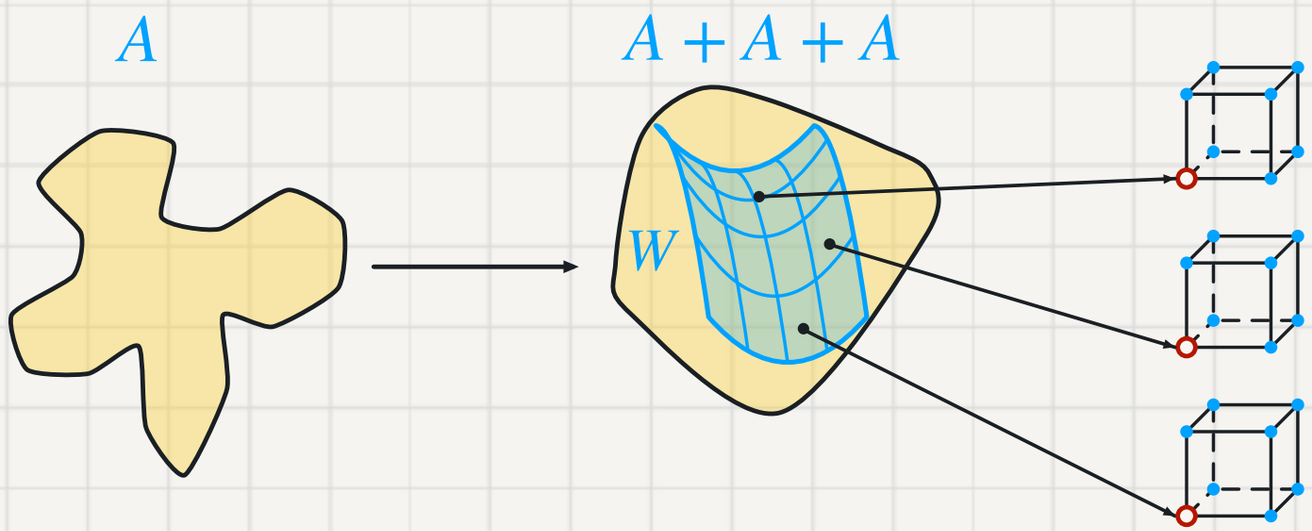
Quantum Complexity Theory

Boosting quantum algorithms



Tom Gur

UNIVERSITY OF CAMBRIDGE

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"

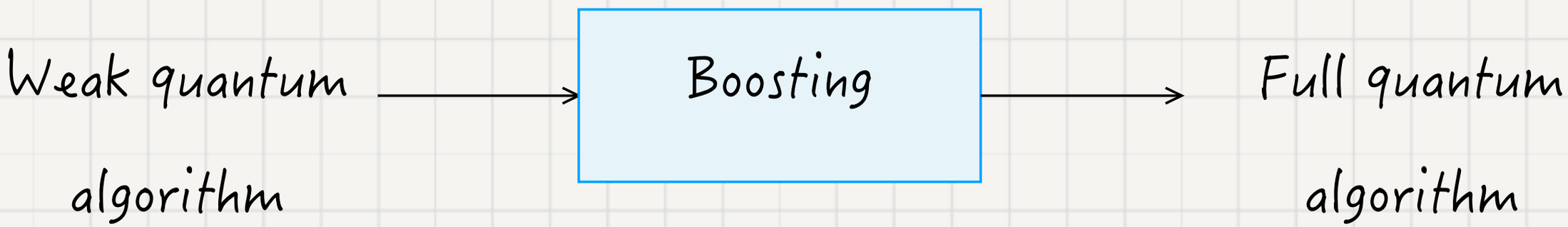
George Pólya

Boosting quantum algorithms

Designing new quantum algorithms is one of the most important problems in quantum computing

But it is notoriously hard!

Can we make it easier?



Worst-case to average-case reductions

Suppose we know how to solve a problem on a few instances

Can we derive how to solve all of them?

Focus on linear problems $\mathscr{M} = \{M_n\}_{n \in \mathbb{N}}$, with $M_n \in \mathbb{F}^{n \times n}$

Given $x \in \mathbb{F}^n$, compute Mx

Suppose ALG_M satisfies $\Pr_{x \in \mathbb{F}^n} [\mathrm{ALG}_M(x) = Mx] \geq \alpha$

Can we boost α to 1?

Two perspectives

Worst-case to average-case reductions



Optimist

"A new paradigm for designing algorithms!"

