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 has not become stranger to this trend. Numerous applications of random unitaries have been discovered in the areas of quantum tomography, quantum cryptography, and, rather naturally, quantum 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.

Date: November 21, 2020.

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

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 introduced by Harrow and Low.

Remark 2.1. As dissecting every proof in [1] may unnecessarily length this report, we occasionally omit proofs of lemmas. Some major theorems will have their proofs delegated to the appendix of this report.

Definition 2.2. 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 in order to utilize the diamond norm:

Definition 2.3. The diamond norm of an operator T is defined as

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

Definition 2.4. $\mathcal{G}_W$ is an *ϵ-approximate k-design* if

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

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 2.5. 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 2.6. 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 2.7. This is the convolution product in the context of *measures*. For example, if we let μ, σ be two finite Borel measures over $\mathbb{R}$, then we have a new finite Borel measure on $\mathbb{R}$, $\mu \star \sigma$:

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

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 2.8. *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 2.9. Let ρ be an initial state of an n-qubit system i.e $\rho \in (\mathbb{C}^2)^{\otimes n}$. 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 the output state after applying random circuit W, $\rho_W = W^{\otimes 2}\rho(W^\dagger)^{\otimes 2}$. Extending this notation allows us to express the expected coefficient after t-samples from our distribution μ as $\gamma_t(p_1,p_2) = \mathbb{E}_W[\gamma_W(p_1,p_2)]$. Note that the expectation is taken over all t-length random circuits.

Lemma 2.10. *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 2.8. Then there exists constant C such that for $\epsilon > 0$*

$$\sum_{p_1,p_2\neq 00} \left(\gamma_t(p_1,p_2) - \delta_{p_1p_2}\frac{1}{2^n(2^n+1)}\right)^2 \leq \epsilon \tag{2.7}$$

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

$$\sum_{p_1,p_2\neq 00} \left|\gamma_t(p_1,p_2) - \delta_{p_1p_2}\frac{1}{2^n(2^n+1)}\right| \leq \epsilon \tag{2.8}$$

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

Corollary 2.10.1. *Let μ, W, γ_W be as above. Then for* any *initial state ρ, there exists constant C such that for $\epsilon > 0$,*

$$\sum_{p_1,p_2\neq 00} \left(\gamma_t(p_1,p_2) - \delta_{p_1p_2}(\frac{\sum_{p\neq 0}\gamma_0(p,p)}{4^n-1}\right)^2 \leq \epsilon \tag{2.9}$$

$$\sum_{p_1,p_2\neq 00} \left|\gamma_t(p_1,p_2) - \delta_{p_1p_2}(\frac{\sum_{p\neq 0}\gamma_0(p,p)}{4^n-1}\right| \leq \epsilon \tag{2.10}$$

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

2.2. **Analysis of Moments.** We turn back to the general case and begin to define concepts and definitions for group $\mathbb{U}(d)$ and for d-qudit states. Set a Hermitian basis of $d \times d$ to be $\sigma_0, \sigma_1, \cdots \sigma_{d^2-1}$ such that $\sigma_0 = I$. These basis elements span the d-qudit states. Here we stress that we sample our unitaries over the *Haar distribution* over $\mathbb{U}(d)$. We denote sampling from the Haar distribution with the notation $U \sim \mathbb{U}(d)$ when necessary. Furthermore, our Hermitian basis operators are such that $Tr(\sigma_p\sigma_q) = d \cdot \delta_{p,q}$ i,e orthogonal under the Hilbert-Schmidt inner product.

Let $\mathbf{p} = (p_1, \cdots, p_k) \in \{0,1,\cdots,d^2-1\}^k$ denote a k-string of basis indices. We will be interested in the quantity:

$$T(\mathbf{p}) := \mathbb{E}_{U\sim\mathbb{U}(d)}\left[U^{\otimes k}\sigma_{p_1}\otimes\sigma_{p_2}\otimes\cdots\otimes\sigma_{p_k}(U^\dagger)^{\otimes k}\right] \tag{2.11}$$

This will be the expected state after applying a sampled unitary U from the uniform distribution over $\mathbb{U}(d)$. Naturally, we can reexpress this resulting state into the σ_p basis:

$$T(\mathbf{p}) = \sum_{\mathbf{q}} \widehat{G}(\mathbf{p}, \mathbf{q}) \sigma_{q_1} \otimes \cdots \otimes \sigma_{q_k} \tag{2.12}$$

where the same is taken over all k-strings in $\{0, \cdots, d^2 - 1\}^k$. This allows us to define the matrix $\widehat{G}$ where the rows and columns are indiced by k-strings with entries $\widehat{G}(\mathbf{q}, \mathbf{p})$. This matrix turns out to be a *symmetric projector.*

