Shadows and cryptology

جولا کاتنا

Gyula O.H. Katona
Rényi Institute, Budapest

ICTP-IPM Conference in
Combinatorics and Graph Theory

The Abdul Salam International Centre
for Theoretical Physics Trieste, Italy

September 10, 2012

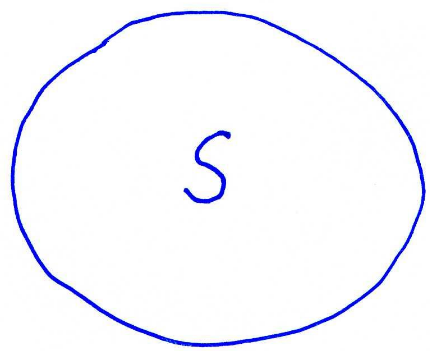
The practical problem

label,

impossible to copy because of its 3-dimensional nature

A mapping

$f :$



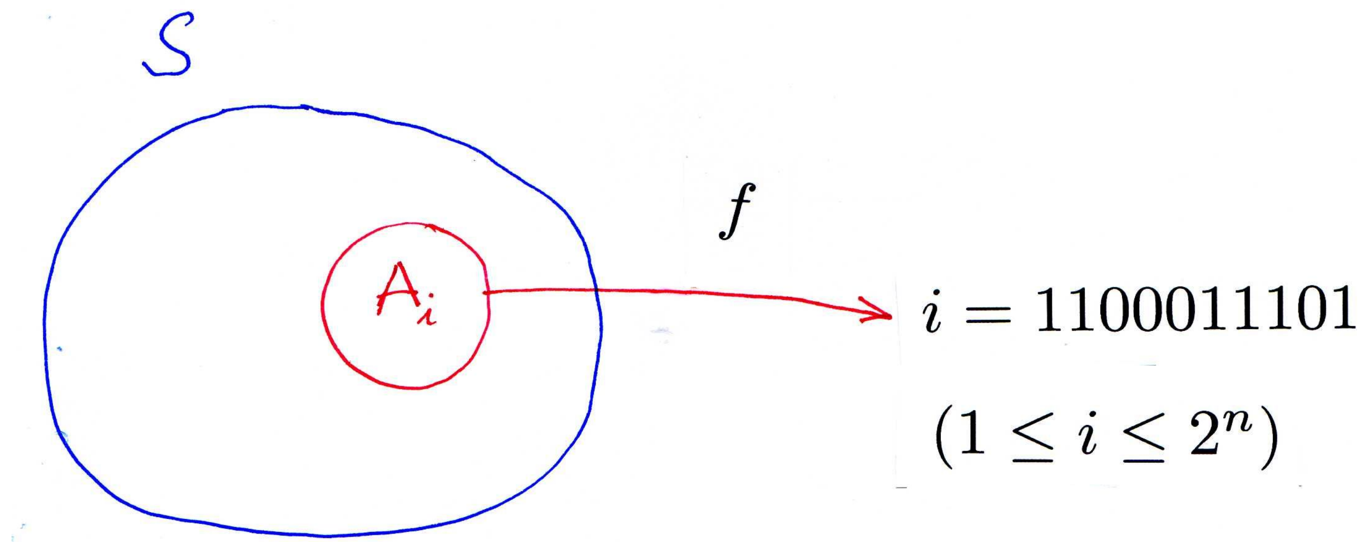
$\longrightarrow \{0,1\}^n$

space of all possible labels

$|S| >>> 2^n$


2230 6643 0044 3333
GALILEO GALILEI
1100011101
VISA

Its properties



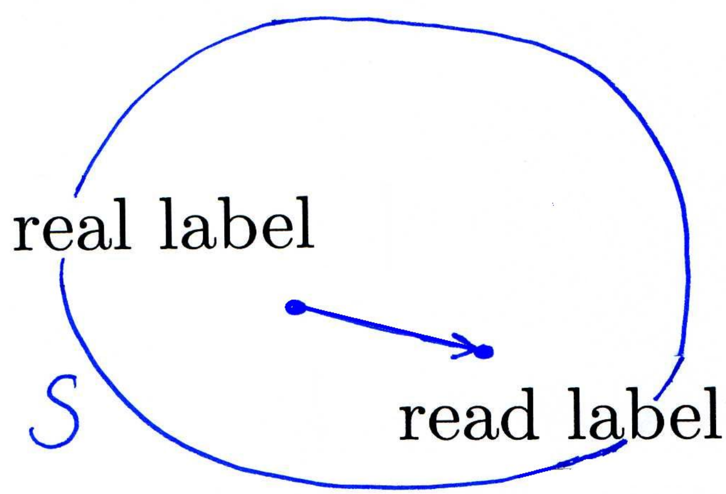
$$A_i \cap A_j = \emptyset \quad (i \neq j)$$

Reading with error

a distance is given on S

$$0 \leq d(a,b) \quad a,b \in S$$

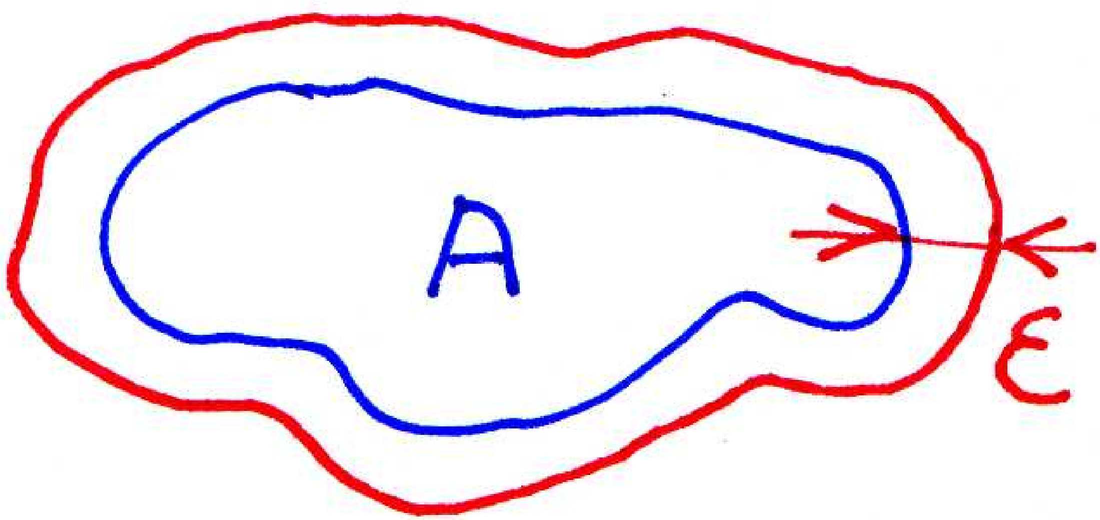
$$d(\text{real label},\ \text{read label}) \leq \varepsilon$$ where $0 < \varepsilon$ is given