Pessimist



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

An easy special case: high-agreement regime

Suppose $\Pr_{v \in \mathbb{F}^n}[\mathrm{ALG}_M(v) = Mv] \geq 0.99$

Idea: linear local correction

1. Sample $r \sim U(\mathbb{F}^n)$

2. Write $v = r + (v - r)$ Each component is uniformly distributed

3. Compute $v' := \mathrm{ALG}_M(r) + \mathrm{ALG}_M(v - r)$

Then $\Pr[v' = Mv] \geq 1 - 2 \cdot 0.01 > 9/10$

The challenge: low-agreement regime

In the 1% regime, $\Pr_{v \in \mathbb{F}^n}[\mathrm{ALG}_M(v) = Mv] \geq 0.01$,

this approach completely breaks

Example

Fix $\mathbb{F} = \mathrm{GF}(2)$ Suppose $\mathrm{ALG}_M(v) = \begin{cases} Mv & v_1 = 0, \\ 0 & \text{otherwise.} \end{cases}$

This works on 50% of inputs, but decomposition fails:

$$\begin{pmatrix} 1 \\ \vdots \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \end{pmatrix} + \begin{pmatrix} 1 \\ \vdots \end{pmatrix}$$

Is all hope lost?

Boosting quantum algorithms for linear problems

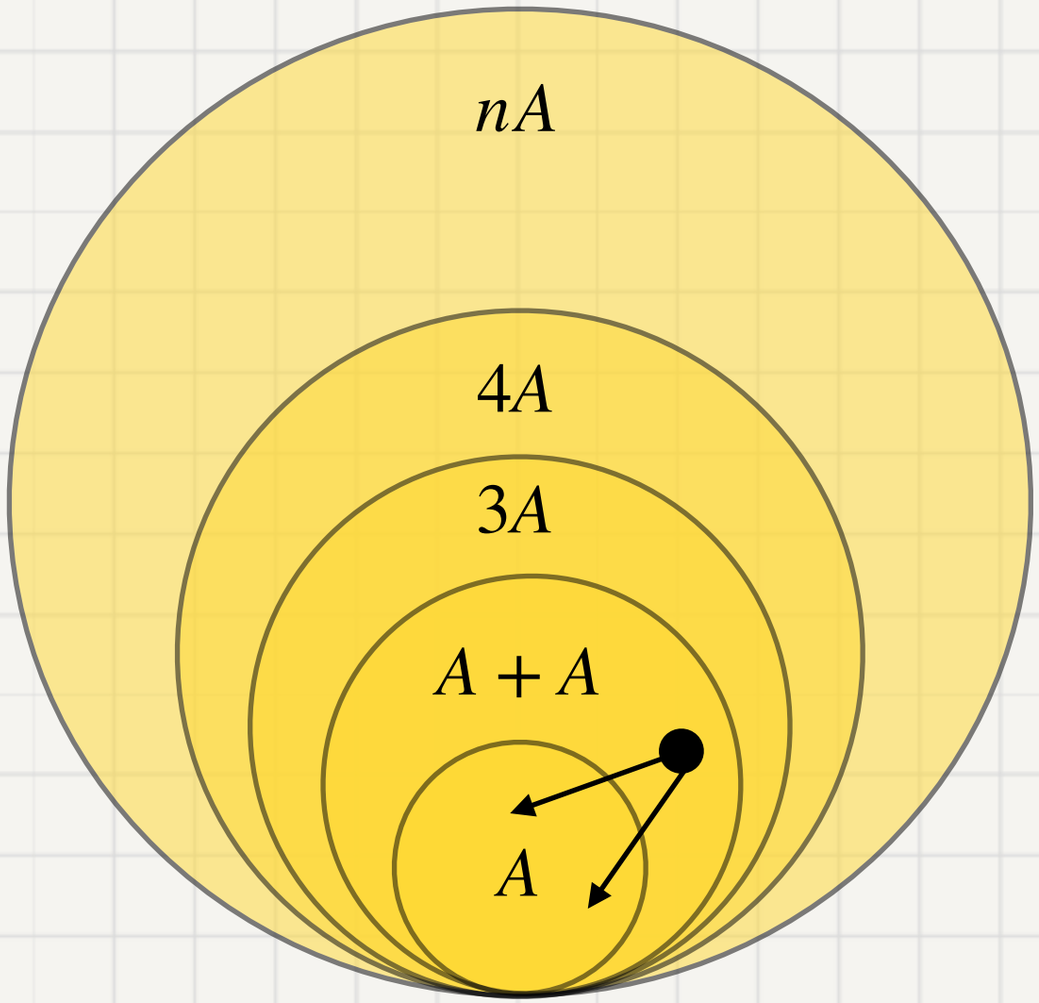
Theorem. Let ALG be a quantum algorithm for a linear problem $\mathscr{M}$ that can solve $1\,\%$ of the inputs

Then there exists ALG′ for $\mathscr{M}$, with only $O(n^{3/2})$ extra gates, that can solve $100\,\%$ of the inputs

In fact, the success rate may tend to zero: $\alpha \to 0$

High-level approach

Let A be the set of instances we can solve



Two problems

① Will we cover the entire space?

