State Synthesis Using PRS.

David Ponarovsky

September 28, 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 depend on a security parameter 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 circuits¹ $G: R^A \otimes R^B \to R^A \otimes R^B$ 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 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 initilized 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.

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 classic bits. Then for any unitary $V: \mathcal{H}_n \to \mathcal{H}_n$ it holds that $(V \otimes I^{\otimes k})G$ is also a PRS.

Proof.	
	٦

¹On 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 function 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 ε 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:

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

Proof.

Claim 1.4. Probablisite counting argument and ε -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 $\langle \tau^{\perp}|p(G_i)\rangle \langle p(G_i)|\tau^{\perp}\rangle < b$ for any $i \neq j$.

Claim 1.6. bla bla bla

Definition 1.4. ε -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 $\operatorname{poly}(n)$ more random qubits obtained from the random Haar masure, can we simulate the circuit in $\log n$ time?

approximate the absoulte 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

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

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 simplified to $|x| = q_d(x) + O(\binom{1/2}{d}) = q_d(x) + O(1/d^{1+1/2})$.

$$\begin{split} \mathbf{E}_{U \sim D} \left[(\langle \Phi(\tau, U) | \operatorname{Re} U\tau \rangle)^2 \right] &= \mathbf{E}_{U \sim D} \left[\frac{1}{2^{n/2}} \sum_x (-1)^{\operatorname{sign}(\operatorname{Re}\langle x | U\tau \rangle)} \operatorname{Re} \langle x | x \rangle \langle x | U\tau \rangle \right] \\ &= \mathbf{E}_{U \sim D} \left[\frac{1}{2^{n/2}} \sum_x |\operatorname{Re} \langle x | U\tau \rangle | \right] \\ &= \mathbf{E}_{U \sim D} \left[\sum_x |\operatorname{Re} \langle x | U\tau \rangle / 2^{n/2} | \right] \\ &\geq \mathbf{E}_{U \sim D} \left[\sum_x q_d \left(\operatorname{Im} \langle x | U\tau \rangle | / 2^{n/2} \right) - \binom{1/2}{d} \left(\frac{|\operatorname{Im} \langle x | U\tau \rangle|}{2^{n/2}} \right)^d \right] \\ &\geq \mathbf{E}_{U \sim Haar} \left[\sum_x q_d \left(\operatorname{Im} \langle x | U\tau \rangle | / 2^{n/2} \right) - \binom{1/2}{d} \left(\frac{|\operatorname{Im} \langle x | U\tau \rangle|}{2^{n/2}} \right)^d \right] - \delta \cdot 2^n \\ &\geq \mathbf{E}_{U \sim Haar} \left[\sum_x |\operatorname{Re} \langle x | U\tau \rangle / 2^{n/2} | - \mathbf{2} \cdot \binom{1/2}{d} \left(\frac{|\operatorname{Im} \langle x | U\tau \rangle|}{2^{n/2}} \right)^d \right] - \delta \cdot 2^n \\ &\sim \mathbf{E}_{U \sim Haar} \left[\sum_x |\operatorname{Re} \langle x | U\tau \rangle / 2^{n/2} | - \delta \cdot 2^n \right] \\ &= \mathbf{E}_{U,U_2 \sim D} \left[\langle \Phi(\tau, U) | U\tau^{\perp} \rangle \langle \tau^{\perp} U_2^{\dagger} | \Phi(\tau, U_2) \rangle \right] = \end{split}$$

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 distribution over V is also a k-design relative to the Haar mesure on $|\tau^{\perp}\rangle$.

Proof.

Definition 2.2. Denote by

$$M(\tau, U)(x) = \max \{ |\operatorname{Re} \langle x|U\tau\rangle|, |\operatorname{Im} \langle x|U\tau\rangle| \}$$

$$\bar{M}(\tau, U)(x) = \min \{ |\operatorname{Re} \langle x|U\tau\rangle|, |\operatorname{Im} \langle x|U\tau\rangle| \}$$

When it will be clear form the context we omit τ , U and use only M(x), $\bar{M}(x)$.