neighborhood

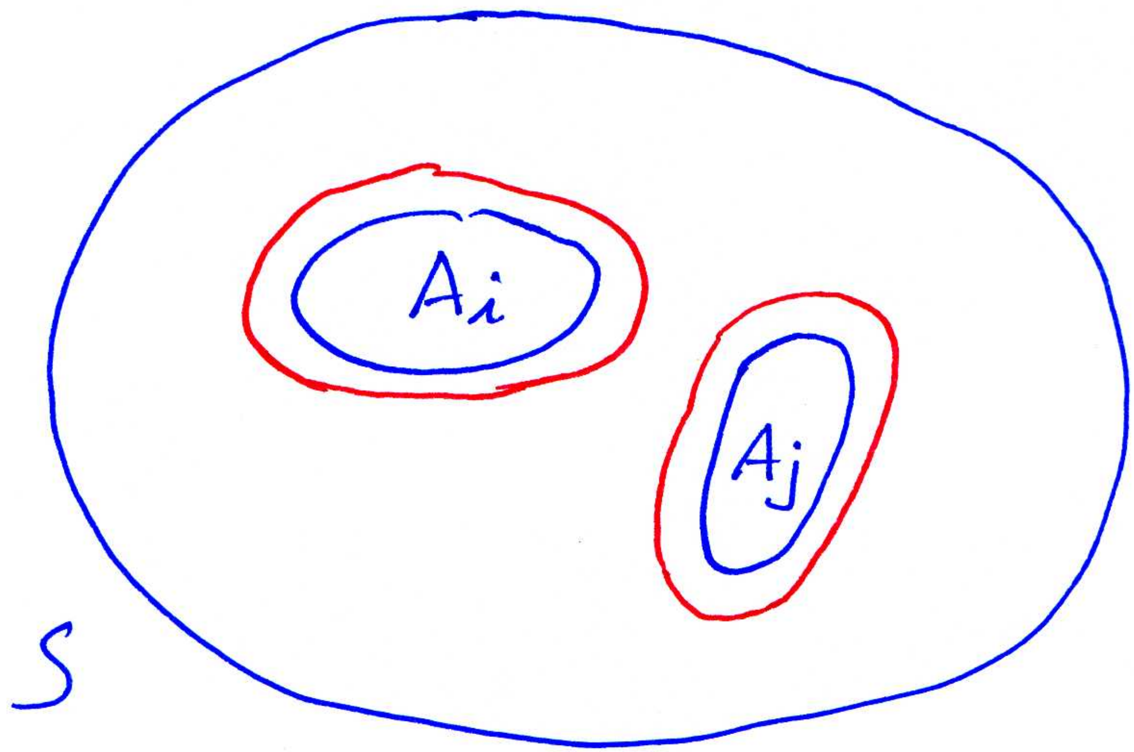
$A \subset S$

$n(A, \varepsilon) = \{x \in S : \ d(A, x) \leq \varepsilon\}$



neighborhoods are disjoint

$$n(A_i, \varepsilon) \cap n(A_j, \varepsilon) = \emptyset \ (i \neq j)$$



A_i cannot be large

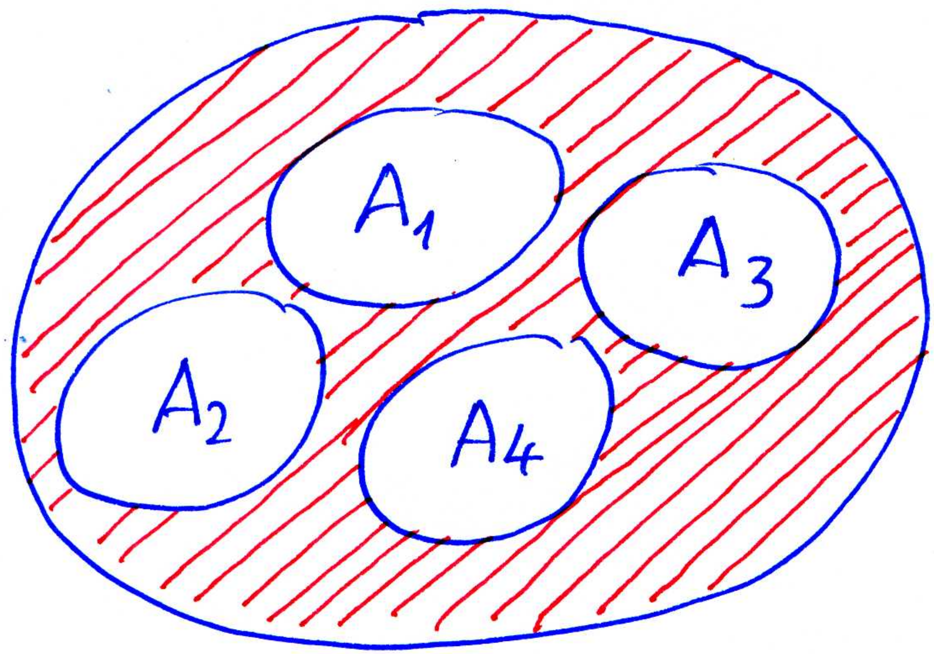
If A_i is large then the swindler chooses an $x \in S$ “randomly” and $x \in A_i$ will have a “large probability”.

This is why a measure μ must be considered on S.

$\mu(A_i) \leq \rho \; (1 \leq i \leq 2^n)$

where $0 < \rho$ is given.

waste



waste cannot be too large:

$\mu\left(\cup_{i=1}^{n} A_i\right) \geq \alpha$ where $0 < \alpha$ is not very small, say 0.1.

Definition

Geometric identifying code in S

(endowed with a distance d and a measure μ) with

error tolerance ε (> 0),

waste rate α (> 0),

security ρ (> 0)

is a family of sets $A_1, \ldots, A_{2^n} \subset S$ such that

$n(A_i, \varepsilon) \cap n(A_j, \varepsilon) = \emptyset \ (1 \leq i < j \leq 2^n)$,

$\mu\left(\cup_{i=1}^n A_i\right) \geq \alpha$,

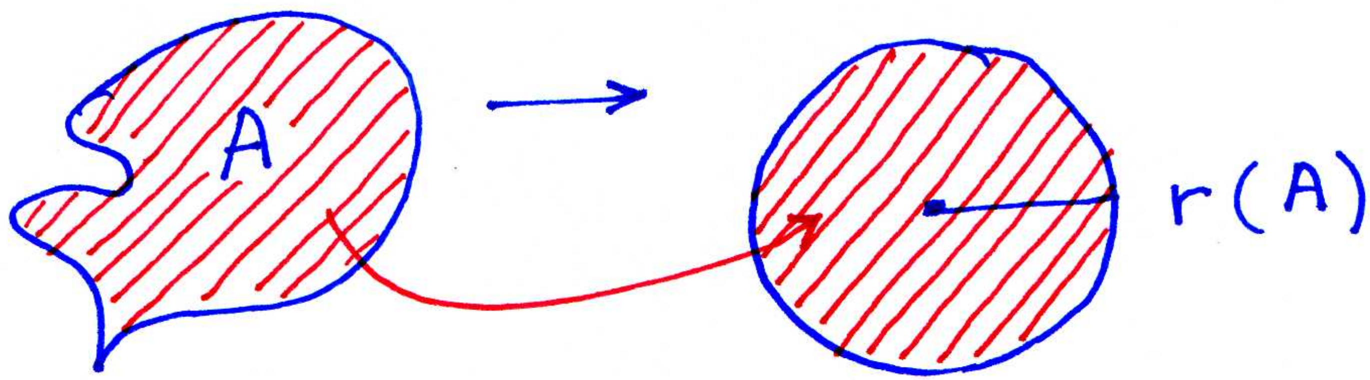
$\mu(A_i) \leq \rho \ (1 \leq i \leq 2^n)$.