② The complexity blows up!

The sumset of a set A is defined as $A + A = \{a_1 + a_2 : a_1, a_2 \in A\}$.

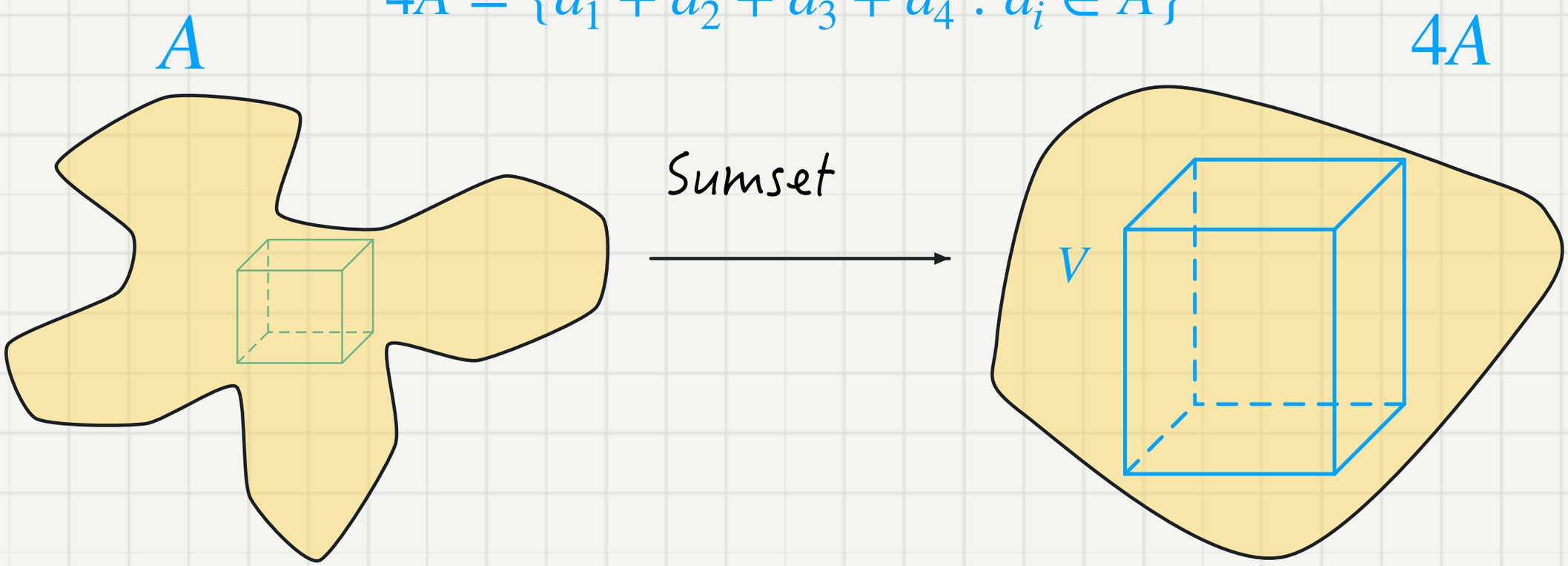
Generally: $t \cdot A = \left\{ \sum_{i=1}^{t} a_i : a_1, \ldots, a_t \in A \right\}$.

Bogolyubov's lemma: extracting linear structure

Let $A \subseteq \mathbb{F}_2^n$ have density $|A|/2^n \geq \alpha$

There exists a subspace $V \subseteq 4A$ with $\dim(V) \geq n - 1/\alpha^2$

$$4A = \{a_1 + a_2 + a_3 + a_4 : a_i \in A\}$$



TCS perspective: local correction of linear structure

Bogolyubov's lemma

Let $A \subseteq \mathbb{F}_2^n$ have density $|A|/2^n \geq \alpha$

There exists a subspace $V \subseteq 4A$ with $\dim(V) \geq n - 1/\alpha^2$

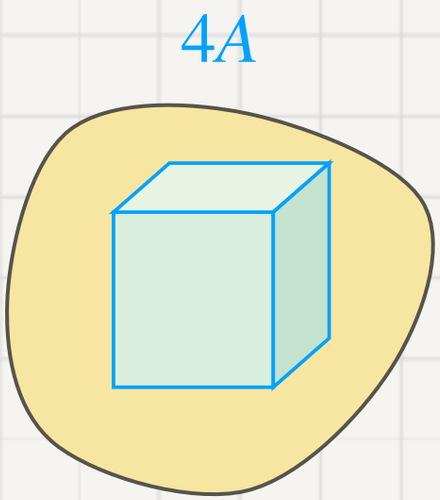
Key idea: use Bogolyubov's lemma for local correction

