

Exponential Quantum Speed-ups are Generic

Fernando G.S.L. Brandão¹ and Michał Horodecki²

1. Universidade Federal de Minas Gerais, Brazil

2. University of Gdansk, Poland

The Role of Fourier Transform in Quantum Speed-ups

The Role of Fourier Transform in Quantum Speed-ups

Two opposing views:

- (van Dam) The Quantum Fourier Transform (QFT) is all there is to quantum algorithms, since the **Toffoli** gate and the **Hadamard** gate (the Z_2 QFT) is an **universal gate set**
- (Hallgren, Harrow '08) **Almost any** sufficiently long quantum circuit is useful for quantum speed-ups in the **query complexity** setting

The Role of the Quantum Fourier Transform in Quantum Speed-ups

(Hallgren, Harrow '08) **Almost any** sufficiently long quantum circuit is useful for quantum speed-ups in the **query complexity** setting

The Role of Fourier in The Fourier Sampling Problem

(Hallgren, Harrow '08) **Almost any** sufficiently long quantum circuit is useful for quantum speed-ups in the **query complexity** setting

- Almost any circuit can be used to solve a certain variant of Bernstein and Vazirani Fourier Sampling Problem with $O(1)$ queries vs. $\Omega(n)$ classical queries.
- The linear separation can be boosted by recursion to a **polynomial** versus **superpolynomial** gap, as in the original FSP

Can we apply the same trick to other oracle problems?

Can we get exponential speed-ups?

Can we get a simpler oracle problem? 😊

Yes we can

We show how generic circuits are “useful” for **superexponential speed-ups** by a simple adaptation of **Fourier Checking Problem (Aar ‘09)**

The plan

1. Review **Fourier Checking**
1. Introduce ***U*-Circuit Checking**
2. **Classical Query Complexity** of **U-Circuit Checking**
1. **Quantum Query Complexity** **U-Circuit Checking**
2. Family of unitaries exhibiting **exponential** speed-ups
1. Random Quantum Circuits are **Unitary 3-designs**

Fourier Checking

(Aaronson '09) Given two functions

$$f, g : \{0, 1\}^n \rightarrow \{-1, 1\}$$

with the promise that either

- f and g are chosen independently and uniformly at random
- f and g are *forrelated*: $f(x) = \text{sgn}(u_x)$ and $g(x) = \text{sgn}(\hat{u}_x)$ for a vector $u = (u_1, u_2, \dots)$ with i.i.d. entries drawn from a Normal $N(0, 1)$ distribution and

$$\hat{u}_x = \sum_{y \in \{0, 1\}^n} a_{x,y} (-1)^{x \cdot y} u_y$$

Decide which is the case

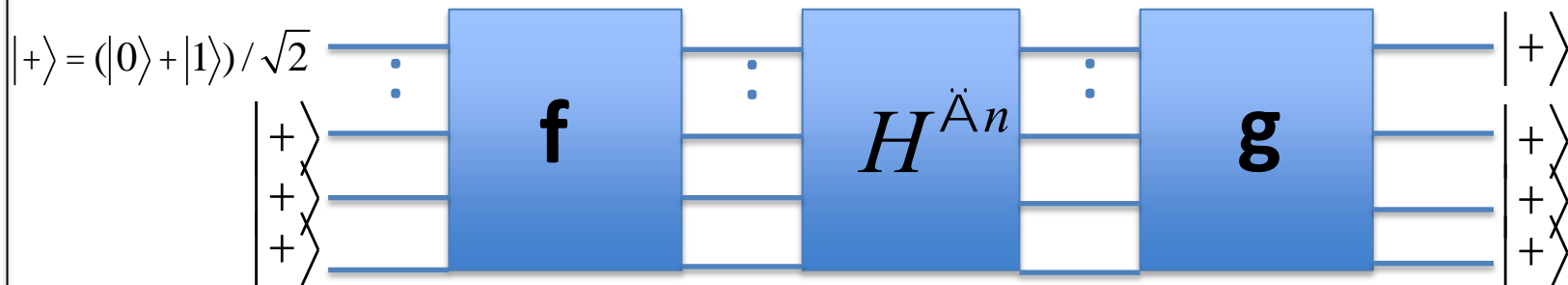
Query Complexity of Fourier Checking

(Aar '09) Fourier Checking can be solved with $O(1)$ quantum queries and $O(1)$ quantum time

