# A Polynomial Lower Bound for Monotonicity Testing of Boolean Functions

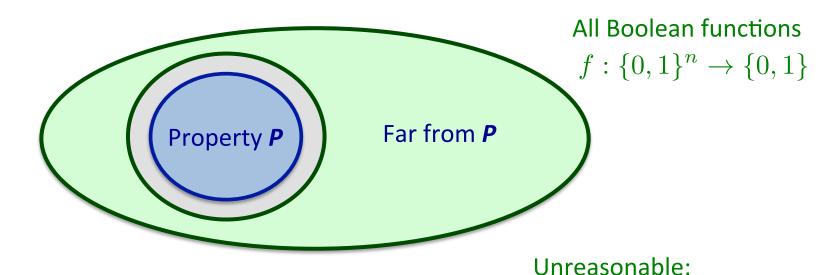
Joint work with Xi Chen and Rocco Servedio





# **Property Testing**

Simplest question about a Boolean function: Does it have some property **P**?



Easy lower bound of  $\Omega(2^n)$ 

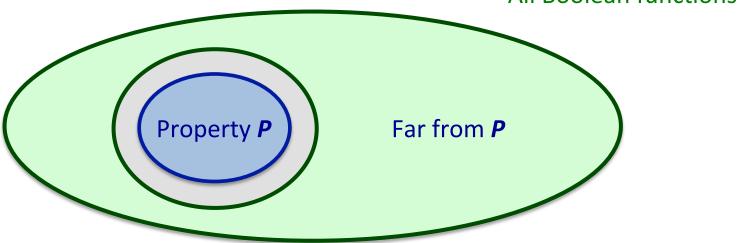
- Query access to unknown f on any input x
- With as few queries as possible, decide if

f has Property P vs. f does not have Property P

f is far from having Property P

## Rules of the game

All Boolean functions



Query access to unknown f on any input x

- 1. If f has Property P, accept w.p. > 2/3.
- 2. If f is  $\varepsilon$ -far from having Property P, reject w.p. > 2/3.
- 3. Otherwise: doesn't matter what we do.

# Super-efficient algorithms

Sublinear Space
Streaming,
Sketching

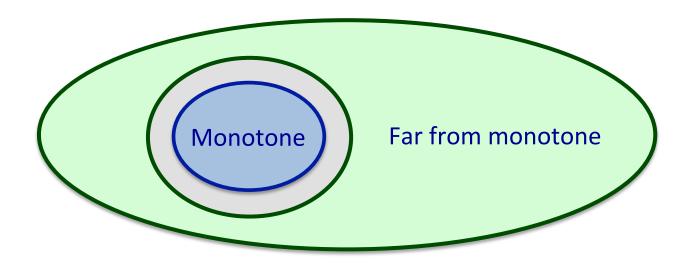
**Sublinear Time Property Testing** 

Sublinear Measurement
Sparse Recovery,
Compressed Sensing

#### Two recurring messages:

- Many properties P testable with surprisingly few queries.
- 2. Rich connections with many other areas:
  - Learning theory
  - Hardness of approximation
  - Communication complexity
  - ...

# This work: *P* = monotonicity



#### Well-studied problem:

[GGR98, GGL+98, DGL+99, FLN+02, HK08, BCGM12, RRS+12, BBM12, BRY13, CS13, ...] but still significant gaps in our understanding.

#### This talk

- The natural tester and its analysis [Goldreich et al. 1998]
- Our main result:

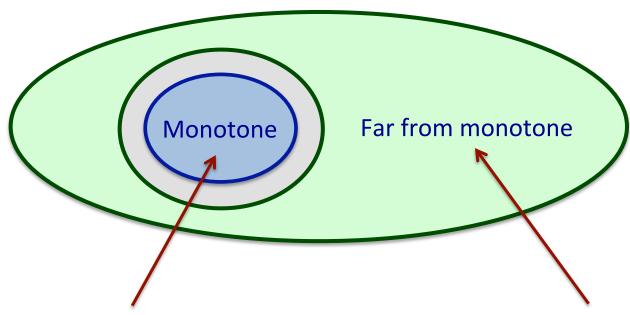
A **polynomial lower bound** on query complexity

Our main technical ingredient:

**Multidimensional Central Limit Theorems** 

Generalizing our main result: Testing monotonicity on hypergrids

# A quick reminder



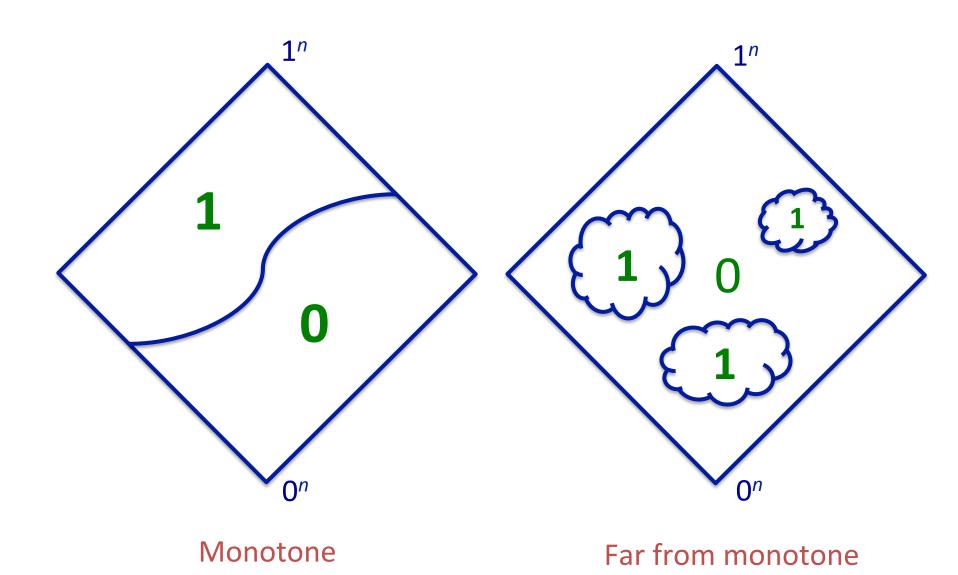
A monotone function is one that satisfies:

For all monotone functions *g*:

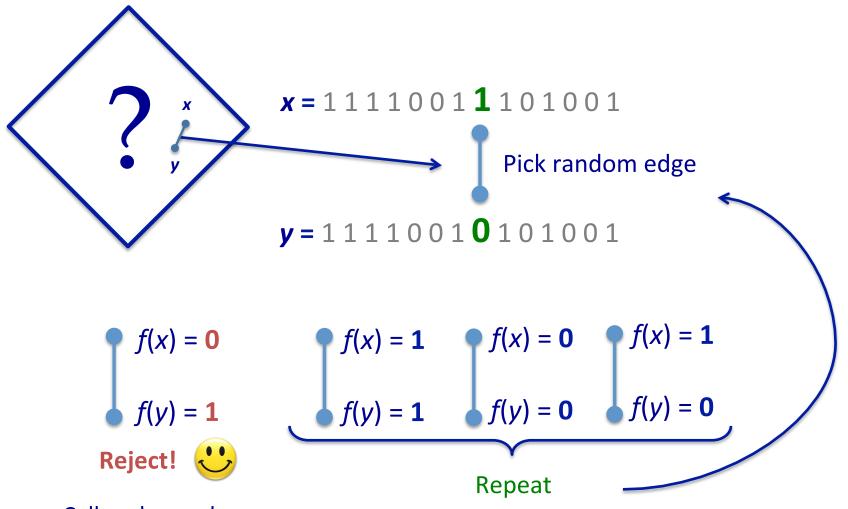
$$\forall \underline{x} \leq \underline{y}, \ f(x) \leq f(y)$$
 
$$\Pr_{\mathbf{x} \in \{0,1\}^n} [f(\mathbf{x}) \neq g(\mathbf{x})] \geq \varepsilon$$

$$x_i \leq y_i \ \forall i \in [n]$$

"Flipping an input bit from  ${\bf 0}$  to  ${\bf 1}$  cannot make f go from  ${\bf 1}$  to  ${\bf 0}$ "

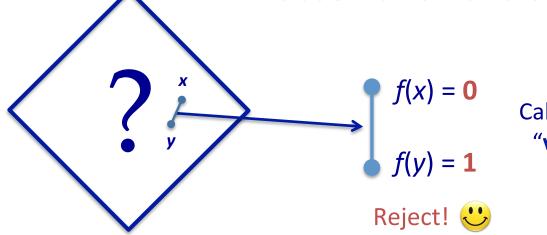


#### First test that comes to mind



Call such an edge a "violating edge"

## An observation and a theorem



Call such an edge a "violating edge"

Tester = Sample random edges, check for violations.

**Simple observation**: If *f* is monotone, tester never rejects.

**Question**: If f is  $\varepsilon$ -far from monotone, how likely to catch violating edge?

#### **Theorem** [Goldreich *et al.* 1998, 2000]

If f is  $\varepsilon$ -far from monotone,  $\Omega(\varepsilon/n)$  fraction of edges are violations. Therefore tester will reject within  $O(n/\varepsilon)$  queries.

## An exponential gap

- Goldreich et al. [FOCS 1998, SICOMP 2000]
  - Introduced problem, gave tester with O(n) query complexity.
- Fischer et al. [STOC 2002]
  - Any non-adaptive tester must make  $\Omega(\log n)$  queries.
  - Therefore, any adaptive tester must make  $\Omega(\log \log n)$  queries.

[GGR98, DGL+99, HK08, BCGM12, RRS+12, BRY13, CS13, ...]

- Chakrabarty-Seshadhri [STOC 2013]
  - $O(n^{7/8})$ -query non-adaptive tester!





#### **Theorem** [Chen-Servedio-T 2014]

Any non-adaptive tester must make  $\widetilde{\Omega}(n^{1/5})$  queries. Therefore, any adaptive tester must make  $\Omega(\log n)$  queries.

Exponential improvements over  $\Omega(\log n)$  and  $\Omega(\log \log n)$  lower bounds of Fischer *et al.* (2002)

#### Theorem [Chen-Servedio-T 2014]

There is a non-adaptive tester that makes  $\widetilde{O}(n^{5/6})$  queries.

