Hard Instances of the Constrained Discrete Logarithm Problem

Ilya Mironov	Microsoft Research
Anton Mityagin	UCSD
Kobbi Nissim	Ben Gurion University

Speaker: Ramarathnam Venkatesan
(Microsoft Research)

DLP

Discrete Logarithm Problem:

Given g^x find x

Believed to be hard in some groups:

- $\mathbb{Z}_p{}^*$
- elliptic curves

Hardness of DLP

Hardness of the DLP:

- specialized algorithms (index-calculus)

  complexity: depends on the algorithm

- generic algorithms (rho, lambda, baby-step giant-step…)

  complexity: $\sqrt{p}$ if group has order p

Constrained DLP

Constrained Discrete Logarithm Problem:

Given g^x find x, when $x \in S$

Example: S consists of exponents with short addition chains.

Hardness of the Constrained DLP

Bad sets (DLP is relatively easy):

x with low Hamming weight

$x \in [a, b]$

$\{x^2 \mid x < \sqrt{p}\}$

Good sets (DLP is hard) - ?

Generic Group Model [Nec94,Sho97]

Group G, random encoding $\sigma : G \to \Sigma$

Group operations oracle:

$$\sigma(g), \sigma(h), a, b \to \sigma(g^a h^b)$$

Formally, DLP:

given $\sigma(g)$ and $\sigma(g^x)$, find x

Assume order of g = p is prime

DLP is hard [Nec94,Sho97]

Suppose there is an algorithm that solves the DLP in the generic group model:

1. The algorithm makes n queries
   $\sigma(g), \sigma(g^x), \sigma(g^{a_1 x+b_1}), \sigma(g^{a_2 x+b_2}),\ldots, \sigma(g^{a_n x+b_n})$
2. The simulator answers randomly but consistently, treating x as a formal variable.
3. The algorithm outputs its guess y
4. The simulator chooses x at random.
5. The simulator loses if there is:
   - inconsistency: $g^{a_i x+b_i} = g^{a_j x+b_j}$ for some i, j;
   - $x = y$.

Pr < n^2/p

Pr = $1/p$

DLP is hard [Nec94,Sho97]

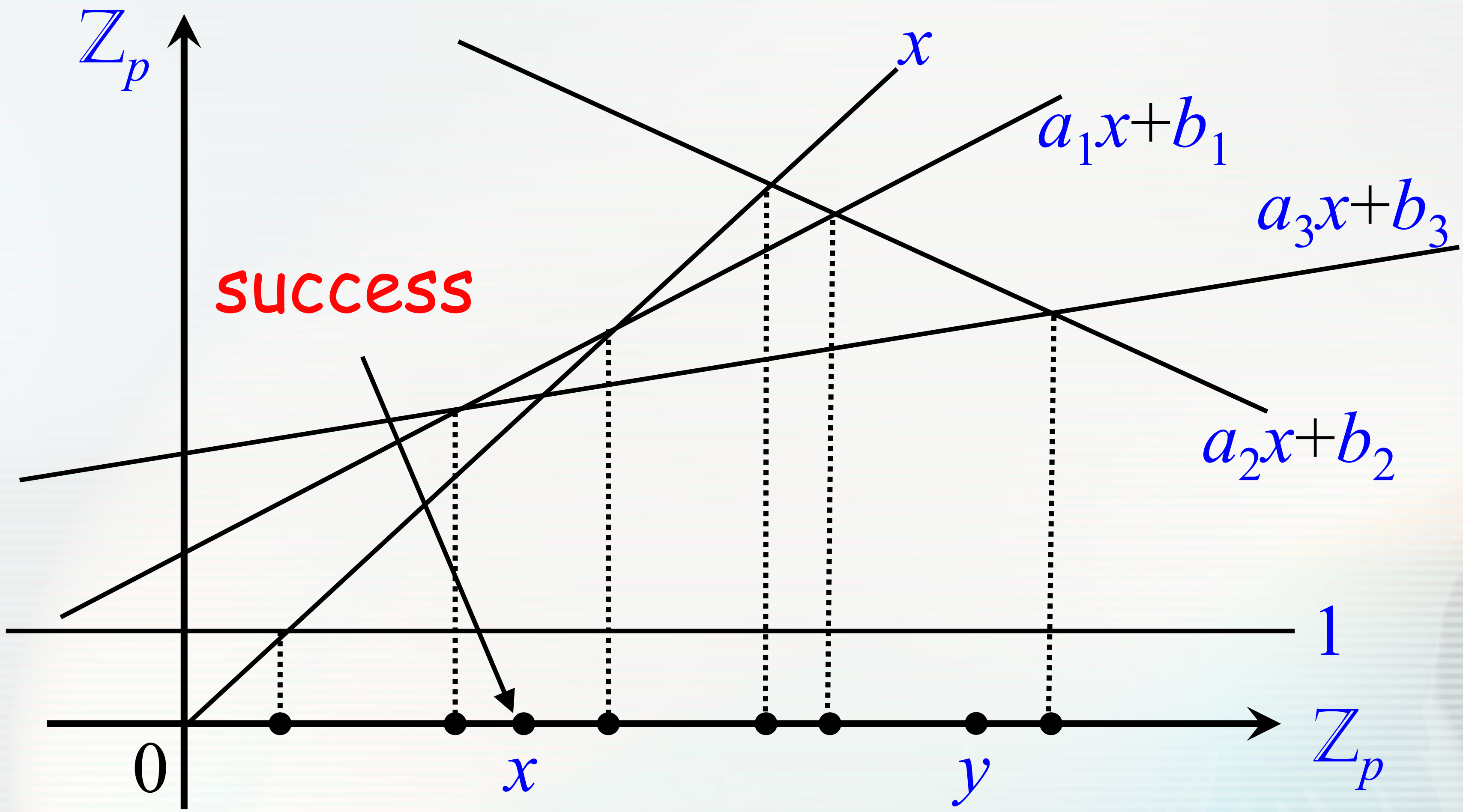
Probability of success of any algorithm for the DLP in the generic group model is at most:

$$n^2/p + 1/p,$$

where n is the number of group operations.