It requires $\Omega(2^{n/4})$ classical queries, even with **postselection**

A superexponential separation of quantum and postselected classical query complexities

Quantum Algorithm:



Query Complexity of Fourier Checking

(Aaronson '09) Fourier Checking can be solved with $O(1)$ quantum

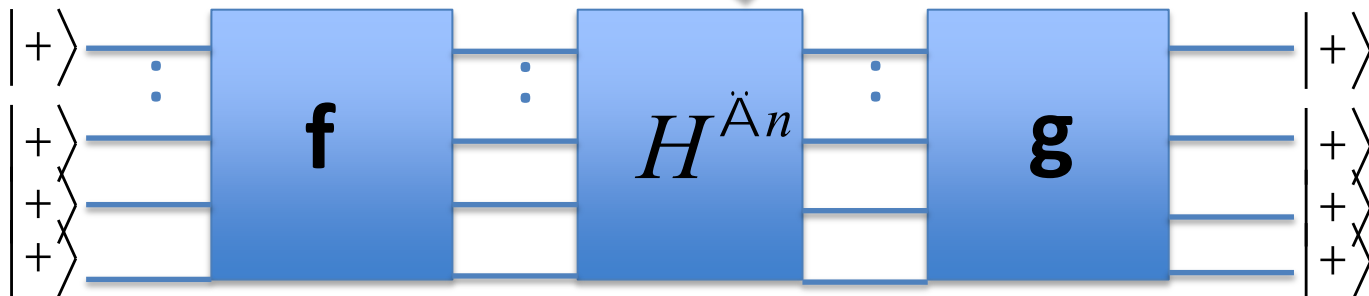
queries and $O(1)$ quantum time

- If f and g are independent random: $\Pr(\text{Accept}) = 2^{-n}$
- If f and g are correlated: $\Pr(\text{Accept}) \geq W(1)$

(Aaronson '09) A superexponential separation of quantum and postselected classical query complexities

A superexponential separation of quantum and postselected classical query complexities

Quantum Algorithm:



The Role of Fourier in Fourier Checking

The **Fourier Transform** appears both in the definition of Fourier Checking and in the quantum algorithm solving it.

What property of the Fourier Transform is being exploited?
Can we replace it by other mapping?

U-Circuit Checking

Given two functions

$$f, g : \{0, 1\}^n \rightarrow \{-1, 1\}$$

with the promise that either

- f and g are chosen independently and uniformly at random
- f and g are ***U-correlated***: $f(x) = \text{sgn}(u_x)$ and $g(x) = \text{sgn}(\text{Re}(\hat{u}_x))$ for a vector $u = (u_1, u_2, \dots)$ with i.i.d. entries drawn from a Normal $N(0, 1)$ distribution and

$$\hat{u}_x = \sum_{y \in \{0, 1\}^n} U_{x,y} u_y$$

For a unitary U . Decide which is the case

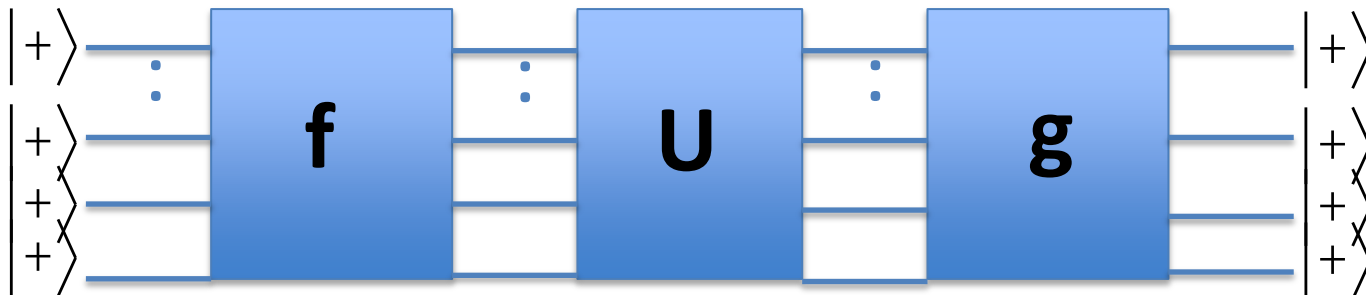
Quantum Query Complexity of U -Circuit Checking

