On Multidimensional and Monotone k-SUM

Chloe Ching-Yun Hsu Chris Umans

Department of Computing and Mathematical Sciences
California Institute of Technology

MFCS 2017

Outline

1. Background
2. Monotone k-SUM
3. Standard vs Strong 3SUM Conjecture
4. Multidimensional k-SUM
5. Proof Outline
6. Open Problems

Outline

Integer 3-SUM

The Integer 3-SUM Problem

Given three sets A_1, A_2, A_3 of integers,
Are there $a_1 \in A_1, a_2 \in A_2, a_3 \in A_3$ such that $a_1 + a_2 = a_3$?

Integer 3-SUM

The Integer 3-SUM Problem

Given three sets A_1, A_2, A_3 of integers,
Are there $a_1 \in A_1, a_2 \in A_2, a_3 \in A_3$ such that $a_1 + a_2 = a_3$?

History

- Introduced as an underlying problem for many computational geometry problems [Gajentaan and Overmars, 1995]
- No significance progress in 20 years
- Subquadratic $O(n^2/(\log n/\log\log n)^{2/3})$ algorithm [Grønlund and Pettie, 2014]

The k-SUM Conjecture

The k-SUM Problem

Given subsets $A_1, \cdots, A_k$ of an abelian group G,
Are there $a_1 \in A_1, \cdots, a_k \in A_k$ such that $\sum_{i=1}^{k} a_i = 0$?

The k-SUM Conjecture

k-SUM in $\mathbb{Z}$ requires randomized time $\Omega(n^{\lceil k/2 \rceil - o(1)})$.

Note: There is a simple $\tilde{O}(n^{\lceil k/2 \rceil})$ time meet-in-the-middle algorithm.

k-SUM Variants

Central Question

What can the standard k-SUM conjecture say about the variants?

k-SUM Variants

Central Question

What can the standard k-SUM conjecture say about the variants?

Motivation

Variants of k-SUM are related to other problems.

- Multidimensional k-SUM:
  Coding theory [Downey et al., 1999]
  Reduction from listing triangles [Jafargholi and Viola, 2016]
- Monotone k-SUM:
  Bounded monotone $(\min, +)$-convolution
  Histogram indexing [Chan and Lewenstein, 2015]

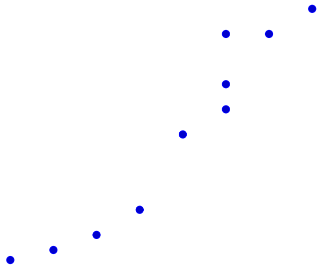
Outline

Bounded Monotone 3SUM

Monotone Set

A set $A \subset \mathbb{Z}^d$ is *monotone* if it can be sorted as monotone increasing in each coordinate.

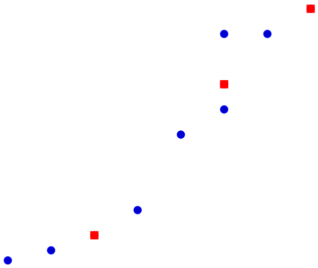
Example (in two dimensions)



Bounded Monotone 3SUM

Given monotone sets $A, B, S \subset [n]^d$,
Are $a \in A, b \in B, s \in S$ such that $a + b = s$?

Example (in two dimensions)



Bounded Monotone 3SUM

- First studied in [Chan and Lewenstein, 2015]
- Chan and Lewenstein gave a remarkable $\tilde{O}(n^{2-\frac{2}{d+13}})$ algorithm using additive combinatorics techniques.

- Can we further improve the algorithm for monotone 3SUM? Or is there a matching lower bound?

Bounded Monotone 3SUM

- First studied in [Chan and Lewenstein, 2015]
- Chan and Lewenstein gave a remarkable $\tilde{O}(n^{2-\frac{2}{d+13}})$ algorithm using additive combinatorics techniques.
- Can we further improve the algorithm for monotone 3SUM? Or is there a matching lower bound?
- Our Result:
  Chan and Lewenstein's algorithm is essentially optimal!

