Algorithmic Polynomials

Alexander Sherstov
UCLA

Approximate degree

$f : X \to \mathbb{R}, \qquad X \subseteq \{0,1\}^n$

Definition (Nisan-Szegedy 1992)

The ϵ-*approximate degree* of f is the minimum degree of a polynomial $\tilde{f}$ such that

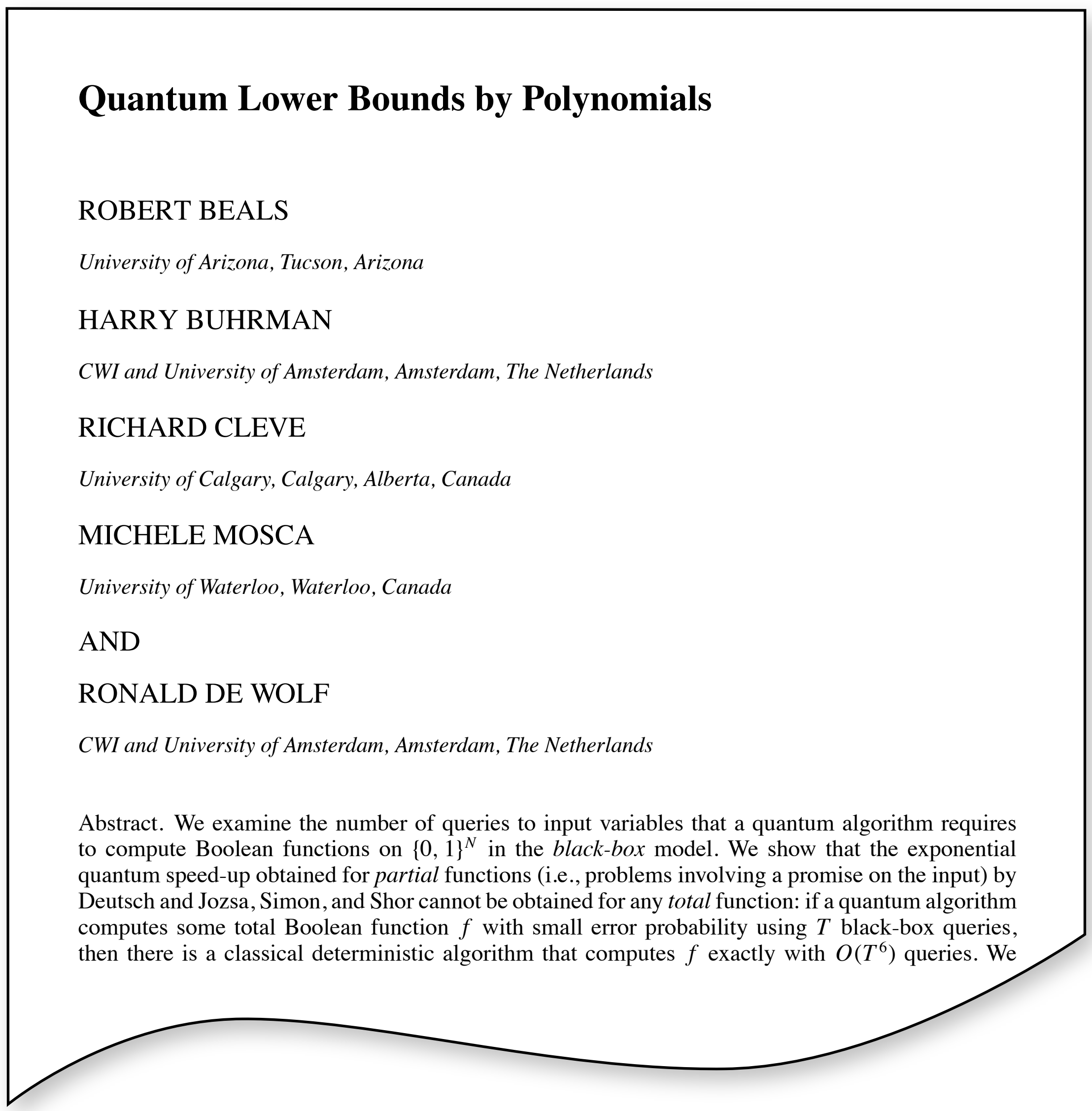
$$|f(x) - \tilde{f}(x)| \le \epsilon \qquad \forall x.$$

