How to guess an n-digit number

ACM-SIAM Symposium on Discrete Algorithms

January 6-9, 2019

Nikita Polyanskii (Skoltech)

Joint work with Zilin Jiang (MIT)

This talk is about

The metric dimension of the Hamming graph

This talk is about

The metric dimension (2) of the Hamming graph (1)

1. The Hamming graph is the Cartesian product of n complete graphs K_q
2. The metric dimension of a graph is the minimum cardinality of a subset S of vertices such that all other vertices are uniquely determined by their distances to the vertices in S

This talk is about

The metric dimension (2) of the Hamming graph (1), denoted by $\boldsymbol{m(K_q, n)}$

1. The Hamming graph is the Cartesian product of n complete graphs K_q
2. The metric dimension of a graph is the minimum cardinality of a subset S of vertices such that all other vertices are uniquely determined by their distances to the vertices in S

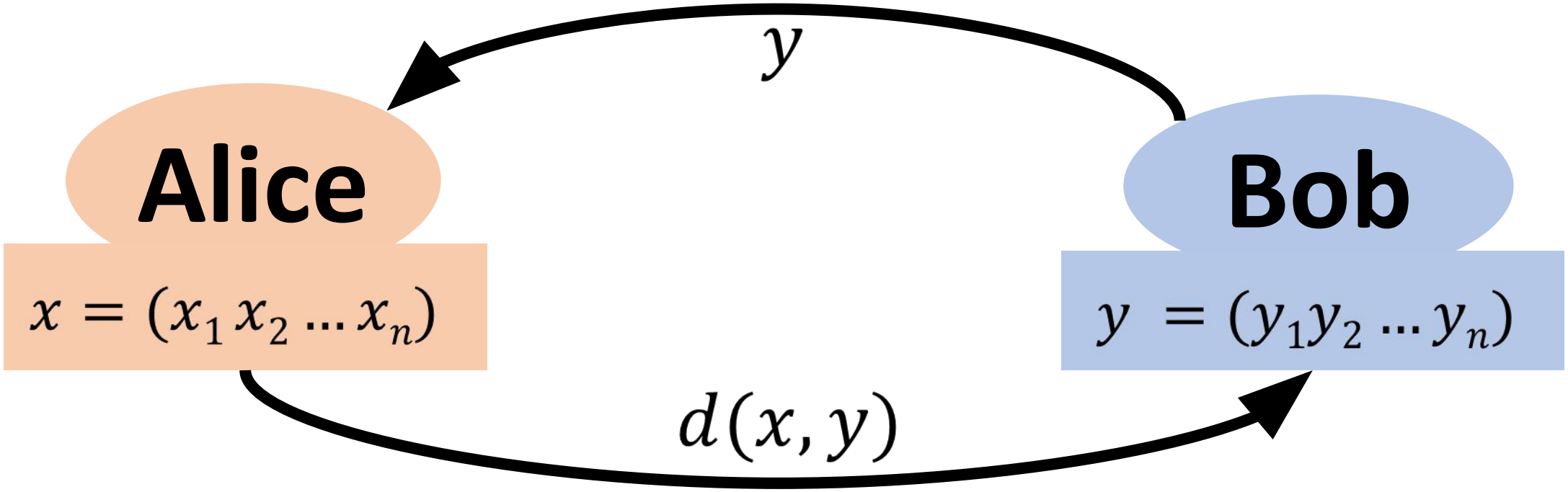
Our contribution: the asymptotic (q is fixed, n is large) of $m(K_q, n)$ *is*

