EIROPAS SOCIĀLAIS FONDS

EIROPAS SAVIENĪBA

IEGULDĪJUMS TAVĀ NĀKOTNĒ

Quantum complexity of random Boolean functions

Andris Ambainis
Artūrs Bačkurs
Juris Smotrovs
Ronald de Wolf

Eiropas Sociālā fonda projekts "Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku" Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

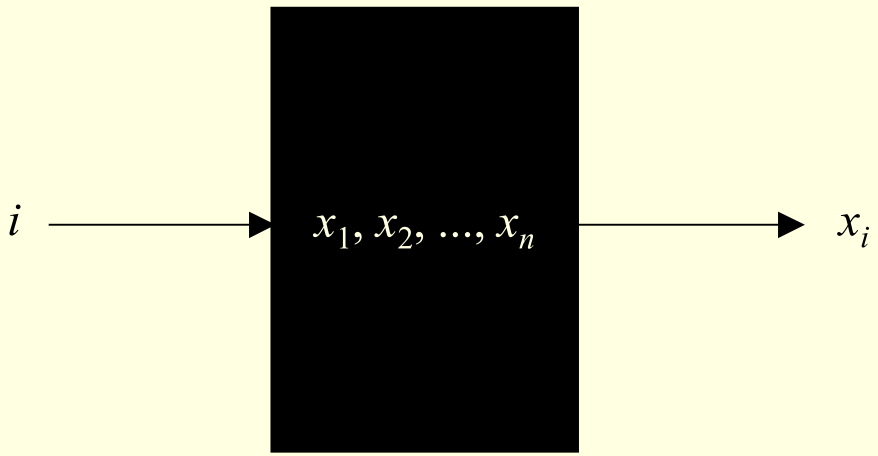
Outline of the talk

- Query algorithm model
- Representing polynomials of Boolean functions
- Known query complexity bounds
- Our result
- Polynomial method
- Proof of our result

Eiropas Sociālā fonda projekts "Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku" Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Query algorithm model

- A known Boolean function $f: \{0,1\}^n \rightarrow \{0,1\}$
- The input bit values are unknown, in a black box which can be queried, at a cost:



- The aim: to output the value of f

Eiropas Sociālā fonda projekts "Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku" Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Query algorithm model

- Quantum black box query can be a superposition of the input bit indices
- Its answer is a similar superposition where each input bit is encoded in the sign of the corresponding amplitude:

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_{ij}\left|i,j\right\rangle \longrightarrow \boxed{x_1, x_2, \ldots, x_n} \longrightarrow \sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_{ij}\left(-1\right)^{x_i}\left|i,j\right\rangle$$

- Between the queries a quantum query algorithm can perform any unitary transformation of its state
- In the end a 0/1 outcome measurement is performed

Eiropas Sociālā fonda projekts “Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku” Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Query algorithm model

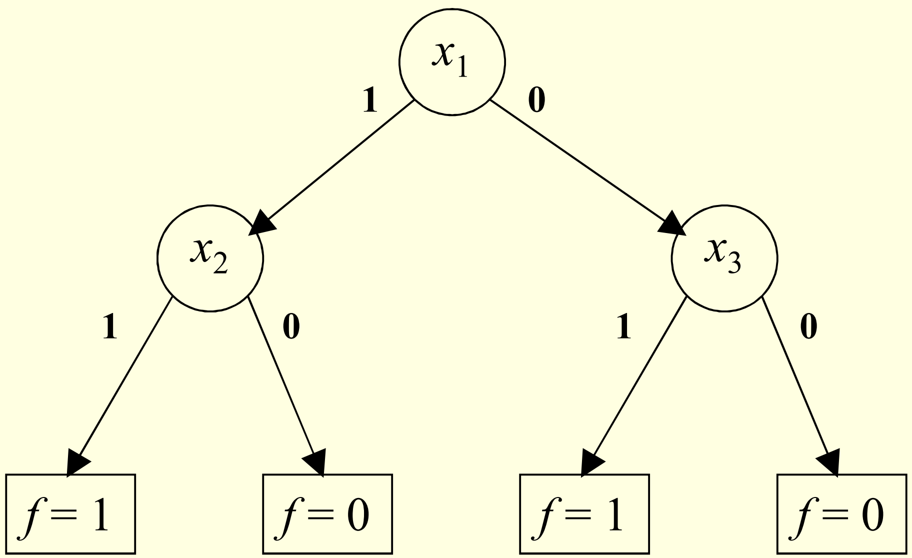
- Complexity of a query algorithm (query complexity): the maximum number of queries on all possible input bit strings
- Notation of the query complexity of a
  - deterministic algorithm: $D(f)$
  - quantum algorithm with success probability 1 (an exact quantum algorithm): $Q_E(f)$
  - quantum algorithm with error probability $\varepsilon < ½$: $Q_\varepsilon(f)$

