# State Synthesis Using PRS.

David Ponarovsky

September 20, 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 famliy $\{|\psi_k\rangle\}_{k \in \mathcal{K}}$ 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 computationaly indistinguishable from the same number of copies of the Haar random state.*

**Definition 1.2** (Pseudorandom Unitary Operators). *A famliy 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[1] $G : R^A \otimes R^B \to R^A \otimes R^B$ such that it is gurnted that the register $R^B$ cann't be acssed 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 initiliazied to $|0\rangle$ and the seconed contain a classic string initiliezed to be the seed $k$.*

*Proof.* Given a PRS $G : R^A \to R^A$ define $\tilde{G} : R^A \otimes R^B \to R^A \otimes R^B$ as follow, first $\tilde{G}$ copy the calsical 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 distingushier-canidate $D$ has acsses only for $|\psi_k\rangle$, So if $D$ distinguish between the distrubition generated by $\tilde{G}$ and the Haar measure then it also distingush between $G$ and Haar measure. $\square$

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

*Proof.* $\square$

---

[1]On which we think as a canidate for PRS/PRF/PRG generator.

**Claim 1.3** (Levis Lemma for PRS). *Let $f : \mathcal{H} \to R$ be a **BQP**-computible fuction on the n-qubits hilbert space, and let $g : (0,1) \to \mathbb{R}$ a function such that:*

$$\mathbf{Pr}_{|\psi\rangle \sim U} \left[ f\left(|\psi\rangle\right) > \varepsilon \right] < g(\varepsilon)$$

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

$$\mathbf{Pr}_{|\psi\rangle \sim |\psi_k\rangle} \left[ f\left(|\psi\rangle\right) > \varepsilon \right] < g(2\varepsilon)$$

*In praticular, Levi's lemma has a version that capture consetration of states sampled by PRS generator, states the following: Assume there exsists $K$ 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 exsists a universal constant $C > 0$ such:*

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

*Proof.* $\square$

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

**Claim 1.5.** *exsistness of poly(n) gates $G_1, G_2..$ 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.* $\square$

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

**Definition 1.4.** *$\varepsilon$-bised 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 quantenty as polynomail?.*

# 2 What We Need for Synthesis.

**Definition 2.1** (Pseudorandom Unitary for Synthesis). *A famliy 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 $U_1, U_2..U_m$. Then:*

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

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

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

What about, Assume that $U$ is a quantum circuit such that $\log n$ qubits are intilaized to some to some input and instead anciles, we have noisy ancilea, can we show that circuit is equavilanent to $\log n$ circuit? That will enable us to prove a quantum version for Nisan Wigerzdon PRG (BPP = P).

**Problem.** Let $U$ be a quntum circuit which get $\log n$ stable qubits and $\text{poly}(n)$ more random qubits obtained from the random Haar masure, 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 $|x| = \sqrt{1-y} = \sum_{m=0}^{\infty} \binom{1/2}{m}(-y)^m, \quad x \in [-1,1]$. That will allow me to bound the $k$-design.

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

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

and as the series is convergres 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 simpllified to $|x| = q_d(x) + O(\binom{1/2}{d}) = q_d(x) + O(1/d^{1+1/2})$.

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

$$
= \mathbf{E}_{U \sim D}\left[\frac{1}{2^{n/2}}\sum_x |\operatorname{Re}\langle x|U\tau\rangle|\right]
$$

$$
= \mathbf{E}_{U \sim D}\left[\sum_x |\operatorname{Re}\langle x|U\tau\rangle/2^{n/2}|\right]
$$

$$
\geq \mathbf{E}_{U \sim D}\left[\sum_x q_d\left(\operatorname{Im}\langle x|U\tau\rangle|/2^{n/2}\right) - \binom{1/2}{d}\left(\frac{|\operatorname{Im}\langle x|U\tau\rangle|}{2^{n/2}}\right)^d\right]
$$

$$
\geq \mathbf{E}_{U \sim Haar}\left[\sum_x q_d\left(\operatorname{Im}\langle x|U\tau\rangle|/2^{n/2}\right) - \binom{1/2}{d}\left(\frac{|\operatorname{Im}\langle x|U\tau\rangle|}{2^{n/2}}\right)^d\right] - \delta \cdot 2^n
$$

$$
\geq \mathbf{E}_{U \sim Haar}\left[\sum_x |\operatorname{Re}\langle x|U\tau\rangle/2^{n/2}| - \mathbf{2} \cdot \binom{1/2}{d}\left(\frac{|\operatorname{Im}\langle x|U\tau\rangle|}{2^{n/2}}\right)^d\right] - \delta \cdot 2^n
$$

$$
\sim \mathbf{E}_{U \sim Haar}\left[\sum_x |\operatorname{Re}\langle x|U\tau\rangle/2^{n/2}|\right] - \delta \cdot 2^n
$$

$$
\mathbf{E}_{U,U_2 \sim D}\left[\langle\Phi(\tau,U)|U\tau^\perp\rangle\langle\tau^\perp U_2^\dagger|\Phi(\tau,U_2)\rangle\right] =
$$

**Claim 2.1.** *fix a state $|\tau\rangle$. Let $U$ be a unitary sampled from $k$-design distribution $D$ and denote by $|s\rangle$ the vector which $U$ sends $|\tau\rangle$ to. Now, observes that $U$ can be written as $U = |s\rangle\langle\tau| + V$ when $V$ act on space ortogonal to $|\tau\rangle$ denote it by $|\tau^\perp\rangle$. Then the distribuation over $V$ is also a $k$-design relative to the Haar mesure on $|\tau^\perp\rangle$.*

*Proof.* □

**Claim 2.2.** $|\langle\Phi(\tau,U_k)|U_k\tau^\perp\rangle\langle\tau^\perp U_j^\dagger|\Phi(\tau,U_j)\rangle|^2 < b$

*Proof.*

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

□

# 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].