀随机采样, 因此正确性上是没有问题的, 而且去掉限制以后可以让代码实现变得简短, 唯一的代价是消耗了额外的随机比特.

Qiskit 中所实现的 random_clifford 方法就采用了这种策略.

[2] 准确来说限制在了 $\mathcal{B}_n/\mathcal{B}_n(h,\sigma) \cong \mathcal{B}_n(\overline{h},\sigma)/\mathcal{P}_n$ 里.

Reference

Sergey Bravyi and Dmitri Maslov.
Hadamard-free circuits expose the structure of the clifford group.
IEEE Transactions on Information Theory, 67(7):4546–4563, Jul 2021.

Dmitri Maslov and Martin Roetteler.
Shorter stabilizer circuits via bruhat decomposition and quantum circuit transformations.
IEEE Transactions on Information Theory, 64(7):4729–4738, Jul 2018.

Wikipedia contributors.
Lagrange's theorem (group theory) — Wikipedia, the free encyclopedia.
https://en.wikipedia.org/w/index.php?title=Lagrange%27s_theorem_(group_theory)&oldid=1039199376, 2021.
[Online; accessed 11-December-2021].