$$m(K_q, n) \sim 2n/\log_q n$$

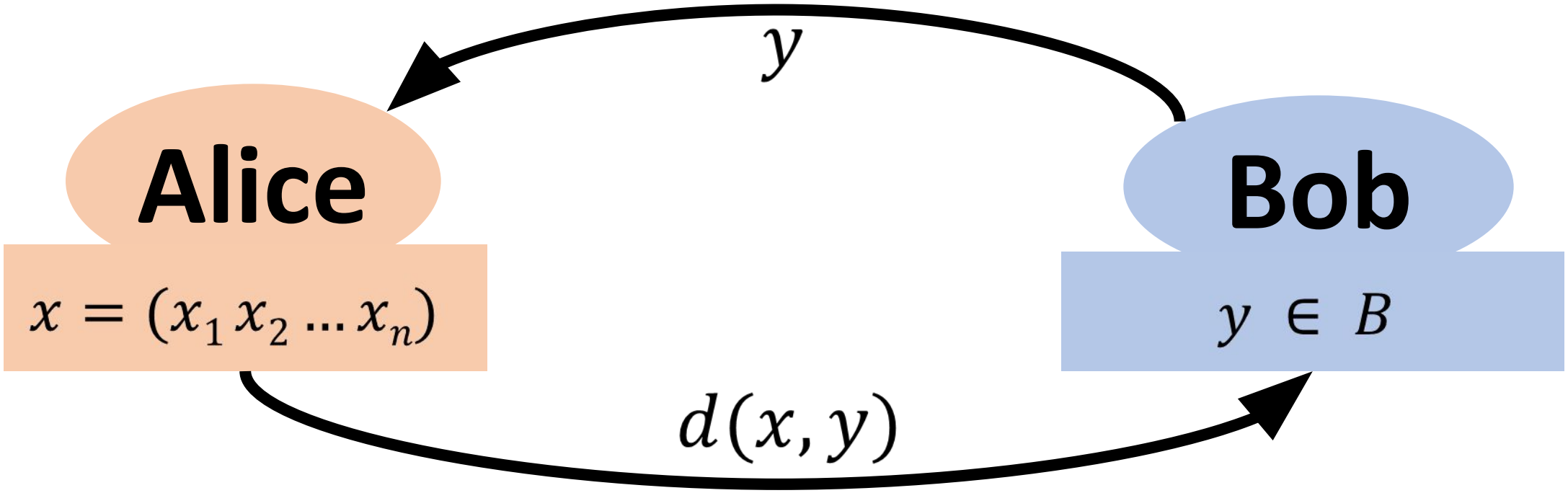
Outline

1. Introduction and related problems
   - Coin-weighing problem, Mastermind game
2. Construction (upper bound)
   - is based on the theory of Mobius functions
3. Lower bound
   - is based on the information-theoretic method
4. A more general problem…
   - The metric dimension of the Cartesian powers of a graph
5. The End

1. Introduction and related problems


y
Alice
$x = (x_1 x_2 \dots x_n)$
Bob
$y = (y_1 y_2 \dots y_n)$
$d(x, y)$

Goal: Bob must identify any hidden n-digit x based on $(d(x,y))_{y\in B}$



Definition: If so, B is called a ***base*** (of the q-ary n-dim. Hamming space).

Definition: The ***metric dimension*** $m(K_q, n)$ of the q-ary n-dim. Hamming space (or equivalently the Cartesian n-th power of K_q) is

$$m(K_q, n) := \min_{\text{base } B} |B|.$$

Problem: Given $q \geq 2$, find the asymptotic behavior $m(K_q, n)$ as $n \to \infty$.

Binary case (coin-weighing problem)

The problem was posed by Söderberg-Shapiro’63

Binary case (coin-weighing problem)

$m(K_2, n) \gtrsim 2n/\log_2 n$
by Erdös-Rényi'63
Moser'70, Pippenger'77

$m(K_2, n) \lesssim 2n/\log_2 n$
by Lindström'64
Cantor-Mills'66
Martirosyan-Khachatryan'89
Bshouty'09

q-ary case (Mastermind game)

- The commercial version was invented by Meirowitz'70 and was solved y Knuth'76
- The study of **non-adaptive** Mastermind game was initiated by Chvatal'83

q-ary case (Mastermind game)

$$m(K_q, n) \gtrsim 2n/\log_q n$$

by Kabatianskii et al'99

for $q = 3,4$, $m(K_q, n) \lesssim 2n/\log_q n$

by Kabatianskii-Lebedev'18

2. Construction (upper bound)

Let $(\mathbb{N}, \prec)$ be a *poset*, where $i \preccurlyeq j$ iff $i = i\&j$.

