Discrepancy Problems for Linear Codes

Nicolas Resch

University of Amsterdam

Joint work with:

Dean Doron — Ben-Gurion University

Tal Leonov — Ben-Gurion University

Jonathan Mosheiff — Ben-Gurion University

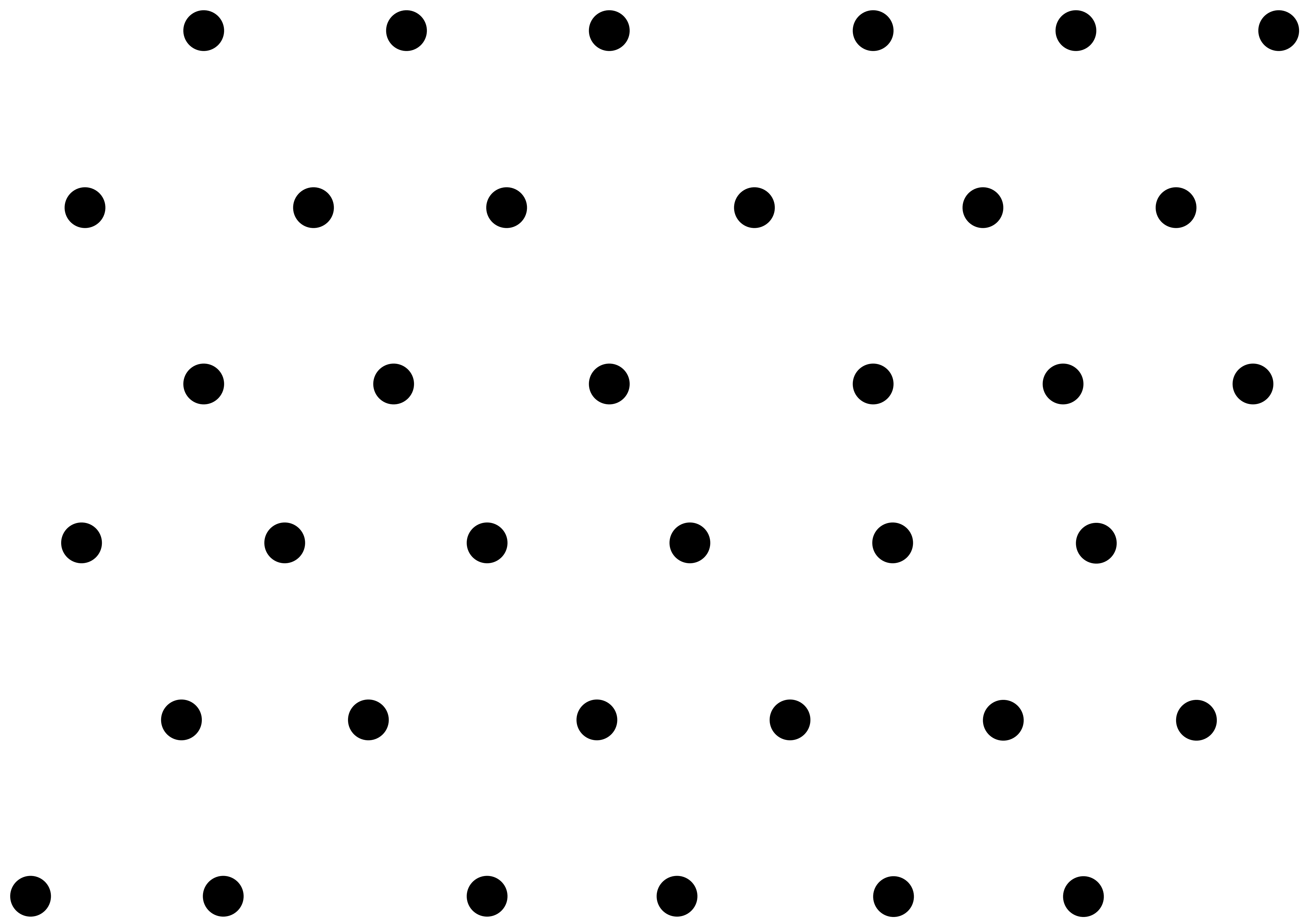
Henrique Navas — Universidade de Lisboa

João Ribeiro — Universidade de Lisboa

Paris Groupe de Travail July 6 2026

List-Decodability

$\mathscr{C} \leq \mathbb{F}_q^n$ a linear code

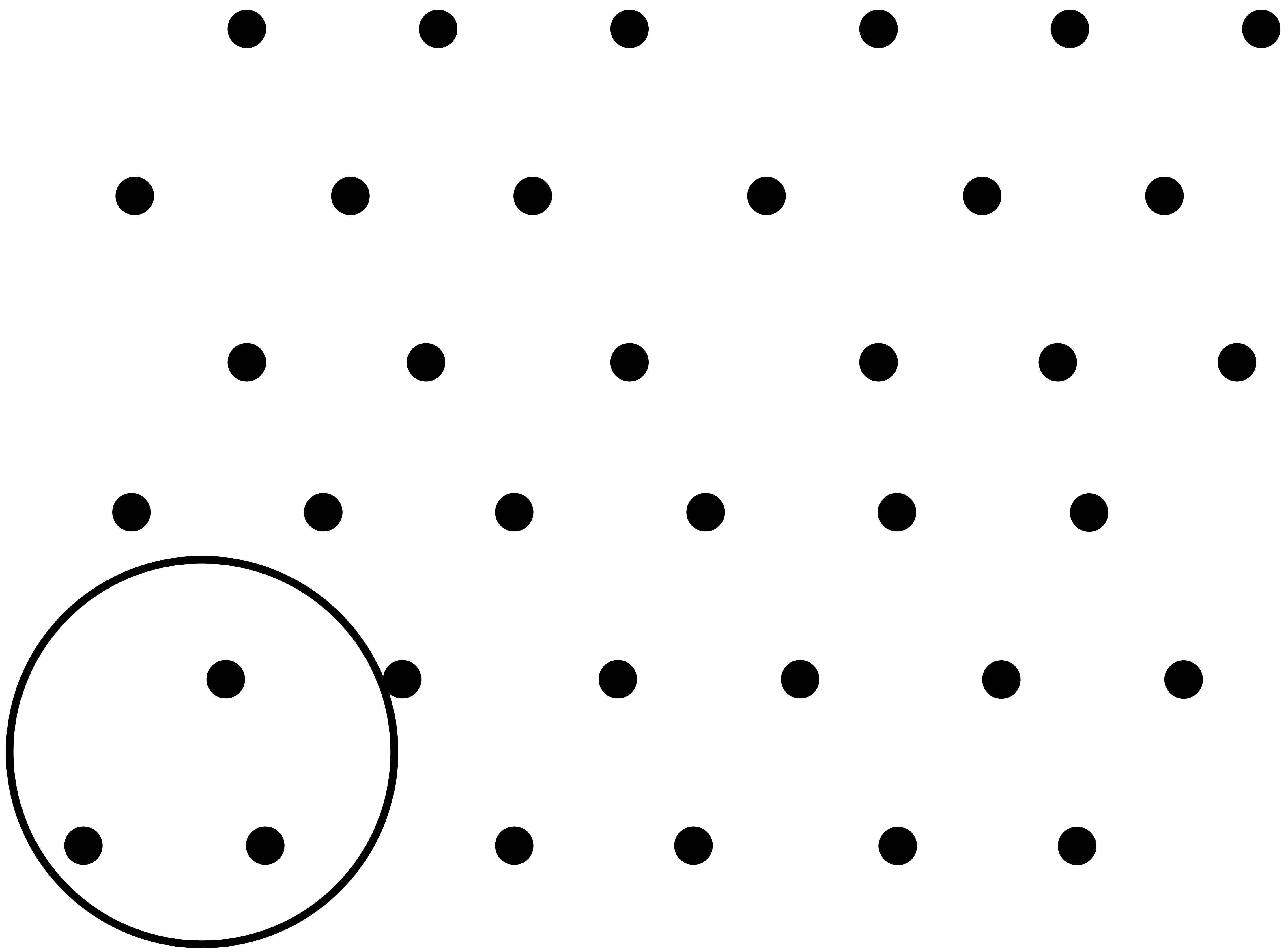


List-Decodability

$\mathscr{C} \leq \mathbb{F}_q^n$ a linear code

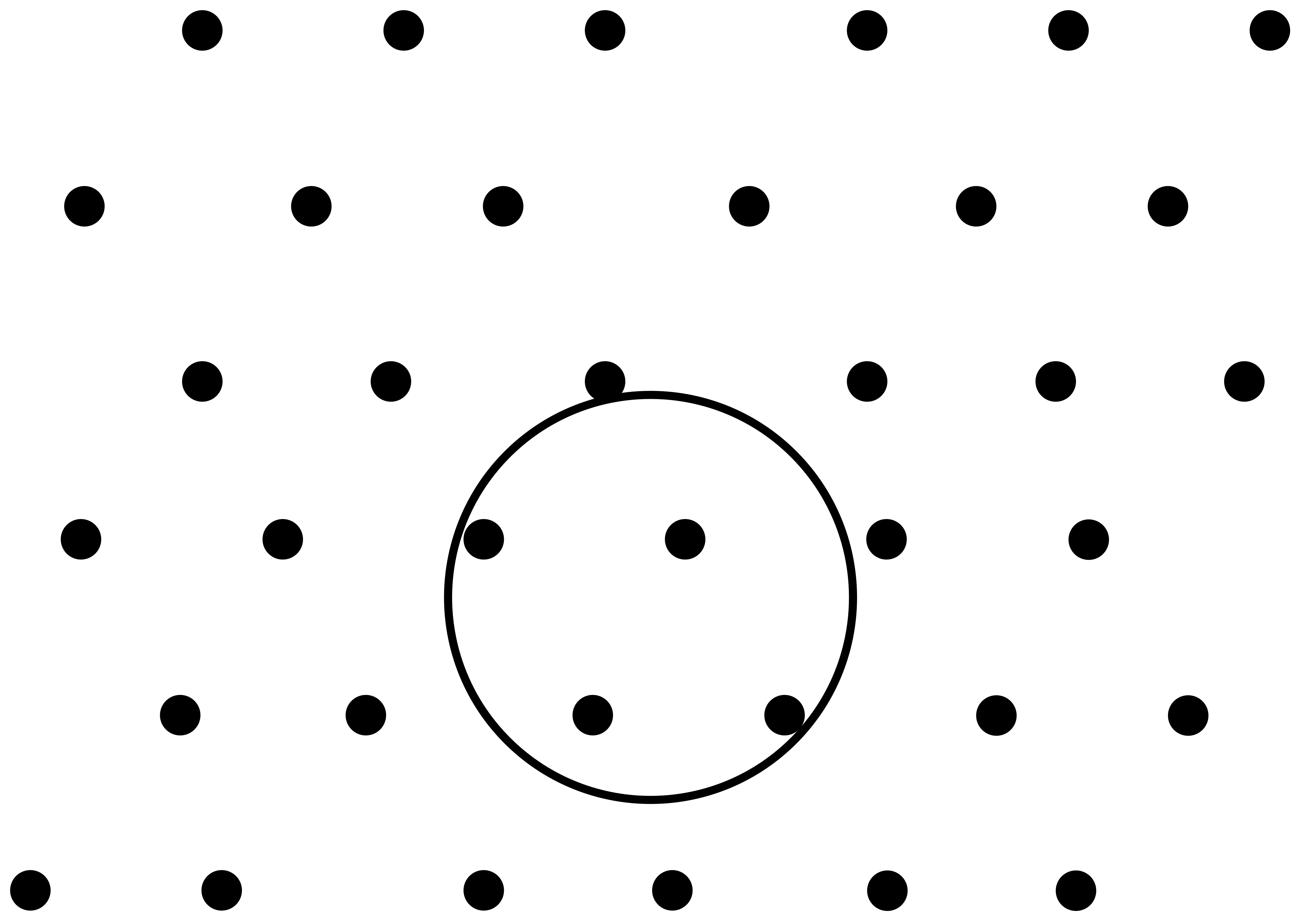
Hamming ball

$$B_\rho := \{x \in \mathbb{F}_q^n : \mathrm{wt}(x) \leq \rho n\}$$



List-Decodability

$\mathscr{C} \leq \mathbb{F}_q^n$ a linear code

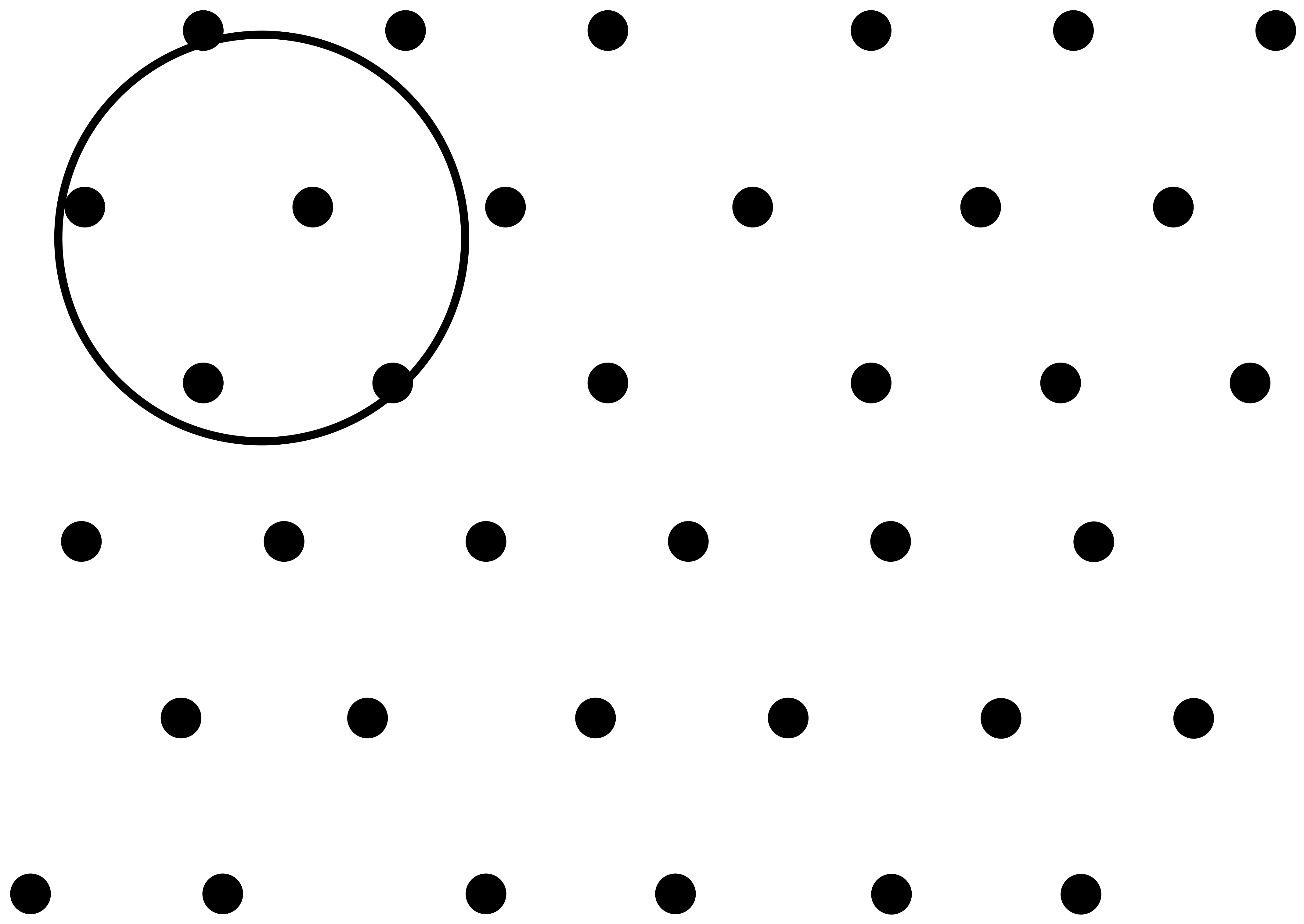


Hamming ball

$$B_\rho := \{x \in \mathbb{F}_q^n : \mathrm{wt}(x) \leq \rho\, n\}$$

List-Decodability

$\mathscr{C} \leq \mathbb{F}_q^n$ a linear code

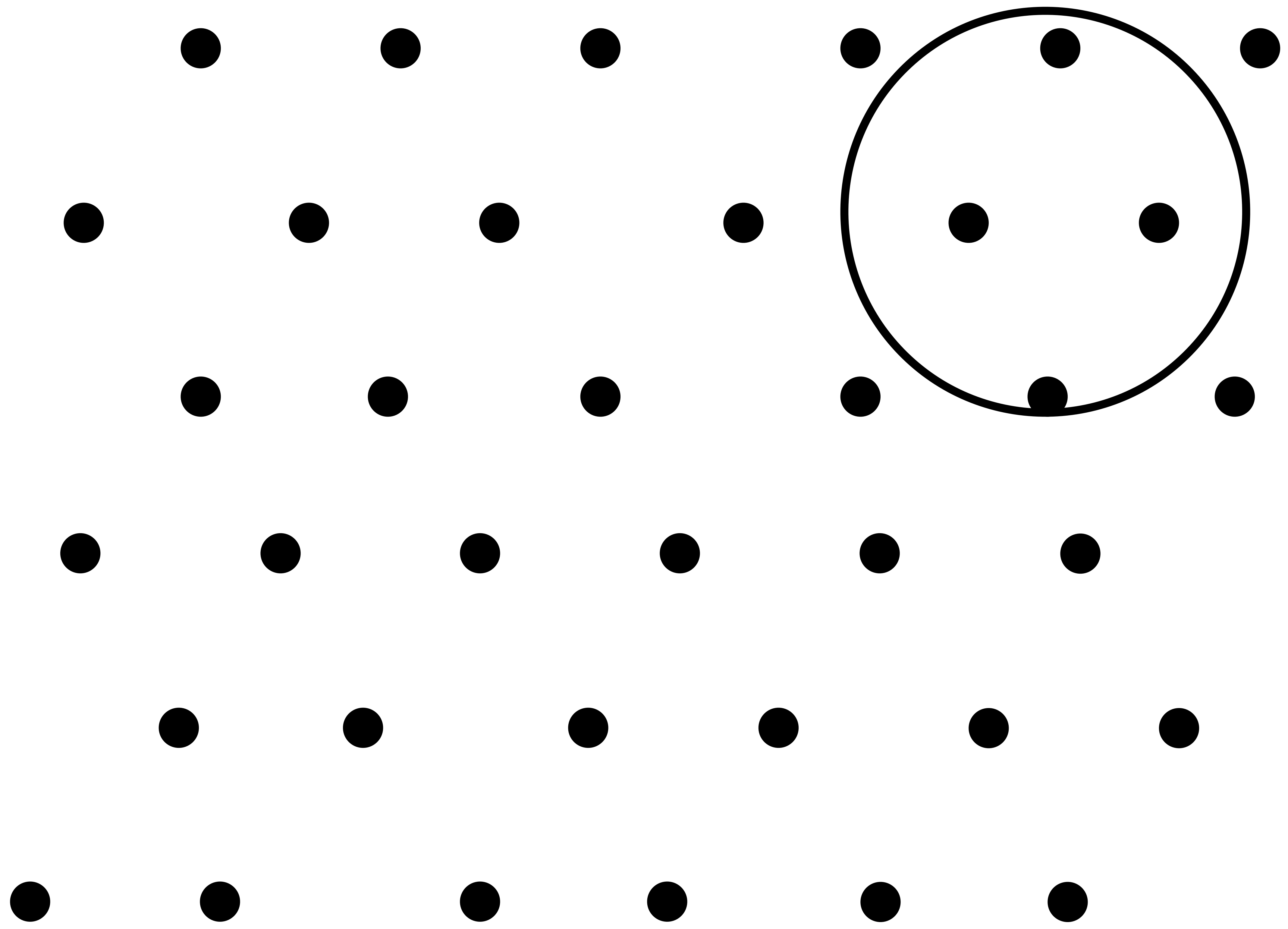


Hamming ball

$$B_\rho := \{x \in \mathbb{F}_q^n : \mathrm{wt}(x) \leq \rho n\}$$

List-Decodability

$\mathscr{C} \leq \mathbb{F}_q^n$ a linear code

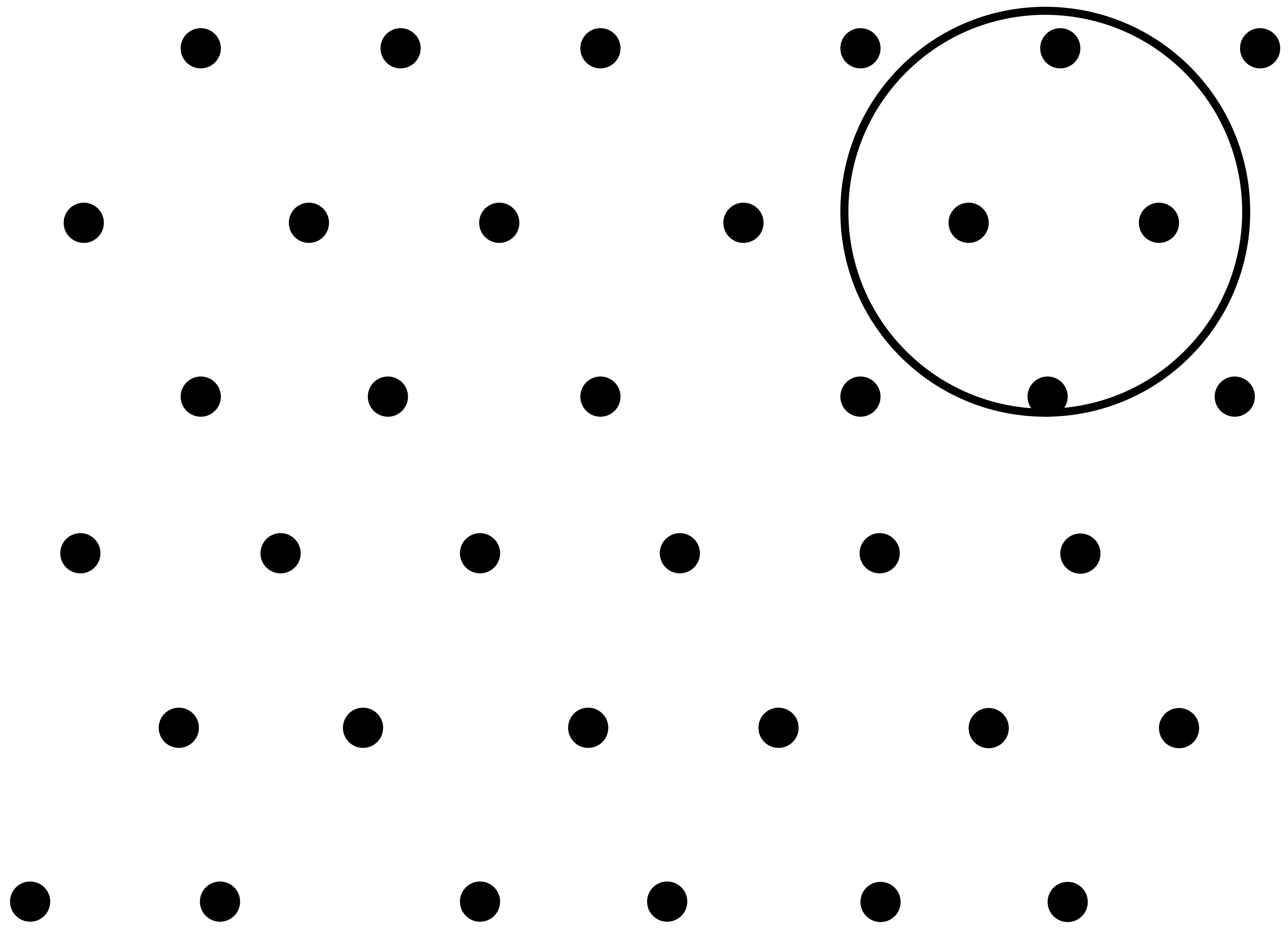


Hamming ball

$$B_\rho := \{x \in \mathbb{F}_q^n : \mathrm{wt}(x) \leq \rho n\}$$

List-Decodability

$\mathscr{C} \leq \mathbb{F}_q^n$ a linear code



Hamming ball

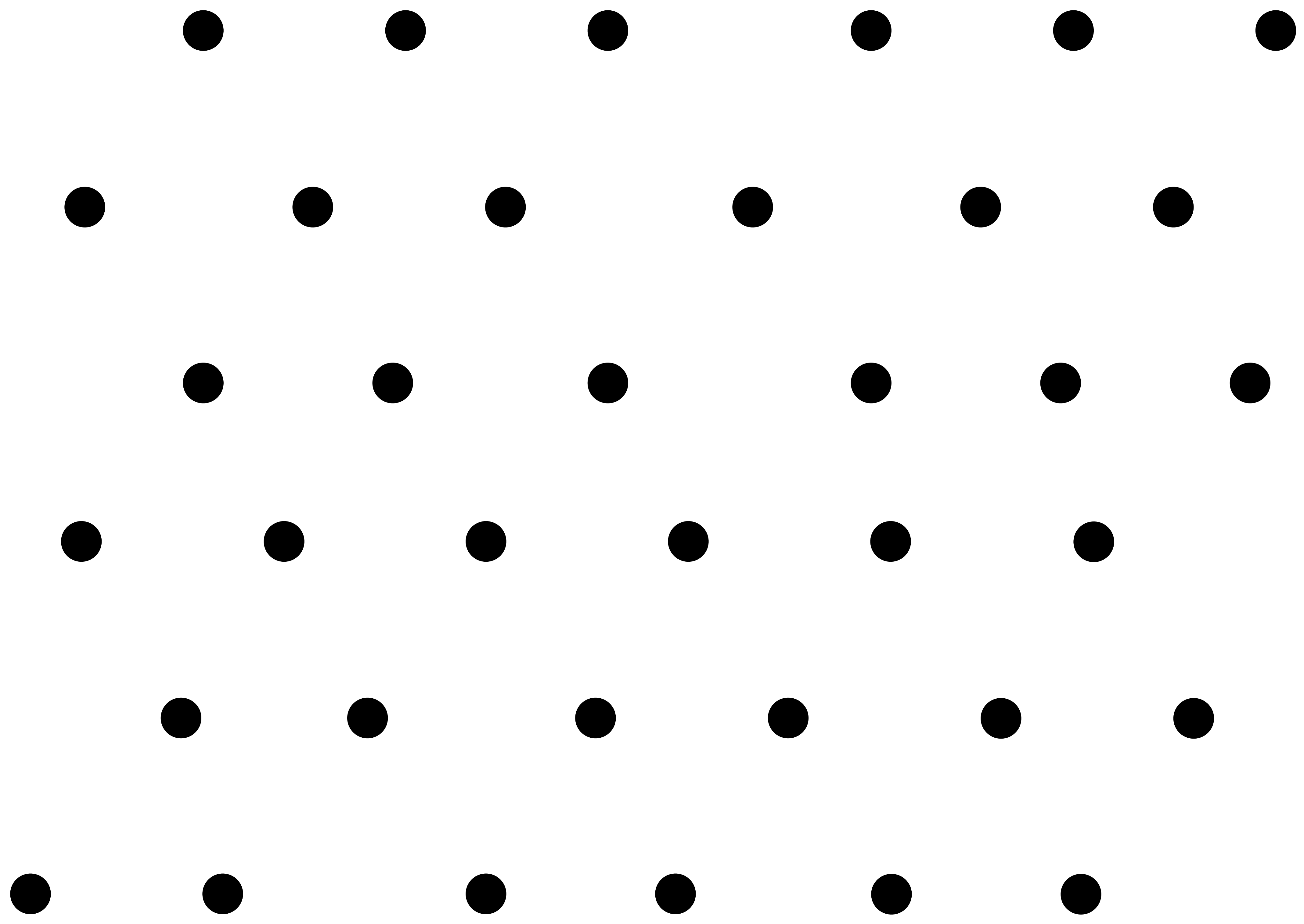
$$B_\rho := \{x \in \mathbb{F}_q^n : \mathrm{wt}(x) \leq \rho n\}$$

Call $\mathscr{C}$ (ρ, L)-***list-decodable*** if
$\forall z \in \mathbb{F}_q^n, |(z + B_\rho) \cap \mathscr{C}| \leq L$

