All Non-trivial Variants of 3-LDT Are Equivalent

Bartłomiej Dudek[1] Paweł Gawrychowski[1]
Tatiana Starikovskaya[2]

[1]University of Wrocław, Poland

[2]École normale supérieure, France

3-SUM

Given a set $X \subseteq U$ of n numbers, are there distinct $x_1, x_2, x_3 \in X$ such that $x_1 + x_2 + x_3 = 0$?

Folklore $\mathcal{O}(n^2)$ algorithm:

Gajentaan and Overmars 1995

Multiple geometric problems are 3-SUM-hard.

3-SUM

Given a set $X \subseteq U$ of n numbers, are there distinct $x_1, x_2, x_3 \in X$ such that $x_1 + x_2 + x_3 = 0$?

Folklore $\mathcal{O}(n^2)$ algorithm:

$$-8 \quad -5 \quad -2 \quad 1 \quad 4 \quad 7 \quad 8$$

Gajentaan and Overmars 1995

Multiple geometric problems are 3-SUM-hard.

3-SUM

Given a set $X \subseteq U$ of n numbers, are there distinct $x_1, x_2, x_3 \in X$ such that $x_1 + x_2 + x_3 = 0$?

Folklore $\mathcal{O}(n^2)$ algorithm:

$$\begin{array}{ccccccc} & & & x_1 & & & \\ -8 & -5 & -2 & 1 & 4 & 7 & 8 \\ x_2 \rightarrow & & & & & & \leftarrow x_3 \end{array}$$

Gajentaan and Overmars 1995

Multiple geometric problems are 3-SUM-hard.

3-SUM

Given a set $X \subseteq U$ of n numbers, are there distinct $x_1, x_2, x_3 \in X$ such that $x_1 + x_2 + x_3 = 0$?

Folklore $\mathcal{O}(n^2)$ algorithm:

$$\begin{array}{ccccccc} & & & x_1 & & & \\ -8 & -5 & -2 & 1 & 4 & 7 & 8 \\ x_2 \rightarrow & & & & & & \leftarrow x_3 \end{array}$$

Gajentaan and Overmars 1995

Multiple geometric problems are 3-SUM-hard.

3-SUM

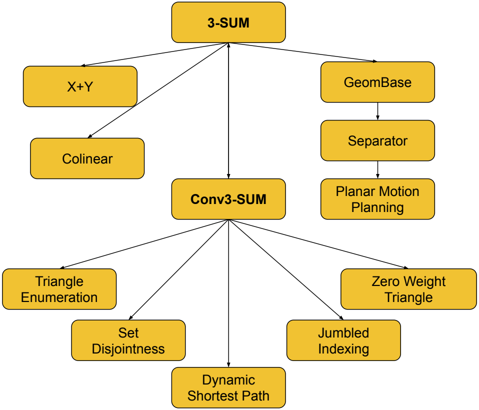
Given a set $X \subseteq [-\mathbf{n^3}, \mathbf{n^3}]$ of n **integers**, are there distinct $x_1, x_2, x_3 \in X$ such that $x_1 + x_2 + x_3 = 0$?

Folklore $\mathcal{O}(n^2)$ algorithm:

$$
\begin{array}{ccccccc}
 & & & x_1 & & & \\
-8 & -5 & -2 & 1 & 4 & 7 & 8 \\
x_2 \rightarrow & & & & & \leftarrow x_3 &
\end{array}
$$

Gajentaan and Overmars 1995

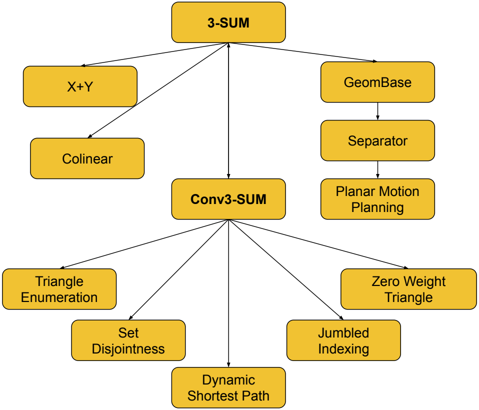
Multiple geometric problems are 3-SUM-hard.



Based on Karl Bringmann's slide (`link`)

3-SUM Conjecture

3-SUM has no $\mathcal{O}(n^{2-\epsilon})$ expected time algorithm, for any $\epsilon > 0$, on Word RAM with words of length $\mathcal{O}(\log n)$.



Based on Karl Bringmann's slide (`link`)

3-SUM Conjecture

3-SUM has no $\mathcal{O}(n^{2-\epsilon})$ expected time algorithm, for any $\epsilon > 0$, on Word RAM with words of length $\mathcal{O}(\log n)$.

State of the art about 3-SUM

Chan 2018

$\mathcal{O}((n^2/\log^2 n)(\log\log n)^{\mathcal{O}(1)})$-time algorithm 3-SUM on n real numbers.

Linear Decision Trees model:

Authors	Year	Linearity	Depth
Grønlund and Pettie	2014	4	$\mathcal{O}(n^{1.5}\sqrt{\log n})$
Gold and Sharir	2015	4	$\mathcal{O}(n^{1.5})$
Kane, Lovett, and Moran	2017	8	$\mathcal{O}(n\log^2 n)$

State of the art about 3-SUM

Chan 2018

$\mathcal{O}((n^2/\log^2 n)(\log\log n)^{\mathcal{O}(1)})$-time algorithm 3-SUM on n real numbers.

Linear Decision Trees model:

Authors	Year	Linearity	Depth
Grønlund and Pettie	2014	4	$\mathcal{O}(n^{1.5}\sqrt{\log n})$
Gold and Sharir	2015	4	$\mathcal{O}(n^{1.5})$
Kane, Lovett, and Moran	2017	8	$\mathcal{O}(n \log^2 n)$

State of the art about 3-SUM

Chan 2018

$\mathcal{O}((n^2/\log^2 n)(\log\log n)^{\mathcal{O}(1)})$-time algorithm 3-SUM on n real numbers.