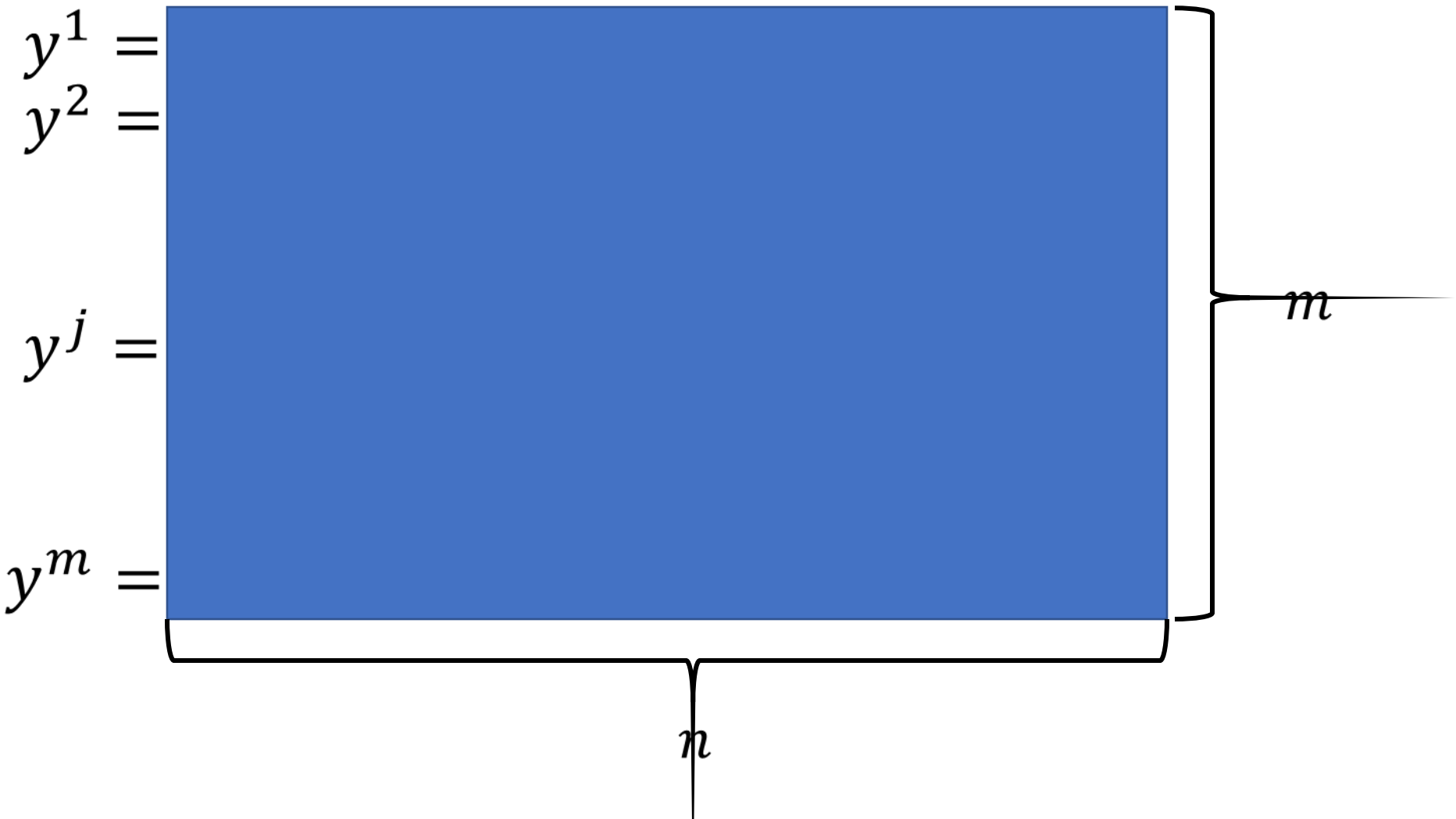
BITWISE AND

Define the *Mobius function*

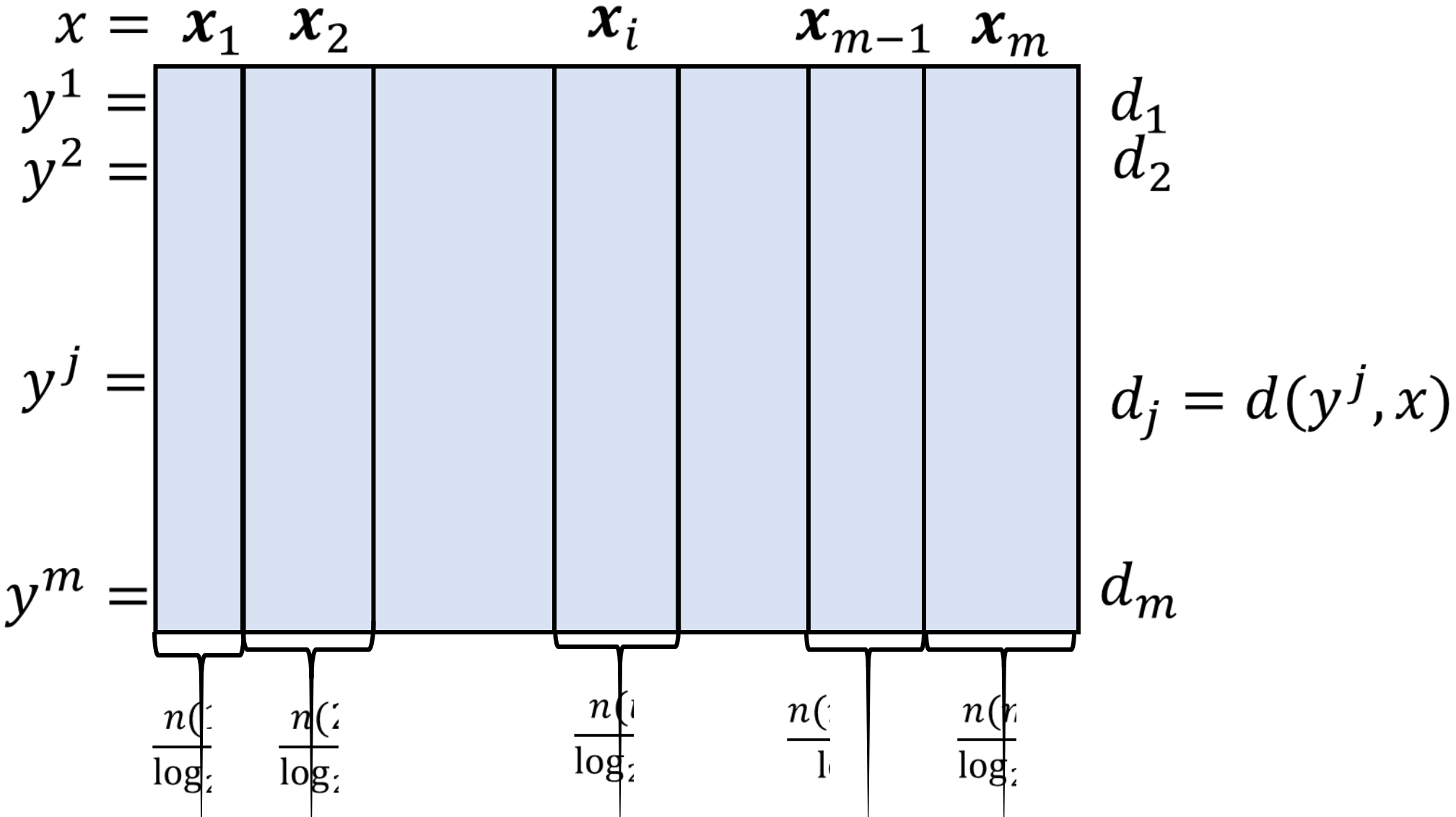
$$\mu(i,j) := \begin{cases} 1 & \text{if } i = j \\ -\sum_{i \preccurlyeq k \prec j} \mu(i,k) & \text{if } i \prec j \end{cases}$$