} $\deg_\epsilon(f)$

Motivation

- **Circuit complexity**
  [PS94, SRK94, BRS95, ABFR94, KP97, KP98, S09, BH12]
- **Quantum query complexity**
  [BBC+01, BCWZ99, AS04, A05, A05, KŠW07, BKT17]
- **Communication complexity**
  [BW01, R02, BVW07, S09, S11, RS10, LS09, CA08, S08, BH12, S14, S16]
- **Learning theory**
  [TT99, KS04, KOS04, KKMS08, OS10, ACR+10]
- **Algorithm design**
  [LN90, KLS96, S09]
- **Differential privacy**
  [TUV12, CTUW14]

A watershed moment


Quantum Lower Bounds by Polynomials

ROBERT BEALS

University of Arizona, Tucson, Arizona

HARRY BUHRMAN

CWI and University of Amsterdam, Amsterdam, The Netherlands

RICHARD CLEVE

University of Calgary, Calgary, Alberta, Canada

MICHELE MOSCA

University of Waterloo, Waterloo, Canada

AND

RONALD DE WOLF

CWI and University of Amsterdam, Amsterdam, The Netherlands

Abstract. We examine the number of queries to input variables that a quantum algorithm requires to compute Boolean functions on $\{0, 1\}^N$ in the *black-box* model. We show that the exponential quantum speed-up obtained for *partial* functions (i.e., problems involving a promise on the input) by Deutsch and Jozsa, Simon, and Shor cannot be obtained for any *total* function: if a quantum algorithm computes some total Boolean function f with small error probability using T black-box queries, then there is a classical deterministic algorithm that computes f exactly with $O(T^6)$ queries. We

Beals, Buhrman, Cleve, Mosca, de Wolf (1998): A quantum query algorithm for f with T queries gives an approximating polynomial for f of degree $2T$.

Virtually all known upper bounds on approximate degree come from quantum algorithms!

Beyond quantum?

"Quantum" polynomials are in general:

- nonconstructive
- more complicated
- less efficient

We construct first-principles approximating polynomials for key functions, matching or improving on quantum.

Our results: Symmetric fns

basic building block in the area

Theorem 1. Let $f : \{0,1\}^n \to \{0,1\}$ be ~~symmetric and~~ constant for inputs of Hamming weight in $(k, n-k)$. Then

$$\deg_\epsilon(f) = O\left(\sqrt{nk + n \log \frac{1}{\epsilon}}\right)$$

- Complete characterization
- Reproves quantum bound (de Wolf 2008)
- Explicit, first-principles proof **— three of them**

Our results: Element distinctness

key problem in quantum query complexity [BDH+05, AS04, A07, A05, K05, B12]

Element Distinctness
Given n integers from a range of size r, are they distinct?

Input representation:

0	0	1	0	0	0	0
0	0	0	1	0	0	0
0	0	1	0	0	0	0
0	0	0	0	1	0	0
0	0	0	0	0	1	0
0	1	0	0	0	0	0
1	0	0	0	0	0	0
0	0	0	0	0	0	1

n

r

Our results: Element distinctness

$$\mathrm{ED}_{n,r} : \{0,1\}^{n \times r}_{\leq n} \to \{0,1\}$$

$$\mathrm{ED}_{n,r}(x) = \begin{cases} 1 & \text{if } x_{1,j} + x_{2,j} + \cdots + x_{n,j} < 2 \qquad \forall j, \\ 0 & \text{otherwise} \end{cases}$$

Our results: Element distinctness

$$\mathrm{ED}_{n,r,k} : \{0,1\}^{n\times r}_{\leq n} \to \{0,1\}$$

$$\mathrm{ED}_{n,r,k}(x) = \begin{cases} 1 & \text{if } x_{1,j} + x_{2,j} + \cdots + x_{n,j} < k \qquad \forall j, \\ 0 & \text{otherwise} \end{cases}$$

Theorem 2.

$$\deg_{1/3}(\mathrm{ED}_{n,r,k}) = O\left(\sqrt{n}\min\{n,r\}^{\frac{1}{2}-\frac{1}{4(1-2^{-k})}}\right).$$

- Re-proves and generalizes best quantum bound (Belovs 2012, $r = \infty$)
- Explicit, first-principles construction