Polynomial improvement over  $O(n^{7/8})$  upper bound of Chakrabarty and Sheshadhri (2013)

# Yao's minimax principle

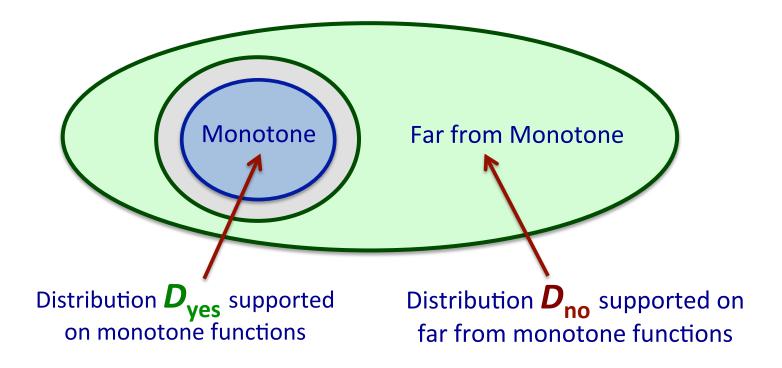
Lower bound against randomized algorithms



Tricky distribution over inputs to **deterministic** algorithms



# Yao's principle in our setting



**Indistinguishability.** For all T = deterministic tester that makes  $o(n^{1/5})$  queries,

$$\left| \frac{\mathbf{Pr}}{\mathbf{f}_{yes} \sim \mathcal{D}_{yes}} \left[ \mathcal{T} \ accepts \ \mathbf{f}_{yes} \right] - \frac{\mathbf{Pr}}{\mathbf{f}_{no} \sim \mathcal{D}_{no}} \left[ \mathcal{T} \ accepts \ \mathbf{f}_{no} \right] \right| = o_n(1)$$

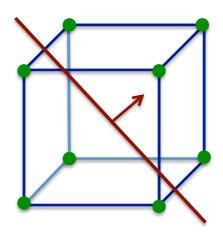
# Our $D_{\text{ves}}$ and $D_{\text{no}}$ distributions

Both supported on *Linear Threshold Functions* (LTFs) over  $\{-1,1\}^n$ :

$$f(x) = \operatorname{sign}(w_1)x_1 + \ldots + w_n x_n) \quad \vec{w} \in \mathbb{R}^n$$

 $D_{\text{ves}}$ :  $\sigma_i$  = uniform from {1,3}

 $D_{\text{no}}$ :  $\nu_i = -1$  with prob 0.1, 7/3 with prob 0.9



**Verify:**  $D_{\text{ves}}$  LTFs are monotone,  $D_{\text{no}}$  LTFs far from monotone w.h.p.

#### Main Structural Result: Indistinguishability

Any deterministic tester that makes few queries cannot tell  $D_{
m yes}$  from  $D_{
m no}$ 

Key property: 
$$\mathbb{E}[m{\sigma_i}] = \mathbb{E}[m{
u_i}]$$
 ,  $ext{Var}[m{\sigma}_i] = ext{Var}[m{
u}_i]$  .

# Indistinguishability

$$q = 1$$
 query

Claim. For all T = deterministic tester that makes  $q = o(n^{1/5})$  queries,

$$\left| \frac{\mathbf{Pr}}{\mathbf{f}_{yes} \sim \mathcal{D}_{yes}} \left[ \mathcal{T} \ accepts \ \mathbf{f}_{yes} \right] - \frac{\mathbf{Pr}}{\mathbf{f}_{no} \sim \mathcal{D}_{no}} \left[ \mathcal{T} \ accepts \ \mathbf{f}_{no} \right] \right| = o_n(1)$$

## Non-trivial proof of a triviality

**Claim.** Let T = deterministic tester that makes 1 query **z**. Then:

$$\left| \frac{\mathbf{Pr}}{\mathbf{f}_{yes} \sim \mathcal{D}_{yes}} \left[ \mathcal{T} \ accepts \ \mathbf{f}_{yes} \right] - \frac{\mathbf{Pr}}{\mathbf{f}_{no} \sim \mathcal{D}_{no}} \left[ \mathcal{T} \ accepts \ \mathbf{f}_{no} \right] \right| = o_n(1)$$

$$(*) \leq d_{\mathrm{TV}}(\mathbf{R}_{yes}, \mathbf{R}_{no})$$

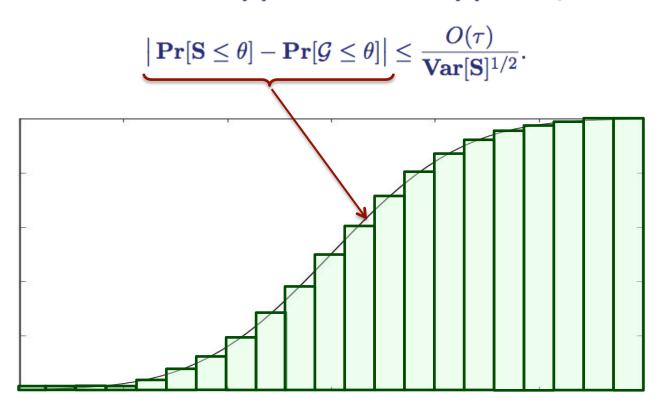
Tester sees:

$$\mathbf{R}_{yes} = \operatorname{sign}(\boldsymbol{\sigma}_1 z_1 + \dots + \boldsymbol{\sigma}_n z_n) \quad \text{vs.} \quad \mathbf{R}_{no} = \operatorname{sign}(\boldsymbol{\nu}_1 z_1 + \dots + \boldsymbol{\nu}_n z_n)$$

**Central Limit Theorems.** Sum of many independent "reasonable" random variables converges to Gaussian of same mean and variance.

