Anti-concentration and the Gap-Hamming problem

Anup Rao
University of Washington

Amir Yehudayoff
Technion

Outline

Anti-concentration

1. The Littlewood-Offord problem
2. Erdos’s answer
3. Halasz’s approach

Communication complexity

1. Rectangle partitions
2. Connection to streaming algorithms
3. Gap-Hamming

Our work

Halasz generalized to rectangles

Littlewood-Offord Problem

Suppose

$x \in \mathbb{R}^n$ has no zero coordinates.

$Y \in \{\pm 1\}^n$ is uniformly random.

$\langle x, Y \rangle = \sum_{i=1}^{n} x_i Y_i$.

Q: What is $\max_k \Pr[\langle x, Y \rangle = k]$?

Littlewood-Offord Problem

Suppose
$x \in \mathbb{R}^n$ has no zero coordinates.
$Y \in \{\pm 1\}^n$ is uniformly random.
$\langle x, Y \rangle = \sum_{i=1}^{n} x_i Y_i$.
Q: What is $\max_k \Pr[\langle x, Y \rangle = k]$?

Example:
$x = (1, 3, 3^2, \ldots, 3^{n-1})$

Then $\langle x, Y \rangle$ determines Y, so $\max_k \Pr[\langle x, Y \rangle = k] = 2^{-n}$.

Littlewood-Offord Problem

Suppose
$x \in \mathbb{R}^n$ has no zero coordinates.
$Y \in \{\pm 1\}^n$ is uniformly random.
$\langle x, Y \rangle = \sum_{i=1}^{n} x_i Y_i$.
Q: What is $\max_k \Pr[\langle x, Y \rangle = k]$?

Example:

$x = (1,1,\ldots,1)$
Let W denote number of coords of Y that are -1.
$\langle x, Y \rangle = k$ means $(n - W) - W = k$, so $W = (n-k)/2$.

$$\Pr[\langle x, Y \rangle = k] = \binom{n}{(n-k)/2} \cdot 2^{-n}.$$

$$\max_k \Pr[\langle x, Y \rangle = k] = \binom{n}{\lfloor n/2 \rfloor} \cdot 2^{-n} = O(1/\sqrt{n}).$$

Littlewood-Offord Problem

Suppose
$x \in \mathbb{R}^n$ has no zero coordinates.
$Y \in \{\pm 1\}^n$ is uniformly random.
Q: What is $\max_k \Pr[\langle x, Y \rangle = k]$?

Erdos:

wlog $x_i > 0$.

Claim: For each k, $S = \{y : \langle x, y \rangle = k\} \subseteq \{\pm 1\}^n$ is an *antichain*.

Antichain: $y, y' \in S$ means cannot have $y_i > y_i'$ for all i.

Sperner's theorem: The largest antichain in $\{\pm 1\}^n$ has size $\binom{n}{\lfloor n/2 \rfloor}$.

Thm: $\max_k \Pr[\langle x, Y \rangle = k] \leq \binom{n}{\lfloor n/2 \rfloor} \cdot 2^{-n} \approx 1/\sqrt{n}$.

Littlewood-Offord Problem

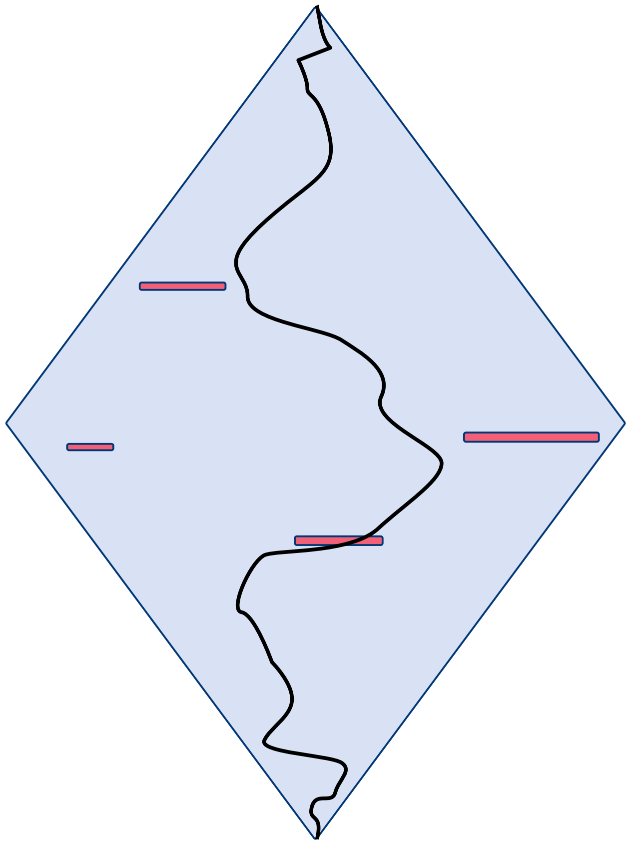
Suppose
$x \in \mathbb{R}^n$ has no zero coordinates.
$Y \in \{\pm 1\}^n$ is uniformly random.
Q: What is $\max_k \Pr[\langle x, Y \rangle = k]$?

Sperner's theorem: The largest antichain in $\{\pm 1\}^n$ has size $\binom{n}{\lfloor n/2 \rfloor}$.

Pf: Let $A \subseteq \{\pm 1\}^n$ be an antichain. Let a_i be number of elements of A with i 1's.

Let

$(-1,\ldots,-1) = Y^{(0)}, Y^{(1)}, \ldots, Y^{(n)} = (1,\ldots,1)$ be a random chain,
Where $Y^{(i)}$ is obtained from $Y^{(i-1)}$ by flipping random -1 to 1.



$$1 \geq \text{probability that the chain passes through } A$$
$$\geq \frac{a_0}{\binom{n}{0}} + \frac{a_1}{\binom{n}{1}} + \ldots + \frac{a_n}{\binom{n}{n}} \geq \frac{|A|}{\binom{n}{\lfloor n/2 \rfloor}}.$$

Littlewood-Offord Problem

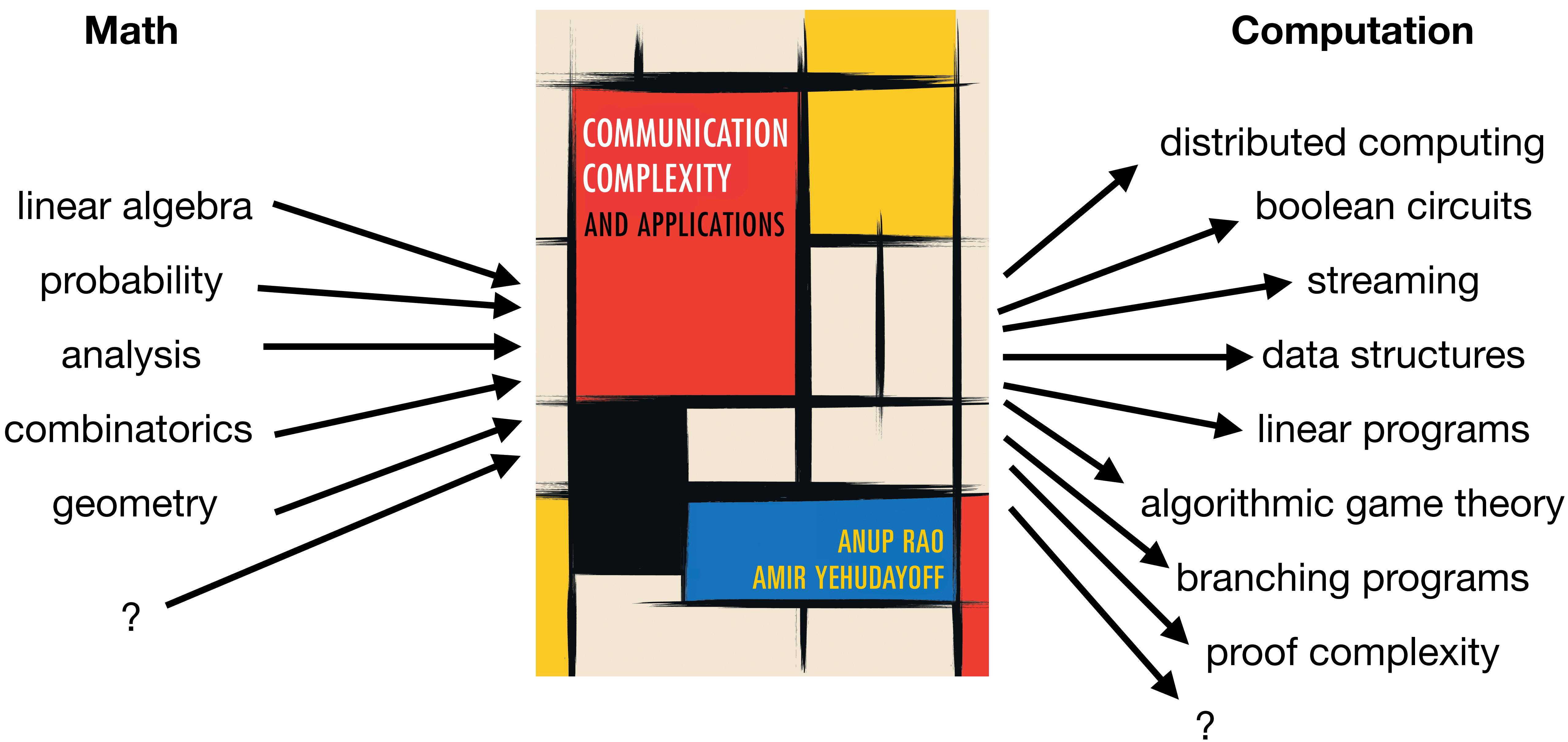
$x \in \mathbb{R}^n$ has no zero coordinates.
$Y \in \{\pm 1\}^n$ is uniformly random.

Erdös: $\max_k \Pr[\langle x, Y \rangle = k] \leq \binom{n}{\lfloor n/2 \rfloor} \cdot 2^{-n} \leq O(1/\sqrt{n})$.