$$|\langle \Phi(\tau, U)|U\phi\rangle|^2 = |\langle \Phi(\tau, U)|\operatorname{Re} U\phi\rangle|^2 + |\langle \Phi(\tau, U)|\operatorname{Im} U\phi\rangle|^2$$

$$\begin{split} \langle \Phi(\tau, U_k) | M U_k \phi \rangle &= \sum_x \left(-1 \right)^{\operatorname{sign} M(\langle x | U \tau \rangle)} \frac{1}{2^{n/2}} \left\langle x | U \phi \right\rangle \\ &= \sum_{\tau, \phi \text{ agree on } x} \left| \frac{1}{2^{n/2}} M \left(\langle x | U \phi \rangle \right) \right| - \sum_{\tau, \phi \text{ disagree on } x} \left| \frac{1}{2^{n/2}} M \left(\langle x | U \phi \rangle \right) \right| \\ &\approx \sum_{\tau, \phi \text{ agree on } x} q_d \left(\frac{1}{2^{n/2}} \bar{M} \left(\langle x | U \phi \rangle \right) \right) - \sum_{\tau, \phi \text{ disagree on } x} q_d \left(\frac{1}{2^{n/2}} \bar{M} \left(\langle x | U \phi \rangle \right) \right) \pm 2^n \zeta_d \left(\frac{1}{2^{n/2}} \right) \end{split}$$

noitce that we obtained a d-degree polinomial, denote it by T_{ϕ}

$$\begin{split} | \left\langle \Phi(\tau, U) | MU\phi \right\rangle | \approx & q_{d'} \left(\left\langle \Phi(\tau, U) | U\phi \right\rangle \right) + \zeta_{d'} \left(\left\langle \Phi(\tau, U) | U\phi \right\rangle \right) \\ \approx & q_{d'} \left(\left\langle \Phi(\tau, U) | U\phi \right\rangle \right) + \zeta_{d'} \left(\left\langle \Phi(\tau, U) | U\phi \right\rangle \right) \\ \approx & q_{d'} \left(T_{\phi} \right) + \zeta_{d'} \left(T_{\phi} \right) \\ \approx & q_{d'} \left(T_{\phi} \right) + \zeta_{d'} \left(T_{\phi} \right) \end{split}$$

Assume that our k-design collection is defined such that for any $|\varphi\rangle$ it holds that:

$$\mathbf{Pr}_{U_1,U_2\sim D}\left[\operatorname{sign}(\operatorname{Re}\langle x|U_1\varphi\rangle) = \operatorname{sign}(\operatorname{Re}\langle x'|U_2\varphi\rangle)\right] = \frac{1}{2}$$

Claim 2.2. left $f: N \to \{\pm\}$ then the set $(-1)^{f(x)} |x\rangle \langle x| U$ is a k-design. Proof.

$$tr\left(U'V'^{\dagger,\dagger}\right) = tr\left((-1)^{f(x)} |x\rangle \langle x| UV^{\dagger}(-1)^{f(x)} |x\rangle \langle x|\right)$$
$$= tr\left((-1)^{f(y)} |y\rangle \langle y| (-1)^{f(x)} |x\rangle \langle x| UV^{\dagger}\right) = tr(UV^{\dagger})$$

So, we get that:

$$\frac{1}{|X|'^{2}} \sum_{U,V \in X'} |tr(UV^{\dagger})|^{2t} = \frac{1}{|X|^{2}} \sum_{U,V \in X} |tr(UV^{\dagger})|^{2t}$$
$$= \int |tr(U)|^{2t} dU$$

Ok the tactics is going to be the follow, we need the k-design property only for the first stage. When we want to show that $|\Phi\rangle$ has an overlap with $|\tau\rangle$ after that, we can give up on that assumption and by using f, g universal we can ensure a small overlap between pair of different U, V.

Claim 2.3. Assume f above sampled from a universal femily hash functions. Then we have that:

$$\mathbf{E}_{U,V \sim X,f \sim \mathcal{H}} \left[|\langle \Phi(\tau,V)V^{\dagger} | \psi \rangle \langle \psi | U \Phi(\tau,U) \rangle|^{2} \right] \approx_{\delta} \mathbf{E}_{U,V \sim Haar} \left[|\langle \Phi(\tau,V)V^{\dagger} | \psi \rangle \langle \psi | U \Phi(\tau,U) \rangle|^{2} \right]$$
Proof.