Our results: *k*-DNFs, *k*-CNFs

most general class of fns in quantum query complexity

Theorem 3. Let $f : \{0,1\}^N_{\leq n} \to \{0,1\}$ be representable by a k-DNF or k-CNF formula. Then

$$\deg_{1/3}(f) = O(n^{\frac{k}{k+1}}).$$

- No dependence on N
- Re-proves and generalizes best quantum bound (Ambainis 2003, Childs & Eisenberg 2005)
- Explicit, first-principles construction

Surjectivity

$$\mathrm{SURJ}_{n,r} \colon \{0,1\}^{n\times r}_{\leq n} \to \{0,1\}$$

$$\mathrm{SURJ}_{n,r}(x) = \bigwedge_{j=1}^{r} \bigvee_{i=1}^{n} x_{i,j}$$

Theorem 4.

$$\deg_{1/3}(\mathrm{SURJ}_{n,r}) = \begin{cases} O(\sqrt{n}\, r^{1/4}) & r \leq n, \\ 0 & \text{otherwise} \end{cases}$$

$$= O(n^{3/4}).$$

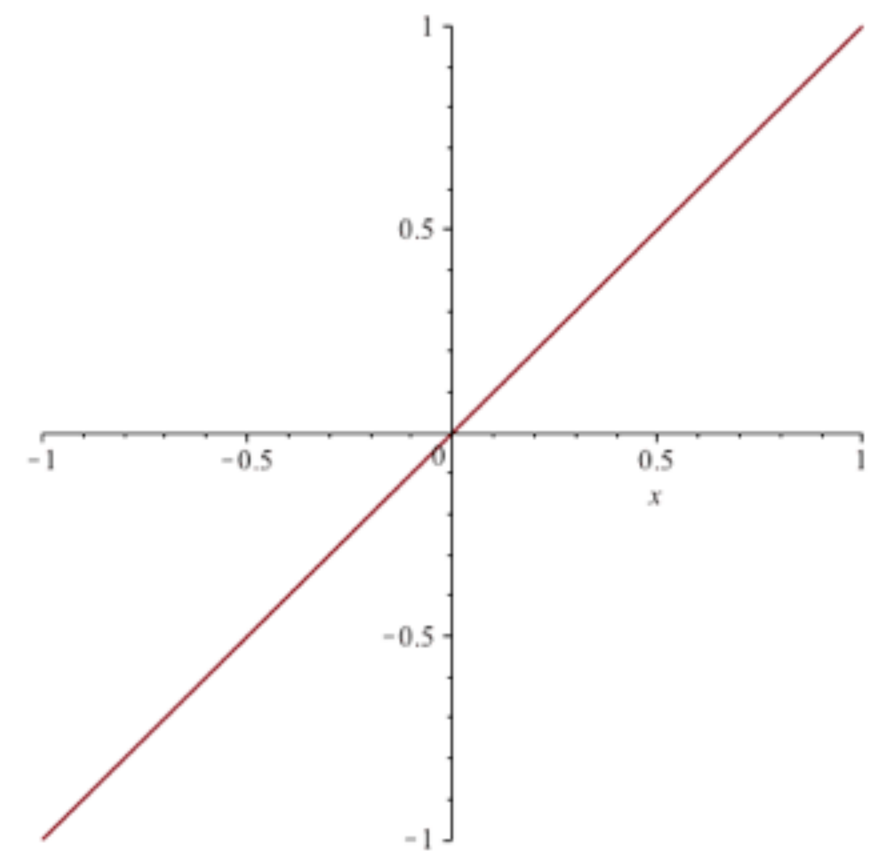
- Beats quantum query complexity: $\Theta(n)$ (Beame & Machmouchi 2012)
- First natural separation of approx. degree & quantum query complexity
- Disproves conjecture on SURJ