Linear Decision Trees model:

Authors	Year	Linearity	Depth
Grønlund and Pettie	2014	4	$\mathcal{O}(n^{1.5}\sqrt{\log n})$
Gold and Sharir	2015	4	$\mathcal{O}(n^{1.5})$
Kane, Lovett, and Moran	2017	8	$\mathcal{O}(n\log^2 n)$

AVERAGE

Given a set $X \subseteq [-n^3, n^3]$ of n integers, are there distinct $x_1, x_2, x_3 \in X$ such that $x_1 + x_2 = 2x_3$?

In other words, is X progression-free?

There exists a reduction from AVERAGE to $\log n$ instances of 3-SUM.

AVERAGE

Given a set $X \subseteq [-n^3, n^3]$ of n integers, are there distinct $x_1, x_2, x_3 \in X$ such that $x_1 + x_2 = 2x_3$?

In other words, is X progression-free?

There exists a reduction from AVERAGE to $\log n$ instances of 3-SUM.

AVERAGE

Given a set $X \subseteq [-n^3, n^3]$ of n integers, are there distinct $x_1, x_2, x_3 \in X$ such that $x_1 + x_2 = 2x_3$?

In other words, is X progression-free?

There exists a reduction from AVERAGE to $\log n$ instances of 3-SUM.

What if 3-SUM is more difficult than AVERAGE?

Erickson 1999

It is not known whether AVERAGE is 3SUM-hard. [...] (Thus, 3SUM-hard problems might better be called “AVERAGE-hard”.)

JeffE on `cs.stackexchange.com` in 2013:

Can we reduce 3-SUM to AVERAGE?

What if 3-SUM is more difficult than AVERAGE?

Erickson 1999

It is not known whether AVERAGE is 3SUM-hard. [...] (Thus, 3SUM-hard problems might better be called “AVERAGE-hard”.)

JeffE on `cs.stackexchange.com` in 2013:

Can we reduce 3-SUM to AVERAGE?

What if 3-SUM is more difficult than AVERAGE?

Erickson 1999

It is not known whether AVERAGE is 3SUM-hard. [...] (Thus, 3SUM-hard problems might better be called "AVERAGE-hard".)

JeffE on `cs.stackexchange.com` in 2013:

Unfortunately, it is not known whether Average is (even weakly) 3SUM-hard! I suspect that Average is actually **not** 3SUM-hard, if only because the $\Omega(n^2)$ lower bound for Average is *considerably* harder to prove than the $\Omega(n^2)$ lower bound for 3SUM.

How to synthesize non-pitched sounds? How pitched is a sound in general?

How can I check if a new group is OK with a

Can we reduce 3-SUM to AVERAGE?

3-Linear Degeneracy Testing (3-LDT)

3-LDT($1, \bar{\alpha}, t$) (1-partite)

Parameters: Integer coefficients $\alpha_1, \alpha_2, \alpha_3$ and t.
Input: Set $X \subseteq \{-n^3, \ldots, n^3\}$ of size n.
Output: Are there distinct $x_1, x_2, x_3 \in X$ such that $\sum_{i=1}^{3} \alpha_i x_i = t$?

3-LDT($3, \bar{\alpha}, t$) (3-partite)

Parameters: Integer coefficients $\alpha_1, \alpha_2, \alpha_3$ and t.
Input: Sets $A_1, A_2, A_3 \subseteq \{-n^3, \ldots, n^3\}$ of size n.
Output: Are there $x_1 \in A_1, x_2 \in A_2, x_3 \in A_3$ such that $\sum_{i=1}^{3} \alpha_i x_i = t$?

3-Linear Degeneracy Testing (3-LDT)

3-LDT($1, \bar{\alpha}, t$) (1-partite)

Parameters: Integer coefficients $\alpha_1, \alpha_2, \alpha_3$ and t.
Input: Set $X \subseteq \{-n^3, \ldots, n^3\}$ of size n.
Output: Are there distinct $x_1, x_2, x_3 \in X$ such that $\sum_{i=1}^{3} \alpha_i x_i = t$?

3-LDT($3, \bar{\alpha}, t$) (3-partite)

Parameters: Integer coefficients $\alpha_1, \alpha_2, \alpha_3$ and t.
Input: Sets $A_1, A_2, A_3 \subseteq \{-n^3, \ldots, n^3\}$ of size n.
Output: Are there $x_1 \in A_1, x_2 \in A_2, x_3 \in A_3$ such that $\sum_{i=1}^{3} \alpha_i x_i = t$?

3-Linear Degeneracy Testing (3-LDT)

3-LDT$(1, \bar{\alpha}, t)$ (1-partite)

Parameters: Integer coefficients $\alpha_1, \alpha_2, \alpha_3$ and t.
Input: Set $\mathbf{X} \subseteq \{-n^3, \ldots, n^3\}$ of size n.
Output: Are there **distinct** $\mathbf{x_1}, \mathbf{x_2}, \mathbf{x_3} \in \mathbf{X}$ such that $\sum_{i=1}^{3} \alpha_i x_i = t$?

3-LDT$(3, \bar{\alpha}, t)$ (3-partite)

Parameters: Integer coefficients $\alpha_1, \alpha_2, \alpha_3$ and t.
Input: Sets $\mathbf{A_1}, \mathbf{A_2}, \mathbf{A_3} \subseteq \{-n^3, \ldots, n^3\}$ of size n.
Output: Are there $\mathbf{x_1} \in \mathbf{A_1}, \mathbf{x_2} \in \mathbf{A_2}, \mathbf{x_3} \in \mathbf{A_3}$ such that $\sum_{i=1}^{3} \alpha_i x_i = t$?

Trivial and non-trivial variants

Some combinations of the parameters $\bar{\alpha}$ and t are easy to solve:

1. any of the coefficients α_i is 0, or
2. $t \neq 0$ and $\gcd(\alpha_1, \alpha_2, \alpha_3) \nmid t$.

We call all other other variants (1- and 3-partite) non-trivial.

Theorem

All non-trivial variants of 3-LDT are subquadratic-equivalent.

In particular, AVERAGE is 3-SUM-hard!

Trivial and non-trivial variants

Some combinations of the parameters $\bar{\alpha}$ and t are easy to solve:

1. any of the coefficients α_i is 0, or
2. $t \neq 0$ and $\gcd(\alpha_1, \alpha_2, \alpha_3) \nmid t$.

