CS59200-PRS: Pseudorandomness Nov 12, 2025

Lecture 22: Pseudorandom Unitaries and Clifford Group

Lecturer: Wei Zhan *Scribe: Xiuyu Ye*

1 PRU and Unitary Design

Similar to the fact that the quantum analog of PRG is pseudorandom quantum states, there is also a quantum analog of PRF which maps every quantum state to a random quantum state. In other words, it mimics the behavior of a uniformly random unitary operator.

Definition 1. *The Haar measure over $\mathbb{U}(N)$, for which we abuse the notation and write $U \sim \mathbb{U}(N)$, is the unique measure that is invariant under unitaries, i,e. U is equidistributed with UV and VU for every $V \in \mathbb{U}(N)$.*

Definition 2. *The unitary ensemble $\{U_k\}$ on n qubits is pseudorandom unitaries (PRU), if:*

- *U_k can be efficiently prepared: There exists a classical poly-time algorithm that given $k \in \{0,1\}^\ell$ with $\ell \leq \mathsf{poly}(\lambda)(n)$, output the quantum circuit that implements U_k;*
- *U_k is indistinguishable from Haar random unitary: That is, for $N = 2^n$,*

$$\left| \mathop{\mathbb{E}}_{k\sim\{0,1\}^\ell}[A^{U_k}(|0^n\rangle)] - \mathop{\mathbb{E}}_{U\sim\mathbb{U}(N)}[A^{U}(|0^n\rangle)] \right| \leq \mathsf{negl}(\lambda)(n)$$

for every poly-time quantum oracle distinguisher $A^{U\text{‘}}$.

Similar to the case of PRS, we need a notion of statistical indistinguishability as an intermediate step to show computational indistinguishability. The notion we introduce here is the unitary design.

Definition 3. *The unitary ensemble $\{U_k\}$ on n qubits is a unitary t-design, if*

$$\mathop{\mathbb{E}}_{k\sim\{0,1\}^\ell}[U_k^{\otimes t}\rho U_k^{\dagger\otimes t}] = \mathop{\mathbb{E}}_{U\sim\mathbb{U}(N)}[U^{\otimes t}\rho U^{\dagger\otimes t}]$$

for every density matrix ρ on nt qubits.

Remark. Similar to the state designs, here given the state ρ, the expectation $\mathop{\mathbb{E}}_{U\sim\mathbb{U}(N)}[U^{\otimes t}\rho U^{\dagger\otimes t}]$ can be also exactly computed. Notice that we already know it is contained in $\mathrm{span}(V_\sigma)$ due to the invariance under $U^{\otimes t}$. The coefficients before each V_σ can be computed through Weingarten calculus, which we will not talk about in details here.

Remark. For the same reason that state design is incomparable with PRS, unitary design is also incomparable with PRU. But unitary design has yet another weakness: In the definition of indistinguishability, the unitaries have to be applied in parallel, while for PRU the oracle algorithm A can apply the unitary oracles adaptively. As a result, even if we proved $\{U_k\}$ is a a unitary t-design for some exponentially large t, it does not imply that $\{U_k\}$ is PRU.

2 Pauli and Clifford Groups

2.1 Pauli Group

Definition 4. *The single-qubit Pauli group P is a subgroup of $\mathbb{U}(2)$ generated by the following Pauli operators:*

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

Notice that the Pauli operators are anticommutative: For instance $XY = -YX = iZ$. As a result, P is in fact a order-16 finite group which can be write as $\{I, X, Y, Z\} \otimes \{\pm 1, \pm i\}$.

Another important property of the Pauli operators is the they span the space of single-qubit states. Every density matrix of such a state ρ can be written as

$$\rho = \frac{1}{2}(I + xX + yY + zZ), \text{ where } x, y, z \in \mathbb{R} \text{ and } |x|^2 + |y|^2 + |z|^2 \leq 1.$$

Therefore the space of single-qubit mixed states correspond exactly to the unit sphere in $\mathbb{R}^3$, which is called the *Bloch sphere*. The center of the sphere is the maximally mixed state, and the surface of the sphere contains all pure states.

Example. We have:

$$\begin{aligned} |0\rangle\langle 0| = \frac{1}{2}(I + Z), \quad |1\rangle\langle 1| = \frac{1}{2}(I - Z) \\ |+\rangle\langle +| = \frac{1}{2}(I + X), \quad |-\rangle\langle -| = \frac{1}{2}(I - X) \\ |i\rangle\langle i| = \frac{1}{2}(I + Y), \quad |-i\rangle\langle -i| = \frac{1}{2}(I - Y). \end{aligned}$$

Here $|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$ and $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)$.

