

# State Synthesis Using PRS.

David Ponarovsky

September 19, 2023

## Abstract

We studies the complexity of synthesis quantum states using PRS, our reasch continues the work by [Ira+22], [Ros23], [RY21], [MY23], [Del+23].

## 1 Pseudorandomness.

**Definition 1.1** (Pseudorandom Quantum states). *Let  $\mathcal{H}, \mathcal{K}$  be the Hilbert and the key spaces, their diminsions depeand on a security paramter  $n$ . A state famliiy  $\{|\psi_k\rangle\}_{k \in \mathcal{K}}$  is a pseudiorandom, if the following hold:*

1. *Efficient generation. There is a polynomial-time quantum algorithm  $G$  that generates state  $|\psi_k\rangle$  on input  $k$ .*
2. *Pseudorandomness. Any polynomially many copies of  $|\phi_k\rangle$  with the same random  $k \in K$  is computationally indistinguishable from the same number of copies of the Haar random state.*

**Definition 1.2** (Pseudorandom Unitary Operators). *A famliiy of unitary operators  $\{U_k \in U(\mathcal{H})\}_{k \in \mathcal{K}}$  is pseudorandom, if two conditions hold:*

1. *Efficient computation. There is an efficient quantum algorithm  $Q$ , such that for all  $k$  and any  $|\psi\rangle \in \mathcal{H}$   $Q(k, |\psi\rangle) = U_k |\psi\rangle$ .*
2. *Pseudorandomness. The uniform random distribution on  $U_k$  is computationally in distinguishable from a Haar random unitary operator.*

**Definition 1.3** (The keeping setting). *Let  $R^A \otimes R^B$  be a general two registers domain. We define the **keeping setting** to let one construct quntum/classical circuits<sup>1</sup>  $G : R^A \otimes R^B \rightarrow R^A \otimes R^B$  such that it is gurnted that the register  $R^B$  can't be accsed after the computation.*

**Claim 1.1.** *Let  $G$  be a PRS generator, than under the the keeping setting one can assume that  $G$  takes as input two register, the first contains  $n$  ancille qubits initiliaized to  $|0\rangle$  and the seconed contain a classic string initiliezied to be the seed  $k$ .*

*Proof.* Given a PRS  $G : R^A \rightarrow R^A$  define  $\tilde{G} : R^A \otimes R^B \rightarrow R^A \otimes R^B$  as follow, first  $\tilde{G}$  copy the calscial state in  $R^B$  (the  $k$ -length seed) to  $R^A$  and then appaly  $G$  on  $R^A$ , Hence on sampled seed  $k \in R^B$  results the output  $|\psi_k\rangle \otimes |k\rangle$ . Under the keeping setting any polynomial distinguishier-canidate  $D$  has accses only for  $|\psi_k\rangle$ , So if  $D$  distinguish between the distrubition generated by  $\tilde{G}$  and the Haar measure then it also distinguish between  $G$  and Haar measure.  $\square$

**Claim 1.2.** *Let  $G : |0\rangle^n \otimes \mathbb{F}_2^k \rightarrow \{|\psi_k\rangle\}_{k \in \mathcal{K}}$  be a PRS generator uses  $n$ - ancilles and  $k$  classicl bits. Then for any unitery  $V : \mathcal{H}_n \rightarrow \mathcal{H}_n$  it holds that  $(V \otimes I^{\otimes k})G$  is also a PRS.*

*Proof.*  $\square$

---

<sup>1</sup>On which we think as a canidate for PRS/PRF/PRG generator.

**Claim 1.3** (Levi's Lemma for PRS). *Let  $f : \mathcal{H} \rightarrow \mathbb{R}$  be a **BQP**-computable function on the  $n$ -qubits Hilbert space, and let  $g : (0, 1) \rightarrow \mathbb{R}$  be a function such that:*

$$\Pr_{|\psi\rangle \sim U} [f(|\psi\rangle) > \varepsilon] < g(\varepsilon)$$

*Then, a similar inequality also holds for states sampled by the PRS, when the probability for the measure  $f$ -value greater than  $\varepsilon$  is bounded by  $g(2\varepsilon)$ . Namely,*

$$\Pr_{|\psi\rangle \sim |\psi_k\rangle} [f(|\psi\rangle) > \varepsilon] < g(2\varepsilon)$$

*In particular, Levi's lemma has a version that captures concentration of states sampled by PRS generator, states the following: Assume there exists  $K$  such that for any  $|\psi\rangle, |\phi\rangle \in \mathcal{S}(\mathbb{C}^d)$   $|f(|\psi\rangle) - f(|\phi\rangle)| < K||\psi\rangle - |\phi\rangle|$ . Then there exists a universal constant  $C > 0$  such:*

$$\Pr_{|\psi\rangle \sim |\psi_k\rangle} [|f(|\psi\rangle) - \mathbf{E}_{|\phi\rangle \sim U} [f(|\phi\rangle)]| > \varepsilon] < \exp\left(-\frac{Cd}{K^2}4\varepsilon^2\right)$$

*Proof.* □

**Claim 1.4.** *Probabilistic counting argument and  $\varepsilon$ -net over PRS.*

**Claim 1.5.** *existence of  $\text{poly}(n)$  gates  $G_1, G_2, \dots$  such that, any  $G_i$  has a polynomial depth,  $\langle p(G_i) | \tau \rangle > a$  and  $\langle \tau^\perp | p(G_j) \rangle \langle p(G_i) | \tau^\perp \rangle < b$  for any  $i \neq j$ .*

*Proof.* □

**Claim 1.6.** *bla bla bla*

**Definition 1.4.**  $\varepsilon$ -biased test 2-degree for testing RPU/RPS.  $f(\langle x_j | G_s | \theta \rangle) = 1$  For example ask if  $\langle \psi_j, \tau^\perp \rangle \langle \tau^\perp | \psi_j \rangle$  what I can say about that quantity as polynomial?