We call all other other variants (1- and 3-partite) non-trivial.

Theorem

All non-trivial variants of 3-LDT are subquadratic-equivalent.

In particular, AVERAGE is 3-SUM-hard!

Trivial and non-trivial variants

Some combinations of the parameters $\bar{\alpha}$ and t are easy to solve:

1. any of the coefficients α_i is 0, or
2. $t \neq 0$ and $\gcd(\alpha_1, \alpha_2, \alpha_3) \nmid t$.

We call all other other variants (1- and 3-partite) non-trivial.

Theorem

All non-trivial variants of 3-LDT are subquadratic-equivalent.

In particular, AVERAGE is 3-SUM-hard!

Trivial and non-trivial variants

Some combinations of the parameters $\bar{\alpha}$ and t are easy to solve:

1. any of the coefficients α_i is 0, or
2. $t \neq 0$ and $\gcd(\alpha_1, \alpha_2, \alpha_3) \nmid t$.

We call all other other variants (1- and 3-partite) non-trivial.

Theorem

All non-trivial variants of 3-LDT are subquadratic-equivalent.

In particular, AVERAGE is 3-SUM-hard!

Trivial and non-trivial variants

Some combinations of the parameters $\bar{\alpha}$ and t are easy to solve:

1. any of the coefficients α_i is 0, or
2. $t \neq 0$ and $\gcd(\alpha_1, \alpha_2, \alpha_3) \nmid t$.

We call all other other variants (1- and 3-partite) non-trivial.

Theorem

All non-trivial variants of 3-LDT are subquadratic-equivalent.

In particular, AVERAGE is 3-SUM-hard!

Trivial and non-trivial variants

Some combinations of the parameters $\bar{\alpha}$ and t are easy to solve:

1. any of the coefficients α_i is 0, or
2. $t \neq 0$ and $\gcd(\alpha_1, \alpha_2, \alpha_3) \nmid t$.

We call all other other variants (1- and 3-partite) non-trivial.

Theorem

All non-trivial variants of 3-LDT are subquadratic-equivalent.

In particular, AVERAGE is 3-SUM-hard!

3-partite variants

Warm-up

All non-trivial 3-partite variants are equivalent.

Proof: scale and shift each A_i appropriately:

- $(\bar{\alpha}, 0) \to (\bar{\alpha}, t)$: set $A'_i = \{x + y_i : x \in A_i\}$ where y_i satisfy: $\sum_i \alpha_i y_i = t$ (from Chinese remainder theorem)
- $(\bar{\alpha}, 0) \to (\bar{\beta}, 0)$: set $A'_i = \{x \frac{\alpha_i \operatorname{lcm}(\beta_1, \beta_2, \beta_3)}{\beta_i} : x \in A_i\}$

Remaining part of the talk

Equivalence between 1- and 3-partite variants with the same $\bar{\alpha}$ and t.

3-partite variants

Warm-up

All non-trivial 3-partite variants are equivalent.

Proof: scale and shift each A_i appropriately:

- $(\bar{\alpha}, 0) \to (\bar{\alpha}, t)$: set $A'_i = \{x + y_i : x \in A_i\}$ where y_i satisfy: $\sum_i \alpha_i y_i = t$ (from Chinese remainder theorem)
- $(\bar{\alpha}, 0) \to (\bar{\beta}, 0)$: set $A'_i = \{x \frac{\alpha_i \operatorname{lcm}(\beta_1, \beta_2, \beta_3)}{\beta_i} : x \in A_i\}$

Remaining part of the talk

Equivalence between 1- and 3-partite variants with the same $\bar{\alpha}$ and t.

3-partite variants

Warm-up

All non-trivial 3-partite variants are equivalent.

Proof: scale and shift each A_i appropriately:

- $(\bar{\alpha}, 0) \to (\bar{\alpha}, t)$: set $A'_i = \{x + y_i : x \in A_i\}$ where y_i satisfy: $\sum_i \alpha_i y_i = t$ (from Chinese remainder theorem)
- $(\bar{\alpha}, 0) \to (\bar{\beta}, 0)$: set $A'_i = \{x \frac{\alpha_i \operatorname{lcm}(\beta_1, \beta_2, \beta_3)}{\beta_i} : x \in A_i\}$

Remaining part of the talk

Equivalence between 1- and 3-partite variants with the same $\bar{\alpha}$ and t.

3-partite variants

Warm-up

All non-trivial 3-partite variants are equivalent.

Proof: scale and shift each A_i appropriately:

- $(\bar{\alpha}, 0) \to (\bar{\alpha}, t)$: set $A'_i = \{x + y_i : x \in A_i\}$ where y_i satisfy: $\sum_i \alpha_i y_i = t$ (from Chinese remainder theorem)
- $(\bar{\alpha}, 0) \to (\bar{\beta}, 0)$: set $A'_i = \{x \frac{\alpha_i \operatorname{lcm}(\beta_1, \beta_2, \beta_3)}{\beta_i} : x \in A_i\}$

Remaining part of the talk

Equivalence between 1- and 3-partite variants with the same $\bar{\alpha}$ and t.

From 1-partite to 3-partite

What if we set all sets A_i equal to X?

- if there is a correct solution, we would find it
- in 3-SUM we could take one element twice, i.e.: 4,4,-8
- in AVERAGE we could take any element 3 times: 4,4,4

We can't set all sets A_i equal to X!

Color-coding, Alon et al. 1995

It suffices to consider $\mathcal{O}(\log^2 n)$ 3-partite instances.

From 1-partite to 3-partite

What if we set all sets A_i equal to X?

- if there is a correct solution, we would find it
- in 3-SUM we could take one element twice, i.e.: 4,4,-8
- in AVERAGE we could take any element 3 times: 4,4,4

We can't set all sets A_i equal to X!

Color-coding, Alon et al. 1995

It suffices to consider $\mathcal{O}(\log^2 n)$ 3-partite instances.

From 1-partite to 3-partite

What if we set all sets A_i equal to X?

- if there is a correct solution, we would find it
- in 3-SUM we could take one element twice, i.e.: 4,4,-8
- in AVERAGE we could take any element 3 times: 4,4,4

We can't set all sets A_i equal to X!