Eiropas Sociālā fonda projekts "Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku" Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Query algorithm model

- An example of a deterministic query algorithm specified as a decision tree (complexity $D(f) = 2$):

$$f(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee (\neg x_1 \wedge x_3)$$



Eiropas Sociālā fonda projekts "Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku" Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Representing polynomials of Boolean functions

- An exact representing polynomial: such multilinear polynomial of n variables the values of which within the domain $\{0,1\}^n$ coincide with the values of f, for example:

$$f(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee (\neg x_1 \wedge x_3) = x_3 + x_1 x_2 - x_1 x_3$$

- For each Boolean function there is a unique such polynomial
- A useful identity in this domain: $a^2 = a$
- Complexity measure $deg(f)$ of a Boolean function: the degree of this polynomial

Eiropas Sociālā fonda projekts "Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku" Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Representing polynomials of Boolean functions

- An approximate representing polynomial: such multilinear polynomial p the values of which are near to the values of f ($0 < \varepsilon < ½$):

$$\forall x_1,\ldots,x_n : \left|p(x_1,\ldots,x_n) - f(x_1,\ldots,x_n)\right| \le \varepsilon$$

- Approximate representing polynomial usually is not unique
- Complexity measure $deg_\varepsilon(f)$: the minimum degree of an approximate representing polynomial
- An example: the "majority function" MAJ, $\varepsilon = 1/3$, $deg(f) = 3$, $deg_\varepsilon(f) = 1$

$$MAJ(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3 - 2x_1x_2x_3 \approx \tfrac{1}{3}x_1 + \tfrac{1}{3}x_2 + \tfrac{1}{3}x_3$$

Eiropas Sociālā fonda projekts "Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku" Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Known query complexity bounds

- Nisan, Szegedy (1994): for all n-bit Boolean functions f

$$\log_2 n - O(\log\log n) \leq^* \deg(f) \leq D(f) \leq 16[\deg(f)]^8$$

* if the function f depends on all n arguments

$$\deg_\varepsilon(f) \leq \deg(f) \leq D(f) \leq c[\deg_\varepsilon(f)]^8$$

Known query complexity bounds

- Beals, Buhrman, Cleve, Mosca, de Wolf (1998): for all n-bit Boolean functions f

$$\frac{1}{2}\deg_{\varepsilon}(f) \le Q_{\varepsilon}(f) \le D(f) \le c(\deg_{\varepsilon}(f))^6$$

and for almost all n-bit Boolean functions f or, equivalently, for a random such function f:

$$\frac{n}{2} - o(n) \le Q_E(f)$$

(proved with the so-called polynomial method introduced in that paper)

Eiropas Sociālā fonda projekts "Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku" Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Known query complexity bounds

- Van Dam (1998): for all n-bit Boolean functions f

$$Q_\varepsilon(f) \le \frac{n}{2} + \sqrt{n}$$

- Ambainis (1999): for almost all n-bit Boolean functions f or for a random such function f with probability $1 - o(n)$:

$$\deg_\varepsilon(f) \ge \frac{n}{2} - o(n), \quad \text{therefore} \quad Q_\varepsilon(f) \ge \frac{n}{4} - o(n)$$

Open problem 1999–2012

- Where exactly between $n/4$ and $n/2$ is the bounded error query complexity Q_ε of a random Boolean function?