Suppose $\Pr_{v \in \mathbb{F}^n}[\mathrm{ALG}_M(v) = Mv] \geq \alpha$

Denote $A = \{v \in \mathbb{F}^n : \mathrm{ALG}_M(v) = Mv\}$

Note that $\mu(A) \geq \alpha$

Each $v \in V$ is $v = x_1 + x_2 + x_3 + x_4$, with $x_i \in A$



Obtaining the decomposition

Supersaturation of Sanders's

quasi-polynomial Bogolyubov–Ruzsa lemma

> Lemma. Let $A \subseteq \mathbb{F}_2^n$ satisfy $|A|/2^n \geq \alpha$
>
> There is a subspace $V \leq \mathbb{F}_2^n$ with $\dim(V) \geq n - \mathrm{polylog}(1/\alpha)$,
>
> and for all $v \in V$, $\Pr_{x_1,x_2,x_3 \in A}[v - x_1 - x_2 - x_3 \in A] \geq \alpha^2$

If this event occurs, then

$$\sum_{i=1}^{4} \mathrm{ALG}_M(x_i) = \sum_{i=1}^{4} Mx_i = M\left(\sum_{i=1}^{4} x_i\right) = Mv$$

Quantum worst-case to average-case reduction

Recap: $A = \{v \in \mathbb{F}^n : \mathrm{ALG}_M(v) = Mv\}$ is the good-input set

The Bogolyubov subspace satisfies $V \subseteq 4A$

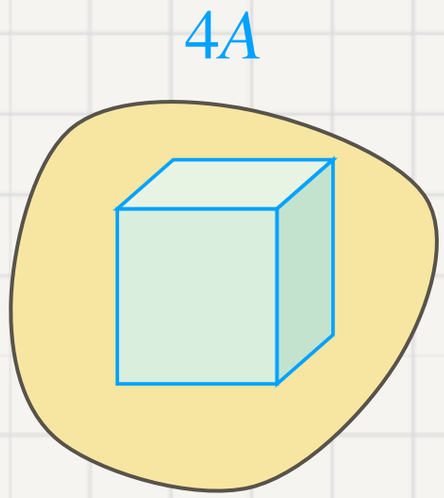
Case 1. If $v \in A$, run $\mathrm{ALG}_M(v)$

Case 2. If $v \in V$, locally correct via Bogolyubov's lemma

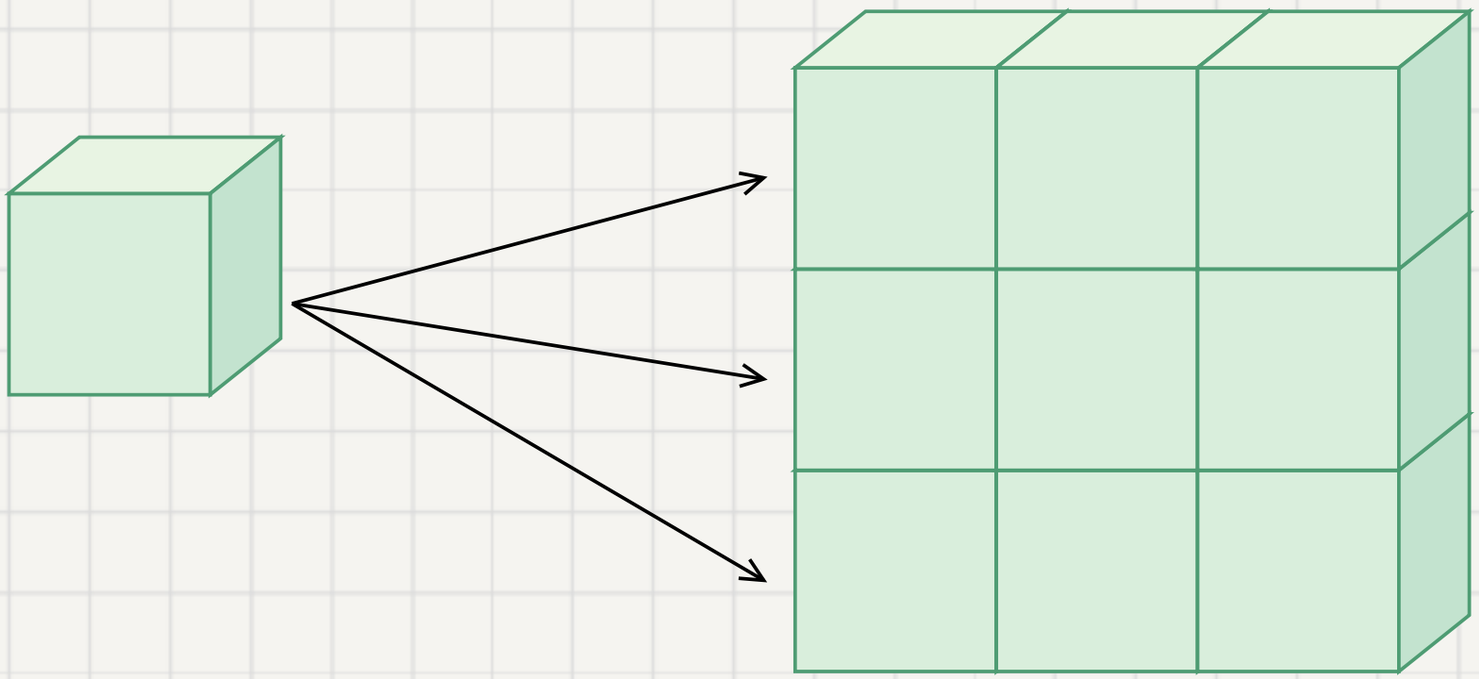
Case 3. If $v \notin V$, did we really gain anything?