Lemma 2.11. *The matrix $\widehat{G}$ above is symmetric i.e. $\widehat{G}(\boldsymbol{p}, \boldsymbol{q}) = \widehat{G}(\boldsymbol{q}, \boldsymbol{p})$*

Proof. By orthogonality:

$$\widehat{G}(\mathbf{q}, \mathbf{p}) = d^{-k} \cdot Tr(\sigma_{q_1} \otimes \cdots \otimes \sigma_{q_k} T(\mathbf{p})) \tag{2.13}$$

$$= d^{-k} \mathbb{E}_U \left[Tr(\sigma_{q_1} \otimes \cdots \otimes \sigma_{q_k}) U^{\otimes k} (\sigma_{p_1} \otimes \sigma_{p_2} \otimes \cdots \otimes \sigma_{p_k}) (U^{\dagger})^{\otimes k} \right] \tag{2.14}$$

□

Note that the expectation and the trace operator commute by linearity of latter. The result follows from the cyclic invariance of trace.

Lemma 2.12. *$\widehat{G}$ fixes permutation operators P_π, $\pi \in S_k$.*

These two results are all that is required to show that $\widehat{G}$ is indeed a projector.

Theorem 2.13. *$\widehat{G}$ is a projector i.e. $\widehat{G}^2 = \widehat{G}$*

Proof. Expanding the matrix product shows that

$$\widehat{G}(\mathbf{p}, \mathbf{q}) = \sum_{\mathbf{q'}} \widehat{G}(\mathbf{p}, \mathbf{q'}) \widehat{G}(\mathbf{q'}, \mathbf{q}) = \tag{2.15}$$

$$= \sum_{\mathbf{q'}} \widehat{G}(\mathbf{p}, \mathbf{q'}) \left(d^{-k} \cdot Tr(\sigma_{q'_1} \otimes \cdots \otimes \sigma_{q'_k} T(\mathbf{q})) \right) \tag{2.16}$$

By Schur-Weyl Duality, $T(\mathrm{q})$ must be a linear combination of permutation operators ($T(\mathbf{p})$ commutes with all unitaries of the form $U^{\otimes k}$ by the invariance of the Haar integral). However, by Lemma (2.12) above, $\widehat{G}$ fixes the permuatation operators. To understand this more explicitly, rewrite the Lemmma (2.12) as follows:

$$\sum_{\mathbf{q}} \widehat{G}(\mathbf{p}, \mathbf{q}) \cdot Tr(\sigma_{q_1} \otimes \cdots \otimes \sigma_{q_k} P_\pi) = Tr(\sigma_{p_1} \otimes \cdots \otimes \sigma_{p_k} P_\pi) \tag{2.17}$$

This simply expressing the equality $\widehat{G}P_\pi = P_\pi$ for permutation operator $p_\pi,\ \pi \in S_k$. By linearity of trace, the equality above reduces to

$$\sum_{\mathbf{q'}} \widehat{G}(\mathbf{p}, \mathbf{q'}) \left(d^{-k} \cdot Tr(\sigma_{q_1'} \otimes \cdots \otimes \sigma_{q_k'} T(\mathbf{q}))\right) = Tr(\sigma_{p_1} \otimes \cdots \otimes \sigma_{p_k} T(\mathrm{q})) \tag{2.18}$$

$$= \widehat{G}(\mathbf{p}, \mathbf{q}) \tag{2.19}$$

□

Corollary 2.13.1. *$\widehat{G}$ has eigenvalues 0 and 1*

2.2.1. *Explicit calculation of $T(\boldsymbol{p})$.* The calculation is divided into the two pertinent cases $k = 1, 2$.

