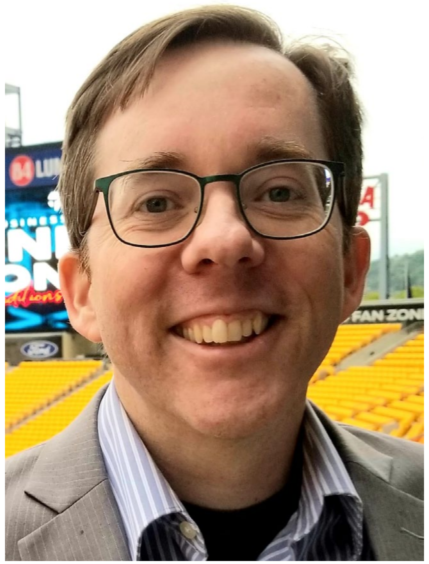
No exponential quantum speedup for SIS^{∞} anymore

Kewen Wu (IAS)



Robin Kothari
Google Quantum AI

Ryan O'Donnell
CMU

Outline

Toy example: $\mathbf{F}_3^n$-Subset-Sum

Motivations

Main problem: the SIS^∞ problem

Cryptographic motivation

Full generalization: the $\boldsymbol{A}$-SIS problem

Quantum motivation

Algorithm overview

A toy SIS^{∞} problem

Given vectors in $\mathbf{F}_3^n$, *efficiently* find a nonempty subset of them that sums to zero

$\mathbf{F}_3^n$-Subset-Sum

A toy SIS^{∞} problem

Given vectors in $\mathbf{F}_3^n$, *efficiently* find a nonempty subset of them that sums to zero

$\mathbf{F}_3^n$-Subset-Sum

Input: $\boldsymbol{v_1}, \dots, \boldsymbol{v_m} \in \mathbf{F}_3^n$

Output: $\emptyset \neq \boldsymbol{S} \subseteq [\boldsymbol{m}]$ or $\perp$

Condition: $\sum_{i \in S} \boldsymbol{v_i} \equiv \vec{\mathbf{0}} \bmod \mathbf{3}$ or no such $\boldsymbol{S}$

A toy SIS$^\infty$ problem

Given vectors in $\mathbf{F}_3^n$, *efficiently* find a nonempty subset of them that sums to zero

$\mathbf{F}_3^n$-Subset-Sum

Input: $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbf{F}_3^n$

Output: $\emptyset \neq \boldsymbol{S} \subseteq [\boldsymbol{m}]$ or $\perp$

Condition: $\sum_{i \in S} \boldsymbol{v}_i \equiv \vec{\mathbf{0}} \bmod \mathbf{3}$ or no such $\boldsymbol{S}$

Only allow $\mathbf{0}, \mathbf{1}$ as coefficients
$\mathbf{2}$ is not allowed

$\mathbf{F}_3^n$-Subset-Sum

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_3^n$

Output: $\emptyset \neq \boldsymbol{S} \subseteq [\boldsymbol{m}]$ or $\perp$ such that $\sum_{i \in S} \boldsymbol{v_i} \equiv \vec{\mathbf{0}} \ \mathbf{mod}\ \mathbf{3}$

$$\boldsymbol{n} = \mathbf{4} \left\{ \begin{matrix} \begin{bmatrix} 0 \\ 2 \\ 1 \\ 2 \end{bmatrix} & \begin{bmatrix} 1 \\ 2 \\ 1 \\ 1 \end{bmatrix} & \begin{bmatrix} 0 \\ 0 \\ 0 \\ 2 \end{bmatrix} & \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \\ 1 \\ 2 \end{bmatrix} & \begin{bmatrix} 2 \\ 2 \\ 2 \\ 1 \end{bmatrix} \end{matrix} \right.$$

$$\underbrace{\hphantom{\begin{bmatrix} 0 \end{bmatrix} \begin{bmatrix} 0 \end{bmatrix} \begin{bmatrix} 0 \end{bmatrix} \begin{bmatrix} 0 \end{bmatrix} \begin{bmatrix} 0 \end{bmatrix} \begin{bmatrix} 0 \end{bmatrix}}}_{\boldsymbol{m} = \mathbf{6}}$$

$\mathbf{F}_3^n$-Subset-Sum

Input: $v_1, \ldots, v_m \in \mathbf{F}_3^n$

Output: $\emptyset \neq S \subseteq [m]$ or $\perp$ such that $\sum_{i \in S} v_i \equiv \vec{0} \bmod 3$

$$n = 4 \left\{ \vphantom{\begin{bmatrix}0\\2\\1\\2\end{bmatrix}} \right. \underbrace{\begin{bmatrix}0\\2\\1\\2\end{bmatrix} \quad \begin{bmatrix}1\\2\\1\\1\end{bmatrix} \quad \begin{bmatrix}0\\0\\0\\2\end{bmatrix} \quad \begin{bmatrix}1\\1\\1\\0\end{bmatrix} \quad \begin{bmatrix}1\\0\\1\\2\end{bmatrix} \quad \begin{bmatrix}2\\2\\2\\1\end{bmatrix}}_{m = 6}$$

$\mathbf{F}_3^n$-Subset-Sum

Input: $v_1, \ldots, v_m \in \mathbf{F}_3^n$

Output: $\emptyset \neq S \subseteq [m]$ or $\perp$ such that $\sum_{i \in S} v_i \equiv \vec{0} \bmod 3$

$$n = 4 \left\{ \underbrace{\begin{bmatrix}0\\2\\1\\2\end{bmatrix} \begin{bmatrix}1\\2\\1\\1\end{bmatrix} \begin{bmatrix}0\\0\\0\\2\end{bmatrix} \begin{bmatrix}1\\1\\1\\0\end{bmatrix} \begin{bmatrix}1\\0\\1\\2\end{bmatrix} \begin{bmatrix}2\\2\\2\\1\end{bmatrix}}_{m = 6} \right.$$

$\mathbf{F}_3^n$-Subset-Sum landscape

Input: $v_1, \dots, v_m \in \mathbf{F}_3^n$

Output: $\emptyset \neq S \subseteq [m]$ or $\perp$ such that $\sum_{i \in S} v_i \equiv \vec{0} \bmod 3$

Harder *Easier*

$\longrightarrow \boldsymbol{m}$

$\mathbf{F}_3^n$-Subset-Sum landscape

Input: $v_1, \ldots, v_m \in \mathbf{F}_3^n$

Output: $\emptyset \neq S \subseteq [m]$ or $\perp$ such that $\sum_{i \in S} v_i \equiv \vec{0} \bmod 3$

Harder *Easier*

n $\longrightarrow$ m

NP-hard

$\mathbb{F}_3^n$-Subset-Sum landscape

Input: $v_1, \dots, v_m \in \mathbb{F}_3^n$

Output: $\emptyset \neq S \subseteq [m]$ or $\perp$ such that $\sum_{i \in S} v_i \equiv \vec{0} \bmod 3$

Harder *Easier*

n $2n$ m

NP-hard

Total-Search

(no $\perp$)

$\mathbf{F}_3^n$-Subset-Sum landscape

Input: $v_1, \dots, v_m \in \mathbf{F}_3^n$

Output: $\emptyset \neq S \subseteq [m]$ or $\perp$ such that $\sum_{i \in S} v_i \equiv \vec{0} \bmod 3$

Harder *Easier*

n $n + \sqrt{n}$ $2n$ $\longrightarrow m$

NP-hard

Learning-With-Error
(Arora-Ge'11)

Total-Search
(no $\perp$)

$\mathbb{F}_3^n$-Subset-Sum landscape

Input: $v_1, \dots, v_m \in \mathbb{F}_3^n$

Output: $\emptyset \neq S \subseteq [m]$ or $\perp$ such that $\sum_{i \in S} v_i \equiv \vec{0} \bmod 3$

Harder *Easier*

n — **NP-hard**

$n + \sqrt{n}$ — **Learning-With-Error** (Arora-Ge'11)

$2n$ — **Total-Search** (no $\perp$)

Cn^2 — **Quantum polytime** (Chen-Liu-Zhandry'21)

m

$\mathbb{F}_3^n$-Subset-Sum landscape

Input: $v_1, \dots, v_m \in \mathbb{F}_3^n$

Output: $\emptyset \neq S \subseteq [m]$ or $\perp$ such that $\sum_{i \in S} v_i \equiv \vec{0} \bmod 3$

Harder *Easier*

n — $n + \sqrt{n}$ — $2n$ — $n^2/2$ → m

NP-hard

Learning-With-Error
(Arora-Ge'11)

Total-Search
(no $\perp$)

Quantum polytime
(Chen-Liu-Zhandry'21)

$\mathbb{F}_3^n$-Subset-Sum landscape

Input: $v_1, \ldots, v_m \in \mathbb{F}_3^n$

Output: $\emptyset \neq S \subseteq [m]$ or $\perp$ such that $\sum_{i \in S} v_i \equiv \vec{0} \bmod 3$

Harder → *Easier*

m

n	$n + \sqrt{n}$	$2n$	$n^2/2$
NP-hard	**Learning-With-Error** (Arora-Ge'11)	**Total-Search** (no $\perp$)	**Quantum polytime** (Chen-Liu-Zhandry'21) **Classical polytime** (Ivanyos-Sanselma-Santha'07)

$\mathbb{F}_3^n$-Subset-Sum landscape

Input: $v_1, \ldots, v_m \in \mathbb{F}_3^n$

Output: $\emptyset \neq S \subseteq [m]$ or $\perp$ such that $\sum_{i \in S} v_i \equiv \vec{0} \bmod 3$

Harder *Easier*

n $\quad n + \sqrt{n}$ $\quad 2n$ $\quad n^2/3$ $\quad n^2/2$ $\quad m$

NP-hard

Learning-With-Error
(Arora-Ge'11)

Total-Search
(no $\perp$)

Classical polytime
(new)

Quantum polytime
(Chen-Liu-Zhandry'21)
Classical polytime
(Ivanyos-Sanselma-Santha'07)

$\mathbb{F}_3^n$-Subset-Sum landscape

Input: $v_1, \dots, v_m \in \mathbb{F}_3^n$

Output: $\emptyset \neq S \subseteq [m]$ or $\perp$ such that $\sum_{i \in S} v_i \equiv \vec{0} \bmod 3$

Harder *Easier*

?

$\underbrace{2n \quad n^2/3}$

n	$n + \sqrt{n}$	$2n$	$n^2/3$	$n^2/2$	m
NP-hard	**Learning-With-Error** (Arora-Ge'11)	**Total-Search** (no $\perp$)	**Classical polytime (new)**	**Quantum polytime** (Chen-Liu-Zhandry'21) **Classical polytime** (Ivanyos-Sanselma-Santha'07)	

Why $\mathbf{F}_3^n$-Subset-Sum

Natural problem with many perspectives

Why $\mathbf{F}_3^n$-Subset-Sum

Natural problem with many perspectives

- Complexity theory: subset-sum and LIN-SAT

Why $\mathbf{F}_3^n$-Subset-Sum

Natural problem with many perspectives

Complexity theory: subset-sum and LIN-SAT

Discrepancy theory: vector balancing over $\mathbf{F}_3$

Why $\mathbf{F}_3^n$-Subset-Sum

Natural problem with many perspectives

- Complexity theory: subset-sum and LIN-SAT
- Discrepancy theory: vector balancing over $\mathbf{F}_3$
- Coding theory: ternary syndrome decoding with maximal weight

Why $\mathbf{F}_3^n$-Subset-Sum

Natural problem with many perspectives

- Complexity theory: subset-sum and LIN-SAT
- Discrepancy theory: vector balancing over $\mathbf{F}_3$
- Coding theory: ternary syndrome decoding with maximal weight
- Cryptography: Learning-With-Error with binary error over $\mathbf{F}_3$

Why $\mathbf{F}_3^n$-Subset-Sum

Natural problem with many perspectives

- Complexity theory: subset-sum and LIN-SAT
- Discrepancy theory: vector balancing over $\mathbf{F}_3$
- Coding theory: ternary syndrome decoding with maximal weight
- Cryptography: Learning-With-Error with binary error over $\mathbf{F}_3$

Security of post-quantum signature scheme

- *Wave* (Debris-Alazard, Sendrier, Tillich'19)
- *CRYSTALS-Dilithium* (Ducas, Kiltz, Lepoint, Lyubashevsky, Schwabe, Seiler, Stehle'18)

Why $\mathbf{F}_3^n$-Subset-Sum

Natural problem with many perspectives

- Complexity theory: subset-sum and LIN-SAT
- Discrepancy theory: vector balancing over $\mathbf{F}_3$
- Coding theory: ternary syndrome decoding with maximal weight
- Cryptography: Learning-With-Error with binary error over $\mathbf{F}_3$

Security of post-quantum signature scheme

- *Wave* (Debris-Alazard, Sendrier, Tillich'19)
- *CRYSTALS-Dilithium* (Ducas, Kiltz, Lepoint, Lyubashevsky, Schwabe, Seiler, Stehle'18)

Quantum advantage

Why $\mathbf{F}_3^n$-Subset-Sum

Natural problem with many perspectives

- Complexity theory: subset-sum and LIN-SAT
- Discrepancy theory: vector balancing over $\mathbf{F}_3$
- Coding theory: ternary syndrome decoding with maximal weight
- Cryptography: Learning-With-Error with binary error over $\mathbf{F}_3$

Security of post-quantum signature scheme

- *Wave* (Debris-Alazard, Sendrier, Tillich'19)
- *CRYSTALS-Dilithium* (Ducas, Kiltz, Lepoint, Lyubashevsky, Schwabe, Seiler, Stehle'18)

Quantum advantage

Warmup for the SIS^∞ problem

The SIS^{∞} problem

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \ldots, c_m}$ such that $\boldsymbol{\sum c_i v_i \equiv \vec{0} \bmod p}$

The SIS$^{\infty}$ problem

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

The SIS^{∞} problem

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \ldots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \ \mathbf{mod}\ \boldsymbol{p}$

Short-**I**nteger-**S**olution

The SIS^∞ problem

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{h} \geq \mathbf{1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \ldots, c_m}$ such that each $\boldsymbol{|c_i| \leq h}$ and $\boldsymbol{\sum c_i v_i \equiv \vec{0}} \ \mathbf{mod}\ \boldsymbol{p}$

Short-**I**nteger-**S**olution

The SIS$^\infty$ problem

Input: $\boldsymbol{v_1, \dots, v_m \in \mathbf{F}_p^n}$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $\boldsymbol{|c_i| \leq h}$ and $\boldsymbol{\sum c_i v_i \equiv \vec{0} \bmod p}$

Short-**I**nteger-**S**olution

Example.

Given $\boldsymbol{m}$ vectors in $\mathbf{F}_{101}^n$, find linear dependence where all coeffs $\boldsymbol{c_i}$ are between $\boldsymbol{\pm 5}$.

The SIS^∞ problem

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_p^n$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \ldots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Remark.

The SIS^∞ problem

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \ldots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Remark.

- $\boldsymbol{p = 2}$ or $\mathbf{3}$: trivial

The SIS^{∞} problem

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_p^n$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \ldots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \ \mathbf{mod}\ \boldsymbol{p}$

Remark.

- $\boldsymbol{p = 2}$ or $\boldsymbol{3}$: trivial
- $\boldsymbol{h \geq \lfloor p/2 \rfloor}$: trivial

The SIS^{∞} problem

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_p^n$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Remark.

- $\boldsymbol{p = 2}$ or $\boldsymbol{3}$: trivial
- $\boldsymbol{h \geq \lfloor p/2 \rfloor}$: trivial

- Smaller $\boldsymbol{h}$ is a harder problem

The SIS^{∞} problem

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Remark.

- $\boldsymbol{p = 2}$ or $\boldsymbol{3}$: trivial
- $\boldsymbol{h \geq \lfloor p/2 \rfloor}$: trivial

- Smaller $\boldsymbol{h}$ is a harder problem
- $\boldsymbol{h = 1}$, allowing coeffs $\{\boldsymbol{-1, 0, +1}\}$: **Collision in linear hash**

The SIS^∞ problem

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_p^n$ and $\boldsymbol{h} \geq \mathbf{1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Remark.

- $\boldsymbol{p} = \mathbf{2}$ or $\mathbf{3}$: trivial
- $\boldsymbol{h} \geq \lfloor \boldsymbol{p}/\mathbf{2} \rfloor$: trivial

- Smaller $\boldsymbol{h}$ is a harder problem
- $\boldsymbol{h} = \mathbf{1}$, allowing coeffs $\{-\mathbf{1}, \mathbf{0}, +\mathbf{1}\}$: **Collision in linear hash**

$\boldsymbol{V} \in \mathbf{F}_p^{n \times m}$ defines a linear hash $\boldsymbol{x} \in \{\mathbf{0}, \mathbf{1}\}^m \rightarrow \boldsymbol{Vx} \in \mathbf{F}_p^n$

The SIS^{∞} problem

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_p^n$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \ \mathbf{mod}\ \boldsymbol{p}$

Remark.

- $\boldsymbol{p = 2}$ or $\mathbf{3}$: trivial
- $\boldsymbol{h} \geq \lfloor \boldsymbol{p/2} \rfloor$: trivial

- Smaller $\boldsymbol{h}$ is a harder problem
- $\boldsymbol{h = 1}$, allowing coeffs $\{\mathbf{-1, 0, +1}\}$: **Collision in linear hash**

$\boldsymbol{V} \in \mathbf{F}_p^{n \times m}$ defines a linear hash $\boldsymbol{x} \in \{\mathbf{0,1}\}^m \ \to \ \boldsymbol{Vx} \in \mathbf{F}_p^n$

$\boldsymbol{Vx = Vx'}$ iff $\boldsymbol{V(x - x') = 0}$ iff $\boldsymbol{Vc = 0}$

The SIS^{∞} problem

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Remark.

- $\boldsymbol{p = 2}$ or $\boldsymbol{3}$: trivial
- $\boldsymbol{h} \geq \lfloor \boldsymbol{p/2} \rfloor$: trivial

- Smaller $\boldsymbol{h}$ is a harder problem
- $\boldsymbol{h = 1}$, allowing coeffs $\{\boldsymbol{-1, 0, +1}\}$: **Collision in linear hash**

- $\boldsymbol{m \geq (p-1)n + 1}$: solution always exists

The SIS^{∞} problem

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \ldots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Cryptography motivation.

The SIS^{∞} problem

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \ldots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Cryptography motivation.

- Our focus: $\boldsymbol{m} \gg \boldsymbol{n}$, many solutions exist, find one

The SIS^{∞} problem

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \ \mathbf{mod}\ \boldsymbol{p}$

Cryptography motivation.

- Our focus: $\boldsymbol{m} \gg \boldsymbol{n^2}$, many solutions exist, find one

The SIS^{∞} problem

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Cryptography motivation.

- Our focus: $\boldsymbol{m} \gg \boldsymbol{n^2}$, many solutions exist, find one
- Learning-With-Error setting: $\boldsymbol{m = n + n^{1/C}}$, a (unique) solution *planted*, find it

The SIS^{∞} problem

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_p^n$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \ldots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Cryptography motivation.

- Our focus: $\boldsymbol{m \gg n^2}$, many solutions exist, find one
- Learning-With-Error setting: $\boldsymbol{m = n + n^{1/C}}$, a (unique) solution *planted*, find it

- CRYSTALS-Dilithium signature scheme: in its *module* variant
  Assume $\boldsymbol{n = 1280, m = 2304, p \approx 2^{23}, h \approx p/8}$, random $\{\boldsymbol{v_i}\}$ is hard

The SIS^{∞} problem

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \ \mathbf{mod}\ \boldsymbol{p}$

Cryptography motivation.

- Our focus: $\boldsymbol{m \gg n^2}$, many solutions exist, find one
- Learning-With-Error setting: $\boldsymbol{m = n + n^{1/C}}$, a (unique) solution *planted*, find it

- CRYSTALS-Dilithium signature scheme: in its *module* variant
  Assume $\boldsymbol{n = 1280}$, $\boldsymbol{m = 2304}$, $\boldsymbol{p \approx 2^{23}}$, $\boldsymbol{h \approx p/8}$, random $\{\boldsymbol{v_i}\}$ is hard
  In general, assume $\boldsymbol{m \approx 1.9n}$, $\boldsymbol{p \gg n}$, $\boldsymbol{h \approx p/8}$, random $\{\boldsymbol{v_i}\}$ is hard

The SIS^∞ problem

Input: $\boldsymbol{v_1, \dots, v_m \in \mathbf{F}_p^n}$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Cryptography motivation.

- Our focus: $\boldsymbol{m \gg n^2}$, many solutions exist, find one
- Learning-With-Error setting: $\boldsymbol{m = n + n^{1/C}}$, a (unique) solution *planted*, find it

- CRYSTALS-Dilithium signature scheme: in its *module* variant
  Assume $\boldsymbol{n = 1280, m = 2304, p \approx 2^{23}, h \approx p/8}$, random $\{\boldsymbol{v_i}\}$ is hard
  In general, assume $\boldsymbol{m \approx 1.9n, p \gg n, h \approx p/8}$, random $\{\boldsymbol{v_i}\}$ is hard

$\boldsymbol{m \approx n \log n, p \approx n^2 \log n, h = O(1)}$, random $\{\boldsymbol{v_i}\}$ is hard,
based on worst-case hardness of lattice problems [Ajtai'96, Micciancio-Regev'04]

The SIS^∞ problem

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{h} \geq \mathbf{1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Theorem (Chen-Liu-Zhandry'21).
Assume $\boldsymbol{k}$ is odd constant and

$$\boldsymbol{m} \gg \boldsymbol{p}^{\mathbf{4}}\boldsymbol{n}^{\boldsymbol{k}}$$

Quantum polytime algorithm for

$$\boldsymbol{h} \geq \frac{\boldsymbol{p}-\boldsymbol{k}}{\mathbf{2}}$$

The SIS^{∞} problem

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Theorem (Chen-Liu-Zhandry'21).
Assume $\boldsymbol{k}$ is odd constant and

$$\boldsymbol{m \gg p^4 n^k}$$

Quantum polytime algorithm for

$$\boldsymbol{h \geq \frac{p-k}{2}}$$

Theorem (Imran-Ivanyos'25).
Assume $\boldsymbol{k}$ is a power of two and

$$\boldsymbol{m \gg p^{k \log k} n^k}$$

Classical polytime algorithm for

$$\boldsymbol{h \geq \frac{p}{2k}}$$

The SIS^∞ problem

Input: $\boldsymbol{v_1, \dots, v_m \in \mathbf{F}_p^n}$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Theorem (Chen-Liu-Zhandry'21).
Assume $\boldsymbol{k}$ is odd constant and

$$\boldsymbol{m \gg p^4 n^k}$$

Quantum polytime algorithm for

$$\boldsymbol{h \geq \frac{p-k}{2}}$$

Theorem (Imran-Ivanyos'25).
Assume $\boldsymbol{k}$ is a power of two and

$$\boldsymbol{m \gg p^{k \log k} n^k}$$

Classical polytime algorithm for

$$\boldsymbol{h \geq \frac{p}{2k}}$$

Theorem (New).
Assume $\boldsymbol{k}$ is any constant and

$$\boldsymbol{m \gg n^k}$$

Classical polytime algorithm for

$$\boldsymbol{h \geq \frac{p}{2k}}$$

The SIS$^\infty$ problem

Input: $\boldsymbol{v_1, \dots, v_m \in \mathbb{F}_p^n}$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i \equiv \vec{0} \bmod p}$

Theorem (Chen-Liu-Zhandry'21).
Assume $\boldsymbol{k}$ is odd constant and
$$\boldsymbol{m \gg p^4 n^k}$$
Quantum polytime algorithm for
$$\boldsymbol{h \geq \frac{p-k}{2}}$$

Theorem (Imran-Ivanyos'25).
Assume $\boldsymbol{k}$ is a power of two and
$$\boldsymbol{m \gg p^{k \log k} n^k}$$
Classical polytime algorithm for
$$\boldsymbol{h \geq \frac{p}{2k}}$$

Theorem (New).
Assume $\boldsymbol{k}$ is any constant and
$$\boldsymbol{m \gg n^k}$$
Classical polytime algorithm for
$$\boldsymbol{h \geq \frac{p}{2k}}$$

Runs in $\mathbf{poly}(\boldsymbol{n}, \mathbf{log}\, \boldsymbol{p})$ time

The SIS^∞ problem

Input: $\boldsymbol{v_1, \dots, v_m \in \mathbf{F}_p^n}$ and $\boldsymbol{h \geq 1}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $|\boldsymbol{c_i}| \leq \boldsymbol{h}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Theorem (Chen-Liu-Zhandry'21).
Assume $\boldsymbol{k}$ is odd constant and

$$\boldsymbol{m \gg p^4 n^k}$$

Quantum polytime algorithm for

$$\boldsymbol{h \geq \frac{p-k}{2}}$$

Theorem (Imran-Ivanyos'25).
Assume $\boldsymbol{k}$ is a power of two and

$$\boldsymbol{m \gg p^{k \log k} n^k}$$

Classical polytime algorithm for

$$\boldsymbol{h \geq \frac{p}{2k}}$$

Theorem (New).
Assume $\boldsymbol{k}$ is any constant and

$$\boldsymbol{m \gg n^k}$$

Classical polytime algorithm for

$$\boldsymbol{h \geq \frac{p}{2k}}$$

Runs in $\mathbf{poly}(\boldsymbol{n}, \mathbf{log}\,\boldsymbol{p})$ time
Allows $\boldsymbol{p} = \mathbf{exp}(\mathbf{poly}(\boldsymbol{n}))$

General allowed set ($\boldsymbol{A}$-SIS)

Input: $\boldsymbol{v_1, \dots, v_m \in \mathbf{F}_p^n}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that $\sum \boldsymbol{c_i v_i \equiv \vec{0} \bmod p}$

General allowed set ($\boldsymbol{A}$-SIS)

Input: $\boldsymbol{v_1, \ldots, v_m \in \mathbf{F}_p^n}$ and $\boldsymbol{A \subseteq \mathbf{F}_p}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \ldots, c_m}$ such that each $\boldsymbol{c_i \in A}$ and $\boldsymbol{\sum c_i v_i \equiv \vec{0} \bmod p}$

General allowed set ($\boldsymbol{A}$-SIS)

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{A} \subseteq \mathbf{F}_{\boldsymbol{p}}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \ldots, c_m}$ such that each $\boldsymbol{c_i} \in \boldsymbol{A}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Example.