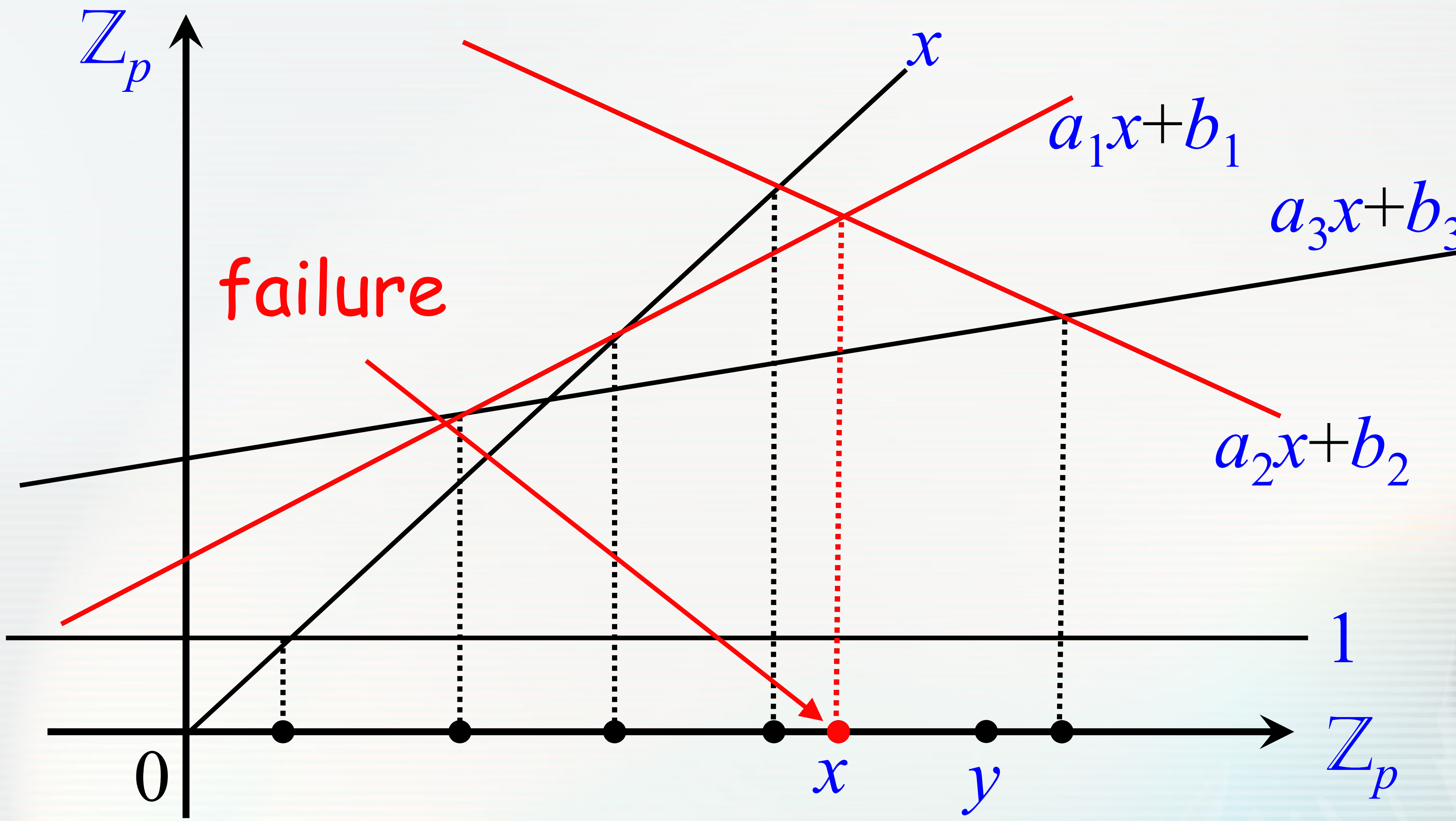
Graphical representation

Queries: $\sigma(g), \sigma(g^x), \sigma(g^{a_1x+b_1}), \sigma(g^{a_2x+b_2}), \ldots, \sigma(g^{a_nx+b_n})$



Graphical representation

Queries: $\sigma(g),\sigma(g^x),\sigma(g^{a_1x+b_1}),\sigma(g^{a_2x+b_2}),\ldots,\sigma(g^{a_nx+b_n})$



Attack

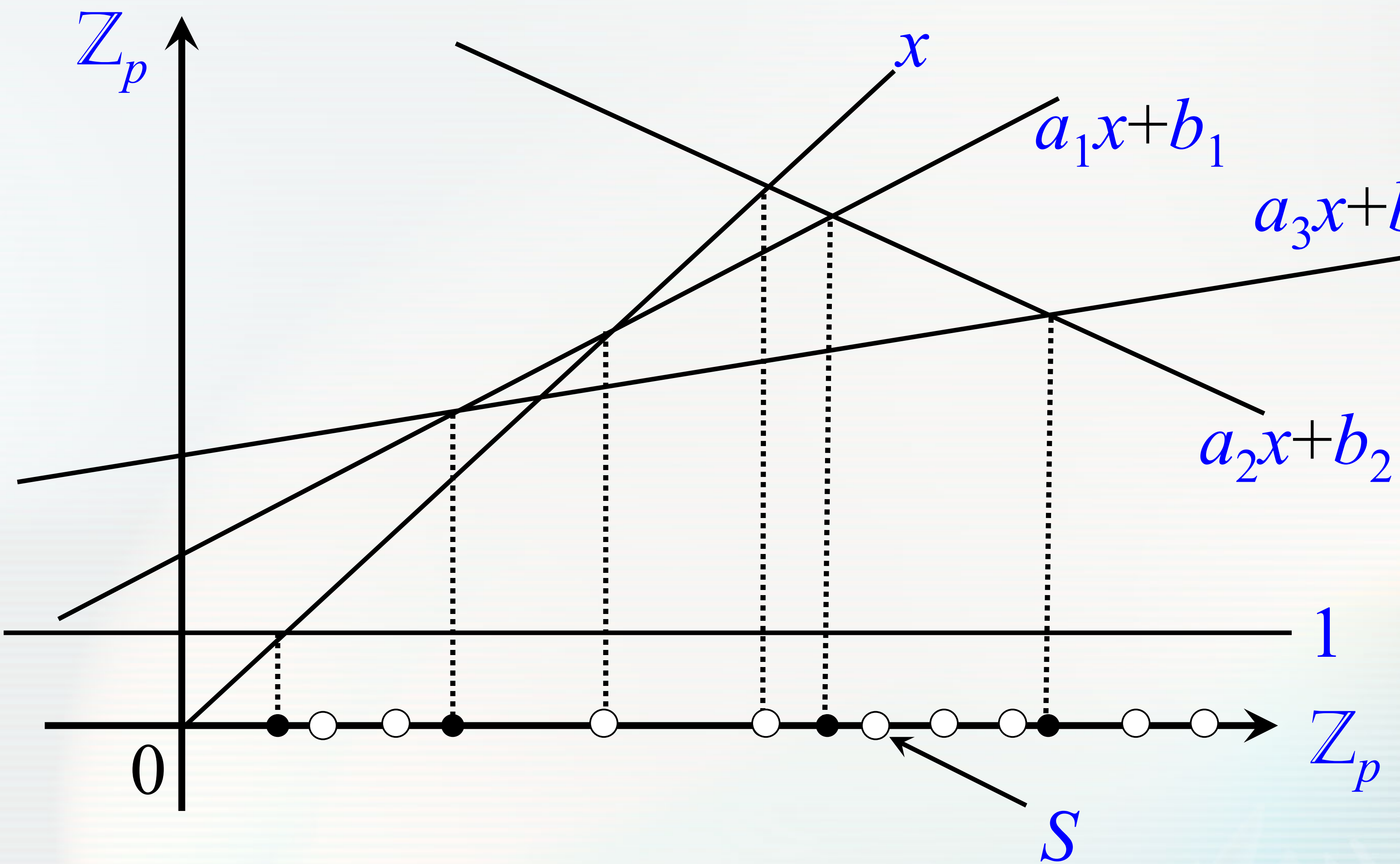
The argument is tight:

if for some $\sigma(g^{a_i x + b_i}) = \sigma(g^{a_j x + b_j})$,

computing x is easy

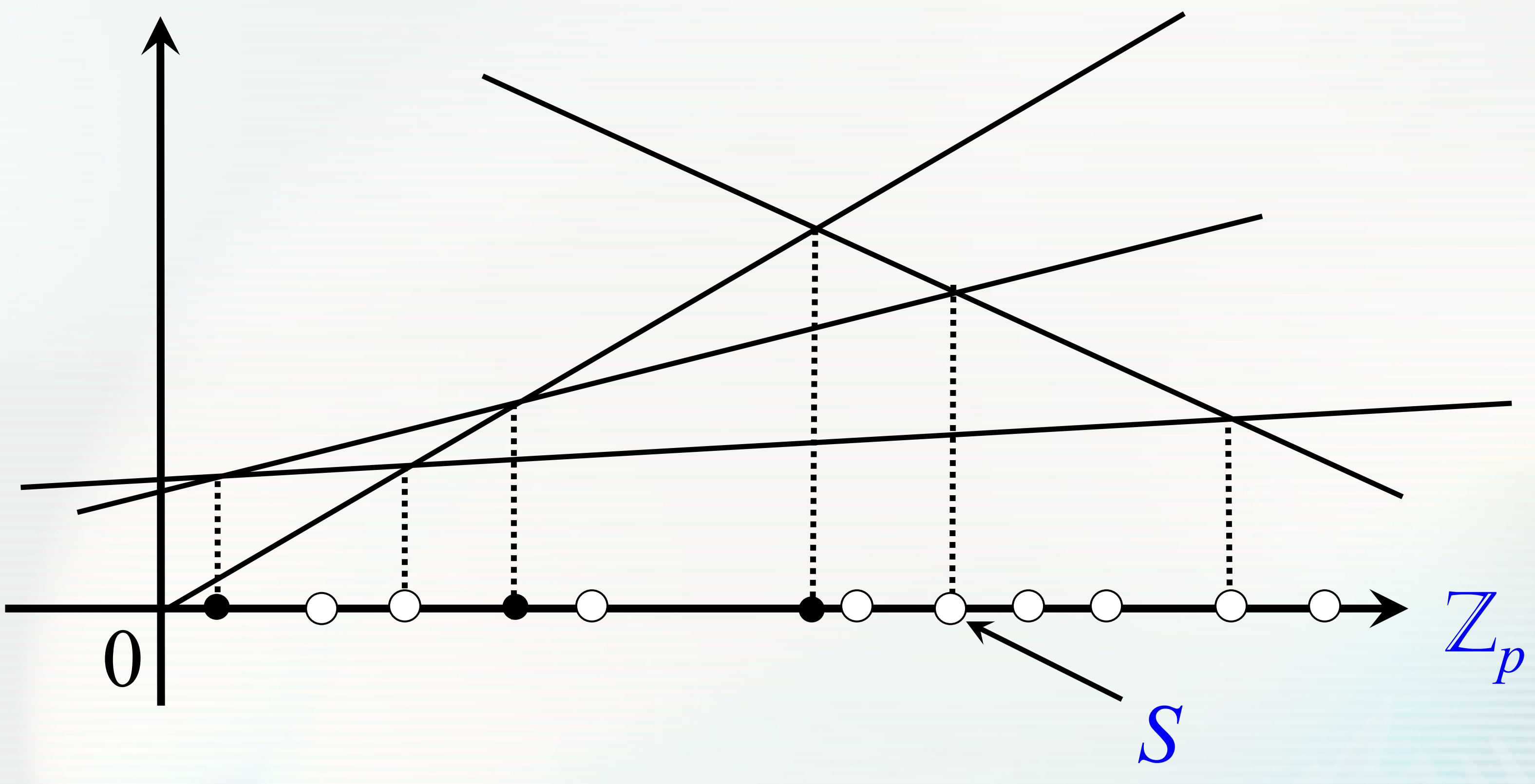
Constrained DLP

given $\sigma(g)$ and $\sigma(g^x)$, find $x \in S$



Generic complexity of S

$C_\alpha(S)$ = **generic α-complexity** of $S \subseteq \mathbb{Z}_p$ is the smallest number of lines such that their **intersection set** covers an α-fraction of S.