Lemma 1. U -circuit checking can be solved with $O(1)$ quantum queries and $O(1)$ quantum time for any unitary U such that

$$\sum_{x,y} \operatorname{Re}(U_{x,y})^2 \geq W(1)$$

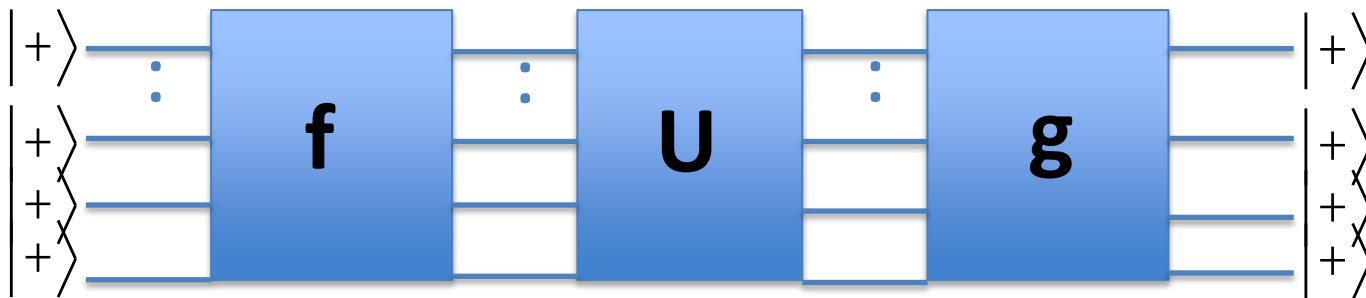
Obs: For any unitary U , either U or iU satisfies the condition of the Lemma

Quantum Algorithm:



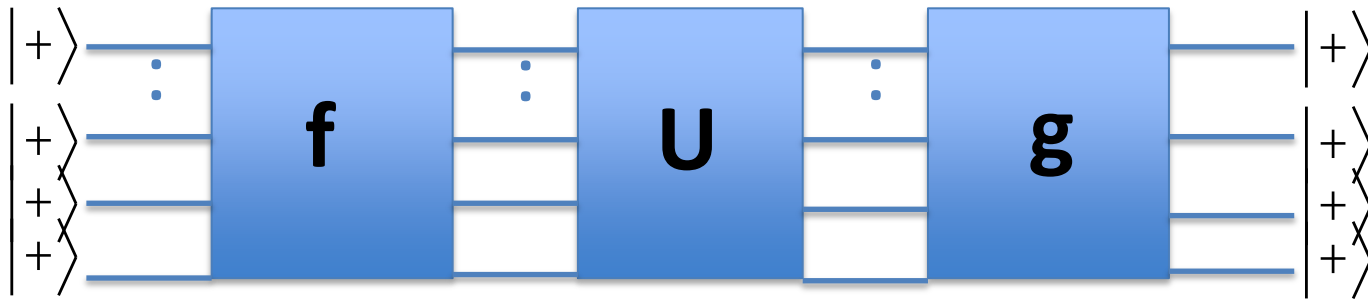
Quantum Query Complexity of U -Circuit Checking

Quantum Algorithm:



Quantum Query Complexity of U -Circuit Checking

Quantum Algorithm:



- If f and g are independent random: $\Pr(\text{Accept}) = 2^{-n}$
- If f and g are correlated: $\Pr(\text{Accept}) \geq \Omega(1)$

