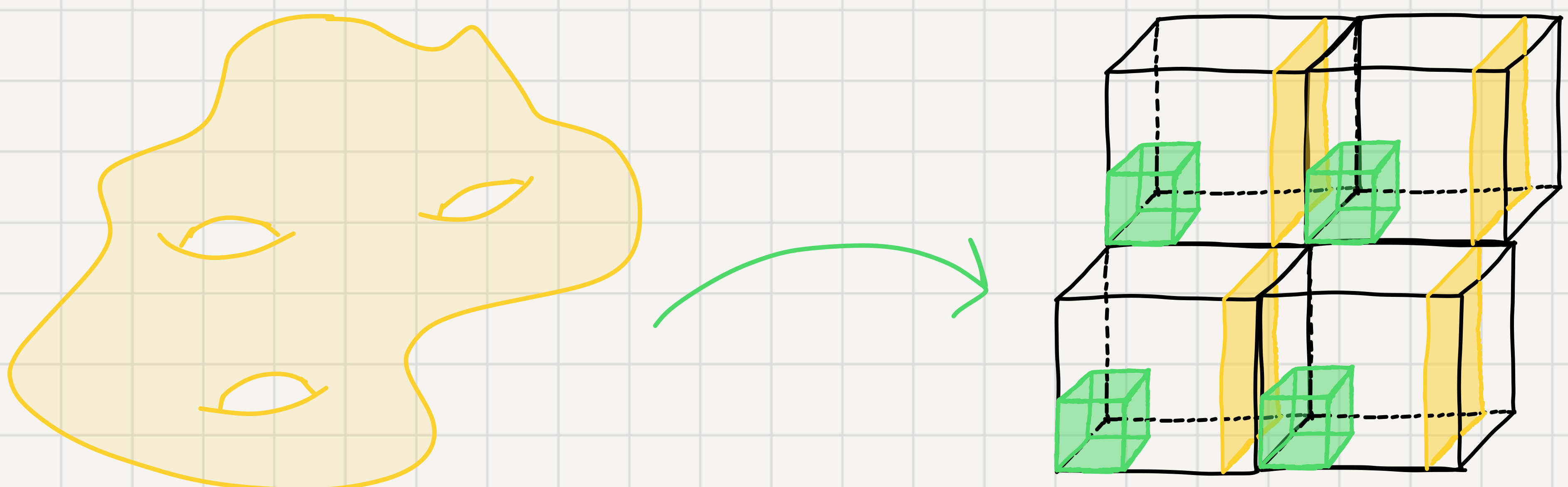
An additive combinatorics approach to average-case complexity



Vahid Asadi   Alexander Golovnev   Tom Gur

Igor Shinkar   Sathya Subramanian

Two motivating quotes

"every mathematician has only a few tricks" – Gian-Carlo Rota

"An idea which can only be used once is a trick. If one can use it more than once it becomes a method" – George Polya

Additive Combinatorics

(The Bogolyubov method)

Local correction via additive combinatorics

A-C studies approximate notions of algebraic structures via the perspective of combinatorics, number theory, harmonic analysis.