Color-coding, Alon et al. 1995

It suffices to consider $\mathcal{O}(\log^2 n)$ 3-partite instances.

From 1-partite to 3-partite

What if we set all sets A_i equal to X?

- if there is a correct solution, we would find it
- in 3-SUM we could take one element twice, i.e.: 4,4,-8
- in AVERAGE we could take any element 3 times: 4,4,4

We can't set all sets A_i equal to X!

Color-coding, Alon et al. 1995

It suffices to consider $\mathcal{O}(\log^2 n)$ 3-partite instances.

From 1-partite to 3-partite

What if we set all sets A_i equal to X?

- if there is a correct solution, we would find it
- in 3-SUM we could take one element twice, i.e.: 4,4,-8
- in AVERAGE we could take any element 3 times: 4,4,4

We can't set all sets A_i equal to X!

Color-coding, Alon et al. 1995

It suffices to consider $\mathcal{O}(\log^2 n)$ 3-partite instances.

From 3-partite to 1-partite

Reduction for 3-SUM

$$X = (8A_1 + 1) \cup (8A_2 + 3) \cup (8A_3 - 4)$$

Goal: any solution consisting of distinct $x_1, x_2, x_3 \in X$ should satisfy that every x_i corresponds to an element of A_i.

For an arbitrary variant of 3-LDT:

$$X = \bigcup_i \{Ca + \gamma_i : a \in A_i\}$$

We need the smaller-order parts to cancel out, so $\sum_i \alpha_i \gamma_i = 0$.

Corner case: some α_is might be equal, we need to allow permuting x_is with equal coefficients.

From 3-partite to 1-partite

Reduction for 3-SUM

$$X = (8A_1 + 1) \cup (8A_2 + 3) \cup (8A_3 - 4)$$

Goal: any solution consisting of distinct $x_1, x_2, x_3 \in X$ should satisfy that every x_i corresponds to an element of A_i.

For an arbitrary variant of 3-LDT:

$$X = \bigcup_i \{Ca + \gamma_i : a \in A_i\}$$

We need the smaller-order parts to cancel out, so $\sum_i \alpha_i \gamma_i = 0$.

Corner case: some α_is might be equal, we need to allow permuting x_is with equal coefficients.

From 3-partite to 1-partite

Reduction for 3-SUM

$$X = (8A_1 + 1) \cup (8A_2 + 3) \cup (8A_3 - 4)$$

Goal: any solution consisting of distinct $x_1, x_2, x_3 \in X$ should satisfy that every x_i corresponds to an element of A_i.

For an arbitrary variant of 3-LDT:

$$X = \bigcup_i \{Ca + \gamma_i : a \in A_i\}$$

We need the smaller-order parts to cancel out, so $\sum_i \alpha_i \gamma_i = 0$.

Corner case: some α_is might be equal, we need to allow permuting x_is with equal coefficients.

From 3-partite to 1-partite

Reduction for 3-SUM

$$X = (8A_1 + 1) \cup (8A_2 + 3) \cup (8A_3 - 4)$$

Goal: any solution consisting of distinct $x_1, x_2, x_3 \in X$ should satisfy that every x_i corresponds to an element of A_i.

For an arbitrary variant of 3-LDT:

$$X = \bigcup_i \{Ca + \gamma_i : a \in A_i\}$$

We need the smaller-order parts to cancel out, so $\sum_i \alpha_i \gamma_i = 0$.

Corner case: some α_is might be equal, we need to allow permuting x_is with equal coefficients.

From 3-partite to 1-partite

Reduction for 3-SUM

$$X = (8A_1 + 1) \cup (8A_2 + 3) \cup (8A_3 - 4)$$

Goal: any solution consisting of distinct $x_1, x_2, x_3 \in X$ should satisfy that every x_i corresponds to an element of A_i.

For an arbitrary variant of 3-LDT:

$$X = \bigcup_i \{Ca + \gamma_i : a \in A_i\}$$

We need the smaller-order parts to cancel out, so $\sum_i \alpha_i \gamma_i = 0$.

Corner case: some α_is might be equal, we need to allow permuting x_is with equal coefficients.

When can we find such a transformation?

Lemma

If $t \neq 0$ or $\sum_i \alpha_i \neq 0$ we can find such "good" coefficients $\gamma_1, \gamma_2, \gamma_3$.

Proof idea: Consider the 3-dimensional space of all possible coefficients, write down a finite set of "forbidden" planes. Show that the plane corresponding to $\sum_i \alpha_i \gamma_i = 0$ contains a point with rational coordinates that doesn't belong to any "forbidden" plane, scale it up.

If $t = 0$ and $\sum_i \alpha_i = 0$, we cannot hope to eliminate solutions that use three elements from the same set A_j.

Problem: some A_j contains a solution to the equation $\sum_i \alpha_i x_i = 0$.

When can we find such a transformation?

Lemma

If $t \neq 0$ or $\sum_i \alpha_i \neq 0$ we can find such "good" coefficients $\gamma_1, \gamma_2, \gamma_3$.

Proof idea: Consider the 3-dimensional space of all possible coefficients, write down a finite set of "forbidden" planes. Show that the plane corresponding to $\sum_i \alpha_i \gamma_i = 0$ contains a point with rational coordinates that doesn't belong to any "forbidden" plane, scale it up.

If $t = 0$ and $\sum_i \alpha_i = 0$, we cannot hope to eliminate solutions that use three elements from the same set A_j.

Problem: some A_j contains a solution to the equation $\sum_i \alpha_i x_i = 0$.

When can we find such a transformation?

Lemma

If $t \neq 0$ or $\sum_i \alpha_i \neq 0$ we can find such "good" coefficients $\gamma_1, \gamma_2, \gamma_3$.

Proof idea: Consider the 3-dimensional space of all possible coefficients, write down a finite set of "forbidden" planes. Show that the plane corresponding to $\sum_i \alpha_i \gamma_i = 0$ contains a point with rational coordinates that doesn't belong to any "forbidden" plane, scale it up.

If $t = 0$ and $\sum_i \alpha_i = 0$, we cannot hope to eliminate solutions that use three elements from the same set A_j.

Problem: some A_j contains a solution to the equation $\sum_i \alpha_i x_i = 0$.