#### Main analytic tool (Baby version):

**Berry–Esséen CLT.** Let  $\mathbf{S} = \mathbf{X}_1 + \cdots + \mathbf{X}_n$  where  $\mathbf{X}_1, \ldots, \mathbf{X}_n$  are independent real-valued random variables satisfying  $|\mathbf{X}_j - \mathbf{E}[\mathbf{X}_j]| \leq \tau$  with probability 1 for all  $j \in [n]$ . Let  $\mathcal{G}$  be a Gaussian with mean  $\mathbf{E}[\mathbf{S}]$  and variance  $\mathbf{Var}[\mathbf{S}]$ . Then for all  $\theta \in \mathbb{R}$ ,



Goal: Upper bound  $d_{\text{TV}}(\text{sign}(\mathbf{S}_{yes}), \text{sign}(\mathbf{S}_{no}))$ 

$$\mathbf{S}_{yes} = \boldsymbol{\sigma_1} z_1 + \dots + \boldsymbol{\sigma_n} z_n$$
  $\mathbf{S}_{no} = \boldsymbol{\nu_1} z_1 + \dots + \boldsymbol{\nu_n} z_n$   $\mathbf{S}_{yes} \rightarrow \mathcal{G}_1$   $\mathbf{S}_{no} \rightarrow \mathcal{G}_2$ 

Recall key property:

$$egin{aligned} \mathbb{E}[oldsymbol{\sigma_i}] &= \mathbb{E}[oldsymbol{
u_i}] \ \mathbf{Var}[oldsymbol{\sigma}_i] &= \mathbf{Var}[oldsymbol{
u_i}] \end{aligned} egin{aligned} &\mathbb{E}[\mathbf{S}_{yes}] &= \mathbb{E}[\mathbf{S}_{no}] \ \mathbf{Var}[\mathbf{S}_{yes}] &= \mathbf{Var}[\mathbf{S}_{no}] \ \mathcal{G}_1 &= \mathcal{G}_2 \end{aligned}$$

## We just proved:

Claim. Let T = deterministic tester that makes 1 query. Then:

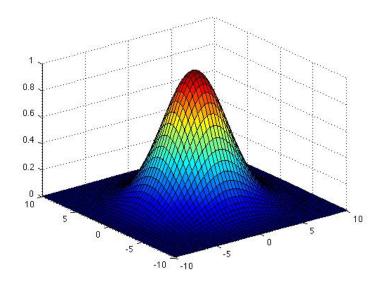
$$igg| egin{aligned} & \mathbf{Pr} \\ oldsymbol{f}_{yes} \sim \mathcal{D}_{yes} \end{aligned} igg[ \mathcal{T} \ accepts \ oldsymbol{f}_{yes} igg] - oldsymbol{Pr} \\ oldsymbol{f}_{no} \sim \mathcal{D}_{no} \end{aligned} igg[ \mathcal{T} \ accepts \ oldsymbol{f}_{no} igg] igg| = O(n^{-1/2})$$

Plenty of room to spare!
Would be happy with < 0.1

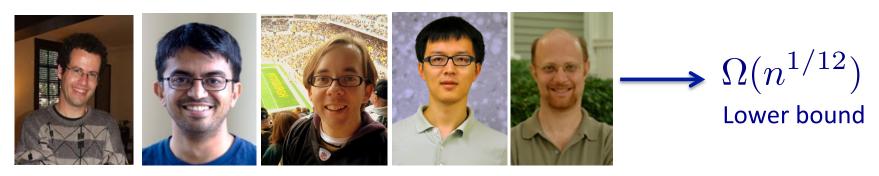
# q queries instead of 1

### Main analytic tool (Grown-up version):

Multidimensional CLTs. Sum of many independent "reasonable" q-dimensional random variables converge to q-dimensional Gaussian of same mean and variance.



### **Multidimensional CLTs**



[Mossel 08, Gopalan-O'Donnell-Wu-Zuckerman 10]



[Valiant-Valiant 11]

#### Main technical work:

Adapting multidimensional CLT for Earth Mover Distance to get

$$\widetilde{\Omega}(n^{1/5})$$

# Let's prove the real thing:

Claim. For all T = deterministic tester that makes  $q = o(n^{1/5})$  queries,

$$\left| \begin{array}{l} \mathbf{Pr} \\ \mathbf{f}_{yes} \sim \mathcal{D}_{yes} \end{array} \right[ \mathcal{T} \ accepts \ \mathbf{f}_{yes} \right] - \left| \begin{array}{l} \mathbf{Pr} \\ \mathbf{f}_{no} \sim \mathcal{D}_{no} \end{array} \right[ \mathcal{T} \ accepts \ \mathbf{f}_{no} \right] \right| = o_n(1)$$