Ball of radius r with center x: $b(x, r)$

Suppose:

$(*)$ $\mu(b(x, r))$ **independent of** x $(= \mu(r))$

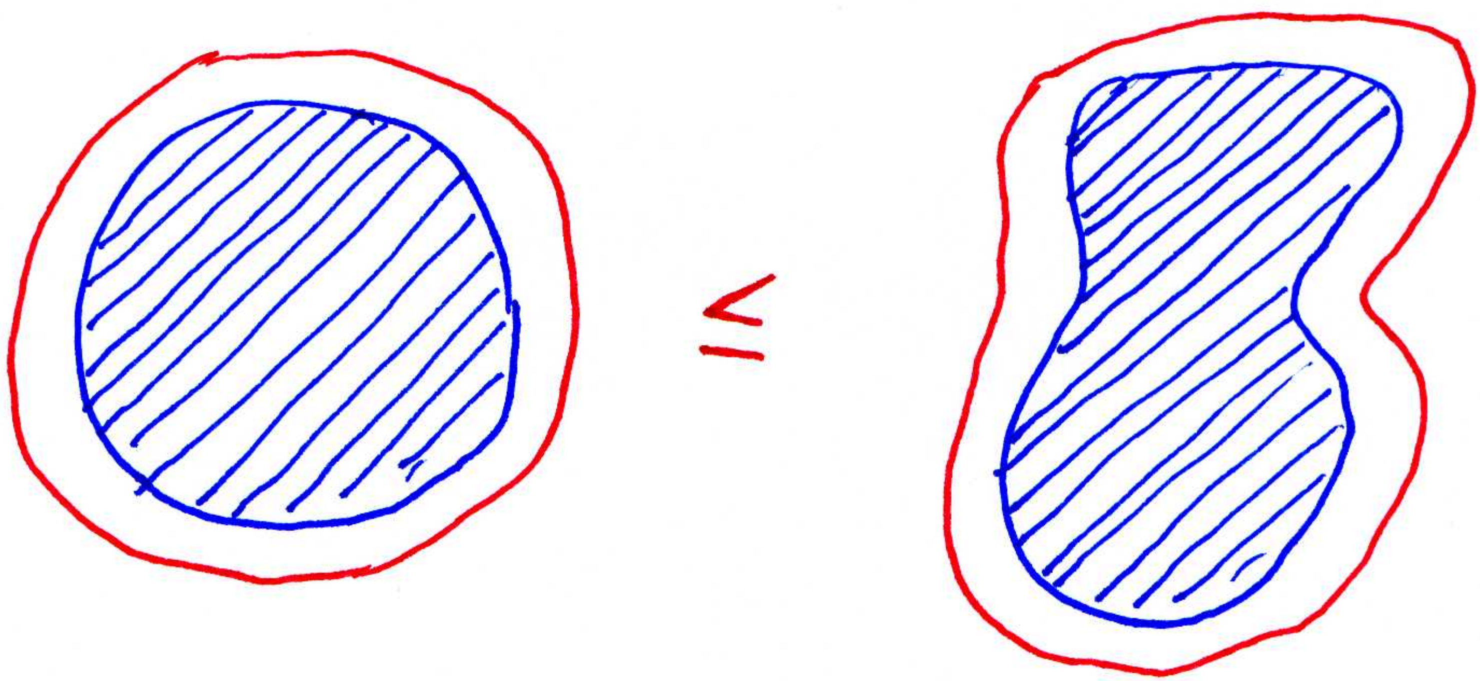
Notation: $r(A) =$ radius of a ball with measure $= \mu(A)$



Brunn-Minkowski property

Suppose:

$$(**) \qquad \mu(n(b(x,r(A))),\varepsilon) \leq \mu(n(A,\varepsilon))$$



$\mu^{-1}(x)$ is the **radius** of a ball with measure x.

Theorem (Csirmaz-Katona, 2003)

If $(*)$ and $(**)$ hold then

$$\varepsilon \le \mu^{-1}\left(\frac{\rho}{\alpha}\right) - \mu^{-1}(\rho)$$

for a geometric identifying code with parameters $\varepsilon, \alpha, \rho$.

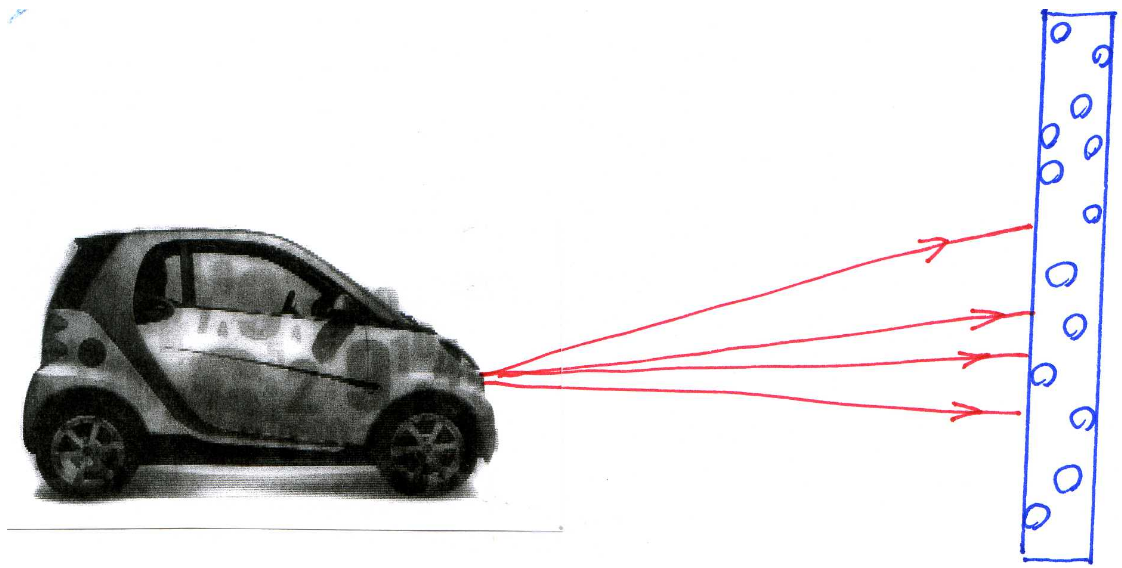
A functioning prototype was constructed by

Haraszti, Marsovszky (Hewlett Packard, Hungary)

and

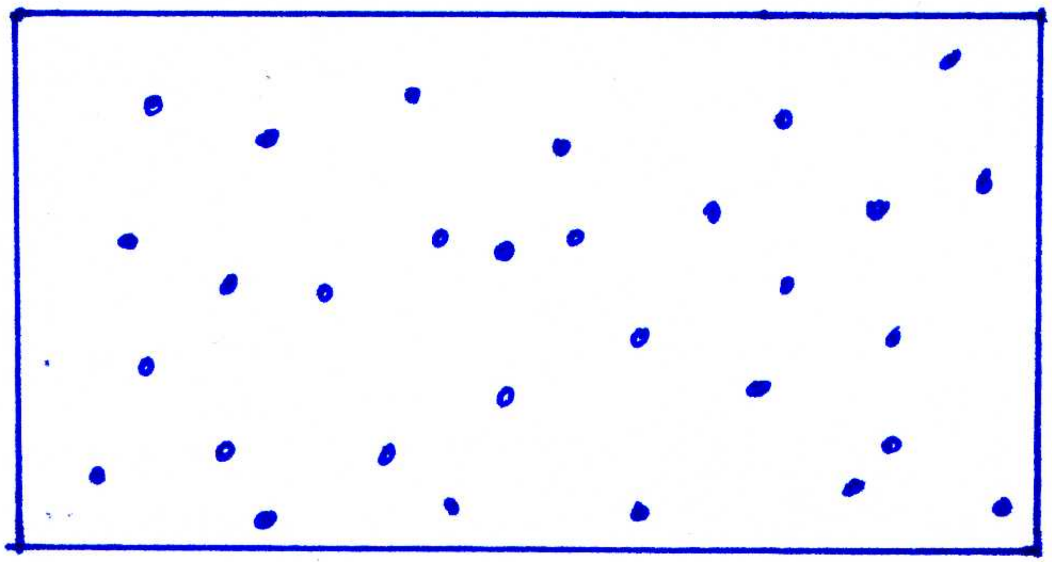
Csirmaz, Katona, Miklós, Nemetz (Rényi Institute, Budapest)

