

State Synthesis Using PRS.

David Ponarovsky

September 17, 2023

Abstract

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

Definition 0.1 (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 $G : R^A \otimes R^B \rightarrow R^A \otimes R^B$ such that it is gurnted that the register R^B can't be accsed after the computation.*

Claim 0.1. *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 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 distingushier-candidate D has accses only for $|\psi_k\rangle$, So if D distinguish between the distrubution generated by \tilde{G} and the Haar measure then it also distingush between G and Haar measure. \square

Claim 0.2. *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

Claim 0.3 (Levis Lemma for PRS). *Let $f : \mathcal{H} \rightarrow \mathbb{R}$ be a **BQP**-computible fuction on the n -qubits hilbert space, and let $g : (0, 1) \rightarrow \mathbb{R}$ 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 grater than ε is bounded by $g(2\varepsilon)$. Namely,

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

In praticular, Levi's lemma has a version that capture consetration of states sampled by PRS generator, states the following: Assume there 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. \square

Claim 0.4. *Probablisitc counting argument and ε -net over PRS.*

Claim 0.5. *exsistness of $\text{poly}(n)$ 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 0.6. *bla bla bla*

Definition 0.2. ε -bised test 2-degree for testing RPU/RPS. $f(\langle \theta | G_s | \theta \rangle) = 1$.

¹On which we think as a candidate for PRS/PRF/PRG generator.

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 \[quant-ph\]](#).