Bound

Adversary who is making at most n queries succeeds in solving

DLP: with probability at most

$$n^2/p + 1/p$$

DLP constrained to set S:

If $n < C_\alpha(S)$, probability is at most

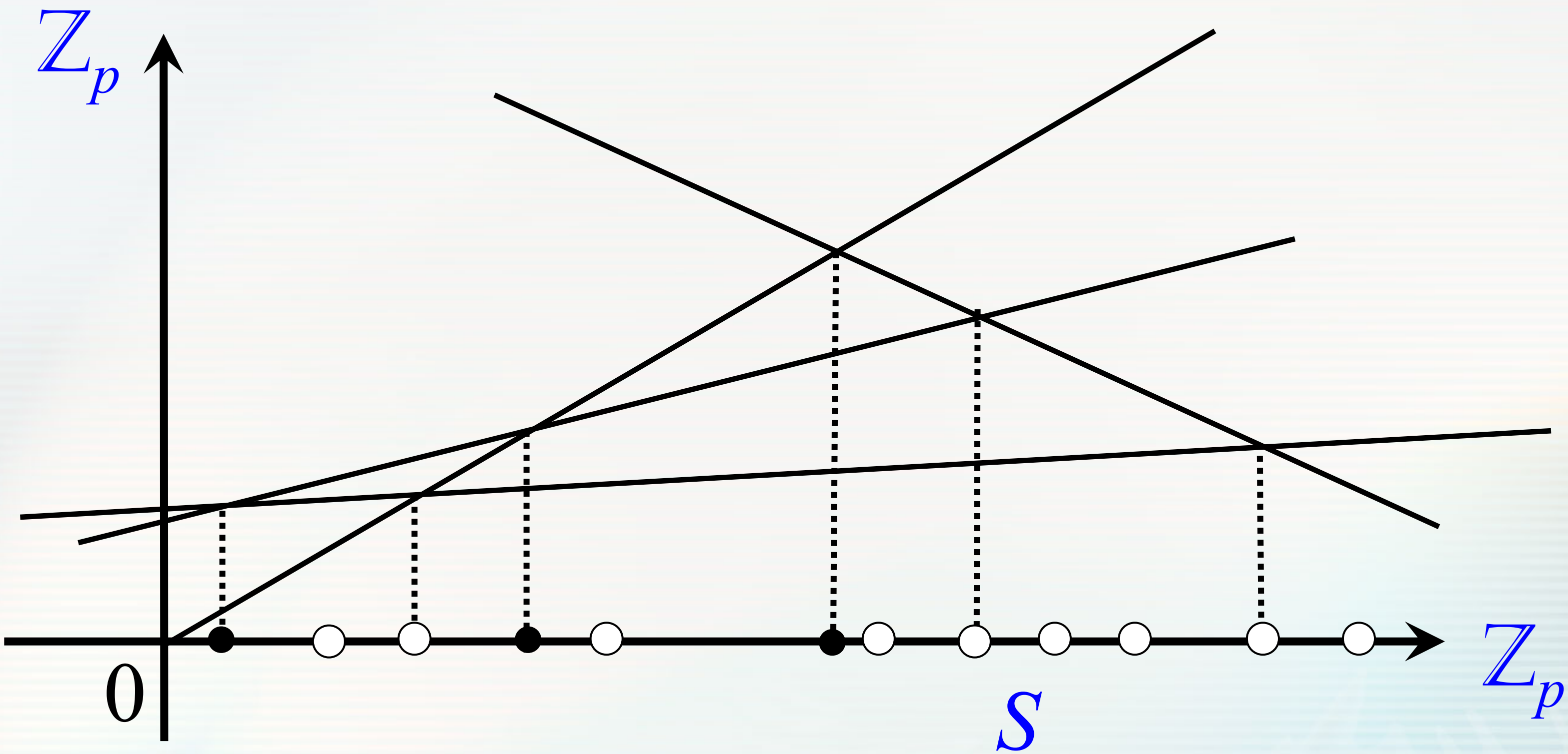
$$\alpha + 1/|S|$$

What's known about $C_\alpha(S)$?

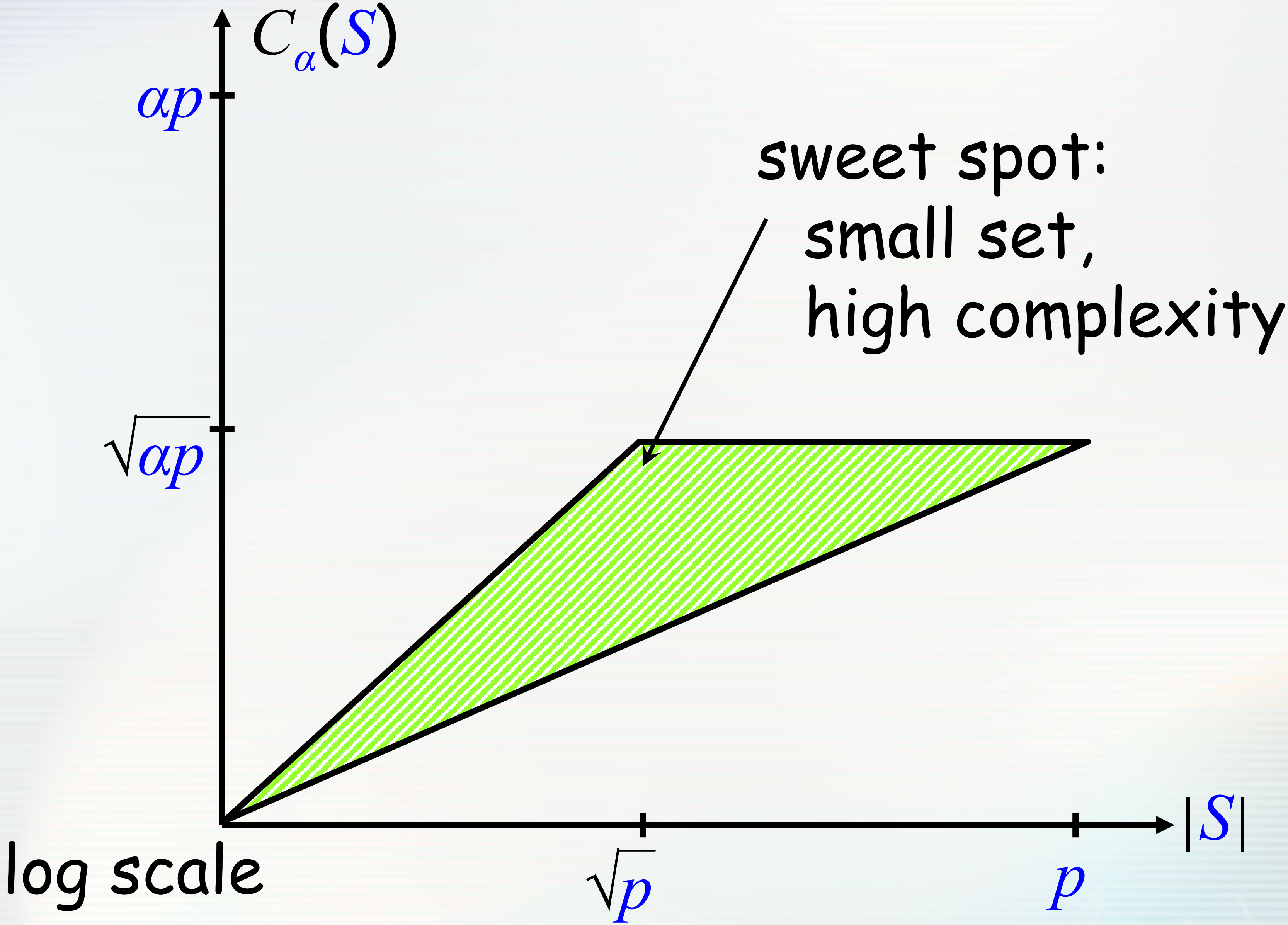
Obvious: $C_\alpha(S) < \sqrt{\alpha p}$ (omitting constants)

