Random Quantum Circuits are Unitary Polynomial-Designs

Fernando G.S.L. Brandão[1]

Aram Harrow[2]

Michal Horodecki[3]

1. Universidade Federal de Minas Gerais, Brazil
2. University of Washington, USA
3. Gdansk University, Poland

IQC, November 2011

Outline

- **The problem**

  Unitary t-designs

  Random Circuits

- **Result**

  Poly(n) Random Circuits are poly(n)-designs

- **Applications**

  Fooling Small Sized Circuits

  Quick Equilibration by Unitary Dynamics

- **Proof**

  Connection to Spectral Gap of Local Hamiltonian

  A Lower Bound on the Spectral Gap

  Path Coupling for the Unitary Group

Haar Random Unitaries

For every integrable function in **U**(d) and every V in **U**(d)

$$E_{U \sim Haar} f(U) = E_{U \sim Haar} f(VU)$$

Applications of Haar Unitaries

(Hayden, Leung, Winter '04) Create entangled states with extreme properties

(Emerson et al '04) Process tomography

(Hayden et al '04) Quantum data hiding and information locking

(Sen '05) State distinguishability

(Abeyesinghe '06) Encode for transmission of quantum information through a quantum channel, state merging, mother protocol, …

The Price You Have to Pay…

To sample from the Haar measure with error ε you need $\exp(4^n \log(1/\varepsilon))$ different unitaries

Exponential amount of random bits and quantum gates…

Quantum Pseudo-Randomness

In many applications, we can replace a Haar random unitary by *pseudo-random* unitaries:

This talk: Quantum Unitary t-designs

Def. An ensemble of unitaries $\{\mu(dU), U\}$ in $\mathbf{U}(d)$ is an ε-approximate unitary t-design if for every monomial $M = U_{p1,\, q1} \ldots U_{pt,\, qt} U^*_{r1,\, s1} \ldots U^*_{rt,\, st,}$

$$|E_\mu(M(U)) - E_{Haar}(M(U))| \leq d^{-2t}\varepsilon$$

Quantum Unitary Designs

Conjecture 1. There are efficient ε-approximate unitary t-designs $\{\mu(dU), U\}$ in $\mathbf{U}(2^n)$

Efficient means:

- unitaries created by poly(n, t, log(1/ε)) two-qubit gates
- $\mu(dU)$ can be sampled in poly(n, t, log(1/ε)) time.

Quantum Unitary Designs

Previous work:

(DiVincenzo, Leung, Terhal '02) Clifford group is an *exact* 2-design

(Dankert el al '06) Efficient construction of 2-design

(Ambainis and Emerson '07) Efficient construction of *state* poly(n)-design

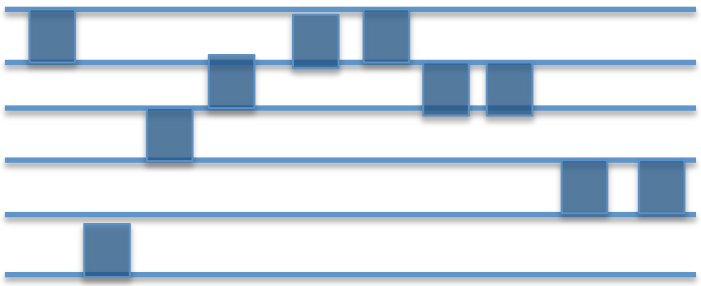
(Harrow and Low '08) Efficient construction of (n/log(n))-design

(Abeyesinghe '06) 2-designs are enough for decoupling

(Low '09) Other applications of t-design (mostly 2-designs) replacing Haar unitaries

Random Quantum Circuits

Local Random Circuit: in each step an index *i* in {1, … ,n} is chosen uniformly at random and a two-qubits Haar unitary is applied to qubits i e i+1



Random Walk in $\mathbf{U}(2^n)$

(Another example: Kac's random walk – toy model Boltzmann gas)

Introduced in (Hayden and Preskill '07) as a toy model for the dynamics of a black hole

Random Quantum Circuits

Previous work:

(Oliveira, Dalhsten, Plenio '07) $O(n^3)$ random circuits are 2-designs

(Harrow, Low '08) $O(n^2)$ random Circuits are 2-designs for every universal gate set

(Arnaud, Braun '08) numerical evidence that $O(n\log(n))$ random circuits are unitary t-design

(Znidaric '08) connection with spectral gap of a mean-field Hamiltonian for 2-designs

(Brown, Viola '09) connection with spectral gap of Hamiltonian for t-designs

(B., Horodecki '10) $O(n^2)$ local random circuits are 3-designs

Random Quantum Circuits as t-designs?