Here, $\mu(i,j) := (-1)^{n(i)-n(j)}$, where $n(u) :=$ #of $1's$ in the binary representation of u.

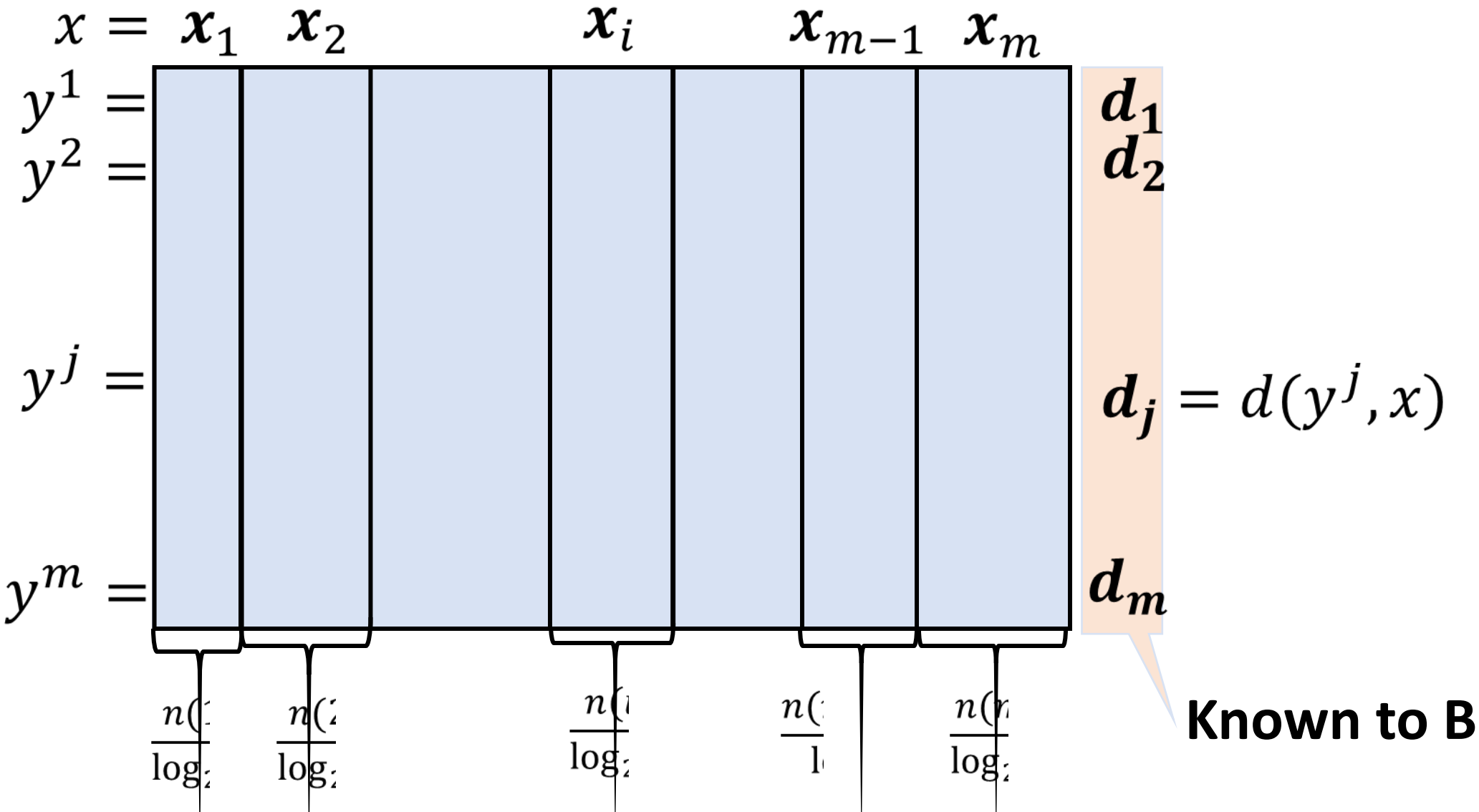
Let us put vectors from a base B of the q-ary n-dim.
Hamming space in rows of matrix $Y = (y^1, y^2, \dots, y^m)^T$



Divide hidden vector $x = (x_1 x_2 \ldots x_n)$ into m subvectors



Divide hidden vector $x = (x_1 x_2 \ldots x_n)$ into m subvectors



Known to Bob!