## 2 What We Need for Synthesis.

**Definition 2.1** (Pseudorandom Unitary for Synthesis). *A family of unitary operators  $\{U_k \in U(\mathcal{H})\}_{k \in \mathcal{K}}$  is pseudorandom for synthesis, if two conditions hold:*

1. *Efficient computation.* There is an efficient quantum algorithm  $Q$ , such that for all  $k$  and any  $|\psi\rangle \in \mathcal{H}$   $Q(k, |\psi\rangle) = U_k |\psi\rangle$ .
2. *Pseudorandomness for synthesis.* Given a state  $|\tau\rangle$  and polynomial number of samples  $U_1, U_2, \dots, U_m$ . Then:

$$(a) \quad |\langle \Phi(\tau, U_k) | U_k \tau \rangle|^2 > a$$

$$(b) \quad |\langle \Phi(\tau, U_k) | U_k \tau^\perp \rangle \langle \tau^\perp | U_j^\dagger | \Phi(\tau, U_j) \rangle|^2 < b$$

*The uniform random distribution on  $U_k$  is computationally indistinguishable from a Haar random unitary operator.*

What about, Assume that  $U$  is a quantum circuit such that  $\log n$  qubits are initialized to some state and instead ancilla, we have noisy ancilla, can we show that circuit is equivalent to  $\log n$  circuit? That will enable us to prove a quantum version for Nisan Wigderson PRG (BPP = P).

**Problem.** Let  $U$  be a quantum circuit which get  $\log n$  stable qubits and  $\text{poly}(n)$  more random qubits obtained from the random Haar measure, can we simulate the circuit in  $\log n$  time?

approximate the absolute value function, For example, you can consider the binomial expansion of  $\sqrt{1-y}$  on  $[0, 1]$ . Namely, setting  $y = 1 - x^2$ , we have  $|x| = \sqrt{1-y} = \sum_{m=0}^{\infty} \binom{1/2}{m} (-y)^m$ ,  $x \in [-1, 1]$ . That will allow me to bound the  $k$ -design.

Denote by  $q_d(x)$  the  $d$ -order approximation of  $|x|$ , Namely

$$q_d(x) = \sum_{m=0}^d \binom{1/2}{m} (-1)^m (1 - x^2)^m$$

and as the series converges to any  $x \in (-1, 1)$  we have that  $|x| = q_d(x) + O(\binom{1/2}{d} (1 - x^2)^d)$  which by the fact that  $1 - x^2 \in (-1, 1)$  can be simplified to  $|x| = q_d(x) + O(\binom{1/2}{d}) = q_d(x) + O(1/d^{1+1/2})$ .

$$\begin{aligned} \mathbf{E}_{U \sim D} [(\langle \Phi(\tau, U) | \text{Re } U\tau \rangle)^2] &= \mathbf{E}_{U \sim D} \left[ \frac{1}{2^{n/2}} \sum_x (-1)^{\text{sign}(\text{Re}(x|U\tau))} \text{Re} \langle x|x \rangle \langle x|U\tau \rangle \right] \\ &= \mathbf{E}_{U \sim D} \left[ \frac{1}{2^{n/2}} \sum_x |\text{Re} \langle x|U\tau \rangle| \right] \\ &\geq \mathbf{E}_{U \sim D} \left[ \frac{1}{2^{n/2}} \sum_x |\text{Re} \langle x|U\tau \rangle| \right] \end{aligned}$$

## References

- [RY21] Gregory Rosenthal and Henry Yuen. *Interactive Proofs for Synthesizing Quantum States and Unitaries*. 2021. arXiv: [2108.07192 \[quant-ph\]](#).
- [Ira+22] Sandy Irani et al. “Quantum Search-To-Decision Reductions and the State Synthesis Problem”. en. In: Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. DOI: [10.4230/LIPICS.CCC.2022.5](#). URL: <https://drops.dagstuhl.de/opus/volltexte/2022/16567/>.
- [Del+23] Hugo Delavenne et al. *Quantum Merlin-Arthur proof systems for synthesizing quantum states*. 2023. arXiv: [2303.01877 \[quant-ph\]](#).
- [MY23] Tony Metger and Henry Yuen. *stateQIP = statePSPACE*. 2023. arXiv: [2301.07730 \[quant-ph\]](#).
- [Ros23] Gregory Rosenthal. *Efficient Quantum State Synthesis with One Query*. 2023. arXiv: [2306.01723 \[quant-ph\]](#).