Label: reflecting foil



random, 3-dimensional

mathematically



a set of points (centers of the glass balls)

their number is between two bounds

unordered

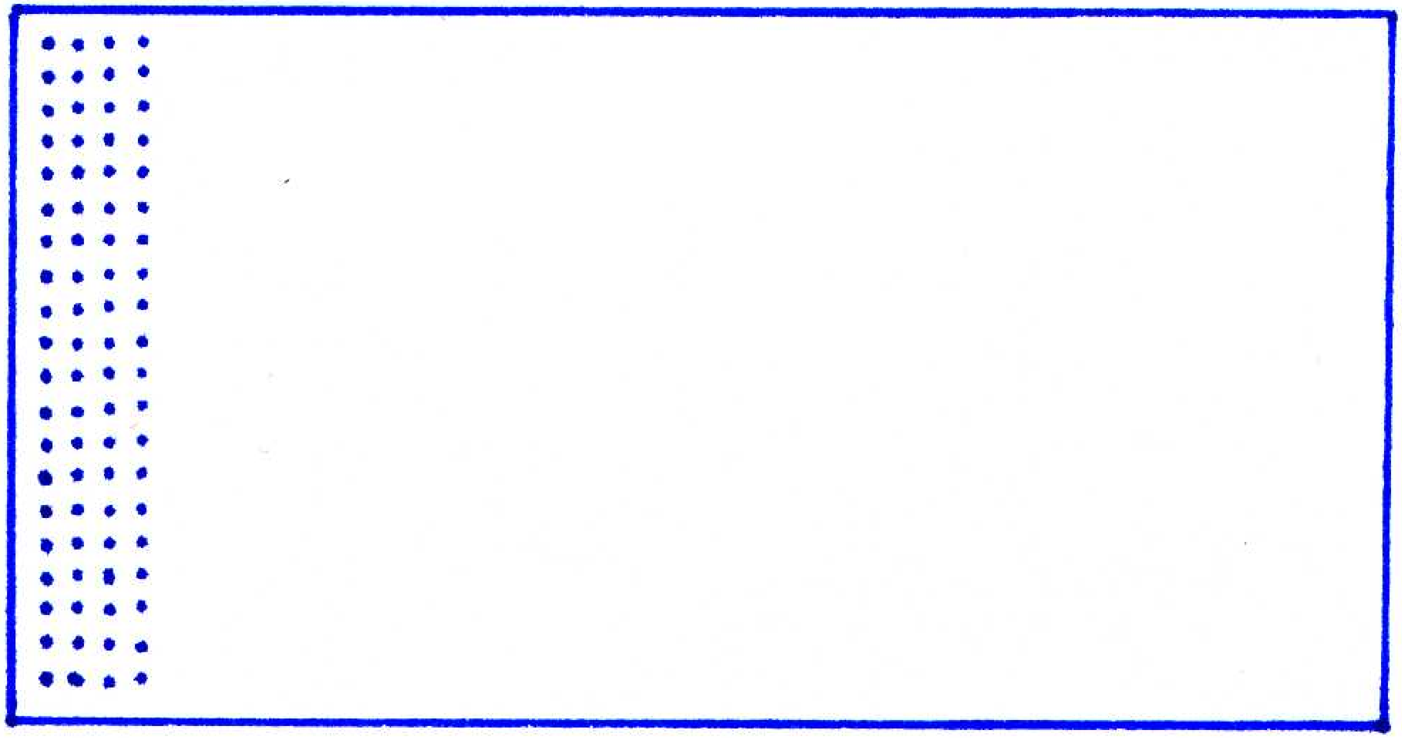
Big surprise: some points disappear at the reading

$\Longrightarrow$

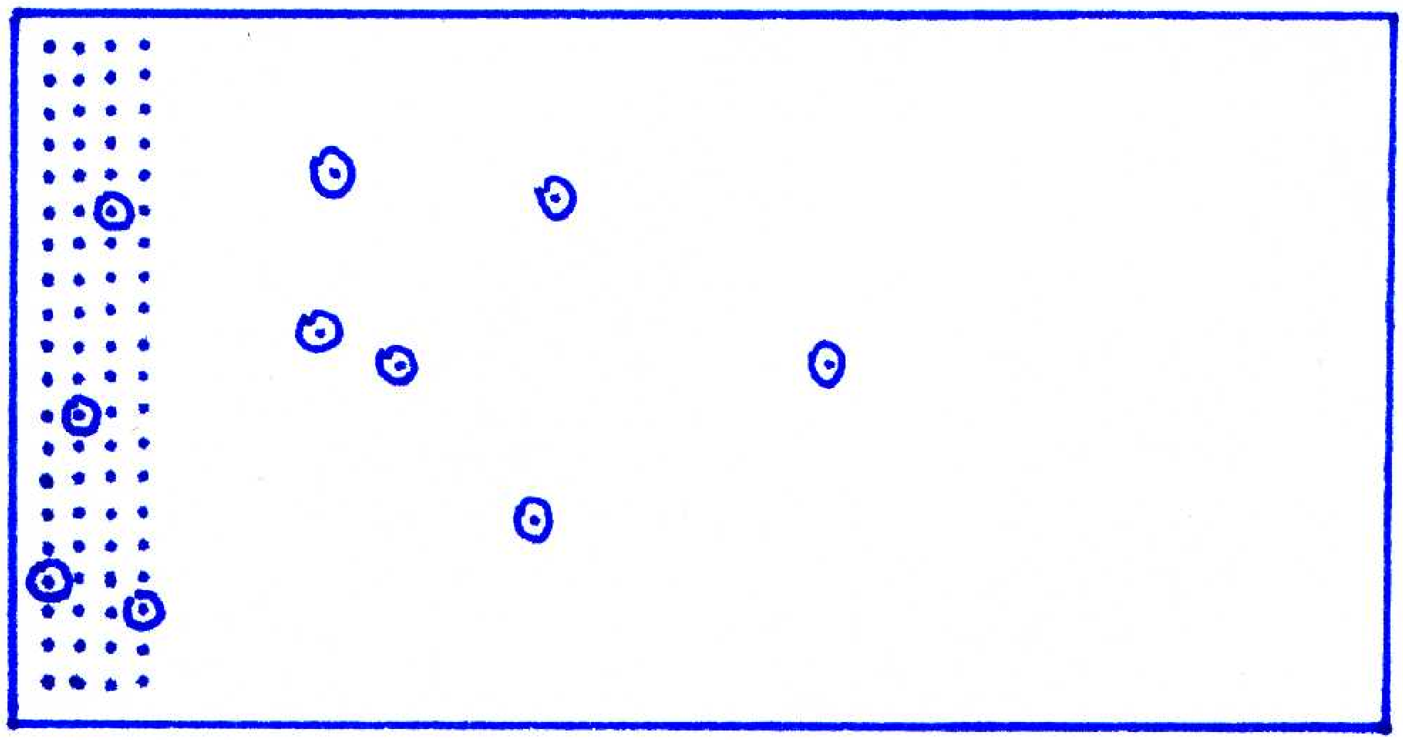
distance d between labels is defined not only by their geometry, but the also by the set distance

computational accuracy $\Longrightarrow$

number of possible points is finite



A **label** is a **subset** of the possible points



Our model in this particular case

Given a finite set of N points.