For any $B \subseteq \mathbb{F}_q^n$, $z + B = \{z + x : x \in B\}$

List-Recoverability*

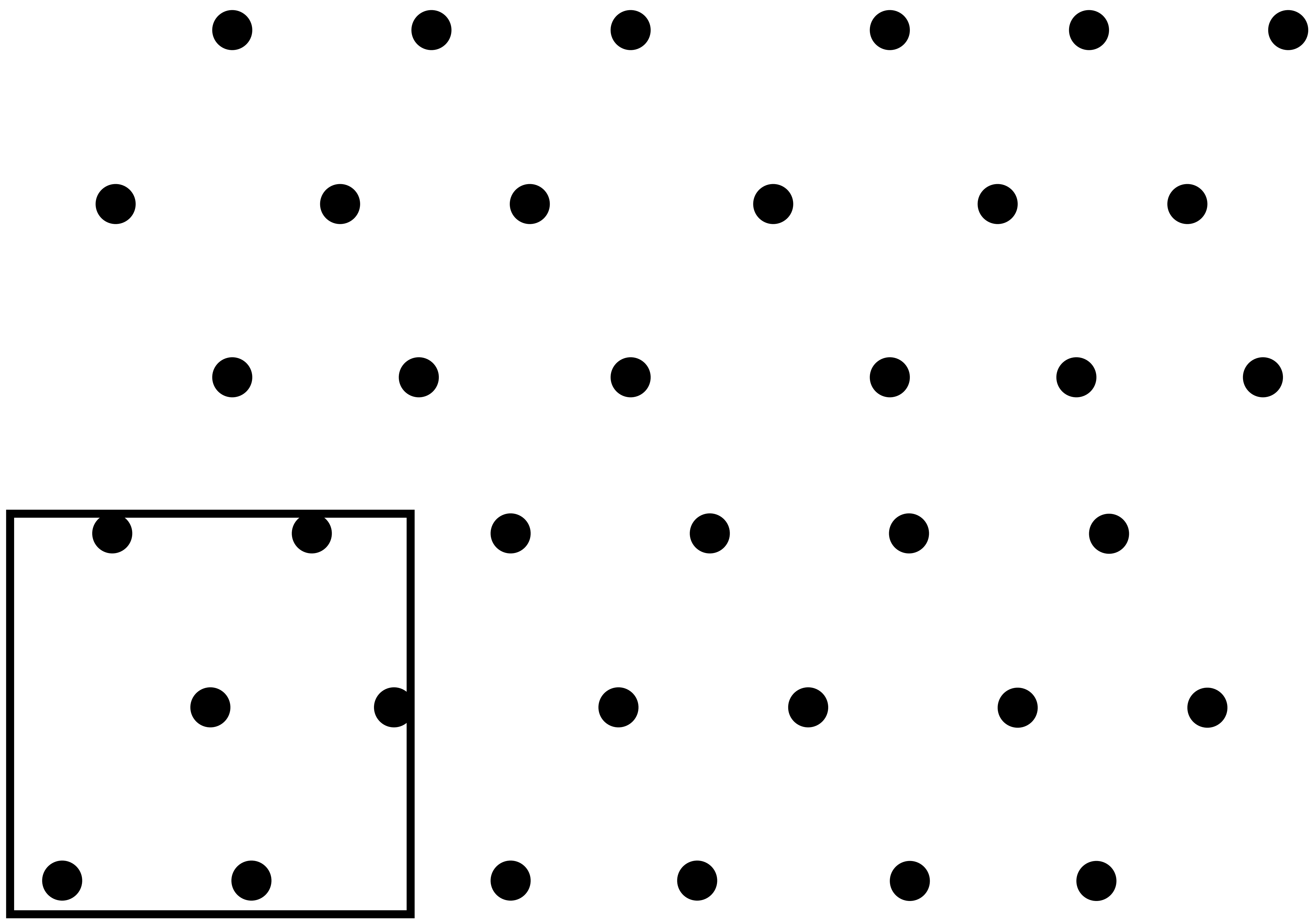
$C \leq \mathbb{F}_q^n$ a linear code



*zero-error

List-Recoverability*

$C \leq \mathbb{F}_q^n$ a linear code



$S_1, \ldots, S_n \subseteq \mathbb{F}_q^n, \ |S_i| = \ell$

Rectangles $S_1 \times \cdots \times S_n$

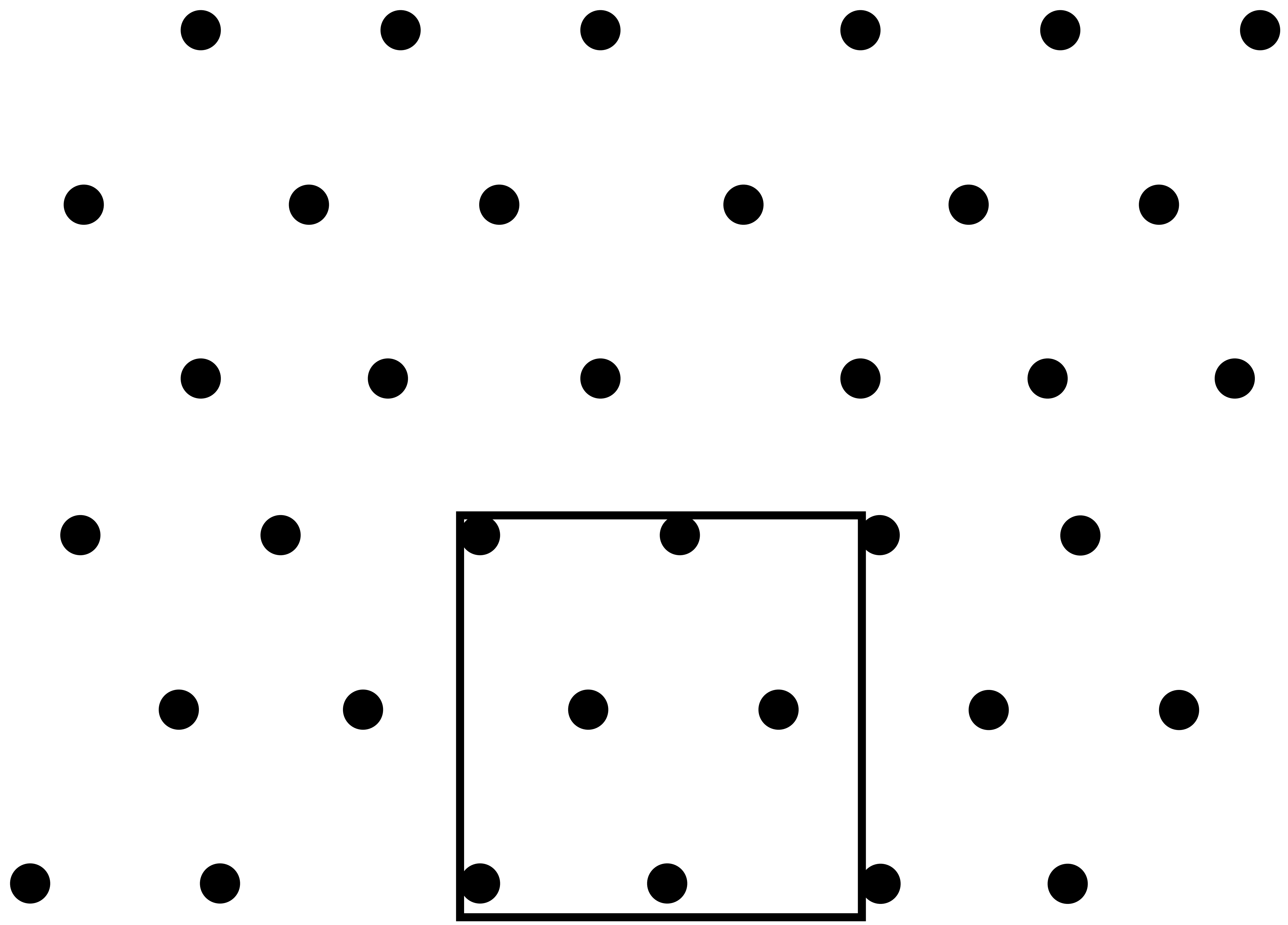
*zero-error

List-Recoverability*

$C \leq \mathbb{F}_q^n$ a linear code

$S_1, \ldots, S_n \subseteq \mathbb{F}_q^n,\ |S_i| = \ell$

Rectangles $S_1 \times \cdots \times S_n$



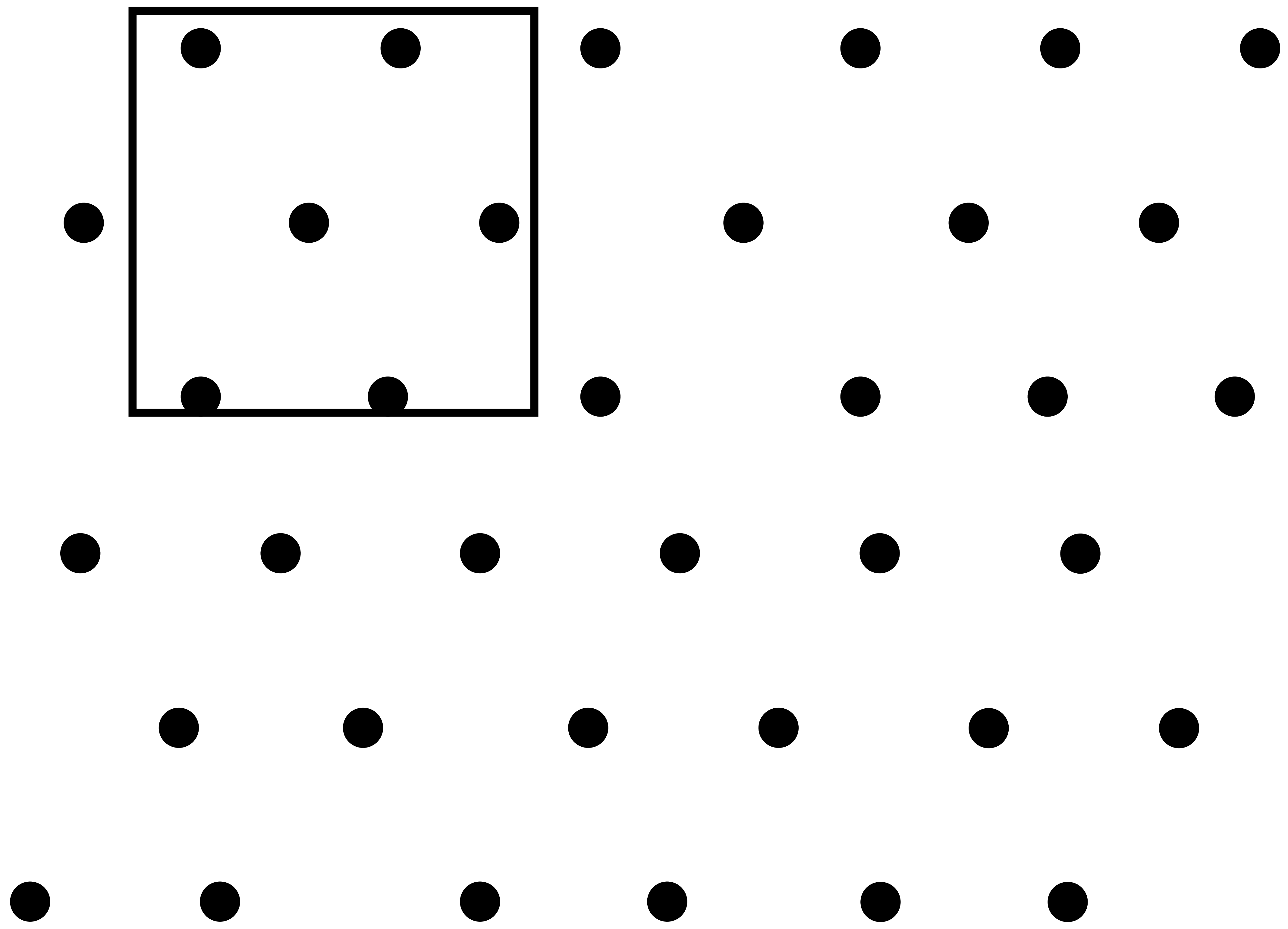
*zero-error

List-Recoverability*

$C \leq \mathbb{F}_q^n$ a linear code

$S_1, \ldots, S_n \subseteq \mathbb{F}_q^n$, $|S_i| = \ell$

Rectangles $S_1 \times \cdots \times S_n$



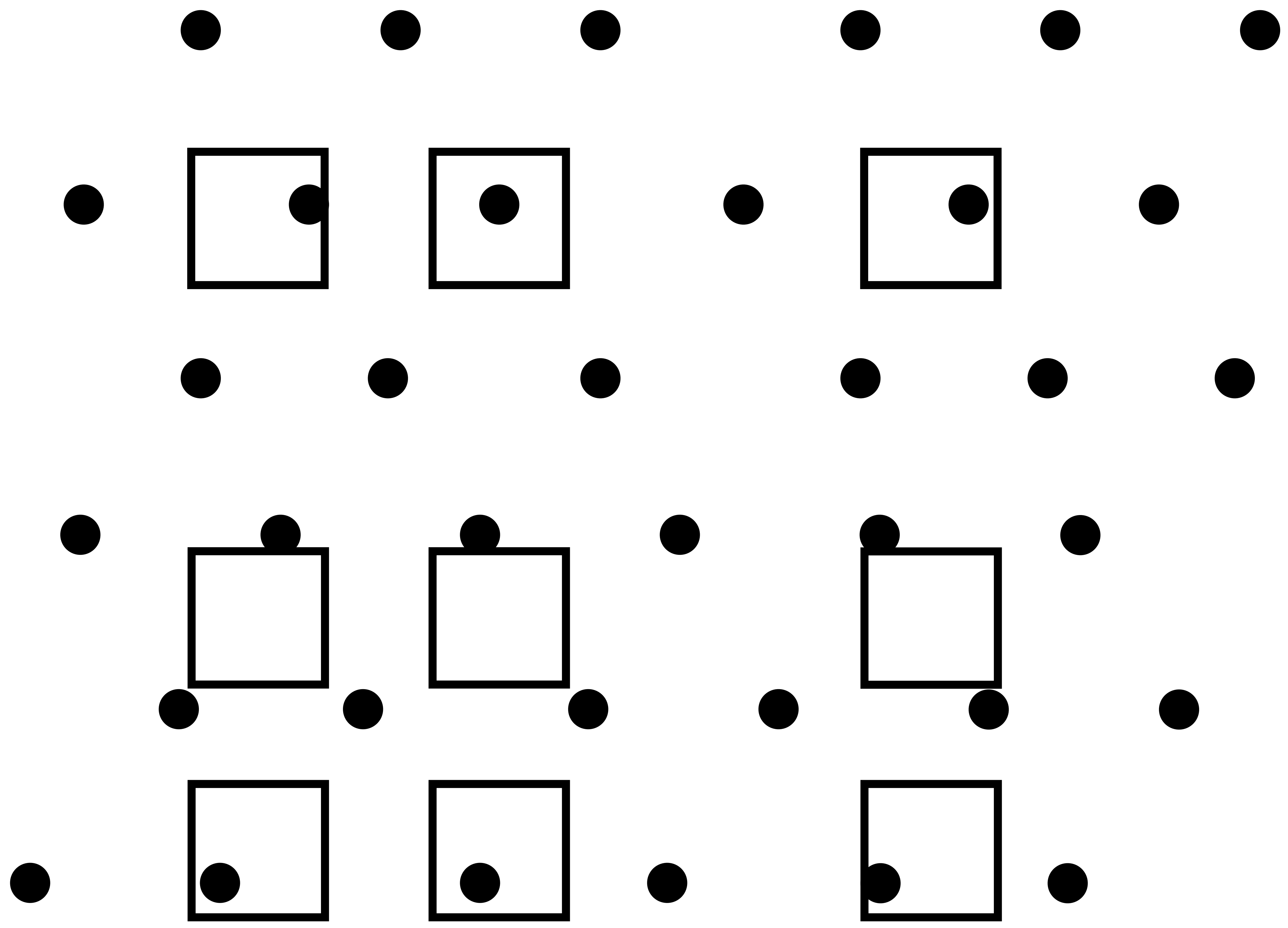
*zero-error

List-Recoverability*

$C \leq \mathbb{F}_q^n$ a linear code

$S_1, \ldots, S_n \subseteq \mathbb{F}_q^n,\ |S_i| = \ell$

Rectangles $S_1 \times \cdots \times S_n$



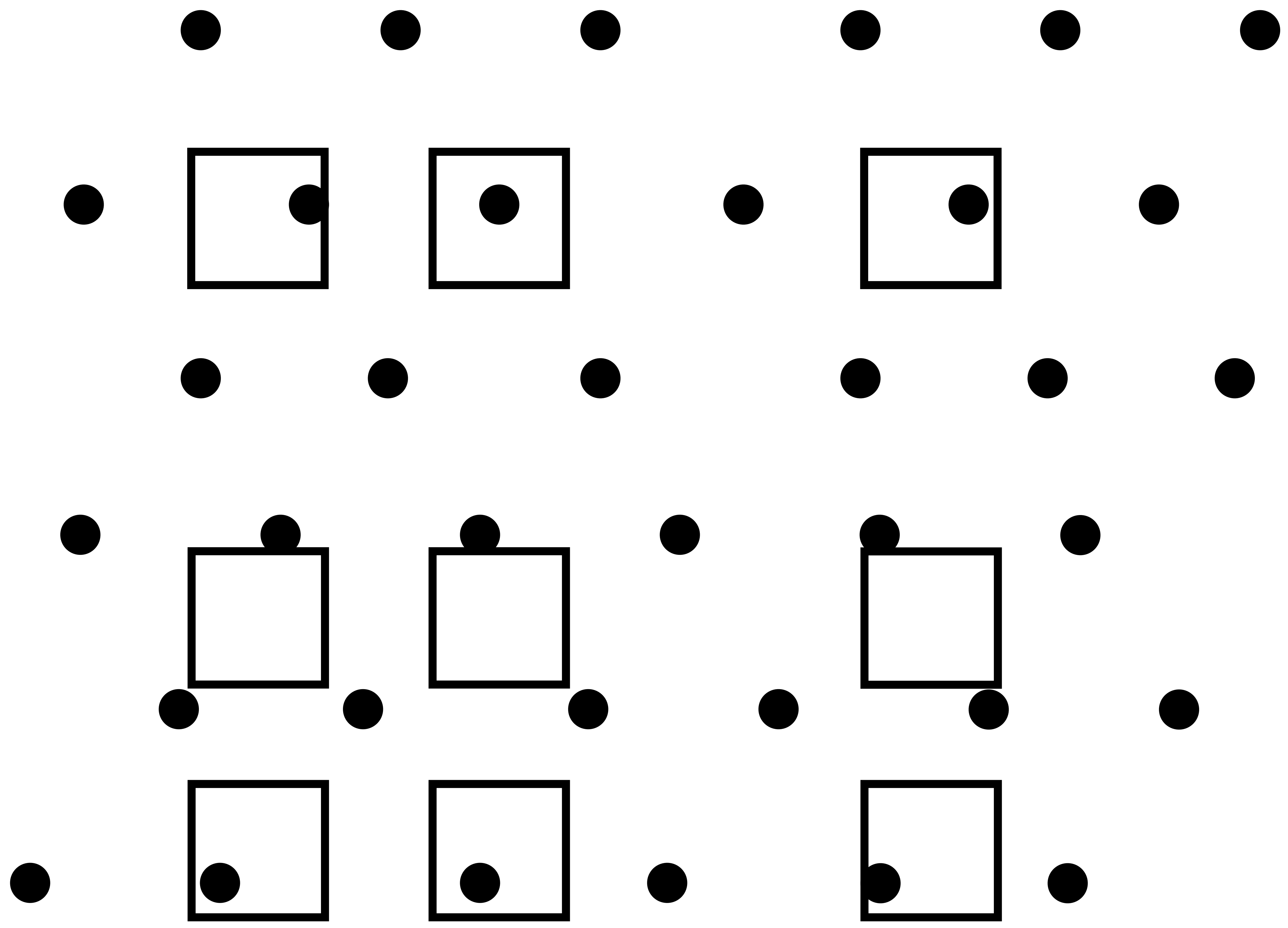
*zero-error

List-Recoverability*

$C \leq \mathbb{F}_q^n$ a linear code

$S_1, \ldots, S_n \subseteq \mathbb{F}_q^n, \ |S_i| = \ell$

Rectangles $S_1 \times \cdots \times S_n$



Call C (ℓ, L)***-list-recoverable*** if
$\forall S_1, \ldots, S_n \subseteq \mathbb{F}_q^n, \ |S_i| = \ell,$
$|(S_1 \times \cdots \times S_n) \cap C| \leq L$

*zero-error

Below Capacity: Small Expectation

Both list-decoding and list-recovery have "***capacities***"

Below Capacity: Small Expectation

Both list-decoding and list-recovery have "***capacities***"

List-decoding at radius ρ:

$$R^*(\rho) := 1 - h_q(\rho)$$

Below Capacity: Small Expectation

Both list-decoding and list-recovery have "***capacities***"

List-decoding at radius ρ:

$$R^*(\rho) := 1 - h_q(\rho)$$

List-recovery w/ input list-size ℓ:

$$R^*(\ell) := 1 - \log_q(\ell)$$

Below Capacity: Small Expectation

Both list-decoding and list-recovery have "***capacities***"

List-decoding at radius ρ:

$R^*(\rho) := 1 - h_q(\rho)$

List-recovery w/ input list-size ℓ:

$R^*(\ell) := 1 - \log_q(\ell)$

These capacities R^* are such that,

if $\mathbf{C}$ is random linear code (RLC) of rate $R^* - \varepsilon$,

$$\mathbb{E}[\,|\mathbf{C} \cap B|\,] \leq q^{-\varepsilon n},$$

where B's either a ball or a rectangle

Below Capacity: Small Expectation

Both list-decoding and list-recovery have "***capacities***"

List-decoding at radius ρ:

$R^*(\rho) := 1 - h_q(\rho)$

List-recovery w/ input list-size ℓ:

$R^*(\ell) := 1 - \log_q(\ell)$

These capacities R^* are such that,

if $\mathbf{C}$ is random linear code (RLC) of rate $R^* - \varepsilon$,

$$\mathbb{E}[\,|\mathbf{C} \cap B|\,] \leq q^{-\varepsilon n},$$

where B's either a ball or a rectangle

I will boldface random variables

Capacity, Abstractly

[Loe94]

Capacity, Abstractly

[Loe94]

More generally, consider *any* subset $B \subseteq \mathbb{F}_q^n$

Define "**capacity**" $\beta := 1 - \frac{1}{n} \log_q |B|$

Capacity, Abstractly

[Loe94]

More generally, consider *any* subset $B \subseteq \mathbb{F}_q^n$

Define "**capacity**" $\beta := 1 - \frac{1}{n}\log_q |B|$

Then, if $\mathbf{C}$ is RLC of rate β,

$$\mathbb{E}\big[\,|\mathbf{C} \cap B|\,\big] = \frac{q^{\beta n}|B|}{q^n} = 1$$

Capacity, Abstractly

[Loe94]

More generally, consider *any* subset $B \subseteq \mathbb{F}_q^n$

Define "**capacity**" $\beta := 1 - \frac{1}{n}\log_q |B|$

E.g., if $B = B_\rho$,

$$1 - \frac{1}{n}\log_q |B_\rho| \approx 1 - h_q(\rho)$$

Then, if $\mathbf{C}$ is RLC of rate β,

$$\mathbb{E}\big[|\mathbf{C} \cap B|\big] = \frac{q^{\beta n}|B|}{q^n} = 1$$

Capacity, Abstractly

[Loe94]

More generally, consider *any* subset $B \subseteq \mathbb{F}_q^n$

Define "**capacity**" $\beta := 1 - \frac{1}{n}\log_q |B|$

Then, if $\mathbf{C}$ is RLC of rate β,

$$\mathbb{E}\big[\,|\mathbf{C} \cap B|\,\big] = \frac{q^{\beta n}|B|}{q^n} = 1$$

E.g., if $B = B_\rho$,

$$1 - \frac{1}{n}\log_q |B_\rho|$$
$$\approx 1 - h_q(\rho)$$

$$B = S_1 \times \cdots \times S_n,$$
$$1 - \frac{1}{n}\log_q |B|$$
$$= 1 - \log_q(\ell)$$

Codes Above Capacity?

Codes Above Capacity?

Usually, study codes C at rate $\beta - \varepsilon$, so $\mathbb{E}[\,|\mathbf{C} \cap B|\,] = q^{-\varepsilon n} \ll 1$, and argue

$|B \cap C| \leq L$ for many sets B (of same size)

Codes Above Capacity?

Usually, study codes C at rate $\beta - \varepsilon$, so $\mathbb{E}[\,|\mathbf{C} \cap B|\,] = q^{-\varepsilon n} \ll 1$, and argue

$$|B \cap C| \leq L \text{ for many sets } B \text{ (of same size)}$$

If code has rate $\beta + \varepsilon$, maybe we could have

$$|B \cap C| = (1 \pm o(1))\,\mathbb{E}[\,|\mathbf{C} \cap B|\,] = (1 \pm o(1))\,q^{\varepsilon n}$$

(again, for many sets B)?

Motivation?

Covering Codes

Covering Codes

Recall: a code $C \leq \mathbb{F}_q^n$ has ***covering radius*** ρ if

$$\forall z \in \mathbb{F}_q^n, \quad |C \cap (z + B_\rho)| \geq 1$$

Covering Codes

Recall: a code $C \leq \mathbb{F}_q^n$ has ***covering radius*** ρ if

$$\forall z \in \mathbb{F}_q^n, \quad |C \cap (z + B_\rho)| \geq 1$$

Prior work [Bli'87,CHLL'97] established that if $\mathbf{C}$ is RLC of rate

$$1 - h_q(\rho) + \varepsilon,$$

it has covering radius ρ with probability $1 - q^{-\Omega(n)}$

Covering Codes

Recall: a code $C \leq \mathbb{F}_q^n$ has ***covering radius*** ρ if

$$\forall z \in \mathbb{F}_q^n, \quad |C \cap (z + B_\rho)| \geq 1$$

Prior work [Bli'87,CHLL'97] established that if $\mathbf{C}$ is RLC of rate

$$1 - h_q(\rho) + \varepsilon,$$

Above capacity!

it has covering radius ρ with probability $1 - q^{-\Omega(n)}$

Covering Codes

Recall: a code $C \leq \mathbb{F}_q^n$ has ***covering radius*** ρ if

$$\forall z \in \mathbb{F}_q^n, \;\; |C \cap (z + B_\rho)| \geq 1$$

Prior work [Bli'87,CHLL'97] established that if $\mathbf{C}$ is RLC of rate

$$1 - h_q(\rho) + \varepsilon,$$

Above capacity!

it has covering radius ρ with probability $1 - q^{-\Omega(n)}$

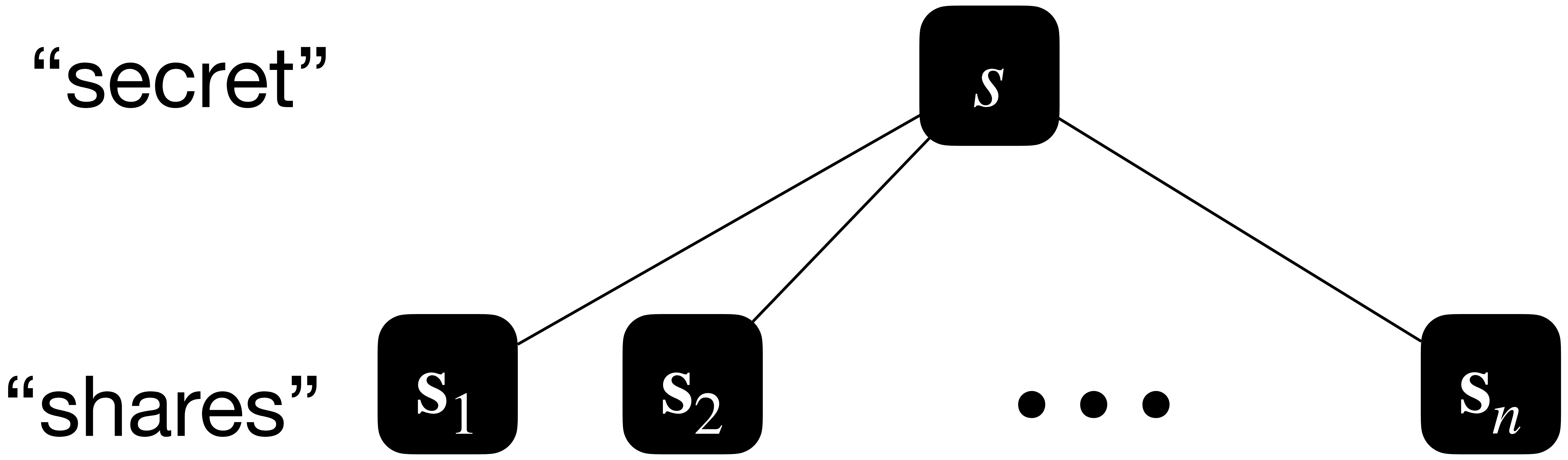
Could hope for: $\forall z \in \mathbb{F}_q^n, \;\; |C \cap (z + B_\rho)| \approx \dfrac{|C||B_\rho|}{q^n}$