OUR TOOLS

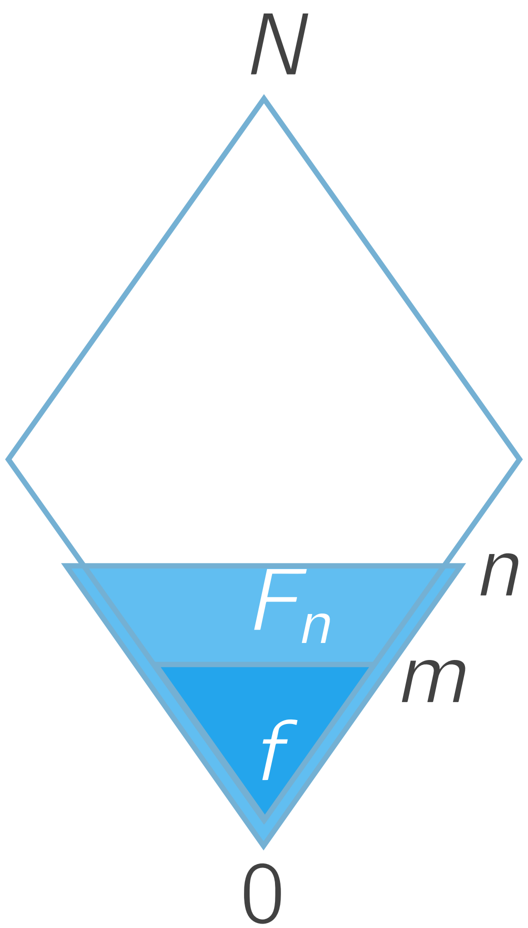
Chebyshev polynomials

$$T_d(x) = 2^{d-1} \prod_{i=1}^{d} \left(x - \cos\left(\frac{2i-1}{2d} \pi \right) \right)$$

- Bounded by ±1 on [–1,+1]
- Extremal growth on $(1, \infty)$



Extension theorem



$$f\colon \{0,1\}^N_{\le m} \to [0,1]$$

Extension:

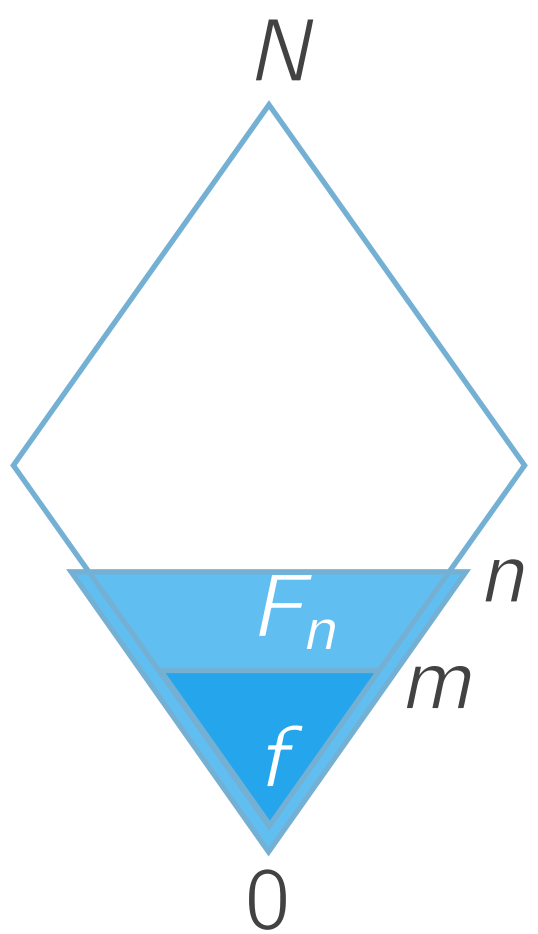
$$F_n\colon \{0,1\}^N_{\le n} \to [0,1]$$

$$F_n(x) = \begin{cases} f(x) & \text{if } |x| \le m, \\ 0 & \text{otherwise} \end{cases}$$

Efficiently transform approximants for ~~*f*~~ into approximants for *F_n*

Impossible!
Use *F_{2m}*

Extension theorem



$$f : \{0,1\}^N_{\le m} \to [0,1]$$

Extension:

$$F_n : \{0,1\}^N_{\le n} \to [0,1]$$

$$F_n(x) = \begin{cases} f(x) & \text{if } |x| \le m, \\ 0 & \text{otherwise} \end{cases}$$

✔ **Optimal**

Theorem (This work).

$$\deg_{\epsilon+\delta}(F_n) \le O\left(\sqrt{\frac{n}{m}}\right) \cdot \left(\deg_\epsilon(F_{2m}) + \log\frac{1}{\delta}\right)$$

Decoupling theorem

$$F\colon \{0,1\}^N_{\le n} \times \mathcal{Y} \to \{0,1\}$$

$$F(x,y) = \bigvee_{i=1}^{N} x_i \wedge f_i(y)$$

Theorem (This work).