General allowed set ($\boldsymbol{A}$-SIS)

Input: $\boldsymbol{v_1, \dots, v_m \in \mathbf{F}_p^n}$ and $\boldsymbol{A \subseteq \mathbf{F}_p}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $\boldsymbol{c_i \in A}$ and $\boldsymbol{\sum c_i v_i \equiv \vec{0} \bmod p}$

Example.

- $\boldsymbol{A = \{-h, -h+1, \dots, h-1, h\}}$ for $\mathbf{SIS}^{\infty}$

General allowed set ($\boldsymbol{A}$-SIS)

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{A} \subseteq \mathbf{F}_{\boldsymbol{p}}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $\boldsymbol{c_i} \in \boldsymbol{A}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \ \mathbf{mod}\ \boldsymbol{p}$

Example.

- $\boldsymbol{A} = \{-\boldsymbol{h}, -\boldsymbol{h} + \mathbf{1}, \dots, \boldsymbol{h} - \mathbf{1}, \boldsymbol{h}\}$ for $\mathbf{SIS}^{\infty}$
- $\boldsymbol{A} = \{\mathbf{0}, \mathbf{1}\}$ for $\mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$-Subset-Sum

General allowed set ($\boldsymbol{A}$-SIS)

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{A} \subseteq \mathbf{F}_{\boldsymbol{p}}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $\boldsymbol{c_i} \in \boldsymbol{A}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \mathbf{\ mod\ } \boldsymbol{p}$

Example.

- $\boldsymbol{A} = \{-\boldsymbol{h}, -\boldsymbol{h} + \mathbf{1}, \dots, \boldsymbol{h} - \mathbf{1}, \boldsymbol{h}\}$ for $\mathbf{SIS}^{\infty}$
- $\boldsymbol{A} = \{\mathbf{0}, \mathbf{1}\}$ for $\mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$-Subset-Sum
- $\boldsymbol{A} = \{-\mathbf{1}, \mathbf{0}, \mathbf{1}\}$ for Collision-Finding

General allowed set ($\boldsymbol{A}$-SIS)

Input: $\boldsymbol{v_1}, \dots, \boldsymbol{v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{A} \subseteq \mathbf{F}_{\boldsymbol{p}}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1}, \dots, \boldsymbol{c_m}$ such that each $\boldsymbol{c_i} \in \boldsymbol{A}$ and $\sum \boldsymbol{c_i} \boldsymbol{v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Example.

- $\boldsymbol{A} = \{-\boldsymbol{h}, -\boldsymbol{h}+\mathbf{1}, \dots, \boldsymbol{h}-\mathbf{1}, \boldsymbol{h}\}$ for $\mathbf{SIS}^{\infty}$
- $\boldsymbol{A} = \{\mathbf{0}, \mathbf{1}\}$ for $\mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$-Subset-Sum
- $\boldsymbol{A} = \{-\mathbf{1}, \mathbf{0}, \mathbf{1}\}$ for Collision-Finding

If $\mathbf{0} \notin \boldsymbol{A}$ and $\boldsymbol{v_1} = \boldsymbol{v_2} = \cdots = \boldsymbol{v_{m-1}} = \vec{\mathbf{0}}$ and $\boldsymbol{v_m} \neq \vec{\mathbf{0}}$, then it has no solution

General allowed set ($\boldsymbol{A}$-SIS)

Input: random $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{A} \subseteq \mathbf{F}_{\boldsymbol{p}}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $\boldsymbol{c_i} \in \boldsymbol{A}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Example.

- $\boldsymbol{A} = \{\boldsymbol{-h, -h+1, \dots, h-1, h}\}$ for $\mathbf{SIS}^{\infty}$
- $\boldsymbol{A} = \{\mathbf{0}, \mathbf{1}\}$ for $\mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$-Subset-Sum
- $\boldsymbol{A} = \{-\mathbf{1}, \mathbf{0}, \mathbf{1}\}$ for Collision-Finding

If $\mathbf{0} \notin \boldsymbol{A}$ and $\boldsymbol{v_1} = \boldsymbol{v_2} = \cdots = \boldsymbol{v_{m-1}} = \vec{\mathbf{0}}$ and $\boldsymbol{v_m} \neq \vec{\mathbf{0}}$,
then it has no solution

General allowed set ($\boldsymbol{A}$-SIS)

Input: random $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{A} \subseteq \mathbf{F}_{\boldsymbol{p}}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $\boldsymbol{c_i} \in \boldsymbol{A}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Theorem (Chen-Liu-Zhandry'21).
Assume $\mathbf{2} \leq \boldsymbol{k} \leq \boldsymbol{p} - \mathbf{1}$ is a constant and

$$\boldsymbol{m} \gg \boldsymbol{p}^{\mathbf{4}} \boldsymbol{n}^{\boldsymbol{k}}$$

Quantum polytime algorithm for $|\boldsymbol{A}| \geq \boldsymbol{p} - \boldsymbol{k} + \mathbf{1}$

General allowed set ($\boldsymbol{A}$-SIS)

Input: random $\boldsymbol{v_1, \ldots, v_m \in \mathbf{F}_p^n}$ and $\boldsymbol{A \subseteq \mathbf{F}_p}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \ldots, c_m}$ such that each $\boldsymbol{c_i \in A}$ and $\boldsymbol{\sum c_i v_i \equiv \vec{0} \bmod p}$

Theorem (Chen-Liu-Zhandry'21).
Assume $\boldsymbol{2 \leq k \leq p-1}$ is a constant and

$$\boldsymbol{m \gg p^4 n^k}$$

Quantum polytime algorithm for $\boldsymbol{|A| \geq p-k+1}$

$\boldsymbol{k = 1}$: every coeff is allowed

General allowed set (A-SIS)

Input: random $v_1, \ldots, v_m \in \mathbf{F}_p^n$ and $A \subseteq \mathbf{F}_p$ where p is a prime

Output: $c_1, \ldots, c_m$ such that each $c_i \in A$ and $\sum c_i v_i \equiv \vec{0} \bmod p$

Theorem (Chen-Liu-Zhandry'21).
Assume $2 \leq k \leq p-1$ is a constant and

$$m \gg p^4 n^k$$

Quantum polytime algorithm for $|A| \geq p-k+1$

$k = 1$: every coeff is allowed
$k = p$: only one coeff is allowed

General allowed set (A-SIS)

Input: random $v_1, \dots, v_m \in \mathbb{F}_p^n$ and $A \subseteq \mathbb{F}_p$ where p is a prime

Output: $c_1, \dots, c_m$ such that each $c_i \in A$ and $\sum c_i v_i \equiv \vec{0} \bmod p$

Theorem (Chen-Liu-Zhandry'21).
Assume $2 \le k \le p-1$ is a constant and

$$m \gg p^4 n^k$$

Quantum polytime algorithm for $|A| \ge p-k+1$

$k = 1$: every coeff is allowed
$k = p$: only one coeff is allowed

Theorem (New).
Under the same $|A| \ge p-k+1$ condition
Classical polytime algorithm only needs

$$m \gg \log(p) \cdot \left\{ \vphantom{\begin{matrix} a \\ b \\ c \end{matrix}} \right.$$

General allowed set (A-SIS)

Input: random $v_1, \dots, v_m \in \mathbf{F}_p^n$ and $A \subseteq \mathbf{F}_p$ where p is a prime

Output: $c_1, \dots, c_m$ such that each $c_i \in A$ and $\sum c_i v_i \equiv \vec{0} \bmod p$

Theorem (Chen-Liu-Zhandry'21).
Assume $2 \le k \le p-1$ is a constant and

$$m \gg p^4 n^k$$

Quantum polytime algorithm for $|A| \ge p-k+1$

$k = 1$: every coeff is allowed
$k = p$: only one coeff is allowed

Theorem (New).
Under the same $|A| \ge p-k+1$ condition
Classical polytime algorithm only needs

$$m \gg \log(p) \cdot \begin{cases} n^2 & \text{if } p > 4^{k-1} \\ & \end{cases}$$

General allowed set (A-SIS)

Input: random $v_1, \ldots, v_m \in \mathbb{F}_p^n$ and $A \subseteq \mathbb{F}_p$ where p is a prime

Output: $c_1, \ldots, c_m$ such that each $c_i \in A$ and $\sum c_i v_i \equiv \vec{0} \bmod p$

Theorem (Chen-Liu-Zhandry'21).
Assume $2 \le k \le p-1$ is a constant and

$$m \gg p^4 n^k$$

Quantum polytime algorithm for $|A| \ge p-k+1$

$k=1$: every coeff is allowed
$k=p$: only one coeff is allowed

Theorem (New).
Under the same $|A| \ge p-k+1$ condition
Classical polytime algorithm only needs

$$m \gg \log(p) \cdot \begin{cases} n^2 & \text{if } p > 4^{k-1} \\ n^{k-1} & \text{if } p \ge 7 \text{ and } k \ge 3 \end{cases}$$

General allowed set (A-SIS)

Input: random $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_p^n$ and $\boldsymbol{A} \subseteq \mathbf{F}_p$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $\boldsymbol{c_i} \in \boldsymbol{A}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Theorem (Chen-Liu-Zhandry'21).
Assume $\mathbf{2} \leq \boldsymbol{k} \leq \boldsymbol{p} - \mathbf{1}$ is a constant and

$$\boldsymbol{m} \gg \boldsymbol{p}^{\mathbf{4}} \boldsymbol{n}^{\boldsymbol{k}}$$

Quantum polytime algorithm for $|\boldsymbol{A}| \geq \boldsymbol{p} - \boldsymbol{k} + \mathbf{1}$

$\boldsymbol{k} = \mathbf{1}$: every coeff is allowed
$\boldsymbol{k} = \boldsymbol{p}$: only one coeff is allowed

Theorem (New).
Under the same $|\boldsymbol{A}| \geq \boldsymbol{p} - \boldsymbol{k} + \mathbf{1}$ condition
Classical polytime algorithm only needs

$$\boldsymbol{m} \gg \mathbf{log}(\boldsymbol{p}) \cdot \begin{cases} \boldsymbol{n}^{\mathbf{2}} & \text{if } \boldsymbol{p} > \mathbf{4}^{\boldsymbol{k}-\mathbf{1}} \\ \boldsymbol{n}^{\boldsymbol{k}-\mathbf{1}} & \text{if } \boldsymbol{p} \geq \mathbf{7} \text{ and } \boldsymbol{k} \geq \mathbf{3} \\ \boldsymbol{n}^{\boldsymbol{k}} & \text{in general for all } \boldsymbol{p} \geq \mathbf{3} \text{ and } \boldsymbol{k} \geq \mathbf{2} \end{cases}$$

General allowed set (A-SIS)

Input: random $v_1, \dots, v_m \in \mathbf{F}_p^n$ and $A \subseteq \mathbf{F}_p$ where p is a prime

Output: $c_1, \dots, c_m$ such that each $c_i \in A$ and $\sum c_i v_i \equiv \vec{0} \bmod p$

Theorem (Chen-Liu-Zhandry'21).
Assume $2 \le k \le p-1$ is a constant and

$$m \gg p^4 n^k$$

Quantum polytime algorithm for $|A| \ge p-k+1$

$k=1$: every coeff is allowed
$k=p$: only one coeff is allowed

Theorem (New).
Under the same $|A| \ge p-k+1$ condition
Classical polytime algorithm only needs

$$m \gg \log(p) \cdot \begin{cases} n^2 & \text{if } p > 4^{k-1} \\ n^{k-1} & \text{if } p \ge 7 \text{ and } k \ge 3 \\ n^k & \text{in general for all } p \ge 3 \text{ and } k \ge 2 \end{cases}$$

A full dequantization!

General allowed set (A-SIS)

Input: random $v_1, \dots, v_m \in \mathbb{F}_p^n$ and $A \subseteq \mathbb{F}_p$ where p is a prime

Output: $c_1, \dots, c_m$ such that each $c_i \in A$ and $\sum c_i v_i \equiv \vec{0} \bmod p$

Theorem (Chen-Liu-Zhandry'21).
Assume $2 \le k \le p-1$ is a constant and

$$m \gg p^4 n^k$$

Quantum polytime algorithm for $|A| \ge p - k + 1$

$k = 1$: every coeff is allowed
$k = p$: only one coeff is allowed

Theorem (New).
Under the same $|A| \ge p - k + 1$ condition
Classical polytime algorithm

A full dequantization!

Why is this dequantization interesting?

$$m \gg \log(p) \cdot \begin{cases} n^2 & \text{if } p > 4^{k-1} \\ n^{k-1} & \text{if } p \ge 7 \text{ and } k \ge 3 \\ n^k & \text{in general for all } p \ge 3 \text{ and } k \ge 2 \end{cases}$$

On quantum speedup

On quantum speedup

Find problems where quantum algorithms have exponential speedup over classical ones

On quantum speedup

Find problems where quantum algorithms have exponential speedup over classical ones

- Simulation of quantum systems
- Hidden subgroup problem (factoring, discrete log)

On quantum speedup

Find problems where quantum algorithms have exponential speedup over classical ones

- Simulation of quantum systems
- Hidden subgroup problem (factoring, discrete log)

Candidate problem based on Regev's reduction (Regev'05)

On quantum speedup

Find problems where quantum algorithms have exponential speedup over classical ones

- Simulation of quantum systems
- Hidden subgroup problem (factoring, discrete log)

Candidate problem based on Regev's reduction (Regev'05)

- Chen-Liu-Zhandry'21

On quantum speedup

Find problems where quantum algorithms have exponential speedup over classical ones

- Simulation of quantum systems
- Hidden subgroup problem (factoring, discrete log)

Candidate problem based on Regev's reduction (Regev'05)

- Chen-Liu-Zhandry'21
- Yamakawa-Zhandry'22

On quantum speedup

Find problems where quantum algorithms have exponential speedup over classical ones

- Simulation of quantum systems
- Hidden subgroup problem (factoring, discrete log)

Candidate problem based on Regev's reduction (Regev'05)

- Chen-Liu-Zhandry'21
- Yamakawa-Zhandry'22
- (DQI team) Jordan, Shutty, Wootters, Zalcman, Schmidhuber, King, Isakov, Khattar, Babbush'24
- Chailloux-Tillich'24

On quantum speedup

Find problems where quantum algorithms have exponential speedup over classical ones

Simulation of quantum systems

Hidden subgroup problem (factoring, discrete log)

Candidate problem based on Regev's reduction (Regev'05)

Chen-Liu-Zhandry'21

Yamakawa-Zhandry'22

(DQI team) Jordan, Shutty, Wootters, Zalcman, Schmidhuber, King, Isakov, Khattar, Babbush'24

Chailloux-Tillich'24

Captured by $\boldsymbol{A}$-SIS

Regev-reduction quantum alg via $\boldsymbol{A}$-SIS

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{A} \subseteq \mathbf{F}_{\boldsymbol{p}}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $\boldsymbol{c_i} \in \boldsymbol{A}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \ \mathbf{mod}\ \boldsymbol{p}$

Chen-Liu-Zhandry'21	**Yamakawa-Zhandry'22**	**DQI'24, Chailloux-Tillich'24**

Regev-reduction quantum alg via $\boldsymbol{A}$-SIS

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{A} \subseteq \mathbf{F}_{\boldsymbol{p}}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \ldots, c_m}$ such that each $\boldsymbol{c_i} \in \boldsymbol{A}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Chen-Liu-Zhandry'21

Random $\{\boldsymbol{v_i}\}$
$\boldsymbol{A}$ arbitrary

Yamakawa-Zhandry'22

DQI'24, Chailloux-Tillich'24

Regev-reduction quantum alg via $\boldsymbol{A}$-SIS

Input: $\boldsymbol{v_1}, \dots, \boldsymbol{v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{A} \subseteq \mathbf{F}_{\boldsymbol{p}}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1}, \dots, \boldsymbol{c_m}$ such that each $\boldsymbol{c_i} \in \boldsymbol{A}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Chen-Liu-Zhandry'21

Random $\{\boldsymbol{v_i}\}$
$\boldsymbol{A}$ arbitrary
$\boldsymbol{p} = \mathbf{poly}(\boldsymbol{n})$
$|\boldsymbol{A}| = \boldsymbol{p} - \boldsymbol{k} + \mathbf{1}$
$\boldsymbol{m} \approx \boldsymbol{n}^{\boldsymbol{k}}$

Yamakawa-Zhandry'22

DQI'24, Chailloux-Tillich'24

Regev-reduction quantum alg via $\boldsymbol{A}$-SIS

Input: $\boldsymbol{v_1}, \dots, \boldsymbol{v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{A} \subseteq \mathbf{F}_{\boldsymbol{p}}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1}, \dots, \boldsymbol{c_m}$ such that each $\boldsymbol{c_i} \in \boldsymbol{A}$ and $\sum \boldsymbol{c_i} \boldsymbol{v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Chen-Liu-Zhandry'21

Random $\{\boldsymbol{v_i}\}$
$\boldsymbol{A}$ arbitrary
$\boldsymbol{p} = \mathbf{poly}(\boldsymbol{n})$
$|\boldsymbol{A}| = \boldsymbol{p} - \boldsymbol{k} + \mathbf{1}$
$\boldsymbol{m} \approx \boldsymbol{n}^{\boldsymbol{k}}$

Yamakawa-Zhandry'22

$\{\boldsymbol{v_i}\}$ folded RS code
$\boldsymbol{A}$ random

DQI'24, Chailloux-Tillich'24

Regev-reduction quantum alg via $\boldsymbol{A}$-SIS

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{A} \subseteq \mathbf{F}_{\boldsymbol{p}}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $\boldsymbol{c_i} \in \boldsymbol{A}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Chen-Liu-Zhandry'21

Random $\{\boldsymbol{v_i}\}$
$\boldsymbol{A}$ arbitrary
$\boldsymbol{p} = \mathbf{poly}(\boldsymbol{n})$
$|\boldsymbol{A}| = \boldsymbol{p} - \boldsymbol{k} + \mathbf{1}$
$\boldsymbol{m} \approx \boldsymbol{n}^{\boldsymbol{k}}$

Yamakawa-Zhandry'22

$\{\boldsymbol{v_i}\}$ folded RS code
$\boldsymbol{A}$ random
$\boldsymbol{p} = \mathbf{exp}(\boldsymbol{n} \log \boldsymbol{n})$
$|\boldsymbol{A}| = \boldsymbol{p}/\mathbf{2}$
$\boldsymbol{m} \approx \mathbf{6}\boldsymbol{n}$

DQI'24, Chailloux-Tillich'24

Regev-reduction quantum alg via $\boldsymbol{A}$-SIS

Input: $\boldsymbol{v_1}, \dots, \boldsymbol{v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{A} \subseteq \mathbf{F}_{\boldsymbol{p}}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1}, \dots, \boldsymbol{c_m}$ such that each $\boldsymbol{c_i} \in \boldsymbol{A}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Chen-Liu-Zhandry'21

Random $\{\boldsymbol{v_i}\}$
$\boldsymbol{A}$ arbitrary
$\boldsymbol{p} = \mathbf{poly}(\boldsymbol{n})$
$|\boldsymbol{A}| = \boldsymbol{p} - \boldsymbol{k} + \mathbf{1}$
$\boldsymbol{m} \approx \boldsymbol{n^k}$

Yamakawa-Zhandry'22

$\{\boldsymbol{v_i}\}$ folded RS code
$\boldsymbol{A}$ random
$\boldsymbol{p} = \mathbf{exp}(\boldsymbol{n} \log \boldsymbol{n})$
$|\boldsymbol{A}| = \boldsymbol{p}/\mathbf{2}$
$\boldsymbol{m} \approx \mathbf{6}\boldsymbol{n}$

DQI'24, Chailloux-Tillich'24

$\{\boldsymbol{v_i}\}$ RS code
$\boldsymbol{A}$ random

Regev-reduction quantum alg via $\boldsymbol{A}$-SIS

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{A} \subseteq \mathbf{F}_{\boldsymbol{p}}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $\boldsymbol{c_i} \in \boldsymbol{A}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Chen-Liu-Zhandry'21

Random $\{\boldsymbol{v_i}\}$
$\boldsymbol{A}$ arbitrary
$\boldsymbol{p} = \mathbf{poly}(\boldsymbol{n})$
$|\boldsymbol{A}| = \boldsymbol{p} - \boldsymbol{k} + \mathbf{1}$
$\boldsymbol{m} \approx \boldsymbol{n}^{\boldsymbol{k}}$

Yamakawa-Zhandry'22

$\{\boldsymbol{v_i}\}$ folded RS code
$\boldsymbol{A}$ random
$\boldsymbol{p} = \mathbf{exp}(\boldsymbol{n} \log \boldsymbol{n})$
$|\boldsymbol{A}| = \boldsymbol{p}/\mathbf{2}$
$\boldsymbol{m} \approx \mathbf{6}\boldsymbol{n}$

DQI'24, Chailloux-Tillich'24

$\{\boldsymbol{v_i}\}$ RS code
$\boldsymbol{A}$ random
$\boldsymbol{p} = \mathbf{4}\boldsymbol{n}$
$|\boldsymbol{A}| = \boldsymbol{p}/\mathbf{2}$
$\boldsymbol{m} = \mathbf{4}\boldsymbol{n}$

Regev-reduction quantum alg via $\boldsymbol{A}$-SIS

Input: $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in \mathbf{F}_p^n$ and $\boldsymbol{A} \subseteq \mathbf{F}_p$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c}_1, \dots, \boldsymbol{c}_m$ such that each $\boldsymbol{c}_i \in \boldsymbol{A}$ and $\sum \boldsymbol{c}_i \boldsymbol{v}_i \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Chen-Liu-Zhandry'21

Random $\{\boldsymbol{v}_i\}$
$\boldsymbol{A}$ arbitrary
$\boldsymbol{p} = \mathbf{poly}(\boldsymbol{n})$
$|\boldsymbol{A}| = \boldsymbol{p} - \boldsymbol{k} + \mathbf{1}$
$\boldsymbol{m} \approx \boldsymbol{n}^{\boldsymbol{k}}$

Now classically easy

Yamakawa-Zhandry'22

$\{\boldsymbol{v}_i\}$ folded RS code
$\boldsymbol{A}$ random
$\boldsymbol{p} = \mathbf{exp}(\boldsymbol{n} \log \boldsymbol{n})$
$|\boldsymbol{A}| = \boldsymbol{p}/\mathbf{2}$
$\boldsymbol{m} \approx \mathbf{6}\boldsymbol{n}$

DQI'24, Chailloux-Tillich'24

$\{\boldsymbol{v}_i\}$ RS code
$\boldsymbol{A}$ random
$\boldsymbol{p} = \mathbf{4}\boldsymbol{n}$
$|\boldsymbol{A}| = \boldsymbol{p}/\mathbf{2}$
$\boldsymbol{m} = \mathbf{4}\boldsymbol{n}$

Regev-reduction quantum alg via $\boldsymbol{A}$-SIS

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{A} \subseteq \mathbf{F}_{\boldsymbol{p}}$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \ldots, c_m}$ such that each $\boldsymbol{c_i} \in \boldsymbol{A}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Chen-Liu-Zhandry'21

Random $\{\boldsymbol{v_i}\}$
$\boldsymbol{A}$ arbitrary
$\boldsymbol{p} = \mathbf{poly}(\boldsymbol{n})$
$|\boldsymbol{A}| = \boldsymbol{p} - \boldsymbol{k} + \mathbf{1}$
$\boldsymbol{m} \approx \boldsymbol{n}^{\boldsymbol{k}}$

Now classically easy

Yamakawa-Zhandry'22

$\{\boldsymbol{v_i}\}$ folded RS code
$\boldsymbol{A}$ random
$\boldsymbol{p} = \mathbf{exp}(\boldsymbol{n} \log \boldsymbol{n})$
$|\boldsymbol{A}| = \boldsymbol{p}/\mathbf{2}$
$\boldsymbol{m} \approx \mathbf{6}\boldsymbol{n}$

Classically hard
in the query model

DQI'24, Chailloux-Tillich'24

$\{\boldsymbol{v_i}\}$ RS code
$\boldsymbol{A}$ random
$\boldsymbol{p} = \mathbf{4}\boldsymbol{n}$
$|\boldsymbol{A}| = \boldsymbol{p}/\mathbf{2}$
$\boldsymbol{m} = \mathbf{4}\boldsymbol{n}$

Regev-reduction quantum alg via $\boldsymbol{A}$-SIS

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_p^n$ and $\boldsymbol{A} \subseteq \mathbf{F}_p$ where $\boldsymbol{p}$ is a prime

Output: $\boldsymbol{c_1, \dots, c_m}$ such that each $\boldsymbol{c_i} \in \boldsymbol{A}$ and $\sum \boldsymbol{c_i v_i} \equiv \vec{\mathbf{0}} \bmod \boldsymbol{p}$

Chen-Liu-Zhandry'21

Random $\{\boldsymbol{v_i}\}$
$\boldsymbol{A}$ arbitrary
$\boldsymbol{p} = \mathbf{poly}(\boldsymbol{n})$
$|\boldsymbol{A}| = \boldsymbol{p} - \boldsymbol{k} + \mathbf{1}$
$\boldsymbol{m} \approx \boldsymbol{n^k}$

Now classically easy

Yamakawa-Zhandry'22

$\{\boldsymbol{v_i}\}$ folded RS code
$\boldsymbol{A}$ random
$\boldsymbol{p} = \mathbf{exp}(\boldsymbol{n} \log \boldsymbol{n})$
$|\boldsymbol{A}| = \boldsymbol{p}/\mathbf{2}$
$\boldsymbol{m} \approx \mathbf{6}\boldsymbol{n}$

Classically hard
in the query model

DQI'24, Chailloux-Tillich'24

$\{\boldsymbol{v_i}\}$ RS code
$\boldsymbol{A}$ random
$\boldsymbol{p} = \mathbf{4}\boldsymbol{n}$
$|\boldsymbol{A}| = \boldsymbol{p}/\mathbf{2}$
$\boldsymbol{m} = \mathbf{4}\boldsymbol{n}$

Still seems
classically hard

Regev-reduction quantum alg via $\boldsymbol{A}$-SIS

Why?