Erdös-Moser, Sárkozy-Szemerédi: If coordinates x_i distinct,
$\Pr[\langle x, Y \rangle = k] \leq O(n^{-3/2})$.

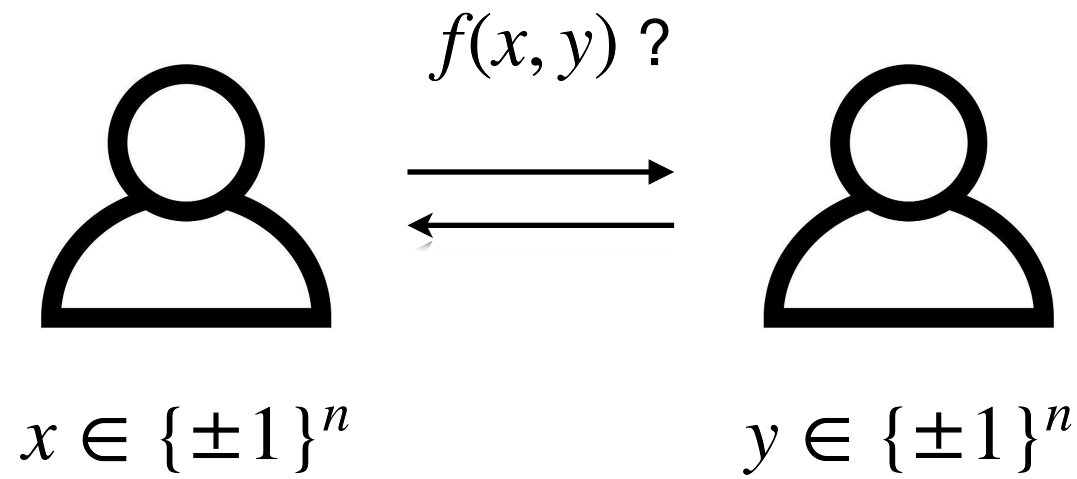
Halász: Suppose $x \in \mathbb{Z}^n$, let $0 \leq \theta \leq 1$ be uniform.

$$\begin{aligned}
\Pr[\langle x, Y \rangle = k] &= \mathbb{E}_{\theta,Y}[\exp(2\pi i \cdot \theta \cdot (\langle x, Y \rangle - k))] \\
&\leq \mathbb{E}_\theta | \mathbb{E}_Y[\exp(2\pi i \cdot \theta \cdot \langle x, Y \rangle)] | \\
&= \mathbb{E}_\theta \left| \mathbb{E}_Y \left[\prod_{j=1}^{n} \exp(2\pi i \cdot \theta \cdot x_j Y_j) \right] \right| \\
&= \mathbb{E}_\theta \left| \prod_{j=1}^{n} \cos(2\pi \theta x_j) \right| \leq O(1/\sqrt{n}).
\end{aligned}$$


Math
Computation
COMMUNICATION COMPLEXITY
AND APPLICATIONS
ANUP RAO
AMIR YEHUDAYOFF
linear algebra
probability
analysis
combinatorics
geometry
?
distributed computing
boolean circuits
streaming
data structures
linear programs
algorithmic game theory
branching programs
proof complexity
?

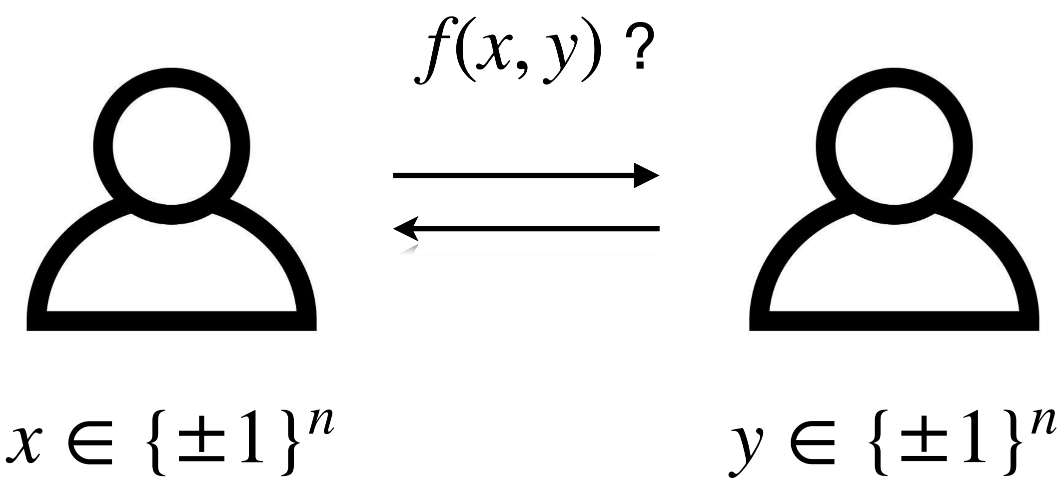

Math
linear algebra
probability
analysis
combinatorics
geometry
Fourier analysis
COMMUNICATION COMPLEXITY
AND APPLICATIONS
ANUP RAO
AMIR YEHUDAYOFF
Computation
distributed computing
boolean circuits
streaming
data structures
linear programs
algorithmic game theory
branching programs
proof complexity
?

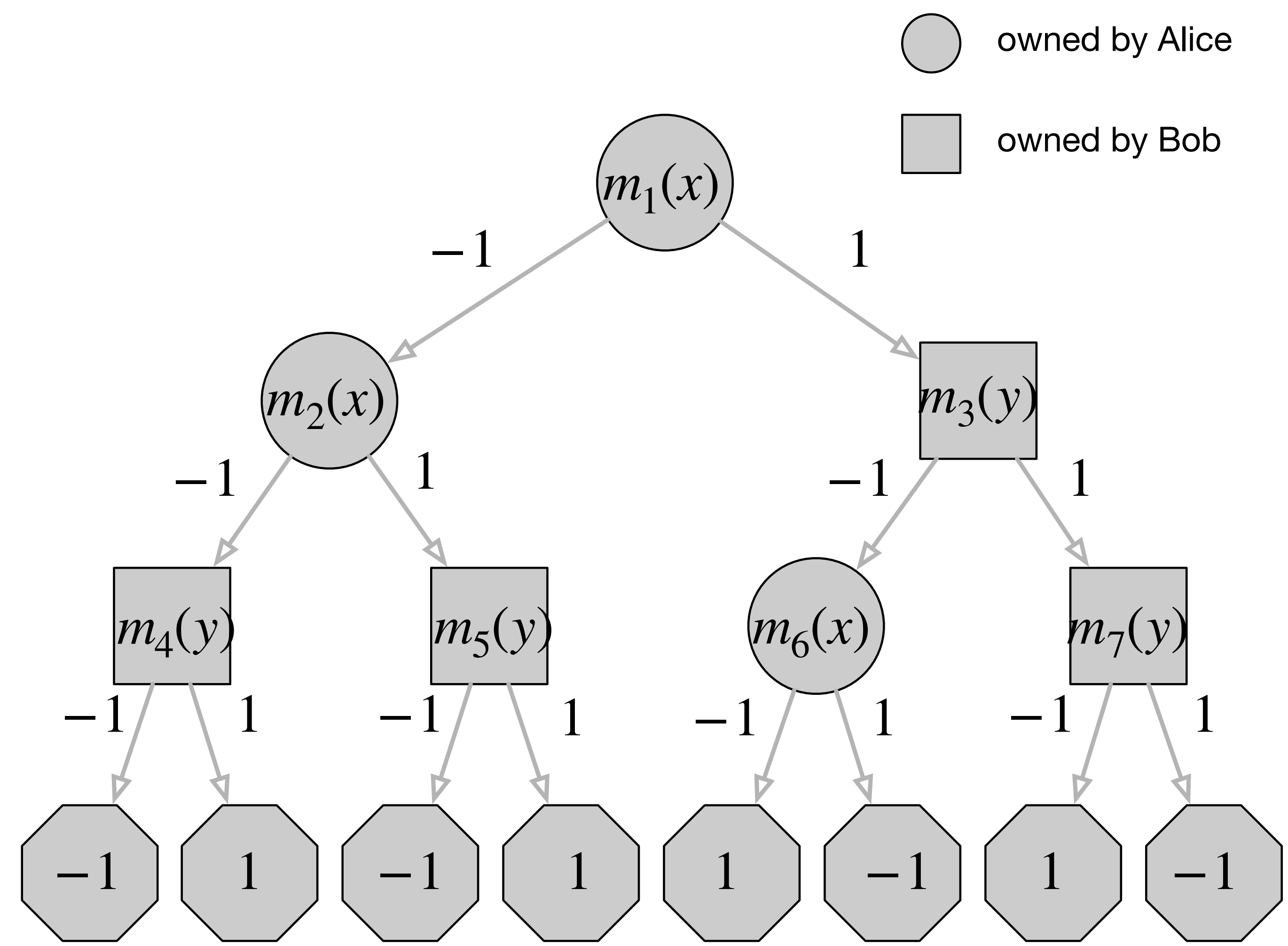
Communication complexity



How long does their conversation need to be?