Conjecture 2. Random Circuits of size poly(n, log(1/ε)) are an ε-approximate unitary poly(n)-design

Main Result

Conjecture 2. Random Circuits of size poly(n, log(1/ε)) are an ε-approximate unitary poly(n)-design

(B., Harrow, Horodecki '11) Local Random Circuits of size $\tilde{O}(n^2 t^5 \log(1/\varepsilon))$ are an ε-approximate unitary t-design

Data Hiding

Computational Data Hiding:
"Most quantum states look maximally mixed for all polynomial sized circuits"

e.g. most quantum states are useless for measurement based quantum computation (Gross et al '08, Bremner et al '08)

Let QC(k) be the set of 2-outcome POVM {A, I-A} that can Be implemented by a circuit with *k* gates

$$\Pr_{|\psi\rangle \sim Haar}\left(\max_{A \in QC(poly(n))} \left| \langle \psi | A | \psi \rangle - 2^{-n} tr(A) \right| \geq \varepsilon \right) \leq 2^{n^{\log(n)}} 4^{-c\varepsilon^2 2^n}$$

Data Hiding

Computational Data Hiding:
"Most quantum states look maximally mixed for all polynomial sized circuits"

1. By Levy's Lemma, for every 0 < A < I,

$$\Pr_{|\psi\rangle \sim Haar}\left(\left|\langle\psi|A|\psi\rangle - 2^{-n} tr(A)\right| \geq \varepsilon\right) \leq e^{-c\varepsilon^2 2^n}$$

2. There is a eps-net of size < exp($n^{\log(n)}$) for poly(n) implementable POVMs. By union bound

$$\Pr_{|\psi\rangle \sim Haar}\left(\max_{A \in QC(poly(n))} \left|\langle\psi|A|\psi\rangle - 2^{-n} tr(A)\right| \geq \varepsilon\right) \leq 2^{n^{\log(n)}} 4^{-c\varepsilon^2 2^n}$$

Data Hiding

Computational Data Hiding:
"Most quantum states look maximally mixed for all polynomial sized circuits"

1. By Levy's Lemr ery 0 < A < I,

$$\Pr_{|\psi\rangle\sim}$$

But most states also require $2^{O(n)}$ quantum gates to be approximately created…

2. There is a eps-net of size < exp(n^) for poly(n) implementable POVMs. By union bound

$$\Pr_{|\psi\rangle\sim Haar}\left(\max_{A\in QC(poly(n))} |\langle\psi|A|\psi\rangle - 2^{-n}tr(A)| \geq \varepsilon\right) \leq 2^{n^{\log(n)}} 4^{-c\varepsilon^2 2^n}$$

Efficient Data Hiding

Corollary 1: Most quantum states formed by $O(n^k)$ circuits look maximally mixed for every circuit of size $O(n^{(k+4)/6})$

Efficient Data Hiding

Corollary 1: Most quantum states formed by $O(n^k)$ circuits look maximally mixed for every circuit of size $O(n^{(k+4)/6})$

Same idea (small probability + eps-net), but replace Levy's lemma by a *t*-design bound from (Low '08):

$$\Pr_{U\sim\nu_{s,n}}\left(\left|\langle 0|UAU|0\rangle - 2^{-n}tr(A)\right| \geq \delta\right) \leq \exp\left(O(t\log(1/\delta) - nt)\right)$$

with $t = s^{1/6}n^{-1/3}$ and $\nu_{s,n}$ the measure on $U(2^n)$ induced by s steps of the local random circuit model

ε-net of POVMs with r gates has size $\exp(O(r(\log(n)+\log(1/\varepsilon)))$

Circuit Minimization Problem

Goal: Given a unitary, what is the minimum number of gates needed to approximate it to an error ε?