We started with A of density α

V has smaller density, **but it has structure!**



Sparse-shifting Bogolyubov subspaces



$z = s + x_1 + x_2 + x_3 + x_4$

Here $x_1, \ldots, x_4 \in A$, and s is sparse, so it is efficiently computable

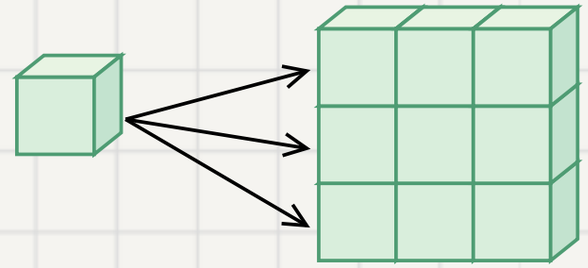
Sparse-shifting Bogolyubov subspaces

Claim. Let $V \leq \mathbb{F}_2^n$ have $\operatorname{codim}(V) = k$

For every $y \in \mathbb{F}_2^n$, there is $s \in \mathbb{F}_2^n$ with $|s| = k$ and $y \in s + V$

Proof. Consider the linear constraints defining V:

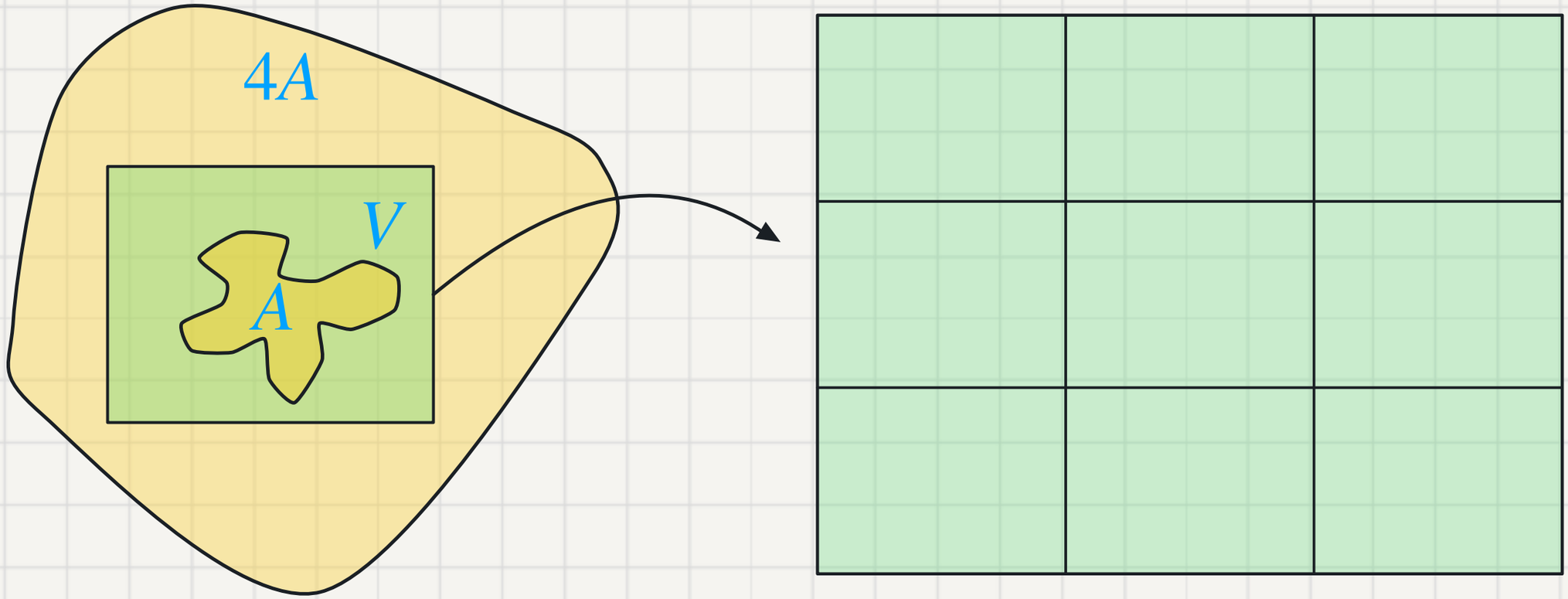
$$\sum_{i=1}^{n} \alpha_i^{(1)} x_i = 0, \quad \ldots, \quad \sum_{i=1}^{n} \alpha_i^{(k)} x_i = 0$$