# Setting things up

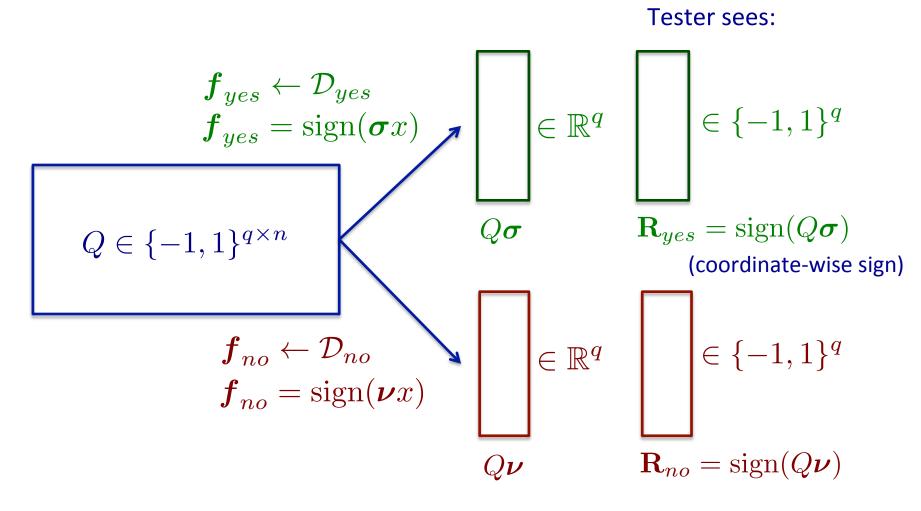
Arrange the q queries of tester T in a q x n matrix  $\mathbf{Q} \in \{-1,1\}^{q \times n}$ 

$$egin{array}{c} Q_1 \ Q_2 \ Q_3 \ & Q \in \{-1,1\}^{q imes n} \ & Q_i = \emph{i-} ext{th query string} \ & Q_q \ & & & & & & & & \end{array}$$

Recall: Tester's goal is to distinguish

$$oldsymbol{f}_{yes} = ext{sign}(oldsymbol{\sigma} x) ext{ versus } oldsymbol{f}_{no} = ext{sign}(oldsymbol{
u} x)$$

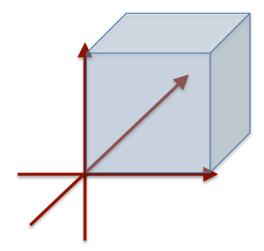
#### What does the tester see?



Goal: Upper bound  $d_{\mathrm{TV}}(\mathbf{R}_{yes}, \mathbf{R}_{no}) = d_{\mathrm{TV}}(\mathrm{sign}(Q\boldsymbol{\sigma}), \mathrm{sign}(Q\boldsymbol{\nu}))$ 

Goal: Upper bound 
$$d_{\mathrm{TV}}(\mathbf{R}_{yes}, \mathbf{R}_{no}) = d_{\mathrm{TV}}(\mathrm{sign}(Q\boldsymbol{\sigma}), \mathrm{sign}(Q\boldsymbol{\nu}))$$

$$\{\pm 1\}^q$$



 $\mathbf{R}_{yes} \equiv \text{orthant of } \mathbb{R}^q \text{ that } Q\boldsymbol{\sigma} \text{ falls in } \mathbf{R}_{no} \equiv \text{orthant of } \mathbb{R}^q \text{ that } Q\boldsymbol{\nu} \text{ falls in }$ 

Random variables supported on  $2^q$  orthants of  $R^q$ 

$$d_{\text{TV}}(\mathbf{R}_{yes}, \mathbf{R}_{no}) = \sum_{\substack{2^q \text{ orthants} \\ O_i \text{ of } \mathbb{R}^q}} \left| \Pr[Q\boldsymbol{\sigma} \in O_i] - \Pr[Q\boldsymbol{\nu} \in O_i] \right|$$

 $= \max_{\mathcal{O} \subseteq \mathbb{R}^q} \big| \Pr[Q \sigma \in \mathcal{O}] - \Pr[Q \nu \in \mathcal{O}] \big|$  union of orthants

"roughly equal weight on any union of orthants"

$$d_{\text{TV}}(\mathbf{R}_{yes}, \mathbf{R}_{no}) = \max_{\mathcal{O} \subseteq \mathbb{R}^q} \left| \Pr[Q\boldsymbol{\sigma} \in \mathcal{O}] - \Pr[Q\boldsymbol{\nu} \in \mathcal{O}] \right|$$

$$Q_{\star 1}$$
  $Q_{\star 2}$   $\dots$   $Q_{\star n}$   $Q_{1}$   $Q_{2}$   $Q_{2}$   $Q_{3}$   $Q_{4}$   $Q_{4}$   $Q_{4}$   $Q_{4}$   $Q_{4}$   $Q_{4}$   $Q_{4}$   $Q_{5}$   $Q_{7}$   $Q_{8}$   $Q_{8}$   $Q_{8}$   $Q_{8}$   $Q_{8}$   $Q_{8}$ 

Fixed 
$$Q {m \sigma} = \sum_{i=1}^n Q_{\star i} {m \sigma}_i$$
 Ditto:  $Q {m \nu} = \sum_{i=1}^n Q_{\star i} {m \nu}_i$  from product

distribution over  $R^n$  sum of n independent vectors in  $R^q$ 

$$\mathbb{E}[oldsymbol{\sigma_i}] = \mathbb{E}[oldsymbol{
u_i}] \ \mathbf{Var}[oldsymbol{\sigma_i}] = \mathbf{Var}[oldsymbol{
u_i}] \ \mathbf{Cov}[Qoldsymbol{\sigma}] = \mathbf{Cov}[Qoldsymbol{
u}] \ \mathbf{Cov}[Qoldsymbol{\sigma}] = \mathbf{Cov}[Qoldsymbol{
u}] \ \mathbf{Cov}[Qoldsymbol{
u}]$$