Secret-Sharing Schemes

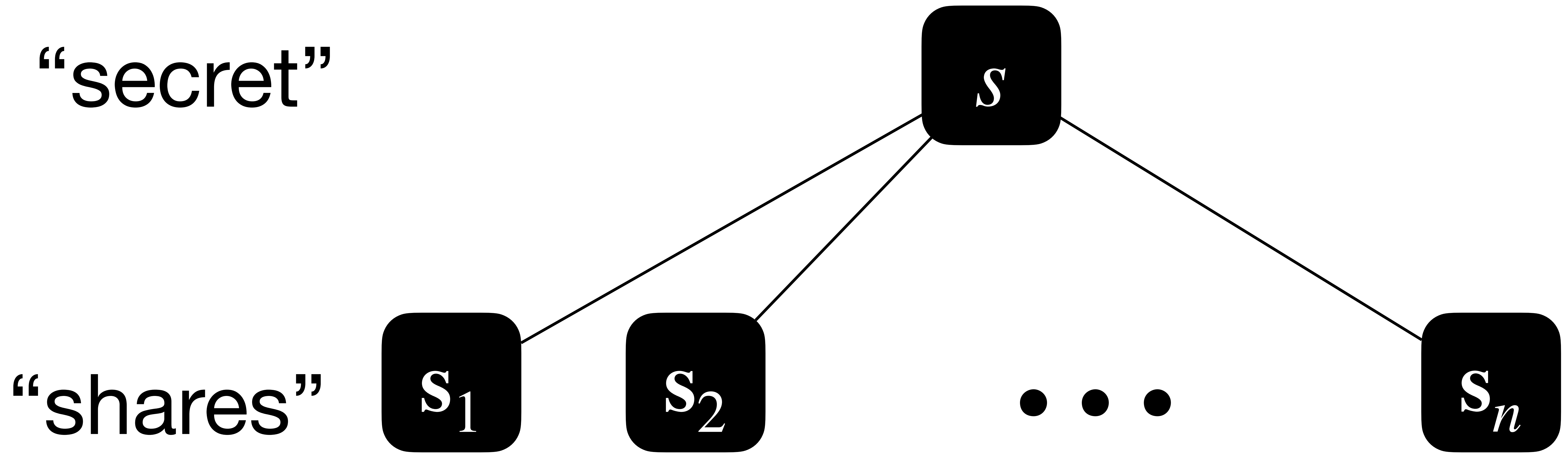
“secret”

s

Secret-Sharing Schemes



Secret-Sharing Schemes

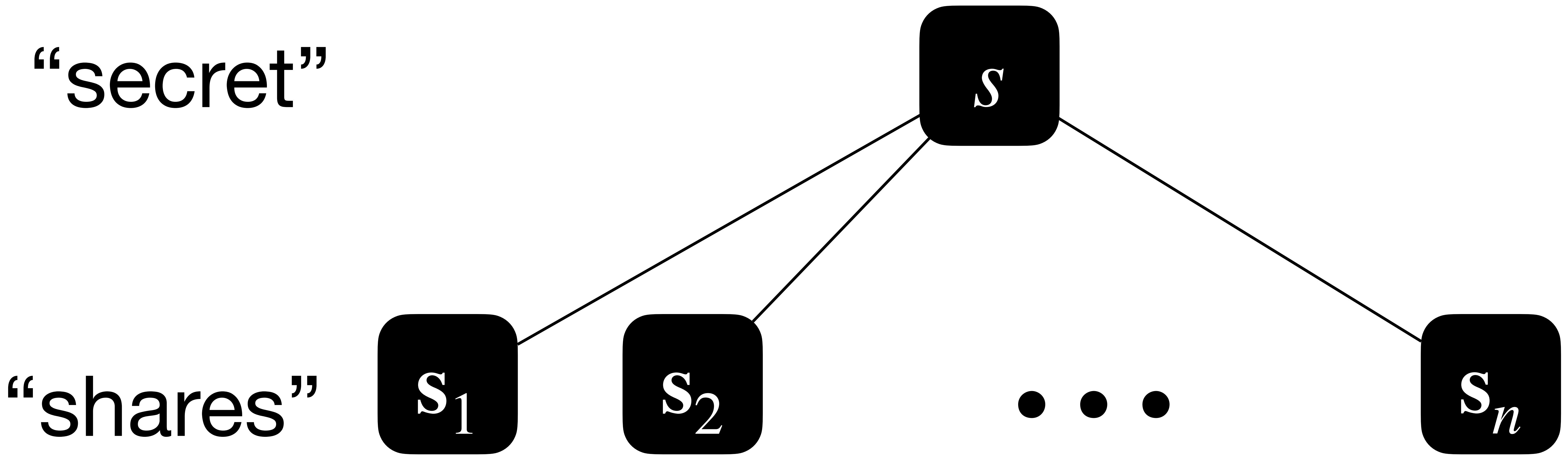


$(n, t_{\text{rec}}, t_{\text{pri}})$-secret sharing scheme:

$$\text{Recon}(\mathbf{s}_i : i \in T) = s \text{ if } |T| \geq t_{\text{rec}}$$

Furthermore, $(\mathbf{s}_i : i \in T) \sim \text{Unif}(\mathbb{F}_q^{|T|})$ if $|T| \leq t_{\text{pri}}$

Secret-Sharing Schemes



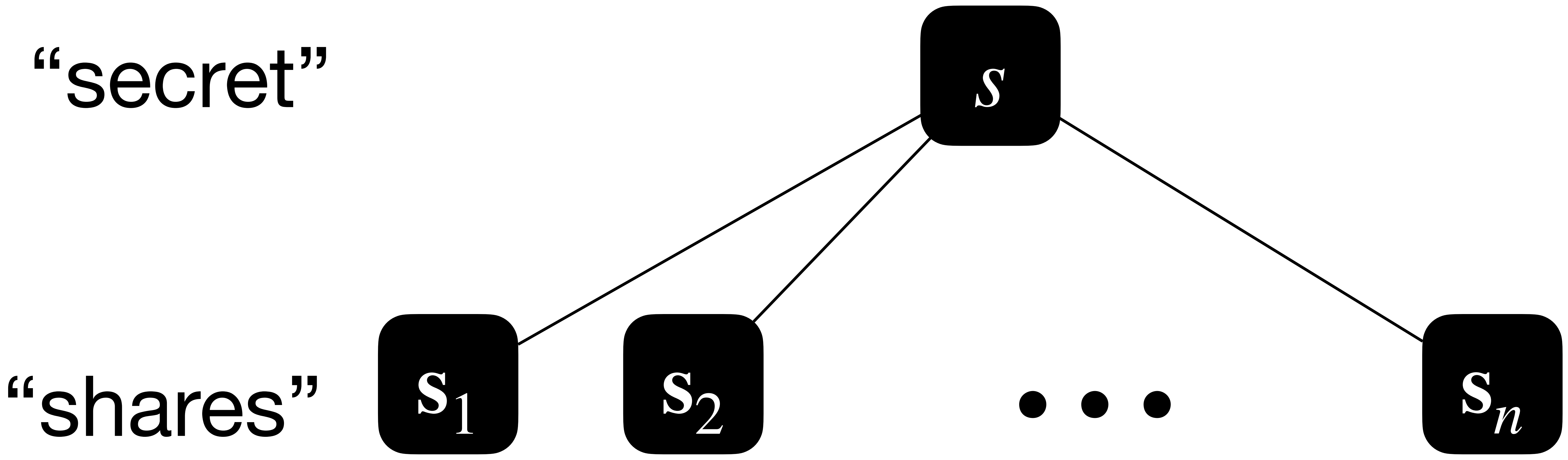
$(n, t_{\text{rec}}, t_{\text{pri}})$-secret sharing scheme:

$\text{Recon}(\mathbf{s}_i : i \in T) = s$ if $|T| \geq t_{\text{rec}}$

Furthermore, $(\mathbf{s}_i : i \in T) \sim \text{Unif}(\mathbb{F}_q^{|T|})$ if $|T| \leq t_{\text{pri}}$

Use randomness to sample $\mathbf{s}_i$'s

Secret-Sharing Schemes



$(n, t_{\text{rec}}, t_{\text{pri}})$-secret sharing scheme:

$\text{Recon}(\mathbf{s}_i : i \in T) = s$ if $|T| \geq t_{\text{rec}}$

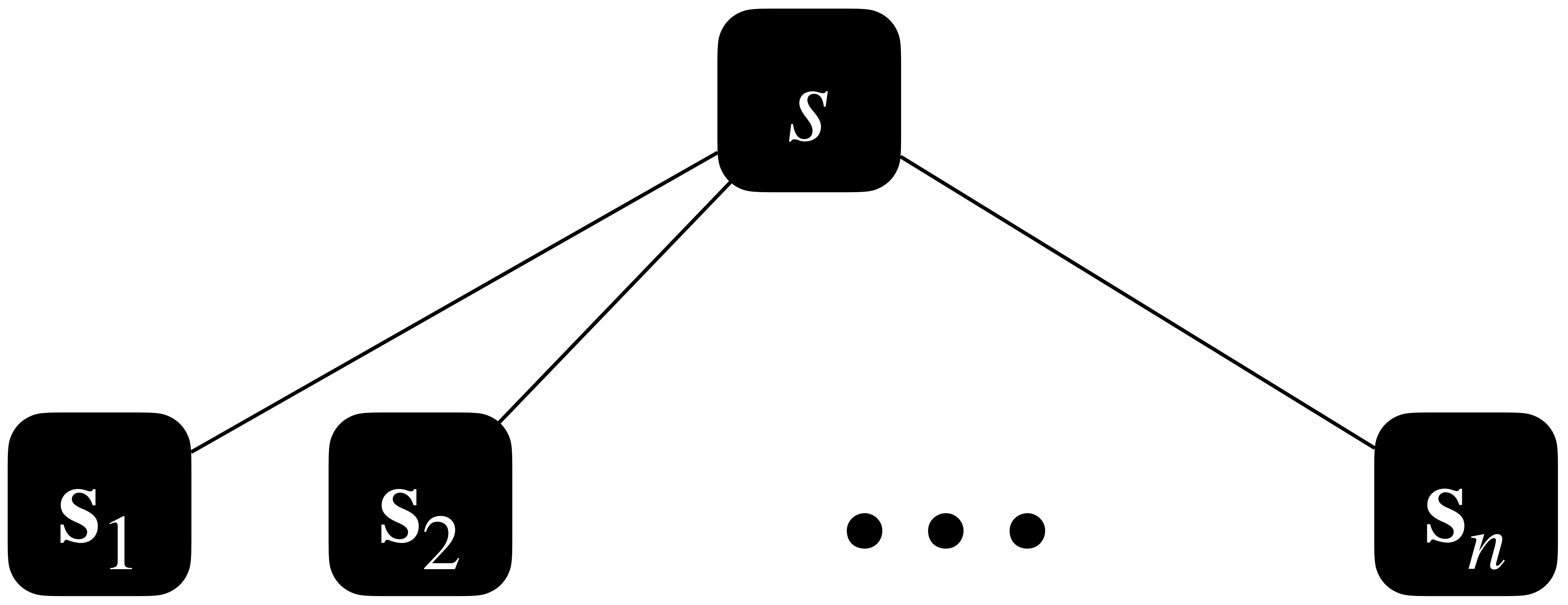
Furthermore, $(\mathbf{s}_i : i \in T) \sim \text{Unif}(\mathbb{F}_q^{|T|})$ if $|T| \leq t_{\text{pri}}$

Use randomness to sample $\mathbf{s}_i$'s

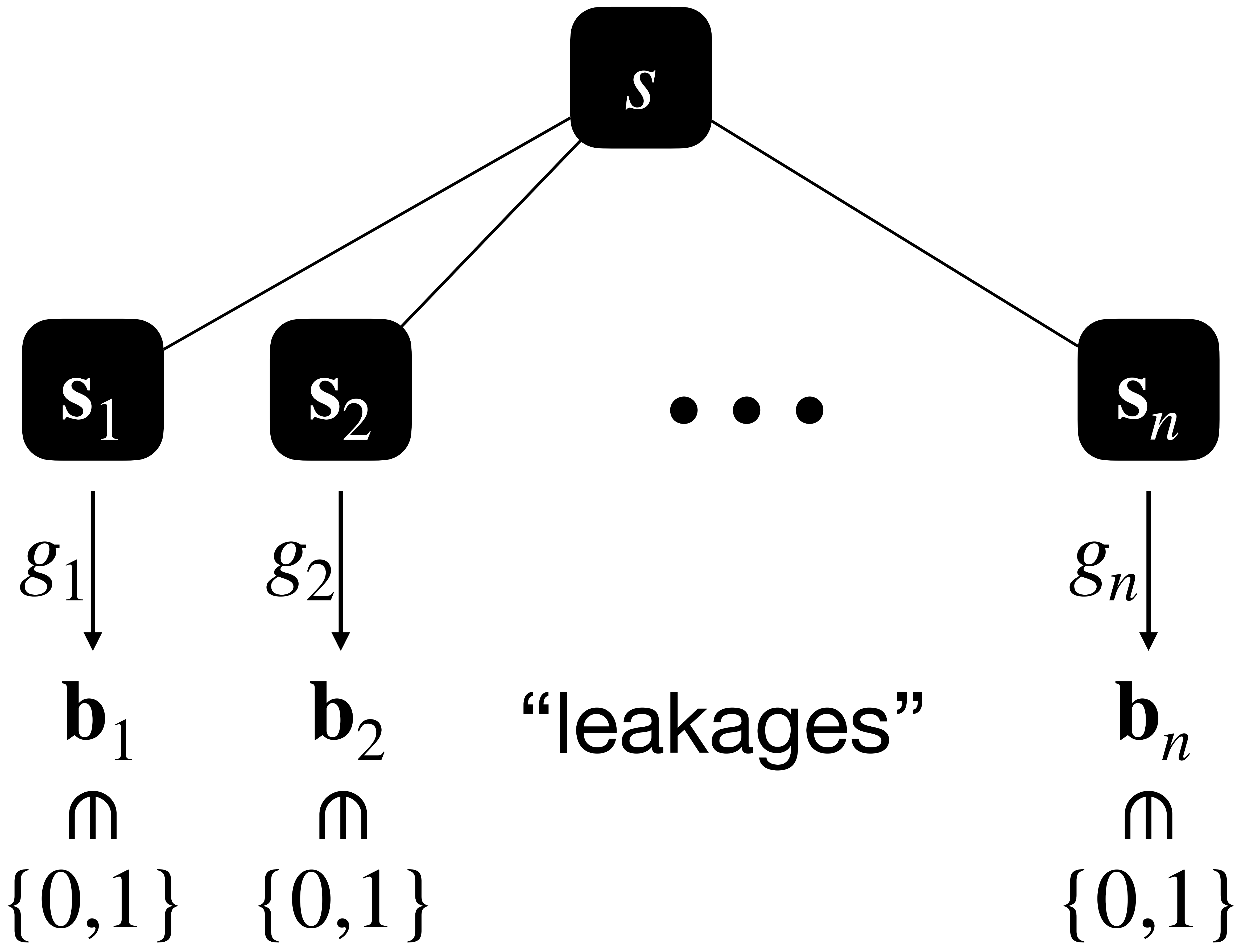
Massey's scheme: shares $(\mathbf{s}_1, \ldots, \mathbf{s}_n)$ correspond to codewords* in C, $t_{\text{rec}} = n - d(C) + 1$, $t_{\text{pri}} = d(C^{\perp}) - 1$

*technically from coset of C

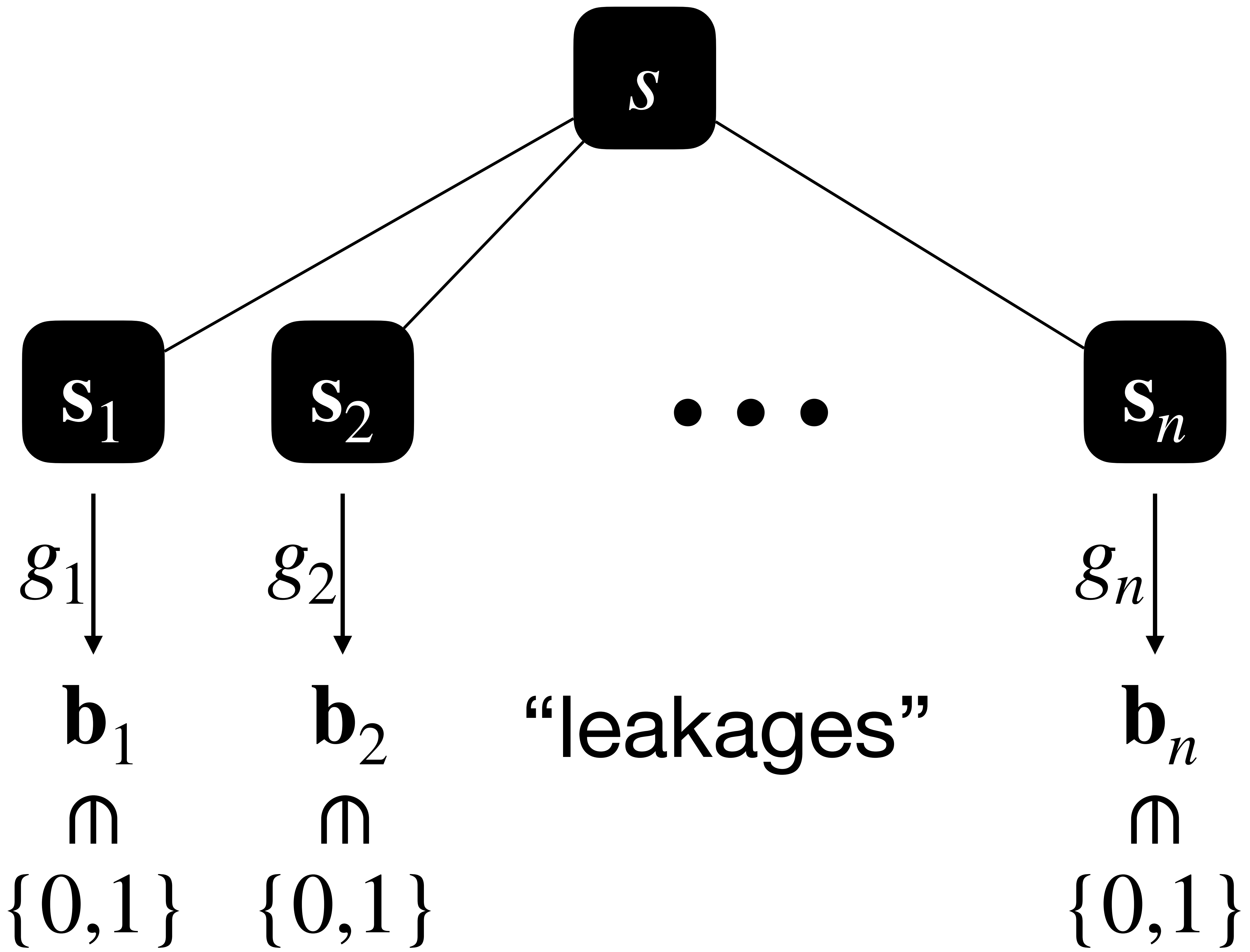
(Local) Leakage Resilience



(Local) Leakage Resilience

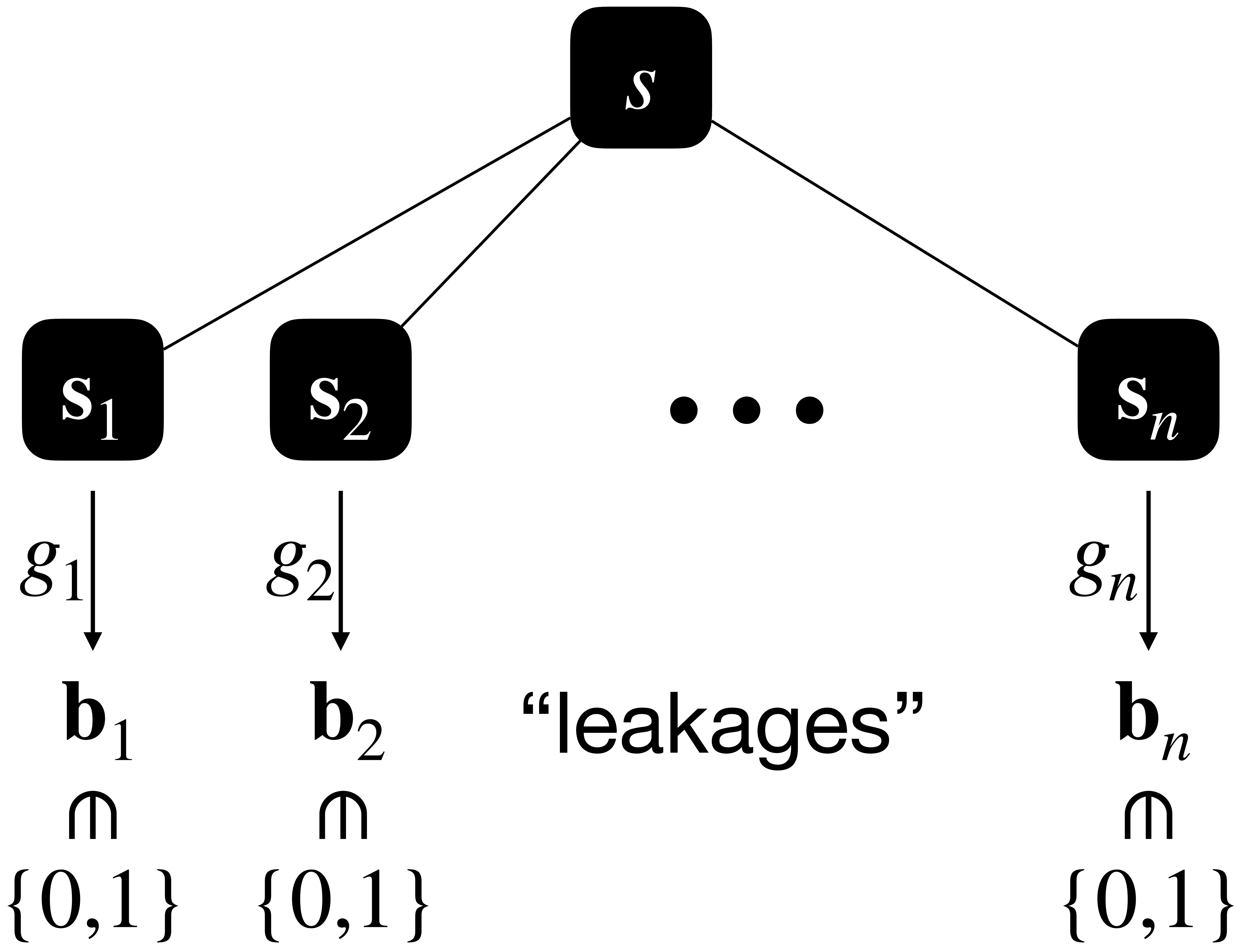


(Local) Leakage Resilience



Goal: $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is "roughly" uniform

(Local) Leakage Resilience



Goal: $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is "roughly" uniform

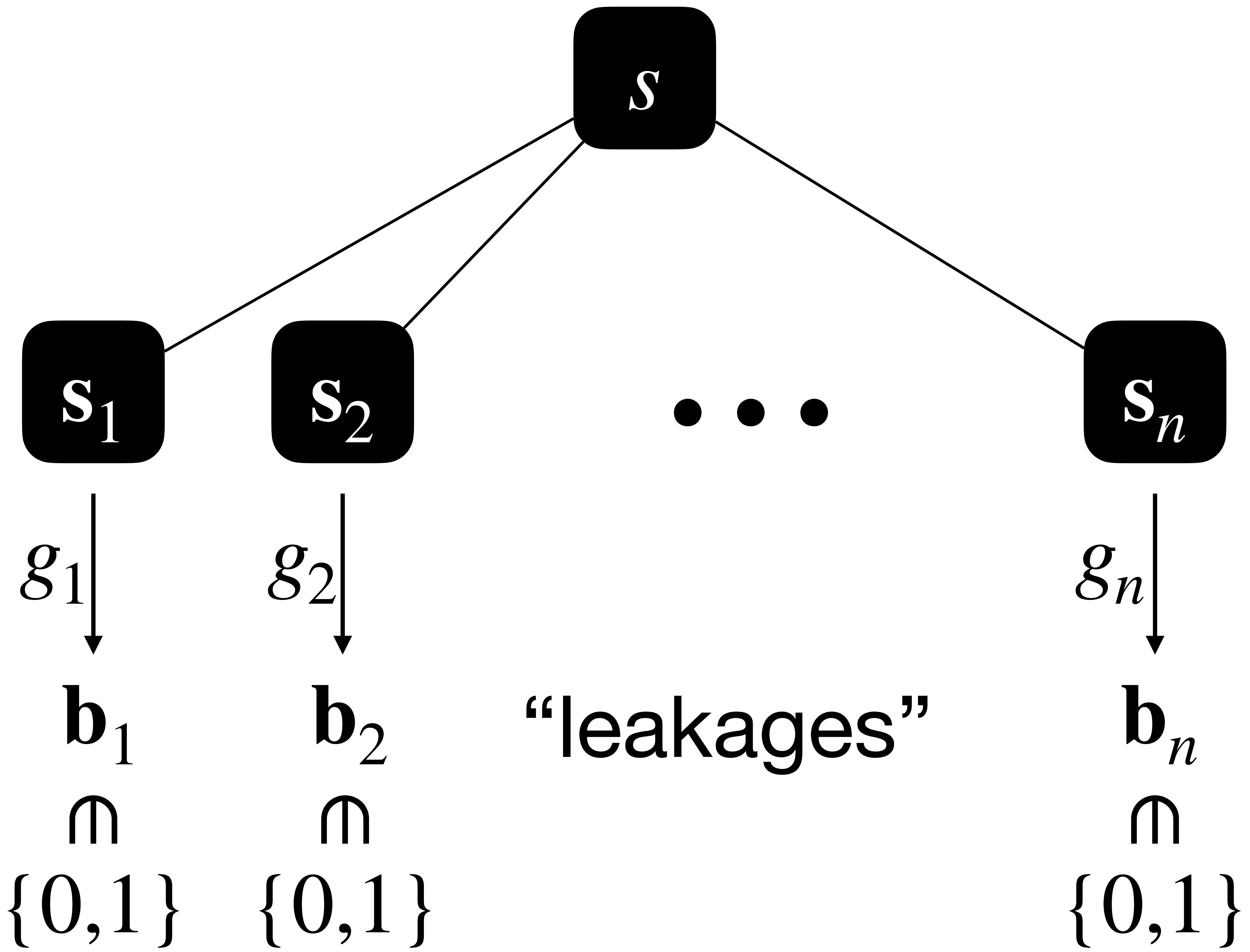
Assume each g_i balanced, e.g.,

$$g_i^{-1}(1) = g_i^{-1}(0) \approx \frac{q}{2}$$

Putting $S_i = g_i^{-1}(b_i)$, need to argue

$$\Pr_{\mathbf{c} \sim C}[\mathbf{c} \in S_1 \times \cdots \times S_n] \approx 2^{-n}$$

(Local) Leakage Resilience



Goal: $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is "roughly" uniform

Assume each g_i balanced, e.g.,

$$g_i^{-1}(1) = g_i^{-1}(0) \approx \frac{q}{2}$$

Putting $S_i = g_i^{-1}(b_i)$, need to argue

$$\Pr_{\mathbf{c} \sim C}[\mathbf{c} \in S_1 \times \cdots \times S_n] \approx 2^{-n}$$

$$|C \cap (S_1 \times \cdots \times S_n)| \approx \frac{|C|}{2^n} = \mathbb{E}[\,|\mathbf{C} \cap (S_1 \times \cdots \times S_n)|\,]$$

What is known?

What is known?

[GW16]: codes over characteristic 2 fields are ***not*** leakage resilient

Corollary of fact they make very good regenerating codes!

What is known?

[GW16]: codes over characteristic 2 fields are ***not*** leakage resilient

Corollary of fact they make very good regenerating codes!

Thus, line of works [MPSW21,TX22,KK23,Kas24,Ngu24] studies leakage-resilience over ***prime fields***

What is known?

[GW16]: codes over characteristic 2 fields are ***not*** leakage resilient

Corollary of fact they make very good regenerating codes!

Thus, line of works [MPSW21,TX22,KK23,Kas24,Ngu24] studies leakage-resilience over ***prime fields***

Notable challenge:

Codes of rate $< 1/2$?

Additional Examples

Additional Examples

Linear Hashing

[ADMPT97,DD23,JKZ25]

Additional Examples

Linear Hashing

[ADMPT97,DD23,JKZ25]

Given any $S \subseteq \mathbb{F}_q^n$, wish to show:

$$\max_{z \in \mathbb{F}_q^n} \mathbb{E}\,|(z+S) \cap \mathbf{C}| \le O\left(\frac{\log n}{\log\log n}\right)$$

where $|\mathbf{C}|\,|S| = q^{n+O(1)}$

Additional Examples

View $\mathbf{C} = \ker(\mathbf{H})$
for uniform $\mathbf{H}$

Linear Hashing

[ADMPT97,DD23,JKZ25]

Given any $S \subseteq \mathbb{F}_q^n$, wish to show:

$$\max_{z \in \mathbb{F}_q^n} \mathbb{E}\,|(z+S) \cap \mathbf{C}| \leq O\left(\frac{\log n}{\log \log n}\right)$$

where $|\mathbf{C}|\,|S| = q^{n+O(1)}$

Additional Examples

View $\mathbf{C} = \ker(\mathbf{H})$
for uniform $\mathbf{H}$

Linear Hashing

[ADMPT97,DD23,JKZ25]

Given any $S \subseteq \mathbb{F}_q^n$, wish to show:

$$\max_{z \in \mathbb{F}_q^n} \mathbb{E}\,|(z+S) \cap \mathbf{C}| \le O\left(\frac{\log n}{\log\log n}\right)$$

where $|\mathbf{C}|\,|S| = q^{n+O(1)}$

Optimal Polynomial Intersection (OPI); Quantum advantage?