Decoding:

1. Consider the value

$$D_m := \sum_{i=1}^{m} \mu(i,m) d_i \ = f_m(\boldsymbol{x}_m),$$

and $\boldsymbol{x}_m$ can be extracted ($\boldsymbol{x}_m$ is a somewhat q-ary expansion of D_m).

2. Consider the value

$$D_{m-1} := \sum_{i=1}^{m} \mu(i,m-1) d_i = f_{m-1}(\boldsymbol{x}_m, \boldsymbol{x}_{m-1}),$$

and $\boldsymbol{x}_{m-1}$ can be extracted.

And so on…

3. Lower bound

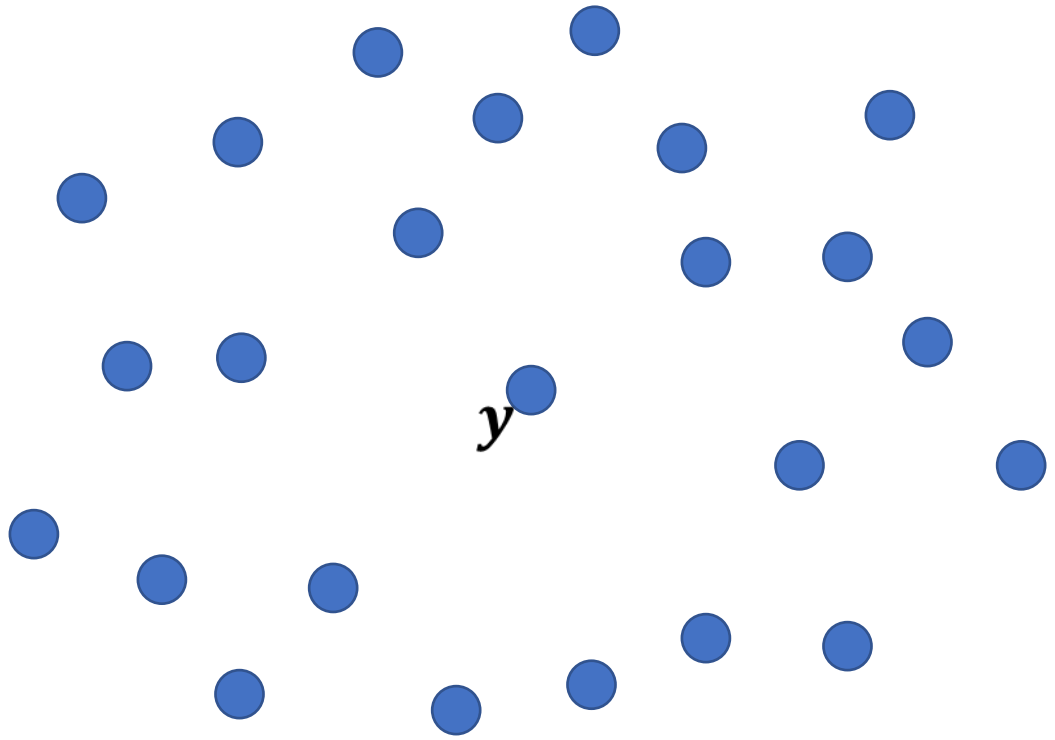
Claim (informal)

For any base B, its size m is at least $2n/\log_q n$

Proof idea is a modification of the Erdös-Rényi'63 arguments…

Claim (informal)