## The final setup

**Goal**: Two sums of *n* independent vectors in R<sup>q</sup> are "close"

$$Q\boldsymbol{\sigma} = \sum_{i=1}^{n} Q_{\star i} \boldsymbol{\sigma_i} \qquad Q\boldsymbol{\nu} = \sum_{i=1}^{n} Q_{\star i} \boldsymbol{\nu_i}$$

where closeness = roughly equal weight on any union of orthants.

Furthermore, since

$$\mathbb{E}[Qoldsymbol{\sigma}] = \mathbb{E}[Qoldsymbol{
u}]$$
  
 $\mathbf{Cov}[Qoldsymbol{\sigma}] = \mathbf{Cov}[Qoldsymbol{
u}]$ 

suffices to show each are close to *q*-dimensional Gaussian with matching mean and covariance matrix.

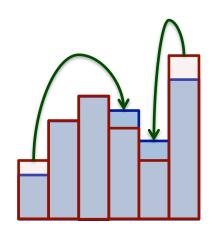
#### Valiant-Valiant Multidimensional CLT

Sum of many independent "reasonable" **q-dimensional** random variables is close to **q-dimensional** Gaussian of same mean and variance.

with respect to **Earth Mover Distance**:

Minimum amount of work necessary to "get one PDF to look like the other", where work := mass x distance





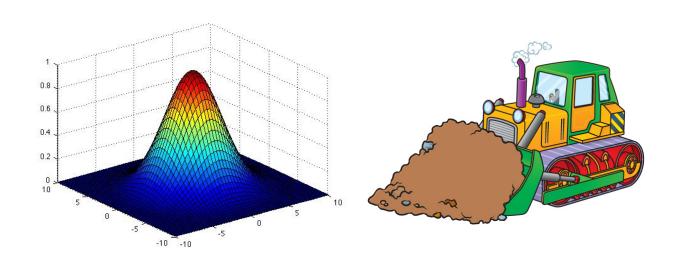
#### Key technical lemma:

Closeness in EMD —— roughly equal weight on any union of orthants

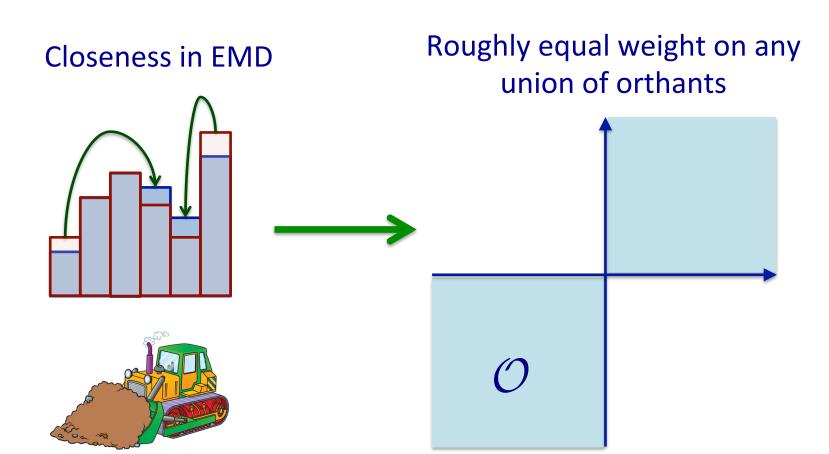
#### Valiant-Valiant Multidimensional CLT

Let  $\mathbf{S} = \mathbf{X}_1 + \cdots + \mathbf{X}_n$ , where the  $\mathbf{X}_j$ 's are independent  $\mathbb{R}^q$ -valued random variables satisfying  $\|\mathbf{X}_j - \mathbf{E}[\mathbf{X}_j]\|_2 \leq \tau$  with probability 1 for all  $j \in [n]$ . Let  $\mathcal{G}$  be the q-dimensional Gaussian with the same mean and covariance matrix as  $\mathbf{S}$ . Then