Proof: Berry-Esseen theorem + simple algebra

Classical Query Complexity of U -Circuit Checking

We show an **exponential lower bound** for the classical query complexity of U -Circuit Checking for any unitary U which is *fairly flat*

Classical Query Complexity of U -Circuit Checking

We show an **exponential lower bound** for the classical query complexity of U -Circuit Checking for any unitary U which is *fairly flat*

Def 1. (Flatness measure) For a unitary U we define

$$C(U) := -\log(\max_{x,y} |U_{x,y}|^2)$$

Classical Query Complexity of U -Circuit Checking

We show an **exponential lower bound** for the classical query complexity of U -Circuit Checking for any unitary U which is *fairly flat*

Def 1. (Flatness measure) For a unitary U we define

$$C(U) := -\log(\max_{x,y} |U_{x,y}|^2)$$

Lemma 2. The classical query complexity of U -Circuit Checking, with postselection, is lower bounded by $2^{C(U)/7}$

Thus there is a **superexponential gap** of quantum and classical query complexities for every n -qubit U such that $C(U)$

$$\geq \Omega(n) \quad C(H^{\wedge n}) = n \quad C(\text{Diag}(w_1, \dots, w_{2^n})) = 0$$

Families of “Flat” Circuits

Lemma 3. (i) Let U_G be the the QFT over the group G . Then

$$C(U_G) \geq \log |G| / 2$$

(ii) Given an 2^{-9n} -approximate unitary **3**-design on n qubits all but a $2^{-n/2}$ -fraction of its elements satisfy

$$C(U) \geq n/6$$

Def 2. An ensemble of unitaries $\{\mu(dU), U\}$ on $U(d)$ is an ε -approximate unitary t -design if for every balanced monomial

$$M = U_{p1, q1} \dots U_{pt, qt} U_{r1, s1}^* \dots U_{r1, s1}^*$$

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

Families of “Flat” Circuits

Lemma 3. (i) Let U_G be the the QFT over the group G . Then

$$C(U_G) \geq \log |G| / 2$$

(ii) Given an 2^{-9n} -approximate unitary **3**-design on n qubits all but a $2^{-n/2}$ -fraction of its elements satisfy

$$C(U) \geq n/6$$

Def 2. An ensemble of unitaries $\{\mu(dU), U\}$ on $U(d)$ is an ε -approximate unitary t -design if for every balanced monomial

$$M = U_{p1, q1...} U_{pt, qt} U_{r1, s1...}^* U_{r1, s1}^*$$

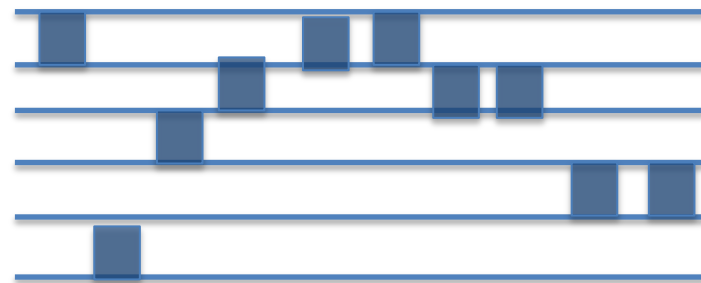
$$|E_{\mu}(M(U)) - E_{\text{haar}}(M(U))| \leq d^{2t}\varepsilon$$

Most Quantum Circuits Are Flat

Main Technical Result:

Lemma 4. $5n \log(1/\epsilon)$ -size local random quantum circuits form a ϵ -approximate unitary **3**-design

Def 3. Local Random Circuit: In each step an index is chosen uniformly at random and a two-qubit Haar unitary on $U(4)$ is applied to qubits i and $i+1$



Hence all but a $2^{-\Omega(n)}$ -fraction of $O(n^2)$ -sized quantum circuits U are such that U -Circuit Checking has a $O(1)$ vs $2^{\Omega(n)}$ quantum-to-classical gap in query complexity

Random Circuits as t -Designs

Previous work:

1. (Oliveira, Dalhsten, Plenio '07; Harrow, Low '08): Random Quantum Circuits are **approximate 2-design**
2. (Arnaud, Braun '08): Numerical evidence that random quantum circuits are **t -design** for **arbitrary t**
3. (Znidaric '08): Proof that RQC are **approximate 2-design** by mapping the mixing time of the walk to spectral properties of **local quantum Hamiltonians**
4. (Brown, Viola '09): Argument that RQC are **t -design** for **arbitrary t** using connection to local quantum Hamiltonians and using a plausible - but unproven - assumption of the **spectral gap** of a **Lipkin-Meshkov-Glick** model ($SU(4^t)$ multilevel)

Random Circuits are 3-design

Lemma 4 (again). $5n \log(1/\epsilon)$ -size local random quantum circuits form a ϵ -approximate unitary **3**-design

The **main ingredient** in the proof is the following technique from quantum many-body theory for bounding the spectral gap of local quantum Hamiltonians:

(Knabe '88) Let $\mathbf{H} = \sum_k \mathbf{H}_{k,k+1}$ be a **1D TI frustration-free** local Hamiltonian with **zero groundstate energy**. Then

$$D\left(\sum_{k=1}^N H_{k,k+1}\right) \geq \frac{n}{n-1} \left(D\left(\sum_{k=1}^n H_{k,k+1}\right) - \frac{1}{n} \right)$$

In particular,
$$D\left(\sum_{k=1}^N H_{k,k+1}\right) \geq 2D(H_{1,2} + H_{2,3}) - 1$$

Random Circuits are 3-design

Lemma 4 (again). $5n \log(1/\epsilon)$ -size local random quantum circuits form a ϵ -approximate unitary **3**-design

Proof Sketch: Let $G_{m^{*k},t} := \int_{U(d)} m^{*k} (dU) U^{\otimes t} \overline{U}^{\otimes t}$

with $m^{*k} := \int_{U_1 \dots U_k} m(dU_1) \dots m(dU_k)$

We show: $\|G_{m^{*k},t} - G_{m_H,t}\|_{\text{F}} \leq \frac{1}{\epsilon} \left(1 - \frac{1}{5n}\right)^k$, with μ_H the Haar measure.

We have $\|G_{m^{*k},t} - G_{m_H,t}\|_{\text{F}} \leq \left(\frac{1}{2} \text{Tr}(M_{t,n})\right)^k$, with $M_{t,n} := \frac{1}{n} \sum_i P_{i,i+1}$

and $P_{i,i+1} := \int_{U(d)} m_H(dU) U_{i,i+1}^{\otimes t} \overline{U}_{i,i+1}^{\otimes t}$

Random Circuits are 3-design

Lemma 4 (again). $5n \log(1/\epsilon)$ -size local random quantum circuits form a ϵ -approximate unitary **3**-design

Proof Sketch (part 2): The **key step** is the inequality:

$$\lambda_2(M_{t,n}) \leq 1 - \frac{3 - 4\lambda_2(M_{t,3})}{n}$$

(We can bound the mixing time of the random walk on n qubits but the mixing time of the same walk on **3** qubits!)

It follows by applying Knabe's trick to $H := \hat{\Delta} H_{i,i+1} = n(I - M_{t,n})$ with $H_{i,i+1} := I - P_{i,i+1}$ (H is TI, frustration free and has zero ground-energy).

Finally we compute $\lambda_2(M_{3,3}) = 7/10$, giving $\lambda_2(M_{3,n}) \leq 1 - (5n)^{-1}$ ■

Open Questions

- Can the Fourier transform be replaced by generic circuits in other oracle problems (e.g Simon's, ...)?
- Does U-Circuit Checking for a generic family of $\{U_n\}$ provide an oracle separation of BQP and the polynomial hierarchy? (See talk on work by Fefferman and Umans on Friday)
- Are random quantum circuits approximate $\text{poly}(n)$ -designs? Can the same technique be applied to $t > 3$?

Thank you!