Efficient quantum TPEs and k-designs

Aram Harrow and Richard Low

University of Bristol
UK

arXiv:0811.2597

Talk Outline

- Introduction
- Definitions
- Main Result
- Proof Outline
- Further Work

Random Unitaries

What is a random unitary?

$$\int dU\, f(U) = \int dU\, f(UV)$$

What can we do with random unitaries?

- Random states
- Random measurements
- Randomisation (for e.g. cryptography)
- Data hiding
- Locking
- Remote state preparation
- Decoupling

Other Applications

- Can twirling be implemented efficiently?

$$\mathcal{T}(\rho) = \int dU (U \otimes U) \rho (U^\dagger \otimes U^\dagger)$$

- What about higher moments for use in algorithms and other problems?
  - State discrimination [1,2,3]
  - Derandomisation (i.e. use less randomness)
  - Quantum cryptography
  - Tamper resistant encryption [4]

[1] Ambainis and Emerson, Complexity'06
[2] Sen, quant-ph/0512085
[3] Massar and Popescu, PRL (1995)
[4] Ambainis, Bouda and Winter, arXiv:0808.0353

Pseudo-random Unitaries

- Constructing a uniformly random unitary is exponentially hard
- Can we make a pseudo-random unitary efficiently?
- Much like classical case where we use pseudo-random numbers to minimise use of randomness

Unitary k-designs

- Let $\{p_i, U_i\}$ be an ensemble of unitary operators. Define

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

$$\mathcal{G}_H(\rho) = \int_U dU U^{\otimes k} \rho \left(U^\dagger\right)^{\otimes k}$$

- The ensemble is a unitary k-design if

$$\mathcal{G}_W(\rho) = \mathcal{G}_H(\rho) \, \forall \rho$$

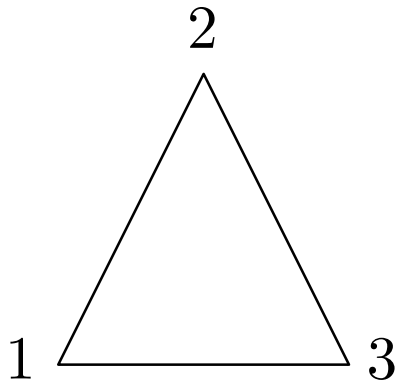
- Approximate if (choose appropriate norm for application)

$$||\mathcal{G}_W - \mathcal{G}_H|| \leq \epsilon$$

- Efficient if can sample and implement each U_i with resources scaling as $\mathrm{poly}(k, \log N)$ (*N* is the dimension)

Expanders

- Let *G* be a graph with degree *D* and *N* vertices. Let its adjacency matrix be *A*.
- Then *G* is a (N, D, λ)-expander if the second largest eigenvalue of *A*/*D* is $\leq \lambda$
- E.g.



$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

$$N = 3, D = 2, \lambda = 1/2$$

Expanders (2)

- Normally we have a family of expander graphs for each *N*
- We want λ and *D* to be constant
- Then a random walk on the graph mixes quickly

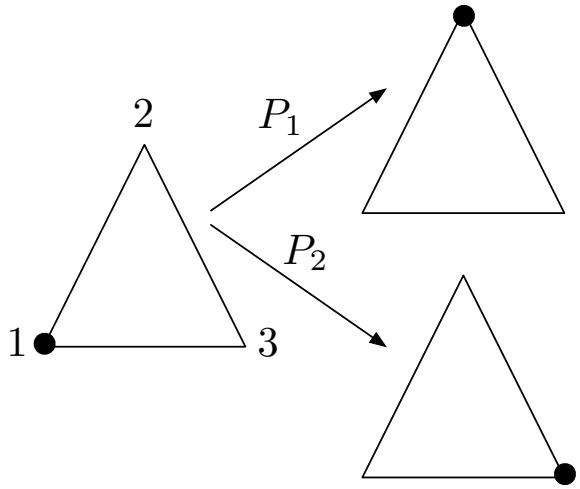
- We can decompose the adjacency matrix into sums of permutations
- For our example,

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Random walks on graphs

- Choose one of the permutations at random:

$$P_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \qquad P_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$



Expanders (3)

- In general we have *D* permutations for a degree *D* graph
- To execute the random walk, choose one of the *D* permutations at random
- Then the expander gap condition becomes

$$||\mathbb{E}_{\pi\sim\nu}B(\pi) - \mathbb{E}_{\pi\sim S_N}B(\pi)||_\infty \leq \lambda$$