Our Result on Bounded Monotone 3SUM

Theorem (this work)

Under the standard 3SUM conjecture, bounded d-dimensional monotone 3SUM requires time $\Omega(n^{2-\frac{4}{d}-o(1)})$.

Theorem (this work)

Under the strong 3SUM conjecture, bounded d-dimensional monotone 3SUM requires time $\Omega(n^{2-\frac{2}{d}-o(1)})$.

Very close to Chan and Lewenstein's $\tilde{O}(n^{2-\frac{2}{d+13}})$ algorithm!

Outline

Standard vs Strong 3SUM Conjecture

Standard 3SUM Conjecture

Integer 3SUM requires time $\Omega(n^{2-o(1)})$.

Strong 3SUM Conjecture

3SUM on n integers in $\{-n^2, \cdots, n^2\}$ requires time $\Omega(n^{2-o(1)})$.

Are they equivalent?

Note: 3SUM on n integers can be reduced to the bounded domain of $\{-n^3, \cdots, n^3\}$ via randomized reduction.

Standard vs Strong 3SUM Conjecture

$3SUM^+$

Report all "hits" $a_3 \in A_3$ such that $a_1 + a_2 + a_3 = 0$ for some $a_1 \in A_1, a_2 \in A_2$.

Partial result towards showing equivalence:

Theorem (this work)

Under the standard 3SUM conjecture, $3SUM^+$ in the domain of $\{-n^{2+\delta}, \cdots, n^{2+\delta}\}$ requires time $\Omega(n^{2-o(1)})$ for any $\delta > 0$.

Outline

Multidimensional k-SUM in $\mathbb{F}_p^d$

- Instead of $\mathbb{Z}$, take $\mathbb{F}_p^d$ as the underlying abelian group.

- Is multidimensional k-SUM equivalent to integer k-SUM?
- This is not obvious if one tries the straight-forward translation between $\mathbb{Z}$ and $\mathbb{F}_p^d$, due to carries in integer addition.

- The meet-in-the-middle algorithm still runs in $\tilde{O}(n^{\lceil k/2 \rceil})$.
- Is there a matching $\Omega(n^{\lceil k/2 \rceil} - o(1))$ lower bound?

Results on Multidimensional k-SUM

Known lower bounds for multidimensional k-SUM under ETH:

- $\min(n^{\Omega(k)}, 2^{\Omega(d)})$ lower bound. [Bhattacharyya et al., 2011]
- There is no $n^{o(k)}$ algorithm for k-SUM for all k.
  [Pătrașcu and Williams, 2010]

Results on Multidimensional k-SUM

Known lower bounds for multidimensional k-SUM under ETH:

- $\min(n^{\Omega(k)}, 2^{\Omega(d)})$ lower bound. [Bhattacharyya et al., 2011]
- There is no $n^{o(k)}$ algorithm for k-SUM for all k. [Pătrașcu and Williams, 2010]

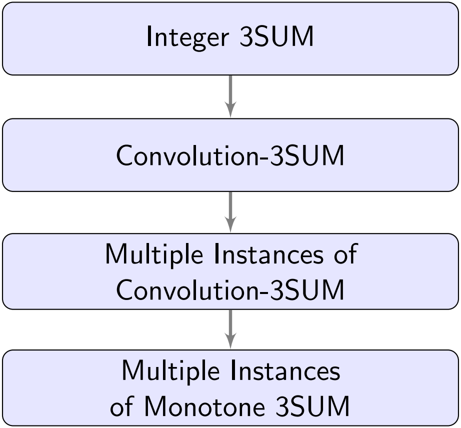
Theorem (this work)

Under the k-SUM conjecture, for sufficiently large p, k-SUM in $\mathbb{F}_p^d$ requires:

- $\Omega(n^{k/2-o(1)})$ *for even* k. *Matching!*
- $\Omega(n^{\lceil k/2 \rceil - 2k\frac{\log k}{\log p} - o(1)})$ *for odd* k. *???*

Outline

Proof Outline for Bounded Monotone 3SUM Result



Integer 3SUM $\rightarrow$ Convolution-3SUM

Convolution-3SUM

Given an array $A[1 \cdots n]$, determine whether there exist $i \neq j$ such that $A[i] + A[j] = A[i + j]$.