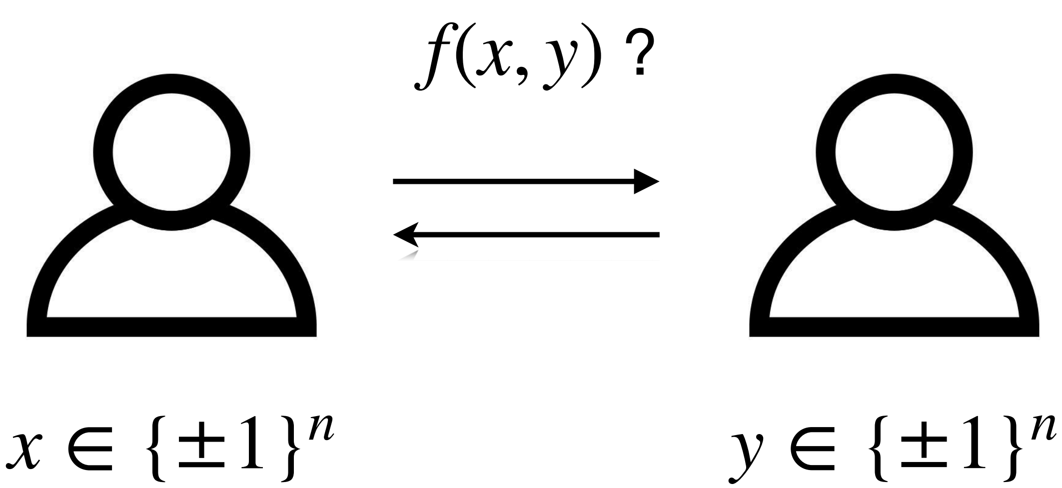
Communication complexity

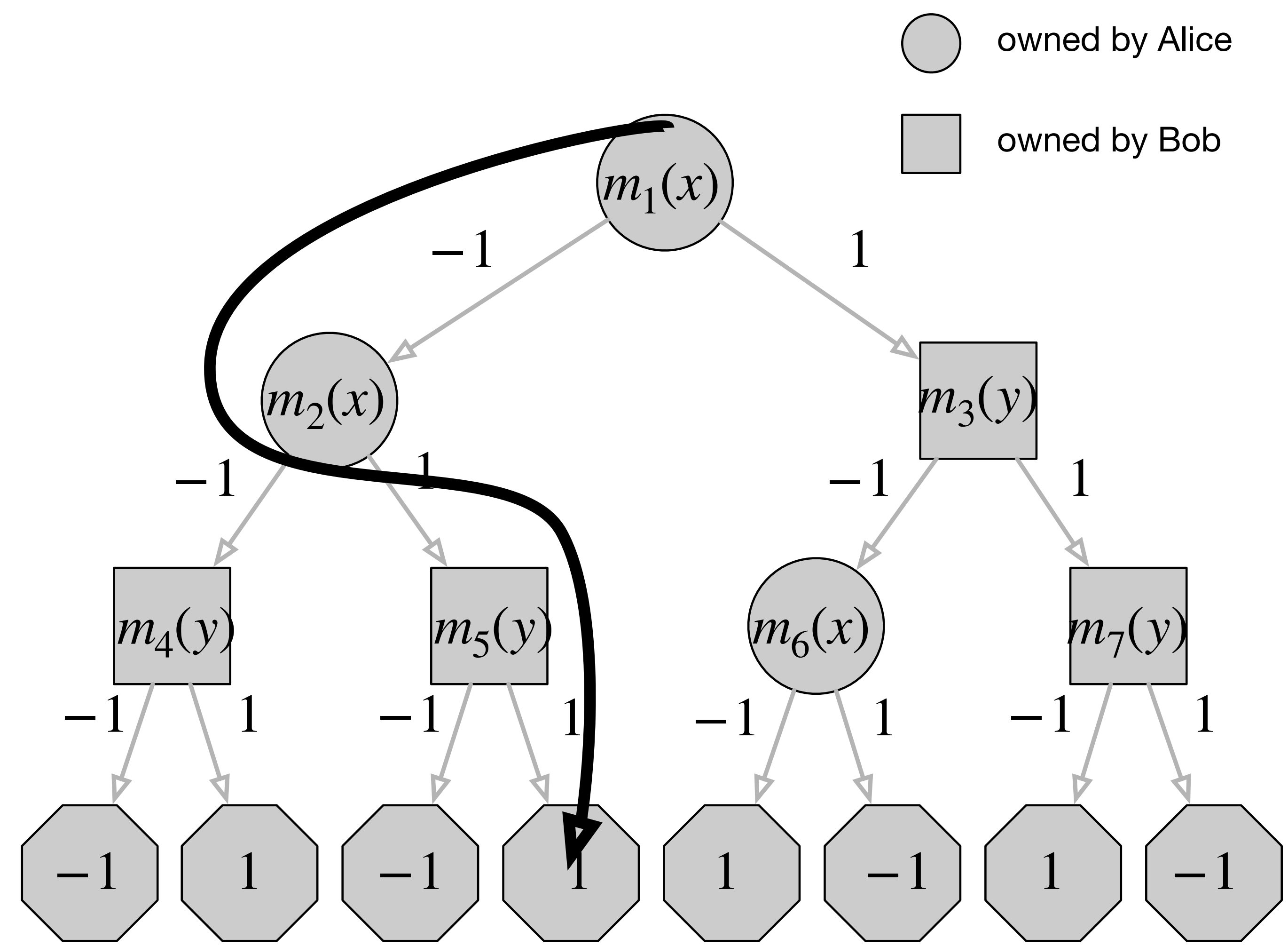




How long does their conversation need to be?

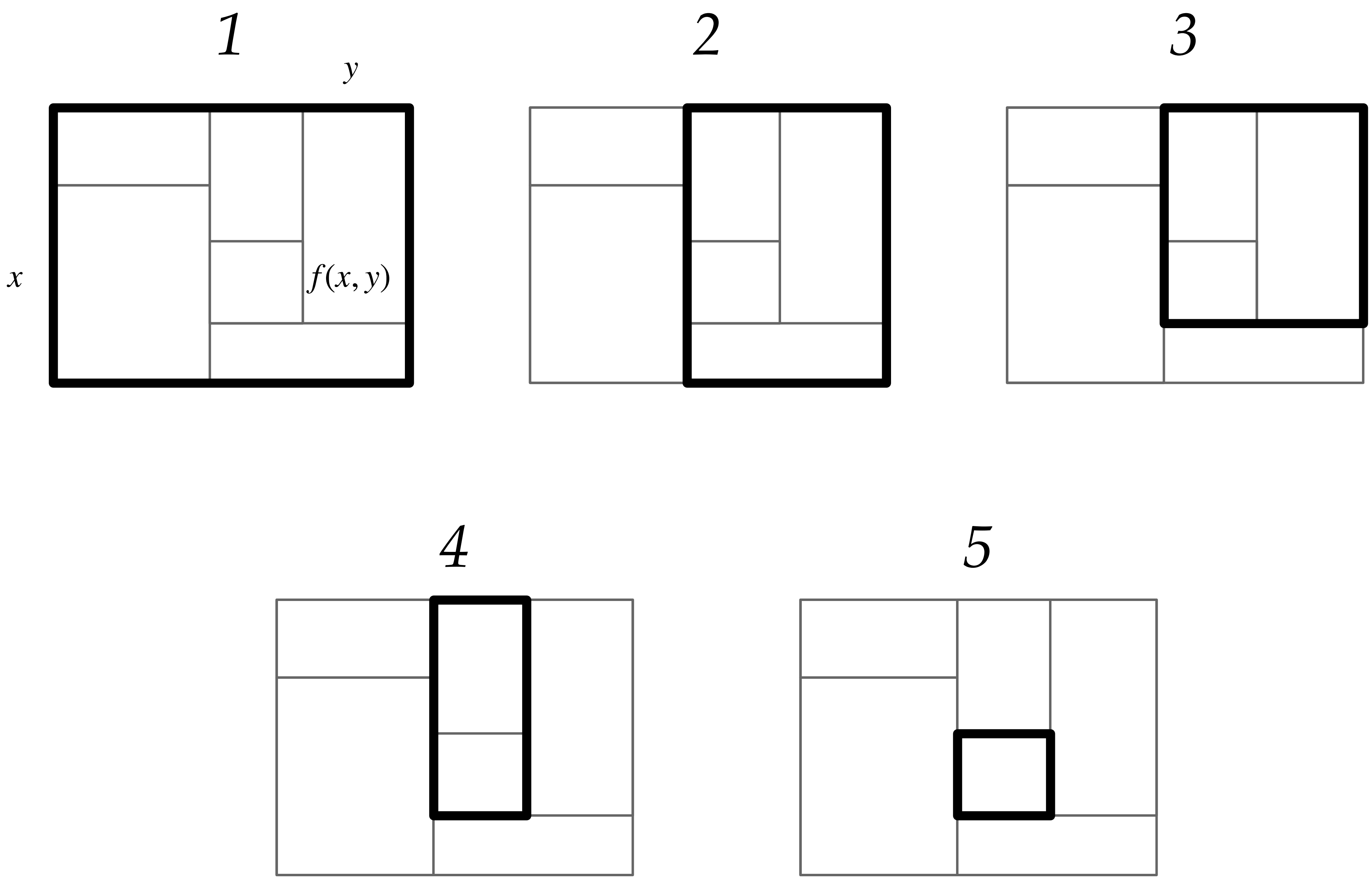
Communication complexity





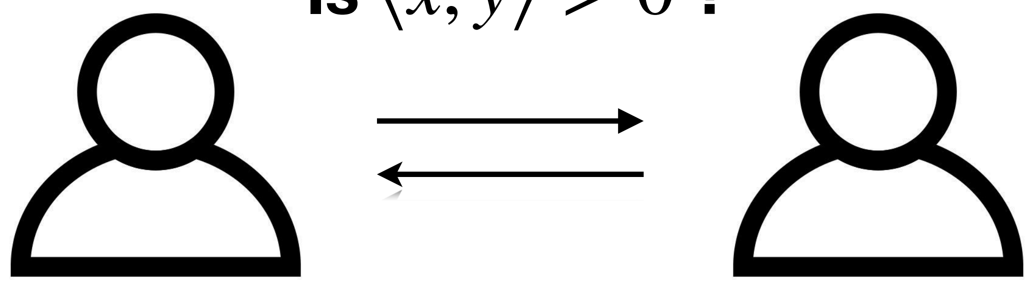
How long does their conversation need to be?