Circuit Complexity:

$C_\varepsilon(U) := \min\{k : \text{there exists } V \text{ with } k \text{ gates s.t. } ||V - U|| \leq \varepsilon\}$

Question: Lower bound to the circuit complexity?

Corollary 2: Most circuits of size $O(n^k)$ have $C_\varepsilon(U) > O(n^{(k+4)/6})$

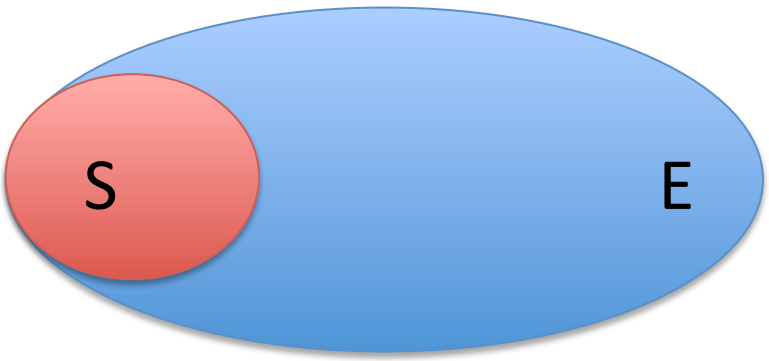
Haar Randomness Not Needed

More generally,

Any quantum algorithm that has m uses of a Haar unitary and l gates and accepts, on average, with probability p, will accept with probability in $(p - \varepsilon, p + \varepsilon)$ if we replace the Haar unitary by a random circuit of size $\mathrm{poly}(m, l, \log(1/\varepsilon))$

Equilibration by Unitary Dynamics

Problem: Let H_{SE} be a Hamiltonian of two quantum systems, S and E with |S| << |E|



State at time *t*:

$$\rho_S(t) := tr_E\left(e^{-itH_{SE}}\rho_0 e^{itH_{SE}}\right)$$

On physical grounds we expect that for most times

$$\rho_S(t) \approx \rho_{equi}$$

This is true, in the limit of infinite times! (Linden et al '08)

Fast Equilibration by Unitary Dynamics

How about the time scale of equilibration?
For which *T* do we have

$$\frac{1}{T}\int_{1}^{T}\left\|\rho_S(t)-\rho_{equi}\right\|dt \le \varepsilon \quad ?$$

(Linden et al '08) only gives the bound T ≤ 1/(min. energy gap)

But we know equilibration is fast:
coffee gets cold quickly, beer gets warm quickly ☹

Fast Equilibration by Unitary Dynamics

Toy model for equilibration: Let $H_{SE} = UDU'$, with U taken from the Haar measure in $U(|S||E|)$ and $D := \mathrm{diag}(E_1, E_2, \ldots)$.

$$\frac{1}{T}\int_{U(|S||E|)} tr\left(\left(\rho_S(t)-\rho_{equi}\right)^2\right)\mu_{Haar}(dU) \le O\left(\frac{\left(\sum_k e^{i2tE_k}\right)^2}{|S||E|^2}+\ldots\right)$$

(B., Ciwiklinski et al '11, Masanes et al '11, Vinayak, Znidaric '11)

Time of equilibration: Average energy gap: $\frac{1}{|S|^2|E|^2}\sum_{j,l}(E_j-E_l)^{-1}$

For typical eigenvalue distribution goes with $O(1/\log(|E|))$

Fast Equilibration by Unitary Dynamics

Calculation only involves 4th moments:

$$\frac{1}{T}\int_{U(|S||E|)} tr\left(\left(tr_E\left(Ue^{-itD}U'\rho_0 Ue^{itD}U'\right)-\rho_{equi}\right)^2\right)\mu_{Haar}(dU)$$

Can replace Haar measure by an approximate unitary 4-design

Corollary 3. For most Hamiltonians of the form UDU' with U a random quantum circuit of $O(n^3)$ size, small subsystems equilibrate fast.

