Worst-case to average-case reductions
via additive combinatorics

[STOC ’22]

Vahid Asadi, Alexander Golovnev, Tom Gur, Igor Shinkar
Plan

① What we do, and why?

② A naive approach + challenges

③ The key idea: local-correction via additive combinatorics

④ Sketch of proof
What we do, and why?
"Boosting knowledge" via average-to-worst case reductions

MATHEMATICIANS ARE WEIRD

YOU KNOW THAT THING THAT WAS 2.3728642?

YES?

Thunderous applause

WE GOT IT DOWN TO 2.3728596

MATHEMATICIANS ARE WEIRD

YOU KNOW THAT THING THAT WAS 2.3728639?

YES?

Thunderous applause

I GOT IT DOWN TO 2.3728639.

smbc-comics.com

smbc-comics.com
"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.

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

Can we boost $\alpha$ 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"

This work focuses on the $1\%$ regime, and even $o(1)$!
Our contribution

A new framework for worst-case to average-case reductions via local-correction lemmas based on additive combinatorics

Applications

1) Algorithms for matrix multiplication

2) Data structures for all linear problems

3) Online matrix-vector multiplication

4) Weak average case: polynomial evaluation
(2) naive approach + challenges

via a concrete example
This talk

Illustrate the framework via matrix multiplication

**Theorem:** If there exists $\text{ALG}$ running in time $T$

s.t. $\Pr[\text{ALG}(A, B) = A \cdot B] \geq \alpha,$

$A, B \in \mathbb{F}^{n \times n}$

then there exists $\text{ALG'}$ running in time $O(T)$

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

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

**Remark:** $O(T)$ hides a factor of roughly $1/8 \alpha$
A trivial special case: high-agreement regime

Suppose \( \Pr[A \cdot B \in \mathbb{F}^n] \geq 0.99 \)
\( A, B \in \mathbb{F}^{n \times n} \)

Same holds for \( \alpha \geq \frac{3}{4} + \varepsilon \)

Idea: BLR-type local correction

1) Sample \( R, S \sim U(\mathbb{F}^{n \times n}) \)

2) Write \( A = R + (A - R), B = S + (B - S) \)

3) Compute \( M = \text{ALG}(R, S) + \text{ALG}(A - R, S) + \text{ALG}(R, B - S) + \text{ALG}(A - R, B - S) \)

Note that \( \Pr[M = A \cdot B] \geq 1 - 4 \cdot 0.01 > \frac{9}{10} \)
The challenge: low-agreement regime

In the 1% regime \( \Pr[A_{\text{alg}}(A, B) = A \cdot B] \geq 0.01 \)

this approach completely breaks

Even for \( \alpha < 0.75 \)

Example:

Suppose \( A_{\text{alg}}(A, B) = A \cdot B \iff A_{11} = 0 \) (o/w \( A_{\text{alg}}(A, B) = 0 \))

Here \( \alpha = 1/2 \), yet no such decomposition

self-correct \( A \cdot B \) if \( A_{11} = 1 \)

Is all hope lost?
③ The key idea:

local-correction via additive combinatorics
Local correction via additive combinatorics

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

The sumset of a set $X$ is defined as

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

These notions quantify a combinatorial analogue of approximate subgroup 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 $\dim(V) \geq n - \frac{1}{2\alpha^2}$.

Key idea: Use Bogolyubov's lemma for local correction.

How? Suppose $\Pr[A \otimes \alpha G(A, B) = A \cdot B] \geq \alpha$

$A, B \in \mathbb{F}_n^{n \times n}$

Denote $X = \{(A, B) : A \otimes \alpha G(A, B) = A \cdot B\}$. Note $\mu(X) \geq \alpha$

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

decomposes to $V = v_1 + v_2 + v_3 + v_4$, $v_1, \ldots, v_4 \in X$
Problems with Bogolyubov local correction

Denote $X = \{ (A, B) : \text{ALG}(A, B) = A \cdot B \}$. Note $\mu(x) \geq \alpha$.

Hence, there exist a large subspace $V$ s.t. $v \in V$ decomposes to $V = X_1 + X_2 + X_3 + X_4$, $x_1, \ldots, x_4 \in X$.

How do we obtain the decomposition?

How to deal with inputs outside of $V$?
Obtaining the decomposition

All we shall need is a probabilistic Bogolyubov lemma.

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. \( \forall v \in V, \Pr[\{x_1, x_2, x_3, v-x_1-x_2-x_3 \in X\}] \geq \alpha^5 \).