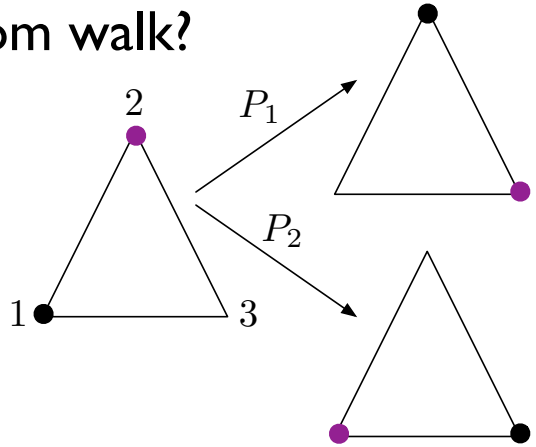
- Or equivalently:

$$||A/D - A_{\text{complete}}/N||_\infty \leq \lambda$$

$$A = \sum_{\pi\in\nu} B(\pi) \qquad A_{\text{complete}} = \frac{1}{(N-1)!}\sum_{\pi\in S_N} B(\pi)$$

Tensor Product Expanders

- What happens if we have multiple markers executing a correlated random walk?



- Want them to mix quickly and break correlations
- For *k* walkers,

$$\left\| \mathbb{E}_{\pi \sim \nu} B(\pi)^{\otimes k} - \mathbb{E}_{\pi \sim S_N} B(\pi)^{\otimes k} \right\|_\infty \leq \lambda$$

- This is a (N, D, λ, k)-TPE [Hastings & Harrow 08]
- Efficient const degree and gap construction [Kassabov05]

Quantum TPEs

- Instead of permutations, we have unitaries

$$\left\| \mathbb{E}_{U\sim\nu} U^{\otimes k,k} - \mathbb{E}_{U\sim\mathcal{U}(N)} U^{\otimes k,k} \right\|_\infty \leq \lambda$$

- where

$$U^{\otimes k,k} = U^{\otimes k} \otimes \left(U^*\right)^{\otimes k}$$

- Note this is equivalent to, for all ρ

$$\left|\left| \mathbb{E}_{U\sim\nu} \left[U^{\otimes k} \rho \left(U^\dagger\right)^{\otimes k} \right] - \mathbb{E}_{U\sim\mathcal{U}(N)} \left[U^{\otimes k} \rho \left(U^\dagger\right)^{\otimes k} \right] \right|\right|_2 \leq \lambda ||\rho||_2$$

- So 'applying the expander map' means draw a unitary at random from the ensemble ν, take k copies and apply it to the state

k-designs from TPEs

- Firstly, let's show how we get a k-design from this:
- Define an ϵ-approximate *k*-design ν by

$$\left|\left|\mathbb{E}_{U\sim\nu}U^{\otimes k,k} - \mathbb{E}_{U\sim\mathcal{U}(N)}U^{\otimes k,k}\right|\right|_1 \leq \epsilon$$

- Iterate the TPE *m* times to get

$$\left|\left|\mathbb{E}_{U\sim\nu_m}U^{\otimes k,k} - \mathbb{E}_{U\sim\mathcal{U}(N)}U^{\otimes k,k}\right|\right|_\infty \leq \lambda^m$$

- So

$$\left|\left|\mathbb{E}_{U\sim\nu_m}U^{\otimes k,k} - \mathbb{E}_{U\sim\mathcal{U}(N)}U^{\otimes k,k}\right|\right|_1 \leq N^{2k}\lambda^m$$

- Take *m* such that

$$N^{2k}\lambda^m \leq \epsilon$$

Our construction

- Let ν_C be a classical $(N, D, \lambda_C, 2k)$-TPE
- Let U_{QFT} be the QFT on *N* dimensions
- Then let ν_Q be the operation that randomly chooses between applying ν_C or U_{QFT}
- This is a quantum $(N, D+1, \lambda_Q, k)$-TPE
- Has $\lambda_Q < 1$ and constant provided $\lambda_C < 1$ and constant and

$$N > 4(2k)^{8k}$$

- Further, if the classical TPE has an efficient construction then the quantum TPE is efficient also

k-design construction

- We therefore obtain an efficient k-design construction on *n* qubits that runs in time $\mathrm{poly}(n,k)$, uses $O(nk)$ random bits and works for $k = O(n/\log(n))$. ($N = 2^n$)

Proof outline

- The classical TPE has many fixed points (vectors with eigenvalue 1)
- Every fixed point of the quantum TPE is a fixed point of the classical TPE, but reverse not true
- Need to kill off the other fixed points
- The QFT does the job: moves these 'bad' fixed points to vectors that are decayed by the classical TPE

Conclusions

- Have introduced tensor product expanders, both classical and quantum
- Shown how to construct a quantum k-TPE from a classical 2k-TPE: just mix the classical TPE with the QFT
- Shown this can be iterated to give an efficient approximate k-design

[1] Hastings and Harrow, arXiv:0804.0011
[2] Harrow and Low, arXiv:0811.2597

Future

- Can we find an efficient construction for all k and N?
- What can we derandomise with k-designs with high k?