Use row echelon form and flip the unsatisfied constraints

Quantum Goldreich–Levin makes this algorithmic

What is missing?



I. How do we know whether we are in A?

II. How do we obtain $v = x_1 + x_2 + x_3 + x_4$?

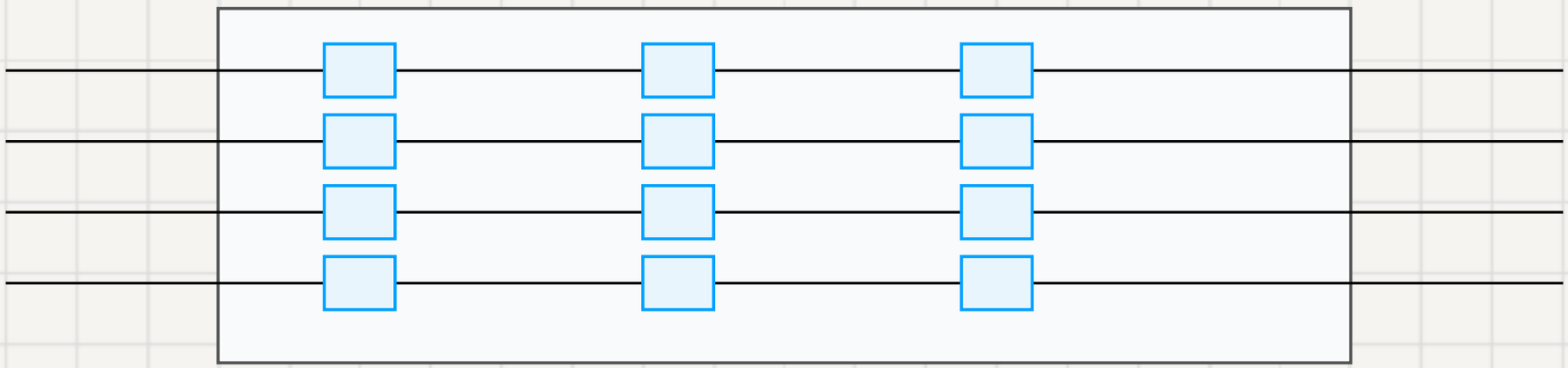
III. How do we shift the Bogolyubov space?

Verifying solutions in superposition

Quantum algorithm 1: Matrix-vector multiplication checking

$$\sum_{v \in \mathbb{F}^n} |v\rangle\,|\mathrm{ALG}_M(v)\rangle$$

$T = O(n^{3/2})$



$$\sum_{v \in \mathbb{F}^n} |v\rangle\,|\mathrm{ALG}_M(v)\rangle\,|\mathrm{flag}(v)\rangle$$

Idea (very roughly): evaluate $(Mv)_i$ locally in time $O(n)$

Construct an oracle for $|\mathrm{ALG}_M(v)_i - (Mv)_i|$

Apply a careful version of Grover search

Sampling and learning the heavy Fourier spectrum

Quantum algorithm II: sampling from A

An $O(n^{3/2})$-gate quantum algorithm synthesizes

$$|\psi\rangle = \frac{1}{\sqrt{|A|}} \sum_{x \in A} |x\rangle$$

Quantum algorithm III: learning the heavy Fourier spectrum

An $O(n)$-gate quantum algorithm, given a noisy quantum oracle U_f, outputs $y \in \mathbb{F}^n$ with probability p_y such that

$$|p_y - |\hat{f}(y)|^2| = o(1)$$

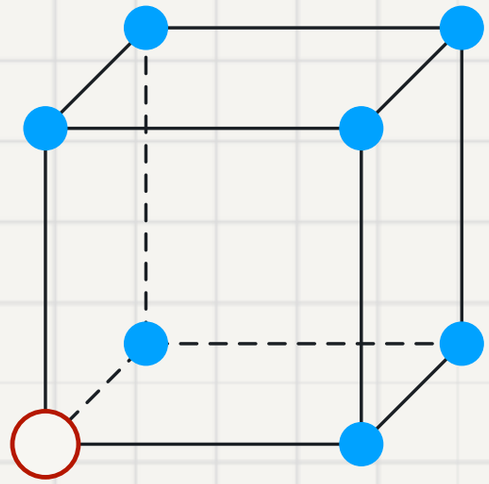
Beyond linear structure

Let $q : \mathbb{F}^n \to \mathbb{F}^n$ be a quadratic map,

$q(x) = (xQ_1x^\mathsf{T}, \ldots, xQ_nx^\mathsf{T})$, for $Q_i \in \mathbb{F}^{n\times n}$