For any base B, its size m is at least $2n/\log_q n$



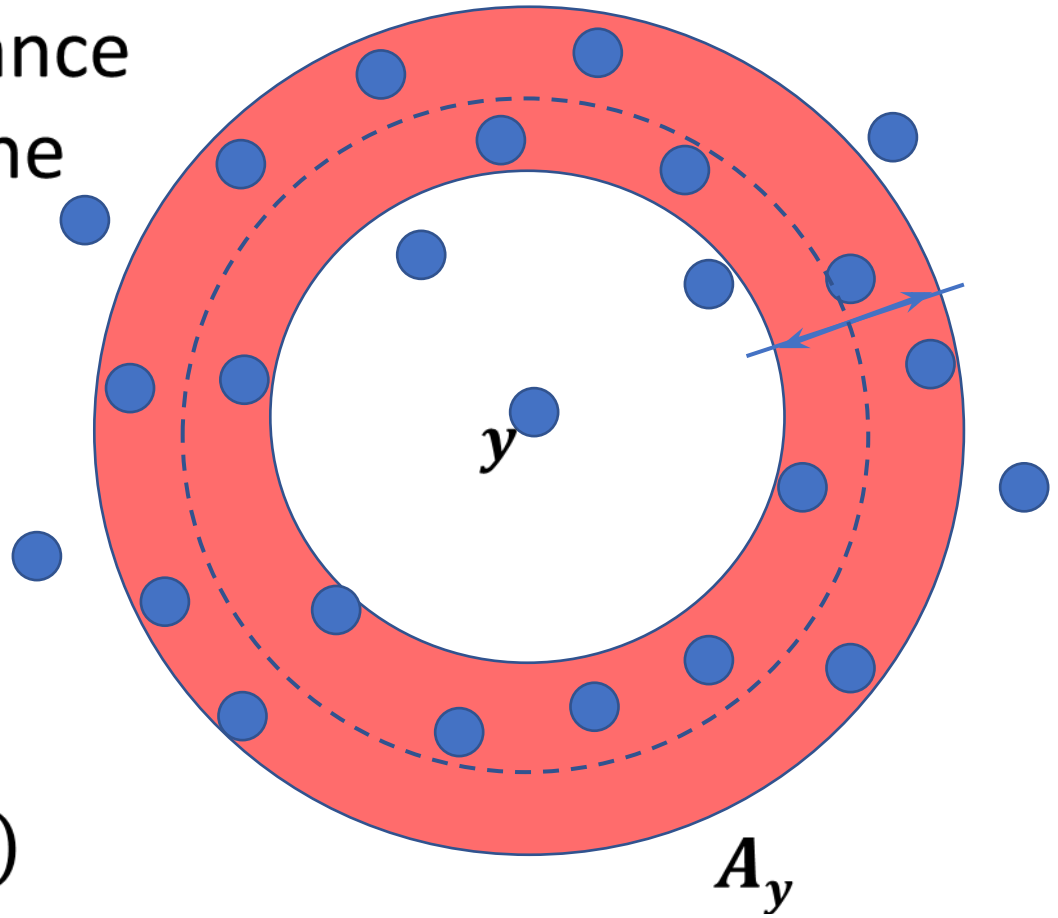
point in Base B

$y = (y_1, \ldots, y_n)$

Claim (informal)