Small communication = partition into few rectangles



The Gap-Hamming Problem

Is $\langle x, y \rangle > 0$ **?**



$x \in \{\pm 1\}^n$ $y \in \{\pm 1\}^n$

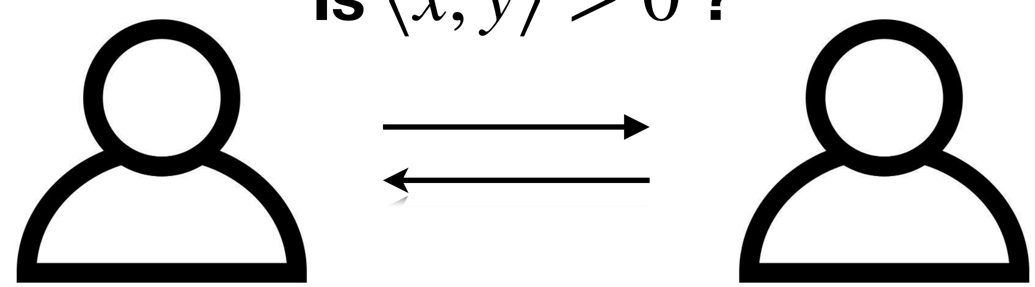
promise

$|\langle x, y \rangle| \geq \sqrt{n}$

How long does their conversation need to be?

Exact Gap-Hamming Problem

Is $\langle x, y \rangle > 0$ **?**



$x \in \{\pm 1\}^n$ $\quad$ $y \in \{\pm 1\}^n$

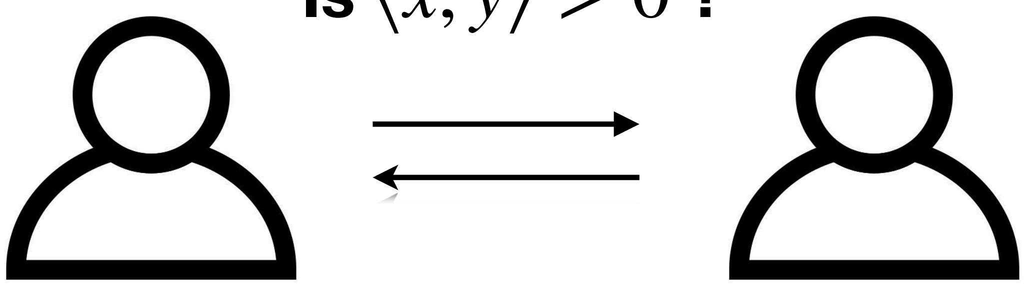
promise

$$|\langle x, y \rangle| = \sqrt{n}$$

How long does their conversation need to be?

Gap-Hamming Problem

Is $\langle x, y \rangle > 0$ **?**



$x \in \{\pm 1\}^n$ $y \in \{\pm 1\}^n$

promise

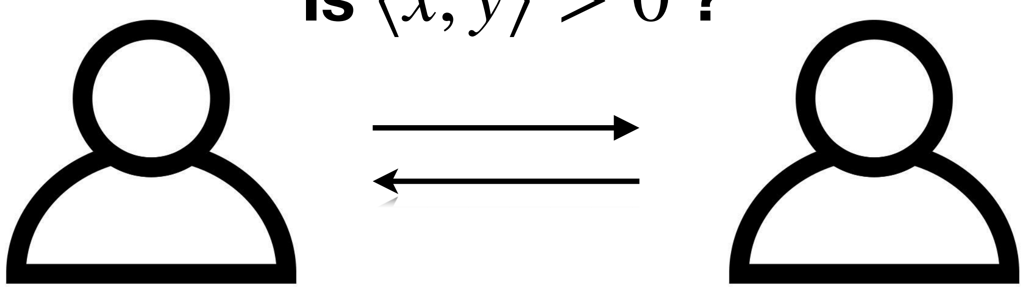
$|\langle x, y \rangle| \geq \sqrt{n}$

History:

1. Posed by [**Indyk-Woodruff**], motivated by streaming.
2. $\Omega(n)$ communication required [**Chakrabarti-Regev**]: cube -> Gaussians
3. [**Sherstov**]: SVD, Talagrand's inequality
4. [**Vidick**]: cube -> Gaussians
5. [**Our work**]: Fourier analysis

Exact Gap-Hamming Problem

Is $\langle x, y \rangle > 0$ **?**



$x \in \{\pm 1\}^n$ $y \in \{\pm 1\}^n$

promise

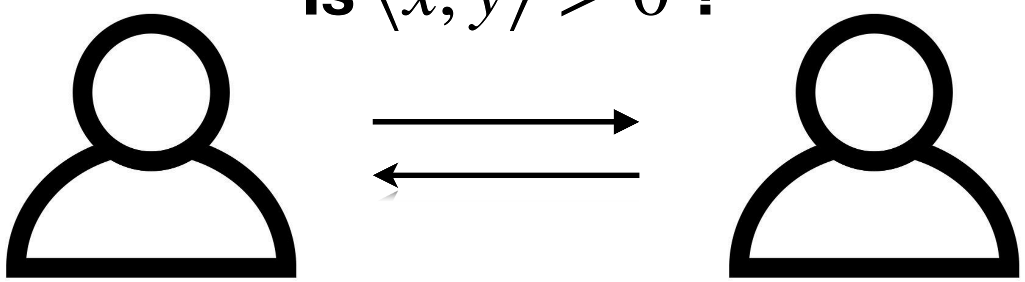
$|\langle x, y \rangle| = \sqrt{n}$

Observation:	*flipping* x_1 *changes*
n **and** $\prod_{j=1}^{n} x_j y_j$	sign
determine	
$\langle x, y \rangle \mod 4$	$+2 \mod 4$

[**Chakrabarti-Regev**]: What is the communication required in general?

Exact Gap-Hamming Problem

Is $\langle x, y \rangle > 0$ **?**



$x \in \{\pm 1\}^n$ $y \in \{\pm 1\}^n$

promise

$|\langle x, y \rangle| = \sqrt{n}$

New in our work:

$\Omega(n)$ communication is required
in general
(Fourier analysis)

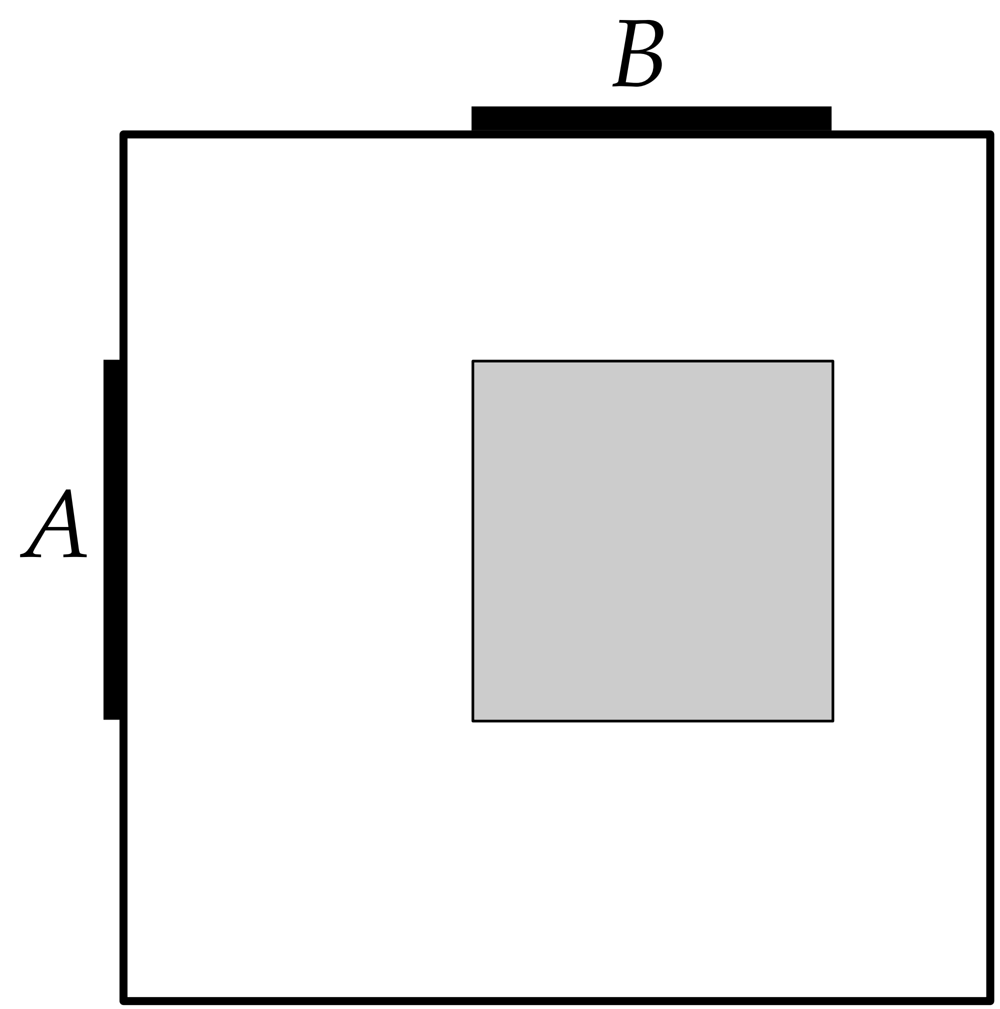
Large Rectangles

$X \in_R A \subseteq \{\pm 1\}^n$
$Y \in_R B \subseteq \{\pm 1\}^n$

What can we say about the distribution of $\langle X, Y \rangle$ if $|A| \cdot |B|$ is large?