Chen-Liu-Zhandry'21

Random $\{\boldsymbol{v}_i\}$
$\boldsymbol{A}$ arbitrary
$\boldsymbol{p = \mathrm{poly}(n)}$
$\boldsymbol{|A| = p - k + 1}$
$\boldsymbol{m \approx n^k}$

Now classically easy

Yamakawa-Zhandry'22

$\{\boldsymbol{v}_i\}$ folded RS code
$\boldsymbol{A}$ random
$\boldsymbol{p = \exp(n \log n)}$
$\boldsymbol{|A| = p/2}$
$\boldsymbol{m \approx 6n}$

Classically hard
in the query model

DQI'24, Chailloux-Tillich'24

$\{\boldsymbol{v}_i\}$ RS code
$\boldsymbol{A}$ random
$\boldsymbol{p = 4n}$
$\boldsymbol{|A| = p/2}$
$\boldsymbol{m = 4n}$

Still seems
classically hard

Regev-reduction quantum alg via $\boldsymbol{A}$-SIS

Why? We can handle worst-case $\{\boldsymbol{v_i}\}$, exponential $\boldsymbol{p}$, and $\boldsymbol{A}$ of large size

Chen-Liu-Zhandry'21

Random $\{\boldsymbol{v_i}\}$
$\boldsymbol{A}$ arbitrary
$\boldsymbol{p = \mathrm{poly}(n)}$
$\boldsymbol{|A| = p - k + 1}$
$\boldsymbol{m \approx n^k}$

Now classically easy

Yamakawa-Zhandry'22

$\{\boldsymbol{v_i}\}$ folded RS code
$\boldsymbol{A}$ random
$\boldsymbol{p = \exp(n \log n)}$
$\boldsymbol{|A| = p/2}$
$\boldsymbol{m \approx 6n}$

Classically hard
in the query model

DQI'24, Chailloux-Tillich'24

$\{\boldsymbol{v_i}\}$ RS code
$\boldsymbol{A}$ random
$\boldsymbol{p = 4n}$
$\boldsymbol{|A| = p/2}$
$\boldsymbol{m = 4n}$

Still seems
classically hard

Regev-reduction quantum alg via $\boldsymbol{A}$-SIS

Why? We can handle worst-case $\{\boldsymbol{v}_i\}$, exponential $\boldsymbol{p}$, and $\boldsymbol{A}$ of large size
But we cannot handle $\boldsymbol{m} \ll \boldsymbol{n}^2$

Chen-Liu-Zhandry'21

Random $\{\boldsymbol{v}_i\}$
$\boldsymbol{A}$ arbitrary
$\boldsymbol{p} = \mathbf{poly}(\boldsymbol{n})$
$|\boldsymbol{A}| = \boldsymbol{p} - \boldsymbol{k} + \mathbf{1}$
$\boldsymbol{m} \approx \boldsymbol{n}^{\boldsymbol{k}}$

Now classically easy

Yamakawa-Zhandry'22

$\{\boldsymbol{v}_i\}$ folded RS code
$\boldsymbol{A}$ random
$\boldsymbol{p} = \mathbf{exp}(\boldsymbol{n} \log \boldsymbol{n})$
$|\boldsymbol{A}| = \boldsymbol{p}/\mathbf{2}$
$\boldsymbol{m} \approx \mathbf{6}\boldsymbol{n}$

Classically hard
in the query model

DQI'24, Chailloux-Tillich'24

$\{\boldsymbol{v}_i\}$ RS code
$\boldsymbol{A}$ random
$\boldsymbol{p} = \mathbf{4}\boldsymbol{n}$
$|\boldsymbol{A}| = \boldsymbol{p}/\mathbf{2}$
$\boldsymbol{m} = \mathbf{4}\boldsymbol{n}$

Still seems
classically hard

Regev-reduction quantum alg via $\boldsymbol{A}$-SIS

Why?

We can handle worst-case $\{\boldsymbol{v_i}\}$, exponential $\boldsymbol{p}$, and $\boldsymbol{A}$ of large size
But we cannot handle $\boldsymbol{m} \ll \boldsymbol{n}^2$

Chen-Liu-Zhandry'21	**Yamakawa-Zhandry'22**	**DQI'24, Chailloux-Tillich'24**
Random $\{\boldsymbol{v_i}\}$	$\{\boldsymbol{v_i}\}$ folded RS code	$\{\boldsymbol{v_i}\}$ RS code
$\boldsymbol{A}$ arbitrary	$\boldsymbol{A}$ random	$\boldsymbol{A}$ random
$\boldsymbol{p = \mathrm{poly}(n)}$	$\boldsymbol{p = \exp(n \log n)}$	$\boldsymbol{p = 4n}$
$\boldsymbol{\lvert A \rvert = p - k + 1}$	$\boldsymbol{\lvert A \rvert = p/2}$	$\boldsymbol{\lvert A \rvert = p/2}$
$\boldsymbol{m \approx n^k}$	$\boldsymbol{m \approx 6n}$	$\boldsymbol{m = 4n}$
Now classically easy	Classically hard in the query model	Still seems classically hard

Outline

Toy example: $\mathbf{F}_3^n$-Subset-Sum

Motivations

Main problem: the SIS^∞ problem

Cryptographic motivation

Full generalization: the $\boldsymbol{A}$-SIS problem

Quantum motivation

Algorithm overview

Algorithm overview

$\mathbf{F}_3^n$-Subset-Sum

Reducible vector

The SIS^∞ problem

Weight reduction

The $\boldsymbol{A}$-SIS problem

General reduction

$\mathbb{F}_3^n$-Subset-Sum

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_3^n$ where $\boldsymbol{m \approx n^2/3}$

Output: a nontrivial subset that sums to $\vec{\mathbf{0}}$

$\mathbf{F}_3^n$-Subset-Sum

$\boldsymbol{n^2} \;\rightarrow\; \boldsymbol{n^2/2} \;\rightarrow \boldsymbol{n^2/3}$

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_3^n$ where $\boldsymbol{m \approx n^2/3}$

Output: a nontrivial subset that sums to $\vec{\mathbf{0}}$

$\mathbb{F}_3^n$-Subset-Sum

Input: $v_1, \dots, v_m \in \mathbb{F}_3^n$ where $m = (n+1)^2 \approx n^2$

Output: a nontrivial subset that sums to $\vec{0}$

$\mathbb{F}_3^n$-Subset-Sum

Input: $v_1, \dots, v_m \in \mathbb{F}_3^n$ where $m = (n+1)^2 \approx n^2$

Output: a nontrivial subset that sums to $\vec{0}$

Partition m input vectors into $n+1$ batches of $n+1$ vectors

$v_1^{(1)}, \dots, v_{n+1}^{(1)}$	$v_1^{(2)}, \dots, v_{n+1}^{(2)}$	$\dots\dots$	$v_1^{(n+1)}, \dots, v_{n+1}^{(n+1)}$

$\mathbf{F}_3^n$-Subset-Sum

Input: $v_1, \ldots, v_m \in \mathbf{F}_3^n$ where $m = (n+1)^2 \approx n^2$

Output: a nontrivial subset that sums to $\vec{0}$

Partition m input vectors into $n+1$ batches of $n+1$ vectors

Compute linear dependence in each batch

$\mathbf{F}_3^n$-Subset-Sum

Input: $v_1, \ldots, v_m \in \mathbf{F}_3^n$ where $m = (n+1)^2 \approx n^2$

Output: a nontrivial subset that sums to $\vec{0}$

Partition m input vectors into $n+1$ batches of $n+1$ vectors

Compute linear dependence in each batch

$\sum_i \alpha_i v_i^{(1)} = \vec{0}$ where $\alpha_i \in \{0, 1, -1\}$ not all-0

$v_1^{(1)}, \ldots, v_{n+1}^{(1)}$

$\mathbf{F}_3^n$-Subset-Sum

Input: $v_1, \dots, v_m \in \mathbf{F}_3^n$ where $m = (n+1)^2 \approx n^2$

Output: a nontrivial subset that sums to $\vec{0}$

Partition m input vectors into $n+1$ batches of $n+1$ vectors

Compute linear dependence in each batch

$\sum_i \alpha_i v_i^{(1)} = \vec{0}$ where $\alpha_i \in \{0, 1, -1\}$ not all-$\mathbf{0}$

$v_1^{(1)}, \dots, v_{n+1}^{(1)}$

Define $u^{(1)} = \sum_{i:\alpha_i=1} v_i^{(1)}$ and $w^{(1)} = \sum_{i:\alpha_i=-1} v_i^{(1)}$

$\mathbb{F}_3^n$-Subset-Sum

Input: $v_1, \dots, v_m \in \mathbb{F}_3^n$ where $m = (n+1)^2 \approx n^2$

Output: a nontrivial subset that sums to $\vec{0}$

Partition m input vectors into $n+1$ batches of $n+1$ vectors

Compute linear dependence in each batch

$v_1^{(1)}, \dots, v_{n+1}^{(1)}$

$\sum_i \alpha_i v_i^{(1)} = \vec{0}$ where $\alpha_i \in \{0, 1, -1\}$ not all-$\mathbf{0}$

Define $u^{(1)} = \sum_{i:\alpha_i=1} v_i^{(1)}$ and $w^{(1)} = \sum_{i:\alpha_i=-1} v_i^{(1)}$

Then $u^{(1)} = w^{(1)}$ are disjoint subset-sum in this batch

$\mathbb{F}_3^n$-Subset-Sum

Input: $v_1, \dots, v_m \in \mathbb{F}_3^n$ where $m = (n+1)^2 \approx n^2$

Output: a nontrivial subset that sums to $\vec{0}$

Partition m input vectors into $n+1$ batches of $n+1$ vectors

Compute **2** disjoint subset-sums that are equal in each batch

$v_1^{(1)}, \dots, v_{n+1}^{(1)}$

$\sum_i \alpha_i v_i^{(1)} = \vec{0}$ where $\alpha_i \in \{0, 1, -1\}$ not all-$\mathbf{0}$

Define $u^{(1)} = \sum_{i:\alpha_i=1} v_i^{(1)}$ and $w^{(1)} = \sum_{i:\alpha_i=-1} v_i^{(1)}$

Then $u^{(1)} = w^{(1)}$ are disjoint subset-sum in this batch

$\mathbb{F}_3^n$-Subset-Sum

Input: $v_1, \dots, v_m \in \mathbb{F}_3^n$ where $m = (n+1)^2 \approx n^2$

Output: a nontrivial subset that sums to $\vec{0}$

Partition m input vectors into $n+1$ batches of $n+1$ vectors

Compute **2** disjoint subset-sums that are equal in each batch

$v_1^{(1)}, \dots, v_{n+1}^{(1)}$

$\sum_i \alpha_i v_i^{(1)} = \vec{0}$ where $\alpha_i \in \{0, 1, -1\}$ not all-$\mathbf{0}$

Define $u^{(1)} = \sum_{i:\alpha_i=1} v_i^{(1)}$ and $w^{(1)} = \sum_{i:\alpha_i=-1} v_i^{(1)}$

Then $u^{(1)} = w^{(1)}$ are disjoint subset-sum in this batch

If $u^{(1)} = w^{(1)} = \vec{0}$, we are done

$\mathbb{F}_3^n$-Subset-Sum

Input: $v_1, \dots, v_m \in \mathbb{F}_3^n$ where $m = (n+1)^2 \approx n^2$

Output: a nontrivial subset that sums to $\vec{0}$

Partition m input vectors into $n+1$ batches of $n+1$ vectors

Compute **2** disjoint subset-sums that are equal in each batch

$v_1^{(1)}, \dots, v_{n+1}^{(1)}$	$v_1^{(2)}, \dots, v_{n+1}^{(2)}$	……	$v_1^{(n+1)}, \dots, v_{n+1}^{(n+1)}$
$\Downarrow$	$\Downarrow$		$\Downarrow$
$u^{(1)} = w^{(1)}$	$u^{(2)} = w^{(2)}$	……	$u^{(n+1)} = w^{(n+1)}$

$\mathbf{F}_3^n$-Subset-Sum

Input: $v_1, \dots, v_m \in \mathbf{F}_3^n$ where $m = (n+1)^2 \approx n^2$

Output: a nontrivial subset that sums to $\vec{\mathbf{0}}$

Partition m input vectors into $n+1$ batches of $n+1$ vectors

Compute **2** disjoint subset-sums $u^{(i)} = w^{(i)}$ in each batch

$\mathbf{F}_3^n$-Subset-Sum

Input: $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in \mathbf{F}_3^n$ where $\boldsymbol{m} = (\boldsymbol{n} + \mathbf{1})^2 \approx \boldsymbol{n}^2$

Output: a nontrivial subset that sums to $\vec{\mathbf{0}}$

Partition $\boldsymbol{m}$ input vectors into $\boldsymbol{n} + \mathbf{1}$ batches of $\boldsymbol{n} + \mathbf{1}$ vectors

Compute **2** disjoint subset-sums $\boldsymbol{u}^{(i)} = \boldsymbol{w}^{(i)}$ in each batch

Compute linear dependence of the subset-sums

$\mathbf{F}_3^n$-Subset-Sum

Input: $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in \mathbf{F}_3^n$ where $\boldsymbol{m = (n+1)^2 \approx n^2}$

Output: a nontrivial subset that sums to $\vec{\mathbf{0}}$

Partition $\boldsymbol{m}$ input vectors into $\boldsymbol{n+1}$ batches of $\boldsymbol{n+1}$ vectors

Compute **2** disjoint subset-sums $\boldsymbol{u}^{(i)} = \boldsymbol{w}^{(i)}$ in each batch

Compute linear dependence of the subset-sums

$$\boldsymbol{\beta}_1 \boldsymbol{u}^{(1)} + \boldsymbol{\beta}_2 \boldsymbol{u}^{(2)} + \cdots + \boldsymbol{\beta}_{n+1} \boldsymbol{u}^{(n+1)} = \vec{\mathbf{0}} \quad \text{where} \quad \boldsymbol{\beta}_i \in \{\mathbf{0}, \mathbf{1}, \mathbf{2}\} \text{ not all-}\mathbf{0}$$

$\mathbf{F}_3^n$-Subset-Sum

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_3^n$ where $\boldsymbol{m = (n+1)^2 \approx n^2}$

Output: a nontrivial subset that sums to $\vec{\mathbf{0}}$

Partition $\boldsymbol{m}$ input vectors into $\boldsymbol{n+1}$ batches of $\boldsymbol{n+1}$ vectors

Compute **2** disjoint subset-sums $\boldsymbol{u^{(i)}} = \boldsymbol{w^{(i)}}$ in each batch

Compute linear dependence of the subset-sums

$$\boldsymbol{\beta_1 u^{(1)} + \beta_2 u^{(2)} + \cdots + \beta_{n+1} u^{(n+1)}} = \vec{\mathbf{0}} \quad \text{where} \quad \boldsymbol{\beta_i} \in \{\mathbf{0}, \mathbf{1}, \mathbf{2}\} \text{ not all-}\mathbf{0}$$

$$\boldsymbol{\beta_i} = \begin{cases} \mathbf{0} \\ \mathbf{1} \\ \mathbf{2} \end{cases}$$

$\mathbf{F}_3^n$-Subset-Sum

Input: $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in \mathbf{F}_3^n$ where $\boldsymbol{m} = (\boldsymbol{n}+\mathbf{1})^2 \approx \boldsymbol{n}^2$

Output: a nontrivial subset that sums to $\vec{\mathbf{0}}$

Partition $\boldsymbol{m}$ input vectors into $\boldsymbol{n}+\mathbf{1}$ batches of $\boldsymbol{n}+\mathbf{1}$ vectors

Compute **2** disjoint subset-sums $\boldsymbol{u}^{(i)} = \boldsymbol{w}^{(i)}$ in each batch

Compute linear dependence of the subset-sums

$$\boldsymbol{\beta}_1\boldsymbol{u}^{(1)} + \boldsymbol{\beta}_2\boldsymbol{u}^{(2)} + \cdots + \boldsymbol{\beta}_{n+1}\boldsymbol{u}^{(n+1)} = \vec{\mathbf{0}} \quad \text{where} \quad \boldsymbol{\beta}_i \in \{\mathbf{0}, \mathbf{1}, \mathbf{2}\} \text{ not all-}\mathbf{0}$$

$$\boldsymbol{\beta}_i = \begin{cases} \mathbf{0} & \boldsymbol{\beta}_i\boldsymbol{u}^{(i)} = \vec{\mathbf{0}} \text{ is a trivial subset-sum} \\ \mathbf{1} & \\ \mathbf{2} & \end{cases}$$

$\mathbb{F}_3^n$-Subset-Sum

Input: $v_1, \ldots, v_m \in \mathbb{F}_3^n$ where $m = (n+1)^2 \approx n^2$

Output: a nontrivial subset that sums to $\vec{0}$

Partition m input vectors into $n+1$ batches of $n+1$ vectors

Compute **2** disjoint subset-sums $u^{(i)} = w^{(i)}$ in each batch

Compute linear dependence of the subset-sums

$$\beta_1 u^{(1)} + \beta_2 u^{(2)} + \cdots + \beta_{n+1} u^{(n+1)} = \vec{0} \quad \text{where} \quad \beta_i \in \{0, 1, 2\} \text{ not all-}0$$

$$\beta_i = \begin{cases} 0 & \beta_i u^{(i)} = \vec{0} \text{ is a trivial subset-sum} \\ 1 & \beta_i u^{(i)} = u^{(i)} \text{ is a subset-sum} \\ 2 & \end{cases}$$

$\mathbb{F}_3^n$-Subset-Sum

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbb{F}_3^n$ where $\boldsymbol{m = (n+1)^2 \approx n^2}$

Output: a nontrivial subset that sums to $\vec{\mathbf{0}}$

Partition $\boldsymbol{m}$ input vectors into $\boldsymbol{n+1}$ batches of $\boldsymbol{n+1}$ vectors

Compute **2** disjoint subset-sums $\boldsymbol{u^{(i)} = w^{(i)}}$ in each batch

Compute linear dependence of the subset-sums

$$\boldsymbol{\beta_1 u^{(1)} + \beta_2 u^{(2)} + \cdots + \beta_{n+1} u^{(n+1)} = \vec{0}} \quad \text{where} \quad \boldsymbol{\beta_i} \in \{\mathbf{0}, \mathbf{1}, \mathbf{2}\} \text{ not all-}\mathbf{0}$$

$$\boldsymbol{\beta_i} = \begin{cases} \mathbf{0} & \boldsymbol{\beta_i u^{(i)}} = \vec{\mathbf{0}} \text{ is a trivial subset-sum} \\ \mathbf{1} & \boldsymbol{\beta_i u^{(i)} = u^{(i)}} \text{ is a subset-sum} \\ \mathbf{2} & \boldsymbol{\beta_i u^{(i)} = 2u^{(i)} = u^{(i)} + w^{(i)}} \text{ is a subset-sum} \end{cases}$$

$\mathbf{F}_3^n$-Subset-Sum

Input: $v_1, \ldots, v_m \in \mathbf{F}_3^n$ where $m = (n+1)^2 \approx n^2$

Output: a nontrivial subset that sums to $\vec{0}$

Partition m input vectors into $n+1$ batches of $n+1$ vectors

Compute 2 disjoint subset-sums $u^{(i)} = w^{(i)}$ in each batch

Compute linear dependence of the subset-sums

$$\beta_1 u^{(1)} + \beta_2 u^{(2)} + \cdots + \beta_{n+1} u^{(n+1)} = \vec{0} \quad \text{where} \quad \beta_i \in \{0, 1, 2\} \text{ not all-}0$$

Substitute back

$$\beta_i = \begin{cases} 0 & \beta_i u^{(i)} = \vec{0} \text{ is a trivial subset-sum} \\ 1 & \beta_i u^{(i)} = u^{(i)} \text{ is a subset-sum} \\ 2 & \beta_i u^{(i)} = 2u^{(i)} = u^{(i)} + w^{(i)} \text{ is a subset-sum} \end{cases}$$

$\mathbf{F}_3^n$-Subset-Sum

Input: $v_1, \ldots, v_m \in \mathbf{F}_3^n$ where $m \approx n^2 \rightarrow n^2/2$

Output: a nontrivial subset that sums to $\vec{\mathbf{0}}$

$\mathbf{F}_3^n$-Subset-Sum

Dimension reduction

Input: $v_1, \dots, v_m \in \mathbf{F}_3^n$ where $m \approx n^2 \to n^2/2$

Output: a nontrivial subset that sums to $\vec{\mathbf{0}}$

$\mathbf{F}_3^n$-Subset-Sum

Dimension reduction

Input: $v_1, \dots, v_m \in \mathbf{F}_3^n$ where $m \approx n^2 \to n^2/2$

Output: a nontrivial subset that sums to $\vec{\mathbf{0}}$

$v_1, \dots, v_{n+1}$

$v_{n+2}, v_{n+3}, \dots, v_m$

$\mathbf{F}_3^n$-Subset-Sum

Dimension reduction

Input: $v_1, \dots, v_m \in \mathbf{F}_3^n$ where $m \approx n^2 \to n^2/2$

Output: a nontrivial subset that sums to $\vec{0}$

$v_1, \dots, v_{n+1}$

$u = w$

$v_{n+2}, v_{n+3}, \dots, v_m$

$0 \cdot u = \vec{0}$ is a subset-sum

$1 \cdot u = u$ is a subset-sum

$2 \cdot u = u + w$ is a subset-sum

$\mathbb{F}_3^n$-Subset-Sum

Dimension reduction

Input: $v_1, \dots, v_m \in \mathbb{F}_3^n$ where $m \approx n^2 \to n^2/2$

Output: a nontrivial subset that sums to $\vec{0}$

$v_1, \dots, v_{n+1}$

$u = w$

$0 \cdot u = \vec{0}$ is a subset-sum

$1 \cdot u = u$ is a subset-sum

$2 \cdot u = u + w$ is a subset-sum

$v_{n+2}, v_{n+3}, \dots, v_m$

$v_j = c_j u + v'_j$ where

- $v'_j \in u^{\perp}$ (complement space of u)
- $c_j = 0, 1, 2$

$\mathbb{F}_3^n$-Subset-Sum

Dimension reduction

Input: $v_1, \dots, v_m \in \mathbb{F}_3^n$ where $m \approx n^2 \to n^2/2$

Output: a nontrivial subset that sums to $\vec{0}$

$v_1, \dots, v_{n+1}$

$u = w$

$0 \cdot u = \vec{0}$ is a subset-sum
$1 \cdot u = u$ is a subset-sum
$2 \cdot u = u + w$ is a subset-sum

$v_{n+2}, v_{n+3}, \dots, v_m$

$v_j = c_j u + v_j'$ where

- $v_j' \in u^\perp$ (complement space of u)
- $c_j = 0, 1, 2$

A subset sums to $\vec{0}$ in $u^\perp$ is a multiple of u in the whole space

$\mathbb{F}_3^n$-Subset-Sum

Dimension reduction

Input: $v_1, \dots, v_m \in \mathbb{F}_3^n$ where $m \approx n^2 \to n^2/2$

Output: a nontrivial subset that sums to $\vec{0}$

$v_1, \dots, v_{n+1}$

$u = w$

$0 \cdot u = \vec{0}$ is a subset-sum
$1 \cdot u = u$ is a subset-sum
$2 \cdot u = u + w$ is a subset-sum

$v_{n+2}, v_{n+3}, \dots, v_m$

$v_j = c_j u + v_j'$ where

- $v_j' \in u^\perp$ (complement space of u)
- $c_j = 0, 1, 2$

A subset sums to $\vec{0}$ in $u^\perp$ is a multiple of u in the whole space

$\mathbb{F}_3^n$-Subset-Sum

Dimension reduction

Input: $v_1, \dots, v_m \in \mathbb{F}_3^n$ where $m \approx n^2 \to n^2/2$

Output: a nontrivial subset that sums to $\vec{0}$

$v_1, \dots, v_{n+1}$

$u = w$

$0 \cdot u = \vec{0}$ is a subset-sum
$1 \cdot u = u$ is a subset-sum
$2 \cdot u = u + w$ is a subset-sum

$v_{n+2}, v_{n+3}, \dots, v_m$

$v_j = c_j u + v_j'$ where

- $v_j' \in u^\perp$ (complement space of u)
- $c_j = 0, 1, 2$

One dimension smaller

A subset sums to $\vec{0}$ in $u^\perp$ is a multiple of u in the whole space

$\mathbb{F}_3^n$-Subset-Sum

Dimension reduction

Input: $v_1, \dots, v_m \in \mathbb{F}_3^n$ where $m \approx n^2 \to n^2/2$

Output: a nontrivial subset that sums to $\vec{0}$

$v_1, \dots, v_{n+1}$

$v_{n+2}, v_{n+3}, \dots, v_m$

$$\underbrace{n+1 \qquad\qquad \text{\#vectors needed for dim } n-1}_{\text{\#vectors needed for dim } n}$$

$\mathbb{F}_3^n$-Subset-Sum

Dimension reduction

Input: $v_1, \dots, v_m \in \mathbb{F}_3^n$ where $m \approx n^2 \to n^2/2$

Output: a nontrivial subset that sums to $\mathbf{0}$

$v_1, \dots, v_{n+1}$ | $v_{n+2}, v_{n+3}, \dots, v_m$

$$\underbrace{n + 1 \qquad \text{\#vectors needed for dim } n - 1}_{\text{\#vectors needed for dim } n}$$

$\mathbf{F}_3^n$-Subset-Sum

Input: $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in \mathbf{F}_3^n$ where $\boldsymbol{m \approx n^2 \to n^2/2 \to n^2/3}$

Output: a nontrivial subset that sums to $\vec{\mathbf{0}}$

$\mathbf{F}_3^n$-Subset-Sum

Explore sparsity

Input: $v_1, \dots, v_m \in \mathbf{F}_3^n$ where $m \approx n^2 \to n^2/2 \to n^2/3$

Output: a nontrivial subset that sums to $\vec{0}$

$\mathbb{F}_3^n$-Subset-Sum

Explore sparsity

Input: $v_1, \dots, v_m \in \mathbb{F}_3^n$ where $m \approx n^2 \to n^2/2 \to n^2/3$

Output: a nontrivial subset that sums to $\vec{0}$

$v_1, \dots, v_{n+1}$

$$u = w$$

$0 \cdot u = \vec{0}$ is a subset-sum
$1 \cdot u = u$ is a subset-sum
$2 \cdot u = u + w$ is a subset-sum

$\mathbb{F}_3^n$-Subset-Sum

Explore sparsity

Input: $v_1, \ldots, v_m \in \mathbb{F}_3^n$ where $m \approx n^2 \to n^2/2 \to n^2/3$

Output: a nontrivial subset that sums to $\vec{0}$

$v_1, \ldots, v_{n+1}$

$u = w$

$0 \cdot u = \vec{0}$ is a subset-sum

$1 \cdot u = u$ is a subset-sum

$2 \cdot u = u + w$ is a subset-sum

Def (reducible vector).
u is reducible in $T \subseteq [m]$ if any multiple of u is a subset-sum of vectors in T