When can we find such a transformation?

Lemma

If $t \neq 0$ or $\sum_i \alpha_i \neq 0$ we can find such "good" coefficients $\gamma_1, \gamma_2, \gamma_3$.

Proof idea: Consider the 3-dimensional space of all possible coefficients, write down a finite set of "forbidden" planes. Show that the plane corresponding to $\sum_i \alpha_i \gamma_i = 0$ contains a point with rational coordinates that doesn't belong to any "forbidden" plane, scale it up.

If $t = 0$ and $\sum_i \alpha_i = 0$, we cannot hope to eliminate solutions that use three elements from the same set A_j.

Problem: some A_j contains a solution to the equation $\sum_i \alpha_i x_i = 0$.

When can we find such a transformation?

Lemma

If $t \neq 0$ or $\sum_i \alpha_i \neq 0$ we can find such “good” coefficients $\gamma_1, \gamma_2, \gamma_3$.

Proof idea: Consider the 3-dimensional space of all possible coefficients, write down a finite set of “forbidden” planes. Show that the plane corresponding to $\sum_i \alpha_i \gamma_i = 0$ contains a point with rational coordinates that doesn’t belong to any “forbidden” plane, scale it up.

If $t = 0$ and $\sum_i \alpha_i = 0$, we cannot hope to eliminate solutions that use three elements from the same set A_j.

Problem: some A_j contains a solution to the equation $\sum_i \alpha_i x_i = 0$.

When can we find such a transformation?

Lemma

If $t \neq 0$ or $\sum_i \alpha_i \neq 0$ we can find such "good" coefficients $\gamma_1, \gamma_2, \gamma_3$.

Proof idea: Consider the 3-dimensional space of all possible coefficients, write down a finite set of "forbidden" planes. Show that the plane corresponding to $\sum_i \alpha_i \gamma_i = 0$ contains a point with rational coordinates that doesn't belong to any "forbidden" plane, scale it up.

If $t = 0$ and $\sum_i \alpha_i = 0$, we cannot hope to eliminate solutions that use three elements from the same set A_j.

Problem: some A_j contains a solution to the equation $\sum_i \alpha_i x_i = 0$.

Behrend's set

A set $S \subseteq [1, N]$ is progression-free if it contains no three distinct elements a, b, c such that $a + b = 2c$.

Behrend 1946

There exists a progression-free set of size $\Omega(N/(2^{\sqrt{8 \log N}} \log^{1/4} N))$.

This can be easily generalised to avoid any fixed linear combination $\gamma a + \delta b = (\gamma + \delta)c$ at the expense of decreasing the size of the set to $N/2^{\mathcal{O}(\sqrt{\log N})}$. We call such set (γ, δ)-free.

The trick

Partition every A_j into not too many (γ, δ)-free subsets A_j^i. Run the previous reduction on every triple $A_1^{i_1}, A_2^{i_2}, A_3^{i_3}$.

Behrend's set

A set $S \subseteq [1, N]$ is progression-free if it contains no three distinct elements a, b, c such that $a + b = 2c$.

Behrend 1946

There exists a progression-free set of size $\Omega(N/(2^{\sqrt{8 \log N}} \log^{1/4} N))$.

This can be easily generalised to avoid any fixed linear combination $\gamma a + \delta b = (\gamma + \delta)c$ at the expense of decreasing the size of the set to $N/2^{\mathcal{O}(\sqrt{\log N})}$. We call such set (γ, δ)-free.

The trick

Partition every A_j into not too many (γ, δ)-free subsets A_j^i. Run the previous reduction on every triple $A_1^{i_1}, A_2^{i_2}, A_3^{i_3}$.

Behrend's set

A set $S \subseteq [1, N]$ is progression-free if it contains no three distinct elements a, b, c such that $a + b = 2c$.

Behrend 1946

There exists a progression-free set of size $\Omega(N/(2^{\sqrt{8 \log N}} \log^{1/4} N))$.

This can be easily generalised to avoid any fixed linear combination $\gamma a + \delta b = (\gamma + \delta)c$ at the expense of decreasing the size of the set to $N/2^{\mathcal{O}(\sqrt{\log N})}$. We call such set (γ, δ)-free.

The trick

Partition every A_j into not too many (γ, δ)-free subsets A_j^i. Run the previous reduction on every triple $A_1^{i_1}, A_2^{i_2}, A_3^{i_3}$.

Behrend's set

A set $S \subseteq [1, N]$ is progression-free if it contains no three distinct elements a, b, c such that $a + b = 2c$.

Behrend 1946

There exists a progression-free set of size $\Omega(N/(2^{\sqrt{8 \log N}} \log^{1/4} N))$.

This can be easily generalised to avoid any fixed linear combination $\gamma a + \delta b = (\gamma + \delta)c$ at the expense of decreasing the size of the set to $N/2^{\mathcal{O}(\sqrt{\log N})}$. We call such set (γ, δ)-free.

The trick

Partition every A_j into not too many (γ, δ)-free subsets A_j^i. Run the previous reduction on every triple $A_1^{i_1}, A_2^{i_2}, A_3^{i_3}$.

Applying Behrend's set

Lemma

For any N, γ, δ, there exists a collection of (γ, δ)-free sets $S_1, S_2, \ldots, S_c$ such that $c = 2^{\mathcal{O}(\sqrt{\log N})}$ and $\bigcup_i S_i = [1, N]$.

Proof:

- By Behrend's construction, there exists a (γ, δ)-free set $Q \subseteq [1, N]$ of size N/w, for $w = 2^{\mathcal{O}(\sqrt{\log N})}$.
- For $y \in [1, N]$, $P(y \in (Q + \Delta)) \geq 1/2w$ when $\Delta \in_{\text{u.a.r.}} [-N, N]$.
- For $c = \mathcal{O}(w \log N)$ we get $P(y \notin \bigcup_i^c (Q + \Delta_i)) < 1/N^2$.

Applying Behrend's set

Lemma

For any N, γ, δ, there exists a collection of (γ, δ)-free sets $S_1, S_2, \ldots, S_c$ such that $c = 2^{\mathcal{O}(\sqrt{\log N})}$ and $\bigcup_i S_i = [1, N]$.