The <u>sumset</u> of a set X is defined as

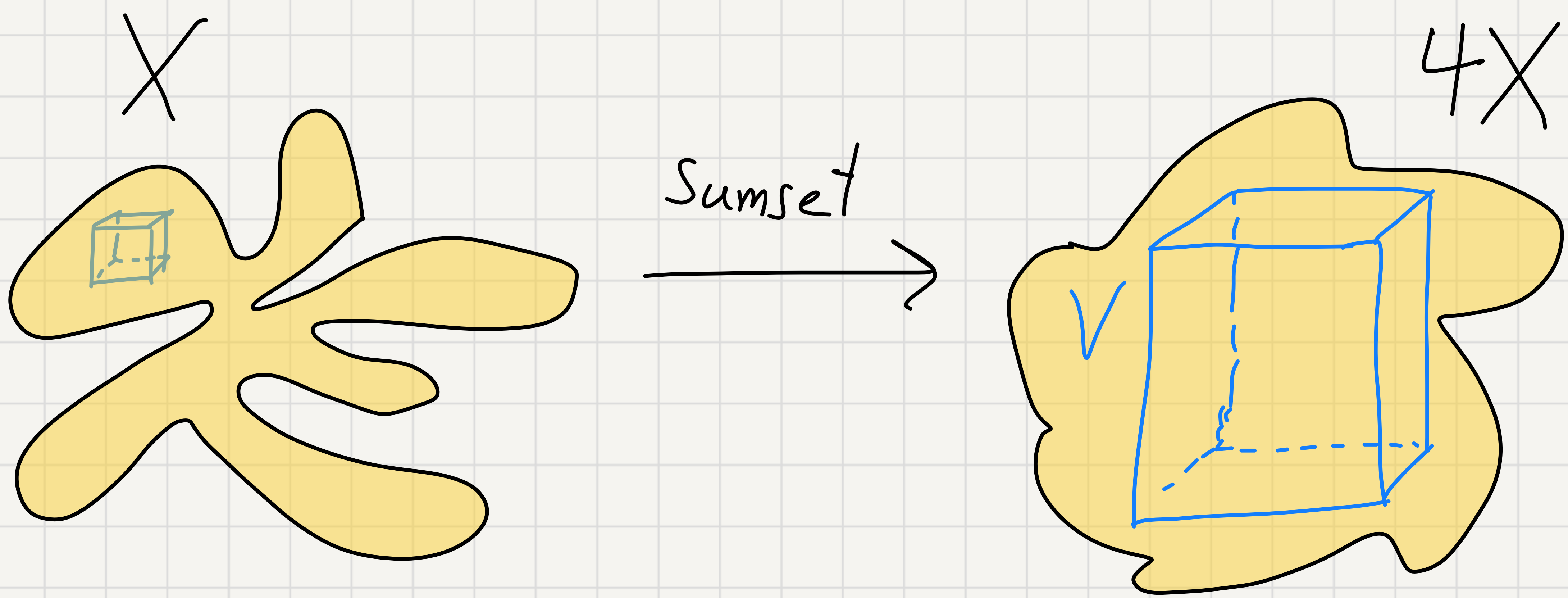
$X+X=\{x_1+x_2 : x_1,x_2\in X\}$. Generally: $t\cdot X=\{\sum_{i=1}^{t} x_i : x_1,\dots,x_t\in X\}$.

These notions quantify a <u>combinatorial</u> analogue of approximate <u>subgroup</u> structure.

Small sumsets imply approximate closure.

Bogolyubov's lemma

Let $X \subseteq \mathbb{F}_2^n$ of density $\frac{|X|}{2^n} \geq \alpha$. Then, there exists a subspace $V \subseteq 4X$ of dimension $\dim(V) \geq n - 1/\alpha^2$.



Bogolyubor's lemma

Let $X \subseteq \mathbb{F}_2^n$ of density $\frac{|X|}{2^n} \geq \alpha$. Then, there exists a subspace $V \subseteq 4X$ of dimension $\dim(V) \geq n - 1/\alpha^2$.

Strengthenings

- Quasi-polynomial Bogolyubov-Ruzsa lemma
- Probabilistic Bogolybov decompositions
- Sparse-shifting to Bogolyubov subspaces

Average-Case Complexity

Worst-case to average-case reductions

Goal: use average-case algorithms to solve worst-case problems

OPTIMIST

"A new paradigm for designing algorithms!"

PESSIMIST

"Show lower bounds even for weak average-case complexity"

"Boosting knowledge" via average-to-worst case reductions

"Boosting knowledge" via average-to-worst case reductions

Suppose we know how to solve a problem on few instances

Can we derive how to solve all of them?

Example – Matrix multiplication

Problem: Given $A, B \in \mathbb{F}^{n \times n}$, compute $A \cdot B$.

Suppose ALG s.t.

$$\Pr_{A,B \in \mathbb{F}^{n\times n}}\left[ALG(A,B) = A \cdot B\right] \geq \alpha$$

$\alpha = 0.01$

$\alpha = o(1)$

Can we boost α to 1?

This talk

worst-case to average-case reductions for

matrix multiplication

Theorem: If there exists ALG running in time T

s.t. $\Pr_{A,B\in\mathbb{F}^{n\times n}}[\text{ALG}(A,B)=A\cdot B]\geq\alpha$,

then there exists ALG' running in time $O(T)$

s.t. for all $A,B\in\mathbb{F}^{n\times n}$, w.p. $1-\delta$

$$\text{ALG}(A,B)=A\cdot B$$

Simplify: Fix A

Remark: $O(T)$ hides a factor of roughly $1/\delta\cdot\alpha$

A trivial special case: high-agreement regime

Suppose $\Pr_{B \in \mathbb{F}^n}[\mathrm{ALG}_A(B) = A \cdot B] \geq 0.99$

<u>Idea:</u> linear local correction

1) Sample $R \sim \mathcal{U}(\mathbb{F}^{n \times n})$

2) Write $B = R + (B-R) \longrightarrow$ Each component is uniformly distributed

3) Compute $C := \mathrm{ALG}_A(R) + \mathrm{ALG}_A(B-R)$

Note that $\Pr[C = AB] \geq 1 - 2 \cdot 0.01 > 9/10$

The challenge: low-agreement regime

In the 1% regime $\left(\Pr_{B \in \mathbb{F}^n}\left[ALG_A(B) = AB\right] = 0.01\right)$

this approach completely breaks!