Fast Equilibration vs Diagonalizing Complexity

Let H = UDU', with D diagonal. Then we call $C_\varepsilon(U)$ the diagonalizing complexity of U.

Corollary 4. For most Hamiltonians with $O(n^3)$ diagonalizing complexity, small subsystems equilibrate fast.

Connection suggested in (Masanes, Roncaglia, Acin '11)

In contrast: Hamitonians with $O(n)$ diagonalizing complexity Do not equilibrate in general

Open question: Can we prove something for the more interesting case of few-body Hamiltonians?

Proof of Main Result

1. Another characterization of unitary t-designs
2. Mapping the problem to bounding spectral gap of a Local Hamiltonian
3. Technique for bounding spectral gap

"It suffices to get a *exponential small* bound on the convergence rate"

4. Path Coupling applied to the unitary group

t-Copy Tensor Product Quantum Expanders

An ensemble of unitaries {μ(dU), U} is an (t, 1-ε) tensor product expander if

$$\left\| \int \mu(dU) U^{\otimes t} \otimes \bar{U}^{\otimes t} - \int \mu_H(dU) U^{\otimes t} \otimes \bar{U}^{\otimes t} \right\|_\infty \leq \varepsilon$$

Obs: Implies it is a $d^{2t}\varepsilon$-approximate unitary t-design

Relating to Spectral Gap

μ_n : measure on $U(2^n)$ induced by one step of the local random circuit model

$(\mu_n)^{*k}$: k-fold convolution of μ_n (measure induced by k steps of the local random circuit model)

We show:

$$\left\| \int \mu_n^{*k}(dU) U^{\otimes t} \otimes \bar{U}^{\otimes t} - \int \mu_H(dU) U^{\otimes t} \otimes \bar{U}^{\otimes t} \right\|_\infty = \lambda_2 \left(\int \mu_n(dU) U^{\otimes t} \otimes \bar{U}^{\otimes t} \right)^k$$

Relating to Spectral Gap

μ_n : measure on $U(2^n)$ induced by one step of the local random circuit model

$(\mu_n)^{*k}$: k-fold convolution of μ_n (measure induced by k steps of the local random circuit model)

We show:

$$\left\| \int \mu_n^{*k}(dU) U^{\otimes t} \otimes \bar{U}^{\otimes t} - \int \mu_H(dU) U^{\otimes t} \otimes \bar{U}^{\otimes t} \right\|_\infty = \lambda_2 \left(\int \mu_n(dU) U^{\otimes t} \otimes \bar{U}^{\otimes t} \right)^k$$

It suffices to a prove upper bound on λ_2 of the form $1 - \Omega(t^{-4}n^{-1})$ since $(1 - \Omega(t^{-4}n^{-2}))^k \leq 2^{-2nt}\varepsilon$ for $k = O(n^2 t^5 \log(1/\varepsilon))$

Relating to Spectral Gap

But $\mu_n = \frac{1}{n}\sum_{i=1}^{n} \mu_{Haar}(i,i+1)$

So $\lambda_2\left(\int \mu_n(dU) U^{\otimes t} \otimes \bar{U}^{\otimes t}\right) = 1 - \frac{\Delta(H_{n,t})}{n}$

with $H_{n,t} := \sum_{i=1}^{n} h_{i,i+1}$ $\quad h_{i,i+1} := I - \int_{U(4)} U_{i,i+1}^{\otimes t} \otimes \bar{U}_{i,i+1}^{\otimes t} \mu_H(dU)$

and $\Delta(H_{n,t})$ the spectral gap of the local Hamiltonian $H_{n,t}$

$H_{n,t}$:

Relating to Spectral Gap

But $\mu_n = \frac{1}{n}\sum_{i=1}^{n} \mu_{Haar}(i,i+1)$

So $\lambda_2\left(\int \mu_n(dU) U^{\otimes t} \otimes \bar{U}^{\otimes t}\right) = 1 - \frac{\Delta(H_{n,t})}{n}$

wit $\ldots U_{i,i+1}^{\otimes t} \otimes \bar{U}_{i,i+1}^{\otimes t} \mu_H(dU)$

an $\ldots$ Hamiltonian $H_{n,t}$

Want to lower bound spectral gap by $O(t^{-4})$

$H_{n,t}$:

Structure of $H_{n,t}$

i. The minimum eigenvalue of $H_{n,t}$ is zero and the zero eigenspace is

$$G_{n,t} := span\left\{ \left|\psi_\pi\right\rangle^{\otimes n}, \left|\psi_\pi\right\rangle := (I \otimes V(\pi))\left|\Phi(2^t)\right\rangle : \pi \in S_t \right\}$$

ii. Approximate orthogonality of permutation matrices:

$$\sum_{\pi \in S_t} \left|\langle \psi_\sigma | \psi_\pi \rangle\right|^n \le 1 + \frac{2t^2}{2^n}, \qquad \left\| \sum_{\pi \in S_t} \left(\left|\psi_\pi\right\rangle\left\langle\psi_\pi\right|\right)^{\otimes n} - G_{n,t} \right\|_\infty \le \frac{2t^2}{d^n}$$

Structure of $H_{n,t}$

Follows from

$$[X, U^{\otimes t}] = 0 \Leftrightarrow X = V(\pi)$$

i. The minimum eigenv

eigenspace is

$$G_{n,t} := span\left\{ |\psi_\pi\rangle^{\otimes n}, |\psi_\pi\rangle := (I \otimes V(\pi))|\Phi(2^t)\rangle : \pi \in S_t \right\}$$

ii. Approximate orthogonality of permutation matrices:

$$\sum_{\pi \in S_t} |\langle \psi_\sigma | \psi_\pi \rangle|^n \leq 1 + \frac{2t^2}{2^n}, \qquad \left\| \sum_{\pi \in S_t} \left(|\psi_\pi\rangle\langle\psi_\pi| \right)^{\otimes n} - G_{n,t} \right\|_\infty \leq \frac{2t^2}{d^n}$$

Structure of $H_{n,t}$

Follows from

$$[X, U^{\otimes t}] = 0 \Leftrightarrow X = V(\pi)$$

i. The minimum eigen

Follows from

$$P_{sym} = \frac{1}{t!}\sum_{t \in S_t} V(\pi)$$

$$, |\psi_\pi\rangle := (I \otimes V(\pi))|\Phi(2^t)\rangle : \pi \in S_t \}$$

ii. Approxim orthogonality of permutation matrices:

$$\sum_{\pi \in S_t} |\langle \psi_\sigma | \psi_\pi \rangle|^n \leq 1 + \frac{2t^2}{2^n}, \qquad \left\| \sum_{\pi \in S_t} \left(|\psi_\pi\rangle\langle\psi_\pi| \right)^{\otimes n} - G_{n,t} \right\|_\infty \leq \frac{2t^2}{d^n}$$

Lower Bounding $\Delta(H_{n,t})$

We prove: $$\Delta(H_{n,t}) \geq \frac{\Delta(H_{2\log(t),t})}{8\log(t)}$$

Follows from structure of $H_{n,t}$ and

(Nachtergaele '96) Suppose there exists l, n_l, ε_l such that

for all $n_l < m < n-1$ $$\left\|(I_{A_1} \otimes G_{A_2B})(G_{A_1A_2} \otimes I_B) - G_{A_1A_2B}\right\|_\infty \leq \varepsilon_l$$

with $A_1 := [1, m-l-1]$, $A_2:=[m-l,m-1]$, $B:=m$ and $\varepsilon_l < l^{-1/2}$. Then

$$\Delta(H_{[1,n]}) \geq \Delta(H_{[1,l]})\left(\frac{\left(1-\varepsilon_l\sqrt{l}\right)}{l-1}\right)$$