$$\begin{split} \langle \Phi(\tau,V) V^{\dagger} | \psi \rangle &= \frac{1}{2^{n/2}} \sum_{x} (-1)^{\operatorname{sign}(\operatorname{Re}\langle x|V|\tau\rangle)} \langle x|V\psi \rangle \\ &= \frac{1}{2^{n/2}} \sum_{x} (-1)^{f(x) + \operatorname{sign}(\operatorname{Re}\langle x|V|\tau\rangle)} \langle x|V'\psi \rangle \\ &= \frac{1}{2^{n/2}} \sum_{x} (-1)^{f(x) + f(x) \cdot \operatorname{sign}(\operatorname{Re}\langle x|V'|\tau\rangle)} \langle x|V'\psi \rangle \\ &= \frac{1}{2^{n/2}} \sum_{x} (-1)^{f(x)(1 + \operatorname{sign}(\operatorname{Re}\langle x|V'|\tau\rangle))} \langle x|V'\psi \rangle \\ &= \frac{1}{2^{n/2}} \sum_{x} (-1)^{f(x)(1 + \operatorname{sign}(\operatorname{Re}\langle x|V'|\tau\rangle))} \langle x|V'\psi \rangle \end{split}$$

$$\Rightarrow \langle \Phi(\tau, V) V^{\dagger} | \psi \rangle \langle \psi | U \Phi(\tau, U) \rangle$$

$$= \frac{1}{2^{n}} \sum_{x, x'} (-1)^{g(x') + f(x) + \operatorname{sign}(\operatorname{Re}\langle x | V | \tau \rangle) + \operatorname{sign}(\operatorname{Re}\langle x' | U | \tau \rangle)}.$$

$$\cdot \langle x | V' \psi \rangle \langle x' | U' \psi \rangle$$

$$\Rightarrow | \langle \Phi(\tau, V) V^{\dagger} | \psi \rangle \langle \psi | U \Phi(\tau, U) \rangle |^{2}$$

$$= \frac{1}{2^{2n}} \sum_{y, y', x, x'} (-1)^{g(x') + f(x) + \operatorname{sign}(\operatorname{Re}\langle x | V | \tau \rangle) + \operatorname{sign}(\operatorname{Re}\langle x' | U | \tau \rangle)}.$$

$$\cdot \langle y | V' \psi \rangle \langle y' | U' \psi \rangle \cdot$$

$$\cdot (-1)^{g(y') + f(y) + \operatorname{sign}(\operatorname{Re}\langle y | V | \tau \rangle) + \operatorname{sign}(\operatorname{Re}\langle y' | U | \tau \rangle)}.$$

$$\cdot \langle y | V' \psi \rangle^{*} \langle y' | U' \psi \rangle^{*}$$

$$\mathbf{E}_{U, V \sim X, f, g \sim \mathcal{H}^{2}} \left[| \langle \Phi(\tau, V) V^{\dagger} | \psi \rangle \langle \psi | U \Phi(\tau, U) \rangle |^{2} \right]$$

$$\mathbf{E}_{U, V \sim X, f, g \sim \mathcal{H}^{2}} \left[| \langle \varphi V', ^{\dagger} | x \rangle \langle x | U' \varphi \rangle |^{2} \right]$$

$$= \mathbf{E}_{U, V \sim X, f, g \sim \mathcal{H}^{2}} \left[| \langle y | U' | \phi \rangle^{*} \langle y' | V^{\dagger}, ' | \phi \rangle^{*} \langle x | U' | \phi \rangle \langle x' | V^{\dagger}, ' | \phi \rangle \right]$$

$$= \mathbf{E}_{U, V \sim X, f, g \sim \mathcal{H}^{2}} \left[(-1)^{f(x) + g(x') + f(y) + g(y')} \langle y | U | \phi \rangle^{*} \langle y' | V | \phi \rangle^{*} \langle x | U | \phi \rangle \langle x' | V | \phi \rangle \right]$$

$$\leq \frac{2^{n}}{3^{2n}} = \frac{1}{2^{n}}$$

Claim 2.4. $|\langle \Phi(\tau, U_k)|U_k\tau^{\perp}\rangle \langle \tau^{\perp}U_j^{\dagger}|\Phi(\tau, U_j)\rangle|^2 < b$

Proof.