Space S consists of subsets of this N-element set X.

Illustrated by 0,1 sequences of length N.

Given $0 < k < N$, suppose that the number of elements (number of 1s in the sequence) is exactly k.

This is a condition to make the model mathematically treatable. The real condition would be: the number of 1s is between two bounds.

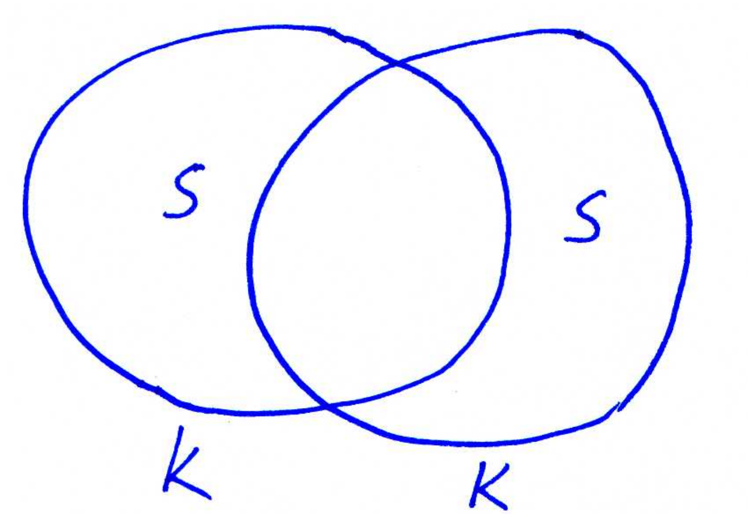
The size of the space is

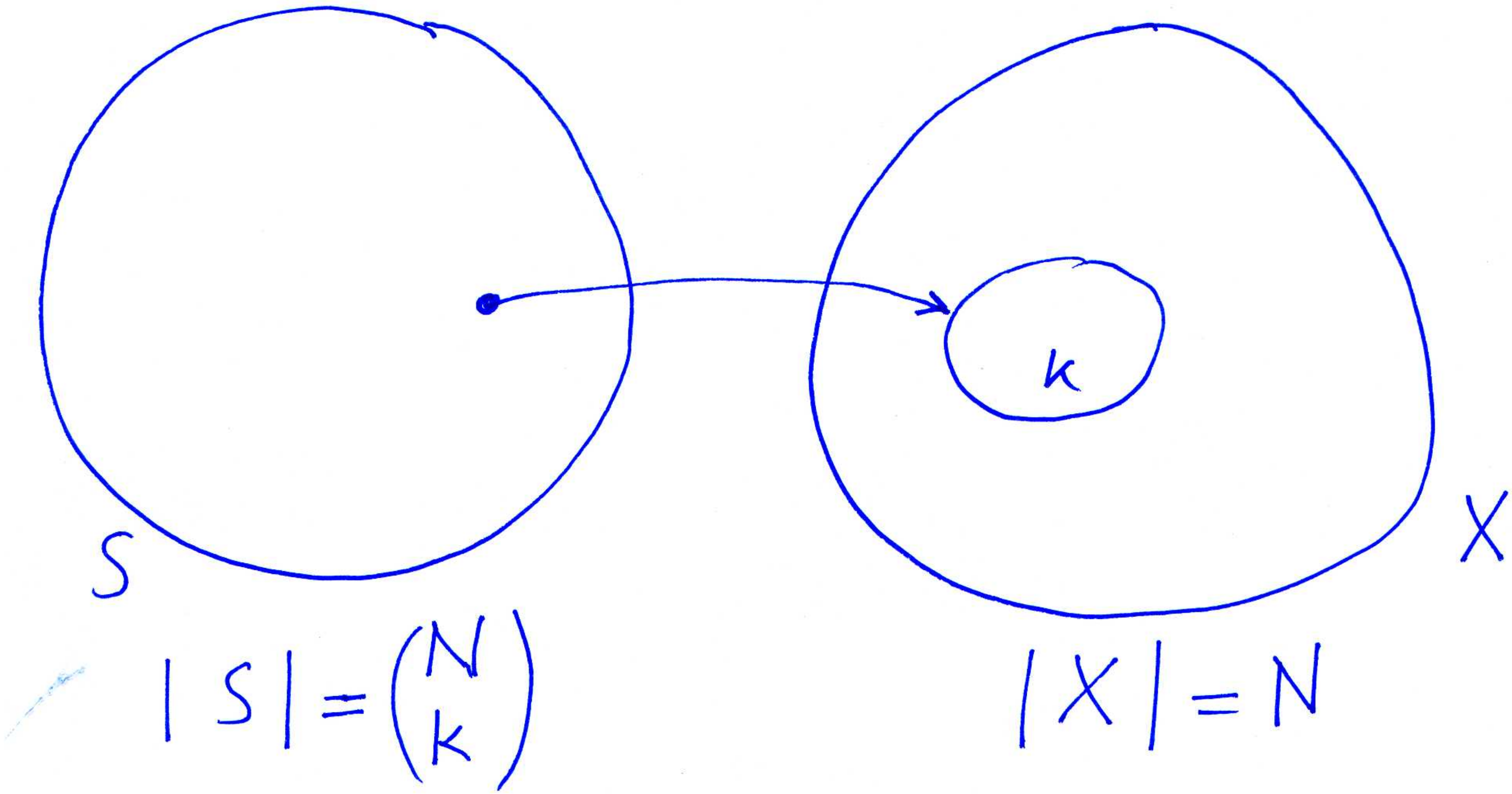
$$|S| = \binom{N}{k}.$$

Distance d of two sequences in S $=$ Hamming distance

(= number of different digits = size of the symmetric difference)

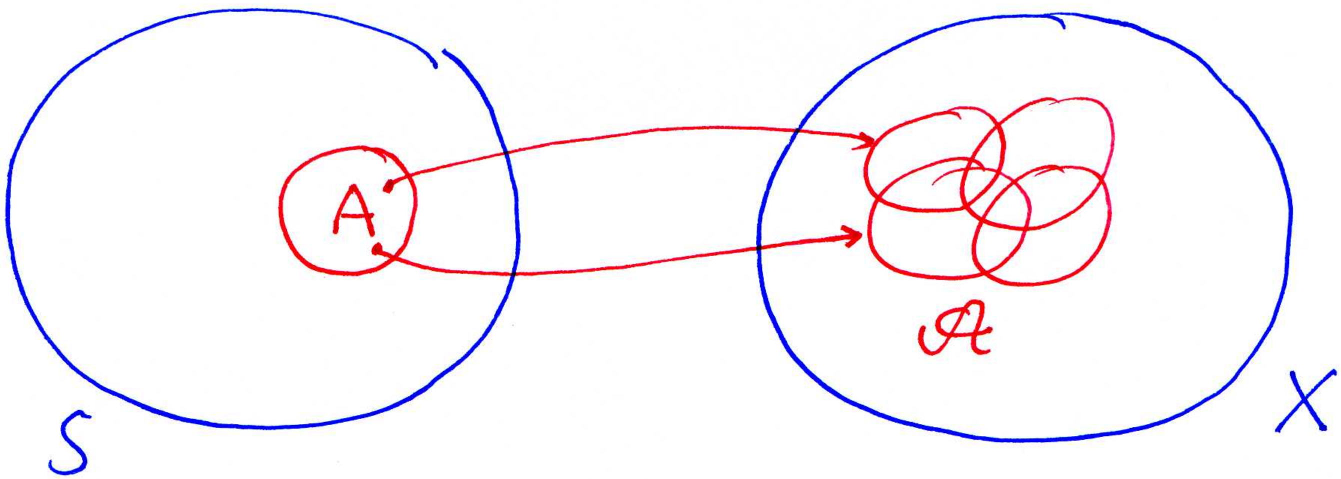
This is a condition to make the model mathematically treatable. The real distance would be a combination of this with the geometrical distance. For instance, the distance of two such sets is $2s$ if:





One element of S is a k-element subset of (the N-element) X.