$\mathbf{F}_3^n$-Subset-Sum

Explore sparsity

Input: $v_1, \dots, v_m \in \mathbf{F}_3^n$ where $m \approx n^2 \to n^2/2 \to n^2/3$

Output: a nontrivial subset that sums to $\vec{0}$

$v_1, \dots, v_{n+1}$

$u = w$

$0 \cdot u = \vec{0}$ is a subset-sum

$1 \cdot u = u$ is a subset-sum

$2 \cdot u = u + w$ is a subset-sum

Def (reducible vector).
u is reducible in $T \subseteq [m]$ if any multiple of u is a subset-sum of vectors in T

Fact.
Reducible vector u exists with $|T| = n + 1$

$\mathbf{F}_3^n$-Subset-Sum

Explore sparsity

Input: $v_1, \dots, v_m \in \mathbf{F}_3^n$ where $m \approx n^2 \to n^2/2 \to n^2/3$

Output: a nontrivial subset that sums to $\vec{\mathbf{0}}$

$v_1, \dots, v_{n+1}$

$\Downarrow$

$u = w$

$0 \cdot u = \vec{\mathbf{0}}$ is a subset-sum
$1 \cdot u = u$ is a subset-sum
$2 \cdot u = u + w$ is a subset-sum

Def (reducible vector).
u is reducible in $T \subseteq [m]$ if any multiple of u is a subset-sum of vectors in T

Fact.
Reducible vector u exists with $|T| = n + 1$

Claim.
Reducible vector u exists with $|T| \approx 2n/3$ whenever $m \geq n + \log n$

$\mathbf{F}_3^n$-Subset-Sum

Explore sparsity

Input: $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in \mathbf{F}_3^n$ where $\boldsymbol{m \approx n^2 \to n^2/2 \to n^2/3}$

Output: a nontrivial subset that sums to $\vec{\mathbf{0}}$

Claim.
Reducible vector $\boldsymbol{u}$ exists with $|\boldsymbol{T}| \approx \boldsymbol{2n/3}$ whenever $\boldsymbol{m} \geq \boldsymbol{n} + \mathbf{log}\, \boldsymbol{n}$

$\mathbf{F}_3^n$-Subset-Sum

Explore sparsity

Input: $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbf{F}_3^n$ where $\boldsymbol{m} \approx \boldsymbol{n}^2 \to \boldsymbol{n}^2/2 \to \boldsymbol{n}^2/3$

Output: a nontrivial subset that sums to $\vec{\mathbf{0}}$

Claim.
Reducible vector $\boldsymbol{u}$ exists with $|\boldsymbol{T}| \approx \mathbf{2}\boldsymbol{n}/\mathbf{3}$ whenever $\boldsymbol{m} \geq \boldsymbol{n} + \log \boldsymbol{n}$

$\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$

Reducible $\boldsymbol{u}$

Find $\vec{\mathbf{0}}$ in $\boldsymbol{u}^{\perp}$ (dim $\boldsymbol{n} - \mathbf{1}$)

$\mathbb{F}_3^n$-Subset-Sum

Explore sparsity

Input: $v_1, \dots, v_m \in \mathbb{F}_3^n$ where $m \approx n^2 \to n^2/2 \to n^2/3$

Output: a nontrivial subset that sums to $\vec{0}$

Claim.
Reducible vector u exists with $|T| \approx 2n/3$ whenever $m \geq n + \log n$

$v_1, \dots, v_m$

$v_1, \dots, v_{2n/3}$ $\Rightarrow$ Reducible u

$v_{2n/3+1}, \dots, v_m$ $\Rightarrow$ Find $\vec{0}$ in $u^\perp$ (dim $n-1$)

$\mathbf{F}_3^n$-Subset-Sum

Explore sparsity

Input: $v_1, \dots, v_m \in \mathbf{F}_3^n$ where $m \approx n^2 \to n^2/2 \to n^2/3$

Output: a nontrivial subset that sums to $\vec{\mathbf{0}}$

Claim.
Reducible vector u exists with $|T| \approx 2n/3$ whenever $m \geq n + \log n$

$$\frac{n^2}{3} = \frac{n^2}{2} \cdot \frac{2}{3}$$

$v_1, \dots, v_m$

$v_1, \dots, v_{2n/3}$ | $v_{2n/3+1}, \dots, v_m$

Reducible u

Find $\vec{\mathbf{0}}$ in $u^{\perp}$ (dim $n-1$)

$\mathbb{F}_3^n$-Subset-Sum

Def (reducible vector).
$\boldsymbol{u}$ is reducible in $\boldsymbol{T} \subseteq [\boldsymbol{m}]$ if any multiple of $\boldsymbol{u}$ is a subset-sum of vectors in $\boldsymbol{T}$

Claim.
Reducible vector $\boldsymbol{u}$ exists with $|\boldsymbol{T}| \approx \boldsymbol{2n/3}$ whenever $\boldsymbol{m} \geq \boldsymbol{n} + \log \boldsymbol{n}$

$\mathbb{F}_3^n$-Subset-Sum

Def (reducible vector).
u is reducible in $T \subseteq [m]$ if any multiple of u is a subset-sum of vectors in T

Claim.
Reducible vector u exists with $|T| \approx 2n/3$ whenever $m \geq n + \log n$

Claim.
Linear dependence exists with $|T| \approx 2n/3$ whenever $m \geq n + \log n$

$\mathbb{F}_3^n$-Subset-Sum

$\sum_{i \in T} \alpha_i v_i = \vec{0}$ where $\alpha_i \in \{1, -1\}$

Def (reducible vector).
u is reducible in $T \subseteq [m]$ if any multiple of u is a subset-sum of vectors in T

Claim.
Reducible vector u exists with $|T| \approx 2n/3$ whenever $m \geq n + \log n$

Claim.
Linear dependence exists with $|T| \approx 2n/3$ whenever $m \geq n + \log n$

$\mathbb{F}_3^n$-Subset-Sum

$\sum_{i \in T} \alpha_i v_i = \vec{0}$ where $\alpha_i \in \{1, -1\}$

Let $u = \sum_{i:\alpha_i = 1} v_i$ and $w = \sum_{i:\alpha_i = -1} v_i$

Then $u = w$ are disjoint subset-sum in $\{v_i\}$

Def (reducible vector).
u is reducible in $T \subseteq [m]$ if any multiple of u is a subset-sum of vectors in T

Claim.
Reducible vector u exists with $|T| \approx 2n/3$ whenever $m \geq n + \log n$

Claim.
Linear dependence exists with $|T| \approx 2n/3$ whenever $m \geq n + \log n$

$\mathbb{F}_3^n$-Subset-Sum

$\sum_{i\in T} \alpha_i v_i = \vec{0}$ where $\alpha_i \in \{1, -1\}$

Let $u = \sum_{i:\alpha_i=1} v_i$ and $w = \sum_{i:\alpha_i=-1} v_i$

Then $u = w$ are disjoint subset-sum in $\{v_i\}$

$\Downarrow$

$0 \cdot u = \vec{0}$ is a subset-sum
$1 \cdot u = u$ is a subset-sum
$2 \cdot u = u + w$ is a subset-sum

Def (reducible vector).
u is reducible in $T \subseteq [m]$ if any multiple of u is a subset-sum of vectors in T

Claim.
Reducible vector u exists with $|T| \approx 2n/3$ whenever $m \geq n + \log n$

Claim.
Linear dependence exists with $|T| \approx 2n/3$ whenever $m \geq n + \log n$

$\mathbb{F}_3^n$-Subset-Sum

Def (reducible vector).
u is reducible in $T \subseteq [m]$ if any multiple of u is a subset-sum of vectors in T

Claim.
Reducible vector u exists with $|T| \approx 2n/3$ whenever $m \geq n + \log n$

Claim.
Linear dependence exists with $|T| \approx 2n/3$ whenever $m \geq n + \log n$

$\sum_{i \in T} \alpha_i v_i = \vec{0}$ where $\alpha_i \in \{1, -1\}$

Let $u = \sum_{i:\alpha_i=1} v_i$ and $w = \sum_{i:\alpha_i=-1} v_i$

Then $u = w$ are disjoint subset-sum in $\{v_i\}$

$0 \cdot u = \vec{0}$ is a subset-sum
$1 \cdot u = u$ is a subset-sum
$2 \cdot u = u + w$ is a subset-sum

$\Rightarrow$ u is reducible

$\mathbf{F}_3^n$-Subset-Sum

Claim.
Linear dependence exists with $|T| \approx 2n/3$ whenever $m \geq n + \log n$

$v_1, \dots, v_n$

$y_1, \dots, y_k$ for $k = \log n$

$\mathbb{F}_3^n$-Subset-Sum

Claim.
Linear dependence exists with $|T| \approx 2n/3$ whenever $m \geq n + \log n$

$v_1, \dots, v_n$

$y_1, \dots, y_k$ for $k = \log n$

Basis change

$e_1, \dots, e_n$

$z_1, \dots, z_k$

$\mathbb{F}_3^n$-Subset-Sum

Claim.
Linear dependence exists with $|T| \approx 2n/3$ whenever $m \geq n + \log n$

$v_1, \dots, v_n$

Basis change

$e_1, \dots, e_n$

$y_1, \dots, y_k$ for $k = \log n$

$z_1, \dots, z_k$

Random linear comb with $\alpha_1, \dots, \alpha_k \in \mathbb{F}_3$

In expectation $z = \sum_i \alpha_i z_i$ has at most $2n/3$ nonzero entries

$\mathbf{F}_3^n$-Subset-Sum

Claim.
Linear dependence exists with $|T| \approx 2n/3$ whenever $m \geq n + \log n$

$v_1, \dots, v_n$

Basis change

$e_1, \dots, e_n$

$y_1, \dots, y_k$ for $k = \log n$

$z_1, \dots, z_k$

Random linear comb with $\alpha_1, \dots, \alpha_k \in \mathbf{F}_3$

In expectation $z = \sum_i \alpha_i z_i$ has at most $2n/3$ nonzero entries

Derandom and exclude $\alpha_1 = \cdots = \alpha_k = 0$

Some explicit nontrivial $z = \sum_i \alpha_i z_i$ has at most $\frac{2n/3}{1-3^{-k}} \approx 2n/3$ nonzero entries

$\mathbf{F}_3^n$-Subset-Sum

Claim.
Linear dependence exists with $|T| \approx 2n/3$ whenever $m \geq n + \log n$

$v_1, \dots, v_n$

$y_1, \dots, y_k$ for $k = \log n$

Basis change

$e_1, \dots, e_n$

$z_1, \dots, z_k$

Random linear comb with $\alpha_1, \dots, \alpha_k \in \mathbf{F}_3$

In expectation $z = \sum_i \alpha_i z_i$ has at most $2n/3$ nonzero entries

Derandom and exclude $\alpha_1 = \cdots = \alpha_k = 0$

Some explicit nontrivial $z = \sum_i \alpha_i z_i$ has at most $\frac{2n/3}{1-3^{-k}} \approx 2n/3$ nonzero entries

Use $\approx 2n/3$ of them to produce $-z$

$\mathbf{F}_3^n$-Subset-Sum

Claim.
Linear dependence exists with $|T| \approx 2n/3$ whenever $m \geq n + \log n$

$v_1, \dots, v_n$

Basis change

$e_1, \dots, e_n$

Use $\approx 2n/3$ of them to produce $-z$

$y_1, \dots, y_k$ for $k = \log n$

$z_1, \dots, z_k$

Random linear comb with $\alpha_1, \dots, \alpha_k \in \mathbf{F}_3$

In expectation $z = \sum_i \alpha_i z_i$ has at most $2n/3$ nonzero entries

Derandom and exclude $\alpha_1 = \cdots = \alpha_k = 0$

Some explicit nontrivial $z = \sum_i \alpha_i z_i$ has at most $\frac{2n/3}{1-3^{-k}} \approx 2n/3$ nonzero entries

Linear dependence using $\approx 2n/3 + k \approx 2n/3$ vectors

Open problem on $\mathbb{F}_3^n$-Subset-Sum

Given $m \approx n^2/3$ vectors in $\mathbb{F}_3^n$, we can efficiently find a nontrivial subset that sums to $\vec{\mathbf{0}}$

Open problem on $\mathbf{F}_3^n$-Subset-Sum

Given $m \approx n^2/3$ vectors in $\mathbf{F}_3^n$, we can efficiently find a nontrivial subset that sums to $\vec{\mathbf{0}}$

Is $m \ll n^2/3$ possible?

Open problem on $\mathbb{F}_3^n$-Subset-Sum

Given $m \approx n^2/3$ vectors in $\mathbb{F}_3^n$, we can efficiently find a nontrivial subset that sums to $\vec{0}$

Is $m \ll n^2/3$ possible?

$m = 2n + 1$ guarantees solution

Open problem on $\mathbf{F}_3^n$-Subset-Sum

Given $m \approx n^2/3$ vectors in $\mathbf{F}_3^n$, we can efficiently find a nontrivial subset that sums to $\vec{\mathbf{0}}$

Is $m \ll n^2/3$ possible?

$m = 2n + 1$ guarantees solution

Average case?

Open problem on $\mathbf{F}_3^n$-Subset-Sum

Given $m \approx n^2/3$ vectors in $\mathbf{F}_3^n$, we can efficiently find a nontrivial subset that sums to $\vec{\mathbf{0}}$

Is $m \ll n^2/3$ possible?

$m = 2n + 1$ guarantees solution

Average case?

Given $m \approx (1 + o(1))n$ vectors in $\mathbf{F}_3^n$, we can efficiently find linear dependence that uses only $R \approx 2n/3$ vectors

Open problem on $\mathbf{F}_3^n$-Subset-Sum

Given $m \approx n^2/3$ vectors in $\mathbf{F}_3^n$, we can efficiently find a nontrivial subset that sums to $\vec{\mathbf{0}}$

Is $m \ll n^2/3$ possible?

$m = 2n + 1$ guarantees solution

Average case?

Given $m \approx (1 + o(1))n$ vectors in $\mathbf{F}_3^n$, we can efficiently find linear dependence that uses only $R \approx 2n/3$ vectors

Is $R \ll 2n/3$ possible?

Open problem on $\mathbb{F}_3^n$-Subset-Sum

Given $m \approx n^2/3$ vectors in $\mathbb{F}_3^n$, we can efficiently find a nontrivial subset that sums to $\vec{0}$

Is $m \ll n^2/3$ possible?

$m = 2n + 1$ guarantees solution

Average case?

Given $m \approx (1 + o(1))n$ vectors in $\mathbb{F}_3^n$, we can efficiently find linear dependence that uses only $R \approx 2n/3$ vectors

Is $R \ll 2n/3$ possible?

Open problem on $\mathbb{F}_3^n$-Subset-Sum

Given $m \approx n^2/3$ vectors in $\mathbb{F}_3^n$, we can efficiently find a nontrivial subset that sums to $\vec{0}$

Is $m \ll n^2/3$ possible?

$m = 2n + 1$ guarantees solution

Average case?

Given $m \approx \big(1 + o(1)\big)n$ vectors in $\mathbb{F}_3^n$, we can efficiently find linear dependence that uses only $R \approx 2n/3$ vectors

Is $R \ll 2n/3$ possible?

No, consider $e_1, \dots, e_n$ and $o(n)$ random vectors

Open problem on $\mathbf{F}_3^n$-Subset-Sum

Given $m \approx n^2/3$ vectors in $\mathbf{F}_3^n$, we can efficiently find a nontrivial subset that sums to $\vec{\mathbf{0}}$

Is $m \ll n^2/3$ possible?

$m = 2n + 1$ guarantees solution

Average case?

Given $m \approx n^{1.99}$ vectors in $\mathbf{F}_3^n$, we can efficiently find linear dependence that uses only $R \approx 2n/3$ vectors

Is $R \ll 2n/3$ possible?

Open problem on $\mathbf{F}_3^n$-Subset-Sum

Given $m \approx n^2/3$ vectors in $\mathbf{F}_3^n$, we can efficiently find a nontrivial subset that sums to $\vec{\mathbf{0}}$

Is $m \ll n^2/3$ possible?

$m = 2n + 1$ guarantees solution

Average case?

Given $m \approx n^{1.99}$ vectors in $\mathbf{F}_3^n$, we can efficiently find linear dependence that uses only $R \approx 2n/3$ vectors

Is $R \ll 2n/3$ possible?

$R \approx n/\log n$ is possible, ignoring efficiency

Open problem on $\mathbf{F}_3^n$-Subset-Sum

Given $m \approx n^{100}$ vectors in $\mathbf{F}_3^n$, we can efficiently find linear dependence that uses only $R \approx 2n/3$ vectors

Is $R \ll 2n/3$ possible?

$R \approx n/\log n$ is possible, ignoring efficiency

Open problem on $\mathbf{F}_3^n$-Subset-Sum

Given $m \approx n^{100}$ vectors in $\mathbf{F}_3^n$, we can efficiently find linear dependence that uses only $R \approx 2n/3$ vectors

Is $R \ll 2n/3$ possible?

$R \approx n/\log n$ is possible, ignoring efficiency

Given $m \approx n^{100}$ vectors in $\mathbf{F}_2^n$, we can efficiently find linear dependence that uses only $R \approx n/2$ vectors

Is $R \ll n/2$ possible?

$R \approx n/\log n$ is possible, ignoring efficiency

Algorithm overview

$\mathbf{F}_3^n$-Subset-Sum

Reducible vector

The SIS^∞ problem

Weight reduction

The $\boldsymbol{A}$-SIS problem

General reduction

The SIS^{∞} problem

Input: $\boldsymbol{v_1}, \dots, \boldsymbol{v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$

Output: linear dependence using coeffs in $\pm\boldsymbol{h}$

The SIS^{∞} problem

Input: $\boldsymbol{v_1}, \ldots, \boldsymbol{v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Fact. If $\boldsymbol{h} = \boldsymbol{p}/\mathbf{2}$, then $\boldsymbol{m} = \boldsymbol{n} + \mathbf{1}$ suffices

The SIS^{∞} problem

Input: $\boldsymbol{v_1}, \dots, \boldsymbol{v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Fact. If $\boldsymbol{h} = \boldsymbol{p}/\mathbf{2}$, then $\boldsymbol{m} = \boldsymbol{n} + \mathbf{1}$ suffices

Proof. View $\mathbf{F}_{\boldsymbol{p}}$ as $\{-\lfloor \boldsymbol{p}/\mathbf{2} \rfloor, \dots, \lfloor \boldsymbol{p}/\mathbf{2} \rfloor\}$

The SIS^{∞} problem

Input: $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Fact. If $\boldsymbol{h} = \boldsymbol{p}/2$, then $\boldsymbol{m} = \boldsymbol{n} + 1$ suffices

Lemma (weight halving).
If $\boldsymbol{m} = \boldsymbol{R}$ suffices for $\boldsymbol{h} = \boldsymbol{B}$, then $\boldsymbol{m} = \boldsymbol{R}^2$ suffices for $\boldsymbol{h} = \boldsymbol{B}/2$

The SIS^{∞} problem

Input: $\boldsymbol{v_1, \dots, v_m \in \mathbf{F}_p^n}$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Fact. If $\boldsymbol{h = p/2}$, then $\boldsymbol{m = n + 1}$ suffices

Lemma (weight halving).

If $\boldsymbol{m = R}$ suffices for $\boldsymbol{h = B}$, then $\boldsymbol{m = R^2}$ suffices for $\boldsymbol{h = B/2}$

Theorem (Imran-Ivanyos'25).

Assume $\boldsymbol{k}$ is a power of two and

$$\boldsymbol{m \gg p^{k \log k} n^k}$$

Classical polytime algorithm for

$$\boldsymbol{h = \frac{p}{2k}}$$

The SIS^∞ problem

Input: $\boldsymbol{v_1, \dots, v_m \in \mathbf{F}_p^n}$

Output: linear dependence using coeffs in $\boldsymbol{\pm h}$

Fact. If $\boldsymbol{h = p/2}$, then $\boldsymbol{m = n + 1}$ suffices

Lemma (weight halving).

If $\boldsymbol{m = R}$ suffices for $\boldsymbol{h = B}$, then $\boldsymbol{m = R^2}$ suffices for $\boldsymbol{h = B/2}$

Theorem (Imran-Ivanyos'25).

Assume $\boldsymbol{k}$ is a power of two and

$$\boldsymbol{m \gg \cancel{p^{k \log k}} n^k}$$

Classical polytime algorithm for

$$\boldsymbol{h = \frac{p}{2k}}$$

The SIS^{∞} problem

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Fact. If $\boldsymbol{h = p/2}$, then $\boldsymbol{m = n + 1}$ suffices

Lemma (weight halving).
If $\boldsymbol{m = R}$ suffices for $\boldsymbol{h = B}$, then $\boldsymbol{m = R^2}$ suffices for $\boldsymbol{h = B/2}$

Theorem (Imran-Ivanyos'25).
Assume $\boldsymbol{k}$ is a power of two and

$$\boldsymbol{m \gg \cancel{p^{k \log k}} n^k}$$

Classical polytime algorithm for

$$\boldsymbol{h = \frac{p}{2k}}$$

Proof.
By induction on $\boldsymbol{k = 2^i}$

The SIS$^\infty$ problem

Input: $\boldsymbol{v_1, \dots, v_m \in \mathbf{F}_p^n}$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Fact. If $\boldsymbol{h = p/2}$, then $\boldsymbol{m = n + 1}$ suffices

Lemma (weight halving).
If $\boldsymbol{m = R}$ suffices for $\boldsymbol{h = B}$, then $\boldsymbol{m = R^2}$ suffices for $\boldsymbol{h = B/2}$

Theorem (Imran-Ivanyos'25).
Assume $\boldsymbol{k}$ is a power of two and

$$\boldsymbol{m \gg \cancel{p^{k \log k}} n^k}$$

Classical polytime algorithm for

$$\boldsymbol{h = \frac{p}{2k}}$$

Proof.

By induction on $\boldsymbol{k = 2^i}$

Base case is $\boldsymbol{i = 0}$ and $\boldsymbol{h = \frac{p}{2}}$

Then $\boldsymbol{m \geq n + 1}$ suffices

The SIS^{∞} problem

Input: $v_1, \dots, v_m \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm h$

Fact. If $h = p/2$, then $m = n + 1$ suffices

Lemma (weight halving).
If $m = R$ suffices for $h = B$, then $m = R^2$ suffices for $h = B/2$

Theorem (Imran-Ivanyos'25).
Assume k is a power of two and

$$m \gg \cancel{p^{k\log k}} n^k$$

Classical polytime algorithm for

$$h = \frac{p}{2k}$$

Proof.
By induction on $k = 2^i$
Base case is $i = 0$ and $h = \frac{p}{2}$
Then $m \geq n + 1$ suffices

The SIS$^\infty$ problem

Input: $\boldsymbol{v_1, \dots, v_m \in \mathbf{F}_p^n}$

Output: linear dependence using coeffs in $\pm\boldsymbol{h}$

Fact. If $\boldsymbol{h = p/2}$, then $\boldsymbol{m = n + 1}$ suffices

Lemma (weight halving).
If $\boldsymbol{m = R}$ suffices for $\boldsymbol{h = B}$, then $\boldsymbol{m = R^2}$ suffices for $\boldsymbol{h = B/2}$

Theorem (Imran-Ivanyos'25).
Assume $\boldsymbol{k}$ is a power of two and

$$\boldsymbol{m \gg \cancel{p^{k\log k}} n^k}$$

Classical polytime algorithm for

$$\boldsymbol{h = \frac{p}{2k}}$$

Proof.
By induction on $\boldsymbol{k = 2^i}$

Base case is $\boldsymbol{i = 0}$ and $\boldsymbol{h = \frac{p}{2}}$

Then $\boldsymbol{m \geq n + 1}$ suffices

Since $\boldsymbol{m = (n+1)^k}$ suffices for $\boldsymbol{h = \frac{p}{2k}}$

$\boldsymbol{m = (n+1)^{2k}}$ suffices for $\boldsymbol{h = \frac{p}{4k}}$

The SIS^∞ problem

Input: $v_1, \ldots, v_m \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm h$

Fact. If $h = p/2$, then $m = n + 1$ suffices

Lemma (weight halving).
If $m = R$ suffices for $h = B$, then $m = R^2$ suffices for $h = B/2$

Theorem (Imran-Ivanyos'25).
Assume k is a power of two and

$$m \gg \cancel{p^{k \log k}} n^k$$

Classical polytime algorithm for

$$h = \frac{p}{2k}$$

Proof.
By induction on $k = 2^i$

Base case is $i = 0$ and $h = \frac{p}{2}$

Then $m \geq n + 1$ suffices

Since $m = (n+1)^k$ suffices for $h = \frac{p}{2k}$

$m = (n+1)^{2k}$ suffices for $h = \frac{p}{4k}$

The SIS$^\infty$ problem

Input: $\boldsymbol{v_1, \ldots, v_m \in \mathbf{F}_p^n}$

Output: linear dependence using coeffs in $\pm\boldsymbol{h}$

Dimension reduction and **exploring sparsity** also apply

Fact. If $\boldsymbol{h = p/2}$, then $\boldsymbol{m = n + 1}$ suffices

Lemma (weight halving).
If $\boldsymbol{m = R}$ suffices for $\boldsymbol{h = B}$, then $\boldsymbol{m = R^2}$ suffices for $\boldsymbol{h = B/2}$

Theorem (Imran-Ivanyos'25).
Assume $\boldsymbol{k}$ is a power of two and

$$\boldsymbol{m \gg \cancel{p^{k\log k}} n^k}$$

Classical polytime algorithm for

$$\boldsymbol{h = \frac{p}{2k}}$$

Proof.
By induction on $\boldsymbol{k = 2^i}$
Base case is $\boldsymbol{i = 0}$ and $\boldsymbol{h = \frac{p}{2}}$
Then $\boldsymbol{m \geq n + 1}$ suffices
Since $\boldsymbol{m = (n+1)^k}$ suffices for $\boldsymbol{h = \frac{p}{2k}}$
$\boldsymbol{m = (n+1)^{2k}}$ suffices for $\boldsymbol{h = \frac{p}{4k}}$

Lemma (weight halving).
If $\boldsymbol{m} = \boldsymbol{R}$ suffices for $\boldsymbol{h} = \boldsymbol{B}$,
then $\boldsymbol{m} = \boldsymbol{R}^2$ suffices for $\boldsymbol{h} = \boldsymbol{B}/2$