[JSW+25,CT25,…,SW26]

Additional Examples

View $\mathbf{C} = \ker(\mathbf{H})$ for uniform $\mathbf{H}$

Linear Hashing

[ADMPT97,DD23,JKZ25]

Given any $S \subseteq \mathbb{F}_q^n$, wish to show:

$$\max_{z \in \mathbb{F}_q^n} \mathbb{E}\,|(z+S) \cap \mathbf{C}| \leq O\left(\frac{\log n}{\log \log n}\right)$$

where $|\mathbf{C}|\,|S| = q^{n+O(1)}$

Optimal Polynomial Intersection (OPI); Quantum advantage?

[JSW+25,CT25,…,SW26]

Given $C \leq \mathbb{F}_q^n$, $S_1, \ldots, S_n \subseteq \mathbb{F}_q$ with

$$|\{c \in C : |\{i \in [n] : c_i \notin S_i\}| \leq \rho n\}| \approx q^{\Omega(n)}$$

find one codeword in above set

General “Discrepancy” Problem

General "Discrepancy" Problem

General setting: have many "tests" T_i and one "object" x

assume $\mathbb{E}[T_i(\mathbf{x})] = \mu$ for all i

General "Discrepancy" Problem

General setting: have many "tests" T_i and one "object" x

assume $\mathbb{E}[T_i(\mathbf{x})] = \mu$ for all i

Question: Can we guarantee existence of some x such that

$$\forall i, T_i(x) \approx \mu?$$

General "Discrepancy" Problem

General setting: have many "tests" T_i and one "object" x

assume $\mathbb{E}[T_i(\mathbf{x})] = \mu$ for all i

Question: Can we guarantee existence of some x such that

$$\forall i,\ T_i(x) \approx \mu?$$

Many variants: Spencer's "Six Standard Deviations Suffice," Beck-Fiala Theorem, low-discrepancy sequences (Van Aardenne-Ehrenfest)

General "Discrepancy" Problem

General setting: have many "tests" T_i and one "object" x

assume $\mathbb{E}[T_i(\mathbf{x})] = \mu$ for all i

Question: Can we guarantee existence of some x such that

$$\forall i, T_i(x) \approx \mu?$$

Many variants: Spencer's "Six Standard Deviations Suffice," Beck-Fiala Theorem, low-discrepancy sequences (Van Aardenne-Ehrenfest)

Our case: natural (?) coding-theoretic variant

Our Results

Theorem 1: Translates

Theorem 1: Translates

Let $B \subseteq \mathbb{F}_q^n$ be a set, let $\beta = 1 - \frac{1}{n} \log_q |B|$, and let $\mathbf{C}$ be RLC of rate $\beta + \varepsilon$.

Theorem 1: Translates

Let $B \subseteq \mathbb{F}_q^n$ be a set, let $\beta = 1 - \frac{1}{n}\log_q |B|$, and let $\mathbf{C}$ be RLC of rate $\beta + \varepsilon$.

Then, with probability $1 - q^{-\Omega(n)}$, one has

$$\forall z \in \mathbb{F}_q^n, \quad |\mathbf{C} \cap (z + B)| = \left(1 \pm q^{\Omega(-\varepsilon n)}\right) \cdot \frac{|\mathbf{C}|\,|B|}{q^n}.$$

Theorem 1: Translates

Let $B \subseteq \mathbb{F}_q^n$ be a set, let $\beta = 1 - \frac{1}{n} \log_q |B|$, and let $\mathbf{C}$ be RLC of rate $\beta + \varepsilon$.

Then, with probability $1 - q^{-\Omega(n)}$, one has

$$\forall z \in \mathbb{F}_q^n, \quad |\mathbf{C} \cap (z + B)| = \left(1 \pm q^{\Omega(-\varepsilon n)}\right) \cdot \frac{|\mathbf{C}|\,|B|}{q^n}.$$

Applies to Hamming balls!
Generalizes covering-radius result

Theorem 2: Pseudorandom Sets

Theorem 2: Pseudorandom Sets

Let $\mathscr{B}$ be a family of sets with $|\mathscr{B}| \leq q^{o(n^2)}$ where each set B is "pseudorandom,"* let $\beta = 1 - \frac{1}{n}\log_q \min\{|B| : B \in \mathscr{B}\}$, and let $\mathbf{C}$ be RLC of rate $\beta + \varepsilon$. Then, with prob. $1 - q^{-\Omega(n)}$,

*$\hat{1}_B(y)$ decays exponentially in $\mathrm{wt}(y)$

Theorem 2: Pseudorandom Sets

Let $\mathscr{B}$ be a family of sets with $|\mathscr{B}| \leq q^{o(n^2)}$ where each set B is "pseudorandom,"* let $\beta = 1 - \frac{1}{n}\log_q \min\{|B| : B \in \mathscr{B}\}$, and let $\mathbf{C}$ be RLC of rate $\beta + \varepsilon$. Then, with prob. $1 - q^{-\Omega(n)}$,

$$\forall B \in \mathscr{B}, \quad |\mathbf{C} \cap B| = \left(1 \pm q^{\Omega(-\varepsilon n)}\right) \cdot \frac{|\mathbf{C}||B|}{q^n}$$

*$\hat{1}_B(y)$ decays exponentially in $\mathrm{wt}(y)$

Theorem 2: Pseudorandom Sets

Let $\mathscr{B}$ be a family of sets with $|\mathscr{B}| \leq q^{o(n^2)}$ where each set B is "pseudorandom,"* let $\beta = 1 - \frac{1}{n}\log_q \min\{|B| : B \in \mathscr{B}\}$, and let $\mathbf{C}$ be RLC of rate $\beta + \varepsilon$. Then, with prob. $1 - q^{-\Omega(n)}$,

$$\forall B \in \mathscr{B},\ \ |\mathbf{C} \cap B| = \left(1 \pm q^{\Omega(-\varepsilon n)}\right) \cdot \frac{|\mathbf{C}||B|}{q^n}$$

Applies to Rectangles over *prime fields*,**
i.e., list-recovery

*$\hat{1}_B(y)$ decays exponentially in $\mathrm{wt}(y)$

**assuming q, ℓ not too big

Comments

Comments

Pseudorandomness can *fail* for rectangles $S_1 \times \cdots \times S_n$ once $\ell \geq \mathrm{char}(q)$ (where each $|S_i| = \ell$)

Comments

Pseudorandomness can *fail* for rectangles $S_1 \times \cdots \times S_n$ once $\ell \geq \mathrm{char}(q)$ (where each $|S_i| = \ell$)

Can use Theorem 2 to handle (approximately) balanced leakage functions over *prime* fields for *very small rates!*

Comments

Pseudorandomness can *fail* for rectangles $S_1 \times \cdots \times S_n$ once $\ell \geq \mathrm{char}(q)$ (where each $|S_i| = \ell$)

Can use Theorem 2 to handle (approximately) balanced leakage functions over *prime* fields for *very small rates!*

Corollary: Secret-sharing scheme associated to RLC C of rate ε is whp leakage-resilient against *balanced* leakages, assuming q is not too large

Comments

Pseudorandomness can *fail* for rectangles $S_1 \times \cdots \times S_n$ once $\ell \geq \mathrm{char}(q)$ (where each $|S_i| = \ell$)

Can use Theorem 2 to handle (approximately) balanced leakage functions over *prime* fields for *very small rates!*

Corollary: Secret-sharing scheme associated to RLC $\mathbf{C}$ of rate ε is whp leakage-resilient against *balanced* leakages, assuming q is not too large

More generally: Theorems work w/ non-negative functions, i.e., *weighted* sets

Proof Ideas (for Theorem 1)

Relative Deviation

Relative Deviation

For set B and linear code C, define ***relative deviation***

$$\delta_{C,B} := \frac{\Pr_{\mathbf{c}\sim C}[\mathbf{c} \in B]}{\Pr_{\mathbf{x}\sim \mathbb{F}_q^n}[\mathbf{x} \in B]} - 1 = \frac{q^n \cdot |C \cap B|}{|C||B|} - 1$$

Relative Deviation

For set B and linear code C, define ***relative deviation***

$$\delta_{C,B} := \frac{\Pr_{\mathbf{c}\sim C}[\mathbf{c} \in B]}{\Pr_{\mathbf{x}\sim \mathbb{F}_q^n}[\mathbf{x} \in B]} - 1 = \frac{q^n \cdot |C \cap B|}{|C||B|} - 1$$

Note that $|\delta_{C,B}| \leq \tau$ is equivalent to

$$(1-\tau)\frac{|C||B|}{q^n} \leq |C \cap B| \leq (1+\tau)\frac{|C||B|}{q^n}$$

Relative Deviation

For set B and linear code C, define ***relative deviation***

$$\delta_{C,B} := \frac{\Pr_{\mathbf{c}\sim C}[\mathbf{c} \in B]}{\Pr_{\mathbf{x}\sim \mathbb{F}_q^n}[\mathbf{x} \in B]} - 1 = \frac{q^n \cdot |C \cap B|}{|C||B|} - 1$$

Note that $|\delta_{C,B}| \leq \tau$ is equivalent to

$$(1-\tau)\frac{|C||B|}{q^n} \leq |C \cap B| \leq (1+\tau)\frac{|C||B|}{q^n}$$

Goal: if $\mathbf{C}$ is RLC of rate $\beta + \varepsilon$, $|\delta_{\mathbf{C},B_z}| \leq q^{-\Omega(\varepsilon n)}$ for all z whp, where $B_z := z + B$

Iterative RLC Construction

Iterative RLC Construction

Sample i.i.d. uniform $\mathbf{u}_1, \ldots, \mathbf{u}_k$ for $k = (\beta + \varepsilon)n$, and define

$$C_0 := \{0\}, \mathbf{C}_i := \mathbf{C}_{i-1} + \langle \mathbf{u}_i \rangle$$

Our goal: understand ***evolution*** of $\delta_{\mathbf{C}_i, B_z}$ as i increases

Iterative RLC Construction

Sample i.i.d. uniform $\mathbf{u}_1, \ldots, \mathbf{u}_k$ for $k = (\beta + \varepsilon)n$, and define

$$C_0 := \{0\}, \mathbf{C}_i := \mathbf{C}_{i-1} + \langle \mathbf{u}_i \rangle$$

Our goal: understand ***evolution*** of $\delta_{\mathbf{C}_i, B_z}$ as i increases

Remark: Procedure considered for list-decoding [GHSZ02,LW20] and linear hashing [JKZ25,Bsh26], but ***only over binary field***

Iterative RLC Construction

Sample i.i.d. uniform $\mathbf{u}_1, \ldots, \mathbf{u}_k$ for $k = (\beta + \varepsilon)n$, and define

$$C_0 := \{0\}, \mathbf{C}_i := \mathbf{C}_{i-1} + \langle \mathbf{u}_i \rangle$$

Our goal: understand ***evolution*** of $\delta_{\mathbf{C}_i, B_z}$ as i increases

Remark: Procedure considered for list-decoding [GHSZ02,LW20] and linear hashing [JKZ25,Bsh26], but ***only over binary field***

[Blinovsky'87] analyzed procedure for covering radius

Initial Relative Deviation

$$\delta_{C,B} = \frac{q^n \cdot |C \cap B|}{|C||B|} - 1$$

Given $z \in \mathbb{F}_q$, we have

$$\delta_{\{0\},B_z} =$$

Initial Relative Deviation

$$\delta_{C,B} = \frac{q^n \cdot |C \cap B|}{|C||B|} - 1$$

Given $z \in \mathbb{F}_q$, we have

$$\delta_{\{0\},B_z} =$$

$0 \in B_z \iff z \in B$

otherwise

Initial Relative Deviation

$\delta_{C,B} = \frac{q^n \cdot |C \cap B|}{|C||B|} - 1$

Given $z \in \mathbb{F}_q$, we have

$$\delta_{\{0\},B_z} = \begin{cases} \frac{q^n}{|B|} - 1 & 0 \in B_z \iff z \in B \\ -1 & \text{otherwise} \end{cases}$$

Initial Relative Deviation

$$\delta_{C,B} = \frac{q^n \cdot |C \cap B|}{|C||B|} - 1$$

Given $z \in \mathbb{F}_q$, we have

$$\delta_{\{0\},B_z} = \begin{cases} \dfrac{q^n}{|B|} - 1 & 0 \in B_z \iff z \in B \\ -1 & \text{otherwise} \end{cases}$$

Initial Relative Deviation

$$\delta_{C,B} = \frac{q^n \cdot |C \cap B|}{|C||B|} - 1$$

Given $z \in \mathbb{F}_q$, we have

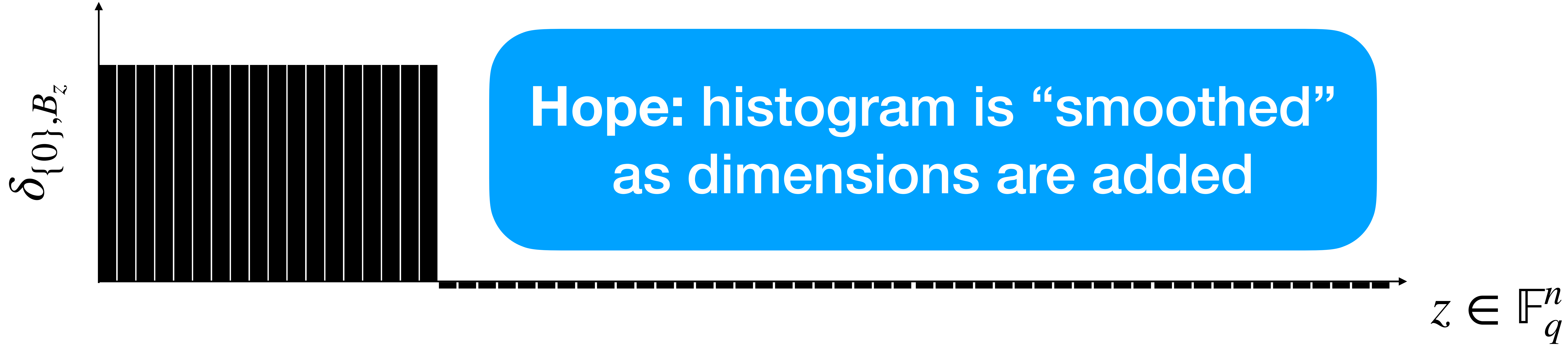
$$\delta_{\{0\},B_z} = \begin{cases} \dfrac{q^n}{|B|} - 1 & 0 \in B_z \iff z \in B \\ -1 & \text{otherwise} \end{cases}$$

Initial Relative Deviation

$$\delta_{C,B} = \frac{q^n \cdot |C \cap B|}{|C||B|} - 1$$

Given $z \in \mathbb{F}_q$, we have

$$\delta_{\{0\},B_z} = \begin{cases} \dfrac{q^n}{|B|} - 1 & 0 \in B_z \iff z \in B \\ -1 & \text{otherwise} \end{cases}$$



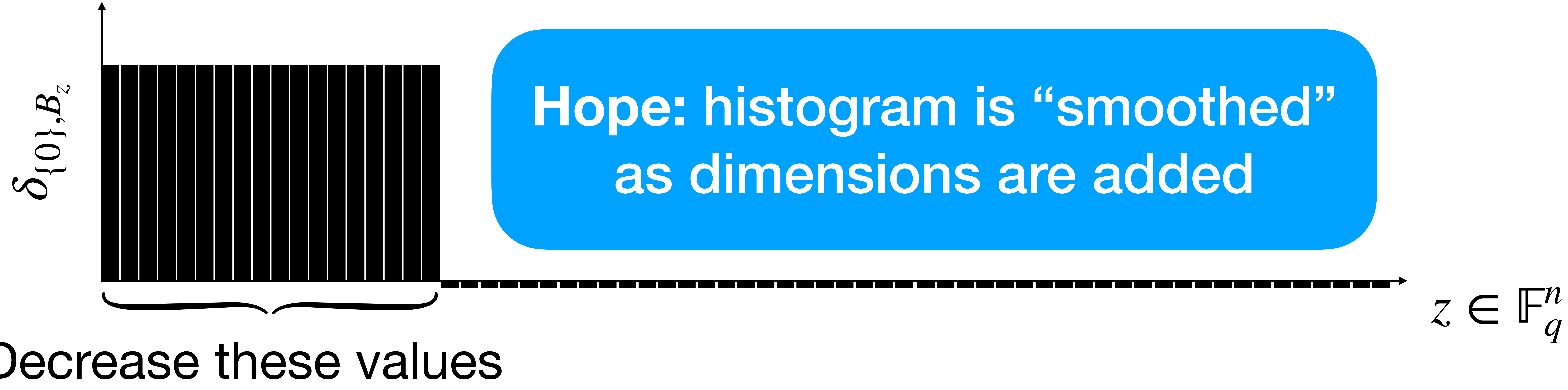
Hope: histogram is "smoothed" as dimensions are added

Initial Relative Deviation

$$\delta_{C,B} = \frac{q^n \cdot |C \cap B|}{|C|\,|B|} - 1$$

Given $z \in \mathbb{F}_q$, we have

$$\delta_{\{0\},B_z} = \begin{cases} \dfrac{q^n}{|B|} - 1 & 0 \in B_z \iff z \in B \\ -1 & \text{otherwise} \end{cases}$$



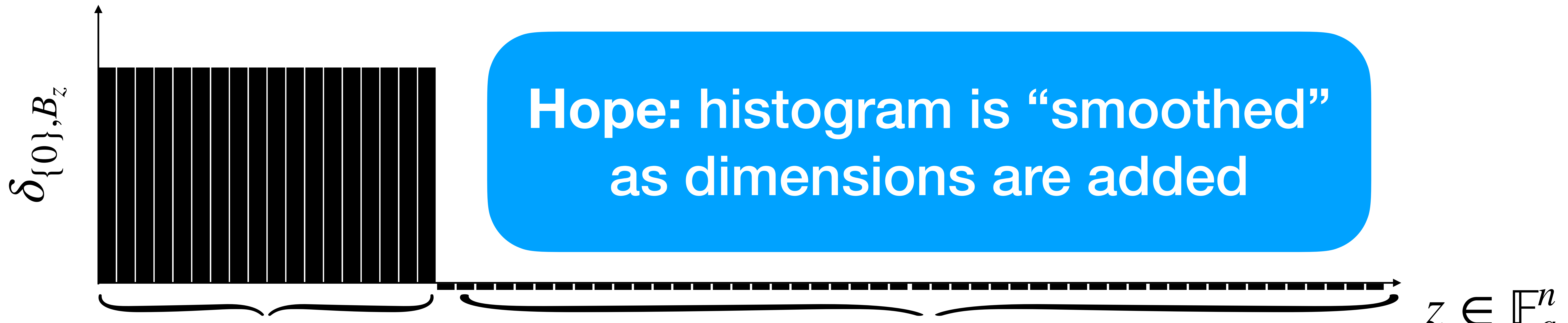
Hope: histogram is "smoothed" as dimensions are added

Initial Relative Deviation

$$\delta_{C,B} = \frac{q^n \cdot |C \cap B|}{|C||B|} - 1$$

Given $z \in \mathbb{F}_q$, we have

$$\delta_{\{0\},B_z} = \begin{cases} \frac{q^n}{|B|} - 1 & 0 \in B_z \iff z \in B \\ -1 & \text{otherwise} \end{cases}$$



Hope: histogram is "smoothed" as dimensions are added

Decrease these values

Increase these values

Expected Behaviour

$$\delta_{C,B} = \frac{q^n \cdot |C \cap B|}{|C||B|} - 1$$

Expected Behaviour

$$\delta_{C,B} = \frac{q^n \cdot |C \cap B|}{|C||B|} - 1$$

Fix some code $C \leq \mathbb{F}_q^n$, let $\mathbf{u} \sim \mathrm{Unif}(\mathbb{F}_q^n)$, and consider

$$\mathbf{C}' = C + \langle \mathbf{u} \rangle = \bigcup_{\lambda \in \mathbb{F}_q} (C + \lambda \mathbf{u})$$

Expected Behaviour

$$\delta_{C,B} = \frac{q^n \cdot |C \cap B|}{|C||B|} - 1$$

Fix some code $C \leq \mathbb{F}_q^n$, let $\mathbf{u} \sim \mathrm{Unif}(\mathbb{F}_q^n)$, and consider

$$\mathbf{C}' = C + \langle \mathbf{u} \rangle = \bigcup_{\lambda \in \mathbb{F}_q} (C + \lambda \mathbf{u})$$

$\lambda = 0$ translate: the “old” deviation

Expected Behaviour

$$\delta_{C,B} = \frac{q^n \cdot |C \cap B|}{|C||B|} - 1$$

Fix some code $C \leq \mathbb{F}_q^n$, let $\mathbf{u} \sim \mathrm{Unif}(\mathbb{F}_q^n)$, and consider

$$\mathbf{C}' = C + \langle \mathbf{u} \rangle = \bigcup_{\lambda \in \mathbb{F}_q} (C + \lambda \mathbf{u})$$

$\lambda = 0$ translate: the “old” deviation

$\lambda \neq 0$ translates: behave “randomly”, so expected deviation $= 0$

Expected Behaviour

$$\delta_{C,B} = \frac{q^n \cdot |C \cap B|}{|C||B|} - 1$$

Fix some code $C \leq \mathbb{F}_q^n$, let $\mathbf{u} \sim \mathrm{Unif}(\mathbb{F}_q^n)$, and consider

$$\mathbf{C}' = C + \langle \mathbf{u} \rangle = \bigcup_{\lambda \in \mathbb{F}_q} (C + \lambda \mathbf{u})$$

$\lambda = 0$ translate: the "old" deviation

$\lambda \neq 0$ translates: behave "randomly", so expected deviation $= 0$

Since dimension increases by one:

Expected Behaviour

$$\delta_{C,B} = \frac{q^n \cdot |C \cap B|}{|C||B|} - 1$$

Fix some code $C \le \mathbb{F}_q^n$, let $\mathbf{u} \sim \mathrm{Unif}(\mathbb{F}_q^n)$, and consider

$$\mathbf{C}' = C + \langle \mathbf{u} \rangle = \bigcup_{\lambda \in \mathbb{F}_q} (C + \lambda \mathbf{u})$$

$\lambda = 0$ translate: the “old” deviation

$\lambda \neq 0$ translates: behave “randomly”, so expected deviation $= 0$

Since dimension increases by one:

$$\mathbb{E}\left[\delta_{\mathbf{C}',B}\right] = \frac{1}{q} \sum_{\lambda \in \mathbb{F}_q} \mathbb{E}\left[\delta_{C+\lambda\mathbf{u},B}\right] = \frac{\delta_{C,B}}{q}.$$

Iterating: get expectation

Iterating: get expectation

So, ideally: with every dimension, deviation divided by q

Iterating: get expectation

So, ideally: with every dimension, deviation divided by q

$$\implies \max_{z \in \mathbb{F}_q^n} \mathbb{E}\left[\delta_{\mathbf{C}_k, B_z}\right] = \max_{z \in \mathbb{F}_q^n} \frac{\mathbb{E}\left[\delta_{\mathbf{C}_{k-1}, B_z}\right]}{q}$$

Iterating: get expectation

So, ideally: with every dimension, deviation divided by q

$$\implies \max_{z \in \mathbb{F}_q^n} \mathbb{E}\left[\delta_{\mathbf{C}_k, B_z}\right] = \max_{z \in \mathbb{F}_q^n} \frac{\mathbb{E}\left[\delta_{\mathbf{C}_{k-1}, B_z}\right]}{q}$$

$$= \cdots = \max_{z \in \mathbb{F}_q^n} \frac{\mathbb{E}\left[\delta_{C_0, B_z}\right]}{q^k}$$

Iterating: get expectation

So, ideally: with every dimension, deviation divided by q

$$\implies \max_{z \in \mathbb{F}_q^n} \mathbb{E}\left[\delta_{\mathbf{C}_k, B_z}\right] = \max_{z \in \mathbb{F}_q^n} \frac{\mathbb{E}\left[\delta_{\mathbf{C}_{k-1}, B_z}\right]}{q}$$

$$= \cdots = \max_{z \in \mathbb{F}_q^n} \frac{\mathbb{E}\left[\delta_{C_0, B_z}\right]}{q^k} = \frac{1}{q^k}\left(\frac{q^n}{|B|} - 1\right)$$

Iterating: get expectation

So, ideally: with every dimension, deviation divided by q

$$\implies \max_{z\in\mathbb{F}_q^n} \mathbb{E}\left[\delta_{\mathbf{C}_k,B_z}\right] = \max_{z\in\mathbb{F}_q^n} \frac{\mathbb{E}\left[\delta_{\mathbf{C}_{k-1},B_z}\right]}{q}$$

$$= \cdots = \max_{z\in\mathbb{F}_q^n} \frac{\mathbb{E}\left[\delta_{C_0,B_z}\right]}{q^k} = \frac{1}{q^k}\left(\frac{q^n}{|B|} - 1\right)$$

With $k = (\beta + \varepsilon)n$, this is $q^{-\varepsilon n}$

Iterating: get expectation

So, ideally: with every dimension, deviation divided by q

$$\implies \max_{z \in \mathbb{F}_q^n} \mathbb{E}\left[\delta_{\mathbf{C}_k, B_z}\right] = \max_{z \in \mathbb{F}_q^n} \frac{\mathbb{E}\left[\delta_{\mathbf{C}_{k-1}, B_z}\right]}{q}$$

$$= \cdots = \max_{z \in \mathbb{F}_q^n} \frac{\mathbb{E}\left[\delta_{C_0, B_z}\right]}{q^k} = \frac{1}{q^k}\left(\frac{q^n}{|B|} - 1\right)$$

With $k = (\beta + \varepsilon)n$, this is $q^{-\varepsilon n}$

Just need "most" steps good; $(1 - \varepsilon/2)$ fraction, say

With high probability?

With high probability?

$\lambda > 0$ small slack

condition on C_{i-1}

Call step i good for z if

$$|\delta_{\mathbf{C}_i, B_z}| \leq \left(\frac{1}{q} + \lambda\right) |\delta_{C_{i-1}, B_z}|$$

With high probability?

$\lambda > 0$ small slack

condition on C_{i-1}

Call step i good for z if

$$|\delta_{\mathbf{C}_i,B_z}| \le \left(\frac{1}{q}+\lambda\right)|\delta_{C_{i-1},B_z}|$$

Via 2nd moment method: can bound

$$\mathbb{P}\left[|\delta_{\mathbf{C}_i,B_z}| \le \left(\frac{1}{q}+\lambda\right)|\delta_{C_{i-1},B_z}|\right] \le q^{-\Omega(\varepsilon n)},$$

and therefore, whp, $|\delta_{\mathbf{C}_k,B_z}| \le q^{-\Omega(\varepsilon n)}$

Problem: union bound…

Problem: union bound…

So, we can argue:

$$\forall z \in \mathbb{F}_q^n, \mathbb{P}\left[|\delta_{\mathbf{C}_k, B_z}| > q^{-\Omega(\varepsilon n)} \right] \leq q^{-\Omega(\varepsilon n)} .$$

Problem: union bound…

So, we can argue:

$$\forall z \in \mathbb{F}_q^n, \mathbb{P}\left[|\delta_{\mathbf{C}_k, B_z}| > q^{-\Omega(\varepsilon n)} \right] \leq q^{-\Omega(\varepsilon n)} \,.$$

However, this is **too weak for union bound**!

Problem: union bound…

So, we can argue:

$$\forall z \in \mathbb{F}_q^n, \mathbb{P}\left[\,|\delta_{\mathbf{C}_k, B_z}| > q^{-\Omega(\varepsilon n)}\right] \leq q^{-\Omega(\varepsilon n)}\,.$$

However, this is **too weak for union bound**!

$$\mathbb{P}\left[\exists z \in \mathbb{F}_q^n \text{ s.t. } |\delta_{\mathbf{C}_k, B_z}| > q^{-\Omega(\varepsilon n)}\right] \leq q^n \cdot q^{-\Omega(\varepsilon n)} \ldots$$

Problem: union bound…

So, we can argue:

$$\forall z \in \mathbb{F}_q^n, \mathbb{P}\left[|\delta_{\mathbf{C}_k, B_z}| > q^{-\Omega(\varepsilon n)} \right] \leq q^{-\Omega(\varepsilon n)} .$$

However, this is **too weak for union bound**!

$$\mathbb{P}\left[\exists z \in \mathbb{F}_q^n \text{ s.t. } |\delta_{\mathbf{C}_k, B_z}| > q^{-\Omega(\varepsilon n)} \right] \leq q^n \cdot q^{-\Omega(\varepsilon n)} \ldots$$

Goal: for step i, find *one event* $\mathcal{G}_i$ such that

Problem: union bound…

So, we can argue:

$$\forall z \in \mathbb{F}_q^n, \mathbb{P}\left[|\delta_{\mathbf{C}_k, B_z}| > q^{-\Omega(\varepsilon n)} \right] \le q^{-\Omega(\varepsilon n)}.$$

However, this is **too weak for union bound**!

$$\mathbb{P}\left[\exists z \in \mathbb{F}_q^n \text{ s.t. } |\delta_{\mathbf{C}_k, B_z}| > q^{-\Omega(\varepsilon n)} \right] \le q^n \cdot q^{-\Omega(\varepsilon n)} \ldots$$

Goal: for step i, find *one event* $\mathcal{G}_i$ such that

$$\mathbb{P}\left[\neg \mathcal{G}_i \right] \le q^{-\Omega(\varepsilon n)}$$

Problem: union bound…

So, we can argue:

$$\forall z \in \mathbb{F}_q^n, \mathbb{P}\left[\,|\,\delta_{\mathbf{C}_k,B_z}| > q^{-\Omega(\varepsilon n)}\right] \leq q^{-\Omega(\varepsilon n)}\,.$$

However, this is **too weak for union bound**!

$$\mathbb{P}\left[\exists z \in \mathbb{F}_q^n \text{ s.t. } |\,\delta_{\mathbf{C}_k,B_z}| > q^{-\Omega(\varepsilon n)}\right] \leq q^n \cdot q^{-\Omega(\varepsilon n)}\ldots$$

Goal: for step i, find *one event* $\mathscr{G}_i$ such that

$$\mathbb{P}\left[\neg \mathscr{G}_i\right] \leq q^{-\Omega(\varepsilon n)}$$

$$\mathbb{P}\left[\exists z \textbf{ s.t. } |\,\delta_{\mathbf{C}_i,B_z}| > \left(\frac{1}{q}+\lambda\right)|\,\delta_{\mathbf{C}_{i-1},B_z}| \wedge \mathscr{G}_i\right] \leq q^{-\Omega(\varepsilon n)}$$

Variance of $\delta_{\mathrm{C}',B}$?