[Chakrabarti-Regev], [Sherstov], [Vidick]:
If $|A| \cdot |B| > 2^{1.99n}$,
$\Pr[\,|\langle X, Y \rangle| \leq \sqrt{n}/100] \leq 0.99.$

Anti-concentration

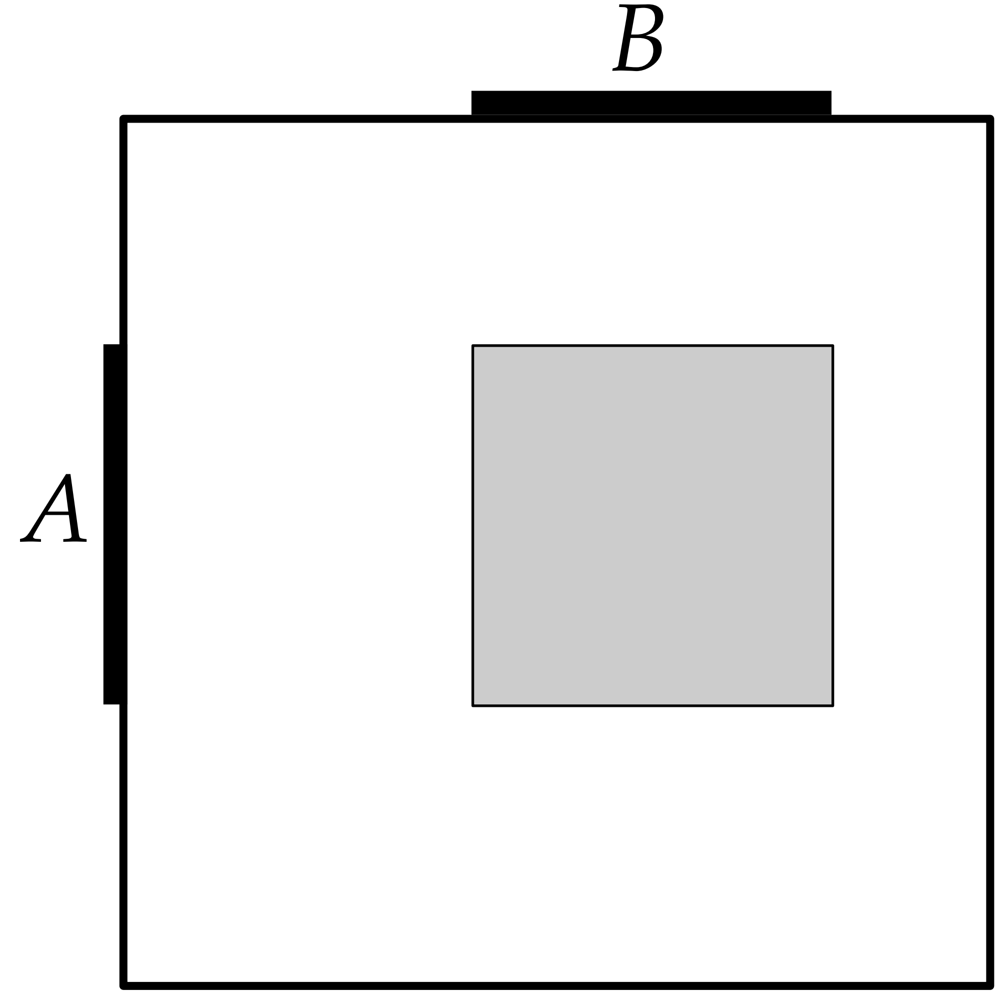


(In our work: optimal anti-concentration)

$X \in_R A \subseteq \{\pm 1\}^n$

$Y \in_R B \subseteq \{\pm 1\}^n$

What can we say about the distribution of $\langle X, Y \rangle$ if $|A| \cdot |B|$ is large?



Example 1:

$A = B = \{\pm 1\}^n$, n even, then $\Pr[\langle X, Y \rangle = 0] = \Theta(1/\sqrt{n})$.

Example 2:

sum to 0

A 11111111111111****************

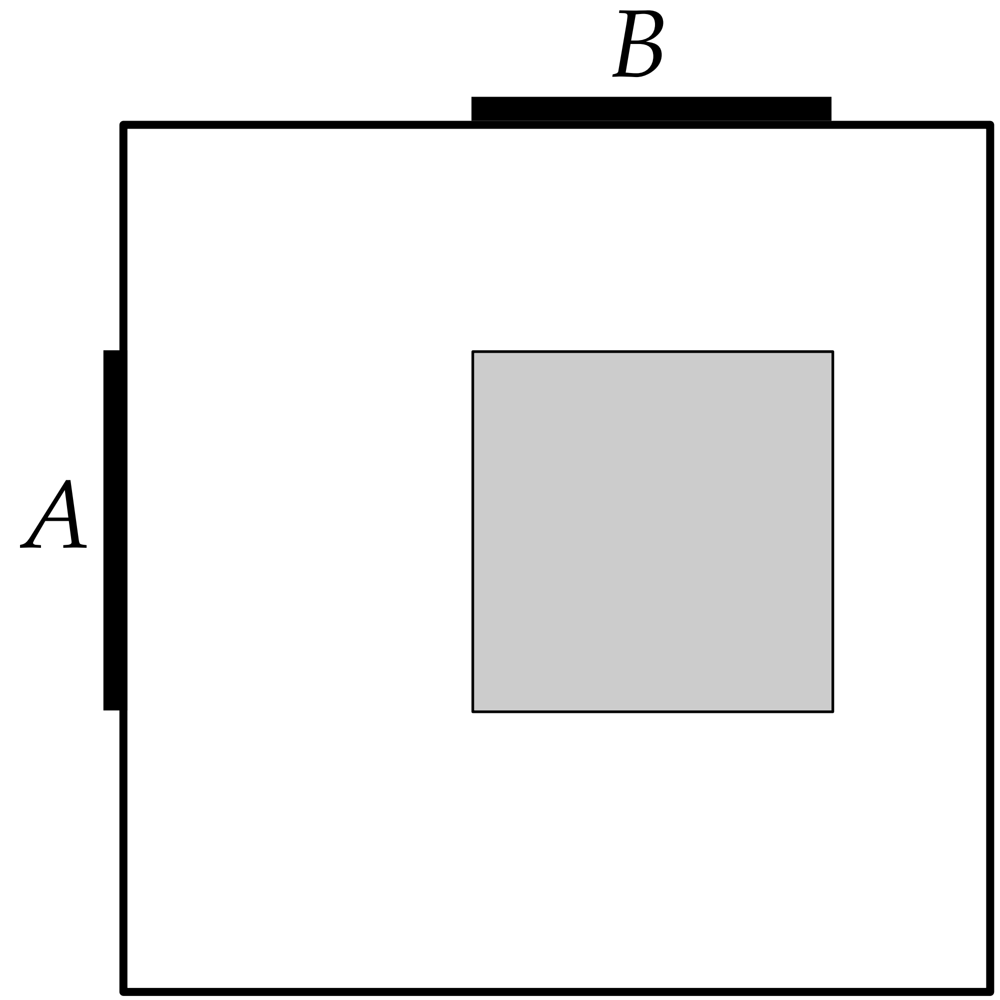
B ****************11111111111111

sum to 0

$|A| \cdot |B| \geq \Omega(2^n/n)$ $\langle X, Y \rangle = 0$

$$X \in_R A \subseteq \{\pm 1\}^n$$
$$Y \in_R B \subseteq \{\pm 1\}^n$$

What can we say about the distribution of $\langle X, Y \rangle$ if $|A| \cdot |B|$ is large?



Our Results

Thm 1: If $|A| \cdot |B| \geq 2^{1.01n}$, for all k, $\Pr[\langle X, Y \rangle = k] \leq O(1/\sqrt{n})$.

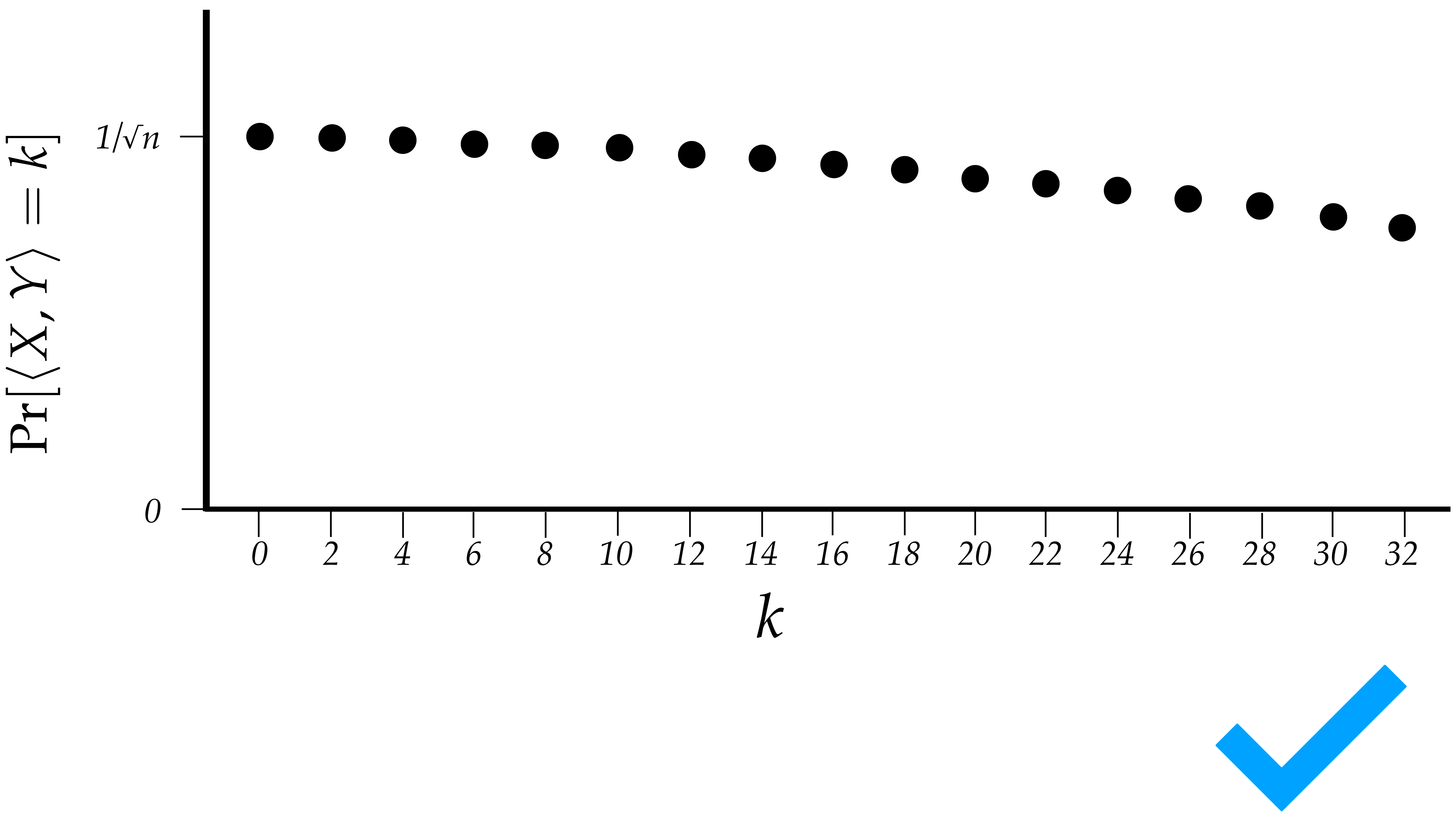
Remark: This implies all past results.