Example

Fix $\mathbb{F} = GF(2)$. Suppose $\begin{cases} ALG_A(B) = AB & B_{11} = 0 \\ ALG_A(B) = \bar{0} & o/w \end{cases}$

Correct on 50%, but decomposition fails:

$$\begin{pmatrix} 1 & \\ & * \end{pmatrix} \neq \begin{pmatrix} 0 & \\ & * \end{pmatrix} + \begin{pmatrix} 0 & \\ & * \end{pmatrix}$$

Is all hope lost?

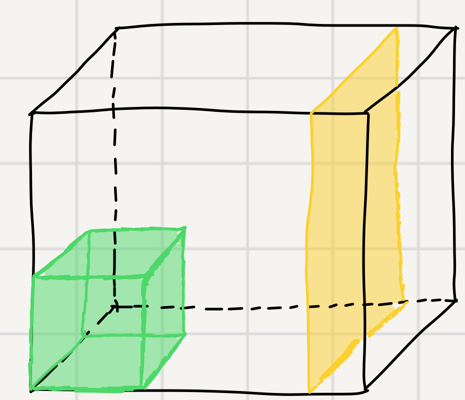
Bogolyubov's lemma

Let $X \subseteq \mathbb{F}_2^n$ of density $\frac{|X|}{2^n} \geq \alpha$. Then, there exists a subspace $V \subseteq 4X$ of dimension $\dim(V) \geq n - 1/\alpha^2$.

key idea: Use Bogolyubov's lemma for local correction!

How? Suppose $\Pr_{B \in \mathbb{F}^n}[ALG_A(B) = AB] \geq \alpha$

Denote $X = \{B \in \mathbb{F}^n : ALG_A(B) = AB\}$. Note $\mu(X) \geq \alpha$



Hence, there exist a large subspace V s.t. $v \in V$

decomposes to $V = x_1 + x_2 + x_3 + x_4$, $x_1, \dots, x_4 \in X$

Local correction via Bogolybov's lemma

More precisely, we'll need the probabilistic version.

Lemma: Let $X \subseteq \mathbb{F}_2^n$ s.t. $|X|/2^n \geq \alpha$.

There exist a subspace V of dim $n - \frac{1}{\alpha^2}$

s.t. $\forall v \in V \quad \Pr_{x_1, x_2, x_3}[x_1, x_2, x_3, v - x_1 - x_2 - x_3 \in X] \geq \alpha^5$.

Given $X = \{B' \in \mathbb{F}^{n \times n} : ALG(A, B') = A \cdot B'\}$ we obtain $V \subseteq \mathbb{F}^n$ with $\dim(V) \geq n^2 - 1/\alpha^2$ s.t. $\forall\ B' \in V$

$\Pr[M_1, M_2, M_3, M_4 \in X] \geq \alpha^5$, where $M_4 = B' - M_1 - M_2 - M_3$

Local correction via Bogolybov's lemma

Given $X = \{B' \in \mathbb{F}^{n \times n} : ALG(A, B') = A \cdot B'\}$ we obtain $V \subseteq \mathbb{F}^n$ with $\dim(V) \geq n^2 - 1/\alpha^2$ s.t. $\forall\ B' \in V$

$$\Pr[M_1, M_2, M_3, M_4 \in X] \geq \alpha^s, \text{ where } M_4 = B' - M_1 - M_2 - M_3$$

If this event occurs, then

$$\sum_{i=1}^{4} ALG(A, M_i) = \sum_{i=1}^{4} A \cdot M_i = A \cdot \left(\sum_{i=1}^{4} M_i\right) = A \cdot B'$$

as required.

But success probability α^s is far smaller than desired...

A simple fact

Given a potentially wrong output $A \cdot B$, we can efficiently check the solution via Freivald's algorithm.

<u>Lemma:</u> Given $A, B, C \in \mathbb{F}^{n \times n}$, there exists a prob. alg. verifying $A \cdot B = C$ with high probability, in time $O(n^2)$

We amplify $O(1/\alpha^s)$ times via Freivald's algorithm!