Variance of $\delta_{\mathbf{C}',B}$?

Fix $C \leq \mathbb{F}_q^n$, let $\mathbf{u} \sim \mathrm{Unif}(\mathbb{F}_q^n)$ and put $\mathbf{C}' := C + \langle \mathbf{u} \rangle$

Variance of $\delta_{\mathbf{C}',B}$?

Fix $C \leq \mathbb{F}_q^n$, let $\mathbf{u} \sim \mathrm{Unif}(\mathbb{F}_q^n)$ and put $\mathbf{C}' := C + \langle \mathbf{u} \rangle$

Via direct calculation: $\forall z \in \mathbb{F}_q^n$, get bound

$$\mathrm{Var}(\delta_{\mathbf{C}',B_z}) = \sum_{x,y \in B_z} \left(\mathbb{P}[x, y \in \mathbf{C}'] - \mathbb{P}[x \in \mathbf{C}'] \cdot \mathbb{P}[y \in \mathbf{C}']\right)$$

$$\leq \ldots \leq \delta_{C,B_z - B_z}$$

Variance of $\delta_{\mathbf{C}',B}$?

Fix $C \leq \mathbb{F}_q^n$, let $\mathbf{u} \sim \mathrm{Unif}(\mathbb{F}_q^n)$ and put $\mathbf{C}' := C + \langle \mathbf{u} \rangle$

Via direct calculation: $\forall z \in \mathbb{F}_q^n$, get bound

$$\mathrm{Var}(\delta_{\mathbf{C}',B_z}) = \sum_{x,y \in B_z} \left(\mathbb{P}[x, y \in \mathbf{C}'] - \mathbb{P}[x \in \mathbf{C}'] \cdot \mathbb{P}[y \in \mathbf{C}']\right)$$

$$\leq \ldots \leq \delta_{C,B_z - B_z}$$

Above, $B_z - B_z = \{x - x' : x, x' \in B_z\}$, viewed as ***multiset***. Note:

Variance of $\delta_{\mathbf{C}',B}$?

Fix $C \leq \mathbb{F}_q^n$, let $\mathbf{u} \sim \mathrm{Unif}(\mathbb{F}_q^n)$ and put $\mathbf{C}' := C + \langle \mathbf{u} \rangle$

Via direct calculation: $\forall z \in \mathbb{F}_q^n$, get bound

$$\mathrm{Var}(\delta_{\mathbf{C}',B_z}) = \sum_{x,y \in B_z} \left(\mathbb{P}[x, y \in \mathbf{C}'] - \mathbb{P}[x \in \mathbf{C}'] \cdot \mathbb{P}[y \in \mathbf{C}']\right)$$

$$\leq \ldots \leq \delta_{C,B_z - B_z}$$

Above, $B_z - B_z = \{x - x' : x, x' \in B_z\}$, viewed as ***multiset***. Note:

$$B_z - B_z = (z + B) - (z + B) = B - B$$

Variance of $\delta_{\mathbf{C}',B}$?

Fix $C \leq \mathbb{F}_q^n$, let $\mathbf{u} \sim \mathrm{Unif}(\mathbb{F}_q^n)$ and put $\mathbf{C}' := C + \langle \mathbf{u} \rangle$

Via direct calculation: $\forall z \in \mathbb{F}_q^n$, get bound

$$\mathrm{Var}(\delta_{\mathbf{C}',B_z}) = \sum_{x,y \in B_z} \left(\mathbb{P}[x, y \in \mathbf{C}'] - \mathbb{P}[x \in \mathbf{C}'] \cdot \mathbb{P}[y \in \mathbf{C}'] \right)$$

$$\leq \ldots \leq \delta_{C,B_z - B_z} = \delta_{C,B-B}$$

Above, $B_z - B_z = \{x - x' : x, x' \in B_z\}$, viewed as ***multiset***. Note:

$$B_z - B_z = (z + B) - (z + B) = B - B$$

Variance of $\delta_{\mathbf{C}',B}$?

Fix $C \leq \mathbb{F}_q^n$, let $\mathbf{u} \sim \mathrm{Unif}(\mathbb{F}_q^n)$ and put $\mathbf{C}' := C + \langle \mathbf{u} \rangle$

Via direct calculation: $\forall z \in \mathbb{F}_q^n$, get bound

$$\mathrm{Var}(\delta_{\mathbf{C}',B_z}) = \sum_{x,y \in B_z} \left(\mathbb{P}[x, y \in \mathbf{C}'] - \mathbb{P}[x \in \mathbf{C}'] \cdot \mathbb{P}[y \in \mathbf{C}']\right)$$

$$\leq \ldots \leq \delta_{C,B_z - B_z} = \delta_{C,B-B}$$

Independent of z!

Above, $B_z - B_z = \{x - x' : x, x' \in B_z\}$, viewed as ***multiset***. Note:

$$B_z - B_z = (z + B) - (z + B) = B - B$$

Work with $B - B$!

Using the same sort of analysis, can also show for $B - B$ that

Work with $B - B$!

Using the same sort of analysis, can also show for $B - B$ that

$$|\delta_{\{0\},B-B}| \leq |\delta_{\{0\},B}|$$

Work with $B - B$!

Using the same sort of analysis, can also show for $B - B$ that

$$|\delta_{\{0\},B-B}| \leq |\delta_{\{0\},B}|$$

$$\mathbb{P}[\,|\delta_{\mathbf{C}_i,B-B}| > \left(\frac{1}{q}+\lambda\right)|\delta_{\mathbf{C}_{i-1},B-B}|\,] \leq q^{-\Omega(\varepsilon n)}$$

Work with $B - B$!

Using the same sort of analysis, can also show for $B - B$ that

$|\delta_{\{0\},B-B}| \leq |\delta_{\{0\},B}|$ $\mathbb{P}[|\delta_{\mathbf{C}_i,B-B}| > \left(\frac{1}{q}+\lambda\right)|\delta_{\mathbf{C}_{i-1},B-B}|] \leq q^{-\Omega(\varepsilon n)}$

Thus, we can show that whp, the construction sequence $C_0 = \{0\}, \mathbf{C}_1, \ldots, \mathbf{C}_k$ is ***smooth*** for $B - B$:

$$\forall i = 1,\ldots,k, \quad |\delta_{\mathbf{C}_i,B-B}| \leq \Gamma q^{\beta n - i}$$

Work with $B - B$!

Using the same sort of analysis, can also show for $B - B$ that

$$|\delta_{\{0\},B-B}| \le |\delta_{\{0\},B}|$$

$$\mathbb{P}\left[|\delta_{\mathbf{C}_i,B-B}| > \left(\frac{1}{q}+\lambda\right)|\delta_{\mathbf{C}_{i-1},B-B}|\right] \le q^{-\Omega(\varepsilon n)}$$

Thus, we can show that whp, the construction sequence $C_0 = \{0\}, \mathbf{C}_1, \ldots, \mathbf{C}_k$ is ***smooth*** for $B - B$:

$$\beta = 1 - \frac{1}{n}\log_q|B|$$

$$\forall i = 1,\ldots,k, \quad |\delta_{\mathbf{C}_i,B-B}| \le \Gamma\, q^{\beta n - i}$$

Work with $B - B$!

Using the same sort of analysis, can also show for $B - B$ that

$$|\delta_{\{0\},B-B}| \leq |\delta_{\{0\},B}|$$

$$\mathbb{P}[\,|\delta_{\mathbf{C}_i,B-B}| > \left(\tfrac{1}{q}+\lambda\right)|\delta_{\mathbf{C}_{i-1},B-B}|\,] \leq q^{-\Omega(\varepsilon n)}$$

Thus, we can show that whp, the construction sequence $C_0 = \{0\}, \mathbf{C}_1, \ldots, \mathbf{C}_k$ is ***smooth*** for $B - B$:

$$\beta = 1 - \tfrac{1}{n}\log_q|B|$$

$$\forall i = 1,\ldots,k, \quad |\delta_{\mathbf{C}_i,B-B}| \leq \Gamma\, q^{\beta n - i}$$

Think

$$\Gamma = q^{\Omega(\varepsilon n)}$$

Smoothness for each B_z?

Smoothness for each B_z?

Our hope is now to argue that, when $B - B$ is smooth, ***also*** B_z is ***smooth:***

$$\forall i = 0,1,\ldots,k, \quad |\delta_{\mathbf{C}_i, B_z}| \leq \Lambda\, q^{\beta n - i}$$

Smoothness for each B_z?

Our hope is now to argue that, when $B - B$ is smooth, ***also*** B_z is ***smooth:***

$$\forall i = 0,1,\ldots,k, \quad |\delta_{\mathbf{C}_i, B_z}| \leq \Lambda\, q^{\beta n - i}$$

Think

$$\Lambda = \sqrt{\Gamma}$$

Smoothness for each B_z?

Our hope is now to argue that, when $B - B$ is smooth, ***also*** B_z is ***smooth:***

$$\forall i = 0,1,\ldots,k, \quad |\delta_{\mathbf{C}_i, B_z}| \leq \Lambda\, q^{\beta n - i}$$

Think

$$\Lambda = \sqrt{\Gamma}$$

with ***very high probability*** $1 - q^{-\Omega_\varepsilon(n^2)}$

Smoothness for each B_z?

Our hope is now to argue that, when $B - B$ is smooth, ***also*** B_z is ***smooth:***

$$\forall i = 0,1,\ldots,k, \quad |\delta_{\mathbf{C}_i, B_z}| \leq \Lambda\, q^{\beta n - i}$$

Think $\Lambda = \sqrt{\Gamma}$

with ***very high probability*** $1 - q^{-\Omega_\varepsilon(n^2)}$

Can then afford union bound over $z \in \mathbb{F}_q^n$!

Smoothness for each B_z?

Our hope is now to argue that, when $B - B$ is smooth, ***also*** B_z is ***smooth:***

$$\forall i = 0,1,\ldots,k, \quad |\delta_{\mathbf{C}_i,B_z}| \le \Lambda\, q^{\beta n - i}$$

Think

$$\Lambda = \sqrt{\Gamma}$$

with ***very high probability*** $1 - q^{-\Omega_\varepsilon(n^2)}$

Can then afford union bound over $z \in \mathbb{F}_q^n$!

$$\mathbb{P}\left[\,|\delta_{\mathbf{C}_i,B_z}| > \left(\frac{1}{q}+\lambda\right)|\delta_{C_{i-1},B_z}|\,\right] \le \frac{\mathrm{Var}(\delta_{\mathbf{C}_i,B_z})}{\lambda^2 \cdot \delta^2_{C_{i-1},B_z}}$$

Smoothness for each B_z?

Our hope is now to argue that, when $B - B$ is smooth, ***also*** B_z is ***smooth:***

$$\forall i = 0,1,\ldots,k, \quad |\delta_{\mathbf{C}_i,B_z}| \leq \Lambda\, q^{\beta n - i}$$

Think $\Lambda = \sqrt{\Gamma}$

with ***very high probability*** $1 - q^{-\Omega_\varepsilon(n^2)}$

Can then afford union bound over $z \in \mathbb{F}_q^n$!

$$\mathbb{P}\left[|\delta_{\mathbf{C}_i,B_z}| > \left(\tfrac{1}{q}+\lambda\right)|\delta_{C_{i-1},B_z}|\right] \leq \frac{\mathrm{Var}(\delta_{\mathbf{C}_i,B_z})}{\lambda^2 \cdot \delta^2_{C_{i-1},B_z}} \leq \frac{\delta_{C_{i-1},B-B}}{\lambda^2 \cdot \delta^2_{C_{i-1},B_z}}$$

Smoothness Transfer Lemma

Smoothness Transfer Lemma

Claim*: for any $z \in \mathbb{F}_q^n$,

$$\mathbb{P}[B - B \text{ smooth and } B_z \text{ not smooth}] \leq q^{-\Omega(n^2)}$$

Smoothness Transfer Lemma

Claim*: for any $z \in \mathbb{F}_q^n$,

$$\mathbb{P}[B - B \text{ smooth and } B_z \text{ not smooth}] \leq q^{-\Omega(n^2)}$$

Idea: Call step i *bad* if (a) $|\delta_{\mathbf{C}_i, B_z}| > \left(\frac{1}{q} + \lambda\right)|\delta_{C_{i-1}, B_z}|$ and (b) $|\delta_{C_{i-1}, B_z}|$ "large"

Smoothness Transfer Lemma

Claim*: for any $z \in \mathbb{F}_q^n$,

$$\mathbb{P}[B - B \text{ smooth and } B_z \text{ not smooth}] \leq q^{-\Omega(n^2)}$$

Idea: Call step i *bad* if (a) $|\delta_{\mathbf{C}_i, B_z}| > \left(\frac{1}{q}+\lambda\right)|\delta_{C_{i-1}, B_z}|$ and (b) $|\delta_{C_{i-1}, B_z}|$ "large"

$$\mathbb{P}\left[\text{step } i \text{ bad} \wedge B - B \text{ smooth}\right] \leq \frac{\delta_{C_{i-1}, B-B}}{\lambda^2 \cdot \delta_{C_{i-1}, B_z}} \leq q^{-\Omega(\varepsilon n)}$$

Smoothness Transfer Lemma

Claim*: for any $z \in \mathbb{F}_q^n$,

$$\mathbb{P}[B - B \text{ smooth and } B_z \text{ not smooth}] \leq q^{-\Omega(n^2)}$$

Idea: Call step i *bad* if (a) $|\delta_{\mathbf{C}_i,B_z}| > \left(\frac{1}{q}+\lambda\right)|\delta_{C_{i-1},B_z}|$ and (b) $|\delta_{C_{i-1},B_z}|$ "large"

Numerator: small since $B - B$ smooth

$$\mathbb{P}\left[\text{step } i \text{ bad} \wedge B - B \text{ smooth}\right] \leq \frac{\delta_{C_{i-1},B-B}}{\lambda^2 \cdot \delta_{C_{i-1},B_z}} \leq q^{-\Omega(\varepsilon n)}$$

Smoothness Transfer Lemma

Claim*: for any $z \in \mathbb{F}_q^n$,

$$\mathbb{P}[B - B \text{ smooth and } B_z \text{ not smooth}] \leq q^{-\Omega(n^2)}$$

Idea: Call step i *bad* if (a) $|\delta_{\mathbf{C}_i, B_z}| > \left(\frac{1}{q} + \lambda\right) |\delta_{C_{i-1}, B_z}|$ and (b) $|\delta_{C_{i-1}, B_z}|$ "large"

Numerator: small since $B - B$ smooth

$$\mathbb{P}\left[\text{step } i \text{ bad} \wedge B - B \text{ smooth}\right] \leq \frac{\delta_{C_{i-1}, B-B}}{\lambda^2 \cdot \delta_{C_{i-1}, B_z}} \leq q^{-\Omega(\varepsilon n)}$$

Denominator: use second condition

Smoothness Transfer Lemma

Smoothness Transfer Lemma

Claim*: for any $z \in \mathbb{F}_q^n$,

$$\mathbb{P}[B - B \text{ smooth and } B_z \text{ not smooth}] \leq q^{-\Omega(n^2)}$$

Smoothness Transfer Lemma

Claim*: for any $z \in \mathbb{F}_q^n$,

$$\mathbb{P}[B - B \text{ smooth and } B_z \text{ not smooth}] \leq q^{-\Omega(n^2)}$$

Idea (con't): For B_z to *not be* smooth, need $\Omega(\varepsilon n)$ ***bad steps***

Smoothness Transfer Lemma

Claim*: for any $z \in \mathbb{F}_q^n$,

$$\mathbb{P}[B - B \text{ smooth and } B_z \text{ not smooth}] \leq q^{-\Omega(n^2)}$$

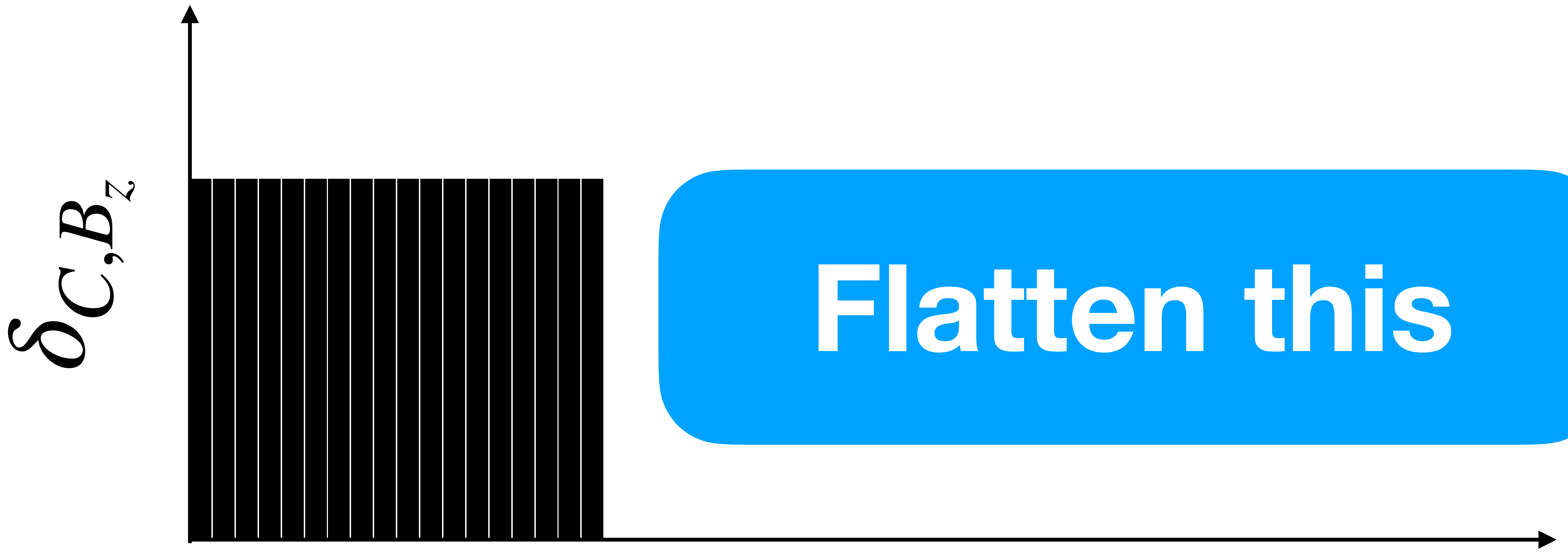
Idea (con't): For B_z to *not be* smooth, need $\Omega(\varepsilon n)$ ***bad steps***

Thus,

$$\mathbb{P}[\text{enough bad steps}] \leq (q^{-\Omega(\varepsilon n)})^{\Omega(\varepsilon n)} = q^{-\Omega(\varepsilon^2 n^2)}.$$

Summary

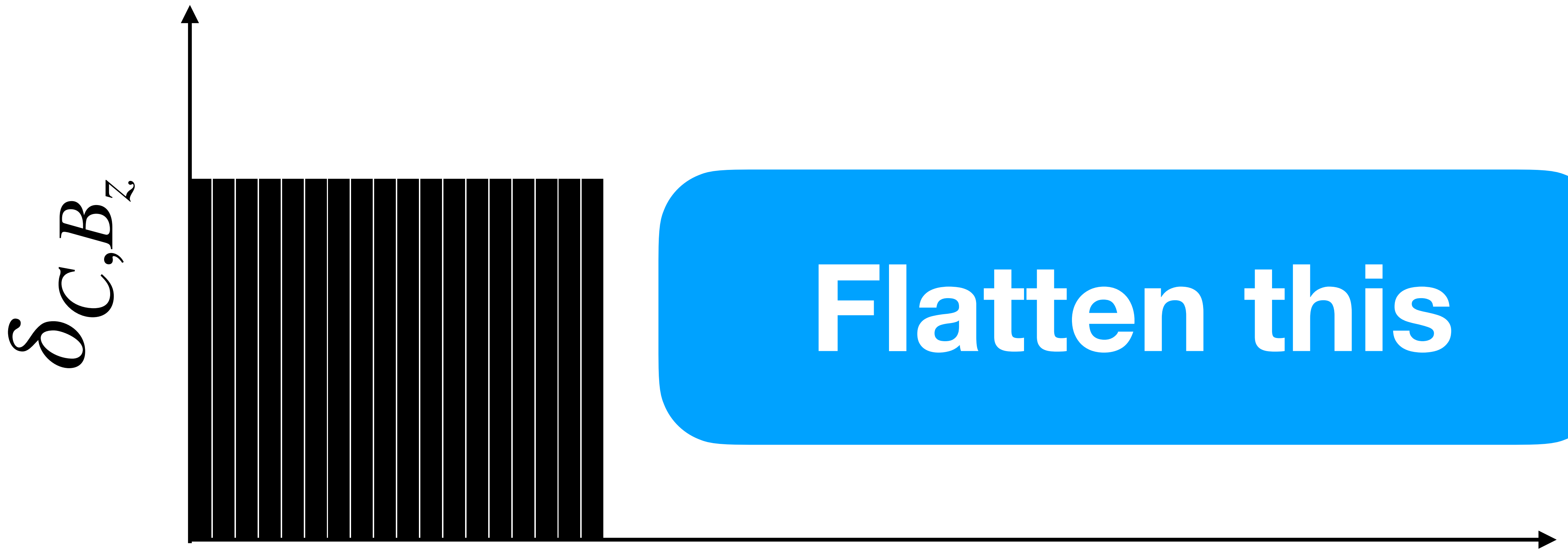
Goal



Flatten this

Summary

Goal



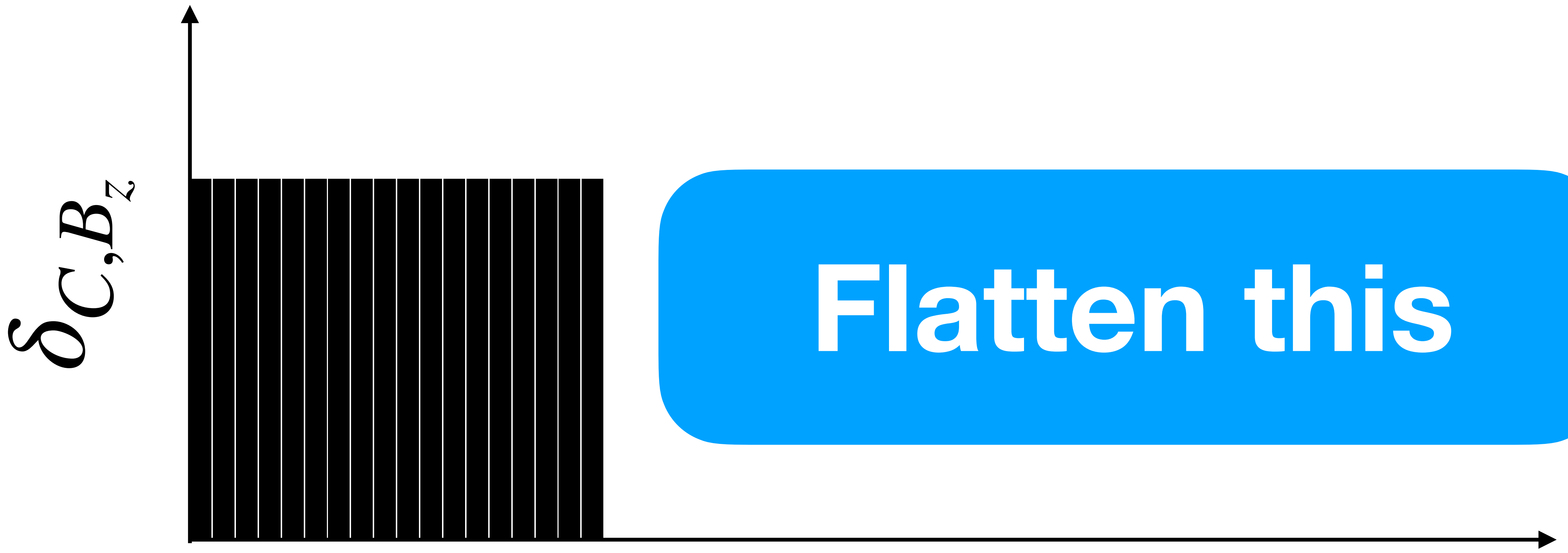
Flatten this

Bound with $B - B$

$$\mathrm{Var}(\delta_{\mathbf{C}_i,B_z}) \lesssim \delta_{C_{i-1},B-B}$$

Summary

Goal



Flatten this

Bound with $B - B$

$$\mathrm{Var}(\delta_{\mathbf{C}_i,B_z}) \lesssim \delta_{C_{i-1},B-B}$$

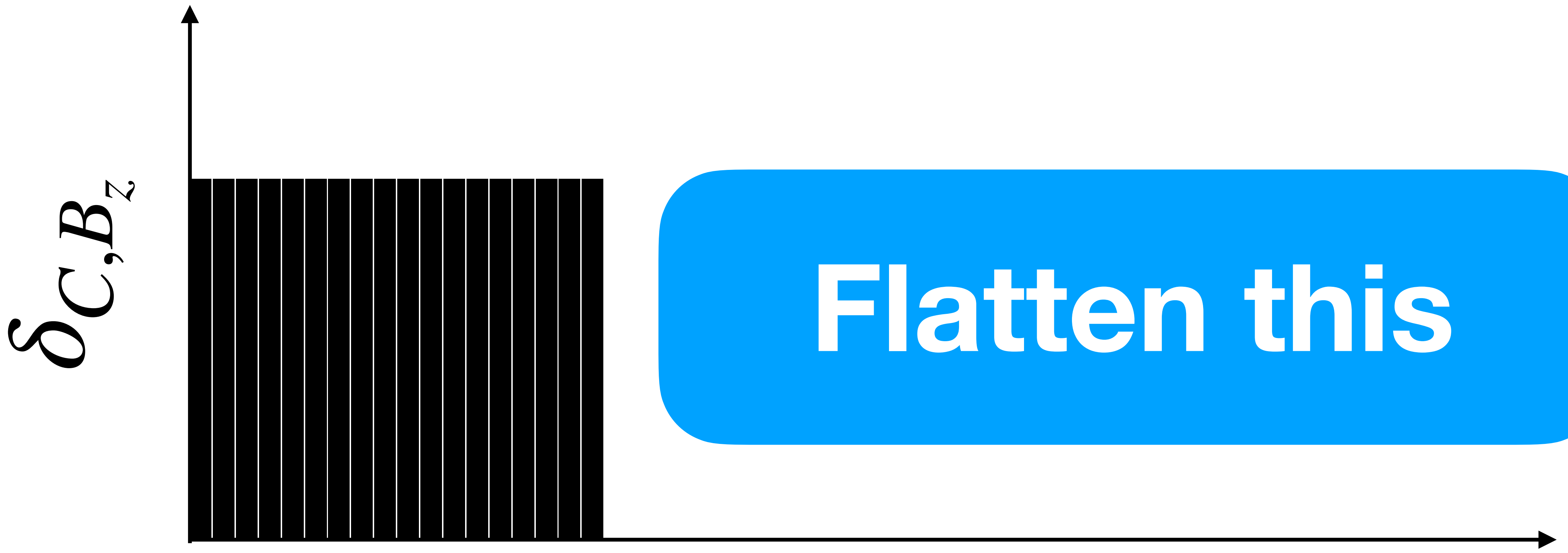
Summary

$B - B$ likely smooth

$$\delta_{\mathbf{C}_i,B-B} \lesssim q^{\beta n-i}$$

Summary

Goal



Flatten this

Bound with $B-B$

$$\mathrm{Var}(\delta_{\mathbf{C}_i,B_z}) \lesssim \delta_{C_{i-1},B-B}$$

$B-B$ likely smooth

$$\delta_{\mathbf{C}_i,B-B} \lesssim q^{\beta n-i}$$

Transfer Smoothness

$\mathbb{P}[B-B$ smooth but $\exists z$ s.t. B_z not smooth$] \leq q^n \cdot q^{-\Omega(n^2)}$

A Word About Theorem 2

Theorem 2: Pseudorandom Sets

Let $\mathscr{B}$ be a family of sets with $|\mathscr{B}| \leq q^{o(n^2)}$ where each set B is "pseudorandom,"* let $\beta = 1 - \frac{1}{n}\log_q \min\{|B| : B \in \mathscr{B}\}$, and let $\mathbf{C}$ be RLC of rate $\beta + \varepsilon$. Then, with prob. $1 - q^{-\Omega(n)}$,

$$\forall B \in \mathscr{B}, \quad |\mathbf{C} \cap B| = \left(1 \pm q^{\Omega(-\varepsilon n)}\right) \cdot \frac{|\mathbf{C}||B|}{q^n}$$