Thm 2: … except with exp small probability over $x \in A$, $\Pr[\langle x, Y \rangle = k] \leq O(1/\sqrt{n})$.

Thm 3: … $|\Pr[\langle x, Y \rangle = k] - \Pr[\langle x, Y \rangle = k + 4]| \leq O(1/n)$.

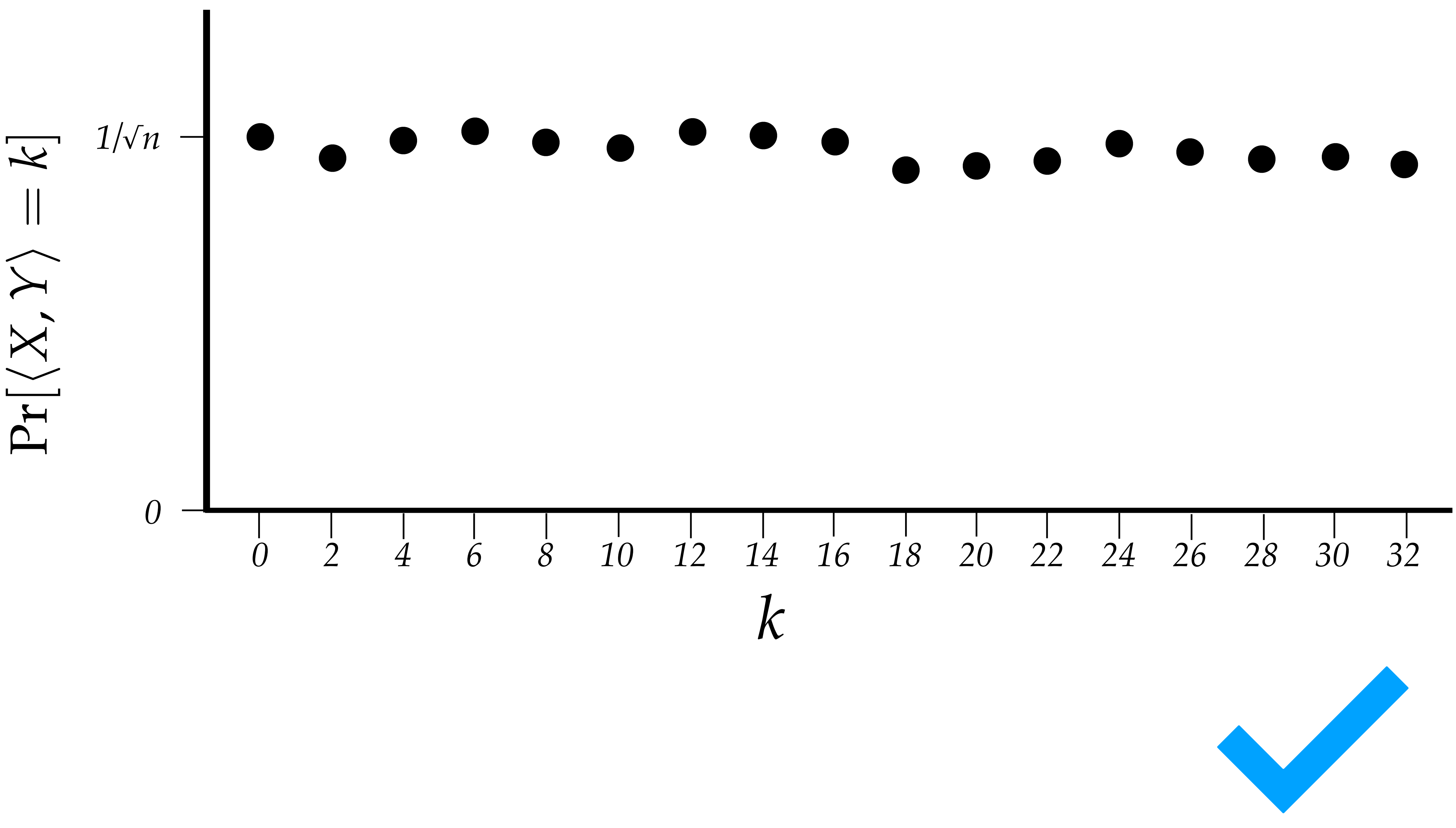
Remark: This is false if 4 is replaced with 6 or 2, as we saw.

Thm: For all k, if $|A| \cdot |B| > 2^{1.01n}$,
$$|\Pr[\langle X, Y \rangle = k] - \Pr[\langle X, Y \rangle = k+4]| \leq O(1/n) .$$



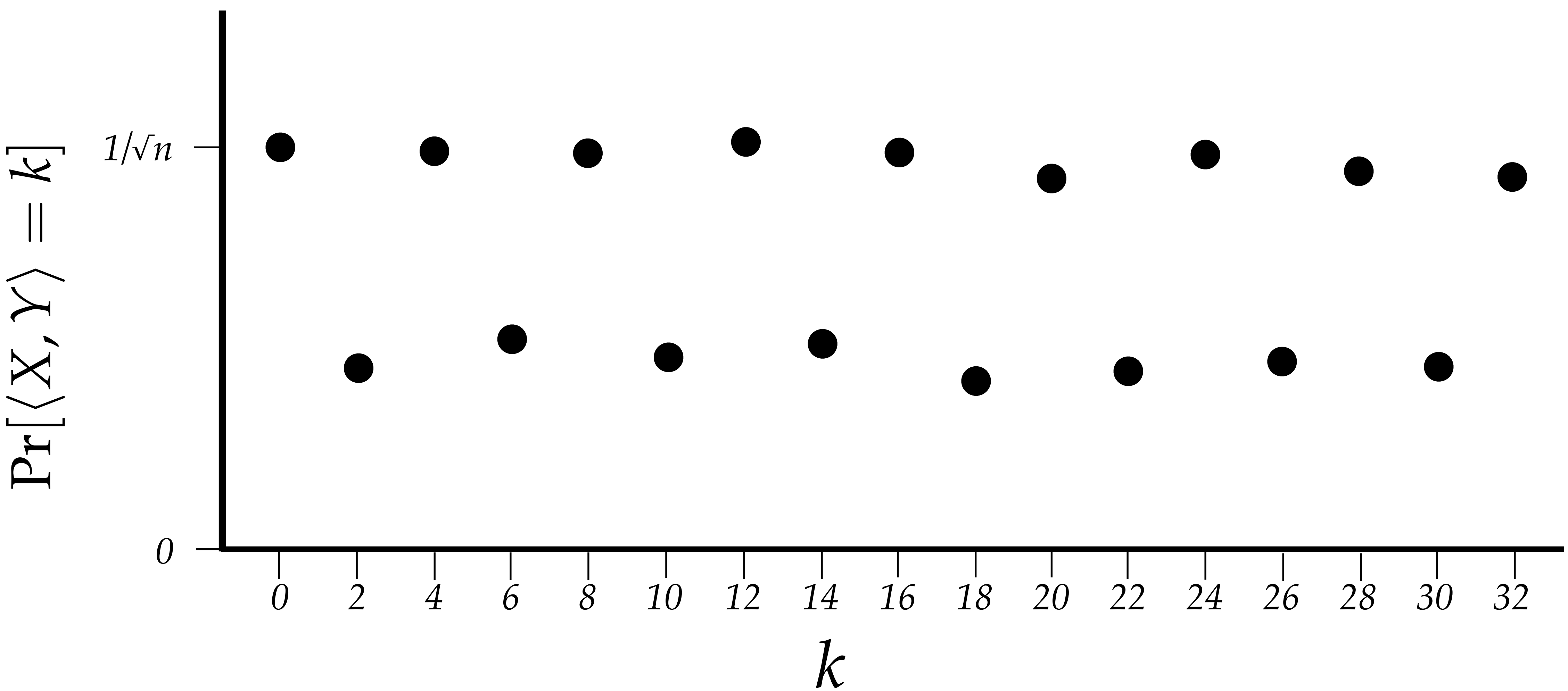
Thm: For all k, if $|A| \cdot |B| > 2^{1.01n}$,

$$|\Pr[\langle X, Y \rangle = k] - \Pr[\langle X, Y \rangle = k+4]| \leq O(1/n)\,.$$