Eiropas Sociālā fonda projekts "Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku" Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Our result

- For almost all n-bit Boolean functions f, or for a random such function f with probability $1-o(n)$:

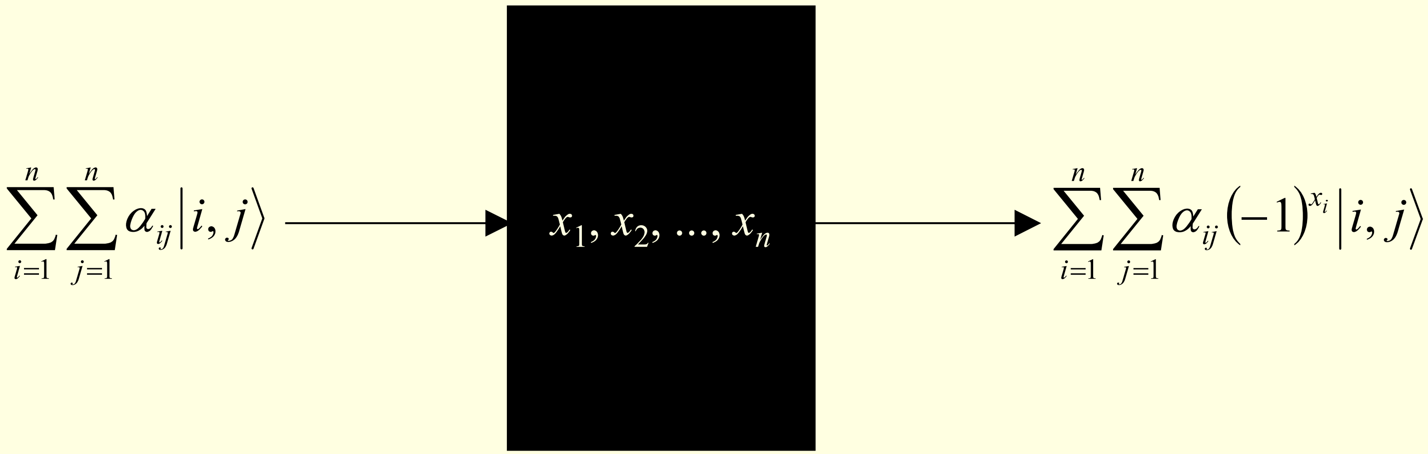
$$Q_{\varepsilon}(f) \geq \frac{n}{2} - o(n)$$

- It coincides with van Dam’s upper bound up to $o(n)$ terms

Eiropas Sociālā fonda projekts “Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku” Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Polynomial method

- Quantum black box query can be a superposition of the input bit indices
- Its answer is a similar superposition where each input bit is encoded in the sign of the corresponding amplitude:



- Between the queries a quantum query algorithm can perform any unitary transformation of its state
- In the end a 0/1 outcome measurement is performed

Polynomial method

- Beals, Buhrman, Cleve, Mosca, de Wolf (1998)
- Initially the amplitudes of a quantum query algorithm are constants
- At each query the amplitudes are multiplied by $(-1)^{x_i} = 1 - 2x_i$ (each by no more than one such factor)
- After any unitary transformation between queries each new amplitude is a linear combination of the old amplitudes
- So after d queries all amplitudes are polynomials of degree $\leq d$ of variables $x_1, x_2, ..., x_n$

Eiropas Sociālā fonda projekts “Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku” Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Polynomial method

- At the final measurement the probability p of the answer $f(x) = 1$ is the sum of modula squares of the corresponding amplitudes:

$$p(x_1,\ldots,x_n) = |\alpha_1(x_1,\ldots,x_n)|^2 + \ldots + |\alpha_k(x_1,\ldots,x_n)|^2$$

- It is thus a real polynomial of degree $\leq 2d$
- This probability must be ε-near to 1 if $f(x) = 1$ and ε-near to 0 if $f(x) = 0$ where ε is the allowed error probability; that is:

$$\forall x_1,\ldots,x_n : |p(x_1,\ldots,x_n) - f(x_1,\ldots,x_n)| \leq \varepsilon$$