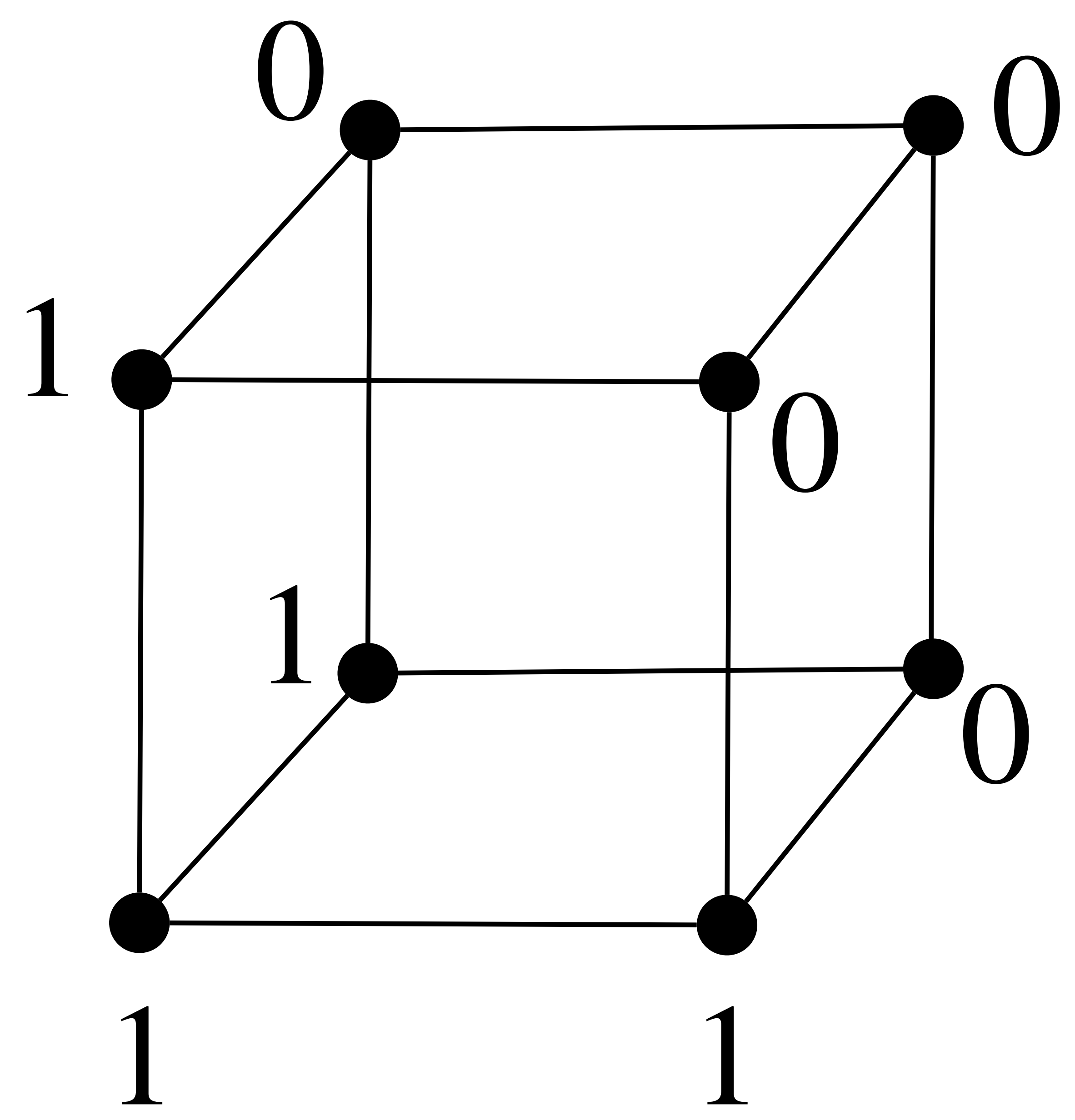
Applies to Rectangles over *prime fields*,**
i.e., list-recovery