Proof:

- By Behrend's construction, there exists a (γ, δ)-free set $Q \subseteq [1, N]$ of size N/w, for $w = 2^{\mathcal{O}(\sqrt{\log N})}$.
- For $y \in [1, N]$, $P(y \in (Q + \Delta)) \geq 1/2w$ when $\Delta \in_{\text{u.a.r.}} [-N, N]$.
- For $c = \mathcal{O}(w \log N)$ we get $P(y \notin \bigcup_i^c (Q + \Delta_i)) < 1/N^2$.

Applying Behrend's set

Lemma

For any N, γ, δ, there exists a collection of (γ, δ)-free sets $S_1, S_2, \ldots, S_c$ such that $c = 2^{\mathcal{O}(\sqrt{\log N})}$ and $\bigcup_i S_i = [1, N]$.

Proof:

- By Behrend's construction, there exists a (γ, δ)-free set $Q \subseteq [1, N]$ of size N/w, for $w = 2^{\mathcal{O}(\sqrt{\log N})}$.
- For $y \in [1, N]$, $P(y \in (Q + \Delta)) \geq 1/2w$ when $\Delta \in_{\text{u.a.r.}} [-N, N]$.
- For $c = \mathcal{O}(w \log N)$ we get $P(y \notin \bigcup_i^c (Q + \Delta_i)) < 1/N^2$.

Applying Behrend's set

Lemma

For any N, γ, δ, there exists a collection of (γ, δ)-free sets $S_1, S_2, \ldots, S_c$ such that $c = 2^{\mathcal{O}(\sqrt{\log N})}$ and $\bigcup_i S_i = [1, N]$.

Proof:

- By Behrend's construction, there exists a (γ, δ)-free set $Q \subseteq [1, N]$ of size N/w, for $w = 2^{\mathcal{O}(\sqrt{\log N})}$.
- For $y \in [1, N]$, $P(y \in (Q + \Delta)) \geq 1/2w$ when $\Delta \in_{\text{u.a.r.}} [-N, N]$.
- For $c = \mathcal{O}(w \log N)$ we get $P(y \notin \bigcup_i^c (Q + \Delta_i)) < 1/N^2$.

Technical difficulties we overcome in the paper

- existence → construction
- $U = [-n^3, n^3]$, so we can't store the whole Behrend's set → implicit representation
- random shifts → derandomization with conditional expectations
- reductions increase the size of the universe → constant number of smaller instances
- efficiency → the whole construction needs to be subquadratic

Technical difficulties we overcome in the paper

- existence $\rightarrow$ construction
- $U = [-n^3, n^3]$, so we can't store the whole Behrend's set $\rightarrow$ implicit representation
- random shifts $\rightarrow$ derandomization with conditional expectations
- reductions increase the size of the universe $\rightarrow$ constant number of smaller instances
- efficiency $\rightarrow$ the whole construction needs to be subquadratic

Technical difficulties we overcome in the paper

- existence $\rightarrow$ construction
- $U = [-n^3, n^3]$, so we can't store the whole Behrend's set $\rightarrow$ implicit representation
- random shifts $\rightarrow$ derandomization with conditional expectations
- reductions increase the size of the universe $\rightarrow$ constant number of smaller instances
- efficiency $\rightarrow$ the whole construction needs to be subquadratic

Technical difficulties we overcome in the paper

- existence $\rightarrow$ construction
- $U = [-n^3, n^3]$, so we can't store the whole Behrend's set $\rightarrow$ implicit representation
- random shifts $\rightarrow$ derandomization with conditional expectations
- reductions increase the size of the universe $\rightarrow$ constant number of smaller instances
- efficiency $\rightarrow$ the whole construction needs to be subquadratic

Technical difficulties we overcome in the paper

- existence $\rightarrow$ construction
- $U = [-n^3, n^3]$, so we can't store the whole Behrend's set $\rightarrow$ implicit representation
- random shifts $\rightarrow$ derandomization with conditional expectations
- reductions increase the size of the universe $\rightarrow$ constant number of smaller instances
- efficiency $\rightarrow$ the whole construction needs to be subquadratic

Behrend's construction

Idea

- Points in $P = [1, m]^d$ can be partitioned into dm^2 spheres $P_r = \{\bar{x} \in P : d^2(o, \bar{x}) = r\}$ for $1 \leq r \leq dm^2$.
- On a sphere there are no 3 collinear points, so no point is the average of two other points.
- One of the spheres contains many points from P
- Choose a mapping $\phi : P \to [1, N]$ with "no carry": $\phi(\bar{x}) = \sum_i x_i (pm)^i$

Then $x = \sum_i x_i (pm)^i \in [1, N]$ belongs to $Q_r = \phi[P_r]$ iff:

- $\sum_i x_i^2 = r$, and
- for all $0 \leq i < d$ it holds that $x_i \in [1, m]$.

and we can check it in $\mathcal{O}(d)$ time.

Set $d = \sqrt{\log_p N}$, $m = p^{d-1}$ to get $r \leq 2^{\mathcal{O}(\sqrt{\log N})}$ and $|P| \geq \frac{N}{2^{\mathcal{O}(\sqrt{\log N})}}$.

Behrend's construction

Idea

- Points in $P = [1, m]^d$ can be partitioned into dm^2 spheres $P_r = \{\bar{x} \in P : d^2(o, \bar{x}) = r\}$ for $1 \leq r \leq dm^2$.
- On a sphere there are no 3 collinear points, so no point is the average of two other points.
- One of the spheres contains many points from P
- Choose a mapping $\phi : P \to [1, N]$ with "no carry": $\phi(\bar{x}) = \sum_i x_i (pm)^i$

Then $x = \sum_i x_i (pm)^i \in [1, N]$ belongs to $Q_r = \phi[P_r]$ iff:

- $\sum_i x_i^2 = r$, and
- for all $0 \leq i < d$ it holds that $x_i \in [1, m]$.

and we can check it in $\mathcal{O}(d)$ time.

Set $d = \sqrt{\log_p N}$, $m = p^{d-1}$ to get $r \leq 2^{\mathcal{O}(\sqrt{\log N})}$ and $|P| \geq \frac{N}{2^{\mathcal{O}(\sqrt{\log N})}}$.