- So p is a representing polynomial, and:

$$Q_E(f) \geq \frac{1}{2}\deg(f), \qquad Q_\varepsilon(f) \geq \frac{1}{2}\deg_\varepsilon(f)$$

Proof of our result

- The idea: the probability p of the answer $f(x) = 1$ is not just some arbitrary-looking approximate representing polynomial of f, it is also a sum of squares of real polynomials:

$$p(x) = (p_1(x))^2 + (p_2(x))^2 + \ldots + (p_k(x))^2$$

- The result was proven by showing that the least degree of such approximate representing polynomial which can be expressed as a sum of squares, tends to n

Eiropas Sociālā fonda projekts "Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku" Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Proof of our result

- If f is random, then approximately half its values are 1, and approximately half of them are 0.
- Then, since p approximates f:

$$\sum_{x:f(x)=1} p(x) \geq\approx 2^{n-1}\cdot(1-\varepsilon) \qquad \text{and} \qquad \sum_{x:f(x)=0} p(x) \leq\approx 2^{n-1}\cdot\varepsilon$$

$$\text{So} \quad \sum_{x:f(x)=1} p(x) \geq\approx \frac{1-\varepsilon}{\varepsilon}\cdot \sum_{x:f(x)=0} p(x) \quad \text{or}$$

$$\sum_{x:f(x)=1} (p_1(x)^2 + \ldots + p_k(x)^2) \geq\approx \frac{1-\varepsilon}{\varepsilon}\cdot \sum_{x:f(x)=0} (p_1(x)^2 + \ldots + p_k(x)^2)$$

$$\text{Then for at least one } j: \quad \sum_{x:f(x)=1} \left(p_j(x)\right)^2 \geq\approx \frac{1-\varepsilon}{\varepsilon}\cdot \sum_{x:f(x)=0} \left(p_j(x)\right)^2$$

Fourier representation

- Values 1 and –1 instead of the bits 0 and 1:

$$\hat{x}_i = (-1)^{x_i} = 1 - 2x_i$$

$$x_i = \frac{1 - \hat{x}_i}{2}$$

$$\hat{f}(x) = 1 - 2f(x)$$

$$\chi_s(x) = (-1)^{x_1 s_1 + x_2 s_2 + \ldots + x_n s_n} = \prod_{i: s_i = 1} \hat{x}_i$$

$$q_j(\hat{x}) = p_j(x) = \sum_{s:|s| \le d} \alpha_s \chi_s(x)$$

Eiropas Sociālā fonda projekts “Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku” Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Proof of our result

- Then: $$\sum_{x:f(x)=1}\left(q_j(\hat{x})\right)^2 \geq \frac{1-\varepsilon}{\varepsilon}\cdot\sum_{x:f(x)=0}\left(q_j(\hat{x})\right)^2 \Leftrightarrow$$

$$\Leftrightarrow \sum_x \left(q_j(\hat{x})\right)^2\left(\frac{1-\hat{f}(x)}{2}\right) \geq \frac{1-\varepsilon}{\varepsilon}\cdot\sum_x \left(q_j(\hat{x})\right)^2\left(\frac{1+\hat{f}(x)}{2}\right) \Leftrightarrow$$

$$\Leftrightarrow -\sum_x \left(q_j(\hat{x})\right)^2 \hat{f}(x) \geq (1-2\varepsilon)\cdot\sum_x \left(q_j(\hat{x})\right)^2 \Leftrightarrow$$

$$\Leftrightarrow -\sum_x \sum_{s:|s|\leq d}\sum_{s':|s'|\leq d}\alpha_s\alpha_{s'}\chi_{s\oplus s'}(x)\hat{f}(x) \geq (1-2\varepsilon)\cdot\sum_x \sum_{s:|s|\leq d}\sum_{s':|s'|\leq d}\alpha_s\alpha_{s'}\chi_{s\oplus s'}(x) \Leftrightarrow$$

$$\Leftrightarrow -\sum_{s:|s|\leq d}\sum_{s':|s'|\leq d}\alpha_s\alpha_{s'}\sum_x \chi_{s\oplus s'}(x)\hat{f}(x) \geq (1-2\varepsilon)\cdot\sum_{s:|s|\leq d}\sum_{s':|s'|\leq d}\alpha_s\alpha_{s'}\sum_x \chi_{s\oplus s'}(x) \Leftrightarrow$$