A set A of elements of S is a family of k-element sets. It will be denoted by $\mathcal{A}$.



Its measure:

$$\mu(\mathcal{A}) = \frac{|\mathcal{A}|}{\binom{N}{k}}.$$

- **security:**

$$\mu(\mathcal{A}_i) = \frac{|\mathcal{A}_i|}{\binom{N}{k}} < \rho,$$

that is,

$$|\mathcal{A}_i| < \rho \binom{N}{k} = \binom{x}{k} = \frac{x(x-1)\ldots(x-k+1)}{k!}$$

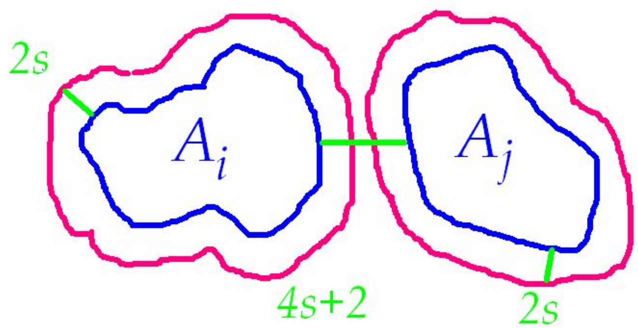
for some positive real number $x > 0$.

Neighbor of $\mathcal{A}$

= $n(\mathcal{A}, 2s)$: all k-element sets of distance at most $2s$ from a member of $\mathcal{A}$, that is, the k-element sets obtained from a member by deleting at most s elements and adding the same number of elements.

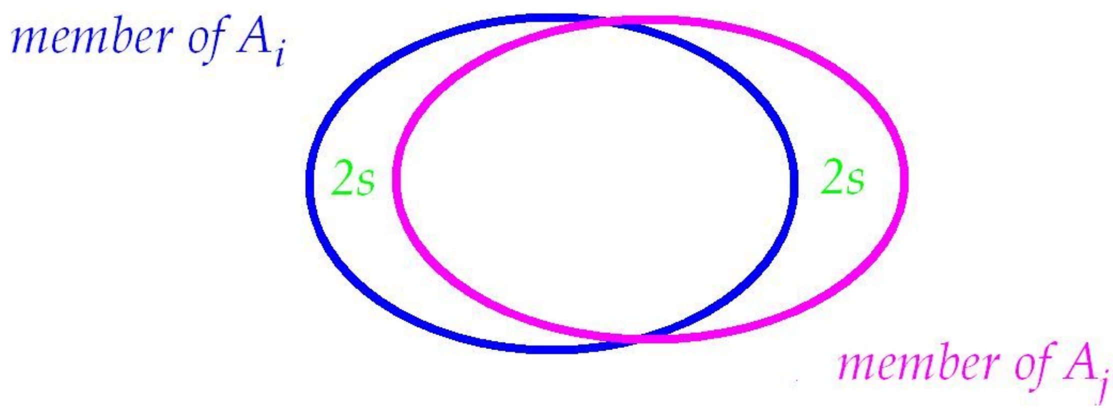
$n(\mathcal{A}_i, 2s) \cap n(A_j, 2s) = \emptyset$ iff $d(\mathcal{A}_i, \mathcal{A}_j) \geq 4s + 2$.

Illustration:

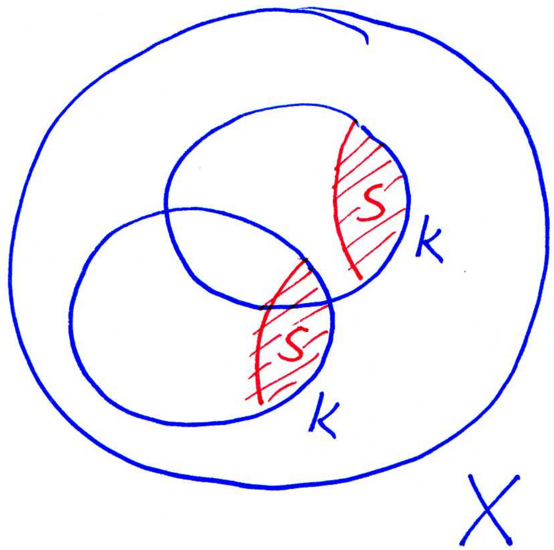


In other words, deleting $2s$ elements from a member of $\mathcal{A}_i$ and deleting $2s$ elements from a member of $\mathcal{A}_j$, two different $k-2s$-element sets are obtained.

This is **forbidden**:



Definition. The s-shadow $\sigma_s(\mathcal{A})$ of $\mathcal{A}$ is the family of all $k - s$-element sets obtained from the members of $\mathcal{A}$ by deleting s elements.



$$\sigma_s(\mathcal{A}) = \{B : \ |B| = k - s, B \subset A \in \mathcal{A}\}$$

- **error tolerance** $2s$

$$n(A_i, 2s) \cap n(A_j, 2s) = \emptyset \ (1 \leq i < j \leq 2^n),$$

or

$$\sigma_{2s}(\mathcal{A}_i) \cap \sigma_{2s}(\mathcal{A}_j) = \emptyset$$

- **waste rate** $\alpha\ (> 0)$

$$\mu\left(\cup_{i=1}^{n}\mathcal{A}_i\right) = \frac{\sum_{i=1}^{n}|\mathcal{A}_i|}{\binom{N}{k}} \geq \alpha,$$

Given the security ρ and the error tolerance $2s$, maximize α.

Combinatorial problem. Given N, maximize $\sum_{i=1}^{n}|\mathcal{A}_i|$ under the conditions

$$|\mathcal{A}_i| \leq \binom{x}{k}$$

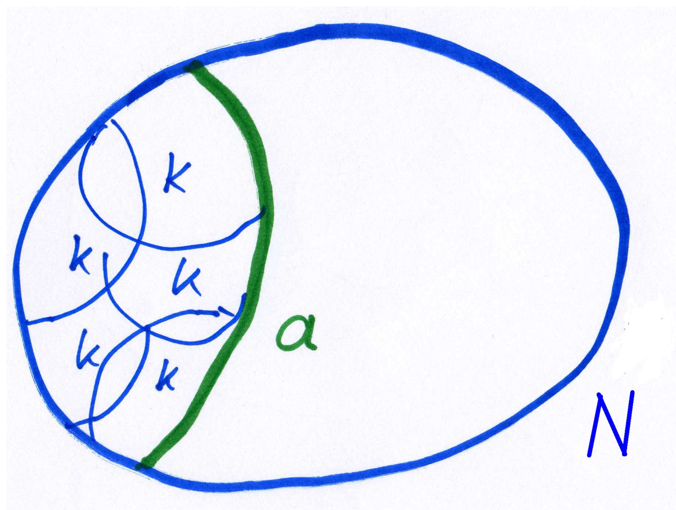
and

$$\sigma_{2s}(\mathcal{A}_i) \cap \sigma_{2s}(\mathcal{A}_j) = \emptyset.$$

Shadow problem

Given N, k and $|\mathcal{F}|$, **minimize** $|\sigma(\mathcal{F})|$.