$$\deg_\epsilon(F) \le \sqrt{nb \log \frac{1}{\epsilon}} + \max_{|S| \le \sqrt{nb\log\frac{1}{\epsilon}}} \deg_{\epsilon \exp(-\frac{n}{b}\log\frac{1}{\epsilon})}\left(\bigvee_{i\in S} f_i\right)$$

x part

y part

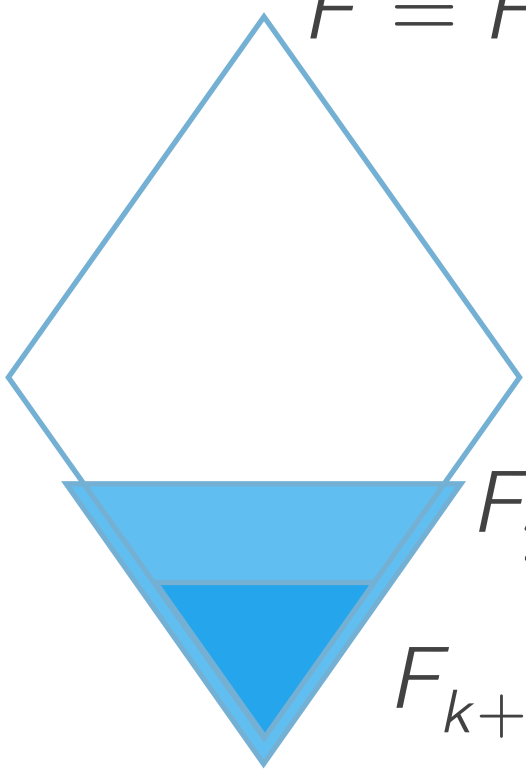
PROOF SKETCHES

Symmetric functions

Theorem 1. Let $F\colon \{0,1\}^n \to \{0,1\}$ be ~~symmetric and~~ constant for inputs of Hamming weight ~~in $(k, n-k)$.~~ $> k$ Then

$$\deg_\epsilon(F) = O\left(\sqrt{nk + n\log\frac{1}{\epsilon}}\right)$$

Proof sketch



$F\colon \{0,1\}^n \to [0,1]$

$F(x) = 0$ for $|x| \geq k$

$\leq 2\left(k + \log\frac{1}{\epsilon}\right)$

By Extension Thm,

$$\deg_{0+\epsilon}(F) = O\left(\sqrt{\frac{n}{k+\frac{1}{\epsilon}}}\right) \cdot \left(\deg_0\left(F_{2\left(k+\log\frac{1}{\epsilon}\right)}\right) + \log\frac{1}{\epsilon}\right)$$

Surjectivity

$$\mathrm{SURJ}_{n,r} \colon \{0,1\}^{n\times r}_{\leq n} \to \{0,1\}$$

$$\mathrm{SURJ}_{n,r}(x) = \bigwedge_{j=1}^{r} \bigvee_{i=1}^{n} x_{i,j}$$

Theorem 4.

$$\deg_{1/3}(\mathrm{SURJ}_{n,r}) = \begin{cases} O(\sqrt{n}\, r^{1/4}) & r \leq n, \\ 0 & \text{otherwise} \end{cases}$$

Proof sketch

$$\mathrm{SURJ}_{n,r}(x) = \bigwedge_{j=1}^{r} (x_{1j} \vee x_{2j} \vee \cdots \vee x_{nj})$$

approximate
by Chebyshev

$$\approx \frac{T_{\sqrt{3r}}\left(\frac{1}{r} + \frac{1}{r}\sum_{j=1}^{r}(x_{1j} \vee x_{2j} \vee \cdots \vee x_{nj})\right)}{T_{\sqrt{3r}}\left(\frac{1}{r}+1\right)}$$

multiply
out

$$= \frac{T_{\sqrt{3r}}\left(\frac{1}{r} + 1 - \frac{1}{r}\sum_{j=1}^{r}\prod_{i=1}^{n}\overline{x}_{ij}\right)}{T_{\sqrt{3r}}\left(\frac{1}{r}+1\right)}$$

Proof sketch

approximate
each to within $2^{-\Theta(\sqrt{r})}$
using degree $O(\sqrt{n\sqrt{r}})$

$\therefore$ $\mathrm{SURJ}_{n,r} \approx$ linear combination of monomials with coefficients that sum in absolute value to $2^{\Theta(\sqrt{r})}$

k-DNF formulas

Theorem 3. Let $f\colon \{0,1\}^N_{\leq n} \to \{0,1\}$ be representable by a k-DNF or k-CNF formula. Then

$$\deg_{1/3}(f) = O(n^{\frac{k}{k+1}}).$$

Note: no dependence on N.