The SIS^∞ problem

Input: $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm\boldsymbol{h}$

Lemma (weight halving).
If $\boldsymbol{m} = \boldsymbol{R}$ suffices for $\boldsymbol{h} = \boldsymbol{B}$,
then $\boldsymbol{m} = \boldsymbol{R}^2$ suffices for $\boldsymbol{h} = \boldsymbol{B}/2$

The SIS^{∞} problem

Input: $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Partition $\boldsymbol{R}^2$ vectors into $\boldsymbol{R}$ batches of $\boldsymbol{R}$ vectors

Compute *reducible vector* $\boldsymbol{u}^{(i)}$ in each batch

Compute linear dependence of $\{\boldsymbol{u}^{(i)}\}$ and substitute back

Lemma (weight halving).
If $\boldsymbol{m} = \boldsymbol{R}$ suffices for $\boldsymbol{h} = \boldsymbol{B}$,
then $\boldsymbol{m} = \boldsymbol{R}^2$ suffices for $\boldsymbol{h} = \boldsymbol{B}/2$

The SIS^∞ problem

Input: $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm\boldsymbol{h}$

Partition $\boldsymbol{R}^2$ vectors into $\boldsymbol{R}$ batches of $\boldsymbol{R}$ vectors

Compute *reducible vector* $\boldsymbol{u}^{(i)}$ in each batch

Compute linear dependence of $\{\boldsymbol{u}^{(i)}\}$ and substitute back

Def (reducible vector).
$\boldsymbol{u}^{(i)}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}^{(i)}$ is a linear comb of vectors in batch $\boldsymbol{i}$
using coeffs in $\pm\boldsymbol{B}/2$

Lemma (weight halving).
If $m = R$ suffices for $h = B$,
then $m = R^2$ suffices for $h = B/2$

The SIS^{∞} problem

Input: $v_1, \ldots, v_m \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm h$

Partition R^2 vectors into R batches of R vectors

Compute *reducible vector* $u^{(i)}$ in each batch

Compute linear dependence of $\{u^{(i)}\}$ and substitute back

Def (reducible vector).
$u^{(i)}$ is reducible if for any $-B \leq c \leq B$,
$c \cdot u^{(i)}$ is a linear comb of vectors in batch i
using coeffs in $\pm B/2$

$$\beta_1 u^{(1)} + \cdots + \beta_R u^{(R)} = \vec{0}$$
where $-B \leq \beta_i \leq B$ not all-$\mathbf{0}$

Lemma (weight halving).
If $m = R$ suffices for $h = B$,
then $m = R^2$ suffices for $h = B/2$

The SIS^∞ problem

Input: $v_1, \ldots, v_m \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm h$

Partition R^2 vectors into R batches of R vectors

Compute *reducible vector* $u^{(i)}$ in each batch

Compute linear dependence of $\{u^{(i)}\}$ and substitute back

Def (reducible vector).
$u^{(i)}$ is reducible if for any $-B \leq c \leq B$,
$c \cdot u^{(i)}$ is a linear comb of vectors in batch i
using coeffs in $\pm B/2$

$$\beta_1 u^{(1)} + \cdots + \beta_R u^{(R)} = \vec{0}$$

where $-B \leq \beta_i \leq B$ not all-$\mathbf{0}$

Replace each $\beta_i u^{(i)}$ by reducibility

The SIS^∞ problem

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$

Output: linear dependence using coeffs in $\pm\boldsymbol{h}$

Def (reducible vector).
$\boldsymbol{u}^{(i)}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}^{(i)}$ is a linear comb of vectors in batch $\boldsymbol{i}$
using coeffs in $\pm\boldsymbol{B}/\boldsymbol{2}$

Partition $\boldsymbol{R}^2$ vectors into $\boldsymbol{R}$ batches of $\boldsymbol{R}$ vectors

Compute *reducible vector* $\boldsymbol{u}^{(i)}$ in each batch

The SIS^∞ problem

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm\boldsymbol{h}$

Def (reducible vector).
$\boldsymbol{u}^{(i)}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}^{(i)}$ is a linear comb of vectors in batch $\boldsymbol{i}$ using coeffs in $\pm\boldsymbol{B}/\mathbf{2}$

Partition $\boldsymbol{R}^2$ vectors into $\boldsymbol{R}$ batches of $\boldsymbol{R}$ vectors

Compute *reducible vector* $\boldsymbol{u}^{(i)}$ in each batch

$\boldsymbol{v}_1^{(i)}, \ldots, \boldsymbol{v}_R^{(i)}$ $\longrightarrow$ $\boldsymbol{c}_1\boldsymbol{v}_1^{(i)} + \cdots + \boldsymbol{c}_R\boldsymbol{v}_R^{(i)} = \vec{\mathbf{0}}$
where $-\boldsymbol{B} \leq \boldsymbol{c}_j \leq \boldsymbol{B}$ not all-$\mathbf{0}$

Since $\boldsymbol{m} = \boldsymbol{R}$ suffices for $\boldsymbol{h} = \boldsymbol{B}$

The SIS$^\infty$ problem

Input: $v_1, \dots, v_m \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm h$

Def (reducible vector).
$u^{(i)}$ is reducible if for any $-B \le c \le B$,
$c \cdot u^{(i)}$ is a linear comb of vectors in batch i using coeffs in $\pm B/2$

Partition R^2 vectors into R batches of R vectors

Compute *reducible vector* $u^{(i)}$ in each batch

$v_1^{(i)}, \dots, v_R^{(i)}$ $\rightarrow$ $c_1 v_1^{(i)} + \cdots + c_R v_R^{(i)} = \vec{0}$ where $-B \le c_j \le B$ not all-0

Since $m = R$ suffices for $h = B$

$\downarrow$

$1 \cdot T_1 + 2 \cdot T_2 + \cdots + B \cdot T_B = \vec{0}$

where $T_s = \sum_{j:c_j=s} v_j^{(i)} + \sum_{j:c_j=-s} -v_j^{(i)}$

The SIS^{∞} problem

Input: $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Def (reducible vector).
$\boldsymbol{u}^{(i)}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}^{(i)}$ is a linear comb of vectors in batch $\boldsymbol{i}$
using coeffs in $\pm \boldsymbol{B}/2$

Partition $\boldsymbol{R}^2$ vectors into $\boldsymbol{R}$ batches of $\boldsymbol{R}$ vectors

Compute *reducible vector* $\boldsymbol{u}^{(i)}$ in each batch

$$\mathbf{1} \cdot \boldsymbol{T}_1 + \mathbf{2} \cdot \boldsymbol{T}_2 + \cdots + \boldsymbol{B} \cdot \boldsymbol{T}_B = \vec{\mathbf{0}}$$

where $\boldsymbol{T}_s = \sum_{j:c_j=s} \boldsymbol{v}_j^{(i)} + \sum_{j:c_j=-s} -\boldsymbol{v}_j^{(i)}$

The SIS^∞ problem

Input: $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Def (reducible vector).
$\boldsymbol{u}^{(i)}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}^{(i)}$ is a linear comb of vectors in batch $\boldsymbol{i}$
using coeffs in $\pm \boldsymbol{B}/2$

Partition $\boldsymbol{R}^2$ vectors into $\boldsymbol{R}$ batches of $\boldsymbol{R}$ vectors

Compute *reducible vector* $\boldsymbol{u}^{(i)}$ in each batch

$$\mathbf{1} \cdot \boldsymbol{T}_1 + \mathbf{2} \cdot \boldsymbol{T}_2 + \cdots + \boldsymbol{B} \cdot \boldsymbol{T}_B = \vec{\mathbf{0}}$$

where $\boldsymbol{T}_s = \sum_{j: c_j = s} \boldsymbol{v}_j^{(i)} + \sum_{j: c_j = -s} -\boldsymbol{v}_j^{(i)}$

Define $\boldsymbol{u}^{(i)} = \boldsymbol{T}_{B/2} + \boldsymbol{T}_{B/2+1} + \cdots + \boldsymbol{T}_B$

The SIS$^\infty$ problem

Input: $\boldsymbol{v_1, \dots, v_m \in \mathbb{F}_p^n}$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Def (reducible vector).
$\boldsymbol{u^{(i)}}$ is reducible if for any $\boldsymbol{-B \le c \le B}$,
$\boldsymbol{c \cdot u^{(i)}}$ is a linear comb of vectors in batch $\boldsymbol{i}$ using coeffs in $\pm \boldsymbol{B/2}$

Partition $\boldsymbol{R^2}$ vectors into $\boldsymbol{R}$ batches of $\boldsymbol{R}$ vectors

Compute *reducible vector* $\boldsymbol{u^{(i)}}$ in each batch

$$\boldsymbol{1 \cdot T_1 + 2 \cdot T_2 + \cdots + B \cdot T_B = \vec{0}}$$

where $\boldsymbol{T_s = \sum_{j: c_j = s} v_j^{(i)} + \sum_{j: c_j = -s} -v_j^{(i)}}$

Define $\boldsymbol{u^{(i)} = T_{B/2} + T_{B/2+1} + \cdots + T_B}$

$$\boldsymbol{c \cdot u^{(i)}} \begin{cases} \boldsymbol{0 \le c \le B/2} \\ \\ \end{cases}$$

The SIS^{∞} problem

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm\boldsymbol{h}$

Def (reducible vector).
$\boldsymbol{u}^{(i)}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}^{(i)}$ is a linear comb of vectors in batch $\boldsymbol{i}$
using coeffs in $\pm\boldsymbol{B}/2$

Partition $\boldsymbol{R}^2$ vectors into $\boldsymbol{R}$ batches of $\boldsymbol{R}$ vectors

Compute *reducible vector* $\boldsymbol{u}^{(i)}$ in each batch

$$\mathbf{1} \cdot \boldsymbol{T}_1 + \mathbf{2} \cdot \boldsymbol{T}_2 + \cdots + \boldsymbol{B} \cdot \boldsymbol{T}_B = \vec{\mathbf{0}}$$

where $\boldsymbol{T}_s = \sum_{j:c_j=s} \boldsymbol{v}_j^{(i)} + \sum_{j:c_j=-s} -\boldsymbol{v}_j^{(i)}$

$$\text{Define } \boldsymbol{u}^{(i)} = \overbrace{\boldsymbol{T}_{B/2} + \boldsymbol{T}_{B/2+1} + \cdots + \boldsymbol{T}_B}^{\text{Coeffs } \pm 1}$$

$$\boldsymbol{c} \cdot \boldsymbol{u}^{(i)} \begin{cases} \mathbf{0} \leq \boldsymbol{c} \leq \boldsymbol{B}/2 \\ \end{cases}$$

has coeffs $\pm\boldsymbol{c} \subseteq \pm\boldsymbol{B}/2$

The SIS$^\infty$ problem

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Def (reducible vector).
$\boldsymbol{u}^{(i)}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}^{(i)}$ is a linear comb of vectors in batch $\boldsymbol{i}$ using coeffs in $\pm \boldsymbol{B}/2$

Partition $\boldsymbol{R}^2$ vectors into $\boldsymbol{R}$ batches of $\boldsymbol{R}$ vectors

Compute *reducible vector* $\boldsymbol{u}^{(i)}$ in each batch

$$\mathbf{1} \cdot \boldsymbol{T}_1 + \mathbf{2} \cdot \boldsymbol{T}_2 + \cdots + \boldsymbol{B} \cdot \boldsymbol{T}_B = \vec{\mathbf{0}}$$

where $\boldsymbol{T}_s = \sum_{j:c_j=s} \boldsymbol{v}_j^{(i)} + \sum_{j:c_j=-s} -\boldsymbol{v}_j^{(i)}$

Define $\boldsymbol{u}^{(i)} = \boldsymbol{T}_{B/2} + \boldsymbol{T}_{B/2+1} + \cdots + \boldsymbol{T}_B$

$$\boldsymbol{c} \cdot \boldsymbol{u}^{(i)} \begin{cases} \mathbf{0} \leq \boldsymbol{c} \leq \boldsymbol{B}/\mathbf{2} & \checkmark \\ \boldsymbol{B}/\mathbf{2} < \boldsymbol{c} \leq \boldsymbol{B} & \end{cases}$$

Def (reducible vector).
$\boldsymbol{u}^{(i)}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}^{(i)}$ is a linear comb of vectors in batch $\boldsymbol{i}$ using coeffs in $\pm \boldsymbol{B}/2$

The SIS$^{\infty}$ problem

Input: $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Partition $\boldsymbol{R}^2$ vectors into $\boldsymbol{R}$ batches of $\boldsymbol{R}$ vectors

Compute *reducible vector* $\boldsymbol{u}^{(i)}$ in each batch

$$\mathbf{1} \cdot \boldsymbol{T}_1 + \mathbf{2} \cdot \boldsymbol{T}_2 + \cdots + \boldsymbol{B} \cdot \boldsymbol{T}_B = \vec{\mathbf{0}}$$

where $\boldsymbol{T}_s = \sum_{j:c_j=s} \boldsymbol{v}_j^{(i)} + \sum_{j:c_j=-s} -\boldsymbol{v}_j^{(i)}$

Define $\boldsymbol{u}^{(i)} = \boldsymbol{T}_{B/2} + \boldsymbol{T}_{B/2+1} + \cdots + \boldsymbol{T}_B$

$$\boldsymbol{c} \cdot \boldsymbol{u}^{(i)} \begin{cases} \mathbf{0} \leq \boldsymbol{c} \leq \boldsymbol{B}/2 & \checkmark \\ \boldsymbol{B}/2 < \boldsymbol{c} \leq \boldsymbol{B} \end{cases}$$

$$= \boldsymbol{c} \cdot \boldsymbol{u}^{(i)} - (\mathbf{1} \cdot \boldsymbol{T}_1 + \mathbf{2} \cdot \boldsymbol{T}_2 + \cdots + \boldsymbol{B} \cdot \boldsymbol{T}_B)$$

The SIS$^{\infty}$ problem

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Def (reducible vector).
$\boldsymbol{u}^{(i)}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}^{(i)}$ is a linear comb of vectors in batch $\boldsymbol{i}$
using coeffs in $\pm \boldsymbol{B}/2$

Partition $\boldsymbol{R}^2$ vectors into $\boldsymbol{R}$ batches of $\boldsymbol{R}$ vectors

Compute *reducible vector* $\boldsymbol{u}^{(i)}$ in each batch

$$1 \cdot T_1 + 2 \cdot T_2 + \cdots + B \cdot T_B = \vec{0}$$

where $T_s = \sum_{j:c_j=s} v_j^{(i)} + \sum_{j:c_j=-s} -v_j^{(i)}$

Define $\boldsymbol{u}^{(i)} = T_{B/2} + T_{B/2+1} + \cdots + T_B$

$$c \cdot u^{(i)} \begin{cases} 0 \leq c \leq B/2 & \checkmark \\ B/2 < c \leq B \end{cases}$$

$$= c \cdot u^{(i)} - (1 \cdot T_1 + 2 \cdot T_2 + \cdots + B \cdot T_B)$$
$$= \sum_{s<B/2} (-s) \cdot T_s + \sum_{s \geq B/2} (c-s) \cdot T_s$$

The SIS^∞ problem

Input: $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in \mathbb{F}_p^n$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Def (reducible vector).
$\boldsymbol{u}^{(i)}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}^{(i)}$ is a linear comb of vectors in batch $\boldsymbol{i}$
using coeffs in $\pm \boldsymbol{B}/2$

Partition $\boldsymbol{R}^2$ vectors into $\boldsymbol{R}$ batches of $\boldsymbol{R}$ vectors

Compute *reducible vector* $\boldsymbol{u}^{(i)}$ in each batch

$$1 \cdot \boldsymbol{T}_1 + 2 \cdot \boldsymbol{T}_2 + \cdots + \boldsymbol{B} \cdot \boldsymbol{T}_{\boldsymbol{B}} = \vec{0}$$

where $\boldsymbol{T}_s = \sum_{j: c_j = s} \boldsymbol{v}_j^{(i)} + \sum_{j: c_j = -s} -\boldsymbol{v}_j^{(i)}$

Define $\boldsymbol{u}^{(i)} = \boldsymbol{T}_{B/2} + \boldsymbol{T}_{B/2+1} + \cdots + \boldsymbol{T}_B$

$$\boldsymbol{c} \cdot \boldsymbol{u}^{(i)} \begin{cases} 0 \le \boldsymbol{c} \le \boldsymbol{B}/2 & ✓ \\ \boldsymbol{B}/2 < \boldsymbol{c} \le \boldsymbol{B} \end{cases}$$

$$= \boldsymbol{c} \cdot \boldsymbol{u}^{(i)} - (1 \cdot \boldsymbol{T}_1 + 2 \cdot \boldsymbol{T}_2 + \cdots + \boldsymbol{B} \cdot \boldsymbol{T}_B)$$

$$= \sum_{s < B/2} (-s) \cdot \boldsymbol{T}_s + \sum_{s \ge B/2} (\boldsymbol{c} - s) \cdot \boldsymbol{T}_s$$

has coeffs $\pm \boldsymbol{B}/2$

since $\boldsymbol{s} \le \boldsymbol{B}/2$ and $|\boldsymbol{c} - \boldsymbol{s}| \le \boldsymbol{B}/2$

and $\boldsymbol{T}_s$ has coeff ± 1

The SIS$^\infty$ problem

Input: $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Def (reducible vector).
$\boldsymbol{u}^{(i)}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}^{(i)}$ is a linear comb of vectors in batch $\boldsymbol{i}$
using coeffs in $\pm \boldsymbol{B}/2$

Partition $\boldsymbol{R}^2$ vectors into $\boldsymbol{R}$ batches of $\boldsymbol{R}$ vectors

Compute *reducible vector* $\boldsymbol{u}^{(i)}$ in each batch

$$\mathbf{1} \cdot \boldsymbol{T}_1 + \mathbf{2} \cdot \boldsymbol{T}_2 + \cdots + \boldsymbol{B} \cdot \boldsymbol{T}_B = \vec{\mathbf{0}}$$

where $\boldsymbol{T}_s = \sum_{j: c_j = s} \boldsymbol{v}_j^{(i)} + \sum_{j: c_j = -s} -\boldsymbol{v}_j^{(i)}$

Define $\boldsymbol{u}^{(i)} = \boldsymbol{T}_{B/2} + \boldsymbol{T}_{B/2+1} + \cdots + \boldsymbol{T}_B$

$$\boldsymbol{c} \cdot \boldsymbol{u}^{(i)} \begin{cases} \mathbf{0} \le \boldsymbol{c} \le \boldsymbol{B}/\mathbf{2} & \checkmark \\ \boldsymbol{B}/\mathbf{2} < \boldsymbol{c} \le \boldsymbol{B} & \checkmark \end{cases}$$

The SIS$^\infty$ problem

Input: $v_1, \dots, v_m \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm h$

Def (reducible vector).
$u^{(i)}$ is reducible if for any $-B \le c \le B$,
$c \cdot u^{(i)}$ is a linear comb of vectors in batch i
using coeffs in $\pm B/2$

Partition R^2 vectors into R batches of R vectors

Compute *reducible vector* $u^{(i)}$ in each batch

$$1 \cdot T_1 + 2 \cdot T_2 + \cdots + B \cdot T_B = \vec{0}$$

where $T_s = \sum_{j:c_j=s} v_j^{(i)} + \sum_{j:c_j=-s} -v_j^{(i)}$

Define $u^{(i)} = T_{B/2} + T_{B/2+1} + \cdots + T_B$

$$c \cdot u^{(i)} \begin{cases} 0 \le |c| \le B/2 & \checkmark \\ B/2 < |c| \le B & \checkmark \end{cases}$$

The SIS$^\infty$ problem

Input: $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Def (reducible vector).
$\boldsymbol{u}^{(i)}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}^{(i)}$ is a linear comb of vectors in batch $\boldsymbol{i}$ using coeffs in $\pm \boldsymbol{B}/2$

Partition $\boldsymbol{R}^2$ vectors into $\boldsymbol{R}$ batches of $\boldsymbol{R}$ vectors

Compute *reducible vector* $\boldsymbol{u}^{(i)}$ in each batch

$$\mathbf{1} \cdot \boldsymbol{T}_1 + \mathbf{2} \cdot \boldsymbol{T}_2 + \cdots + \boldsymbol{B} \cdot \boldsymbol{T}_B = \vec{\mathbf{0}}$$

where $\boldsymbol{T}_s = \sum_{j: c_j = s} \boldsymbol{v}_j^{(i)} + \sum_{j: c_j = -s} -\boldsymbol{v}_j^{(i)}$

Define $\boldsymbol{u}^{(i)} = \boldsymbol{T}_{B/2} + \boldsymbol{T}_{B/2+1} + \cdots + \boldsymbol{T}_B$

$$\boldsymbol{c} \cdot \boldsymbol{u}^{(i)} \begin{cases} \mathbf{0} \leq |\boldsymbol{c}| \leq \boldsymbol{B}/2 & \checkmark \\ \boldsymbol{B}/2 < |\boldsymbol{c}| \leq \boldsymbol{B} & \checkmark \end{cases}$$

$\boldsymbol{u}^{(i)}$ is reducible

The SIS$^\infty$ problem

Input: $v_1, \dots, v_m \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm h$

Def (reducible vector).
$u^{(i)}$ is reducible if for any $-B \leq c \leq B$,
$c \cdot u^{(i)}$ is a linear comb of vectors in batch i
using coeffs in $\pm B/2$

Partition R^2 vectors into R batches of R vectors

Compute *reducible vector* $u^{(i)}$ in each batch

$$1 \cdot T_1 + 2 \cdot T_2 + \cdots + B \cdot T_B = \vec{0}$$

where $T_s = \sum_{j:c_j=s} v_j^{(i)} + \sum_{j:c_j=-s} -v_j^{(i)}$

Define $u^{(i)} = T_{B/2} + T_{B/2+1} + \cdots + T_B$

What if $T_{B/2} + T_{B/2+1} + \cdots + T_B$ is an empty sum?

The SIS$^\infty$ problem

Input: $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Def (reducible vector).
$\boldsymbol{u}^{(i)}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}^{(i)}$ is a linear comb of vectors in batch $\boldsymbol{i}$
using coeffs in $\pm \boldsymbol{B}/2$

Partition $\boldsymbol{R}^2$ vectors into $\boldsymbol{R}$ batches of $\boldsymbol{R}$ vectors

Compute *reducible vector* $\boldsymbol{u}^{(i)}$ in each batch

$$1 \cdot \boldsymbol{T}_1 + 2 \cdot \boldsymbol{T}_2 + \cdots + \boldsymbol{B} \cdot \boldsymbol{T}_B = \vec{\mathbf{0}}$$

where $\boldsymbol{T}_s = \sum_{j:c_j=s} \boldsymbol{v}_j^{(i)} + \sum_{j:c_j=-s} -\boldsymbol{v}_j^{(i)}$

Define $\boldsymbol{u}^{(i)} = \boldsymbol{T}_{B/2} + \boldsymbol{T}_{B/2+1} + \cdots + \boldsymbol{T}_B$

What if $\boldsymbol{T}_{B/2} + \boldsymbol{T}_{B/2+1} + \cdots + \boldsymbol{T}_B$ is an empty sum?

$$\boldsymbol{c}_1 \boldsymbol{v}_1^{(i)} + \cdots + \boldsymbol{c}_R \boldsymbol{v}_R^{(i)} = \vec{\mathbf{0}}$$

where $-\boldsymbol{B}/2 \leq \boldsymbol{c}_j \leq \boldsymbol{B}/2$ not all-$\mathbf{0}$

The SIS$^\infty$ problem

Input: $v_1, \dots, v_m \in \mathbb{F}_p^n$

Output: linear dependence using coeffs in $\pm h$

Def (reducible vector).
$u^{(i)}$ is reducible if for any $-B \le c \le B$,
$c \cdot u^{(i)}$ is a linear comb of vectors in batch i
using coeffs in $\pm B/2$

Partition R^2 vectors into R batches of R vectors

Compute *reducible vector* $u^{(i)}$ in each batch

$$1 \cdot T_1 + 2 \cdot T_2 + \cdots + B \cdot T_B = \vec{0}$$

where $T_s = \sum_{j:c_j=s} v_j^{(i)} + \sum_{j:c_j=-s} -v_j^{(i)}$

Define $u^{(i)} = T_{B/2} + T_{B/2+1} + \cdots + T_B$

What if $T_{B/2} + T_{B/2+1} + \cdots + T_B$ is an empty sum?

$$c_1 v_1^{(i)} + \cdots + c_R v_R^{(i)} = \vec{0}$$

where $-B/2 \le c_j \le B/2$ not all-$\mathbf{0}$

Let $c_j \leftarrow 2c_j$ and try again

The SIS^∞ problem

Input: $\boldsymbol{v_1}, \dots, \boldsymbol{v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$

Output: linear dependence using coeffs in $\pm\boldsymbol{h}$

Lemma (weight halving).
If $\boldsymbol{m} = \boldsymbol{R}$ suffices for $\boldsymbol{h} = \boldsymbol{B}$, then $\boldsymbol{m} = \boldsymbol{R}^2$ suffices for $\boldsymbol{h} = \boldsymbol{B}/2$

The SIS^{∞} problem

Input: $\boldsymbol{v_1, \dots, v_m} \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Lemma (weight halving).
If $\boldsymbol{m} = \boldsymbol{R}$ suffices for $\boldsymbol{h} = \boldsymbol{B}$, then $\boldsymbol{m} = \boldsymbol{R}^2$ suffices for $\boldsymbol{h} = \boldsymbol{B}/2$

Lemma (iterative halving).
If $\boldsymbol{m} = \boldsymbol{R}$ suffices for $\boldsymbol{h} = \boldsymbol{B}$, then $\boldsymbol{m} = \boldsymbol{R}^{2^t}$ suffices for $\boldsymbol{h} = \boldsymbol{B}/2^t$

The SIS$^\infty$ problem

Input: $\boldsymbol{v_1}, \dots, \boldsymbol{v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Lemma (weight halving).
If $\boldsymbol{m} = \boldsymbol{R}$ suffices for $\boldsymbol{h} = \boldsymbol{B}$, then $\boldsymbol{m} = \boldsymbol{R}^2$ suffices for $\boldsymbol{h} = \boldsymbol{B}/2$

Lemma (iterative halving).
If $\boldsymbol{m} = \boldsymbol{R}$ suffices for $\boldsymbol{h} = \boldsymbol{B}$, then $\boldsymbol{m} = \boldsymbol{R}^{2^t}$ suffices for $\boldsymbol{h} = \boldsymbol{B}/2^t$

How about dividing $\mathbf{3}$?