Eiropas Sociālā fonda projekts “Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku” Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Proof of our result

$$\Leftrightarrow -\sum_{s:|s|\le d}\sum_{s':|s'|\le d}\alpha_s\alpha_{s'}\sum_x \chi_{s\oplus s'}(x)\hat{f}(x) \ge (1-2\varepsilon)\cdot \sum_{s:|s|\le d}\sum_{s':|s'|\le d}\alpha_s\alpha_{s'}\sum_x \chi_{s\oplus s'}(x) \Leftrightarrow$$

$$\Leftrightarrow -\sum_{s:|s|\le d}\sum_{s':|s'|\le d}\alpha_s\alpha_{s'}\left(\chi_{s\oplus s'},\hat{f}\right) \ge (1-2\varepsilon)\cdot \sum_{s:|s|\le d}\alpha_s^{\ 2} \quad \text{where} \quad (g,h)=\frac{1}{2^n}\sum_x g(x)h(x)$$

$$\Leftrightarrow q_j^T\cdot \hat{F}_d\cdot q_j \ge (1-2\varepsilon)\cdot q_j^T\cdot q_j \quad \text{where} \quad \left[\hat{F}_d\right]_{s:|s|\le d,\, s':|s'|\le d} = -\left(\chi_{s\oplus s'},\hat{f}\right)$$

$$\Leftrightarrow \left\langle q_j\middle|\hat{F}_d\middle|q_j\right\rangle \ge (1-2\varepsilon)\cdot\left\langle q_j\middle|q_j\right\rangle$$

It follows that the largest eigenvalue of $\hat{F}_d$ must be at least $(1-2\varepsilon)$

Actually, it tends to 0, unless $d \ge n/2 - o(n)$.

Eiropas Sociālā fonda projekts “Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku” Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Proof of our result

- Particularly, we proved that with probability $1 - o(n)$:

$$\left\|\hat{F}_d\right\|_\infty = O\left(\sqrt{\frac{nB^{1+o(1)}}{2^n}}\right) \quad \text{where} \quad B = \sum_{i=0}^{d} \binom{n}{i}$$

$$\text{Since} \quad \left\|\hat{F}_d\right\|_\infty \geq 1 - 2\varepsilon, \quad \text{we get} \quad B \geq 2^{n-o(n)}$$

It is well known that $B \leq 2^{nH(d/n)}$ where H is the binary entropy function

So $2^{nH(d/n)} \geq 2^{n-o(n)}$ which implies $d \geq n/2 - o(n)$.

Eiropas Sociālā fonda projekts “Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku” Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Proof of our result

- The estimation of the largest eigenvalue:

$$\mathop{\mathrm{E}}_{f}\left\|\hat{F}_d\right\|_\infty = \mathop{\mathrm{E}}_{f}\max_i\left|\lambda_i\right| \le \sqrt[2k]{\mathop{\mathrm{E}}_{f}\max_i \lambda_i^{2k}} \le \sqrt[2k]{\mathop{\mathrm{E}}_{f}\sum_i \lambda_i^{2k}} = \sqrt[2k]{\mathop{\mathrm{E}}_{f}\mathrm{Tr}\left(\hat{F}_d^{2k}\right)}$$

Estimating $\mathop{\mathrm{E}}_{f}\mathrm{Tr}\left(\hat{F}_d^{2k}\right)$ by writing out $\mathrm{Tr}\left(\hat{F}_d^{2k}\right)$ explicitly and algebraically manipulating it leads to the result

Eiropas Sociālā fonda projekts "Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku" Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Open problem 1998–2014

- Where exactly between $n/2$ and n is the exact query complexity Q_E of a random Boolean function?

Thank you for attention!

Questions?

Eiropas Sociālā fonda projekts “Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku” Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044