Bogolyubov's lemma gives $v = a_1 + a_2 + a_3 + a_4$,

but $q(v) \neq \sum_i q(a_i)$



Idea: local correction via Gowers U^3-norm constraints

$$q(a_1 + a_2 + a_3) = q(0) + q(a_1) + q(a_2) + q(a_3)$$
$$+ q(a_1 + a_2) + q(a_1 + a_3) + q(a_2 + a_3)$$

Equivalent to vanishing third derivatives

A "quadratic" Bogolyubov lemma

Wish. Let $A \subseteq \mathbb{F}^n$ have density $\alpha > 0$ There exists a dense "structured" set $V \subset 3A$ such that every $v \in V$ can be written as $v = a_1 + a_2 + a_3$, where $a_1, a_2, a_3, a_1 + a_2, a_1 + a_3, a_2 + a_3 \in A$

Recall $q(a_1 + a_2 + a_3) = q(0) + q(a_1) + q(a_2) + q(a_3)$
$+ q(a_1 + a_2) + q(a_1 + a_3) + q(a_2 + a_3)$

Caveat: false! Take $A = \{x \in \mathbb{F}_2^n : x_1 = 1\}$

Then $a, b \in A \implies a + b \notin A$

A "quadratic" Bogolyubov lemma

Wish (revised). Let $A \subseteq \mathbb{F}^n$ have density $\alpha > 0$ There exists a dense "structured" set $V \subset 3A$ and $y \in \mathbb{F}^n$ such that every $v \in V$ can be written as $v = x_1 + x_2 + x_3$, where

$$x_1, x_2, x_3, x_1 + x_2, x_1 + x_3, x_2 + x_3 \in y + A$$

What is "structured"?

At the very least, it admits a sparse-shifting lemma:

$\forall x \in \mathbb{F}^n \; \exists$ sparse s such that $x = v + s$ for $v \in V$

What is "structured"?

For dense $A \subseteq \mathbb{F}^n$, seek a dense "structured" $V \subset 3A$ and a shift y so every $v \in V$ has $v = x_1 + x_2 + x_3$ with

$x_1, x_2, x_3, x_1 + x_2, x_1 + x_3, x_2 + x_3 \in y + A$

In ordinary Bogolyubov, we obtain the linear subspace

$V = \mathrm{Spec}_\rho(1_A)^\perp$, determined by heavy Fourier coefficients

The system of forms $x_1, x_2, x_3, x_1 + x_2 + x_3,$

$x_1 + x_2, x_2 + x_3, x_1 + x_3$ has true complexity 2

Hence we require quadratic phases (Gowers–Wolf)

What is "structured"?

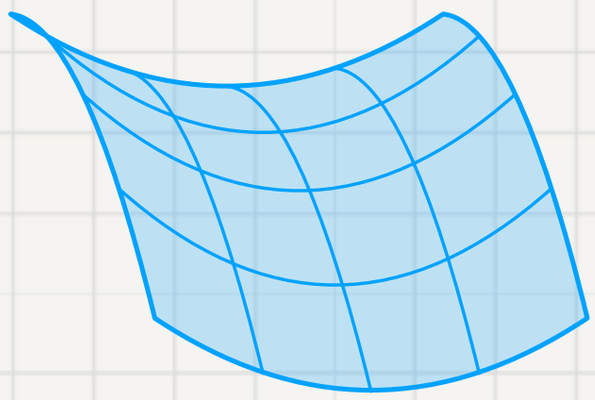
Instead of linear Fourier characters $\chi_s(x) = (-1)^{s \cdot x}$,

we need quadratic phases $(-1)^{xMx^\top + sx}$

The annihilator is a quadratic variety:

$$W = \{x \in \mathbb{F}_2^n : x^\top M_j x + s_i x \quad \forall j \in [q],\ i \in [\ell]\}$$