On n qubits, the Pauli group is simply the direct products of single qubit Pauli groups:

$$P^{\otimes n} = W_1 \otimes \cdots \otimes W_n, \quad W_i \in P.$$

Each element in $P^{\otimes n}$ is an n-qubit Pauli operator, which is a length-n word with alphabet $\{I, X, Y, Z\}$, together with a global phase in $\{\pm 1, \pm i\}$. As a result, the order of $P^{\otimes n}$ is 4^{n+1}. The n-qubit Pauli operators also spans the space of n-qubit states, and we can write

$$\rho = \sum_{W \in \{I,X,Y,Z\}^{\otimes n}} \widehat{\rho}(W) \cdot W, \quad \widehat{\rho}(W) \in \mathbb{R}$$

for every n-qubit state ρ. This is called *Pauli analysis*, which shares a lot of similarities with Fourier analysis. In fact, Fourier analysis can be viewed as a special case of Pauli analysis on the diagonal where only I and Z are involved.

Example. We have:

$$|00\rangle\langle 00| = \left(\frac{1}{2}(I+Z)\right)^{\otimes 2} = \frac{1}{4}(I\otimes I + I\otimes Z + Z\otimes I + Z\otimes Z),$$

$$|11\rangle\langle 11| = \left(\frac{1}{2}(I-Z)\right)^{\otimes 2} = \frac{1}{4}(I\otimes I - I\otimes Z - Z\otimes I + Z\otimes Z).$$

As a result, the mixing between the two states gives

$$\frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|) = \frac{1}{4}(I\otimes I + Z\otimes Z).$$

2.2 Clifford Group

Definition 5. *The n-qubit Clifford group C_n is defined as the normalizer group of the Pauli group, i.e.*

$$C_n = \{C \in \mathbb{U}(N) \mid CWC^\dagger \in P^{\otimes n}, \forall W \in P^{\otimes n}\}.$$

Here are some examples of elements in the Clifford group:

- The Pauli group $P^{\otimes n}$ itself is contained in the Clifford group;
- Every scalar operator, i.e. ωI_N for $|\omega| = 1$;
- The Hadamard operator $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$. To check this, notice that Hadamard sends $|0\rangle$ to $|+\rangle$ and sends $|+\rangle$ to $|1\rangle$. Therefore with the Pauli expansion of these pure states from the examples above, we know that

  $$HZH^\dagger = X,\ HXH^\dagger = -Z.$$

  Moreover, $H|i\rangle = \frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle = \frac{1+i}{\sqrt{2}}|-i\rangle$, which means that $HYH = -Y$.
- The phase operator $S = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$. We can check that

  $$S|0\rangle = |0\rangle,\ S|+\rangle = |i\rangle,\ S|i\rangle = |-\rangle.$$

- The CNOT gate. We will only check its effect on $Z\otimes Z$, by applying it to the state $\frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$. With half probability, the state is $|00\rangle$ and unchanged under CNOT, and with another half the state is mapped to $\texttt{CNOT}|11\rangle = |10\rangle$. The resulting state is thus

  $$\frac{1}{2}(|00\rangle\langle 00| + |10\rangle\langle 10|) = \frac{1}{2}I\otimes|0\rangle\langle 0| = \frac{1}{4}(I\otimes I + I\otimes Z).$$

  This means that $\texttt{CNOT}(Z\otimes Z)\texttt{CNOT}^\dagger = I\otimes Z$.

Interestingly, the Clifford group can be generated from the above examples. It in fact can be generated by merely H, S, CNOT and scalars. As a result, the set of gates $\{H, S, \texttt{CNOT}\}$ is not a universal gate set. However, it can be made universal by simply adding another gate

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

The normalizer property allows us to characterize the states $C|0^n\rangle$ prepared by Clifford operators $C \in C_n$. We call $W \in P^{\otimes n}$ a *stabilizer* of the state $|\psi\rangle$ if $W|\psi\rangle = |\psi\rangle$, and we have:

Theorem 1. *For every $C \in C_n$, the stabilizers of $C|0^n\rangle$ is a order-2^{n+2} subgroup of $P^{\otimes n}$.*

Proof. For state $|0^n\rangle$, the stabilizers are exactly the subgroup

$$\mathrm{Stab}(|0^n\rangle) = \{I, Z\}^{\otimes n} \otimes \{\pm 1, \pm i\}$$

which has order $4 \cdot 2^n$. Notice that $W \in P^{\otimes n}$ is a stabilizer of $C|0^n\rangle$ if and only if

$$WC|0^n\rangle = C|0^n\rangle \iff C^\dagger WC|0^n\rangle = |0^n\rangle,$$

where $C^\dagger WC \in P^{\otimes n}$ because of the normalizer property. Thus the stabilizers of $C|0^n\rangle$ are $C \cdot \mathrm{Stab}(|0^n\rangle) \cdot C^\dagger$, which is also a subgroup of order $4 \cdot 2^n$. □

Using Theorem 1 we can show that the Clifford group, quotienting the scalar phases, is also finite. In fact we have

$$|C_n / \{\omega I_N\}| \leq 2^{O(n^2)}.$$

Another corollary of Theorem 1 is the Gottesman-Knill theorem:

Theorem 2 ([1, 2])**.** *Clifford circuits can be simulated classically in polynomial time.*

This implies that the advantage of quantum computing does not come from the Clifford group. Since adding the T gate to the Clifford group makes it universal, the "magic" of quantum computing actually lies in the T gates and states prepared by T gates, and they are sometimes called *magic gates* and *magic states*.