$$\begin{split} &\mathbf{E}_{U \sim D} \left[| \left\langle \Phi(\tau, U_k) | U_k \tau^{\perp} \right\rangle \left\langle \tau^{\perp} U_j^{\dagger} | \Phi(\tau, U_j) \right\rangle |^2 \right] \\ \leq &\mathbf{E}_{U \sim D} \left[| \left\langle \Phi(\tau, U_k) | U_k \tau^{\perp} \right\rangle |^2 \cdot | \left\langle \tau^{\perp} U_j^{\dagger} | \Phi(\tau, U_j) \right\rangle |^2 \right] \\ =&\mathbf{E}_{U \sim D} \left[| \left\langle \Phi(\tau, U_k) | U_k \tau^{\perp} \right\rangle |^2 \right]^2 \\ =&\mathbf{E}_{U \sim D} \left[| \sum_x \left\langle x U_k \tau^{\perp} \right\rangle |^2 \right]^2 \\ =&\mathbf{E}_{U \sim D} \left[\sum_x | \left\langle x | U_k \tau^{\perp} \right\rangle |^2 \right]^2 \end{split}$$

3 The Distillation.

suppose that for any $|\psi_i^{(k)}\rangle$, $|\psi_j^{(k)}\rangle$ it holds that: $|\langle \psi_i^{(k)}|\psi_j^{(k)}\rangle| < \exp(-n)$. After conditional swap the normalized state has the form:

$$|\psi_i^{(k)}\rangle\,|\psi_j^{(k)}\rangle\,+\,|\psi_j^{(k)}\rangle\,|\psi_i^{(k)}\rangle\,\mapsto\,\frac{|\psi_i^{(k)}\rangle\,|\psi_j^{(k)}\rangle\,+\,|\psi_j^{(k)}\rangle\,|\psi_i^{(k)}\rangle}{\sqrt{2+2|\langle\psi_i^{(k)}|\psi_j^{(k)}\rangle}|^2}$$

So

$$\begin{split} |\left<\psi_i^{(k+1)}|\psi_t^{(k+1)}\right>| = &|\frac{\left<\psi_i^{(k)}|\left<\psi_j^{(k)}|+\left<\psi_j^{(k)}|\left<\psi_i^{(k)}\right|\right|}{\sqrt{2+2|\left<\psi_i^{(k)}|\psi_j^{(k)}\right>|^2}} \cdot \frac{|\psi_t^{(k)}\rangle|\psi_s^{(k)}\rangle+|\psi_s^{(k)}\rangle|\psi_t^{(k)}\rangle}{\sqrt{2+2|\left<\psi_t^{(k)}|\psi_s^{(k)}\rangle|^2}}|\\ \leq &\frac{1}{2+2exp(-2n)} \cdot \sum_{\{v,u\}=\{i,j\},\{v',u'\}=\{t,s\}} |\left<\psi_v^{(k)}|\psi_{v'}^{(k)}\rangle\left<\psi_u^{(k)}|\psi_{u'}^{(k)}\rangle\right|\\ \leq &\frac{1}{2+2exp(-2n)} \cdot 4exp(-2n) \end{split}$$

$$\begin{split} |\frac{1+|\langle\psi_{j}^{(k)}|\psi_{i}^{(k)}\rangle|^{2}}{\sqrt{2+2|\langle\psi_{i}^{(k)}|\psi_{j}^{(k)}\rangle|^{2}}}\,\langle\psi_{i}^{(k)}|\cdot\frac{1+|\langle\psi_{s}^{(k)}|\psi_{t}^{(k)}\rangle|^{2}}{\sqrt{2+2|\langle\psi_{t}^{(k)}|\psi_{s}^{(k)}\rangle|^{2}}}|\psi_{t}^{(k)}\rangle\,|\\ \leq&\frac{1}{2}\sqrt{1+|\langle\psi_{j}^{(k)}|\psi_{i}^{(k)}\rangle|^{2}}\sqrt{1+|\langle\psi_{s}^{(k)}|\psi_{t}^{(k)}\rangle|^{2}}\cdot|\langle\psi_{i}^{(k)}|\psi_{t}^{(k)}\rangle\,|}\\ \leq&\frac{1}{2}\left(1+exp(-2n)\right)|\langle\psi_{i}^{(k)}|\psi_{t}^{(k)}\rangle\,|\leq&\frac{1}{2}\left(exp(-n)+exp(-3n)\right) \end{split}$$

$$\langle \psi_i^{(k)} | \, \frac{|\psi_i^{(k)}\rangle\,|\psi_j^{(k)}\rangle + |\psi_j^{(k)}\rangle\,|\psi_i^{(k)}\rangle}{\sqrt{2+2|\,\langle\psi_i^{(k)}|\psi_j^{(k)}\rangle}|^2}$$

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].