ANNOTATIONS ON QUANTUM PSEUDORANDOMNESS AND k-DESIGNS

EDWARD KIM

ABSTRACT. We investigate constructions of efficient approximate unitary k-designs or distributions over the unitary group which model the Haar distribution up to the k^{th}-moment. In particular, we review the paper by Harrow and Low as a directed reading conducted during the Spring 2020 semester.

CONTENTS

1. INTRODUCTION

The power of randomness in computation is a cornerstone of contemporary computation theory as evidenced by decades of beautiful, celebrated results. Quantum Information is, by no means, a stranger to this trend. Numerous applications of random unitaries have been discovered in the areas of quantum tomography, cryptography, and, rather naturally, randomized algorithms. To gain access to uniformly-sampled elements from $\mathbb{U}(d)$, one must sample from the Haar distribution over $\mathbb{U}(d)$ where $\mathbb{U}(d)$ denotes the group of unitary $d \times d$ matrices. One method of sampling from the Haar distribution is to apply local random unitaries sampled from distributions over lower-dimensional unitary groups. For example, if we consider an n-qubit system, one method of sampling from the Haar distribution over $\mathbb{U}(2^n)$ would be through the following scheme:

(1) Sample from the Haar distribution over $\mathbb{U}(4)$ to produce a random gate G
(2) Uniformly pick two distinct qubits and locally apply G to the pair.

However, this becomes computationally infeasible as even reasonably approximating the Haar distribution under this manner requires an exponential number of local 2-qubit gates

Date: November 19, 2020.

[2]. This hurdle motivates us to study the construction of efficient k-designs i.e distributions over $\mathbb{U}(4)$ such that sampling over these distributions and applying our scheme above will converge to good approximations of the k^{th} moments of the Haar distributon over $\mathbb{U}(2^n)$. To this end, we begin with annotations of the seminal paper by Harrow and Low [1]. We first introduce concepts germane to the area of efficient k-designs and summarize the techniques employed in the analyses presented in the paper. nally infeasible as the number of local random unitaries grows exponentially in the number of qubits.

2. Approximate 2-designs

2.1. **Definitions and Motivations.** In [1], the authors tackle the problem of approximate 2-designs, specifically *unitary* 2-designs. The central result of the paper claims that the scheme of applying sampled 2-qubit unitaries from certain distributions with a k-gapped property converge to the second moment of the Haar distribution rapidly. The crux of the rapid convergence argument relies on mapping the evolution of an initial state under our random circuit to that of a Markov chain's. Consequently, the analysis becomes amenable to classic techniques created to study mixing times of Markov chains. To begin, we first state the relevant definitions as employed by Harrow and Low.

Definition 2.1. An ensemble of operators $\mathcal{E} = \{p_i, U_i\}$ over $\mathbb{U}(d)$ is called an *(exact) unitary k-design* if $\mathcal{G}_W = \mathcal{G}_H$ where

$$\mathcal{G}_W(\rho) = \sum_i p_i U_i^{\otimes k} \rho (U_i^\dagger)^{\otimes k} \tag{2.1}$$

$$\mathcal{G}_H(\rho) = \int_{\mathbb{U}(d)} U^{\otimes k} \rho (U^\dagger)^{\otimes k} \, dU \tag{2.2}$$

We would naturally like to define some distance between $\mathcal{G}_W$ and $\mathcal{G}_H$. One formulation involves interpreting the two $\mathcal{G}_W, \mathcal{G}_H$ as quantum channels to utilize the diamond norm:

Definition 2.2. The diamond norm of an operator T is defined as

$$||T||_\diamond = \sup_d ||T \otimes I_d||_\infty$$

Definition 2.3. $\mathcal{G}_W$ is an *ϵ-approximate k-design* if

$$||\mathcal{G}_W - \mathcal{G}_H||_\diamond \leq \epsilon \tag{2.3}$$

As discussed in the introduction above, the unitary constructed by sampling from a universal gate set and applying them to random pairs of qubits will converge to a unitary sampled from Haar distribution. However, we would like to find *efficient approximate* k-designs. Here, efficient refers to random circuits of length polynomial in the number of qubits. The authors actually prove some stronger, namely that *k-copy gapped* distributions suffice.

Definition 2.4. Let μ be a (possibly continuous) probability measure on $\mathbb{U}(d)$. If

$$\mathcal{G}_\mu = \int_{\mathbb{U}(d)} d\mu(U) U^{\otimes k} \otimes (U^*)^{\otimes k} \tag{2.4}$$

then we say that $\mathcal{G}_\mu$ is k-copy gapped if $\mathcal{G}_\mu$ has only $k!$ unit eigenvalues.