Local correction via Bogolybov's lemma

Recap: good inputs $X = \{B \in \mathbb{F}^{n \times n} : ALG_A(B) = A \cdot B\}$

Bogolybov subspace $V \subseteq 4X$

Case 1: If $B \in X$, just run $ALG(A, B)$

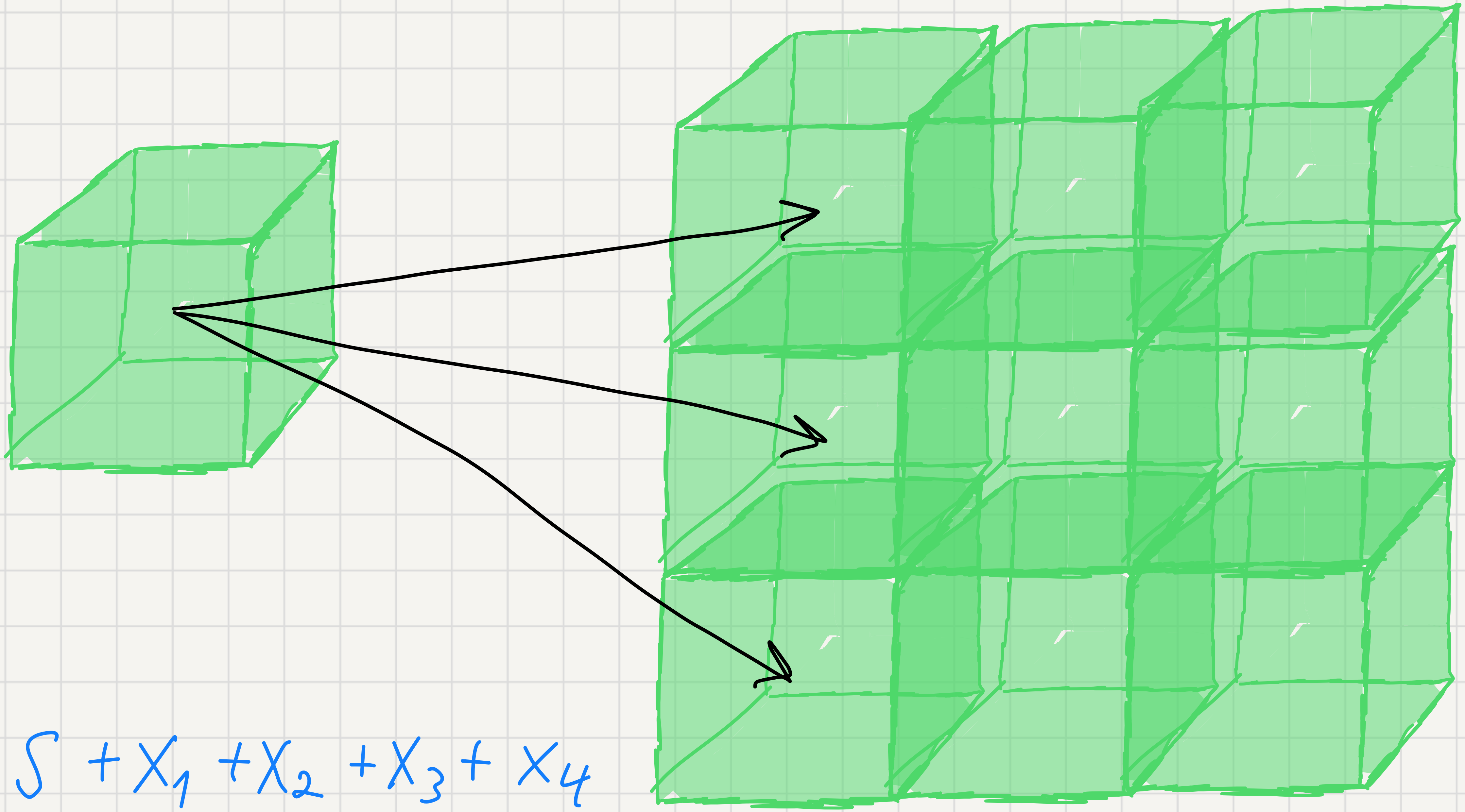
Case 2: If $B \in V$, locally correct via Bogolyubov's lemma

Case 3: If $B \notin V$, um... did we really gain anything?

We started with X of density α

V has smaller density... but it has structure!

Final step: Sparse-shifting Bogolyubov subspaces



$Z = S + X_1 + X_2 + X_3 + X_4$

$X_1, \dots, X_4 \in X$, S is sparse $\Rightarrow$ efficiently computable

Thank you!