[Pătrașcu, 2010] If 3SUM requires $\Omega(n^{2-o(1)})$ time, then so does Convolution 3SUM.

[Amir et al., 2014] Convolution-3SUM can be reduced to the domain $\{-n^2, \cdots, n^2\}$ via randomized reduction.

Convolution-3SUM → Multiple Instances

Lemma

For any given dimension d, Convolution-3SUM in $[m]$ can be reduced to 4^d instances of Convolution-3SUM in $[m^{1/d}]^d$.

Proof idea:

View $[m^{1/d}]^d$ as base-$(m^{1/d})$ integer representation.
There are 4^d different situations of carries in integer addition.

Convolution-3SUM $\rightarrow$ Monotone 3SUM

Lemma

Convolution-3SUM in $[m]^d$ can be reduced to Convolution-3SUM on monotone sets in $[nm]^d$.

Proof idea:

Convolution-3SUM can be seen as 3SUM in $[n] \times [m]$.
Map $[n] \times [m]^d \rightarrow [n] \times [nm]^d$ by

$$(b, a_1, \cdots, a_d) \mapsto (b, mb + a_1, \cdots, mb + a_d)$$

Putting it Together

Lemma

If monotone 3SUM in $[n]^d$ *can be solved in time* $O(n^{2-2c/d-\delta})$, *then Convolution-3SUM in* $[n^c]$ *can be solved in time* $O(n^{2-\delta/2})$.

- Take $c = 2$ for standard 3SUM conjecture.
- Take $c = 1$ for strong 3SUM conjecture.

Outline

Open Problems

- Is there a faster multidimensional k-SUM algorithm for odd k? Or a tighter lower bound?

  In particular, is there a $O(n^{2-\frac{c}{\log p}})$ algorithm for 3SUM in $\mathbb{F}_p^d$?

Open Problems

- Is there a faster multidimensional k-SUM algorithm for odd k? Or a tighter lower bound?

  In particular, is there a $O(n^{2-\frac{c}{\log p}})$ algorithm for 3SUM in $\mathbb{F}_p^d$?

- Is there a lower bound for 3XOR under the 3SUM conjecture?

  Even an $O(n^{1.99})$ algorithm or an $O(n^{1.01})$ lower bound would be significant.

Reference I

Amir, A., Chan, T. M., Lewenstein, M., and Lewenstein, N. (2014).
On hardness of jumbled indexing.
In *Automata, Languages, and Programming*, pages 114–125. Springer.

Bhattacharyya, A., Indyk, P., Woodruff, D. P., and Xie, N. (2011).
The complexity of linear dependence problems in vector spaces.
In *ICS*, pages 496–508.

Chan, T. M. and Lewenstein, M. (2015).
Clustered integer 3SUM via additive combinatorics.
In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing*, pages 31–40. ACM.

Downey, R. G., Fellows, M. R., Vardy, A., and Whittle, G. (1999).
The parametrized complexity of some fundamental problems in coding theory.
SIAM Journal on Computing, 29(2):545–570.

Gajentaan, A. and Overmars, M. H. (1995).
On a class of $O(n^2)$ problems in computational geometry.
Computational Geometry, 5(3):165–185.

Reference II

Grønlund, A. and Pettie, S. (2014).
Threesomes, degenerates, and love triangles.
In *Foundations of Computer Science (FOCS), 2014 IEEE 55th Annual Symposium on*, pages 621–630. IEEE.

Jafargholi, Z. and Viola, E. (2016).
3SUM, 3XOR, triangles.
Algorithmica, 74(1):326–343.

Pătraşcu, M. (2010).
Towards polynomial lower bounds for dynamic problems.
In *Proceedings of the Forty-Second ACM Symposium on Theory of computing*, pages 603–610. ACM.

Pătraşcu, M. and Williams, R. (2010).
On the possibility of faster SAT algorithms.
In *Proceedings of the Twenty-First Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1065–1075. SIAM.