*$\hat{1}_B(y)$ decays exponentially in $\mathrm{wt}(y)$

**assuming q, ℓ not too big

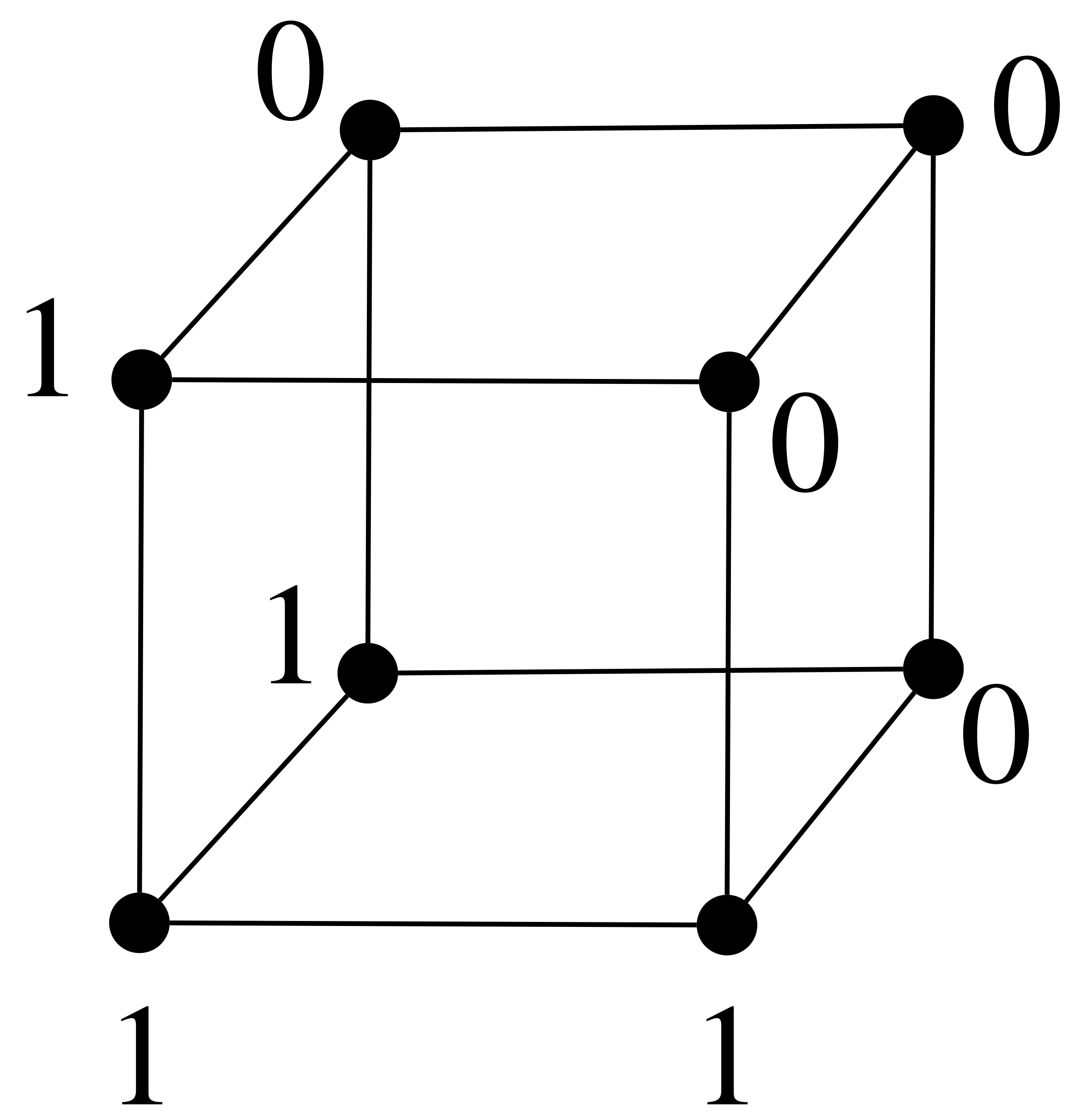
$B - B =$ **more uniform**

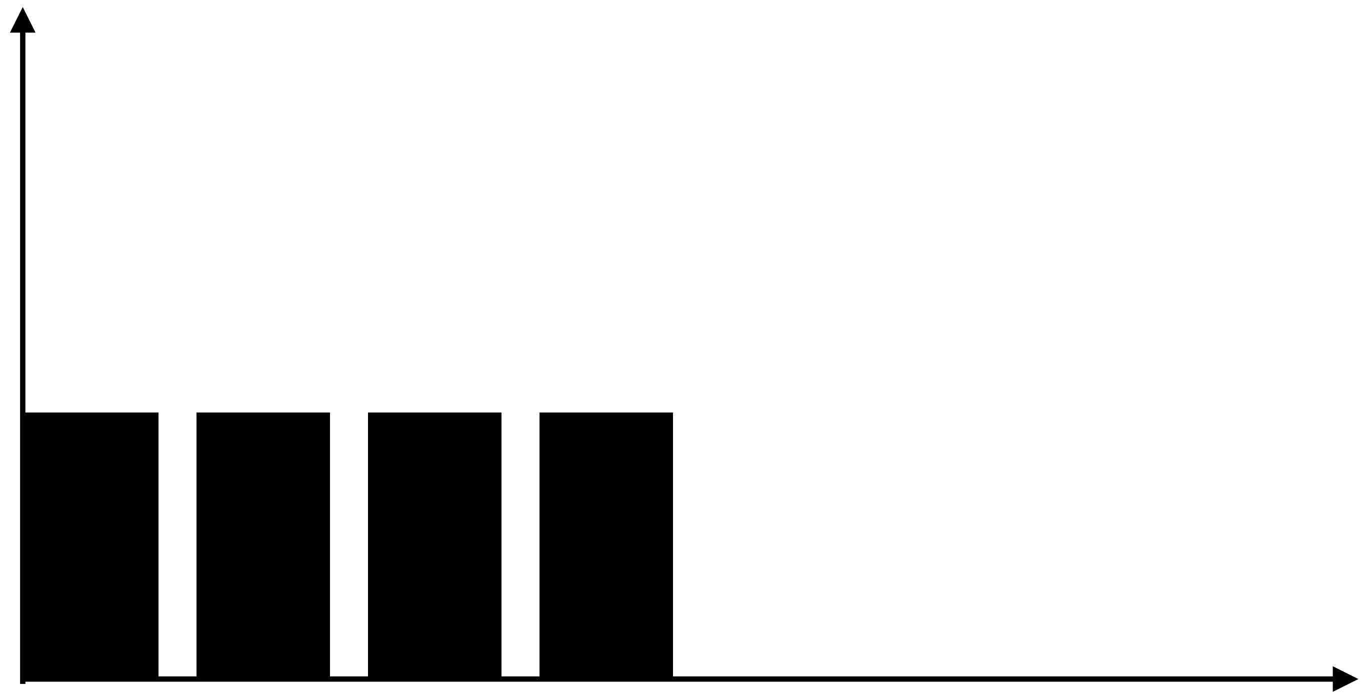
$B_{1/3} = \{000, 001, 010, 100\}$



$B - B =$ more uniform

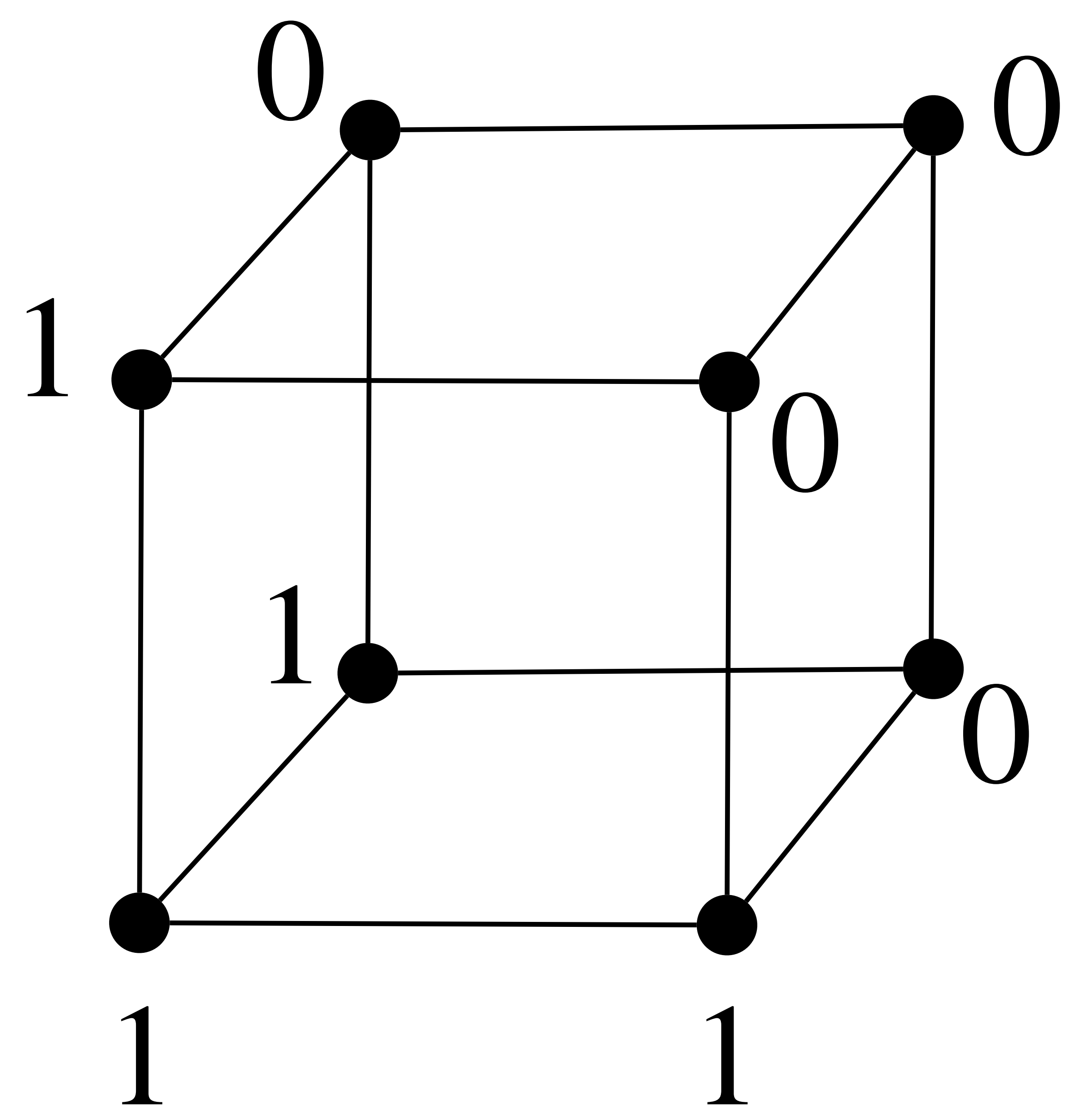
$$B_{1/3} = \{000, 001, 010, 100\}$$

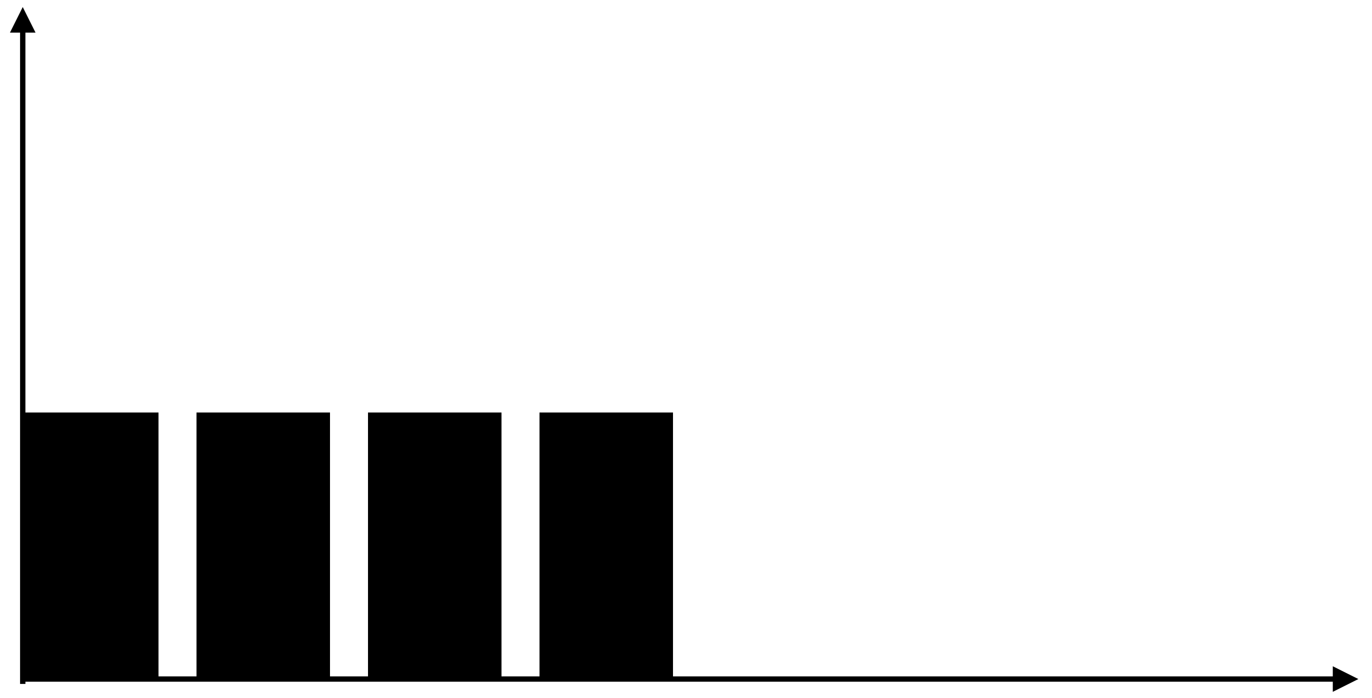




$B - B =$ more uniform

$B_{1/3} = \{000, 001, 010, 100\}$

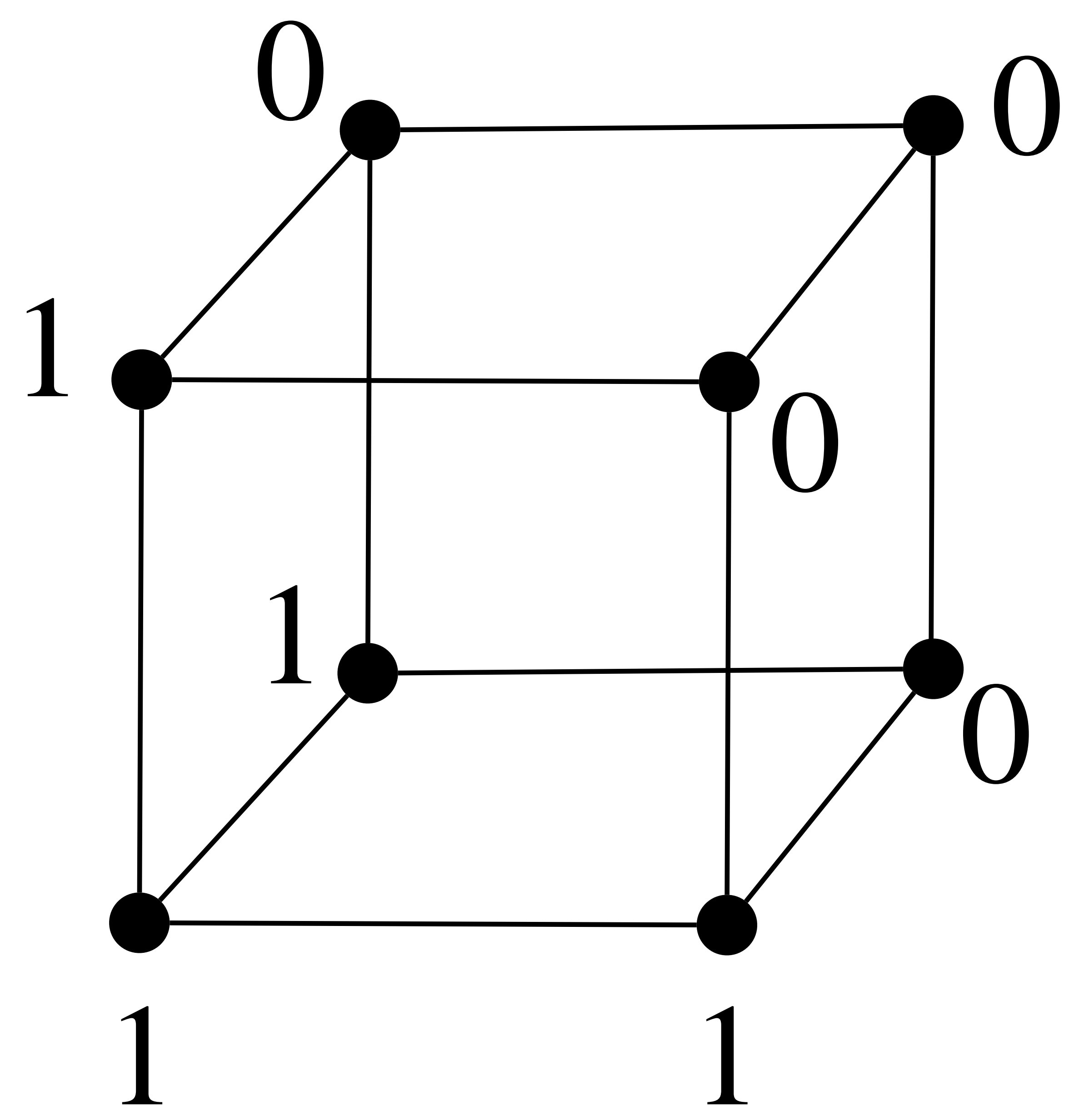


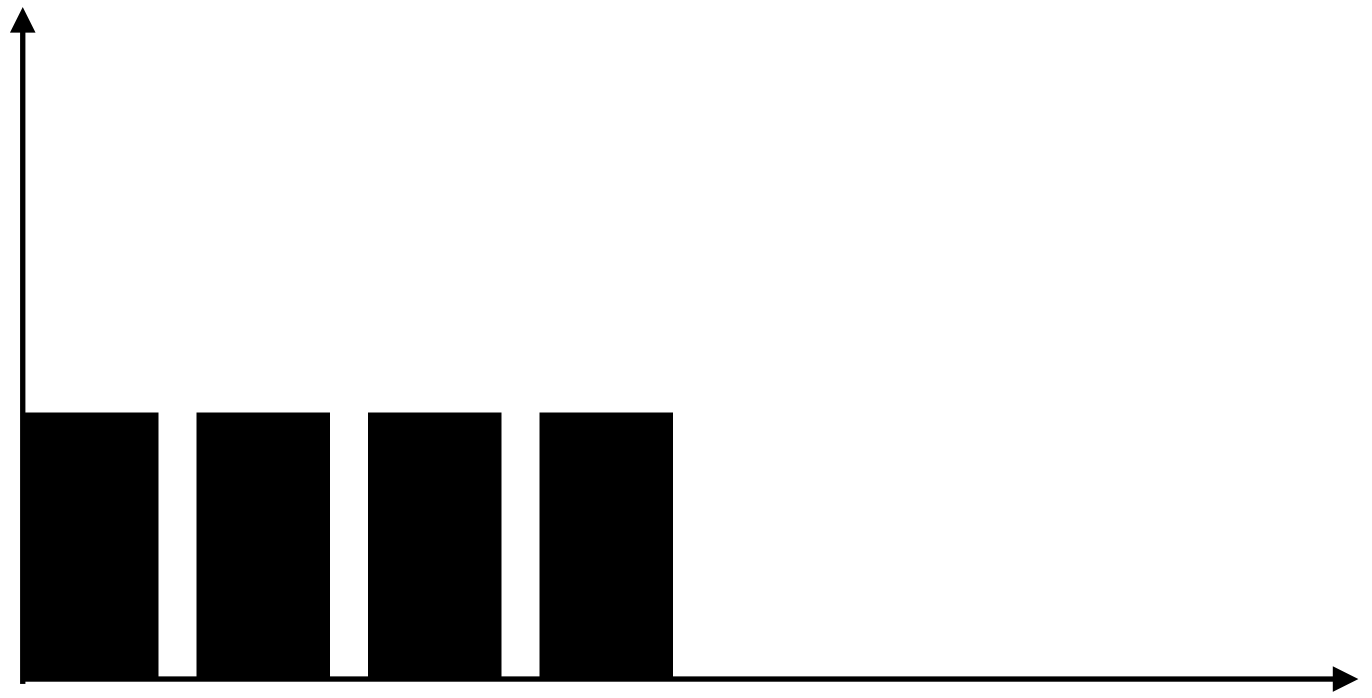


$B_{1/3} - B_{1/3} =$

$B - B =$ more uniform

$B_{1/3} = \{000, 001, 010, 100\}$





$B_{1/3} - B_{1/3} =$

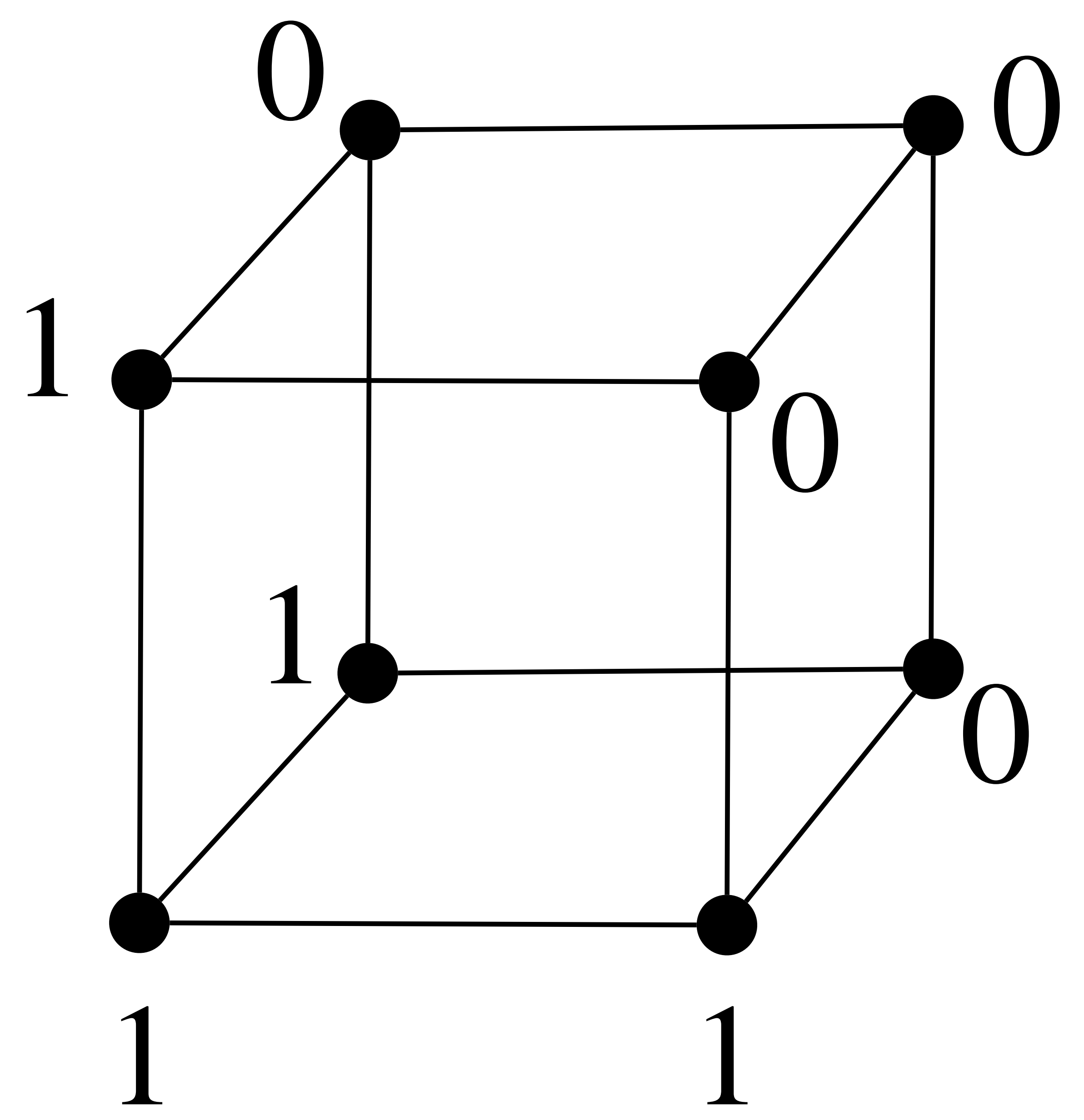
$\{000, 000, 000, 000,$

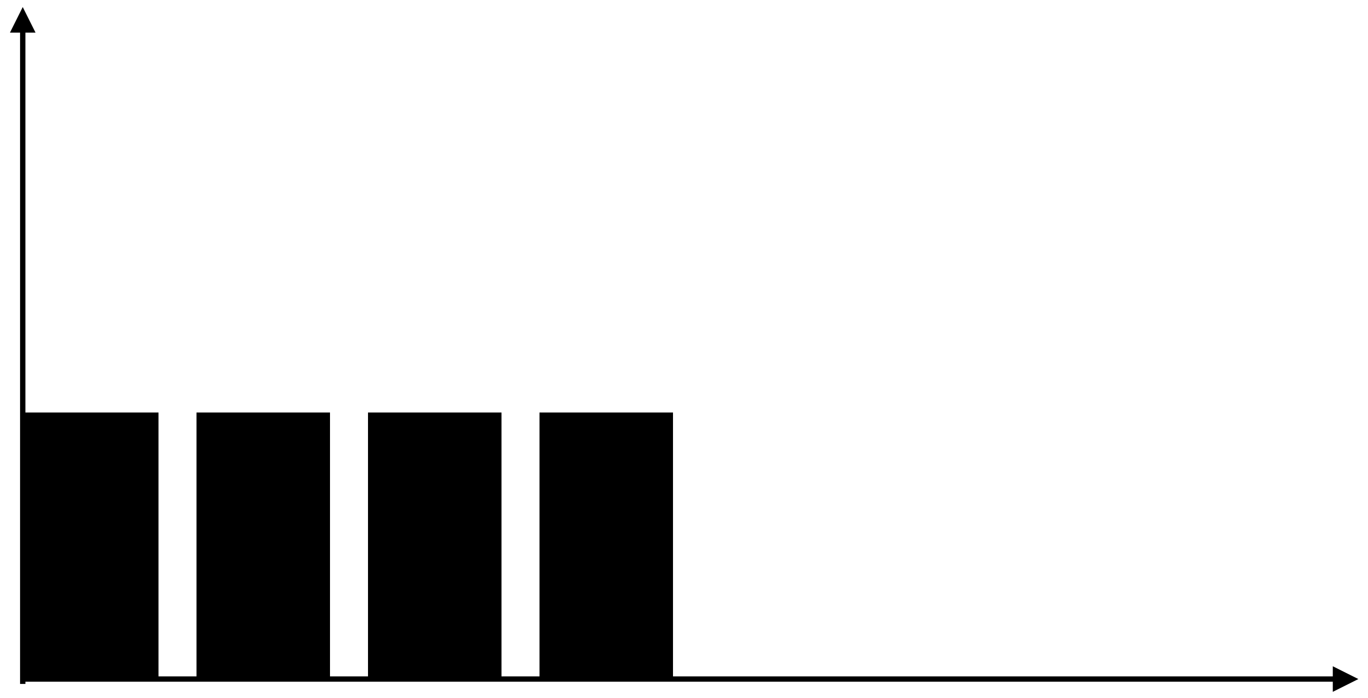
$001, 010, 100,$

$011, 101, 110\}$

$B - B =$ more uniform

$B_{1/3} = \{000, 001, 010, 100\}$



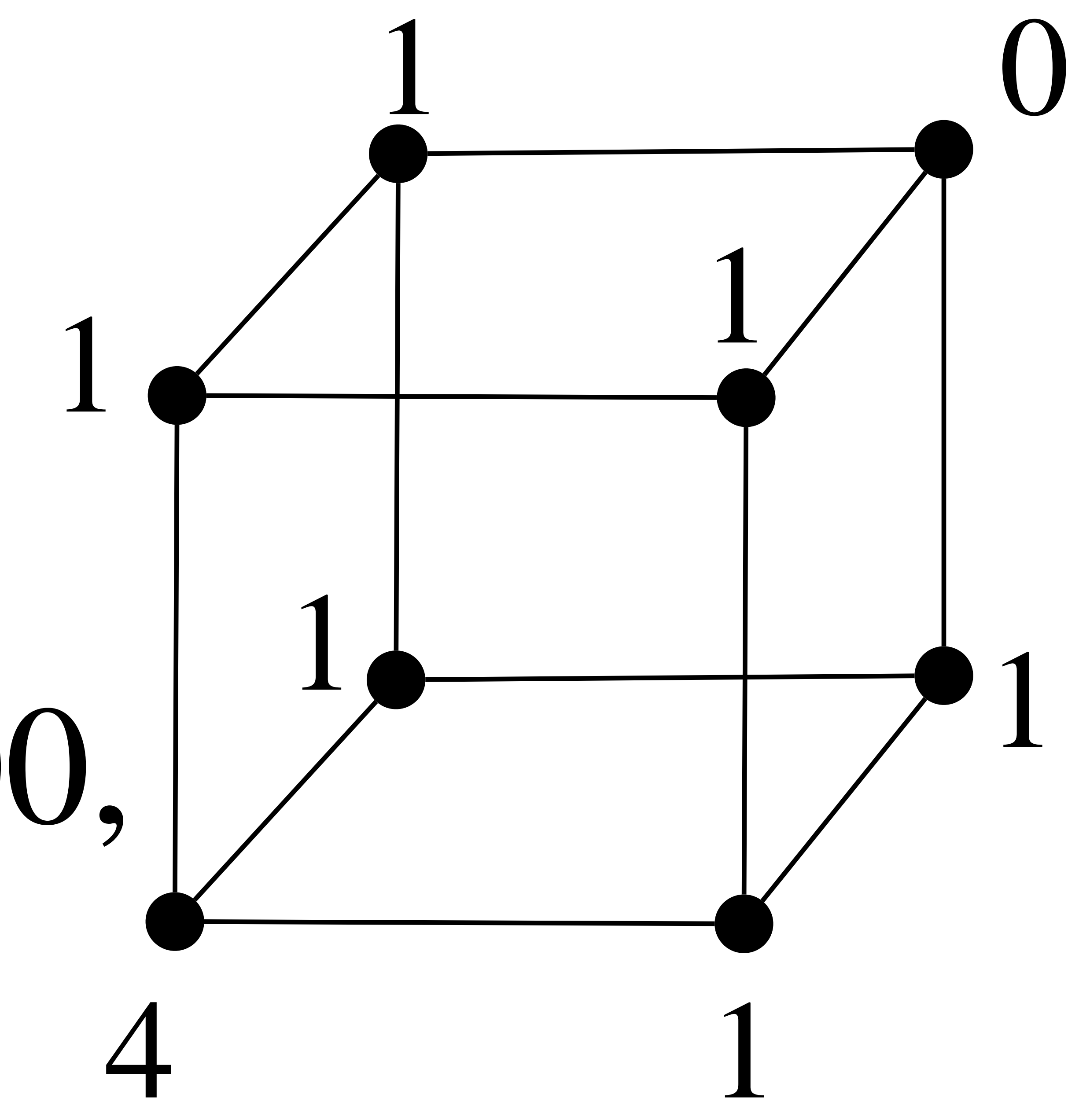


$B_{1/3} - B_{1/3} =$

$\{000, 000, 000, 000,$

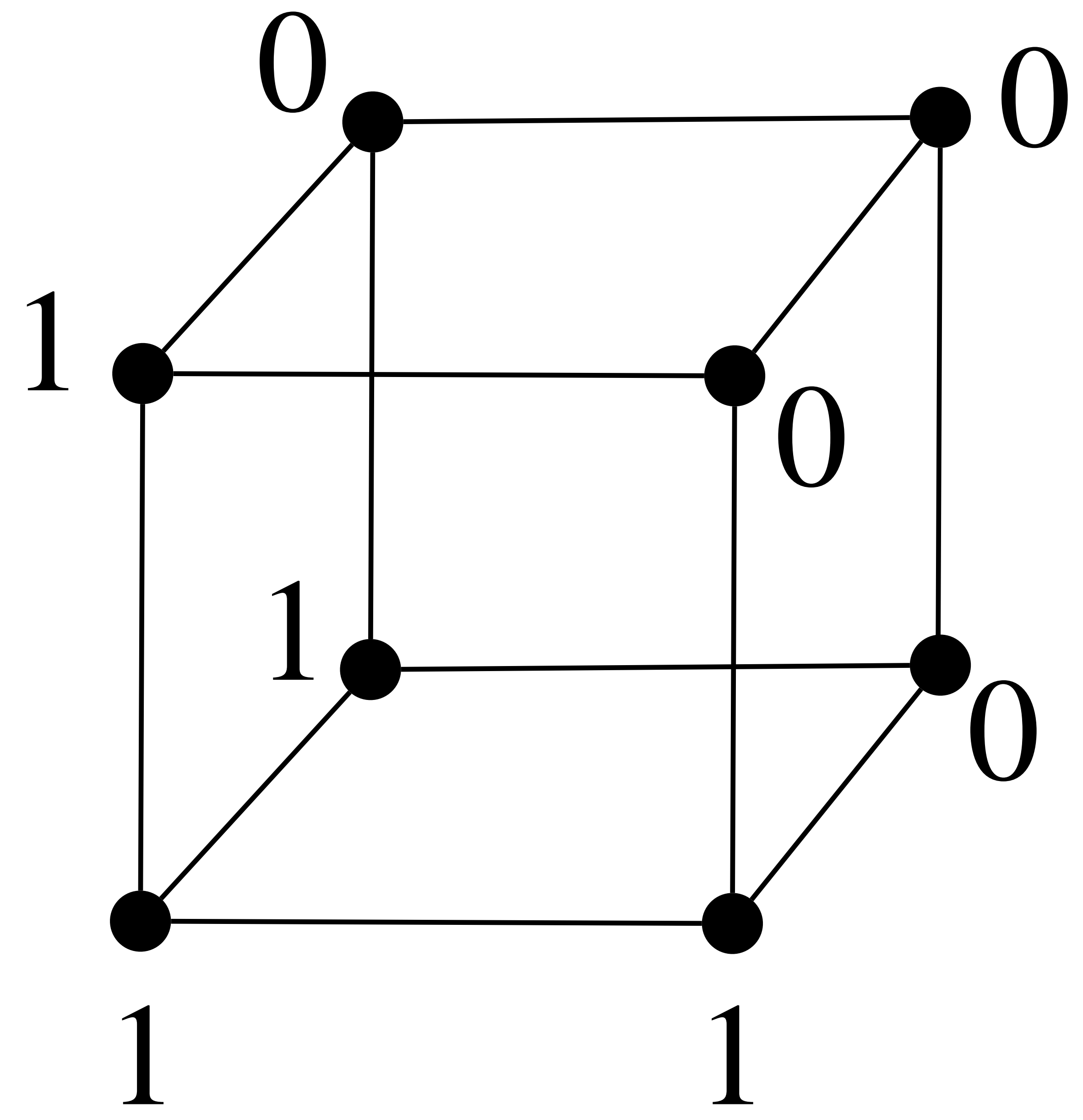
$001, 010, 100,$

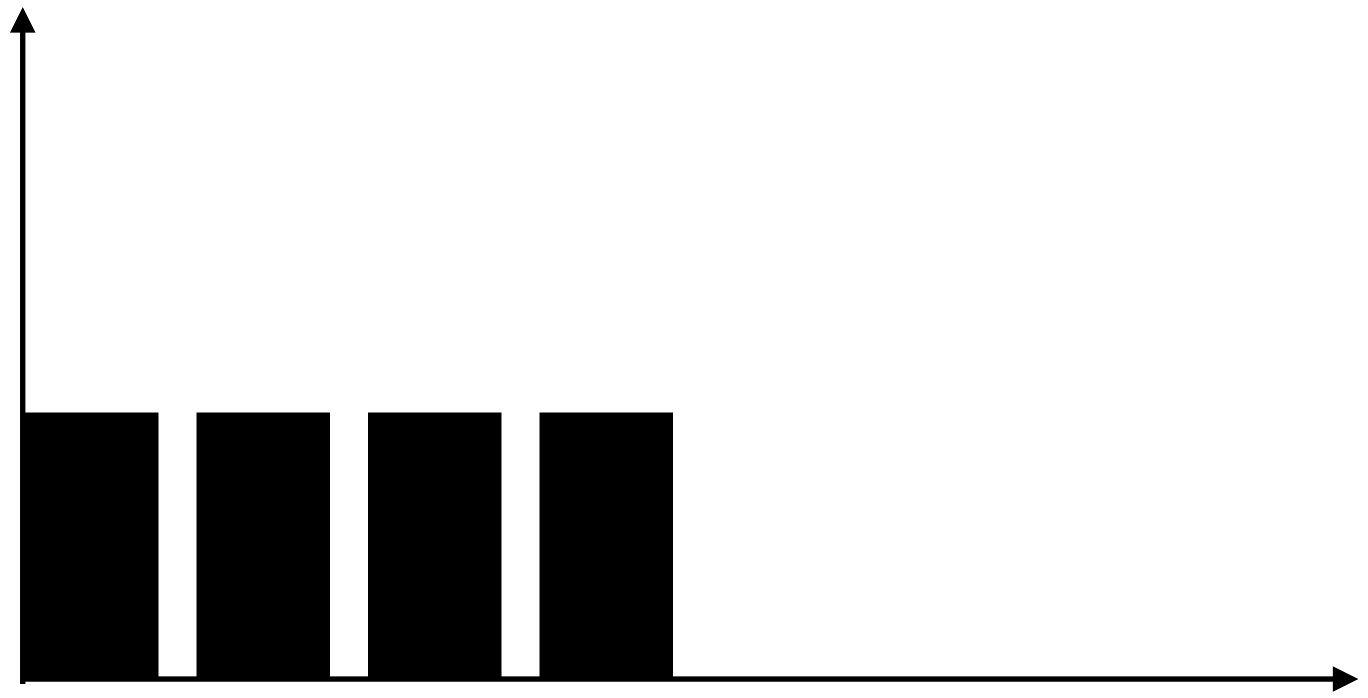
$011, 101, 110\}$



$B - B =$ more uniform

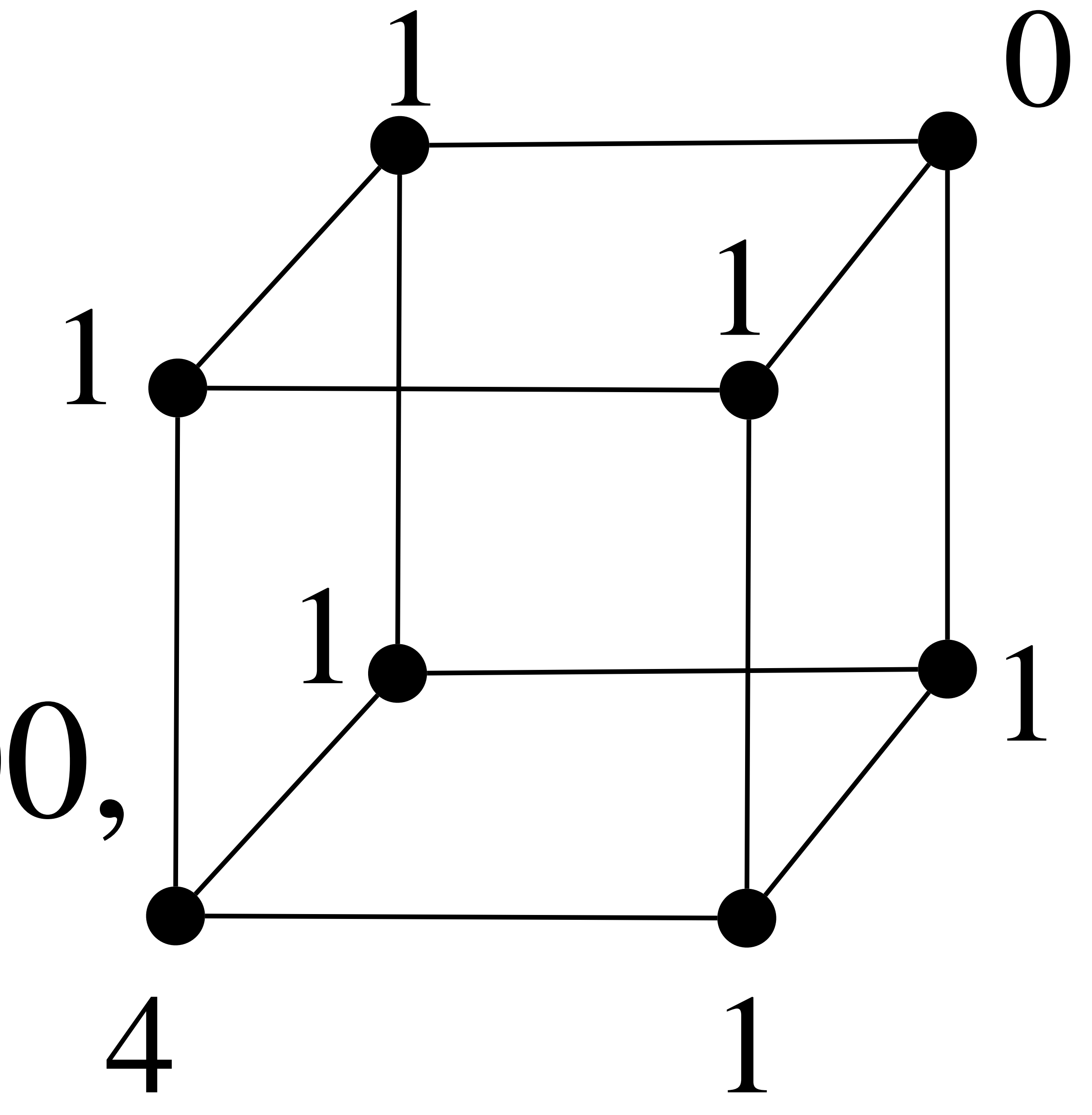
$$B_{1/3} = \{000,001,010,100\}$$





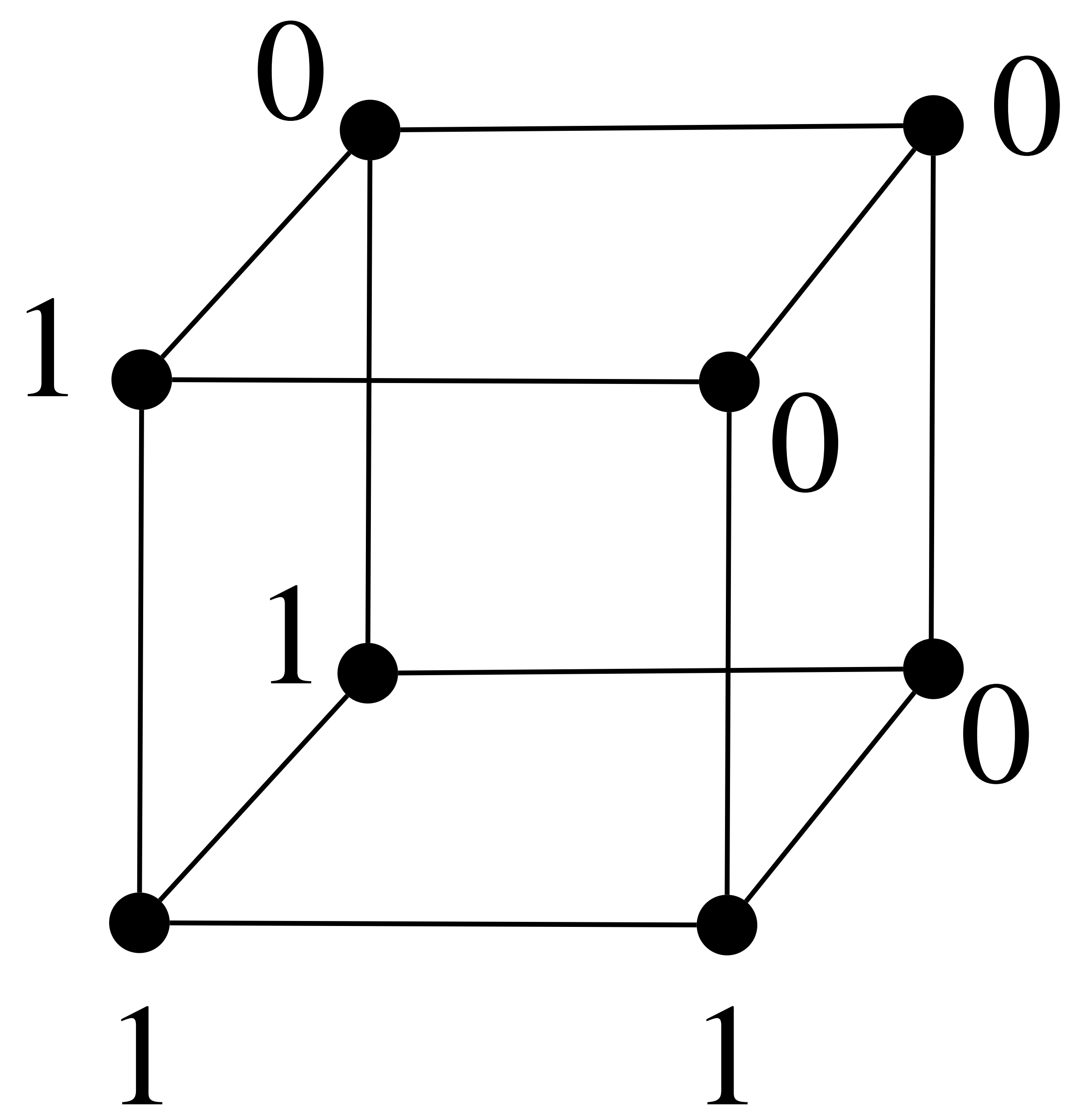
$$B_{1/3} - B_{1/3} =$$

$$\{000,000,000,000,$$
$$001,010,100,$$
$$011,101,110\}$$



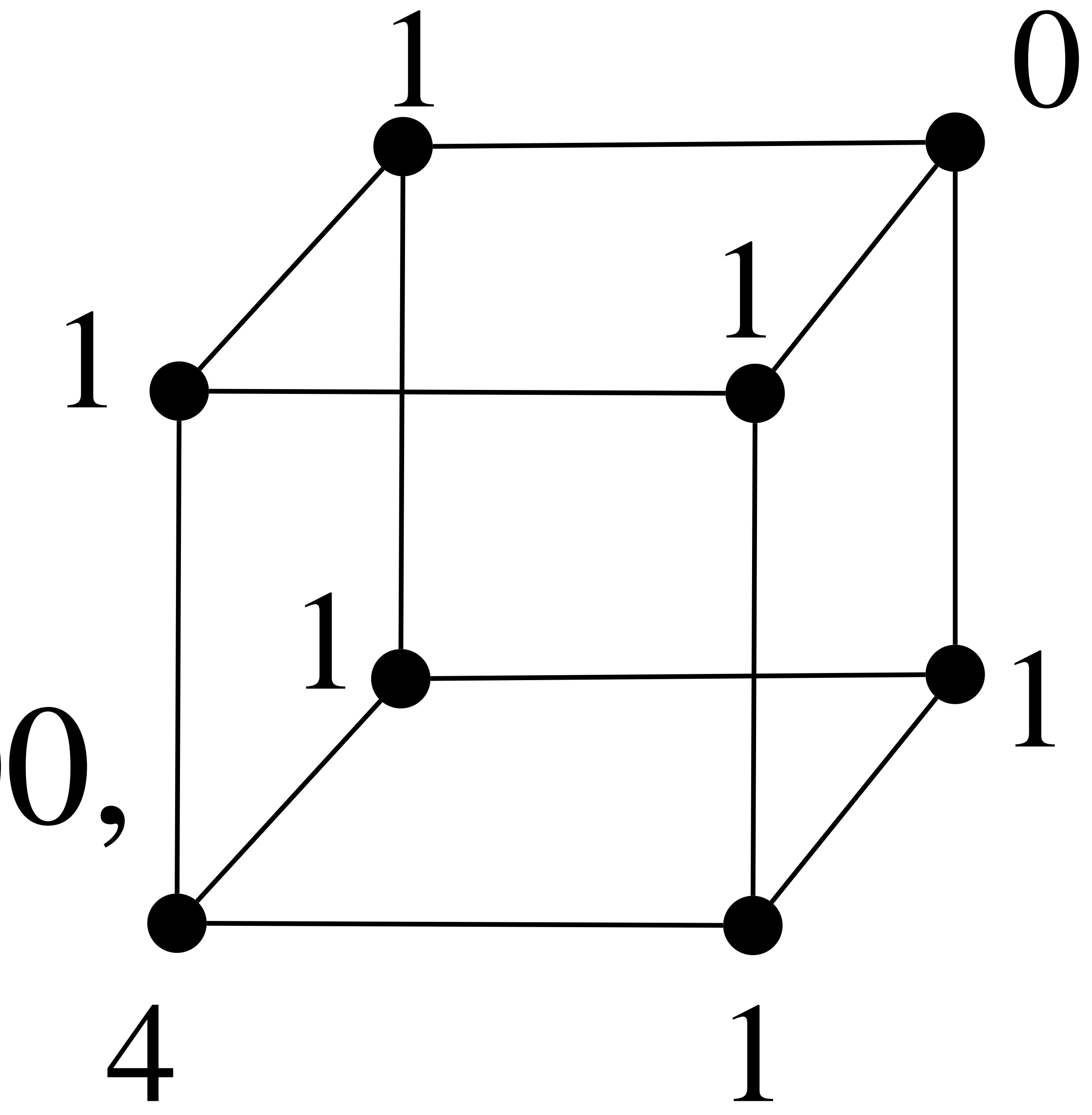
$B - B =$ more uniform

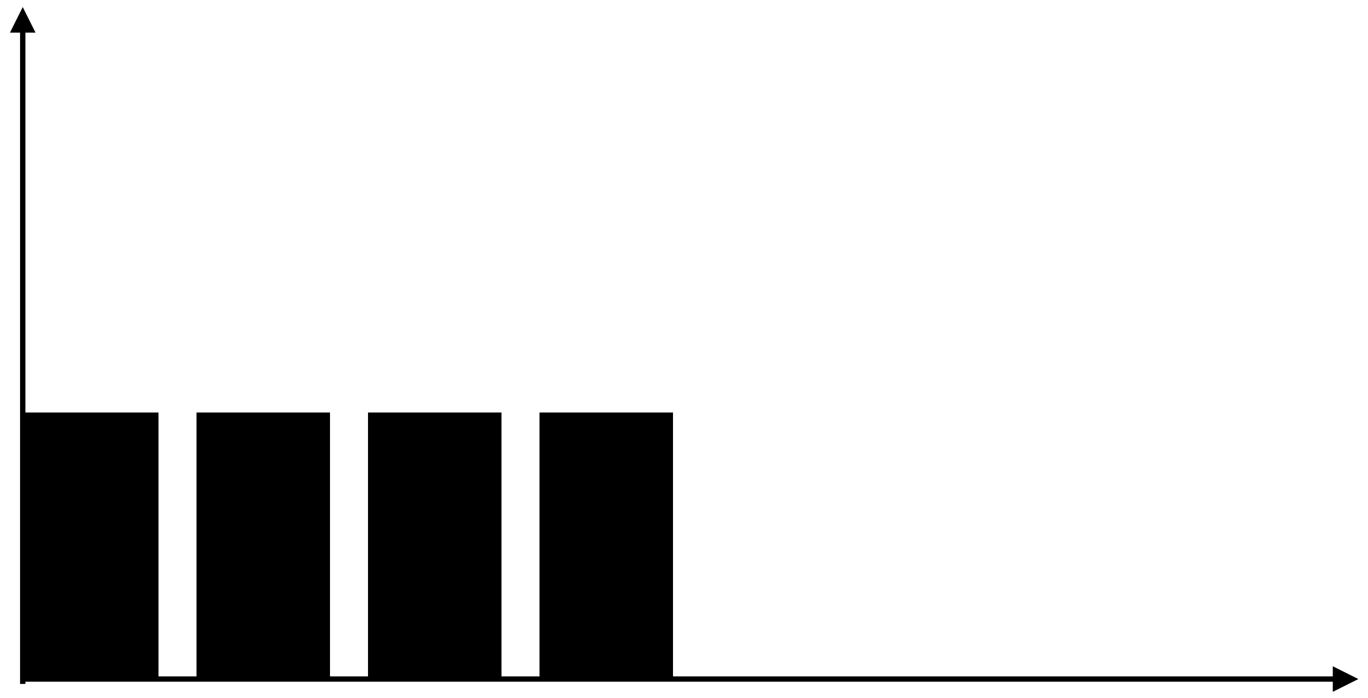
$$B_{1/3} = \{000,001,010,100\}$$

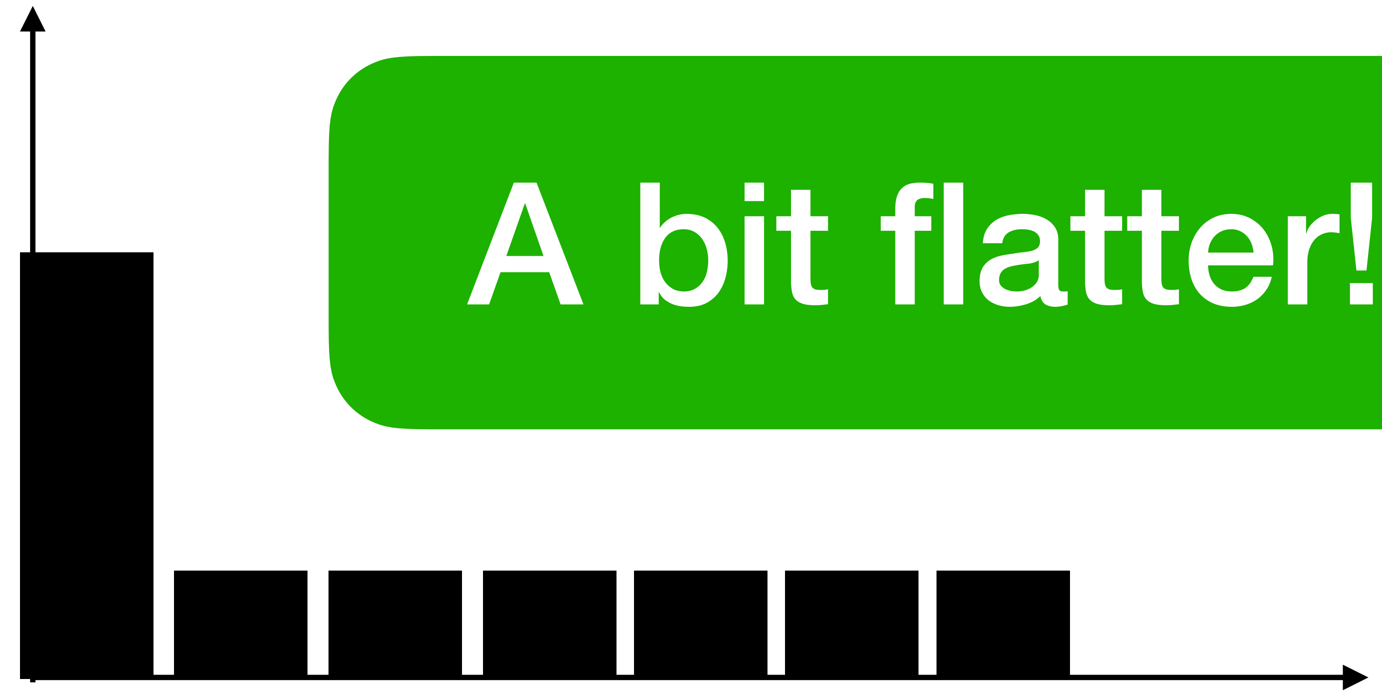


$$B_{1/3} - B_{1/3} =$$

$$\{000,000,000,000,$$
$$001,010,100,$$
$$011,101,110\}$$







A bit flatter!