$C_\alpha(S) < \alpha|S|$

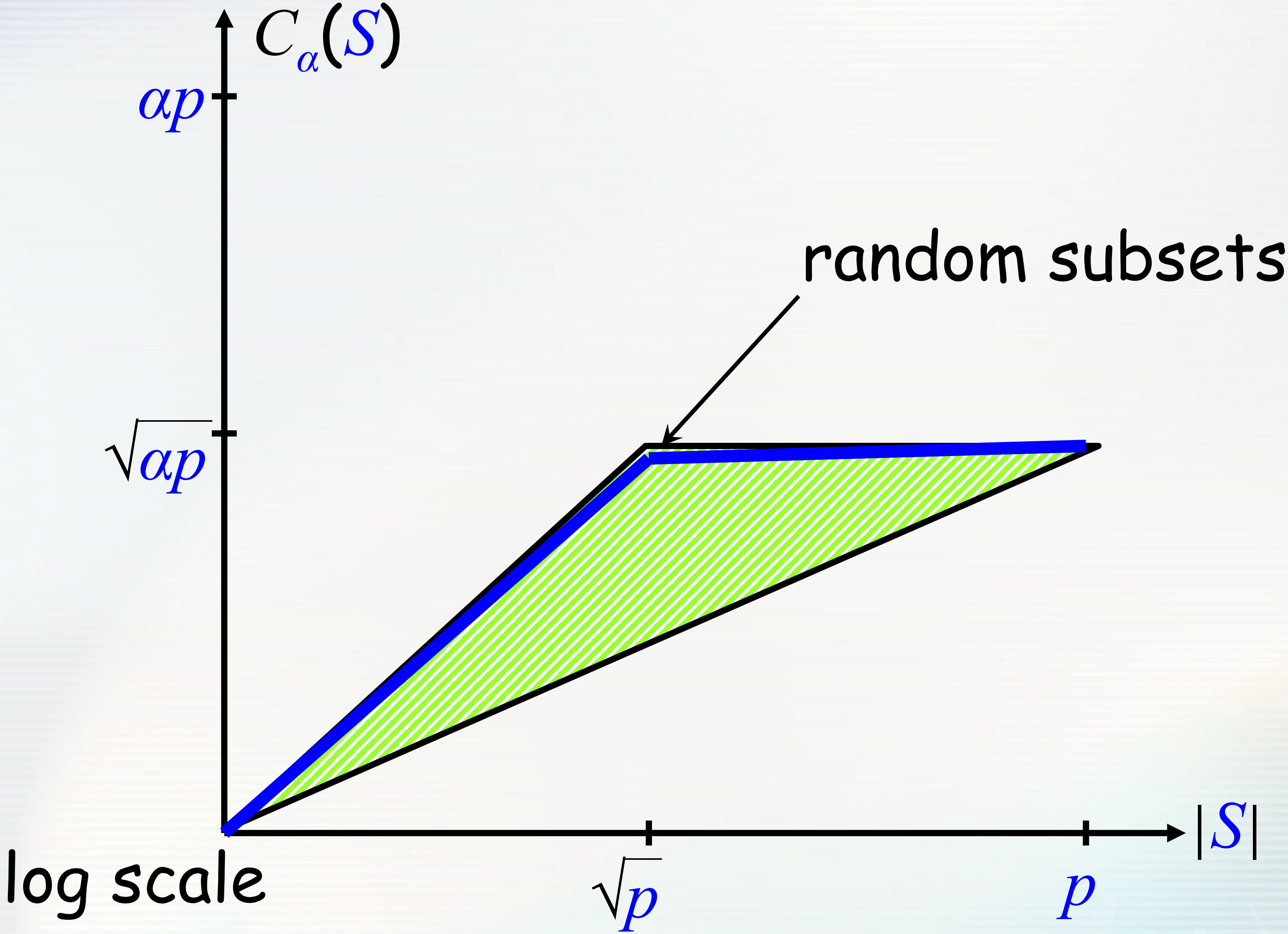
$C_\alpha(S) > \sqrt{\alpha|S|}$



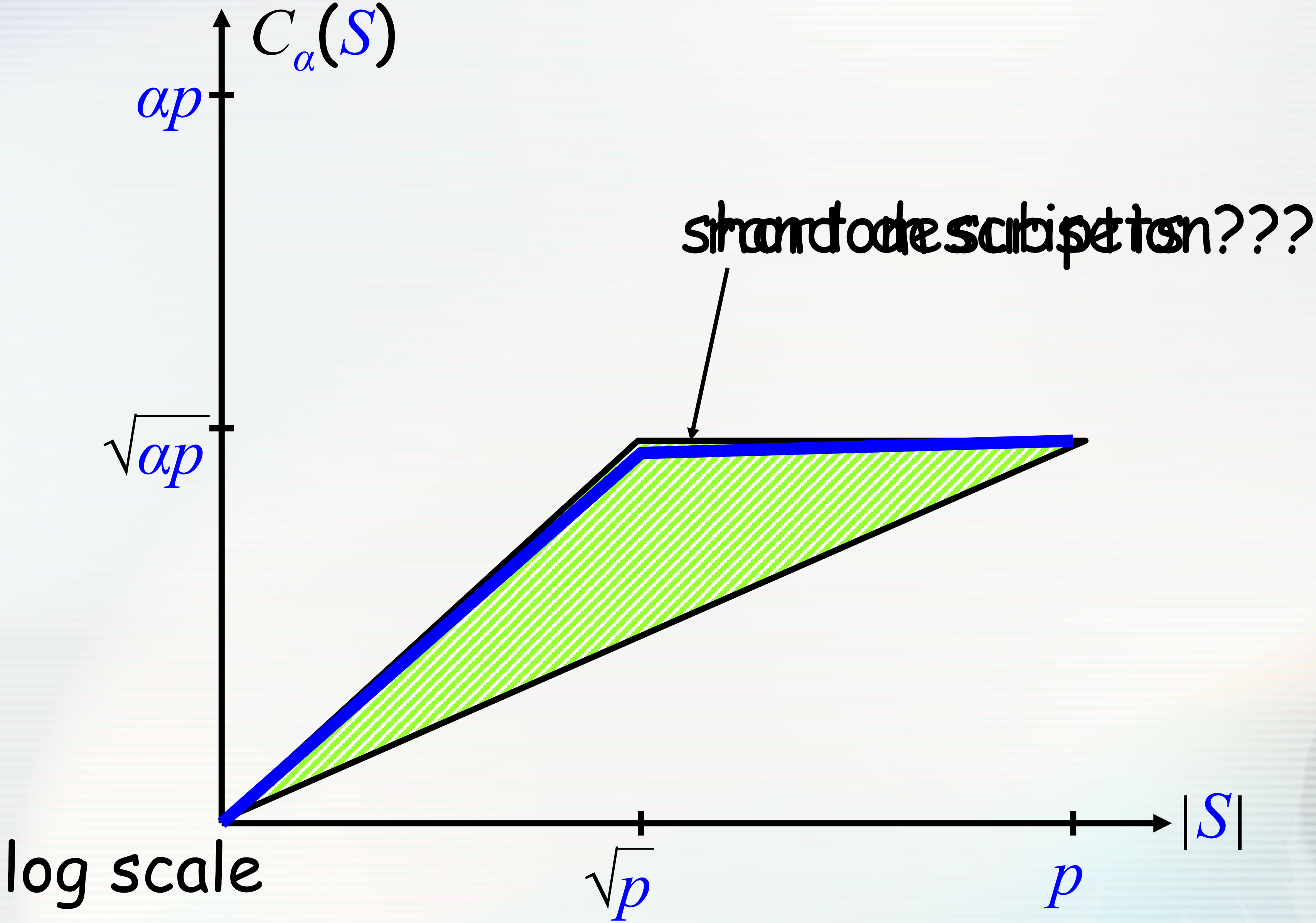
Simple bounds



Random subsets [Sch01]



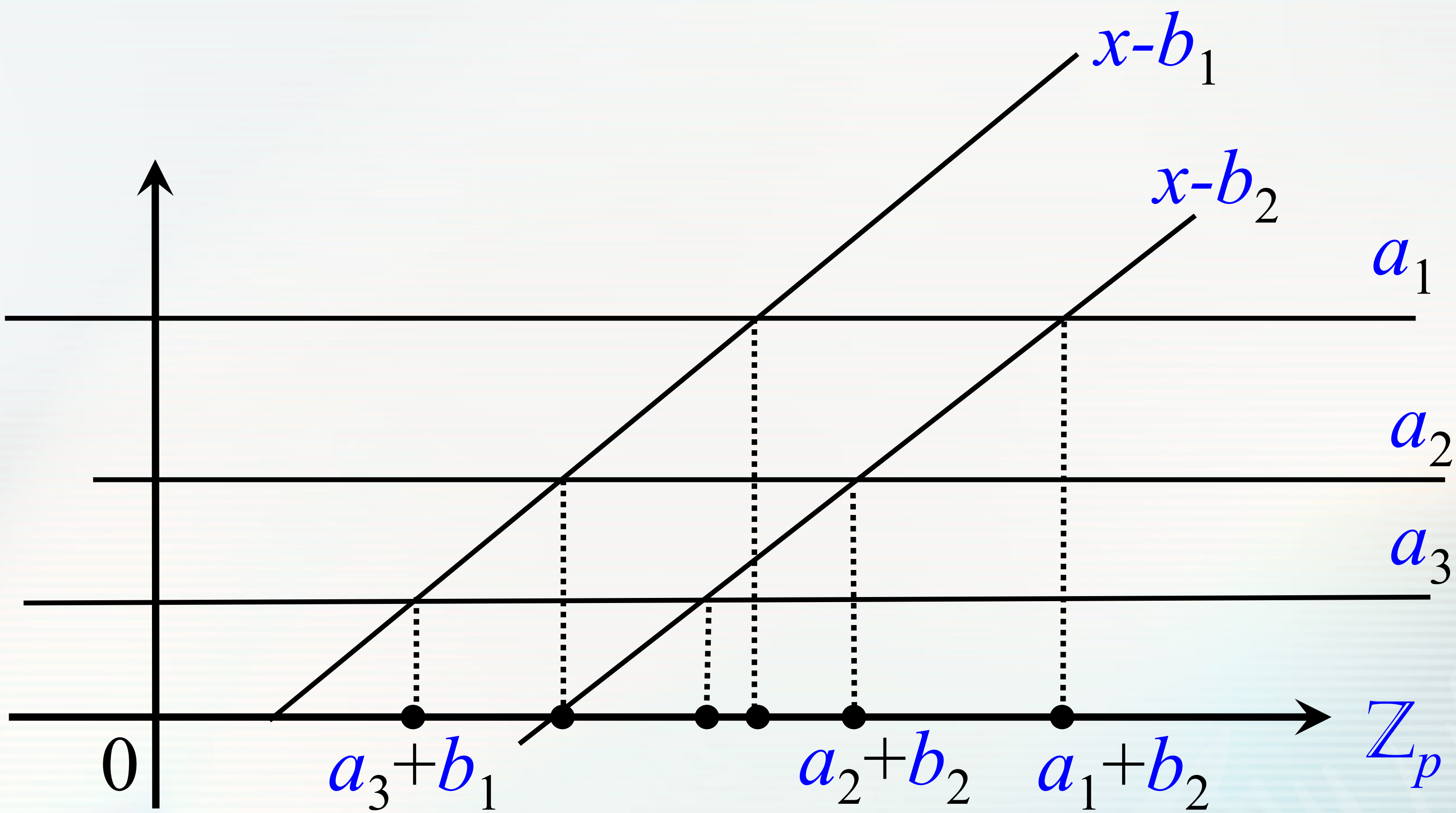
Problem



Relaxing the problem: C^{bsgs1}

$C^{\text{bsgs1}}(S)$ = baby-step-giant-step-1-complexity

Two lists: $g^{a_1}, g^{a_2}, \ldots, g^{a_n}$ and $g^{x\text{-}b_1}, g^{x\text{-}b_2}, \ldots, g^{x\text{-}b_n}$