Behrend's construction

Idea

- Points in $P = [1, m]^d$ can be partitioned into dm^2 spheres $P_r = \{\bar{x} \in P : d^2(o, \bar{x}) = r\}$ for $1 \leq r \leq dm^2$.
- On a sphere there are no 3 collinear points, so no point is the average of two other points.
- One of the spheres contains many points from P
- Choose a mapping $\phi : P \to [1, N]$ with "no carry": $\phi(\bar{x}) = \sum_i x_i(pm)^i$

Then $x = \sum_i x_i(pm)^i \in [1, N]$ belongs to $Q_r = \phi[P_r]$ iff:

- $\sum_i x_i^2 = r$, and
- for all $0 \leq i < d$ it holds that $x_i \in [1, m]$.

and we can check it in $\mathcal{O}(d)$ time.

Set $d = \sqrt{\log_p N}$, $m = p^{d-1}$ to get $r \leq 2^{\mathcal{O}(\sqrt{\log N})}$ and $|P| \geq \frac{N}{2^{\mathcal{O}(\sqrt{\log N})}}$.

Behrend's construction

Idea

- Points in $P = [1, m]^d$ can be partitioned into dm^2 spheres $P_r = \{\bar{x} \in P : d^2(o, \bar{x}) = r\}$ for $1 \le r \le dm^2$.
- On a sphere there are no 3 collinear points, so no point is the average of two other points.
- One of the spheres contains many points from P
- Choose a mapping $\phi : P \to [1, N]$ with "no carry": $\phi(\bar{x}) = \sum_i x_i (pm)^i$

Then $x = \sum_i x_i (pm)^i \in [1, N]$ belongs to $Q_r = \phi[P_r]$ iff:

- $\sum_i x_i^2 = r$, and
- for all $0 \le i < d$ it holds that $x_i \in [1, m]$.

and we can check it in $\mathcal{O}(d)$ time.

Set $d = \sqrt{\log_p N}$, $m = p^{d-1}$ to get $r \le 2^{\mathcal{O}(\sqrt{\log N})}$ and $|P| \ge \frac{N}{2^{\mathcal{O}(\sqrt{\log N})}}$.

Behrend's construction

Idea

- Points in $P = [1, m]^d$ can be partitioned into dm^2 spheres $P_r = \{\bar{x} \in P : d^2(o, \bar{x}) = r\}$ for $1 \leq r \leq dm^2$.
- On a sphere there are no 3 collinear points, so no point is the average of two other points.
- One of the spheres contains many points from P
- Choose a mapping $\phi : P \to [1, N]$ with "no carry": $\phi(\bar{x}) = \sum_i x_i (pm)^i$

Then $x = \sum_i x_i (pm)^i \in [1, N]$ belongs to $Q_r = \phi[P_r]$ iff:

- $\sum_i x_i^2 = r$, and
- for all $0 \leq i < d$ it holds that $x_i \in [1, m]$.

and we can check it in $\mathcal{O}(d)$ time.

Set $d = \sqrt{\log_p N}$, $m = p^{d-1}$ to get $r \leq 2^{\mathcal{O}(\sqrt{\log N})}$ and $|P| \geq \frac{N}{2^{\mathcal{O}(\sqrt{\log N})}}$.

Behrend's construction

Idea

- Points in $P = [1, m]^d$ can be partitioned into dm^2 spheres $P_r = \{\bar{x} \in P : d^2(o, \bar{x}) = r\}$ for $1 \leq r \leq dm^2$.
- On a sphere there are no 3 collinear points, so no point is the average of two other points.
- One of the spheres contains many points from P
- Choose a mapping $\phi : P \to [1, N]$ with "no carry": $\phi(\bar{x}) = \sum_i x_i (pm)^i$

Then $x = \sum_i x_i (pm)^i \in [1, N]$ belongs to $Q_r = \phi[P_r]$ iff:

- $\sum_i x_i^2 = r$, and
- for all $0 \leq i < d$ it holds that $x_i \in [1, m]$.

and we can check it in $\mathcal{O}(d)$ time.

Set $d = \sqrt{\log_p N}$, $m = p^{d-1}$ to get $r \leq 2^{\mathcal{O}(\sqrt{\log N})}$ and $|P| \geq \frac{N}{2^{\mathcal{O}(\sqrt{\log N})}}$.

Behrend's construction

Idea

- Points in $P = [1, m]^d$ can be partitioned into dm^2 spheres $P_r = \{\bar{x} \in P : d^2(o, \bar{x}) = r\}$ for $1 \leq r \leq dm^2$.
- On a sphere there are no 3 collinear points, so no point is the average of two other points.
- One of the spheres contains many points from P
- Choose a mapping $\phi : P \to [1, N]$ with "no carry": $\phi(\bar{x}) = \sum_i x_i (pm)^i$

Then $x = \sum_i x_i (pm)^i \in [1, N]$ belongs to $Q_r = \phi[P_r]$ iff:

- $\sum_i x_i^2 = r$, and
- for all $0 \leq i < d$ it holds that $x_i \in [1, m]$.

and we can check it in $\mathcal{O}(d)$ time.

Set $d = \sqrt{\log_p N}, m = p^{d-1}$ to get $r \leq 2^{\mathcal{O}(\sqrt{\log N})}$ and $|P| \geq \frac{N}{2^{\mathcal{O}(\sqrt{\log N})}}$.