Do we have to pay $\boldsymbol{m} = \boldsymbol{R}^4$ and get the stronger $\boldsymbol{h} = \boldsymbol{B}/4$?

The SIS^{∞} problem

Lemma (weight trisecting).
If $\boldsymbol{m} = \boldsymbol{R}$ suffices for $\boldsymbol{h} = \boldsymbol{B}$,
then $\boldsymbol{m} = \boldsymbol{R^3}$ suffices for $\boldsymbol{h} = \boldsymbol{B/3}$

Input: $\boldsymbol{v_1, \dots, v_m \in \mathbf{F}_p^n}$

Output: linear dependence using coeffs in $\pm\boldsymbol{h}$

Lemma (weight trisecting).
If $m = R$ suffices for $h = B$,
then $m = R^3$ suffices for $h = B/3$

The SIS^∞ problem

Input: $v_1, \dots, v_m \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm h$

Partition R^3 vectors into R batches of R^2 vectors

Compute *reducible vector* $u^{(i)}$ in each batch

Compute linear dependence of $\{u^{(i)}\}$ and substitute back

The SIS$^\infty$ problem

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_p^n$

Output: linear dependence using coeffs in $\pm \boldsymbol{h}$

Lemma (weight trisecting).
If $\boldsymbol{m = R}$ suffices for $\boldsymbol{h = B}$,
then $\boldsymbol{m = R^3}$ suffices for $\boldsymbol{h = B/3}$

Partition $\boldsymbol{R^3}$ vectors into $\boldsymbol{R}$ batches of $\boldsymbol{R^2}$ vectors

Compute *reducible vector* $\boldsymbol{u^{(i)}}$ in each batch

Compute linear dependence of $\left\{\boldsymbol{u^{(i)}}\right\}$ and substitute back

Def (reducible vector).
$\boldsymbol{u^{(i)}}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u^{(i)}}$ is a linear comb of vectors in batch $\boldsymbol{i}$
using coeffs in $\pm \boldsymbol{B/3}$

$$\boldsymbol{\beta_1 u^{(1)}} + \cdots + \boldsymbol{\beta_R u^{(R)}} = \vec{\mathbf{0}}$$

where $-\boldsymbol{B} \leq \boldsymbol{\beta_i} \leq \boldsymbol{B}$ not all-$\mathbf{0}$

Replace each $\boldsymbol{\beta_i u^{(i)}}$ by reducibility

The SIS^{∞} problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm\boldsymbol{B}/\mathbf{3}$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_{\mathbf{1}}, \ldots, \boldsymbol{v}_{R^2}$

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors
using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{\boldsymbol{R}^2}$

$\boldsymbol{v}_1, \dots, \boldsymbol{v}_{\boldsymbol{R}}$ $\Rightarrow$ $\boldsymbol{c}_1 \boldsymbol{v}_1 + \cdots + \boldsymbol{c}_R \boldsymbol{v}_R = \vec{\boldsymbol{0}}$
where $-\boldsymbol{B} \le \boldsymbol{c}_j \le \boldsymbol{B}$ not all-$\boldsymbol{0}$

Since $\boldsymbol{m} = \boldsymbol{R}$ suffices for $\boldsymbol{h} = \boldsymbol{B}$

$\Downarrow$

$\boldsymbol{1} \cdot \boldsymbol{T}_1 + \boldsymbol{2} \cdot \boldsymbol{T}_2 + \cdots + \boldsymbol{B} \cdot \boldsymbol{T}_B = \vec{\boldsymbol{0}}$
where $\boldsymbol{T}_s = \sum_{j:c_j=s} \boldsymbol{v}_j + \sum_{j:c_j=-s} -\boldsymbol{v}_j$

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/\mathbf{3}$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{\boldsymbol{R}^2}$

$\boldsymbol{v}_1, \dots, \boldsymbol{v}_{\boldsymbol{R}}$

$\boldsymbol{c}_1\boldsymbol{v}_1 + \cdots + \boldsymbol{c}_R\boldsymbol{v}_R = \vec{\mathbf{0}}$
where $-\boldsymbol{B} \leq \boldsymbol{c}_j \leq \boldsymbol{B}$ not all-$\mathbf{0}$

Since $\boldsymbol{m} = \boldsymbol{R}$ suffices for $\boldsymbol{h} = \boldsymbol{B}$

$\mathbf{1} \cdot \boldsymbol{T}_1 + \mathbf{2} \cdot \boldsymbol{T}_2 + \cdots + \boldsymbol{B} \cdot \boldsymbol{T}_{\boldsymbol{B}} = \vec{\mathbf{0}}$
where $\boldsymbol{T}_s = \sum_{j:c_j = s} \boldsymbol{v}_j + \sum_{j:c_j=-s} -\boldsymbol{v}_j$

$$\begin{aligned}\vec{\mathbf{0}} \quad &= \textstyle\sum_{s<B/3} s \cdot T_s \\ &+ \textstyle\sum_{B/3 \leq s < 2B/3} s \cdot T_s \\ &+ \textstyle\sum_{s \geq 2B/3} s \cdot T_s\end{aligned}$$

The SIS^{∞} problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\vec{\mathbf{0}} \quad = \sum_{s<B/3} \boldsymbol{s} \cdot \boldsymbol{T}_s + \sum_{B/3 \leq s < 2B/3} \boldsymbol{s} \cdot \boldsymbol{T}_s + \sum_{s \geq 2B/3} \boldsymbol{s} \cdot \boldsymbol{T}_s$$

Each $\boldsymbol{T}_s$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1 \dots, \boldsymbol{v}_R$

The SIS^∞ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{\boldsymbol{R}^2}$

$$\vec{\mathbf{0}} \quad = \sum_{s<B/3} s \cdot T_s + \sum_{B/3 \le s < 2B/3} s \cdot T_s + \sum_{s \ge 2B/3} s \cdot T_s$$

Each $\boldsymbol{T}_s$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1 \dots, \boldsymbol{v}_{\boldsymbol{R}}$

$$\boldsymbol{x} = \begin{bmatrix} \sum_{s<B/3} T_s \\ \sum_{B/3 \le s < 2B/3} T_s \\ \sum_{s \ge 2B/3} T_s \end{bmatrix}$$

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\vec{0} = \sum_{s<B/3} s \cdot T_s + \sum_{B/3 \le s < 2B/3} s \cdot T_s + \sum_{s \ge 2B/3} s \cdot T_s$$

Each $\boldsymbol{T}_s$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1 \ldots, \boldsymbol{v}_R$

$$\boldsymbol{x} = \begin{bmatrix} \sum_{s<B/3} T_s \\ \sum_{B/3 \le s < 2B/3} T_s \\ \sum_{s \ge 2B/3} T_s \end{bmatrix} \begin{array}{l} \textbf{Small} \\ \textbf{Median} \\ \textbf{Large} \end{array}$$

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/\boldsymbol{3}$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\vec{\mathbf{0}} = \sum_{s<B/3} s \cdot T_s + \sum_{B/3 \leq s < 2B/3} s \cdot T_s + \sum_{s \geq 2B/3} s \cdot T_s$$

Each $\boldsymbol{T}_s$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1 \ldots, \boldsymbol{v}_R$

$$\boldsymbol{x} = \begin{bmatrix} \sum_{s<B/3} T_s \\ \sum_{B/3 \leq s < 2B/3} T_s \\ \sum_{s \geq 2B/3} T_s \end{bmatrix} \begin{matrix} \text{Small} \\ \text{Median} \\ \text{Large} \end{matrix}$$

$\boldsymbol{x}$ is a vector in $\mathbf{F}_p^{3n}$

The SIS^∞ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\vec{0} \quad = \sum_{s<B/3} s \cdot T_s + \sum_{B/3 \le s < 2B/3} s \cdot T_s + \sum_{s \ge 2B/3} s \cdot T_s$$

Each $\boldsymbol{T}_s$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1 \dots, \boldsymbol{v}_R$

$$x = \begin{bmatrix} \sum_{s<B/3} T_s \\ \sum_{B/3 \le s < 2B/3} T_s \\ \sum_{s \ge 2B/3} T_s \end{bmatrix} \begin{array}{l} \text{Small} \\ \text{Median} \\ \text{Large} \end{array}$$

$\boldsymbol{x}$ is a vector in $\mathbf{F}_p^{3n}$

Expand $\boldsymbol{x}$ in terms of $\pm \boldsymbol{v}_1 \dots, \pm \boldsymbol{v}_R$

The SIS^∞ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm\boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\vec{0} = \sum_{s<B/3} s \cdot T_s + \sum_{B/3 \le s < 2B/3} s \cdot T_s + \sum_{s \ge 2B/3} s \cdot T_s$$

Each T_s is a disjoint signed-subset-sum of $\boldsymbol{v}_1 \ldots, \boldsymbol{v}_R$

$$\boldsymbol{x} = \begin{bmatrix} \sum_{s<B/3} T_s \\ \sum_{B/3 \le s < 2B/3} T_s \\ \sum_{s \ge 2B/3} T_s \end{bmatrix} \begin{array}{l} \text{Small} \\ \text{Median} \\ \text{Large} \end{array}$$

$\boldsymbol{x}$ is a vector in $\mathbf{F}_p^{3n}$

Expand $\boldsymbol{x}$ in terms of $\pm\boldsymbol{v}_1 \ldots, \pm\boldsymbol{v}_R$ and combine

- **Small** ones with **small** coeffs $\mathbf{0} \sim \boldsymbol{B}/3$
- **Median** ones with **median** coeffs $\boldsymbol{B}/3 \sim 2\boldsymbol{B}/3$
- **Large** ones with **large** coeffs $2\boldsymbol{B}/3 \sim \boldsymbol{B}$

We obtain $\vec{\mathbf{0}}$

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm\boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$\boldsymbol{v}_1, \ldots, \boldsymbol{v}_R$

$$\boldsymbol{x} = \begin{bmatrix} \boldsymbol{x}_{\text{Small}} \\ \boldsymbol{x}_{\text{Median}} \\ \boldsymbol{x}_{\text{Large}} \end{bmatrix}$$

$\boldsymbol{x}_{\text{Small}}, \boldsymbol{x}_{\text{Median}}, \boldsymbol{x}_{\text{Large}}$ are disjoint signed-subset-sums

Expand in terms of $\pm\boldsymbol{v}_1 \ldots, \pm\boldsymbol{v}_R$ and combine

- $\boldsymbol{x}_{\text{Small}}$ ones with **small** coeffs $\mathbf{0} \sim \boldsymbol{B}/\mathbf{3}$
- $\boldsymbol{x}_{\text{Median}}$ ones with **median** coeffs $\boldsymbol{B}/\mathbf{3} \sim \mathbf{2}\boldsymbol{B}/\mathbf{3}$
- $\boldsymbol{x}_{\text{Large}}$ ones with **large** coeffs $\mathbf{2}\boldsymbol{B}/\mathbf{3} \sim \boldsymbol{B}$

We obtain $\vec{\mathbf{0}}$

The SIS^{∞} problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\begin{array}{cccc} \boldsymbol{v}_1^{(1)}, \ldots, \boldsymbol{v}_R^{(1)} & \boldsymbol{v}_1^{(2)}, \ldots, \boldsymbol{v}_R^{(2)} & \cdots\cdots & \boldsymbol{v}_1^{(R)}, \ldots, \boldsymbol{v}_R^{(R)} \\ \downarrow & \downarrow & & \downarrow \\ \boldsymbol{x}^{(1)} & \boldsymbol{x}^{(2)} & & \boldsymbol{x}^{(R)} \end{array}$$

The SIS^∞ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/\boldsymbol{3}$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\boldsymbol{v}_1^{(1)}, \dots, \boldsymbol{v}_R^{(1)} \qquad \boldsymbol{v}_1^{(2)}, \dots, \boldsymbol{v}_R^{(2)} \qquad \cdots\cdots \qquad \boldsymbol{v}_1^{(R)}, \dots, \boldsymbol{v}_R^{(R)}$$

$$\downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow$$

$$\underbrace{\boldsymbol{x}^{(1)} \qquad \boldsymbol{x}^{(2)} \qquad \boldsymbol{x}^{(R)}}$$

$$\boldsymbol{c}_1 \boldsymbol{x}^{(1)} + \cdots + \boldsymbol{c}_R \boldsymbol{x}^{(R)} = \vec{\boldsymbol{0}}$$

where $-\boldsymbol{B} \le \boldsymbol{c}_j \le \boldsymbol{B}$ not all-$\boldsymbol{0}$

Linear dependence of
$\boldsymbol{R}$ vectors using coeffs $\pm \boldsymbol{B}$

The SIS^{∞} problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm\boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{\boldsymbol{R}^2}$

$$\boldsymbol{c}_1 \boldsymbol{x}^{(1)} + \cdots + \boldsymbol{c}_R \boldsymbol{x}^{(R)} = \vec{\mathbf{0}}$$

where $-\boldsymbol{B} \leq \boldsymbol{c}_j \leq \boldsymbol{B}$ not all-$\mathbf{0}$

The SIS^{∞} problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm\boldsymbol{B}/\boldsymbol{3}$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_{\boldsymbol{1}}, \dots, \boldsymbol{v}_{\boldsymbol{R}^{\boldsymbol{2}}}$

$$\mathbf{1} \cdot \boldsymbol{x}^{(\mathbf{1})} - (\boldsymbol{B}/\mathbf{4}) \cdot \boldsymbol{x}^{(\mathbf{2})} + (\boldsymbol{B}/\mathbf{2}) \cdot \boldsymbol{x}^{(\mathbf{4})} + (\mathbf{5}\boldsymbol{B}/\mathbf{6}) \cdot \boldsymbol{x}^{(\mathbf{7})} = \vec{\mathbf{0}}$$

The SIS^{∞} problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm\boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\underbrace{\mathbf{1} \cdot \boldsymbol{x}^{(1)} - (\boldsymbol{B}/4) \cdot \boldsymbol{x}^{(2)}}_{\substack{\textbf{Small}\text{ coeffs} \\ \mathbf{0} \sim \boldsymbol{B}/3}} + \underbrace{(\boldsymbol{B}/2) \cdot \boldsymbol{x}^{(4)}}_{\substack{\textbf{Median}\text{ coeffs} \\ \boldsymbol{B}/3 \sim 2\boldsymbol{B}/3}} + \underbrace{(5\boldsymbol{B}/6) \cdot \boldsymbol{x}^{(7)}}_{\substack{\textbf{Large}\text{ coeffs} \\ 2\boldsymbol{B}/3 \sim \boldsymbol{B}}} = \vec{\mathbf{0}}$$

The SIS^{∞} problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\underbrace{\mathbf{1} \cdot \boldsymbol{x}^{(1)} - (\boldsymbol{B}/4) \cdot \boldsymbol{x}^{(2)}}_{\substack{\text{Small coeffs} \\ 0 \sim B/3}} + \underbrace{(\boldsymbol{B}/2) \cdot \boldsymbol{x}^{(4)}}_{\substack{\text{Median coeffs} \\ B/3 \sim 2B/3}} + \underbrace{(5\boldsymbol{B}/6) \cdot \boldsymbol{x}^{(7)}}_{\substack{\text{Large coeffs} \\ 2B/3 \sim B}} = \vec{\mathbf{0}}$$

$$\boldsymbol{x} = \begin{bmatrix} \boldsymbol{x}_{\text{Small}} \\ \boldsymbol{x}_{\text{Median}} \\ \boldsymbol{x}_{\text{Large}} \end{bmatrix}$$

The SIS^{∞} problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\underbrace{\mathbf{1} \cdot \boldsymbol{x}^{(1)} - (\boldsymbol{B}/4) \cdot \boldsymbol{x}^{(2)}}_{\substack{\textbf{Small coeffs} \\ 0 \sim B/3}} + \underbrace{(\boldsymbol{B}/2) \cdot \boldsymbol{x}^{(4)}}_{\substack{\textbf{Median coeffs} \\ B/3 \sim 2B/3}} + \underbrace{(5\boldsymbol{B}/6) \cdot \boldsymbol{x}^{(7)}}_{\substack{\textbf{Large coeffs} \\ 2B/3 \sim B}} = \vec{\mathbf{0}}$$

$$\boldsymbol{x} = \begin{bmatrix} \boldsymbol{x}_{\mathrm{Small}} \\ \boldsymbol{x}_{\mathrm{Median}} \\ \boldsymbol{x}_{\mathrm{Large}} \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{x}^{(1)}_{\mathrm{Small}} - \boldsymbol{x}^{(2)}_{\mathrm{Small}} & \boldsymbol{x}^{(4)}_{\mathrm{Small}} & \boldsymbol{x}^{(7)}_{\mathrm{Small}} \\ \boldsymbol{x}^{(1)}_{\mathrm{Median}} - \boldsymbol{x}^{(2)}_{\mathrm{Median}} & \boldsymbol{x}^{(4)}_{\mathrm{Median}} & \boldsymbol{x}^{(7)}_{\mathrm{Median}} \\ \boldsymbol{x}^{(1)}_{\mathrm{Large}} - \boldsymbol{x}^{(2)}_{\mathrm{Large}} & \boldsymbol{x}^{(4)}_{\mathrm{Large}} & \boldsymbol{x}^{(7)}_{\mathrm{Large}} \end{bmatrix}$$

The SIS^∞ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/\boldsymbol{3}$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\boldsymbol{M} = \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \begin{bmatrix} \boldsymbol{x}^{(1)}_{\mathbf{Small}} - \boldsymbol{x}^{(2)}_{\mathbf{Small}} & \boldsymbol{x}^{(4)}_{\mathbf{Small}} & \boldsymbol{x}^{(7)}_{\mathbf{Small}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Median}} - \boldsymbol{x}^{(2)}_{\mathbf{Median}} & \boldsymbol{x}^{(4)}_{\mathbf{Median}} & \boldsymbol{x}^{(7)}_{\mathbf{Median}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Large}} - \boldsymbol{x}^{(2)}_{\mathbf{Large}} & \boldsymbol{x}^{(4)}_{\mathbf{Large}} & \boldsymbol{x}^{(7)}_{\mathbf{Large}} \end{bmatrix}$$

The SIS^{∞} problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/\mathbf{3}$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\boldsymbol{M} = \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \begin{bmatrix} \boldsymbol{x}^{(1)}_{\mathbf{Small}} - \boldsymbol{x}^{(2)}_{\mathbf{Small}} & \boldsymbol{x}^{(4)}_{\mathbf{Small}} & \boldsymbol{x}^{(7)}_{\mathbf{Small}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Median}} - \boldsymbol{x}^{(2)}_{\mathbf{Median}} & \boldsymbol{x}^{(4)}_{\mathbf{Median}} & \boldsymbol{x}^{(7)}_{\mathbf{Median}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Large}} - \boldsymbol{x}^{(2)}_{\mathbf{Large}} & \boldsymbol{x}^{(4)}_{\mathbf{Large}} & \boldsymbol{x}^{(7)}_{\mathbf{Large}} \end{bmatrix}$$

Observation.
Every entry of $\boldsymbol{M}$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

The SIS^{∞} problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors
using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\boldsymbol{M} = \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \begin{bmatrix} \boldsymbol{x}^{(1)}_{\mathbf{Small}} - \boldsymbol{x}^{(2)}_{\mathbf{Small}} & \boldsymbol{x}^{(4)}_{\mathbf{Small}} & \boldsymbol{x}^{(7)}_{\mathbf{Small}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Median}} - \boldsymbol{x}^{(2)}_{\mathbf{Median}} & \boldsymbol{x}^{(4)}_{\mathbf{Median}} & \boldsymbol{x}^{(7)}_{\mathbf{Median}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Large}} - \boldsymbol{x}^{(2)}_{\mathbf{Large}} & \boldsymbol{x}^{(4)}_{\mathbf{Large}} & \boldsymbol{x}^{(7)}_{\mathbf{Large}} \end{bmatrix}$$

Observation.
Every entry of $\boldsymbol{M}$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$
Every *row* of $\boldsymbol{M}$ sums to $\vec{\mathbf{0}}$ with proper **small**, **median**, **large** weights

The SIS^{∞} problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors
using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\boldsymbol{M} = \begin{bmatrix} \boxed{\boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t}} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \begin{bmatrix} \boldsymbol{x}_{\textbf{Small}}^{(1)} - \boldsymbol{x}_{\textbf{Small}}^{(2)} & \boldsymbol{x}_{\textbf{Small}}^{(4)} & \boldsymbol{x}_{\textbf{Small}}^{(7)} \\ \boldsymbol{x}_{\textbf{Median}}^{(1)} - \boldsymbol{x}_{\textbf{Median}}^{(2)} & \boldsymbol{x}_{\textbf{Median}}^{(4)} & \boldsymbol{x}_{\textbf{Median}}^{(7)} \\ \boldsymbol{x}_{\textbf{Large}}^{(1)} - \boldsymbol{x}_{\textbf{Large}}^{(2)} & \boldsymbol{x}_{\textbf{Large}}^{(4)} & \boldsymbol{x}_{\textbf{Large}}^{(7)} \end{bmatrix}$$

Observation.
Every entry of $\boldsymbol{M}$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$
Every *row* of $\boldsymbol{M}$ sums to $\vec{\boldsymbol{0}}$ with proper **small**, **median**, **large** weights

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors
using coeffs in $\pm\boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\boldsymbol{M} = \begin{bmatrix} \boxed{\boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t}} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \begin{bmatrix} \boldsymbol{x}^{(1)}_{\textbf{Small}} - \boldsymbol{x}^{(2)}_{\textbf{Small}} & \boldsymbol{x}^{(4)}_{\textbf{Small}} & \boldsymbol{x}^{(7)}_{\textbf{Small}} \\ \boldsymbol{x}^{(1)}_{\textbf{Median}} - \boldsymbol{x}^{(2)}_{\textbf{Median}} & \boldsymbol{x}^{(4)}_{\textbf{Median}} & \boldsymbol{x}^{(7)}_{\textbf{Median}} \\ \boldsymbol{x}^{(1)}_{\textbf{Large}} - \boldsymbol{x}^{(2)}_{\textbf{Large}} & \boldsymbol{x}^{(4)}_{\textbf{Large}} & \boldsymbol{x}^{(7)}_{\textbf{Large}} \end{bmatrix}$$

Observation.
Every entry of $\boldsymbol{M}$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$
Every *row* of $\boldsymbol{M}$ sums to $\vec{\boldsymbol{0}}$ with proper **small**, **median**, **large** weights

$$\mathbf{1} \cdot \boldsymbol{x}^{(1)} - (\boldsymbol{B}/\mathbf{4}) \cdot \boldsymbol{x}^{(2)} + (\boldsymbol{B}/\mathbf{2}) \cdot \boldsymbol{x}^{(4)} + (\mathbf{5}\boldsymbol{B}/\mathbf{6}) \cdot \boldsymbol{x}^{(7)} = \vec{\boldsymbol{0}}$$

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\boldsymbol{M} = \begin{bmatrix} \boxed{\boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t}} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \begin{bmatrix} \boldsymbol{x}^{(1)}_{\mathbf{Small}} - \boldsymbol{x}^{(2)}_{\mathbf{Small}} & \boldsymbol{x}^{(4)}_{\mathbf{Small}} & \boldsymbol{x}^{(7)}_{\mathbf{Small}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Median}} - \boldsymbol{x}^{(2)}_{\mathbf{Median}} & \boldsymbol{x}^{(4)}_{\mathbf{Median}} & \boldsymbol{x}^{(7)}_{\mathbf{Median}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Large}} - \boldsymbol{x}^{(2)}_{\mathbf{Large}} & \boldsymbol{x}^{(4)}_{\mathbf{Large}} & \boldsymbol{x}^{(7)}_{\mathbf{Large}} \end{bmatrix}$$

Observation.
Every entry of $\boldsymbol{M}$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$
Every *row* of $\boldsymbol{M}$ sums to $\vec{\mathbf{0}}$ with proper **small**, **median**, **large** weights

$$\mathbf{1} \cdot \boldsymbol{x}^{(1)} - (\boldsymbol{B}/\mathbf{4}) \cdot \boldsymbol{x}^{(2)} + (\boldsymbol{B}/\mathbf{2}) \cdot \boldsymbol{x}^{(4)} + (\mathbf{5}\boldsymbol{B}/\mathbf{6}) \cdot \boldsymbol{x}^{(7)} = \vec{\mathbf{0}}$$

$$\boldsymbol{x} = \begin{bmatrix} \boldsymbol{x}_{\mathbf{Small}} \\ \boldsymbol{x}_{\mathbf{Median}} \\ \boldsymbol{x}_{\mathbf{Large}} \end{bmatrix}$$

The SIS^∞ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\boldsymbol{M} = \begin{bmatrix} \boxed{\boldsymbol{a} \quad \boldsymbol{b} \quad \boldsymbol{t}} \\ \boldsymbol{d} \quad \boldsymbol{e} \quad \boldsymbol{f} \\ \boldsymbol{g} \quad \boldsymbol{h} \quad \boldsymbol{i} \end{bmatrix} = \begin{bmatrix} \boldsymbol{x}^{(1)}_{\mathbf{Small}} - \boldsymbol{x}^{(2)}_{\mathbf{Small}} & \boldsymbol{x}^{(4)}_{\mathbf{Small}} & \boldsymbol{x}^{(7)}_{\mathbf{Small}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Median}} - \boldsymbol{x}^{(2)}_{\mathbf{Median}} & \boldsymbol{x}^{(4)}_{\mathbf{Median}} & \boldsymbol{x}^{(7)}_{\mathbf{Median}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Large}} - \boldsymbol{x}^{(2)}_{\mathbf{Large}} & \boldsymbol{x}^{(4)}_{\mathbf{Large}} & \boldsymbol{x}^{(7)}_{\mathbf{Large}} \end{bmatrix}$$

Observation.
Every entry of $\boldsymbol{M}$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$
Every *row* of $\boldsymbol{M}$ sums to $\vec{\mathbf{0}}$ with proper **small**, **median**, **large** weights

$$\mathbf{1} \cdot \boldsymbol{x}^{(1)} - (\boldsymbol{B}/\mathbf{4}) \cdot \boldsymbol{x}^{(2)} + (\boldsymbol{B}/\mathbf{2}) \cdot \boldsymbol{x}^{(4)} + (\mathbf{5}\boldsymbol{B}/\mathbf{6}) \cdot \boldsymbol{x}^{(7)} = \vec{\mathbf{0}}$$

$$\mathbf{1} \cdot \boldsymbol{x}^{(1)}_{\mathbf{Small}} - (\boldsymbol{B}/\mathbf{4}) \cdot \boldsymbol{x}^{(2)}_{\mathbf{Small}} + (\boldsymbol{B}/\mathbf{2}) \cdot \boldsymbol{x}^{(4)}_{\mathbf{Small}} + (\mathbf{5}\boldsymbol{B}/\mathbf{6}) \cdot \boldsymbol{x}^{(7)}_{\mathbf{Small}} = \vec{\mathbf{0}}$$

$$\boldsymbol{x} = \begin{bmatrix} \boldsymbol{x}_{\mathbf{Small}} \\ \boldsymbol{x}_{\mathbf{Median}} \\ \boldsymbol{x}_{\mathbf{Large}} \end{bmatrix}$$