Variety Complexity



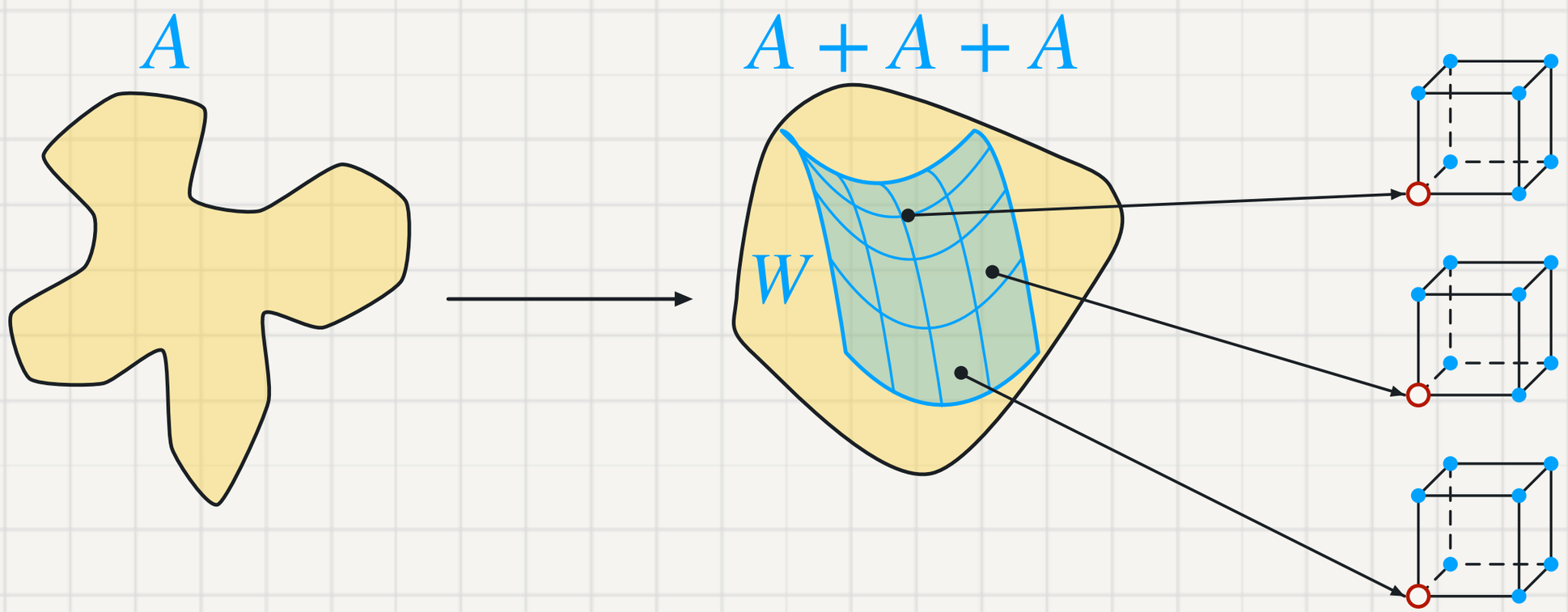
Quadratic Bogolyubov theorem

Theorem 1. Let $A \subseteq \mathbb{F}_2^n$ have density $\alpha > 0$ There exists a quadratic variety $W \subseteq A + A + A$ of complexity $\mathrm{poly}(1/\alpha)$

For every $x \in W$, there are $h_1, h_2, h_3 \in \mathbb{F}_2^n$ such that

$$x + \omega_1 h_1 + \omega_2 h_2 + \omega_3 h_3 \in A \cap W \quad (\forall \omega \in \{0,1\}^3 \setminus \{0\})$$

Peluse [Pel26] independently obtains a similar theorem for $p \geq 5$ in work on the U^4 inverse theorem



Worst-case to average-case for quadratic problems

Theorem 2. Let $Q : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic map

Suppose a uniform quantum algorithm $\mathscr{A}$ runs in time T and

$$\Pr_{x \in \mathbb{F}_2^n}[\mathscr{A}(x) = Q(x)] \geq \alpha$$

Then, for every $\delta > 0$, there is a uniform quantum algorithm $\mathscr{A}'$ with

$$\forall x \in \mathbb{F}_2^n, \quad \Pr[\mathscr{A}'(x) = Q(x)] \geq 1 - \delta$$

Running time: $\widetilde{O}_{\alpha,\delta}(T + n^{5/2})$

Even when the average success is an arbitrarily small constant

Main technical components

1. Algorithmic quadratic Bogolyubov theorem

Density increment and relative U^3 counting give seven-point correction

2. Implicit quadratic Goldreich–Levin

Evaluate the defining polynomials with $\mathrm{polylog}(n)$ queries to A

3. Algorithmic sparse-shift quadratic variety tessellation

Find sparse s with $x + s \in W$, correct there, and shift back

4. Quantum verification and random thresholds

Access the good-input set and amplify the success probability