If lucky then $|\mathcal{F}| = \binom{a}{k}$ holds for an integer a then the best construction is



min$|\sigma(\mathcal{F})| = \binom{a}{k-1}$

Shadow problem

Lemma If $0 < k, m$ are integers then one can find integers $a_k > a_{k-1} > \ldots > a_t \geq t \geq 1$ such that

$$m = \binom{a_k}{k} + \binom{a_{k-1}}{k-1} + \ldots + \binom{a_t}{t}$$

and they are unique.

This is called the **canonical form** of m.

Shadow problem

Shadow Theorem (Kruskal-K) If N, k and $|\mathcal{F}|$ are given,

the canonical form of $|\mathcal{F}|$ is

$$|\mathcal{F}| = \binom{a_k}{k} + \binom{a_{k-1}}{k-1} + \ldots + \binom{a_t}{t}$$

then

$$\min |\sigma(\mathcal{F})| = \binom{a_k}{k-1} + \binom{a_{k-1}}{k-2} + \ldots + \binom{a_t}{t-1}.$$

another formulation

characteristic vector of the set $A \subset [N]$

(0,	0,	1,	1,	0,	...	1,	...,	0)
1	2	3	4	5	...	k	...	n

the kth coordinate is 1 iff $k \in A$

another formulation

The previous construction with $k = 3, a = 5$, that is $|\mathcal{F}| = \binom{5}{3} = 10$

(1,	1,	1,	0,	0,	0,	0,	...	)
(1,	1,	0,	1,	0,	0,	0,	...	)
(1,	0,	1,	1,	0,	0,	0,	...	)
(0,	1,	1,	1,	0,	0,	0,	...	)
(1,	1,	0,	0,	1,	0,	0,	...	)
(1,	0,	1,	0,	1,	0,	0,	...	)
(0,	1,	1,	0,	1,	0,	0,	...	)
(1,	0,	0,	1,	1,	0,	0,	...	)
(0,	1,	0,	1,	1,	0,	0,	...	)
(0,	0,	1,	1,	1,	0,	0,	...	)
1	2	3	4	5	6	7	...	

$$
\begin{array}{l}
(1, \quad 1, \quad 1, \quad 0, \quad 0, \quad 0, \quad 0, \quad \ldots \quad) \\
(1, \quad 1, \quad 0, \quad 1, \quad 0, \quad 0, \quad 0, \quad \ldots \quad) \\
(1, \quad 0, \quad 1, \quad 1, \quad 0, \quad 0, \quad 0, \quad \ldots \quad) \\
(0, \quad 1, \quad 1, \quad 1, \quad 0, \quad 0, \quad 0, \quad \ldots \quad) \\
(1, \quad 1, \quad 0, \quad 0, \quad 1, \quad 0, \quad 0, \quad \ldots \quad) \\
(1, \quad 0, \quad 1, \quad 0, \quad 1, \quad 0, \quad 0, \quad \ldots \quad) \\
(0, \quad 1, \quad 1, \quad 0, \quad 1, \quad 0, \quad 0, \quad \ldots \quad) \\
(1, \quad 0, \quad 0, \quad 1, \quad 1, \quad 0, \quad 0, \quad \ldots \quad) \\
(0, \quad 1, \quad 0, \quad 1, \quad 1, \quad 0, \quad 0, \quad \ldots \quad) \\
(0, \quad 0, \quad 1, \quad 1, \quad 1, \quad 0, \quad 0, \quad \ldots \quad)
\end{array}
$$

(1,	1,	1,	0,	0,	0,	0,	. . .	)
(1,	1,	0,	1,	0,	0,	0,	. . .	)
(1,	0,	1,	1,	0,	0,	0,	. . .	)
(0,	1,	1,	1,	0,	0,	0,	. . .	)
(1,	1,	0,	0,	1,	0,	0,	. . .	)
(1,	0,	1,	0,	1,	0,	0,	. . .	)
(0,	1,	1,	0,	1,	0,	0,	. . .	)
(1,	0,	0,	1,	1,	0,	0,	. . .	)
(0,	1,	0,	1,	1,	0,	0,	. . .	)
(0,	0,	1,	1,	1,	0,	0,	. . .	)
(?					1,			)

$$
\begin{array}{llllllllc}
(1, & 1, & 1, & 0, & 0, & 0, & 0, & \ldots &) \\
(1, & 1, & 0, & 1, & 0, & 0, & 0, & \ldots &) \\
(1, & 0, & 1, & 1, & 0, & 0, & 0, & \ldots &) \\
(0, & 1, & 1, & 1, & 0, & 0, & 0, & \ldots &) \\
(1, & 1, & 0, & 0, & 1, & 0, & 0, & \ldots &) \\
(1, & 0, & 1, & 0, & 1, & 0, & 0, & \ldots &) \\
(0, & 1, & 1, & 0, & 1, & 0, & 0, & \ldots &) \\
(1, & 0, & 0, & 1, & 1, & 0, & 0, & \ldots &) \\
(0, & 1, & 0, & 1, & 1, & 0, & 0, & \ldots &) \\
(0, & 0, & 1, & 1, & 1, & 0, & 0, & \ldots &) \\
(1, & 1, & 0, & 0, & 0, & 1, & & &)
\end{array}
$$

(1, 1, 1, 0, 0, 0, 0, . . .)

(1, 1, 0, 1, 0, 0, 0, . . .)

(1, 0, 1, 1, 0, 0, 0, . . .)

(0, 1, 1, 1, 0, 0, 0, . . .)

(1, 1, 0, 0, 1, 0, 0, . . .)

(1, 0, 1, 0, 1, 0, 0, . . .)

(0, 1, 1, 0, 1, 0, 0, . . .)

(1, 0, 0, 1, 1, 0, 0, . . .)

(0, 1, 0, 1, 1, 0, 0, . . .)

(0, 0, 1, 1, 1, 0, 0, . . .)

(1, 1, 0, 0, 0, 1,)

(1, 0, 1, 0, 0, 1,)

$$
\begin{array}{lllllllll}
(1, & 1, & 1, & 0, & 0, & 0, & 0, & \ldots &) \\
(1, & 1, & 0, & 1, & 0, & 0, & 0, & \ldots &) \\
(1, & 0, & 1, & 1, & 0, & 0, & 0, & \ldots &) \\
(0, & 1, & 1, & 1, & 0, & 0, & 0, & \ldots &) \\
(1, & 1, & 0, & 0, & 1, & 0, & 0, & \ldots &) \\
(1, & 0, & 1, & 0, & 1, & 0, & 0, & \ldots &) \\
(0, & 1, & 1, & 0, & 1, & 0, & 0, & \ldots &) \\
(1, & 0, & 0, & 1, & 1, & 0, & 0, & \ldots &) \\
(0, & 1, & 0, & 1, & 1, & 0, & 0, & \ldots &) \\
(0, & 0, & 1, & 1, & 1, & 0, & 0, & \ldots &) \\
(1, & 1, & 0, & 0, & 0, & 1, & & &) \\
(1, & 0, & 1, & 0, & 0, & 1, & & &) \\
(0, & 1, & 1, & 0, & 0, & 1, & & &)
\end{array}
$$