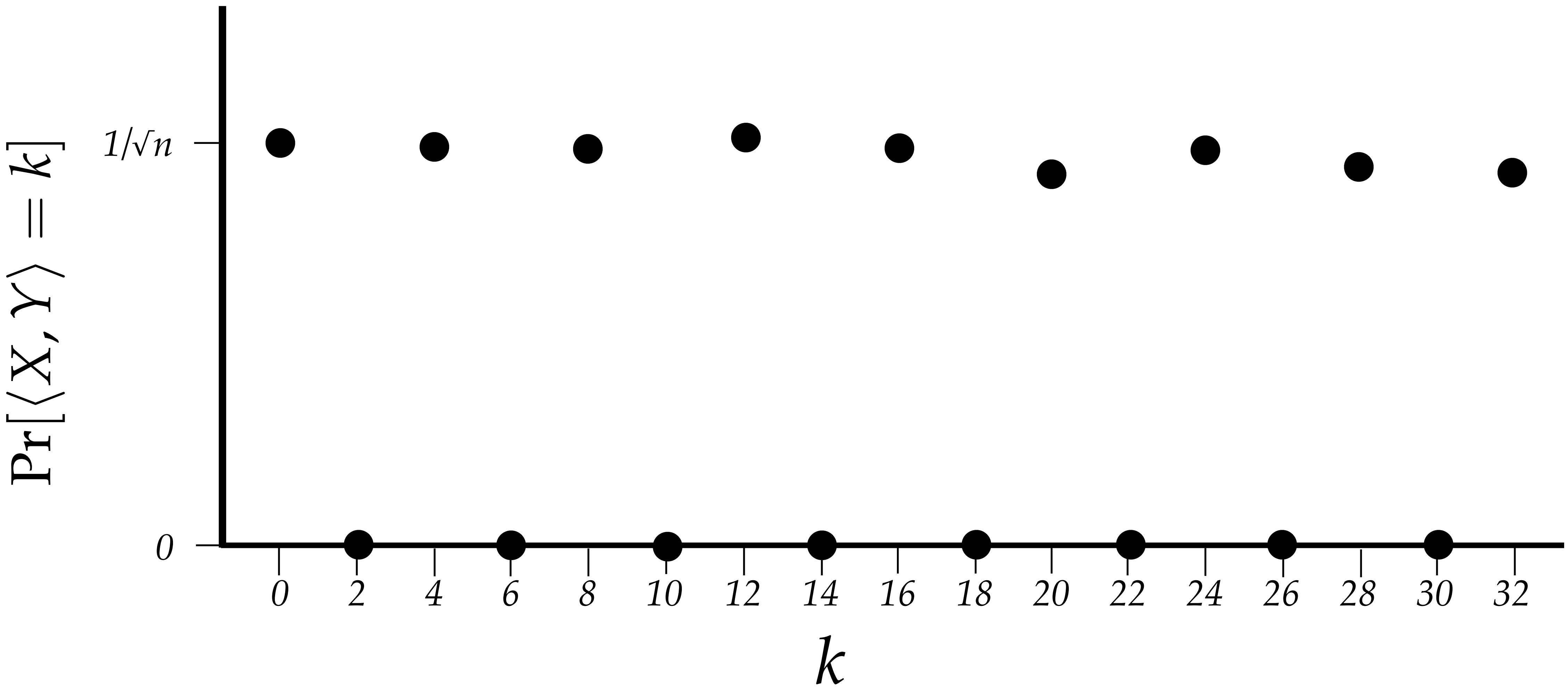


Thm: For all k, if $|A| \cdot |B| > 2^{1.01n}$,

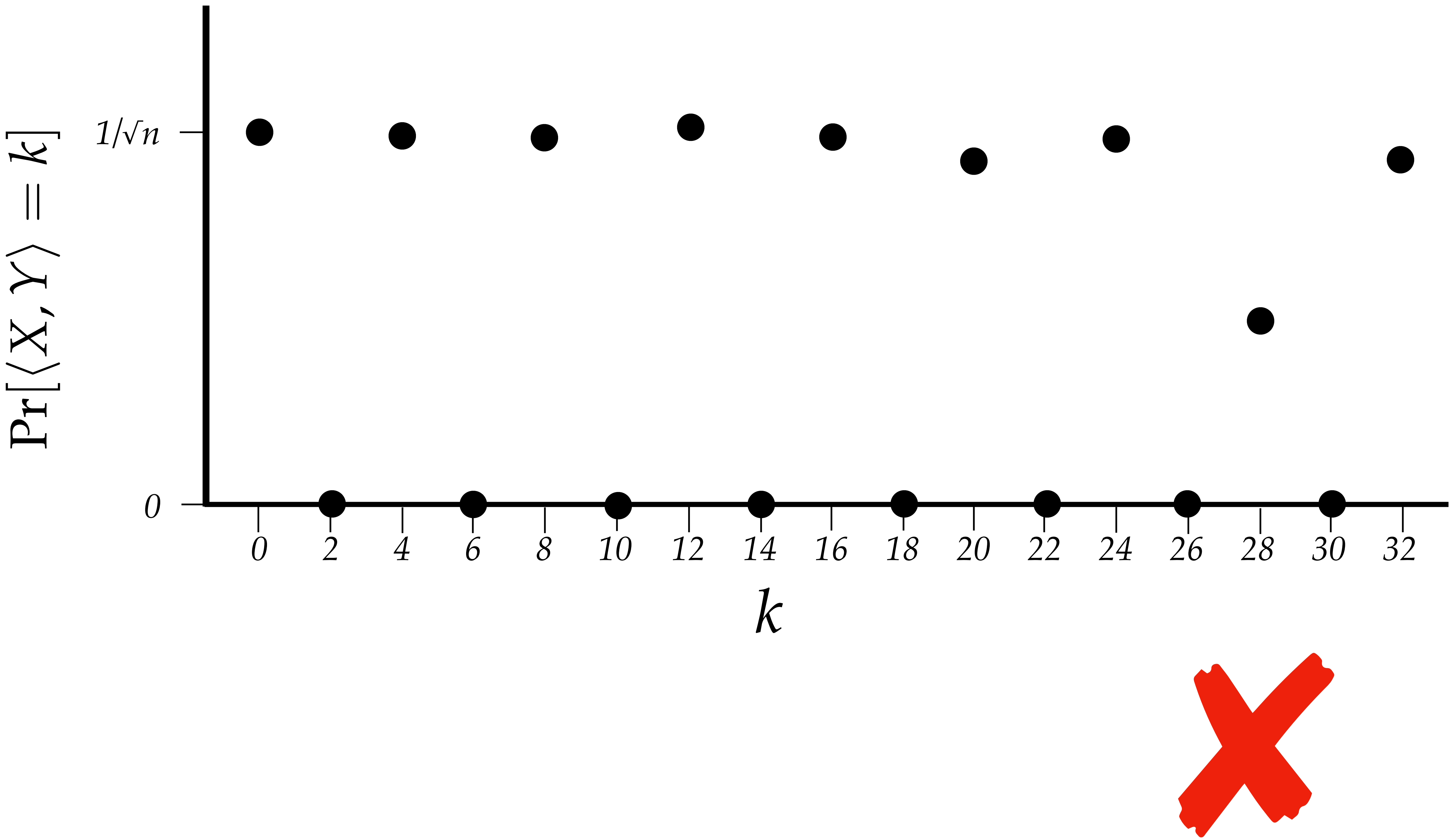
$$|\Pr[\langle X, Y \rangle = k] - \Pr[\langle X, Y \rangle = k + 4]| \leq O(1/n)\,.$$



Thm: For all k, if $|A| \cdot |B| > 2^{1.01n}$,
$$|\Pr[\langle X, Y \rangle = k] - \Pr[\langle X, Y \rangle = k + 4]| \leq O(1/n)\,.$$



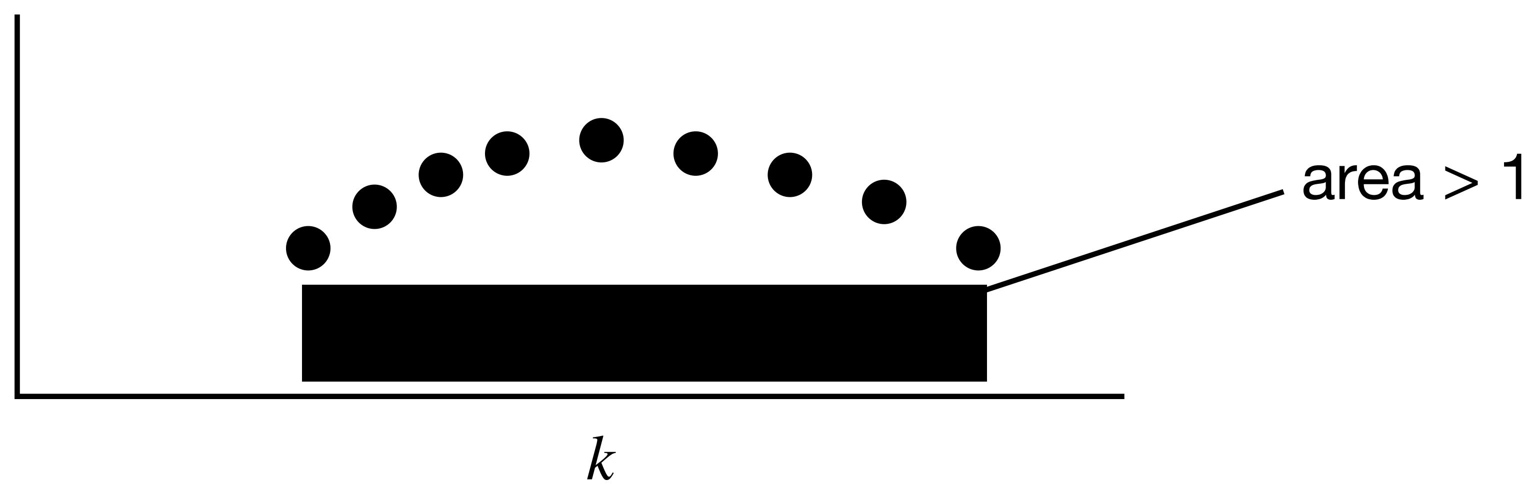
Thm: For all k, if $|A| \cdot |B| > 2^{1.01n}$,
$|\Pr[\langle X, Y \rangle = k] - \Pr[\langle X, Y \rangle = k + 4]| \leq O(1/n)$.



Thm: For all k, if $|A| \cdot |B| > 2^{1.01n}$,
$$|\Pr[\langle X, Y\rangle = k] - \Pr[\langle X, Y\rangle = k+4]| \leq O(1/n)\,.$$

Corollary 1: For all k, $\Pr[\langle X, Y\rangle = k] \leq O(1/\sqrt{n})\,.$

Pf Sketch:



Corollary 2: Exact-gap-Hamming requires $\Omega(n)$ communication.

Pf Sketch:

If not, sample a rectangle R by feeding inputs with $|\langle X', Y'\rangle| = \sqrt{n}$. Then whp,

- $|A| \cdot |B| \geq 2^{1.01n}$
- $\Pr[\,|\langle X, Y\rangle| = \sqrt{n}\,|\,R] \geq \Omega(1/\sqrt{n})$

So, the protocol must make an error with significant probability.