Proof sketch

Let

$$D(n, k, \epsilon) = \max_F \deg_\epsilon(F)$$

where the maximum is over k-DNFs

$$F\colon \{0,1\}^N_{\leq n} \to \{0,1\}$$

where N is unbounded.

Proof sketch

$$D(n, k, \epsilon) \leq n$$

(from first principles)

$$D(n, k, \epsilon) \leq \sqrt{nb \log \frac{1}{\epsilon}} + D\left(n, k-1, \epsilon \cdot 2^{\sqrt{\frac{n \log(1/\epsilon)}{b}}}\right)$$

(using decoupling thm)

$$\therefore D(n, k, \epsilon) = O\left(n^{\frac{k}{k+1}} \left(\log \frac{1}{\epsilon}\right)^{\frac{1}{k+1}}\right). \quad \blacksquare$$

Element distinctness

$$\mathrm{ED}_{n,r,k} \colon \{0,1\}^{n\times r}_{\le n} \to \{0,1\}$$

$$\mathrm{ED}_{n,r,k}(x) = \begin{cases} 1 & \text{if } x_{1,j} + x_{2,j} + \cdots + x_{n,j} < k \qquad \forall j, \\ 0 & \text{otherwise} \end{cases}$$

Theorem 2.

$$\deg_{1/3}(\mathrm{ED}_{n,r,k}) = O\left(\sqrt{n}\min\{n,r\}^{\frac{1}{2}-\frac{1}{4(1-2^{-k})}}\right).$$

Proof sketch

Let

$$D(n, r, k, \epsilon) = \max_F \deg_\epsilon(F)$$

where the maximum is over all

$$F\colon \{0,1\}^N_{\leq n} \to \{0,1\}$$

such that

$$F(x) = \bigvee_{i=1}^{r} \mathrm{THR}_k(x|_{S_i})$$

for pairwise disjoint $S_1, S_2, \ldots, S_r$

$\deg_\epsilon(\mathrm{ED}_{n,r,k})$

$\leq D(n, r, k, \epsilon)$

Proof sketch

$$D(n, \infty, k, \epsilon) \leq n$$

(from first principles)

$$D(n, r, k, \epsilon) \leq \sqrt{\frac{n}{kr}} \cdot O\left(D\left(2kr, r, k, \frac{\epsilon}{2}\right) + \log\frac{1}{\epsilon}\right)$$

(using extension thm)

$$D(n, \infty, k, \epsilon) \leq \sqrt{nb\log\frac{1}{\epsilon}} + \left(1 + \frac{1}{\sqrt{k}}\left(\frac{n}{b\log\frac{1}{\epsilon}}\right)^{1/4}\right) \times$$

$$\times \left(D\left(k\sqrt{nb\log\frac{1}{\epsilon}}, \infty, k-1, 2^{\sqrt{\frac{n\log(1/\epsilon)}{b}}+1}\right) + \sqrt{\frac{n\log\frac{1}{\epsilon}}{b}}\right)$$

(using decoupling + extension thms)

Proof sketch

Solving the recurrence gives:

$$D(n, r, k, \epsilon) \leq O\left(\sqrt{n}\min\{n, kr\}^{\frac{1}{2}-\frac{1}{4(1-2^{-k})}} \log^{\frac{1}{4(1-2^{-k})}} \frac{1}{\epsilon} + \sqrt{n \log \frac{1}{\epsilon}}\right). \quad \blacksquare$$

Open problems

- Does **depth-d AC⁰** have approximate degree $O(n^{1-\epsilon_d})$ for some $\epsilon_d > 0$?

Yes, for linear-size circuits (Bun, Kothari, & Thaler, ECCC 2018)

- Matching lower bound for ***k*-element distinctness**

- Matching lower bound for ***k*-DNF formulas**

- ~~Matching lower bound for **surjectivity**~~

solved by Bun, Kothari, & Thaler (FOCS 2017)

Questions?