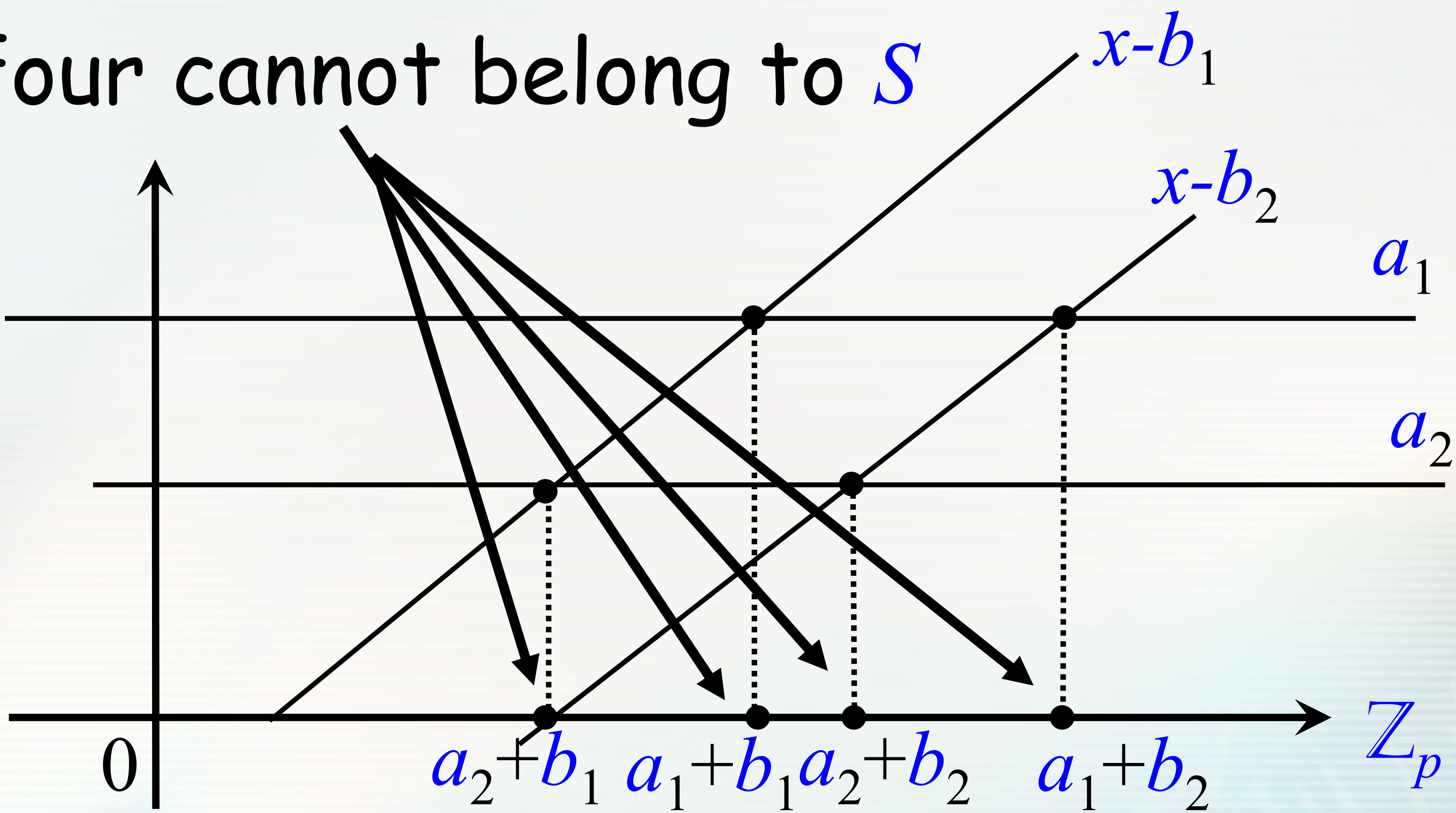


Modular weak Sidon set [EN77]

S is such that for any distinct $s_1, s_2, s_3, s_4 \in S$

$$s_1 + s_2 \neq s_3 + s_4 \pmod{p}$$

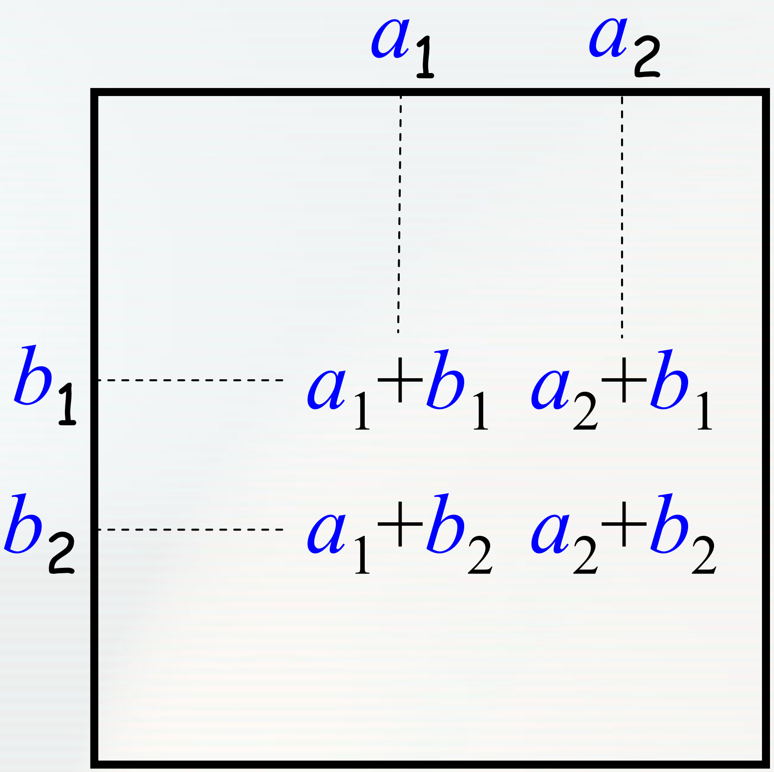
all four cannot belong to S



Zarankiewicz bound

S is such that for any distinct $s_1, s_2, s_3, s_4 \in S$

$$s_1 + s_2 \neq s_3 + s_4 \pmod{p}$$



How many elements of S can be in the table?

Zarankiewicz bound: at most $n^{3/2}$

$$C^{\text{bsgs1}}(S) > |S|^{2/3}$$

Weak modular Sidon sets

S is such that for any distinct $s_1, s_2, s_3, s_4 \in S$

$$s_1 + s_2 \neq s_3 + s_4 \pmod{p}$$

Explicit constructions for such sets exist of size $O(p^{1/2})$.

Higher order Sidon sets :

$$s_1 + s_2 + s_3 \neq s_4 + s_5 + s_6 \pmod{p}$$

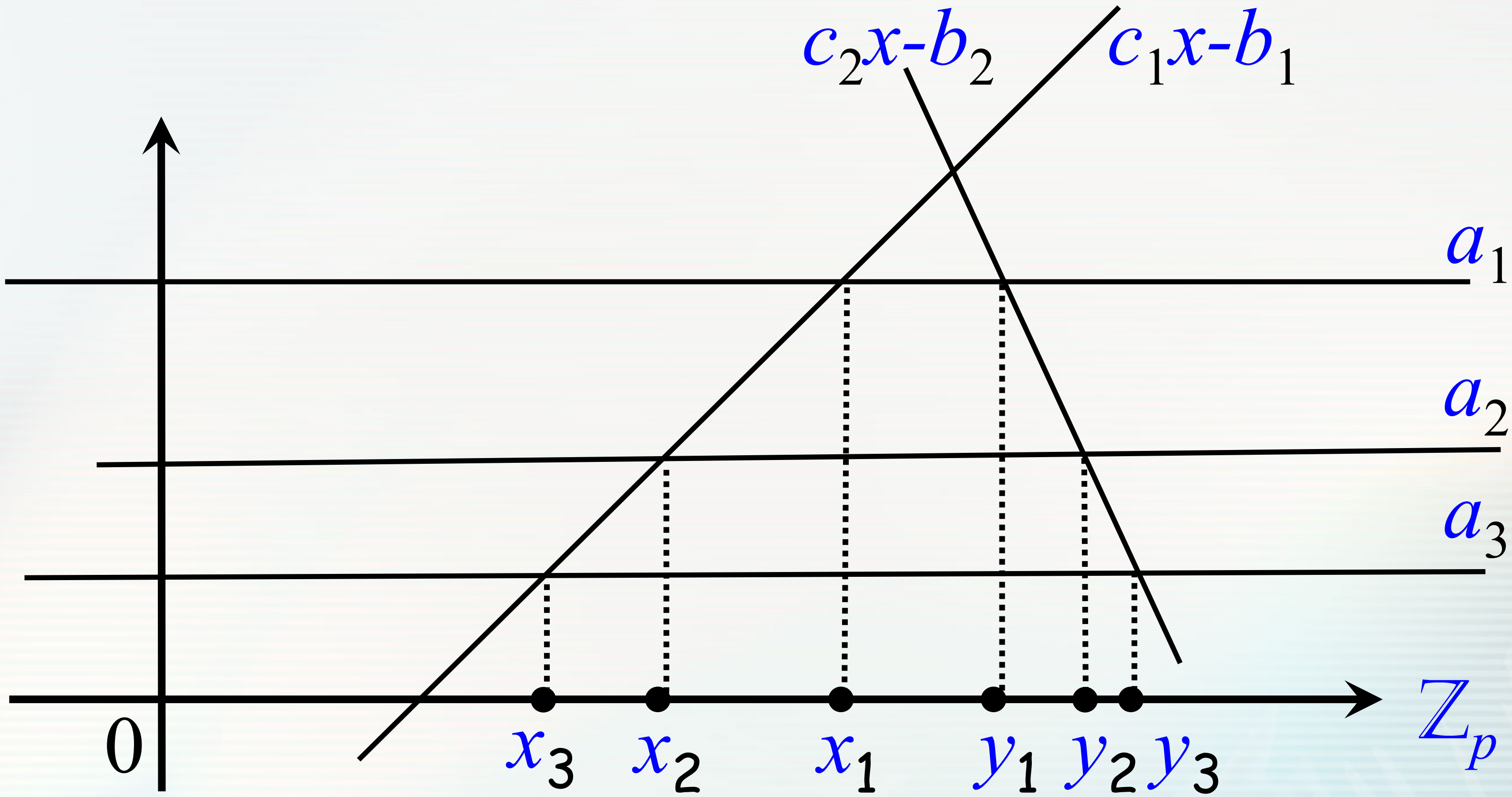
Turan-type bound:

$$C^{\text{bsgs1}}(S) < |S|^{3/4}$$

A harder problem: C^{bsgs}

$C^{\text{bsgs}}(S)$ = baby-step-giant-step-complexity

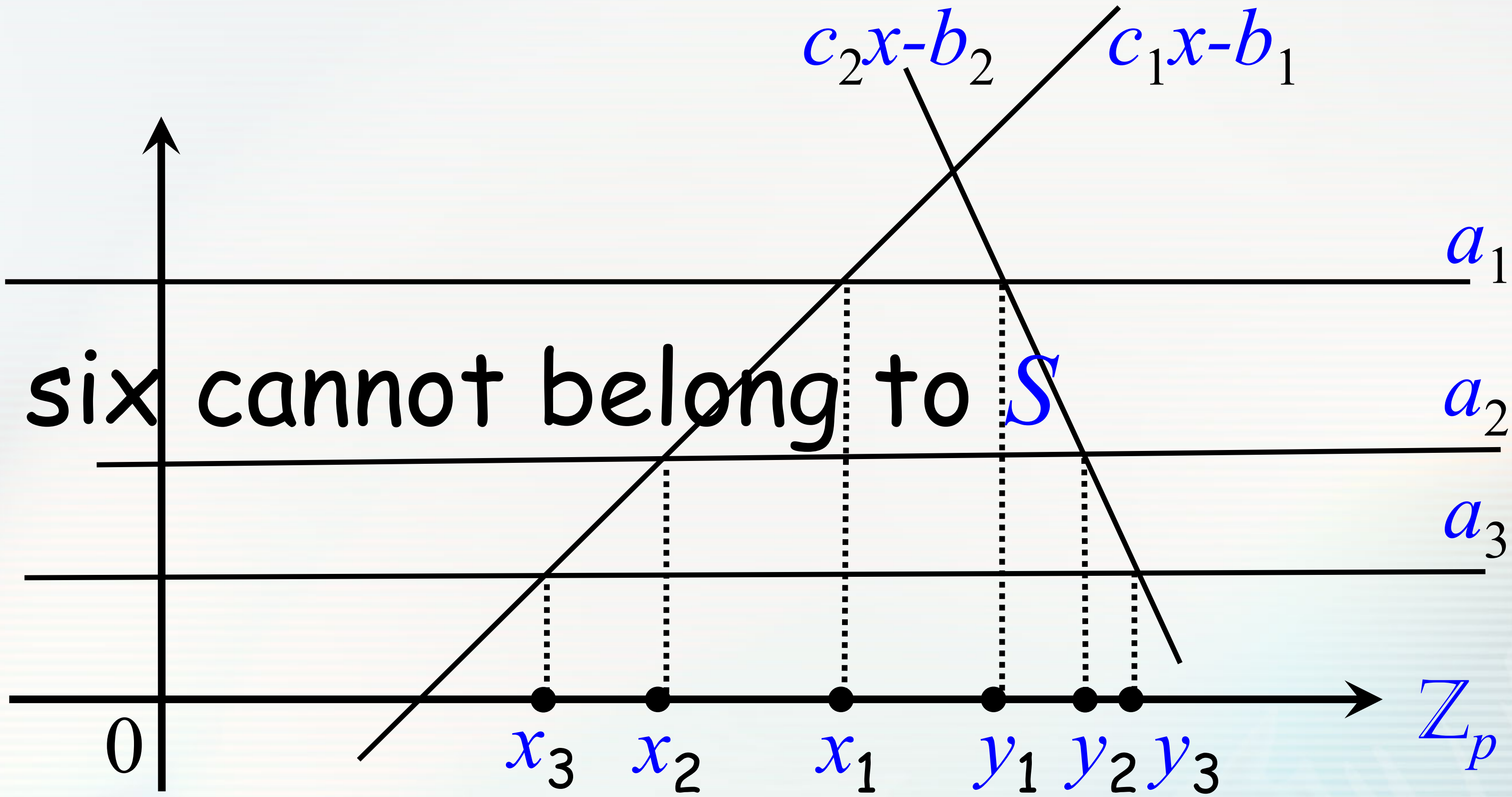
Two lists: $g^{a_1}, g^{a_2},\ldots, g^{a_n}$ and $g^{c_1x\text{-}b_1}, g^{c_2x\text{-}b_2},\ldots, g^{c_nx\text{-}b_n}$



Harder the problem: C^{bsgs}

S: for any six distinct $x_1, x_2, x_3, y_1, y_2, y_3 \in S$

$$(x_1 - x_2)/(x_2 - x_3) \neq (y_1 - y_2)/(y_2 - y_3) \pmod{p}$$

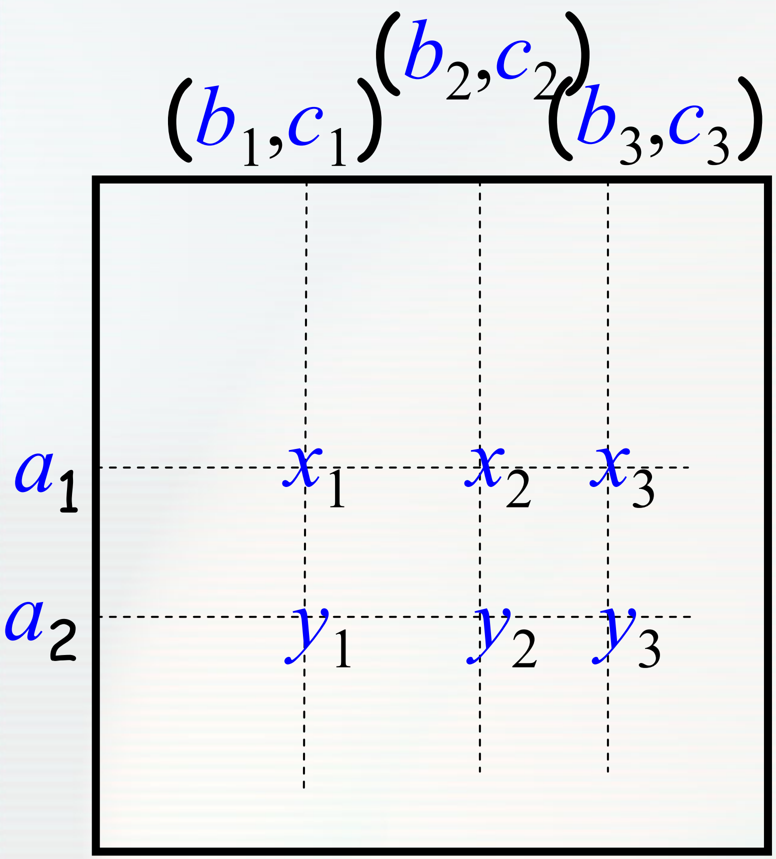


all six cannot belong to S

Zarankiewicz bound

S: for any six distinct $x_1, x_2, x_3, y_1, y_2, y_3 \in S$

$$(x_1 - x_2)/(x_2 - x_3) \neq (y_1 - y_2)/(y_2 - y_3) \pmod{p}$$



How many elements of S can be in the table?

Zarankiewicz bound: **still** at most $n^{3/2}$

$$C^{\text{bsgs}}(S) > |S|^{2/3}$$

How to construct?