3 PFC construction

The Clifford group is still extremely useful in quantum information, due to the fact that it is a discrete subgroup that is also a unitary design.

Theorem 3 ([3])**.** *C_n is a unitary 3-design.*

As an immediate corollary, the states $C|\psi_0\rangle$, prepared by Clifford operators $C \in C_n$ on any fixed initial state $|\psi_0\rangle$, also form a state 3-design. The fact that they are 3-designs (in fact 2-design suffices) implies that with high probability over a random $C \in C_n$, the state $C|\psi_0\rangle$ will have small amplitude in each coordinate and thus is a "flattened" out superposition.

Using the 3-design property of the Clifford group, we can construct higher order designs and PRU through the following PFC construction.

Theorem 4 ([4]). *The PFC unitary ensemble is defined as a product of three random unitaries $P \cdot F \cdot C$, where*

$$P : |x\rangle \mapsto |\pi(x)\rangle$$

for a random permutation π over $\{0,1\}^n$,

$$F : |x\rangle \mapsto (-1)^{f(x)}|x\rangle$$

for a random function $f : \{0,1\}^n \to \{0,1\}$, and C is a random Clifford operator in C_n. Then the PFC ensemble is an ε-approximate unitary t-design for $\varepsilon = O(t/\sqrt{n})$.

Here the approximate unitary design is defined similarly to the approximate state design, but more complicated due to the difference between multiplicative error and additive error, and hence we omit the definition here.

As we remarked earlier, Theorem 4 does not imply PRU property since unitary designs are applied in parallel. Nevertheless, it was proved later that the construction is indeed PRU.

Theorem 5 ([5]). *When instantiated with PRP π and PRF f, the PFC ensemble is a PRU.*

Since post-quantum PRP and PRF are both equivalent to post-quantum OWF, it means that OWF also implies PRU and therefore PRS. Does the inverse also hold, so that they are also equivalent to OWF? It seems that the answer is no. Evidences are given by the oracle separations:

Theorem 6 ([6]). *There exists a classical oracle $\mathcal{O}$, such that $\mathsf{P}^{\mathcal{O}} = \mathsf{NP}^{\mathcal{O}}$, but $PRU^{\mathcal{O}}$ exists, that is, an ensemble $\{U_k\}$ that can be efficiently implemented with access to $\mathcal{O}$, but is indistinguishable from Haar random against any $\mathsf{BQP}^{\mathcal{O}}$ distinguisher.*

In other words, even in a world without OWF (e.g. Impagliazzo's Algorithmica), there likely still exists quantum pseudorandom primitives and therefore cryptography can still be done with the power of quantum computing.

References

[1] Daniel Gottesman. "The Heisenberg representation of quantum computers". In: *arXiv preprint quant-ph/9807006* (1998).

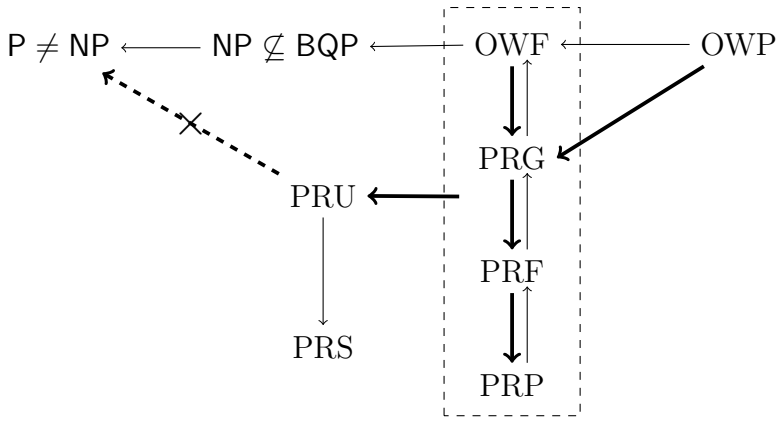

Figure 1: Relations between post-quantum cryptographic primitives. The implication from PRU to $\mathsf{P} \neq \mathsf{NP}$ could not possibly hold in a black-box manner due to [6].

[2] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". In: *Physical Review A—Atomic, Molecular, and Optical Physics* 70.5 (2004), p. 052328.

[3] Zak Webb. "The Clifford group forms a unitary 3-design". In: *arXiv preprint arXiv:1510.02769* (2015).

[4] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. "Simple constructions of linear-depth t-designs and pseudorandom unitaries". In: *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE. 2024, pp. 485–492.

[5] Fermi Ma and Hsin-Yuan Huang. "How to construct random unitaries". In: *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*. 2025, pp. 806–809.

[6] William Kretschmer, Luowen Qian, and Avishay Tal. "Quantum-computable one-way functions without one-way functions". In: *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*. 2025, pp. 189–200.