The SIS^{∞} problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\boldsymbol{M} = \begin{bmatrix} \boxed{\boldsymbol{a} \quad \boldsymbol{b} \quad \boldsymbol{t}} \\ \boldsymbol{d} \quad \boldsymbol{e} \quad \boldsymbol{f} \\ \boldsymbol{g} \quad \boldsymbol{h} \quad \boldsymbol{i} \end{bmatrix} = \begin{bmatrix} \boldsymbol{x}^{(1)}_{\mathbf{Small}} - \boldsymbol{x}^{(2)}_{\mathbf{Small}} & \boldsymbol{x}^{(4)}_{\mathbf{Small}} & \boldsymbol{x}^{(7)}_{\mathbf{Small}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Median}} - \boldsymbol{x}^{(2)}_{\mathbf{Median}} & \boldsymbol{x}^{(4)}_{\mathbf{Median}} & \boldsymbol{x}^{(7)}_{\mathbf{Median}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Large}} - \boldsymbol{x}^{(2)}_{\mathbf{Large}} & \boldsymbol{x}^{(4)}_{\mathbf{Large}} & \boldsymbol{x}^{(7)}_{\mathbf{Large}} \end{bmatrix}$$

Observation.
Every entry of $\boldsymbol{M}$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$
Every *row* of $\boldsymbol{M}$ sums to $\vec{\mathbf{0}}$ with proper **small**, **median**, **large** weights

$$\mathbf{1} \cdot \boldsymbol{x}^{(1)}_{\mathbf{Small}} - (\boldsymbol{B}/\mathbf{4}) \cdot \boldsymbol{x}^{(2)}_{\mathbf{Small}} + (\boldsymbol{B}/\mathbf{2}) \cdot \boldsymbol{x}^{(4)}_{\mathbf{Small}} + (\mathbf{5}\boldsymbol{B}/\mathbf{6}) \cdot \boldsymbol{x}^{(7)}_{\mathbf{Small}} = \vec{\mathbf{0}}$$

The SIS^{∞} problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\boldsymbol{M} = \begin{bmatrix} \boxed{\boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t}} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \begin{bmatrix} \boldsymbol{x}^{(1)}_{\mathbf{Small}} - \boldsymbol{x}^{(2)}_{\mathbf{Small}} & \boldsymbol{x}^{(4)}_{\mathbf{Small}} & \boldsymbol{x}^{(7)}_{\mathbf{Small}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Median}} - \boldsymbol{x}^{(2)}_{\mathbf{Median}} & \boldsymbol{x}^{(4)}_{\mathbf{Median}} & \boldsymbol{x}^{(7)}_{\mathbf{Median}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Large}} - \boldsymbol{x}^{(2)}_{\mathbf{Large}} & \boldsymbol{x}^{(4)}_{\mathbf{Large}} & \boldsymbol{x}^{(7)}_{\mathbf{Large}} \end{bmatrix}$$

Observation.
Every entry of $\boldsymbol{M}$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$
Every *row* of $\boldsymbol{M}$ sums to $\vec{\mathbf{0}}$ with proper **small**, **median**, **large** weights

$$\mathbf{1} \cdot \boldsymbol{x}^{(1)}_{\mathbf{Small}} - (\boldsymbol{B}/\mathbf{4}) \cdot \boldsymbol{x}^{(2)}_{\mathbf{Small}} + (\boldsymbol{B}/\mathbf{2}) \cdot \boldsymbol{x}^{(4)}_{\mathbf{Small}} + (\mathbf{5}\boldsymbol{B}/\mathbf{6}) \cdot \boldsymbol{x}^{(7)}_{\mathbf{Small}} = \vec{\mathbf{0}}$$

$\boldsymbol{a}$ $\quad\quad$ $\boldsymbol{b}$ $\quad\quad$ $\boldsymbol{t}$

The SIS^∞ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm\boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\boldsymbol{M} = \begin{bmatrix} \boxed{\boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t}} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \begin{bmatrix} \boldsymbol{x}^{(1)}_{\mathbf{Small}} - \boldsymbol{x}^{(2)}_{\mathbf{Small}} & \boldsymbol{x}^{(4)}_{\mathbf{Small}} & \boldsymbol{x}^{(7)}_{\mathbf{Small}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Median}} - \boldsymbol{x}^{(2)}_{\mathbf{Median}} & \boldsymbol{x}^{(4)}_{\mathbf{Median}} & \boldsymbol{x}^{(7)}_{\mathbf{Median}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Large}} - \boldsymbol{x}^{(2)}_{\mathbf{Large}} & \boldsymbol{x}^{(4)}_{\mathbf{Large}} & \boldsymbol{x}^{(7)}_{\mathbf{Large}} \end{bmatrix}$$

Observation.
Every entry of $\boldsymbol{M}$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$
Every *row* of $\boldsymbol{M}$ sums to $\vec{\mathbf{0}}$ with proper **small**, **median**, **large** weights

$$1 \cdot \boldsymbol{x}^{(1)}_{\mathbf{Small}} - (\boldsymbol{B}/4) \cdot \boldsymbol{x}^{(2)}_{\mathbf{Small}} + (\boldsymbol{B}/2) \cdot \boldsymbol{x}^{(4)}_{\mathbf{Small}} + (5\boldsymbol{B}/6) \cdot \boldsymbol{x}^{(7)}_{\mathbf{Small}} = \vec{\mathbf{0}}$$

$$\mathbf{small} \cdot \boldsymbol{a} \quad \mathbf{median} \cdot \boldsymbol{b} \quad \mathbf{large} \cdot \boldsymbol{t}$$

The SIS^∞ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\boldsymbol{M} = \begin{bmatrix} \boxed{\boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t}} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \begin{bmatrix} \boldsymbol{x}^{(1)}_{\mathbf{Small}} - \boldsymbol{x}^{(2)}_{\mathbf{Small}} & \boldsymbol{x}^{(4)}_{\mathbf{Small}} & \boldsymbol{x}^{(7)}_{\mathbf{Small}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Median}} - \boldsymbol{x}^{(2)}_{\mathbf{Median}} & \boldsymbol{x}^{(4)}_{\mathbf{Median}} & \boldsymbol{x}^{(7)}_{\mathbf{Median}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Large}} - \boldsymbol{x}^{(2)}_{\mathbf{Large}} & \boldsymbol{x}^{(4)}_{\mathbf{Large}} & \boldsymbol{x}^{(7)}_{\mathbf{Large}} \end{bmatrix}$$

Observation.
Every entry of $\boldsymbol{M}$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$
Every *row* of $\boldsymbol{M}$ sums to $\vec{\mathbf{0}}$ with proper **small**, **median**, **large** weights

$$\mathbf{1} \cdot \boldsymbol{x}^{(1)}_{\mathbf{Small}} - (\boldsymbol{B}/\mathbf{4}) \cdot \boldsymbol{x}^{(2)}_{\mathbf{Small}} + (\boldsymbol{B}/\mathbf{2}) \cdot \boldsymbol{x}^{(4)}_{\mathbf{Small}} + (\mathbf{5}\boldsymbol{B}/\mathbf{6}) \cdot \boldsymbol{x}^{(7)}_{\mathbf{Small}} = \vec{\mathbf{0}}$$

$$\mathbf{small} \cdot \boldsymbol{a} + \mathbf{median} \cdot \boldsymbol{b} + \mathbf{large} \cdot \boldsymbol{t} = \vec{\mathbf{0}}$$

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\boldsymbol{M} = \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \begin{bmatrix} \boldsymbol{x}^{(1)}_{\mathbf{Small}} - \boldsymbol{x}^{(2)}_{\mathbf{Small}} & \boldsymbol{x}^{(4)}_{\mathbf{Small}} & \boldsymbol{x}^{(7)}_{\mathbf{Small}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Median}} - \boldsymbol{x}^{(2)}_{\mathbf{Median}} & \boldsymbol{x}^{(4)}_{\mathbf{Median}} & \boldsymbol{x}^{(7)}_{\mathbf{Median}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Large}} - \boldsymbol{x}^{(2)}_{\mathbf{Large}} & \boldsymbol{x}^{(4)}_{\mathbf{Large}} & \boldsymbol{x}^{(7)}_{\mathbf{Large}} \end{bmatrix}$$

Observation.
Every entry of $\boldsymbol{M}$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$
Every *column* of $\boldsymbol{M}$ sums to $\vec{\mathbf{0}}$ with proper **small**, **median**, **large** weights

The SIS^{∞} problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors
using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\boldsymbol{M} = \begin{bmatrix} \boxed{\begin{matrix} a \\ d \\ g \end{matrix}} & \begin{matrix} b \\ e \\ h \end{matrix} & \begin{matrix} t \\ f \\ i \end{matrix} \end{bmatrix} = \begin{bmatrix} x^{(1)}_{\mathrm{Small}} - x^{(2)}_{\mathrm{Small}} & x^{(4)}_{\mathrm{Small}} & x^{(7)}_{\mathrm{Small}} \\ x^{(1)}_{\mathrm{Median}} - x^{(2)}_{\mathrm{Median}} & x^{(4)}_{\mathrm{Median}} & x^{(7)}_{\mathrm{Median}} \\ x^{(1)}_{\mathrm{Large}} - x^{(2)}_{\mathrm{Large}} & x^{(4)}_{\mathrm{Large}} & x^{(7)}_{\mathrm{Large}} \end{bmatrix}$$

Observation.
Every entry of $\boldsymbol{M}$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$
Every *column* of $\boldsymbol{M}$ sums to $\vec{\boldsymbol{0}}$ with proper **small**, **median**, **large** weights

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors
using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\boldsymbol{M} = \begin{bmatrix} \boxed{\begin{matrix} \boldsymbol{a} \\ \boldsymbol{d} \\ \boldsymbol{g} \end{matrix}} & \begin{matrix} \boldsymbol{b} \\ \boldsymbol{e} \\ \boldsymbol{h} \end{matrix} & \begin{matrix} \boldsymbol{t} \\ \boldsymbol{f} \\ \boldsymbol{i} \end{matrix} \end{bmatrix} = \begin{bmatrix} \boldsymbol{x}^{(1)}_{\text{Small}} - \boldsymbol{x}^{(2)}_{\text{Small}} & \boldsymbol{x}^{(4)}_{\text{Small}} & \boldsymbol{x}^{(7)}_{\text{Small}} \\ \boldsymbol{x}^{(1)}_{\text{Median}} - \boldsymbol{x}^{(2)}_{\text{Median}} & \boldsymbol{x}^{(4)}_{\text{Median}} & \boldsymbol{x}^{(7)}_{\text{Median}} \\ \boldsymbol{x}^{(1)}_{\text{Large}} - \boldsymbol{x}^{(2)}_{\text{Large}} & \boldsymbol{x}^{(4)}_{\text{Large}} & \boldsymbol{x}^{(7)}_{\text{Large}} \end{bmatrix}$$

Observation.
Every entry of $\boldsymbol{M}$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$
Every *column* of $\boldsymbol{M}$ sums to $\vec{\mathbf{0}}$ with proper **small**, **median**, **large** weights

$$\boldsymbol{x}^{(1)} = \begin{bmatrix} \boldsymbol{x}^{(1)}_{\text{Small}} \\ \boldsymbol{x}^{(1)}_{\text{Median}} \\ \boldsymbol{x}^{(1)}_{\text{Large}} \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{x}^{(2)}_{\text{Small}} \\ \boldsymbol{x}^{(2)}_{\text{Median}} \\ \boldsymbol{x}^{(2)}_{\text{Large}} \end{bmatrix} = \boldsymbol{x}^{(2)}$$

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\boldsymbol{M} = \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \begin{bmatrix} \boldsymbol{x}^{(1)}_{\text{Small}} - \boldsymbol{x}^{(2)}_{\text{Small}} & \boldsymbol{x}^{(4)}_{\text{Small}} & \boldsymbol{x}^{(7)}_{\text{Small}} \\ \boldsymbol{x}^{(1)}_{\text{Median}} - \boldsymbol{x}^{(2)}_{\text{Median}} & \boldsymbol{x}^{(4)}_{\text{Median}} & \boldsymbol{x}^{(7)}_{\text{Median}} \\ \boldsymbol{x}^{(1)}_{\text{Large}} - \boldsymbol{x}^{(2)}_{\text{Large}} & \boldsymbol{x}^{(4)}_{\text{Large}} & \boldsymbol{x}^{(7)}_{\text{Large}} \end{bmatrix}$$

Observation.
Every entry of $\boldsymbol{M}$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$
Every *column* of $\boldsymbol{M}$ sums to $\vec{\boldsymbol{0}}$ with proper **small**, **median**, **large** weights

$$x^{(1)} = \begin{bmatrix} x^{(1)}_{\text{Small}} \\ x^{(1)}_{\text{Median}} \\ x^{(1)}_{\text{Large}} \end{bmatrix} \qquad \begin{bmatrix} \boldsymbol{a} \\ \boldsymbol{d} \\ \boldsymbol{g} \end{bmatrix} \qquad \begin{bmatrix} x^{(2)}_{\text{Small}} \\ x^{(2)}_{\text{Median}} \\ x^{(2)}_{\text{Large}} \end{bmatrix} = x^{(2)}$$

The SIS^∞ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\boldsymbol{M} = \begin{bmatrix} \boxed{\begin{matrix} a \\ d \\ g \end{matrix}} & \begin{matrix} b \\ e \\ h \end{matrix} & \begin{matrix} t \\ f \\ i \end{matrix} \end{bmatrix} = \begin{bmatrix} x^{(1)}_{\text{Small}} - x^{(2)}_{\text{Small}} & x^{(4)}_{\text{Small}} & x^{(7)}_{\text{Small}} \\ x^{(1)}_{\text{Median}} - x^{(2)}_{\text{Median}} & x^{(4)}_{\text{Median}} & x^{(7)}_{\text{Median}} \\ x^{(1)}_{\text{Large}} - x^{(2)}_{\text{Large}} & x^{(4)}_{\text{Large}} & x^{(7)}_{\text{Large}} \end{bmatrix}$$

Observation.
Every entry of $\boldsymbol{M}$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$
Every *column* of $\boldsymbol{M}$ sums to $\vec{\boldsymbol{0}}$ with proper **small**, **median**, **large** weights

$$x^{(1)} = \begin{bmatrix} x^{(1)}_{\text{Small}} \\ x^{(1)}_{\text{Median}} \\ x^{(1)}_{\text{Large}} \end{bmatrix} \qquad \begin{bmatrix} a \\ d \\ g \end{bmatrix} \qquad \begin{bmatrix} x^{(2)}_{\text{Small}} \\ x^{(2)}_{\text{Median}} \\ x^{(2)}_{\text{Large}} \end{bmatrix} = x^{(2)}$$

The SIS^∞ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm\boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\boldsymbol{M} = \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \begin{bmatrix} \boldsymbol{x}^{(1)}_{\mathbf{Small}} - \boldsymbol{x}^{(2)}_{\mathbf{Small}} & \boldsymbol{x}^{(4)}_{\mathbf{Small}} & \boldsymbol{x}^{(7)}_{\mathbf{Small}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Median}} - \boldsymbol{x}^{(2)}_{\mathbf{Median}} & \boldsymbol{x}^{(4)}_{\mathbf{Median}} & \boldsymbol{x}^{(7)}_{\mathbf{Median}} \\ \boldsymbol{x}^{(1)}_{\mathbf{Large}} - \boldsymbol{x}^{(2)}_{\mathbf{Large}} & \boldsymbol{x}^{(4)}_{\mathbf{Large}} & \boldsymbol{x}^{(7)}_{\mathbf{Large}} \end{bmatrix}$$

Observation.
Every entry of $\boldsymbol{M}$ is a disjoint signed-subset-sum of $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$
Every *row* of $\boldsymbol{M}$ sums to $\vec{\mathbf{0}}$ with proper **small**, **median**, **large** weights
Every *column* of $\boldsymbol{M}$ sums to $\vec{\mathbf{0}}$ with proper **small**, **median**, **large** weights

The SIS^{∞} problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix}$$

The SIS^{∞} problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\begin{array}{ccc} \textbf{small} & \textbf{median} & \textbf{large} \end{array}$$

$$\begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \vec{\mathbf{0}}$$

Small $0 \sim B/3$
Median $B/3 \sim 2B/3$
Large $2B/3 \sim B$

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm\boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\begin{array}{r c} \text{small}' & \multirow{3}{*}{$\begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix}$} \\ \text{median}' & \\ \text{large}' & \end{array}$$

$$= \vec{\boldsymbol{0}}$$

Small $0 \sim B/3$
Median $B/3 \sim 2B/3$
Large $2B/3 \sim B$

The SIS^∞ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/\boldsymbol{3}$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\begin{array}{c} \\ \text{small}' \\ \text{median}' \\ \text{large}' \end{array} \begin{array}{c} \begin{array}{ccc} \text{small} & \text{median} & \text{large} \end{array} \\ \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} \end{array} = \vec{\mathbf{0}}$$

$$= \vec{\mathbf{0}}$$

Small $0 \sim B/3$
Median $B/3 \sim 2B/3$
Large $2B/3 \sim B$

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm\boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\begin{array}{c c} & \begin{array}{ccc} \textbf{small} & \textbf{median} & \textbf{large} \end{array} \\ \begin{array}{c} \textbf{small}' \\ \textbf{median}' \\ \textbf{large}' \end{array} & \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \vec{\mathbf{0}} \\ & = \vec{\mathbf{0}} \end{array}$$

$$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$$

Small $0 \sim B/3$
Median $B/3 \sim 2B/3$
Large $2B/3 \sim B$

The SIS^∞ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/\mathbf{3}$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\begin{array}{c c} & \begin{array}{ccc} \text{small} & \text{median} & \text{large} \end{array} \\ \begin{array}{c} \text{small}' \\ \text{median}' \\ \text{large}' \end{array} & \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \vec{0} \end{array}$$

$$= \vec{0}$$

$$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$$

$\mathbf{0} \le \boldsymbol{c} \le \boldsymbol{B}/\mathbf{3}$ (**small** $\boldsymbol{c}$)

Small $0 \sim B/3$
Median $B/3 \sim 2B/3$
Large $2B/3 \sim B$

The SIS^{∞} problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/\boldsymbol{3}$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\begin{array}{cc} & \begin{array}{ccc} \text{small} & \text{median} & \text{large} \end{array} \\ \begin{array}{c} \text{small}' \\ \text{median}' \\ \text{large}' \end{array} & \begin{bmatrix} a & b & t \\ d & e & f \\ g & h & i \end{bmatrix} = \vec{0} \\ & = \vec{0} \end{array}$$

Small $0 \sim B/3$
Median $B/3 \sim 2B/3$
Large $2B/3 \sim B$

$$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$$

$\boldsymbol{0} \le \boldsymbol{c} \le \boldsymbol{B}/\boldsymbol{3}$ (**small** $\boldsymbol{c}$)
$\boldsymbol{c} \cdot \boldsymbol{u}$ has coeffs in $\pm \boldsymbol{c} \subseteq \pm \boldsymbol{B}/\boldsymbol{3}$

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\begin{array}{cc} & \begin{array}{ccc} \text{small} & \text{median} & \text{large} \end{array} \\ \begin{array}{c} \text{small}' \\ \text{median}' \\ \text{large}' \end{array} & \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \vec{0} \\ & = \vec{0} \end{array}$$

$$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$$

$\boldsymbol{0} \le \boldsymbol{c} \le \boldsymbol{B}/3$ **(small $\boldsymbol{c}$)** ✓

$\boldsymbol{B}/3 < \boldsymbol{c} \le 2\boldsymbol{B}/3$ **(median $\boldsymbol{c}$)**

$$\boldsymbol{c} \cdot \boldsymbol{u} = \boldsymbol{c} \cdot \boldsymbol{f} - \boldsymbol{c} \cdot \boldsymbol{h}$$

Small $0 \sim B/3$
Median $B/3 \sim 2B/3$
Large $2B/3 \sim B$

The SIS^{∞} problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\begin{array}{cc} & \begin{array}{ccc} \textbf{small} & \textbf{median} & \textbf{large} \end{array} \\ \begin{array}{c} \textbf{small}' \\ \textbf{median}' \\ \textbf{large}' \end{array} & \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \vec{\mathbf{0}} \\ & = \vec{\mathbf{0}} \end{array}$$

Small $0 \sim B/3$
Median $B/3 \sim 2B/3$
Large $2B/3 \sim B$

$$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$$

$\mathbf{0} \le \boldsymbol{c} \le \boldsymbol{B}/\mathbf{3}$ (**small** $\boldsymbol{c}$) ✓

$\boldsymbol{B}/\mathbf{3} < \boldsymbol{c} \le \mathbf{2}\boldsymbol{B}/\mathbf{3}$ (**median** $\boldsymbol{c}$)

$$\begin{aligned} &\boldsymbol{c} \cdot \boldsymbol{u} \\ &= \boldsymbol{c} \cdot \boldsymbol{f} - (\textbf{small}' \cdot \boldsymbol{t} + \textbf{median}' \cdot \boldsymbol{f} + \textbf{large}' \cdot \boldsymbol{i}) \\ &\quad -\boldsymbol{c} \cdot \boldsymbol{h} \end{aligned}$$

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\begin{array}{cc} & \begin{array}{ccc} \textbf{small} & \textbf{median} & \textbf{large} \end{array} \\ \begin{array}{c} \textbf{small}' \\ \textbf{median}' \\ \textbf{large}' \end{array} & \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \vec{\mathbf{0}} \end{array}$$

$$= \vec{\mathbf{0}}$$

Small $0 \sim B/3$
Median $B/3 \sim 2B/3$
Large $2B/3 \sim B$

$$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$$

$0 \le \boldsymbol{c} \le \boldsymbol{B}/3$ (**small** $\boldsymbol{c}$) ✓

$\boldsymbol{B}/3 < \boldsymbol{c} \le 2\boldsymbol{B}/3$ (**median** $\boldsymbol{c}$)

$$\begin{aligned} &\boldsymbol{c} \cdot \boldsymbol{u} \\ &= \boldsymbol{c} \cdot \boldsymbol{f} - (\textbf{small}' \cdot \boldsymbol{t} + \textbf{median}' \cdot \boldsymbol{f} + \textbf{large}' \cdot \boldsymbol{i}) \\ &\quad -\boldsymbol{c} \cdot \boldsymbol{h} + (\textbf{small} \cdot \boldsymbol{g} + \textbf{median} \cdot \boldsymbol{h} + \textbf{large} \cdot \boldsymbol{i}) \end{aligned}$$

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\begin{array}{c|ccc} & \text{small} & \text{median} & \text{large} \\ \hline \text{small}' & & & \\ \text{median}' & & & \\ \text{large}' & & & \end{array} \quad \begin{bmatrix} a & b & t \\ d & e & f \\ g & h & i \end{bmatrix} = \vec{0}$$

$$= \vec{0}$$

$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$

$0 \le c \le B/3$ (small c) ✓

$B/3 < c \le 2B/3$ (median c)

$$\begin{aligned} & c \cdot u \\ &= c \cdot f - (\text{small}' \cdot t + \text{median}' \cdot f + \text{large}' \cdot i) \\ &\quad - c \cdot h + (\text{small} \cdot g + \text{median} \cdot h + \text{large} \cdot i) \\ &= \qquad \cdot t + \qquad \cdot g \\ &\quad + \qquad \cdot f + \qquad \cdot h \\ &\quad + \qquad \cdot i \end{aligned}$$

Small $0 \sim B/3$
Median $B/3 \sim 2B/3$
Large $2B/3 \sim B$

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm\boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\begin{array}{cc} & \begin{array}{ccc} \text{small} & \text{median} & \text{large} \end{array} \\ \begin{array}{c} \text{small}' \\ \text{median}' \\ \text{large}' \end{array} & \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \vec{0} \\ & = \vec{0} \end{array}$$

Small $0 \sim B/3$
Median $B/3 \sim 2B/3$
Large $2B/3 \sim B$

$$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$$

$\boldsymbol{0} \leq \boldsymbol{c} \leq \boldsymbol{B}/3$ (**small** $\boldsymbol{c}$) ✓

$\boldsymbol{B}/3 < \boldsymbol{c} \leq 2\boldsymbol{B}/3$ (**median** $\boldsymbol{c}$)

$$\begin{aligned} &\boldsymbol{c} \cdot \boldsymbol{u} \\ &= \boldsymbol{c} \cdot \boldsymbol{f} - (\mathbf{small}' \cdot \boldsymbol{t} + \mathbf{median}' \cdot \boldsymbol{f} + \mathbf{large}' \cdot \boldsymbol{i}) \\ &\quad -\boldsymbol{c} \cdot \boldsymbol{h} + (\mathbf{small} \cdot \boldsymbol{g} + \mathbf{median} \cdot \boldsymbol{h} + \mathbf{large} \cdot \boldsymbol{i}) \\ &= -\mathbf{small}' \cdot \boldsymbol{t} + \mathbf{small} \cdot \boldsymbol{g} \\ &\quad +(\boldsymbol{c} - \mathbf{median}') \cdot \boldsymbol{f} + (\mathbf{median} - \boldsymbol{c}) \cdot \boldsymbol{h} \\ &\quad +(\mathbf{large} - \mathbf{large}') \cdot \boldsymbol{i} \end{aligned}$$