A more general definition of universality of gatesets can be defined as well:

Definition 2.5. Let μ be a distribution over $\mathbb{U}(d)$. μ is deemed to be *universal* for $\mathbb{U}(d)$ if for any open ball $B \subset \mathbb{U}(d)$, there exists a sufficiently large integer ℓ such that $\mu^{\star\ell}(B) > 0$ where $\mu^{\star\ell}$ refers to the ℓ-fold *convolution* product of μ:

$$\mu^{\star\ell} = \int_{\mathbb{U}(d)} \delta_{U_1,\cdots,U_\ell} d_\mu(U_1) \cdots d_\mu(U_\ell) \tag{2.5}$$

Remark 2.6. This is the convolution product in the sense of measures. For example, if we let μ, σ be two Borel measures over $\mathbb{R}$, then the Borel measure $\mu \star \sigma$:

$$\mu \star \sigma(A) = \int_{\mathbb{R}} \int_{\mathbb{R}} \mathbb{I}_A(x+y) d\mu(x) d\sigma(y)$$

where $\mathbb{I}$ is the characteristic function for measurable set $A \subset \mathbb{R}$.

Intuitively, universality implies that sampling enough times over μ is enough to approximate any gate in $\mathbb{U}(d)$. This aligns with the definition introduced for discrete measures μ over finite gate sets. We will prove later that any universal gate set will be k-copy gapped on $\mathbb{U}(4)$ (Lemma **??**). For now, let us state the main theorem and its auxiliary lemma to guide our upcoming analysis:

Theorem 2.7. *Let μ be a 2-copy gapped distribution over $\mathbb{U}(4)$ and W a random circuit of length t drawn from sampling 2-qubit unitaries from μ and applying them to random pairs of of a system of n-qubits. Then there exists a constant C depending on μ such that for $\epsilon > 0$, $\mathcal{G}_W$ is an ϵ-approximate 2-design if $t \geq n(n + \log 1/\epsilon)$.*

Notation 2.8. Let ρ be an initial state such that $\rho \in \mathbb{C}^{2n}$. We can expand ρ in terms of the Pauli basis $\{\sigma_i\}_{0 \leq i \leq 3}$ as follows:

$$\rho = \frac{1}{2^n} \sum_{p_1,p_2} \gamma_0(p_1,p_2) \sigma_{p_1} \otimes \sigma_{p_2}, \quad \gamma_0(p_1,p_2) \in\in \mathbb{C} \tag{2.6}$$

where p_1, p_2 run over all strings of Pauli indices of length n, $\{0,1,2,3\}^n$. Let $\gamma_W(p_1,p_2)$ be the coefficient of the term $\sigma_{p_1} \otimes \sigma_{p_2}$ for $\rho_W = W^{\otimes 2} \rho (W^\dagger)^{\otimes 2}$. Extending this notation allows us to express the expected coefficient after t-samples from our distribution μ as $\gamma_t(p_1,p_2) = \mathbb{E}_W[\gamma_W(p_1,p_2)]$, averaging over all t-length random circuits.

Lemma 2.9. *Let ρ be a an initial state such that $\gamma_0(p,p) \geq 0$ and $\sum_p \gamma_0(p,p) = 1$ with μ and W as in Theorem 2.7. Then there exists constant C such that for $\epsilon > 0$*

$$\sum_{p_1,p_2 \neq 00} \left(\gamma_t(p_1,p_2) - \delta_{p_1 p_2} \frac{1}{2^n(2^n+1)} \right)^2 \leq \epsilon \tag{2.7}$$

for $t \geq Cn \log 1/\epsilon$.

$$\sum_{p_1,p_2 \neq 00} \left| \gamma_t(p_1,p_2) - \delta_{p_1 p_2} \frac{1}{2^n(2^n+1)} \right| \leq \epsilon \tag{2.8}$$

for $t \geq n(n + \log 1/\epsilon)$

Corollary 2.9.1. *Let μ, W, γ_W be as above. Then for* any *initial state ρ, there exists constant C such that for $\epsilon > 0$,*

$$\sum_{p_1,p_2 \neq 00} \left(\gamma_t(p_1,p_2) - \delta_{p_1 p_2} (\frac{\sum_{p \neq 0} \gamma_0(p,p)}{4^n - 1} \right)^2 \leq \epsilon \tag{2.9}$$

$$\sum_{p_1,p_2 \neq 00} \left| \gamma_t(p_1,p_2) - \delta_{p_1 p_2} (\frac{\sum_{p \neq 0} \gamma_0(p,p)}{4^n - 1} \right| \leq \epsilon \tag{2.10}$$

both for $t \geq Cn(n + \log 1/\epsilon)$

2.2. **Analysis of Moments.**

References

1. Aram W Harrow and Richard A Low, *Random quantum circuits are approximate 2-designs*, Communications in Mathematical Physics **291** (2009), no. 1, 257–302.
2. Emanuel Knill, *Approximation by quantum circuits*, arXiv preprint quant-ph/9508006 (1995).