Lower Bounding $\Delta(H_{n,t})$

We prove: $$\Delta(H_{n,t}) \geq \frac{\Delta(H_{2\log(t),t})}{8\log(t)}$$

Want to lower bound by $O(t^{-4})$, an exponential small bound in the size of the chain (i.e. in $2\log(t)$)

Foll

(Na

for all $n_l < m < n-1$ $$\left\|(I_{A_1} \otimes G_{A_2B})(G_{A_1A_2} \otimes I_B) - G_{A_1A_2B}\right\|_\infty \leq \varepsilon_l$$

with $A_1 := [1, m-l-1]$, $A_2:=[m-l,m-1]$, $B:=m$ and $\varepsilon_l < l^{-1/2}$. Then

$$\Delta(H_{[1,n]}) \geq \Delta(H_{[1,l]})\left(\frac{\left(1-\varepsilon_l\sqrt{l}\right)}{l-1}\right)$$

Exponentially Small Bound to Spectral Gap

Follows from two relations:

1. $$\left(1-\frac{\Delta(H_{n,t})}{n}\right)^k \le 2tW\left((\mu_n)^{*k},\mu_{Haar}\right)$$

Wasserstein distance:

$$W(\nu_1,\nu_2) := \sup\left\{\int f(u)\nu_1(du) - \int f(u)\nu_2(du) : f \ \ is \ \ 1-Lipschitz\right\}$$

2. $$W\left((\mu_n)^{*(n-1)k},\mu_{Haar}\right) \le 2^{n/2}(1-2^{-5n})^{\frac{k}{n-1}}$$

Bounding Convergence with Path Coupling

Key result to 2nd relation: Extension to the unitary group of Bubley and Dyer path coupling

Let $W_p(\nu_1,\nu_2) := \inf\left\{E[d(X,Y)^p]^{1/p} : (X,Y) \ couples \ (\nu_1,\nu_2)\right\}$

(Oliveira '07) Let ν be a measure in U(d) s.t.

$$\lim_{\varepsilon\to 0} \sup_{U_1,U_2\in U(d)} \left\{ \frac{W_2\left(\nu * \delta_{U_1}, \nu * \delta_{U_2}\right)}{\left\|U_1 - U_2\right\|_2} : \left\|U_1 - U_2\right\|_2 \le \varepsilon \right\} \le \eta$$

Then $$W_2(\nu * \nu_1, \nu * \nu_2) \le \eta W_2(\nu_1,\nu_2)$$

Bounding Convergence with Path Coupling

Must consider coupling in n steps of the walk to get non trivial contraction (see paper for details)

(Oliveira '07) Let ν be a measure in U(d) s.t.

$$\lim_{\varepsilon \to 0} \sup_{U_1, U_2 \in U(d)} \left\{ \frac{W_2\left(\nu * \delta_{U_1}, \nu * \delta_{U_2}\right)}{\left\| U_1 - U_2 \right\|_2} : \left\| U_1 - U_2 \right\|_2 \le \varepsilon \right\} \le \eta$$

Then $$W_2(\nu * \nu_1, \nu * \nu_2) \le \eta W_2(\nu_1, \nu_2)$$

Summary

- $\tilde{O}(n^2 t^5 \log(1/\varepsilon))$ local random circuits are ε-approximate unitary t-designs
- Most states of size n^k is indistinguishable from maximally mixed by all circuits of size $n^{(k+4)/6}$
- Proof is based on

  (i) connection to spectral gap local Hamiltonian
  (ii) approximate orthogonality of permutation matrices
  (iii) path coupling for the unitary group
- Another application to fast equilibration of quantum systems by unitary dynamics with an environment

Open Questions

- Is $\tilde{O}(n^2 t^5 \log(1/\varepsilon))$ tight?
- Can we prove that constant depth random circuits are approximate unitary t-designs?
  (we can show they form a t-tensor product expander;
  proof uses the detectability lemma of Aharonov et al)

  Would have applications to:
  (i) fast equilibration of generic few-body Hamiltonians
  (ii) creation of topological order by short circuits
  (counterpart to the no-go result of Bravyi, Hastings, Verstraete for short *local* circuits)