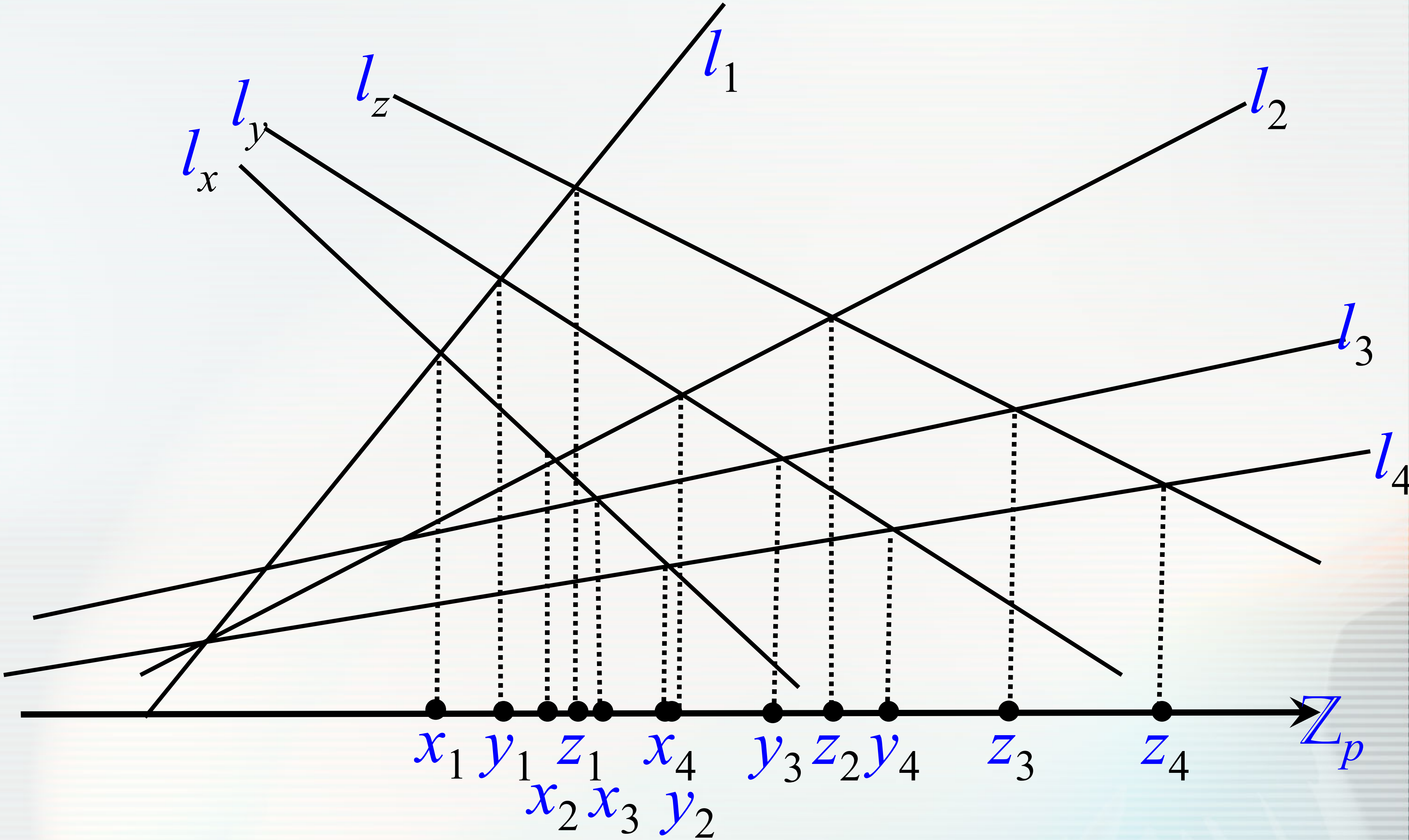
S: for any six distinct $x_1, x_2, x_3, y_1, y_2, y_3 \in S$

$$(x_1 - x_2)/(x_2 - x_3) \neq (y_1 - y_2)/(y_2 - y_3) \pmod{p}$$

"Six-wise independent set" of size $p^{1/6}$

Generic complexity

"Smallest" possible theorem involves 7 lines:



Bipartite Menelaus theorem

S: for any twelve distinct

$x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4, z_1, z_2, z_3, z_4 \in S$

$$\det \begin{vmatrix} x_1 - y_1 & x_1 - z_1 & z_1(x_1 - y_1) & y_1(x_1 - z_1) \\ x_2 - y_2 & x_2 - z_2 & z_2(x_2 - y_2) & y_2(x_2 - z_2) \\ x_3 - y_3 & x_3 - z_3 & z_3(x_3 - y_3) & y_3(x_3 - z_3) \\ x_4 - y_4 & x_4 - z_4 & z_4(x_4 - y_4) & y_4(x_4 - z_4) \end{vmatrix} \neq 0$$

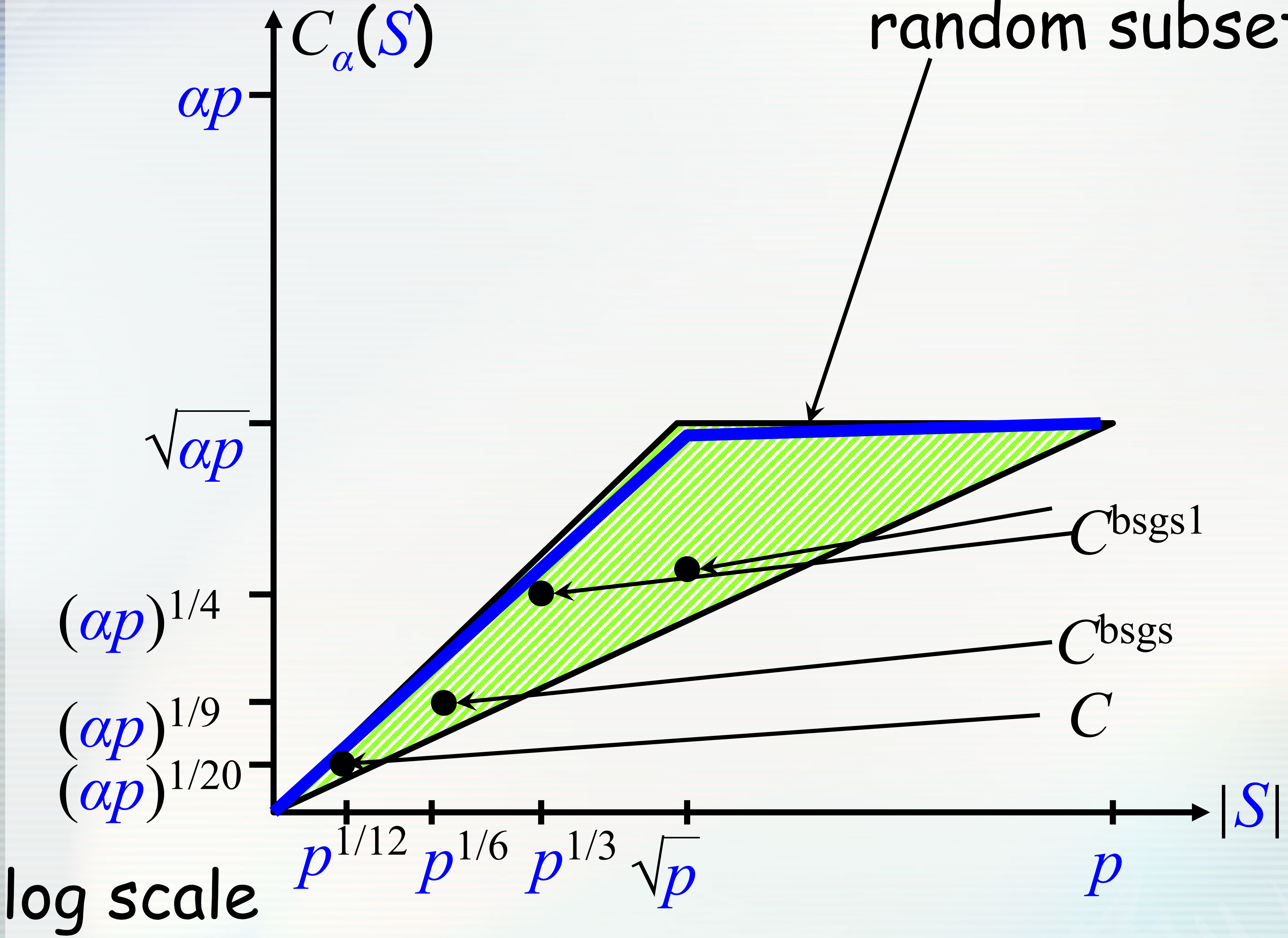
degree 6 polynomial

How to construct?

"12-wise independent set" of size $p^{1/12}$

$$C(S) > |S|^{3/5}$$

Conclusion



$C_\alpha(S)$
random subsets
αp
$\sqrt{\alpha p}$
$(\alpha p)^{1/4}$
$(\alpha p)^{1/9}$
$(\alpha p)^{1/20}$
C^{bsgs1}
C^{bsgs}
C
$|S|$
$p^{1/12}$
$p^{1/6}$
$p^{1/3}$
$\sqrt{p}$
p
log scale

Open problems

Better constructions:

- stronger bounds
- explicit

Constrained DLP for natural sets:

- short addition chains
- compressible binary representation
- three-way products xyz