For any base B, its size m is at least $2n/\log_q n$

A_y - set of points at distance "close" to expected one



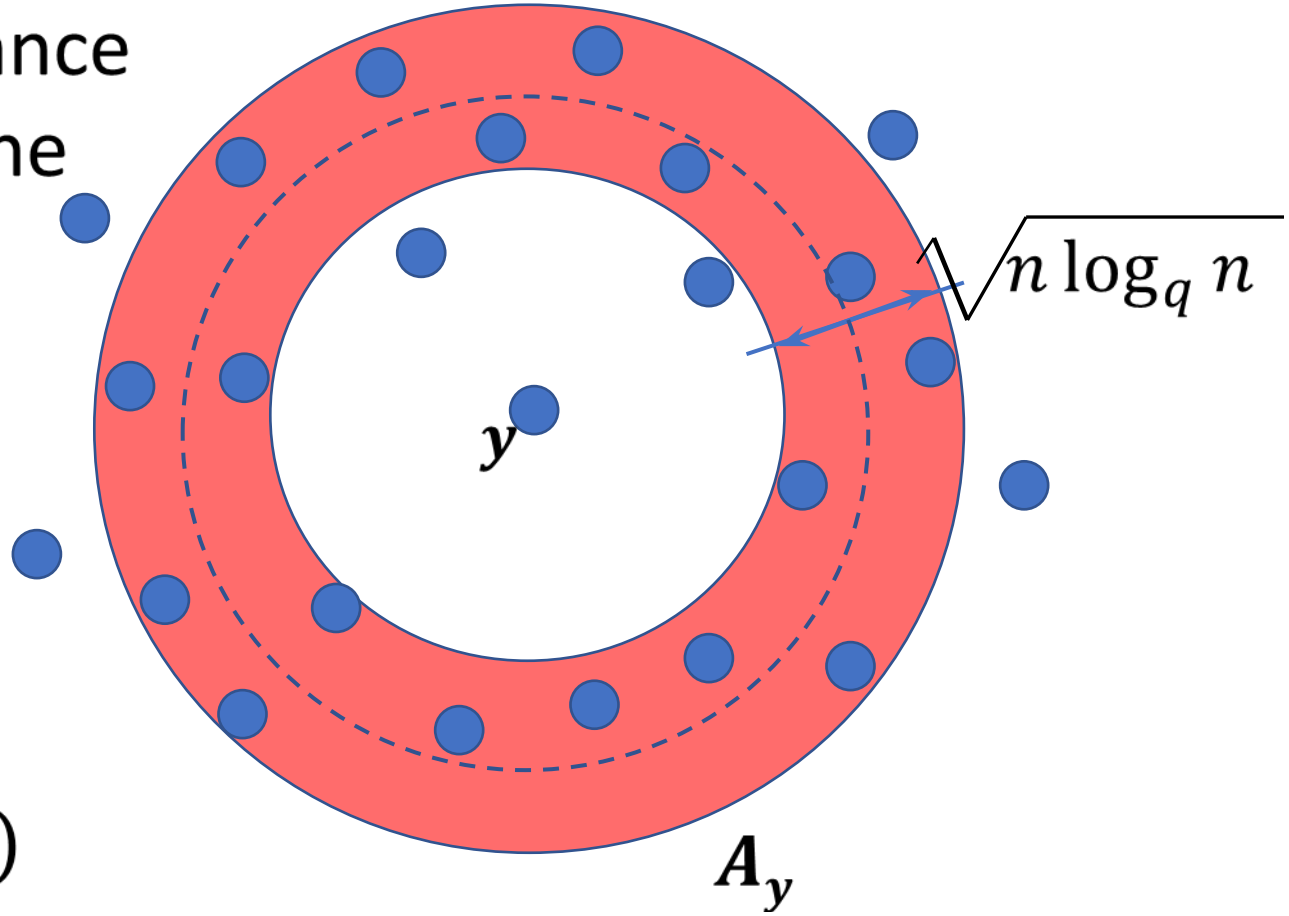
point in Base B

$$y = (y_1, \ldots, y_n)$$

Claim (informal)

For any base B, its size m is at least $2n/\log_q n$

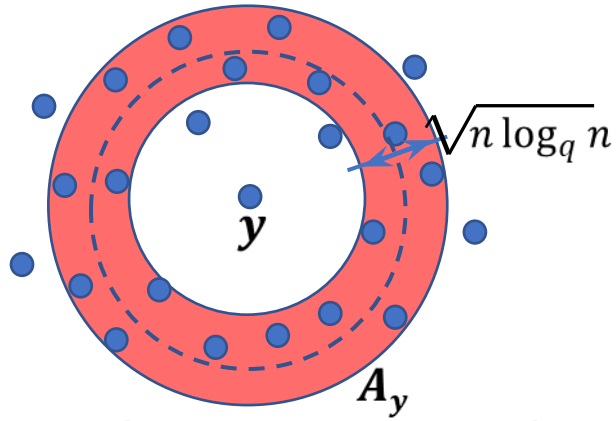
A_y - set of points at distance **"close"** to expected one



point in Base B

$y = (y_1, \ldots, y_n)$

Need two things:



1. From Hoeffding's inequality it follows A_y is large enough. Moreover, the cardinality $|\bigcap_{y \in B} A_y| > (1 - \varepsilon)q^n$.

2. Define the map d_B: $\bigcap_{y \in B} A_y \to \mathbb{N}^m$ as $d_B := \big(d(x, y)\big)_{y \in S}$

This map is **injective**. So the cardinality of the domain is less than or equal to the cardinality of the range

This logic (with some computation) proves the claim!

4. A more general problem…

Definition: A subset S of vertices in a graph $G = (V, E)$ is called a ***base*** of G, if the map

$$d_S\colon V \to \mathbb{N}^{|S|} \text{ defined as } d_S(x) \coloneqq (d(x, y))_{y \in S}$$

is injective.

Definition: Given a connected graph G , the ***metric dimension*** $m(G, n)$ of the Cartesian n-th power of G is

$$m(G, n) \coloneqq \min_{\text{base } B} |B|.$$

Problem: Given G, find the asymptotic behavior $m(G, n)$ as $n \to \infty$.

Theorem (Jiang-P.'18)

Given a connected graph G on q vertices, let M be the distance matrix of G. If the matrix

$$\begin{pmatrix} M & \mathbf{1} \\ \mathbf{1}^T & 0 \end{pmatrix}$$

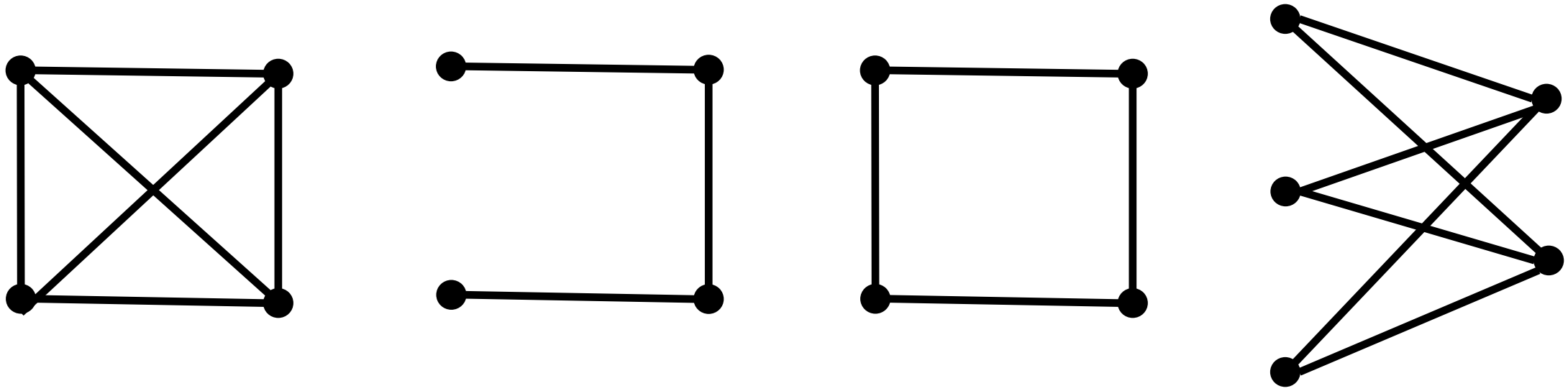
is invertible, then the metric dimension $m(G, n)$ is