This will suffice for matrix multiplication over \( \mathbb{F}_2^n \), and constant \( \alpha > 0 \).
④ Sketch of proof
Matrix multiplication - Sketch of proof

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

Suppose $\text{ALG}$ s.t.

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

Goal: boost $\alpha$ to 1.

For simplicity, assume:

1) $\text{ALG}$ is deterministic.
2) $\mathbb{F} = \mathbb{F}_2$.
3) $\alpha$ is a constant.
4) The input $(A, B)$ satisfies $\Pr_B[\text{ALG}(A, B') = A \cdot B'] \geq \alpha$. 

A \\
(\text{A,B})
Two simple facts

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

**Lemma:** 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 $O(n^2)$

2) Denoting by $X = \{B' \in \mathbb{F}^{n \times n} : \text{ALG}(A, B') = A \cdot B'\}$ the "good" $B$'s, if $B \notin X$, then ALG is successful.

Hence, the goal is to **locally correct** $B \notin X$. 
Local correction via Bogolyubov's lemma

First idea: use Bogolyubov's lemma to locally-correct inputs that lie in a large subspace.

Lemma: Let $X \subseteq \mathbb{F}_2^n$ s.t. $1/2^n \geq \alpha$.

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

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

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

$$\Pr_{x_1,x_2,x_3} \left[ M_1,M_2,M_3,M_4 \in X \right] \geq \alpha^5,$$

where $M_4 = B' - M_1 - M_2 - M_3$.
Local correction via Bogolybov’s lemma

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

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

If this event occurs, then

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

as required.

But success probability $\alpha^5$ is far smaller than desired...

We amplify $O(\frac{1}{\alpha^5})$ times via Freivald’s algorithm?

And what about $B' \not\in V$?
Local correction via Bogolybov’s lemma

Recap: good inputs \( X = \{ B' \in \mathbb{F}^{n \times n} : \text{ALG}(A, B') = A \cdot B' \} \)

Bogolybov subspace \( V \subseteq 4X \)

**Case 1:** If \( B' \in X \), just run \( \text{ALG}(A, B') \)

**Case 2:** If \( B' \in V \), locally correct via Bogolybov’s lemma

**Case 3:** If \( B' \notin V \), um... did we really gain anything?

We started with \( X \) of density \( \alpha \)

\( V \) has smaller density, but it has structure?
Low-rank random matrix shifts

Observation: If $A \in \mathbb{F}^{n \times n}$ has rank $K$, then $AB$ can be computed in time $O(K \cdot n^2)$ given a rank-$K$ decomposition

\[
\begin{array}{ccc}
A & \cdot & B \\
\hline
K \times \text{independent} & & \text{square matrix} \\
(n-K) \times \text{independent} & & \text{square matrix}
\end{array}
\]

- Multiply the indep. rows in time $O(K \cdot n^2)$
- To compute the rest, let $C_i = A_i \cdot B \ \forall i \in [K]$, observe $A_j = \sum_{i=1}^{K} d_i \cdot A_i \implies C_j = \sum_{i=1}^{K} d_i \cdot C_i$, can be computed in time $O(K \cdot n)$ for each $j \in [n]$. 
The reduction

1) Given \((A, B)\), sample \(R_B \in \mathbb{F}^{n \times n}\).

2) Observe that if \(\dim(V) = n^2 - k\), then \(\Pr[B + R_B \in V] \geq \frac{1}{2^{\Omega(k)}}\).

3) Compute \(\text{ALG}_V(A, B + R_B)\).

4) Verify using Freivald's algorithm.

5) Compute \(A \cdot R_B\) in time \(O(k \cdot n^2)\).

6) Return \(\text{ALG}_V(A, B + R_B) - A \cdot R_B\).
Summary & open problems

Worst-case to average-case reductions

**OPTIMIST**

"A new paradigm for designing algorithms?"

**PESSIMIST**

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

This work focuses on the $1\%$ regime and even $o(1)$
Summary & open problems

A new framework for worst-case to average-case reductions via local-correction lemmas based on additive combinatorics

Applications

1) Algorithms for matrix multiplication

2) Data structures for all linear problems

3) Online matrix-vector multiplication

4) Weak average case: polynomial evaluation
Summary & open problems

- Can the framework be extended to other models? E.g., communication complexity, property testing, and PAC learning?

- Can we obtain average-to-worst case reductions for all linear problems for both circuits and uniform algorithms?

Our work reduces the above to efficient verification for the problem.
Thank you!