New Challenge

New Challenge

No longer case that $\forall B, B' \in \mathscr{B}$,

$$B - B = B' - B'$$

New Challenge

No longer case that $\forall B, B' \in \mathscr{B}$,

$$B - B = B' - B'$$

Cannot bound $\delta_{B-B,\mathbf{C}_i}$ for each $B \in \mathscr{B}$ & union-bound…

New Challenge

No longer case that $\forall B, B' \in \mathscr{B}$,

$$B - B = B' - B'$$

Cannot bound $\delta_{B-B,\mathbf{C}_i}$ for each $B \in \mathscr{B}$ & union-bound…

$\alpha < 1$

Observation: if B α-concentrated (i.e., $\frac{q^n}{|B|}\hat{1}_B(y) \leq \alpha^{\mathrm{wt}(y)}$ $\forall y \in \mathbb{F}_q^n$), then $B - B$ α^2-concentrated

New Challenge

No longer case that $\forall B, B' \in \mathscr{B}$,

$$B - B = B' - B'$$

Cannot bound $\delta_{B-B,\mathbf{C}_i}$ for each $B \in \mathscr{B}$ & union-bound…

$\alpha < 1$

Observation: if B α-concentrated (i.e., $\dfrac{q^n}{|B|}\hat{1}_B(y) \leq \alpha^{\mathrm{wt}(y)}$ $\forall y \in \mathbb{F}_q^n$), then $B - B$ α^2-concentrated

Thus: $B^{(d)} := \underbrace{B + B \cdots + B}_{2^d \text{ times}} - \underbrace{B - \cdots - B}_{2^d \text{ times}}$ is α^{2^d}-concentrated

New Challenge

No longer case that $\forall B, B' \in \mathscr{B}$,

$$B - B = B' - B'$$

Cannot bound $\delta_{B-B,\mathbf{C}_i}$ for each $B \in \mathscr{B}$ & union-bound…

$\alpha < 1$

Observation: if B α-concentrated (i.e., $\frac{q^n}{|B|}\hat{1}_B(y) \leq \alpha^{\mathrm{wt}(y)}$

$\forall y \in \mathbb{F}_q^n$), then $B - B$ α^2-concentrated

nearly flat!

Thus: $B^{(d)} := \underbrace{B + B \cdots + B}_{2^d \text{ times}} - \underbrace{B - \cdots - B}_{2^d \text{ times}}$ is α^{2^d}-concentrated

Smoothness Transfer: at Depth

If each $\mathbf{C}_i$ has roughly the correct *dual weight distribution*, every $B^{(d)}$ is *smooth* for $C_0, \mathbf{C}_1, \ldots, \mathbf{C}_k$, with d (large) constant

Smoothness Transfer: at Depth

If each $\mathbf{C}_i$ has roughly the correct *dual weight distribution*, every $B^{(d)}$ is *smooth* for $C_0, \mathbf{C}_1, \ldots, \mathbf{C}_k$, with d (large) constant

One event implies *all* $B^{(d)}$ are smooth!

Smoothness Transfer: at Depth

If each $\mathbf{C}_i$ has roughly the correct *dual weight distribution*, every $B^{(d)}$ is *smooth* for $C_0, \mathbf{C}_1, \ldots, \mathbf{C}_k$, with d (large) constant

One event implies *all* $B^{(d)}$ are smooth!

$B^{(d)}$ smooth

Smoothness Transfer: at Depth

If each $\mathbf{C}_i$ has roughly the correct *dual weight distribution*, every $B^{(d)}$ is *smooth* for $C_0, \mathbf{C}_1, \ldots, \mathbf{C}_k$, with d (large) constant

One event implies *all* $B^{(d)}$ are smooth!

$B^{(d-1)}$ smooth

$B^{(d)}$ smooth

except w/ prob $q^{-\Omega(n^2)}$

Smoothness Transfer: at Depth

If each $\mathbf{C}_i$ has roughly the correct *dual weight distribution*, every $B^{(d)}$ is *smooth* for $C_0, \mathbf{C}_1, \ldots, \mathbf{C}_k$, with d (large) constant

One event implies *all* $B^{(d)}$ are smooth!

$B^{(d-1)}$ smooth

except w/ prob $q^{-\Omega(n^2)}$

$B^{(d)}$ smooth

except w/ prob $q^{-\Omega(n^2)}$

Smoothness Transfer: at Depth

If each $\mathbf{C}_i$ has roughly the correct *dual weight distribution*, every $B^{(d)}$ is *smooth* for $C_0, \mathbf{C}_1, \ldots, \mathbf{C}_k$, with d (large) constant

One event implies *all* $B^{(d)}$ are smooth!

$B^{(0)} = B$ smooth

except w/ prob $q^{-\Omega(n^2)}$

$\cdot^{\cdot^{\cdot}}$

except w/ prob $q^{-\Omega(n^2)}$

$B^{(d-1)}$ smooth

except w/ prob $q^{-\Omega(n^2)}$

$B^{(d)}$ smooth

Smoothness Transfer: at Depth

If each $\mathbf{C}_i$ has roughly the correct *dual weight distribution*, every $B^{(d)}$ is *smooth* for $C_0, \mathbf{C}_1, \ldots, \mathbf{C}_k$, with d (large) constant

One event implies *all* $B^{(d)}$ are smooth!

$B^{(0)} = B$ smooth

$\forall B \in \mathscr{B}$, B smooth w/prob. $1 - q^{-\Omega(n^2)}$

except w/ prob $q^{-\Omega(n^2)}$

$\cdot^{\cdot^{\cdot}}$

except w/ prob $q^{-\Omega(n^2)}$

$B^{(d-1)}$ smooth

except w/ prob $q^{-\Omega(n^2)}$

$B^{(d)}$ smooth

Smoothness Transfer: at Depth

If each $\mathbf{C}_i$ has roughly the correct *dual weight distribution*, every $B^{(d)}$ is *smooth* for $C_0, \mathbf{C}_1, \ldots, \mathbf{C}_k$, with d (large) constant

One event implies *all* $B^{(d)}$ are smooth!

$B^{(0)} = B$ smooth

except w/ prob $q^{-\Omega(n^2)}$

$\therefore$

$B^{(d-1)}$ smooth

except w/ prob $q^{-\Omega(n^2)}$

$B^{(d)}$ smooth

except w/ prob $q^{-\Omega(n^2)}$

$\forall B \in \mathscr{B}, B$ smooth w/prob. $1 - q^{-\Omega(n^2)}$

Can union over $B \in \mathscr{B}$ if $|\mathscr{B}| \leq q^{o(n^2)}$

Summary and Open Problems

Our Results

Let $\mathscr{B}$ be collection of sets, $\beta = 1 - \frac{1}{n} \log_q \min_{B \in \mathscr{B}} |B|$, C an RLC of rate $\beta + \varepsilon$. Have $|\delta_{C,B}| < q^{-\Omega(\varepsilon n)}$ whp in two cases:

Our Results

Let $\mathscr{B}$ be collection of sets, $\beta = 1 - \frac{1}{n} \log_q \min_{B \in \mathscr{B}} |B|$, C an RLC of rate $\beta + \varepsilon$. Have $|\delta_{C,B}| < q^{-\Omega(\varepsilon n)}$ whp in two cases:

$$\mathscr{B} = \{z + B : z \in \mathbb{F}_q^n\}$$

Our Results

Let $\mathscr{B}$ be collection of sets, $\beta = 1 - \frac{1}{n} \log_q \min_{B \in \mathscr{B}} |B|$, C an RLC of rate $\beta + \varepsilon$. Have $|\delta_{C,B}| < q^{-\Omega(\varepsilon n)}$ whp in two cases:

$$\mathscr{B} = \{z + B : z \in \mathbb{F}_q^n\}$$

List-decoding; generalize covering radius

Our Results

Let $\mathscr{B}$ be collection of sets, $\beta = 1 - \frac{1}{n} \log_q \min_{B \in \mathscr{B}} |B|$, C an RLC of rate $\beta + \varepsilon$. Have $|\delta_{C,B}| < q^{-\Omega(\varepsilon n)}$ whp in two cases:

$\mathscr{B} = \{z + B : z \in \mathbb{F}_q^n\}$

$|\mathscr{B}| \leq q^{o(n^2)}$; every B "pseudorandom"

List-decoding; generalize covering radius

Our Results

Let $\mathscr{B}$ be collection of sets, $\beta = 1 - \frac{1}{n}\log_q \min_{B \in \mathscr{B}} |B|$, C an RLC of rate $\beta + \varepsilon$. Have $|\delta_{C,B}| < q^{-\Omega(\varepsilon n)}$ whp in two cases:

$\mathscr{B} = \{z + B : z \in \mathbb{F}_q^n\}$

$|\mathscr{B}| \le q^{o(n^2)}$; every B "pseudorandom"

List-decoding; generalize covering radius

List-recovery (over $\mathbb{F}_p$), & leakage-resilience!

Open Problems

Open Problems

Larger fields? E.g., for leakage-resilience need $q < n^{1/5}$

Open Problems

Larger fields? E.g., for leakage-resilience need $q < n^{1/5}$

- For MDS codes, need $q > \exp(n)$

Open Problems

Larger fields? E.g., for leakage-resilience need $q < n^{1/5}$

- For MDS codes, need $q > \exp(n)$
- (Minor point: remove balancedness assumption)

Open Problems

Larger fields? E.g., for leakage-resilience need $q < n^{1/5}$

- For MDS codes, need $q > \exp(n)$
- (Minor point: remove balancedness assumption)
- Note: this restriction *only* applies to Theorem 2 (at least need $|\mathscr{B}| \leq q^{o(n^2)}$; also field size bound arises when using the pseudorandomness condition)

Open Problems

Larger fields? E.g., for leakage-resilience need $q < n^{1/5}$

- For MDS codes, need $q > \exp(n)$
- (Minor point: remove balancedness assumption)
- Note: this restriction *only* applies to Theorem 2 (at least need $|\mathscr{B}| \leq q^{o(n^2)}$; also field size bound arises when using the pseudorandomness condition)

Rate $\beta + O(1/n)$? Setting of interest for linear hashing

Open Problems

Larger fields? E.g., for leakage-resilience need $q < n^{1/5}$

- For MDS codes, need $q > \exp(n)$
- (Minor point: remove balancedness assumption)
- Note: this restriction *only* applies to Theorem 2 (at least need $|\mathscr{B}| \leq q^{o(n^2)}$; also field size bound arises when using the pseudorandomness condition)

Rate $\beta + O(1/n)$? Setting of interest for linear hashing

- We require constant $\varepsilon > 0$ gap

Poissonness of Weight Distribution?

Poissonness of Weight Distribution?

Let $\mathbf{C}$ be RLC of rate $1 - h_q(\rho) + \gamma$, and consider RV

$$X_\rho := |\mathbf{C} \cap S_\rho|,$$

where $S_\rho := \{x \in \mathbb{F}_q^n : \mathrm{wt}(x) = \rho n\}$.

Poissonness of Weight Distribution?

Let $\mathbf{C}$ be RLC of rate $1 - h_q(\rho) + \gamma$, and consider RV

$$X_\rho := |\mathbf{C} \cap S_\rho|,$$

where $S_\rho := \{x \in \mathbb{F}_q^n : \mathrm{wt}(x) = \rho n\}$.

General belief: should have $X_\rho \approx \mathrm{Poisson}(q^{\gamma n})$

assumed in code-based cryptanalysis, e.g., [MT'23]

Poissonness of Weight Distribution?

Let $\mathbf{C}$ be RLC of rate $1 - h_q(\rho) + \gamma$, and consider RV

$$X_\rho := |\mathbf{C} \cap S_\rho|,$$

where $S_\rho := \{x \in \mathbb{F}_q^n : \mathrm{wt}(x) = \rho n\}$.

General belief: should have $X_\rho \approx \mathrm{Poisson}(q^{\gamma n})$

assumed in code-based cryptanalysis, e.g., [MT'23]

Above could hold for both $\gamma > 0$ and $\gamma < 0$

Open Problem: Codes Below Capacity?

Open Problem: Codes Below Capacity?

E.g., when $\ell, q = O(1)$, what is list-size for RLC of rate $1 - \log_q(\ell) - \varepsilon$?

Open Problem: Codes Below Capacity?

E.g., when $\ell, q = O(1)$, what is list-size for RLC of rate $1 - \log_q(\ell) - \varepsilon$?

- [DMR**R**'25]: $\leq \dfrac{c_{q,\ell}}{\varepsilon}$, with $c_{q,\ell} \approx q^{O(\ell \log q)}$. What is dependence on ℓ? For "plain" random codes, $c_{q,\ell} = O(\ell)$

Open Problem: Codes Below Capacity?

E.g., when $\ell, q = O(1)$, what is list-size for RLC of rate $1 - \log_q(\ell) - \varepsilon$?

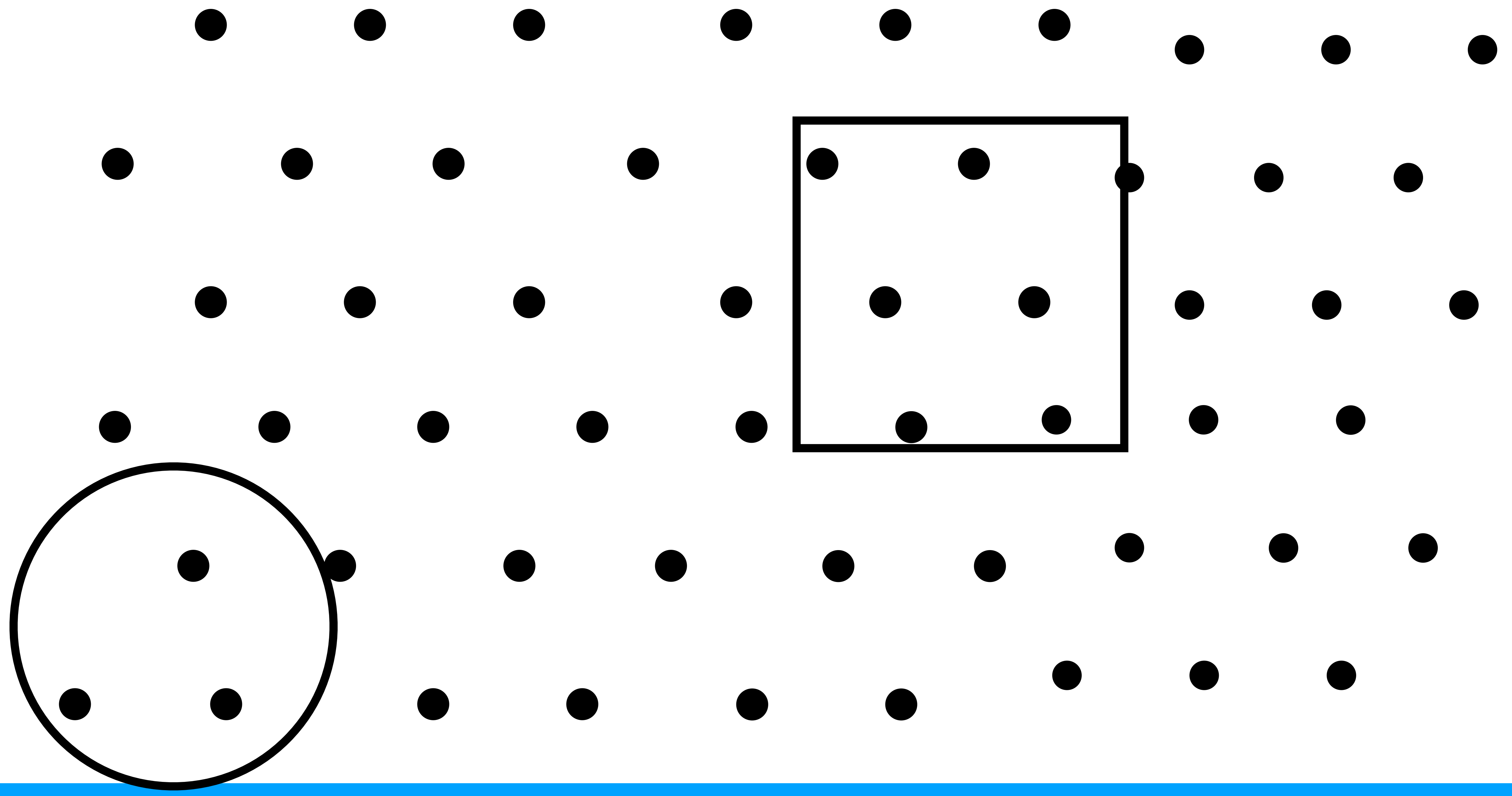
- [DM**R**R'25]: $\leq \dfrac{c_{q,\ell}}{\varepsilon}$, with $c_{q,\ell} \approx q^{O(\ell \log q)}$. What is dependence on ℓ? For "plain" random codes, $c_{q,\ell} = O(\ell)$
- [LS'25]: when $q > \ell^{1/\varepsilon}$, need $L > \ell^{\Omega(R/\varepsilon)}$ for linear codes, and this is sufficient [BCDZ'26]

Open Problem: Codes Below Capacity?

E.g., when $\ell, q = O(1)$, what is list-size for RLC of rate $1 - \log_q(\ell) - \varepsilon$?

- [DM**R**R'25]: $\leq \dfrac{c_{q,\ell}}{\varepsilon}$, with $c_{q,\ell} \approx q^{O(\ell \log q)}$. What is dependence on ℓ? For "plain" random codes, $c_{q,\ell} = O(\ell)$
- [LS'25]: when $q > \ell^{1/\varepsilon}$, need $L > \ell^{\Omega(R/\varepsilon)}$ for linear codes, and this is sufficient [BCDZ'26]

More generally: disjointed landscape for list-decodability of RLC's; is there one unified proof?

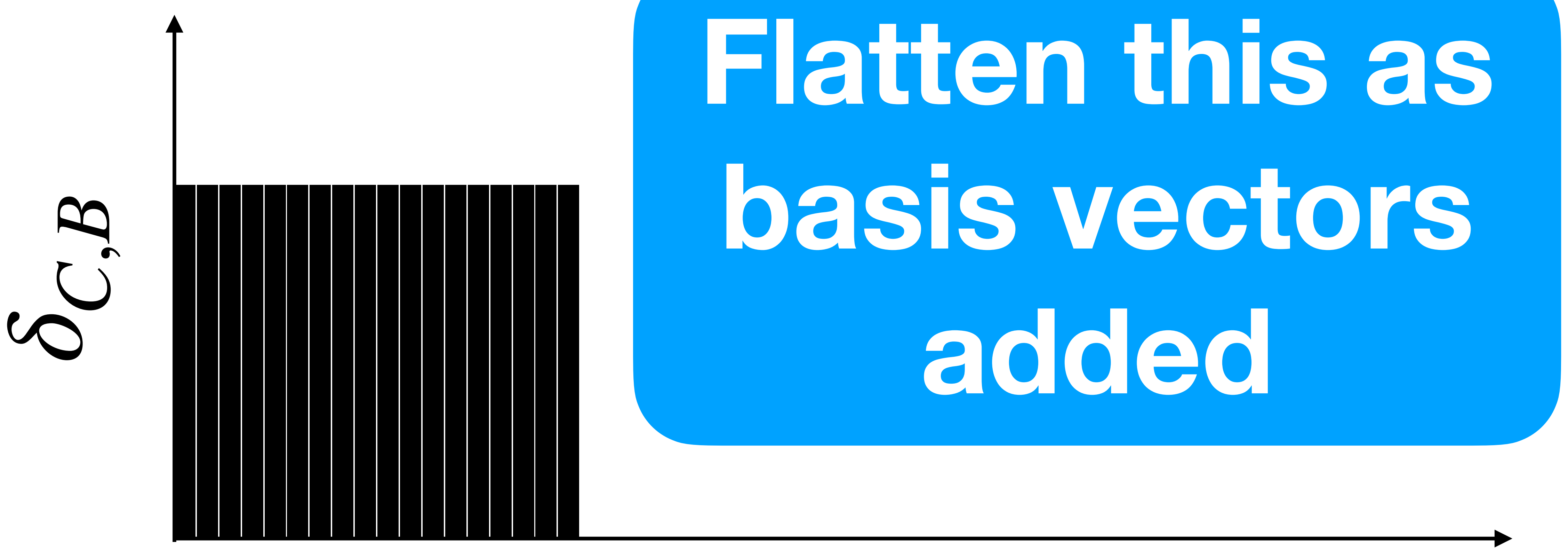


Above Capacity

$$R(C) = 1 - \frac{1}{n}\log_q|B| + \varepsilon, \text{ so}$$

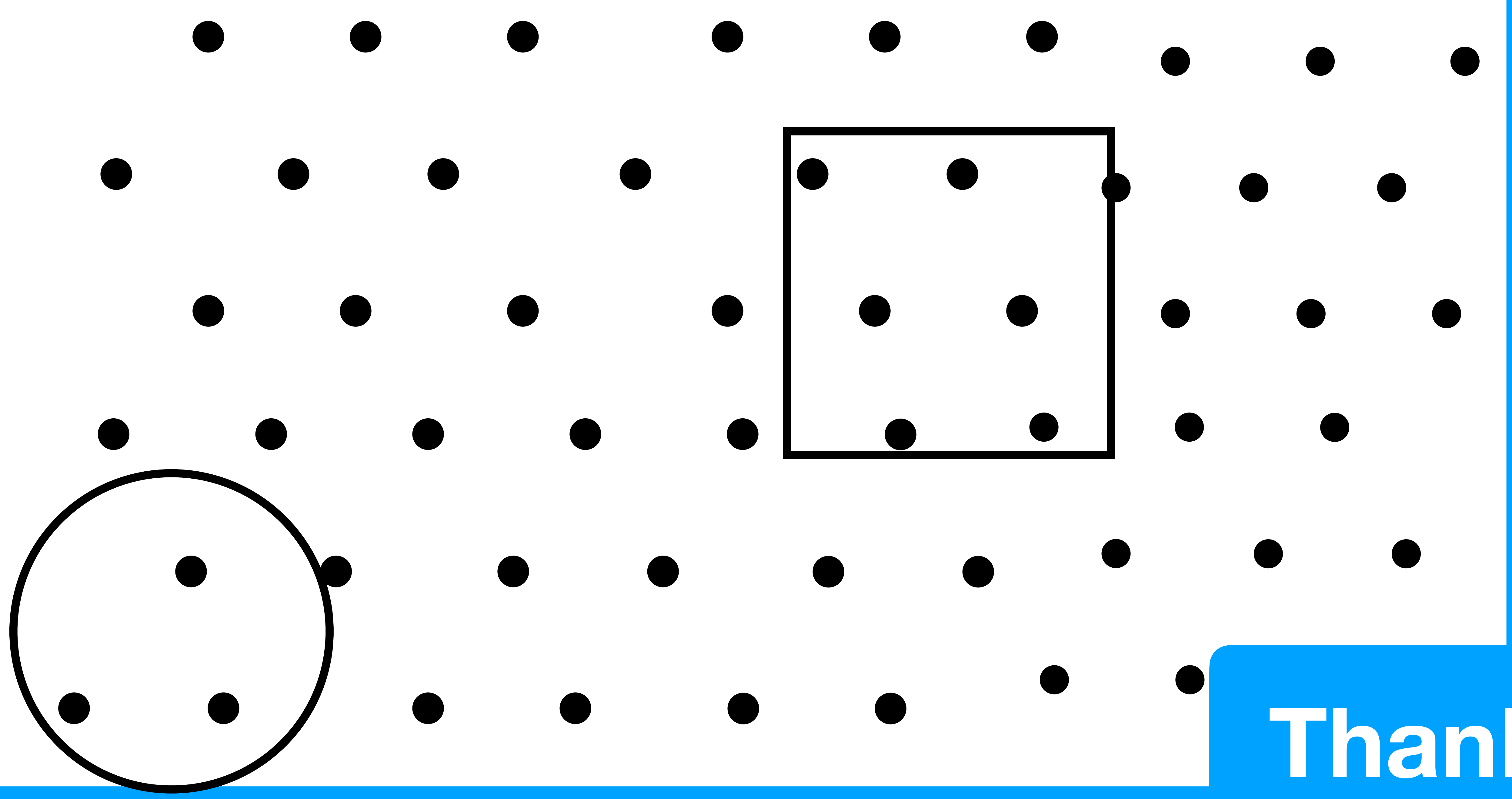
$$\mathbb{E}[\,|C \cap B|\,] = q^{\varepsilon n}$$

Strategy



Main Proof Idea

Transfer smoothness from $B - B$ to B



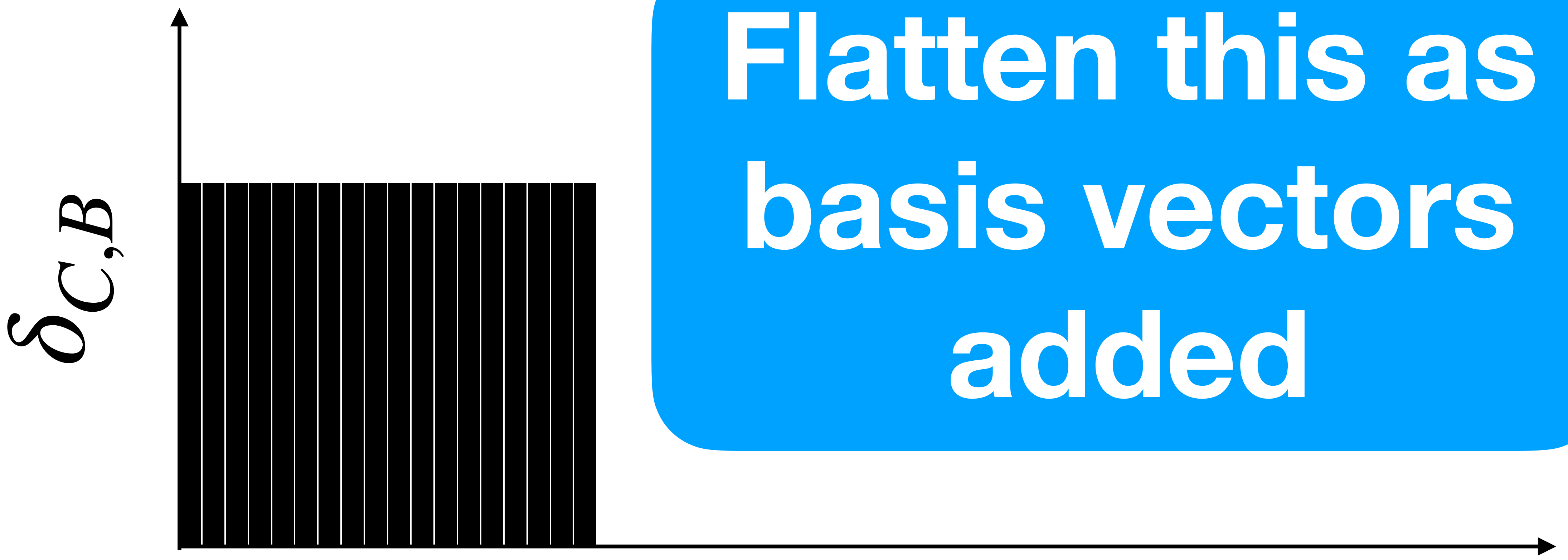
Above Capacity

$$R(C) = 1 - \frac{1}{n}\log_q|B| + \varepsilon\text{, so}$$

$$\mathbb{E}[\,|C \cap B|\,] = q^{\varepsilon n}$$

Thank you!
Questions?

Strategy



Flatten this as basis vectors added

Main Proof Idea

Transfer smoothness from $B - B$ to B