$$d_{\text{EMD}}(\mathbf{S}, \mathcal{G}) \le O(\tau q \log n).$$



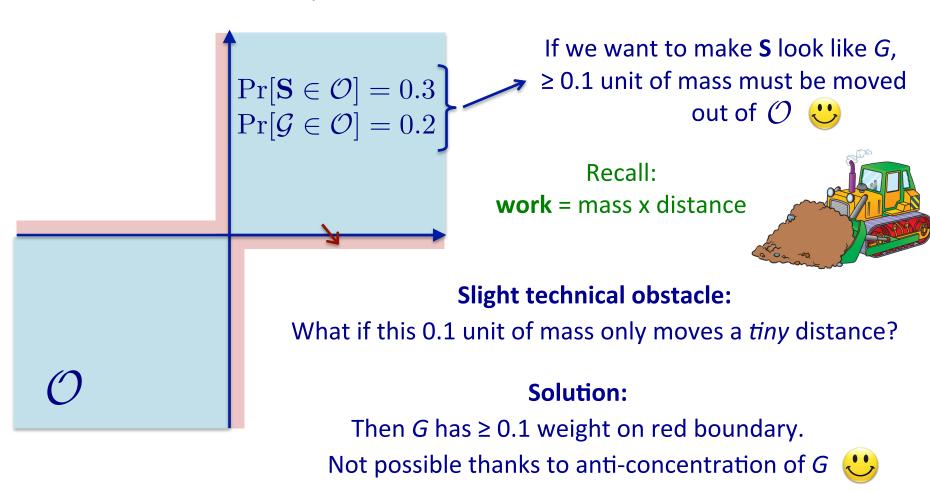
# Key technical lemma



$$d_{\text{EMD}}(\mathbf{S}, \mathcal{G}) \text{ small } \Longrightarrow |\Pr[\mathbf{S} \in \mathcal{O}] - \Pr[\mathcal{G} \in \mathcal{O}]| \text{ small}$$

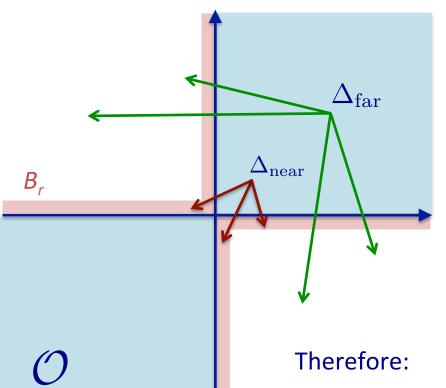
# $d_{\mathrm{EMD}}(\mathbf{S}, \mathcal{G}) \text{ small } \Longrightarrow |\Pr[\mathbf{S} \in \mathcal{O}] - \Pr[\mathcal{G} \in \mathcal{O}]| \text{ small}$ for all unions of orthants $\mathcal{O}$

Let's consider the contrapositive:



# In slightly more detail

$$\Pr[\mathbf{S} \in \mathcal{O}] - \Pr[\mathcal{G} \in \mathcal{O}] = \Delta$$
 , has to be moved out of  $\mathcal{O}$ 



For all r > 0, define  $B_r := \text{radius } r \text{ boundary around } \mathcal{O}$ 

$$\Delta = \Delta_{\rm near} + \Delta_{\rm far}$$

$$\Delta_{near} \le \Pr[\mathcal{G} \in B_r]$$

$$r \cdot \Delta_{far} \le d_{\text{EMD}}(\mathbf{S}, \mathcal{G})$$

$$\Pr[\mathbf{S} \in \mathcal{O}] - \Pr[\mathcal{G} \in \mathcal{O}] \le \frac{d_{\text{EMD}}(\mathbf{S}, \mathcal{G})}{r} + \Pr[\mathcal{G} \in B_r]$$

## We just proved

Let  $\mathbf{S} = \mathbf{X}_1 + \cdots + \mathbf{X}_n$ , where the  $\mathbf{X}_j$ 's are independent  $\mathbb{R}^q$ -valued random variables. Let  $\mathcal{G}$  be the q-dimensional Gaussian with the same mean and covariance matrix as  $\mathbf{S}$ . Then for all unions of orthants  $\mathcal{O} \subseteq \mathbb{R}^q$  and for all r > 0,

$$\left|\Pr[\mathbf{S} \in \mathcal{O}] - \Pr[\mathcal{G} \in \mathcal{O}]\right| \leq \frac{d_{\mathrm{EMD}}(\mathbf{S}, \mathcal{G})}{r} + \Pr[\mathcal{G} \in B_r]$$
Valiant-Valiant Gaussian anti-concentration

## Recap

**Indistinguishability.** For all  $T = \text{deterministic tester that makes } q = o(n^{1/5}) \text{ queries,}$ 

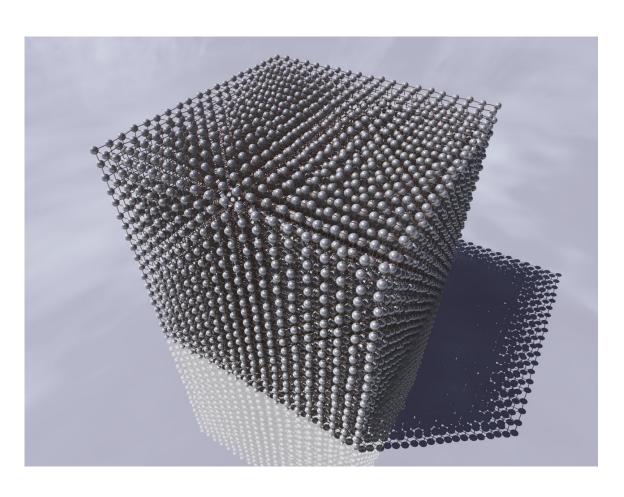
$$\left| \begin{array}{l} \mathbf{Pr} \\ \mathbf{f}_{yes} \sim \mathcal{D}_{yes} \end{array} \left[ \mathcal{T} \ accepts \ \mathbf{f}_{yes} 
ight] - \mathbf{Pr} \\ \mathbf{f}_{no} \sim \mathcal{D}_{no} \end{array} \left[ \mathcal{T} \ accepts \ \mathbf{f}_{no} 
ight] 
ight| = o_n(1)$$



#### **Theorem**

Any non-adaptive tester must make  $\,\widetilde{\Omega}(n^{1/5})$  queries. Therefore, any adaptive tester must make  $\,\Omega(\log n)$  queries.