[Halász]: Fourier analytic approach

Suppose $Y \in \{\pm 1\}^n$ is uniform, $x \in \mathbb{Z}^n_{\neq 0}$

$$\Pr[\langle x, Y\rangle = k] = \mathbb{E}_{\theta,Y}[\exp(2\pi i \cdot \theta \cdot (\langle x, Y\rangle - k))]$$

$$\leq \mathbb{E}_{\theta} | \mathbb{E}_{Y}[\exp(2\pi i \cdot \theta \cdot \langle x, Y\rangle)] |$$

$$= \mathbb{E}_{\theta} \left| \mathbb{E}_{Y}\left[\prod_{j=1}^{n} \exp(2\pi i \cdot \theta \cdot x_j Y_j)\right] \right|$$

$$= \mathbb{E}_{\theta} \left| \prod_{j=1}^{n} \cos(2\pi\theta x_j) \right| \leq O(1/\sqrt{n}) .$$

Challenge:
In our setting the coordinates of Y are correlated!

Technical Thm: For all θ, if $|A| \cdot |B| = 2^{1.01n}$, then except with exp small probability over $x \in A$,
$$|\mathbb{E}_Y[\exp(2\pi i \cdot \theta \cdot \langle x, Y \rangle)]| < \exp(-\Omega(n \sin^2(4\pi\theta))) .$$

Thm: For all k, if $X \in A, Y \in B, |A| \cdot |B| > 2^{1.01n}$,
$$|\Pr[\langle X, Y \rangle = k] - \Pr[\langle X, Y \rangle = k+4]| \le O(1/n) .$$

Pf:

Using: $\Pr[\langle x, Y \rangle = k] = \mathbb{E}_{\theta,Y}[\exp(2\pi i \cdot \theta \cdot (\langle x, Y \rangle - k))]$,

$$|\Pr[\langle X, Y \rangle = k] - \Pr[\langle X, Y \rangle = k + 4]|$$

$$\lessapprox \mathbb{E}_\theta[|\exp(-2\pi i\theta \cdot (k+2))| \cdot |(\exp(4\pi i\theta) - \exp(-4\pi i\theta)) \cdot \exp(-\Omega(n \sin^2(4\pi\theta)))|]$$

$$\le 2 \cdot \mathbb{E}_\theta[|\sin(4\pi\theta) \cdot \exp(-\Omega(n \sin^2(4\pi\theta)))|]$$

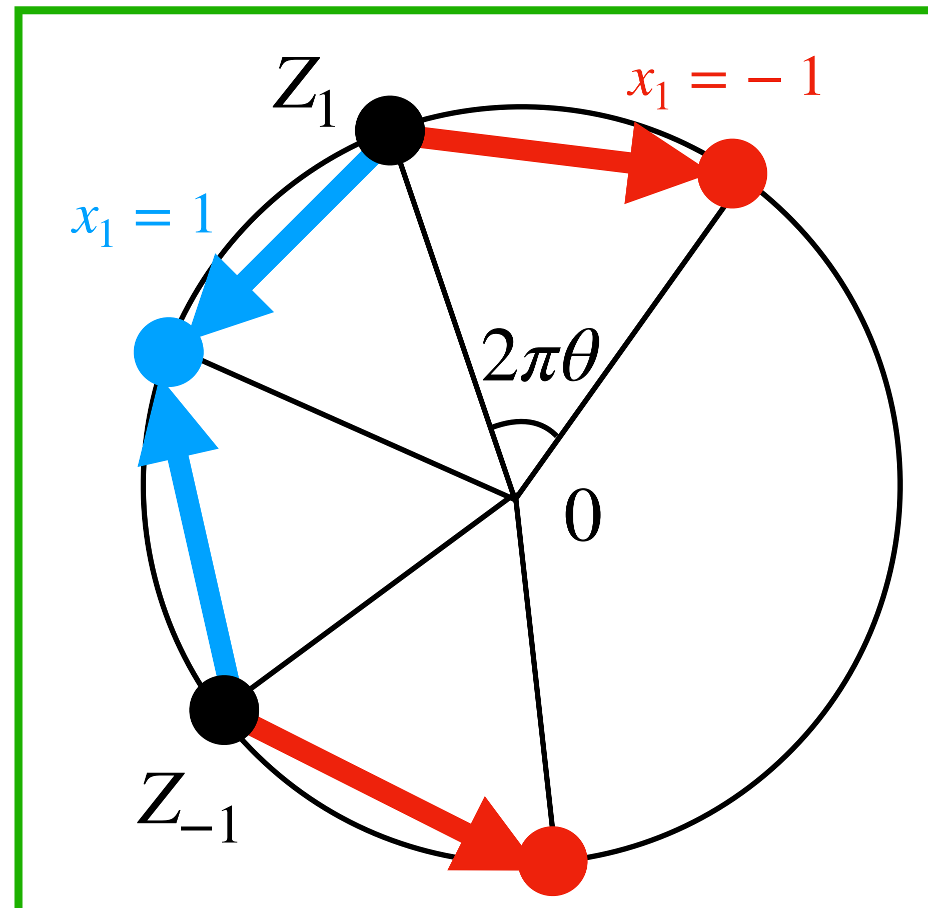
$$\le O(1/n) .$$

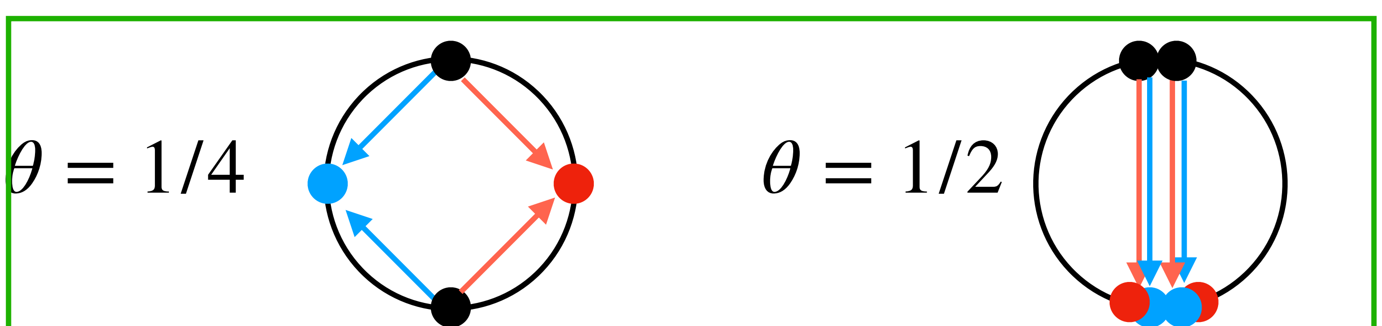
Technical Thm: For all θ, if $|A| \cdot |B| = 2^{1.01n}$, then except with exp small probability over $x \in A$,
$|\mathbb{E}_Y[\exp(2\pi i \cdot \theta \cdot \langle x, Y\rangle)]| < \exp(-\Omega(n \sin^2(4\pi\theta)))$.

$$|\mathbb{E}_Y[\exp(2\pi i \cdot \theta \cdot \langle x, Y\rangle)]|^2$$
$$= |\mathbb{E}_{Y_1}[\exp(2\pi i\theta x_1 Y_1) \cdot \mathbb{E}_{Y_{>1}}[\exp(2\pi i \cdot \theta \cdot \langle x_{>1}, Y_{>1}\rangle)]]|^2$$
$$= |\mathbb{E}_{Y_1}[\exp(2\pi i\theta x_1 Y_1) \cdot Z_{Y_1}]|^2.$$

If Y_1 has entropy, for at least **half** the choices of x_1,
$\leq \exp(-\sin^2(4\pi\theta)) \cdot \mathbb{E}_{Y_1}[|Z_{Y_1}|^2]$

If Y_1 has no entropy,
$\leq \mathbb{E}_{Y_1}[|Z_{Y_1}|^2]$





Technical Thm: For all θ, if $|A| \cdot |B| = 2^{1.01n}$, then except with exp small probability over $x \in A$,
$$|\mathbb{E}_Y[\exp(2\pi i \cdot \theta \cdot \langle x, Y \rangle)]| < \exp(-\Omega(n \sin^2(4\pi\theta)))\,.$$

$$|\mathbb{E}_Y[\exp(2\pi i \cdot \theta \cdot \langle x, Y \rangle)]|^2$$
$$= |\mathbb{E}_{Y_1}[\exp(2\pi i \theta x_1 Y_1) \cdot \mathbb{E}_{Y_{>1}}[\exp(2\pi i \cdot \theta \cdot \langle x_{>1}, Y_{>1} \rangle)]]|^2$$
$$= |\mathbb{E}_{Y_1}[\exp(2\pi i \theta x_1 Y_1) \cdot Z_{Y_1}]|^2.$$

If Y_1 has entropy, for at least **half** the choices of x_1,
$$\leq \exp(-\sin^2(4\pi\theta)) \cdot \mathbb{E}_{Y_1}[|Z_{Y_1}|^2]$$

If Y_1 has no entropy,
$$\leq \mathbb{E}_{Y_1}[|Z_{Y_1}|^2]$$

By counting arguments:

- $\Omega(n)$ coordinates of Y have entropy
- Most x will make the **right** choice in $\Omega(n)$ of these coordinates.

Open Questions

[Erdös-Moser, Sárkozy-Szemerédi]

If the coordinates of x are distinct, $Y \in \{\pm 1\}^n$ uniform,

$$\Pr[\langle x, Y \rangle = k] \leq O(n^{-3/2})\,.$$

Thm [Our work]: If $X \in_R A \subseteq \{\pm 1\} \times \{\pm 2\} \times \ldots \{\pm n\}$, $Y \in_R B \subseteq \{\pm 1\}^n$, and $|A| \cdot |B| > 2^{1.01n}$, then

$$\Pr[\langle X, Y \rangle = k] \leq O(\sqrt{\log n} \cdot n^{-3/2})\,.$$

Conjecture: If $X \in_R A \subseteq \{\pm 1\} \times \{\pm 2\} \times \ldots \{\pm n\}$, $Y \in_R B \subseteq \{\pm 1\}^n$, and $|A| \cdot |B| > 2^{1.01n}$, then

$$\Pr[\langle X, Y \rangle = k] \leq O(n^{-3/2})\,.$$

Thanks!