(1) *(For $k = 1$)* For this case, a random unitary sampled from the uniform distribution will randomize the initial state. Thus:

$$T(p) = \begin{cases} \sigma_0 & p = 0 \\ 0 & p \neq 0 \end{cases}$$

(2) *(For $k = 2$)* From Lemma (2.12) and Theorem (2.13), $\widehat{G}$ must fix the only two permutation operators $I, \mathcal{F}$ where $\mathcal{F}$ is the swap operator on two qubits. We note that we will normalize the swap operator

$$\mathcal{F} = \frac{1}{d^2 - 1} \sum_{1 \leq q \leq d^2 - 1} \sigma_q \otimes \sigma_q \tag{2.20}$$

We then deduce the following about $\widehat{G}$:

(a) $\widehat{G}(p_1, p_2; q_1, q_2) = 0, \quad p_1 \neq p_2$ or $q_1 \neq q_2$

Proof. To see this, observe that both $I, \mathcal{F}$ have vanishing $\sigma_{q_1} \otimes \sigma_{q_2}$ components for $q_1 \neq q_2$. Thus, multiplying $\widehat{G}$ with either one should also result in vanishing $\sigma_{q_1} \otimes \sigma_{q_2}$ components. This with the fact that all other operators are sent to zero by $\widehat{G}$ yields the result. □

(b) $\widehat{G}(p; 0) = \delta_{p0}$ (Here we denote $\widehat{G}(p; 0) := \widehat{G}(p, p; 0, 0)$)

Proof. This just derives from $\widehat{G}$ acting on I □

(c) $\widehat{G}(p, a) = \frac{1}{d^2 - 1}, \quad a, p \neq 0$

Proof. As above, this results from $\widehat{G}$ acting on $\mathcal{F}$ along with the condition that it must send all other operators to zero. □

We conclude from the definition of $T(p,q)$ for $p,q \in \{0,\cdots,d^2-1\}$ that

$$T(p,q) = \begin{cases} 0 & p \neq q \\ \sigma_0 \otimes \sigma_0 & p = q = 0 \\ \frac{1}{d^2-1}\sum_{\ell\neq 0}\sigma_\ell \otimes \sigma_\ell & p = q \neq 0 \end{cases} \tag{2.21}$$

Recall that $T(p,q)$ refers to the expected *state* from applying unitary $U \sim \mathbb{U}(d)$ to the basis state $\sigma_p \otimes \sigma_q$. From the determination above, it is simple to see that U uniformly samples from all diagonal basis states when acting on $\sigma_p \otimes \sigma_p,\ p \neq 0$. Strikingly enough, applying $U \sim \mathbb{U}(d)$ conserves the total sum of the coefficients of the diagonal basis states.

Lemma 2.14. *The total sum of the coefficients $\sum_p \gamma_0(p,p)$ is conserved by $U \sim \mathbb{U}(d)$ for state $\rho = \frac{1}{d}\sum_{p_1,p_2}\gamma_0(p_1,p_2)\sigma_{p_1}\otimes\sigma_{p_2}$.*

Normalizing this sum allows us to view it as a *probability distribution.* Furthermore, the evolution of our random circuit scheme is amenable to Markov chain analysis. As an illustrative example, suppose we have an n-qubit system and so far have appied t steps of our scheme. As per usual, we pick our 2-qubit unitary $U \sim \mathbb{U}(4)$. Now if we were to pick qubits $1, 2$ for our local unitary transformation, the expected *coefficients* for step $t+1$ will work out to be

$$\gamma_{t+1}(p_1,\cdots,p_n,q_1,\cdots,q_n) = \begin{cases} 0 & (p_1,p_2)\neq(q_1,q_2) \\ \gamma_t(0,0,\cdots,p_n,0,0,\cdots,q_n) & (p_1,p_2)=(q_1,q_2)=(0,0) \\ \frac{1}{15}\sum_{\substack{r_1,r_2 \\ r_1r_2\neq 00}}\gamma_t(r_1,r_2,\cdots p_n,r_1,r_2,\cdots,q_n) & (p_1,p_2)=(q_1,q_2)\neq(0,0) \end{cases} \tag{2.22}$$

It is worth reiterating that our random 2-qubit unitary is only acting on the first two qubits non-trivially whereas every other qubit is acted on by identity. Our desired Markov chain is then defined naturally as such

(1) The states of the Markov chain are $\Omega = \{0,1,2,3\}^n$
(2) The transitions adhere to the guidelines below: Suppose we start with a state indexed by string $\alpha = \alpha_1\cdots\alpha_n$
  (a) Pick two distinct sites $i < j$ uniformly at random.
  (b) If $i = j = 0$, remain at the same state. Otherwise pick $\beta_i\beta_j = \{0,1,2,3\}^2/\{00\}$ uniformly at random. Transition to the string

$$\alpha_1\alpha_2,\cdots\alpha_{i-1}\beta_i\alpha_{i+1}\cdots\alpha_{j-1}\beta_j\alpha_{j+1}\cdots\alpha_n$$

2.3. **Convergence of the Random Circuit.**

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).