# Testing monotonicity of Boolean functions over general hypergrid domains



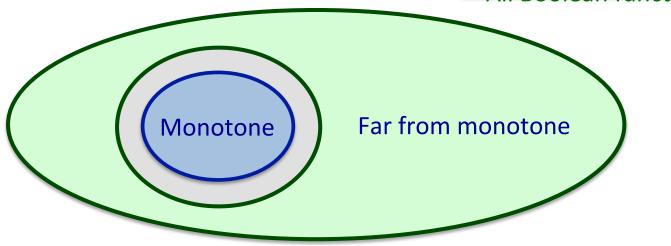
# Boolean functions over hypergrids

$$F: \{1, 2, \dots, m\}^n \to \{0, 1\}$$

Testing monotonicity of Boolean functions over hypergrids

#### All hypergrid functions

All Boolean functions



#### **Theorem** [Chen-Servedio-T 2014]

Any non-adaptive tester for testing monotonicity of  $f:[m]^n \to \{0,1\}$  must make  $\widetilde{\Omega}(n^{1/5})$  queries.

Proof by reduction to m=2 case (Boolean hypercube)

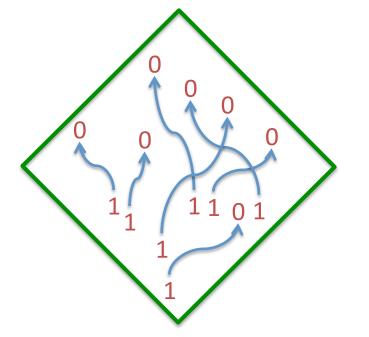
### A useful characterization

#### Theorem. [Dodis et al. 1999]

 $F:\{1,2,\ldots,m\}^n o \{0,1\}$  is  $\emph{arepsilon}$ -far from monotone



There exists  $\varepsilon \cdot m^n$  vertex-disjoint pairs  $(x_i, y_i) \in [m]^n$  such that  $x_i \leq y_i$  and  $f(x_i) > f(y_i)$ .



"violating pair"

(Upward direction is easy)

## Reducing to m = 2

Given any  $f:\{0,1\}^n \to \{0,1\}$ , define  $F:[m]^n \to \{0,1\}$  as follows:

$$F(\underline{x_1,\ldots,x_n}) = f(\underline{\mathbf{1}}[x_1 > \frac{m}{2}],\ldots,\underline{\mathbf{1}}[x_n > \frac{m}{2}])$$
 numbers in [m] bits in {0,1}

Easy: If f is monotone then so is F.

#### Remains to argue:

If f is  $\varepsilon$ -far from monotone then so is F.



Exists  $\varepsilon 2^n$  vertex-disjoint pairs in  $\{0,1\}^n$  that are violations w.r.t. f

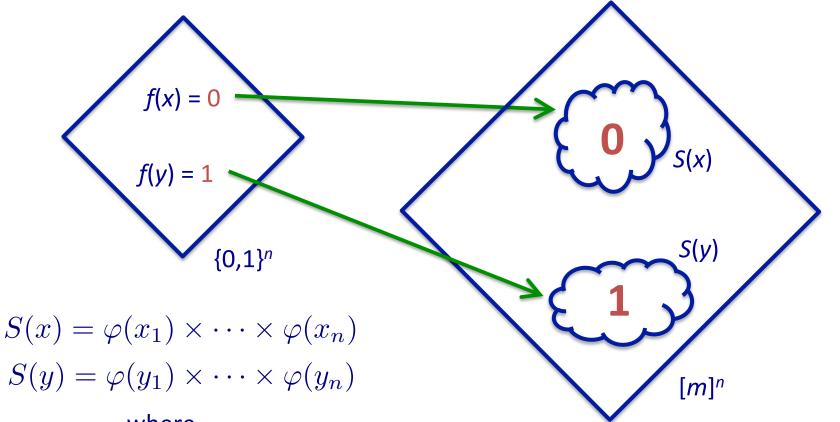
Each violating pair



 $(m/2)^n$  vertex-disjoint violating pairs

 $[m]^n$  that are violations w.r.t. F

Each violating pair in  $\{0,1\}^n \implies \left(\frac{m}{2}\right)^n$  violating pairs in  $[m]^n$ 



$$\varphi(0) = \{0, 1, \dots, \frac{m}{2}\}$$

$$\varphi(1) = \{\frac{m}{2} + 1, \dots, m\}$$

$$|S(x)| = |S(y)| = (m/2)^n$$

Easy end game: exhibit order-preserving bijection between S(x) and S(y)

#### Conclusion

A polynomial lower bound for testing monotonicity of Boolean functions

#### **Theorem**

Any non-adaptive tester must make  $\widetilde{\Omega}(n^{1/5})$  queries. Therefore, any adaptive tester must make  $\Omega(\log n)$  queries.

- Main technical ingredient: multidimensional central limit theorems
- Proof extends to testing monotonicity over general hypergrid domains

**Open Problem:** Polynomial lower bounds against *adaptive* testers?

Thank you!