(1, 1, 1, 0, 0, 0, 0, . . .)
(1, 1, 0, 1, 0, 0, 0, . . .)
(1, 0, 1, 1, 0, 0, 0, . . .)
(0, 1, 1, 1, 0, 0, 0, . . .)
(1, 1, 0, 0, 1, 0, 0, . . .)
(1, 0, 1, 0, 1, 0, 0, . . .)
(0, 1, 1, 0, 1, 0, 0, . . .)
(1, 0, 0, 1, 1, 0, 0, . . .)
(0, 1, 0, 1, 1, 0, 0, . . .)
(0, 0, 1, 1, 1, 0, 0, . . .)
(1, 1, 0, 0, 0, 1,)
(1, 0, 1, 0, 0, 1,)
(0, 1, 1, 0, 0, 1,)
(1, 0, 0, 1, 0, 1,)

(1, 1, 1, 0, 0, 0, 0, . . .)
(1, 1, 0, 1, 0, 0, 0, . . .)
(1, 0, 1, 1, 0, 0, 0, . . .)
(0, 1, 1, 1, 0, 0, 0, . . .)
(1, 1, 0, 0, 1, 0, 0, . . .)
(1, 0, 1, 0, 1, 0, 0, . . .)
(0, 1, 1, 0, 1, 0, 0, . . .)
(1, 0, 0, 1, 1, 0, 0, . . .)
(0, 1, 0, 1, 1, 0, 0, . . .)
(0, 0, 1, 1, 1, 0, 0, . . .)
(1, 1, 0, 0, 0, 1,)
(1, 0, 1, 0, 0, 1,)
(0, 1, 1, 0, 0, 1,)
(1, 0, 0, 1, 0, 1,)
(0, 1, 0, 1, 0, 1,)

another formulation

Arabically lexicographical ordering

Version of the **Shadow Theorem**

If N, k and$|\mathcal{F}|$ are given, then

$|\sigma(\mathcal{F})|$ is minimum for

the lexicographically first $|\mathcal{F}|$ subsets containing k elements.

s-shadow

Shadow Theorem **(Kruskal-K)** If N, k and $|\mathcal{F}|$ are given,

the canonical form of $|\mathcal{F}|$ is

$$|\mathcal{F}| = \binom{a_k}{k} + \binom{a_{k-1}}{k-1} + \ldots + \binom{a_t}{t}$$

then

$$\min |\sigma_s(\mathcal{F})| = \binom{a_k}{k-s} + \binom{a_{k-s}}{k-1-s} + \ldots + \binom{a_t}{t-s}.$$

Only an estimate

If x is a real number, $\binom{x}{k} = \frac{x(x-1)\ldots(x-k+1)}{k!}$.

Theorem. (Lovász' version of the Shadow theorem) If $\mathcal{A}$ is a family of k-element sets,

$$|\mathcal{A}| = \binom{x}{k}$$

then

$$|\sigma_s(\mathcal{A})| \geq \binom{x}{k-s}.$$

Theorem. If $\mathcal{A}_i$ are families of k-element subsets of an N-element set,

$$|\mathcal{A}_i| \le \binom{x}{k} \ (1 \le i \le n)$$

and

$$\sigma_{2s}(\mathcal{A}_i) \cap \sigma_{2s}(\mathcal{A}_j) = \emptyset \ (1 \le i < j \le n)$$

hold, then

$$\frac{\sum_{i=1}^{n} |\mathcal{A}_i|}{\binom{N}{k}} \le \left(\frac{x}{N}\right)^{2s}.$$

Unfortunately this is **not sharp**.

A very special case, modified

$k = 3, s = 1, n = 2$

$\mathcal{A}, \mathcal{B}$ are families of 3-element subsets of an N-element set.

If $A \in \mathcal{A}, B \in \mathcal{B}$ then $|A \cap B| \leq 1$.

$|\mathcal{A}| = |\mathcal{B}|$

Find $\max |\mathcal{A}|$.

A weak estimate from Shadow Theorem

Choose x in this way: $|\mathcal{A}| = |\mathcal{B}| = \binom{x}{3}$

By the Shadow Theorem: $\binom{x}{2} \leq |\sigma(\mathcal{A})|, |\sigma(\mathcal{B})|$

$$2\binom{x}{2} \leq |\sigma(\mathcal{A})| + |\sigma(\mathcal{B})| \leq \binom{N}{2}$$

From here, asymptotically

$$|\mathcal{A}| = \binom{x}{3} \leq \frac{1}{2\sqrt{2}}\binom{N}{3}(1 + o(1))$$

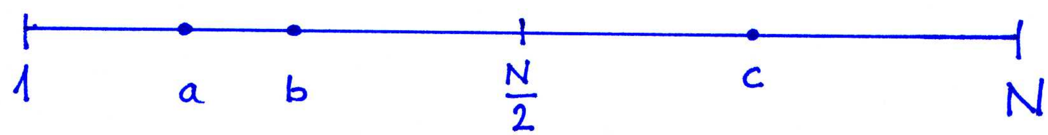
Trivial construction gives:

$$|\mathcal{A}| = \frac{N^3}{48}(1 + o(1)).$$

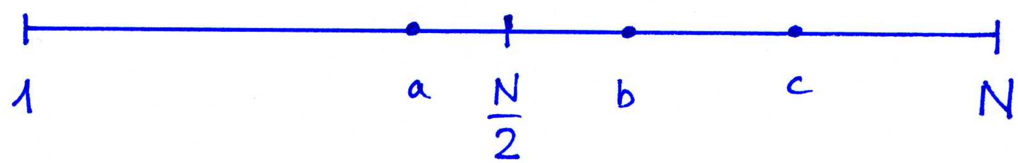
$$\mathcal{A} = \left\{(a, b, c) : a < b < c \leq \frac{N}{2}\right\}, \mathcal{B} = \left\{(a, b, c) : \frac{N}{2} \leq a < b < c\right\}.$$

A better construction: $|\mathcal{A}| = \frac{N^3}{24}(1 + o(1))$.

$$\mathcal{A} = \left\{(a, b, c) : \frac{b+c}{2} \leq \frac{N}{2}\right\}$$



$$\left\{B = \{(a, b, c) : \frac{N}{2} < \frac{a+b}{2}\right\}.$$



Theorem (Frankl-Kato-Katona-Tokushige, 2012+)

$$\max |\mathcal{A}| = \kappa \binom{N}{3} (1 + o(1))$$

where κ is the unique real root in the (0,1)-interval of the equation

$$z^3 = (1 - z)^3 + 3z(1 - z)^2.$$

Theorem (Frankl-Kato-Katona-Tokushige, 2012+)

If $\mathcal{A} \subset \binom{[N]}{k}$ then

$$\max |\mathcal{A}| = \mu_k \binom{N}{k} (1 + o(1))$$

where μ_k is the unique real root in the (0,1)-interval of the equation

$$z^k = (1-z)^k + kz(1-z)^{k-1}.$$

Badly needed generalizations

s-shadows rather than $s = 1$.

Badly needed generalizations

s-shadows rather than $s = 1$.

More families rather than only $n = 2$.

Badly needed generalizations

s-shadows rather than $s = 1$.

More families rather than only $n = 2$.

Combining this distance with the **geometric distance**.

Thanks

Köszönöm

Grazie


تشکر میکنم


谢谢