$$m(G, n) \sim 2n/\log_q n$$

Corollary (*some graph classes*)

If G is a complete graph, a path, a cycle or a complete bipartite graph on q vertices, then the asymptotic of $m(G, n)$ is as follows

$$m(G\,, n) \sim 2n/\log_q n$$



Corollary (*small graphs*)

For any $q \leq 9$ and any* G on q vertices, the asymptotic of $m(G, n)$ is as follows

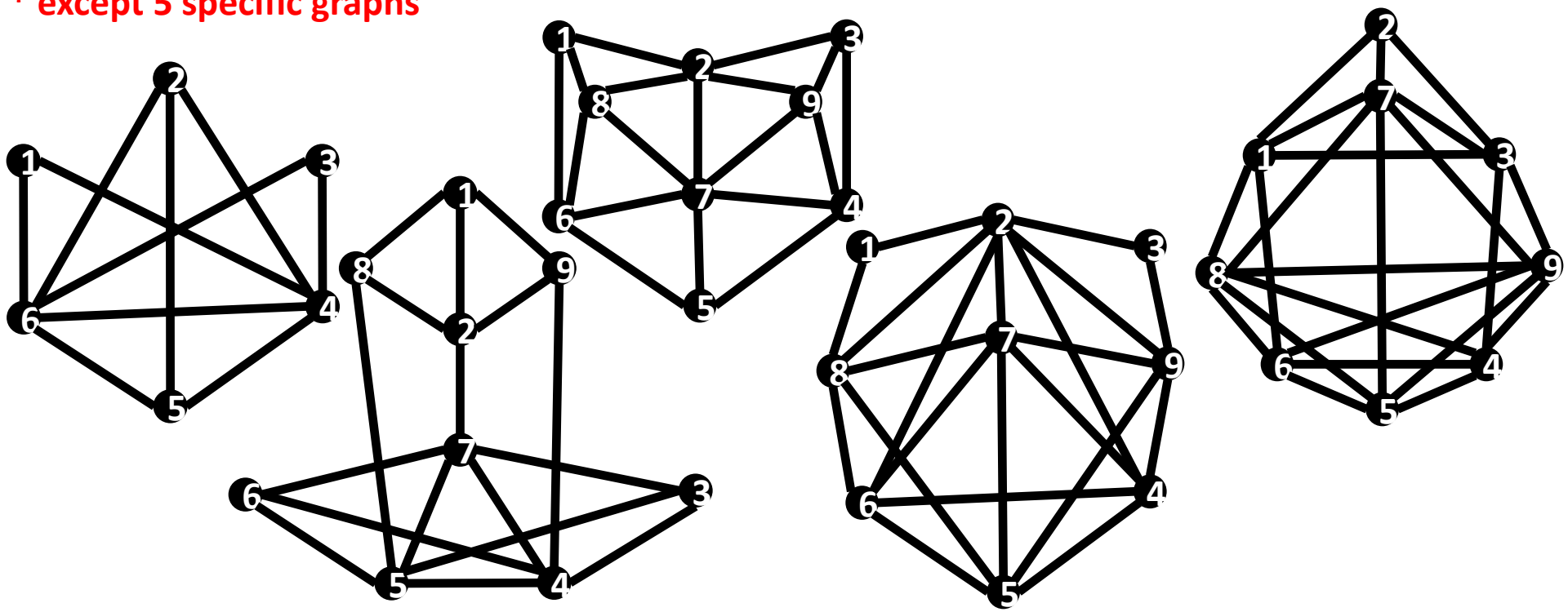
$$m(G, n) \sim 2n / \log_q n$$

Corollary (*small graphs*)

For any $q \leq 9$ and any* G on q vertices, the asymptotic of $m(G,n)$ is as follows

$$m(G,n) \sim 2n/\log_q n$$

* except 5 specific graphs



Open questions

- Can we get the same asymptotic of $m(G, n)$ for any graph G?
  - A subproblem: given n distinct vectors $u_1, u_2, \dots, u_n \in \mathbb{Z}^n$, how to minimize $v \in \mathbb{Z}^n$ so that $< v, u_i >$ are different. Here, $\min \| v \|$ should be $O(n)$.
- What can we say about the metric dimension of other metric spaces?
  - E.g. Johnson and Kneser graphs.

Thanks!

Questions?