Random shifts

Recap

- We have compact representation of Behrend's set Q_r
- There exists $\Delta \in [-N, N]$ such that $|Q_r \cap (A + \Delta)| \geq |A|/2^{\mathcal{O}(\sqrt{\log N})}$

Derandomization in $|A| \cdot 2^{\mathcal{O}(\sqrt{\log N})}$ time

- Use the method of conditional expectations to find bits of Δ starting from the most significant

$$\mathbb{E}[|Q_r \cap (A + \Delta)| | \Delta \in [0, 2^k)] = \frac{1}{2}\Big(\mathbb{E}[|Q_r \cap (A + \Delta)| | \Delta \in [0, 2^{k-1})] + \mathbb{E}[|(Q_r \cap (A + 2^{k-1} + \Delta)| | \Delta \in [0, 2^{k-1})]\Big)$$

- Calculate $|Q_r \cap [x, x + 2^k)|$ in $2^{\mathcal{O}(\sqrt{\log N})}$ time and space using dynamic programming "over base-(pm) digits"

Random shifts

Recap

- We have compact representation of Behrend's set Q_r
- There exists $\Delta \in [-N, N]$ such that $|Q_r \cap (A + \Delta)| \geq |A|/2^{\mathcal{O}(\sqrt{\log N})}$

Derandomization in $|A| \cdot 2^{\mathcal{O}(\sqrt{\log N})}$ time

- Use the method of conditional expectations to find bits of Δ starting from the most significant

$$\mathbb{E}[|Q_r \cap (A + \Delta)| \,|\, \Delta \in [0, 2^k)] =$$

$$\frac{1}{2}\Big(\mathbb{E}[|Q_r \cap (A + \Delta)| \,|\, \Delta \in [0, 2^{k-1})]$$

$$+ \mathbb{E}[|(Q_r \cap (A + 2^{k-1} + \Delta)| \,|\, \Delta \in [0, 2^{k-1})]\Big)$$

- Calculate $|Q_r \cap [x, x + 2^k)|$ in $2^{\mathcal{O}(\sqrt{\log N})}$ time and space using dynamic programming "over base-(pm) digits"

Random shifts

Recap

- We have compact representation of Behrend's set Q_r
- There exists $\Delta \in [-N, N]$ such that $|Q_r \cap (A + \Delta)| \geq |A|/2^{\mathcal{O}(\sqrt{\log N})}$

Derandomization in $|A| \cdot 2^{\mathcal{O}(\sqrt{\log N})}$ time

- Use the method of conditional expectations to find bits of Δ starting from the most significant

$$\mathbb{E}[|Q_r \cap (A + \Delta)| \big| \Delta \in [0, 2^k)] = \frac{1}{2}\Big(\mathbb{E}[|Q_r \cap (A + \Delta)| \big| \Delta \in [0, 2^{k-1})] + \mathbb{E}[|(Q_r \cap (A + 2^{k-1} + \Delta)| \big| \Delta \in [0, 2^{k-1})]\Big)$$

- Calculate $|Q_r \cap [x, x + 2^k)|$ in $2^{\mathcal{O}(\sqrt{\log N})}$ time and space using dynamic programming "over base-(pm) digits"

Random shifts

Recap

- We have compact representation of Behrend's set Q_r
- There exists $\Delta \in [-N, N]$ such that $|Q_r \cap (A + \Delta)| \geq |A|/2^{\mathcal{O}(\sqrt{\log N})}$

Derandomization in $|A| \cdot 2^{\mathcal{O}(\sqrt{\log N})}$ time

- Use the method of conditional expectations to find bits of Δ starting from the most significant

$$\mathbb{E}[|Q_r \cap (A + \Delta)| \big| \Delta \in [0, 2^k)] =$$
$$\frac{1}{2}\Big(\mathbb{E}[|Q_r \cap (A + \Delta)| \big| \Delta \in [0, 2^{k-1})]$$
$$+ \mathbb{E}[|(Q_r \cap (A + 2^{k-1} + \Delta)| \big| \Delta \in [0, 2^{k-1})]\Big)$$

- Calculate $|Q_r \cap [x, x + 2^k)|$ in $2^{\mathcal{O}(\sqrt{\log N})}$ time and space using dynamic programming "over base-(pm) digits"

Random shifts

Recap

- We have compact representation of Behrend's set Q_r
- There exists $\Delta \in [-N, N]$ such that $|Q_r \cap (A + \Delta)| \geq |A|/2^{\mathcal{O}(\sqrt{\log N})}$

Derandomization in $|A| \cdot 2^{\mathcal{O}(\sqrt{\log N})}$ time

- Use the method of conditional expectations to find bits of Δ starting from the most significant

$$\mathbb{E}[|Q_r \cap (A + \Delta)| \,|\, \Delta \in [0, 2^k)] = \frac{1}{2}\Big(\mathbb{E}[|Q_r \cap (A + \Delta)| \,|\, \Delta \in [0, 2^{k-1})] + \mathbb{E}[|(Q_r \cap (A + 2^{k-1} + \Delta)| \,|\, \Delta \in [0, 2^{k-1})]\Big)$$

- Calculate $|Q_r \cap [x, x + 2^k)|$ in $2^{\mathcal{O}(\sqrt{\log N})}$ time and space using dynamic programming "over base-(pm) digits"

Larger values of k

What can we say about k-LDT for larger values of k?

Genus of a linear equation $\sum_{i=1}^{k} \alpha_i x_i = 0$

Largest g such that $[k]$ can be partitioned into disjoint subsets $G_1, \ldots, G_g$ with $\sum_{i \in G_j} \alpha_i = 0$ for every j.

Sidon set: avoiding $x_1 + x_2 = x_3 + x_4$

Thank you!

Video: (link)

Larger values of k

What can we say about k-LDT for larger values of k?

Genus of a linear equation $\sum_{i=1}^{k} \alpha_i x_i = 0$

Largest g such that $[k]$ can be partitioned into disjoint subsets $G_1, \ldots, G_g$ with $\sum_{i \in G_j} \alpha_i = 0$ for every j.

Sidon set: avoiding $x_1 + x_2 = x_3 + x_4$

Thank you!

Video: (link)

Larger values of k

What can we say about k-LDT for larger values of k?

Genus of a linear equation $\sum_{i=1}^{k} \alpha_i x_i = 0$

Largest g such that $[k]$ can be partitioned into disjoint subsets $G_1, \ldots, G_g$ with $\sum_{i \in G_j} \alpha_i = 0$ for every j.

Sidon set: avoiding $x_1 + x_2 = x_3 + x_4$

Thank you!

Video: (link)

Larger values of k

What can we say about k-LDT for larger values of k?

Genus of a linear equation $\sum_{i=1}^{k} \alpha_i x_i = 0$

Largest g such that $[k]$ can be partitioned into disjoint subsets $G_1, \ldots, G_g$ with $\sum_{i \in G_j} \alpha_i = 0$ for every j.

Sidon set: avoiding $x_1 + x_2 = x_3 + x_4$

Thank you!

Video: (link)