The SIS^∞ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\begin{array}{c|c} & \text{small} \quad \text{median} \quad \text{large} \\ \hline \begin{array}{c}\text{small}' \\ \text{median}' \\ \text{large}'\end{array} & \begin{bmatrix} a & b & t \\ d & e & f \\ g & h & i \end{bmatrix} = \vec{0} \end{array}$$

$$= \vec{0}$$

Small $0 \sim B/3$
Median $B/3 \sim 2B/3$
Large $2B/3 \sim B$

$$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$$

$0 \le c \le B/3$ (small c) ✓

$B/3 < c \le 2B/3$ (median c)

$$\begin{aligned} & c \cdot u \\ & = c \cdot f - (\text{small}' \cdot t + \text{median}' \cdot f + \text{large}' \cdot i) \\ & \quad -c \cdot h + (\text{small} \cdot g + \text{median} \cdot h + \text{large} \cdot i) \\ & = \left.\begin{aligned} & -\text{small}' \cdot t + \text{small} \cdot g \\ & +(c - \text{median}') \cdot f + (\text{median} - c) \cdot h \\ & +(\text{large} - \text{large}') \cdot i \end{aligned}\right\} \text{Coeffs in } \pm B/3 \end{aligned}$$

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm\boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\begin{array}{cc} & \begin{array}{ccc} \text{small} & \text{median} & \text{large} \end{array} \\ \begin{array}{c} \text{small}' \\ \text{median}' \\ \text{large}' \end{array} & \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \vec{\mathbf{0}} \\ & = \vec{\mathbf{0}} \end{array}$$

$$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$$

$\mathbf{0} \le \boldsymbol{c} \le \boldsymbol{B}/\mathbf{3}$ (**small** $\boldsymbol{c}$) ✓

$\boldsymbol{B}/\mathbf{3} < \boldsymbol{c} \le \mathbf{2}\boldsymbol{B}/\mathbf{3}$ (**median** $\boldsymbol{c}$) ✓

$\mathbf{2}\boldsymbol{B}/\mathbf{3} < \boldsymbol{c} \le \boldsymbol{B}$ (**Large** $\boldsymbol{c}$)

Small $\mathbf{0} \sim \boldsymbol{B}/\mathbf{3}$
Median $\boldsymbol{B}/\mathbf{3} \sim \mathbf{2}\boldsymbol{B}/\mathbf{3}$
Large $\mathbf{2}\boldsymbol{B}/\mathbf{3} \sim \boldsymbol{B}$

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm\boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\begin{array}{cc} & \begin{array}{ccc} \textbf{small} & \textbf{median} & \textbf{large} \end{array} \\ \begin{array}{c} \textbf{small}' \\ \textbf{median}' \\ \textbf{large}' \end{array} & \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \vec{\mathbf{0}} \end{array}$$

$$= \vec{\mathbf{0}}$$

$$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$$

$\mathbf{0} \le \boldsymbol{c} \le \boldsymbol{B}/\mathbf{3}$ (**small** $\boldsymbol{c}$) ✓

$\boldsymbol{B}/\mathbf{3} < \boldsymbol{c} \le \mathbf{2}\boldsymbol{B}/\mathbf{3}$ (**median** $\boldsymbol{c}$) ✓

$\mathbf{2}\boldsymbol{B}/\mathbf{3} < \boldsymbol{c} \le \boldsymbol{B}$ (**Large** $\boldsymbol{c}$)

$$\begin{aligned} &\boldsymbol{c} \cdot \boldsymbol{u} \\ &= \boldsymbol{c} \cdot \boldsymbol{f} - (\textbf{small} \cdot \boldsymbol{d} + \textbf{median} \cdot \boldsymbol{e} + \textbf{large} \cdot \boldsymbol{f}) \\ &\quad - \boldsymbol{c} \cdot \boldsymbol{h} + (\textbf{small}' \cdot \boldsymbol{b} + \textbf{median}' \cdot \boldsymbol{e} + \textbf{large}' \cdot \boldsymbol{h}) \end{aligned}$$

Small $0 \sim B/3$
Median $B/3 \sim 2B/3$
Large $2B/3 \sim B$

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\begin{array}{cc} & \textbf{small} \quad \textbf{median} \quad \textbf{large} \\ \begin{array}{c} \textbf{small}' \\ \textbf{median}' \\ \textbf{large}' \end{array} & \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \vec{0} \end{array}$$

$$= \vec{0}$$

Small $0 \sim B/3$
Median $B/3 \sim 2B/3$
Large $2B/3 \sim B$

$$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$$

$\mathbf{0} \le \boldsymbol{c} \le \boldsymbol{B}/\mathbf{3}$ (**small** $\boldsymbol{c}$) ✓

$\boldsymbol{B}/\mathbf{3} < \boldsymbol{c} \le \mathbf{2}\boldsymbol{B}/\mathbf{3}$ (**median** $\boldsymbol{c}$) ✓

$\mathbf{2}\boldsymbol{B}/\mathbf{3} < \boldsymbol{c} \le \boldsymbol{B}$ (**Large** $\boldsymbol{c}$)

$$\begin{aligned} &\boldsymbol{c} \cdot \boldsymbol{u} \\ &= \boldsymbol{c} \cdot \boldsymbol{f} - (\textbf{small} \cdot \boldsymbol{d} + \textbf{median} \cdot \boldsymbol{e} + \textbf{large} \cdot \boldsymbol{f}) \\ &\quad -\boldsymbol{c} \cdot \boldsymbol{h} + (\textbf{small}' \cdot \boldsymbol{b} + \textbf{median}' \cdot \boldsymbol{e} + \textbf{large}' \cdot \boldsymbol{h}) \\ &= -\textbf{small} \cdot \boldsymbol{d} + \textbf{small}' \cdot \boldsymbol{b} \\ &\quad +(\textbf{median}' - \textbf{median}) \cdot \boldsymbol{e} \\ &\quad +(\boldsymbol{c} - \textbf{large}) \cdot \boldsymbol{f} + (\textbf{large}' - \boldsymbol{c}) \cdot \boldsymbol{h} \end{aligned}$$

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\begin{array}{c|ccc} & \textbf{small} & \textbf{median} & \textbf{large} \\ \hline \textbf{small}' & & & \\ \textbf{median}' & & \left[\begin{matrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{matrix}\right] & \\ \textbf{large}' & & & \end{array} = \vec{0}$$

$$= \vec{0}$$

$$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$$

$\boldsymbol{0 \le c \le B/3}$ **(small $\boldsymbol{c}$)** ✓

$\boldsymbol{B/3 < c \le 2B/3}$ **(median $\boldsymbol{c}$)** ✓

$\boldsymbol{2B/3 < c \le B}$ **(Large $\boldsymbol{c}$)**

$$\begin{aligned} &\boldsymbol{c} \cdot \boldsymbol{u} \\ &= \boldsymbol{c} \cdot \boldsymbol{f} - (\mathbf{small} \cdot \boldsymbol{d} + \mathbf{median} \cdot \boldsymbol{e} + \mathbf{large} \cdot \boldsymbol{f}) \\ &\quad - \boldsymbol{c} \cdot \boldsymbol{h} + (\mathbf{small}' \cdot \boldsymbol{b} + \mathbf{median}' \cdot \boldsymbol{e} + \mathbf{large}' \cdot \boldsymbol{h}) \\ &= \left.\begin{aligned} & -\mathbf{small} \cdot \boldsymbol{d} + \mathbf{small}' \cdot \boldsymbol{b} \\ & +(\mathbf{median}' - \mathbf{median}) \cdot \boldsymbol{e} \\ & +(\boldsymbol{c} - \mathbf{large}) \cdot \boldsymbol{f} + (\mathbf{large}' - \boldsymbol{c}) \cdot \boldsymbol{h} \end{aligned}\right\} \text{Coeffs in } \pm \boldsymbol{B}/3 \end{aligned}$$

Small $0 \sim B/3$
Median $B/3 \sim 2B/3$
Large $2B/3 \sim B$

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\begin{array}{c} \\ \text{small}' \\ \text{median}' \\ \text{large}' \end{array} \begin{array}{c} \begin{array}{ccc} \text{small} & \text{median} & \text{large} \end{array} \\ \begin{bmatrix} a & b & t \\ d & e & f \\ g & h & i \end{bmatrix} = \vec{0} \\ = \vec{0} \end{array}$$

$$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$$

$\mathbf{0} \le \boldsymbol{c} \le \boldsymbol{B}/\mathbf{3}$ (**small** $\boldsymbol{c}$) ✓

$\boldsymbol{B}/\mathbf{3} < \boldsymbol{c} \le \mathbf{2}\boldsymbol{B}/\mathbf{3}$ (**median** $\boldsymbol{c}$) ✓

$\mathbf{2}\boldsymbol{B}/\mathbf{3} < \boldsymbol{c} \le \boldsymbol{B}$ (**Large** $\boldsymbol{c}$) ✓

The SIS^∞ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{R^2}$

$$\begin{array}{cc} & \begin{array}{ccc} \textbf{small} & \textbf{median} & \textbf{large} \end{array} \\ \begin{array}{c} \textbf{small}' \\ \textbf{median}' \\ \textbf{large}' \end{array} & \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \vec{\mathbf{0}} \\ & = \vec{\mathbf{0}} \end{array}$$

$$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$$

$\mathbf{0} \le |\boldsymbol{c}| \le \boldsymbol{B}/\mathbf{3}$ (**small** $\boldsymbol{c}$) ✓

$\boldsymbol{B}/\mathbf{3} < |\boldsymbol{c}| \le \mathbf{2}\boldsymbol{B}/\mathbf{3}$ (**median** $\boldsymbol{c}$) ✓

$\mathbf{2}\boldsymbol{B}/\mathbf{3} < |\boldsymbol{c}| \le \boldsymbol{B}$ (**Large** $\boldsymbol{c}$) ✓

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\begin{array}{cc} & \begin{array}{ccc} \textbf{small} & \textbf{median} & \textbf{large} \end{array} \\ \begin{array}{c} \textbf{small}' \\ \textbf{median}' \\ \textbf{large}' \end{array} & \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \vec{\mathbf{0}} \\ & = \vec{\mathbf{0}} \end{array}$$

$$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$$

$\mathbf{0} \leq |\boldsymbol{c}| \leq \boldsymbol{B}/\mathbf{3}$ (**small** $\boldsymbol{c}$) ✓

$\boldsymbol{B}/\mathbf{3} < |\boldsymbol{c}| \leq \mathbf{2}\boldsymbol{B}/\mathbf{3}$ (**median** $\boldsymbol{c}$) ✓

$\mathbf{2}\boldsymbol{B}/\mathbf{3} < |\boldsymbol{c}| \leq \boldsymbol{B}$ (**Large** $\boldsymbol{c}$) ✓

$\boldsymbol{u}$ is reducible

The SIS$^\infty$ problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\begin{array}{cc} & \begin{array}{ccc} \text{small} & \text{median} & \text{large} \end{array} \\ \begin{array}{c} \text{small}' \\ \text{median}' \\ \text{large}' \end{array} & \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \vec{0} \end{array}$$

$$= \vec{0}$$

What if $\boldsymbol{f}$ and $\boldsymbol{h}$ are empty?

$$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$$

$0 \le |c| \le B/3$ (small c) ✓

$B/3 < |c| \le 2B/3$ (median c) ✓

$2B/3 < |c| \le B$ (Large c) ✓

$\boldsymbol{u}$ is reducible

The SIS^{∞} problem

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

Construct reducible vector $\boldsymbol{u}$ in $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{R^2}$

$$\begin{array}{c|ccc} & \textbf{small} & \textbf{median} & \textbf{large} \\ \hline \textbf{small}' & \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \textbf{median}' & \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \textbf{large}' & \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{array} = \vec{0}$$

$$= \vec{0}$$

What if $\boldsymbol{f}$ and $\boldsymbol{h}$ are empty?

$$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$$

$\mathbf{0} \leq |\boldsymbol{c}| \leq \boldsymbol{B}/\mathbf{3}$ (**small** $\boldsymbol{c}$) ✓

$\boldsymbol{B}/\mathbf{3} < |\boldsymbol{c}| \leq \mathbf{2}\boldsymbol{B}/\mathbf{3}$ (**median** $\boldsymbol{c}$) ✓

$\mathbf{2}\boldsymbol{B}/\mathbf{3} < |\boldsymbol{c}| \leq \boldsymbol{B}$ (**Large** $\boldsymbol{c}$) ✓

$\boldsymbol{u}$ is reducible

Need to change the base algorithm slightly to ensure nonemptiness

The SIS^{∞} problem

Linear dependence of
$\boldsymbol{R}$ vectors using coeffs $\pm\boldsymbol{B}$

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm\boldsymbol{B}/\boldsymbol{k}$

The SIS^{∞} problem

Linear dependence of
$\boldsymbol{R}$ vectors using coeffs $\pm\boldsymbol{B}$

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors
using coeffs in $\pm\boldsymbol{B}/\boldsymbol{k}$

$$\begin{array}{l} \textbf{small} \\ \textbf{large} \end{array} \begin{bmatrix} \blacksquare \\ \blacksquare \end{bmatrix}$$

$\boldsymbol{k} = \mathbf{2}$
$\boldsymbol{R}$ vectors

The SIS$^\infty$ problem

Linear dependence of
R vectors using coeffs $\pm B$

Def (reducible vector).
u is reducible if for any $-B \leq c \leq B$,
$c \cdot u$ is a linear comb of the given vectors
using coeffs in $\pm B/k$

small
large

$k = 2$
R vectors

small
median
large

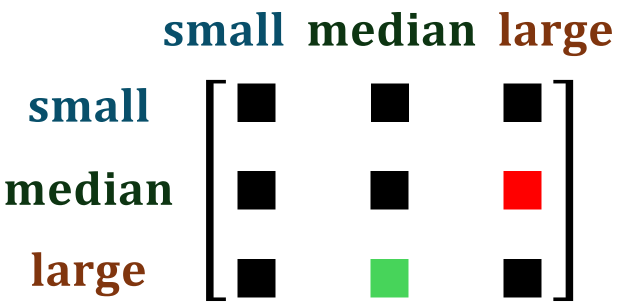
$k = 3$

The SIS$^{\infty}$ problem

Linear dependence of
$\boldsymbol{R}$ vectors using coeffs $\pm\boldsymbol{B}$

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors
using coeffs in $\pm\boldsymbol{B}/\boldsymbol{k}$

$\boldsymbol{k = 2}$
$\boldsymbol{R}$ vectors

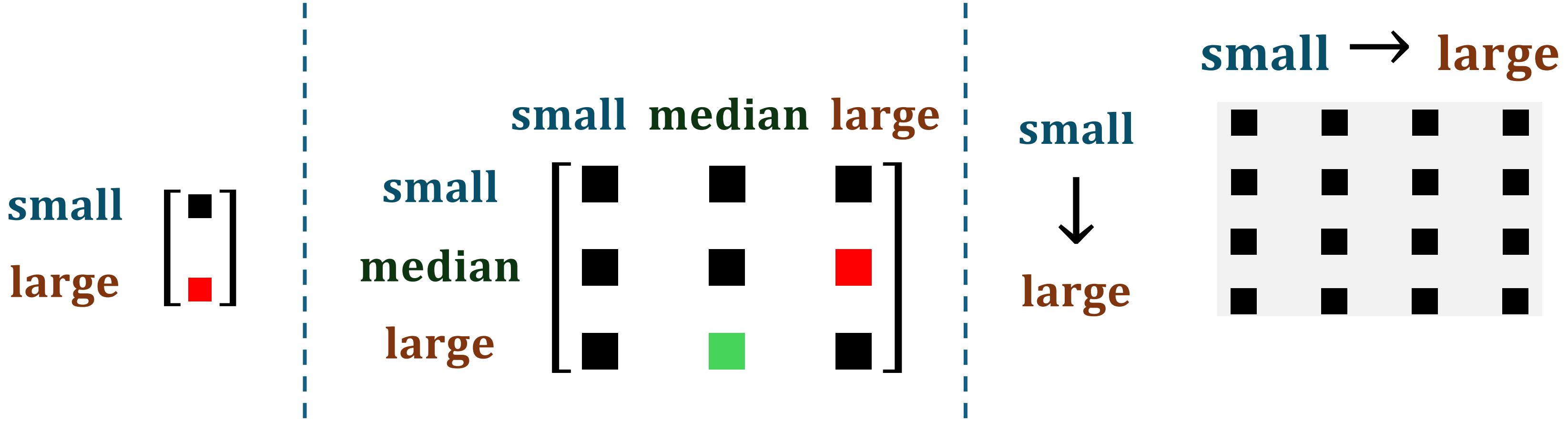


$\boldsymbol{k = 3}$
$\boldsymbol{R^2}$ vectors

The SIS$^\infty$ problem

Linear dependence of
R vectors using coeffs $\pm B$

Def (reducible vector).
u is reducible if for any $-B \leq c \leq B$,
$c \cdot u$ is a linear comb of the given vectors
using coeffs in $\pm B/k$



$k = 2$
R vectors

$k = 3$
R^2 vectors

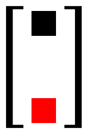
$k = 4$

The SIS$^\infty$ problem

Linear dependence of
$\boldsymbol{R}$ vectors using coeffs $\pm\boldsymbol{B}$

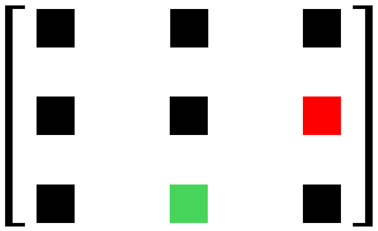
Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors
using coeffs in $\pm\boldsymbol{B}/\boldsymbol{k}$

small
large



$\boldsymbol{k} = \boldsymbol{2}$
$\boldsymbol{R}$ vectors

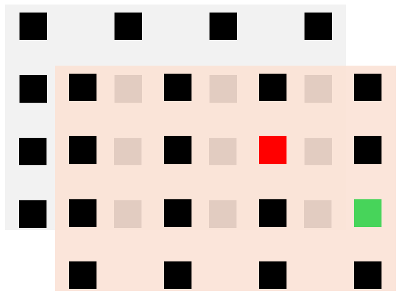
small median large
small
median
large



$\boldsymbol{k} = \boldsymbol{3}$
$\boldsymbol{R}^2$ vectors

small $\rightarrow$ large

small $\downarrow$ large

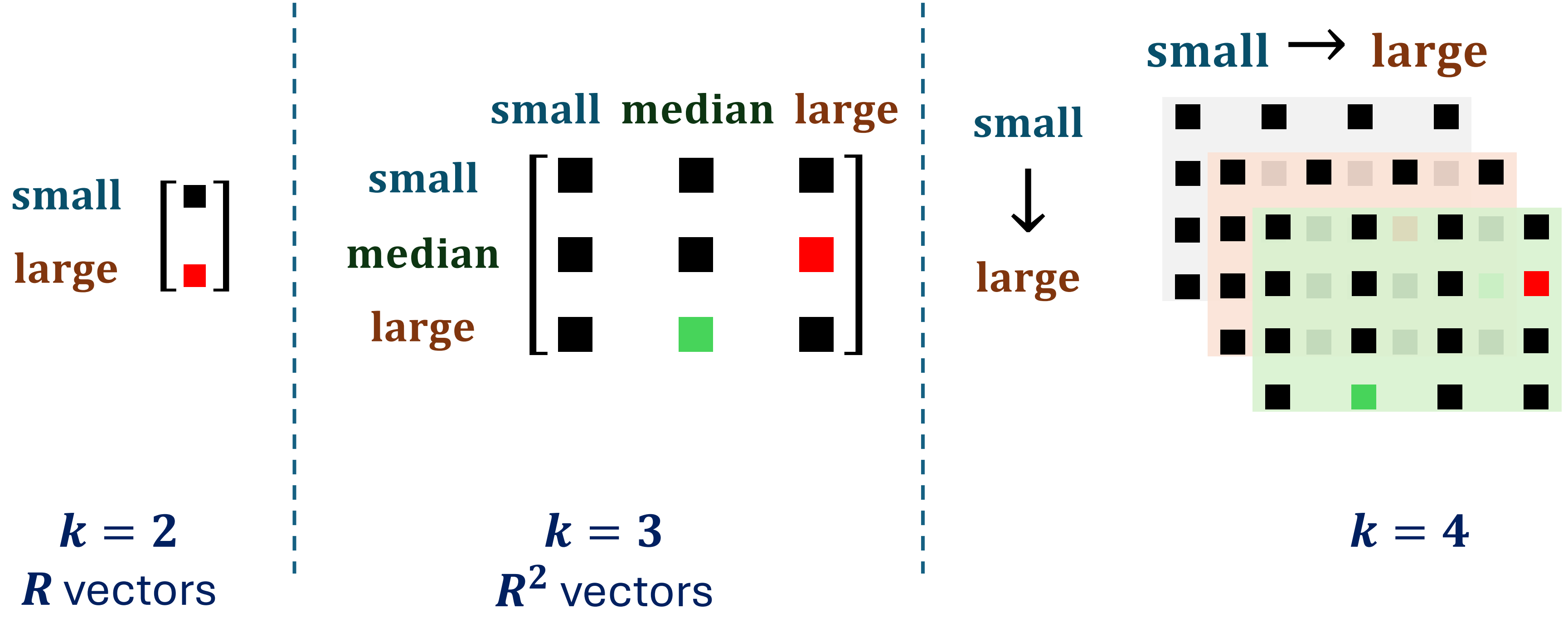


$\boldsymbol{k} = \boldsymbol{4}$

The SIS$^\infty$ problem

Linear dependence of
R vectors using coeffs $\pm B$

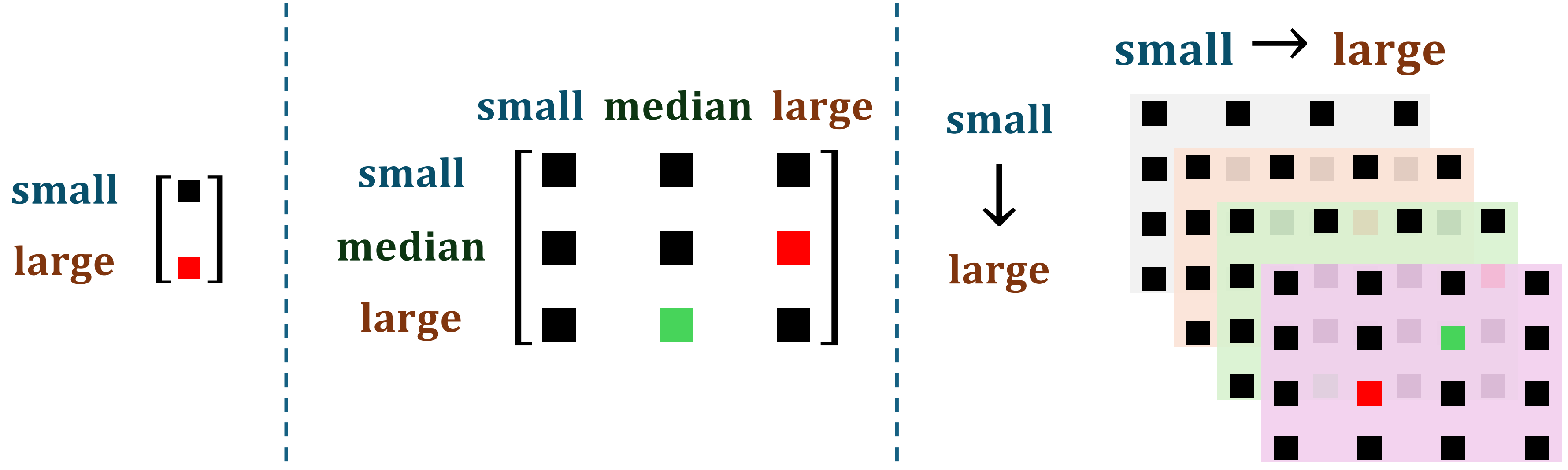
Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-B \le c \le B$,
$c \cdot \boldsymbol{u}$ is a linear comb of the given vectors
using coeffs in $\pm B/k$



The SIS$^\infty$ problem

Linear dependence of
R vectors using coeffs $\pm B$

Def (reducible vector).
u is reducible if for any $-B \le c \le B$,
$c \cdot u$ is a linear comb of the given vectors
using coeffs in $\pm B/k$



$k = 2$
R vectors

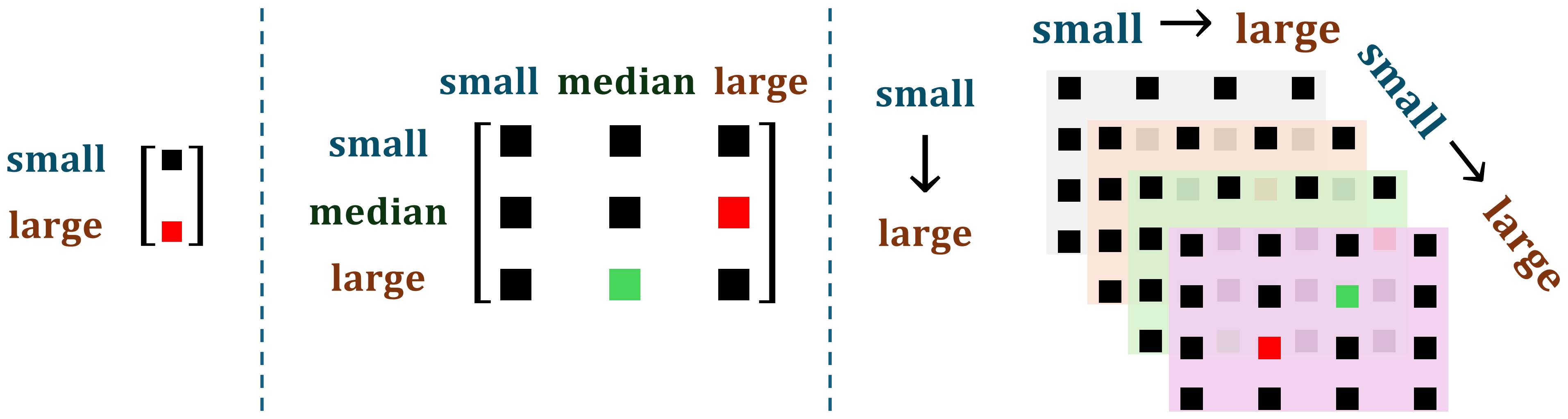
$k = 3$
R^2 vectors

$k = 4$

The SIS^{∞} problem

Linear dependence of
$\boldsymbol{R}$ vectors using coeffs $\pm\boldsymbol{B}$

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors
using coeffs in $\pm\boldsymbol{B}/\boldsymbol{k}$



$\boldsymbol{k} = 2$
$\boldsymbol{R}$ vectors

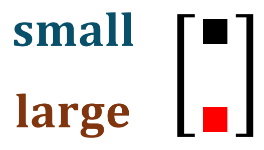
$\boldsymbol{k} = 3$
$\boldsymbol{R}^2$ vectors

$\boldsymbol{k} = 4$
$\boldsymbol{R}^3$ vectors

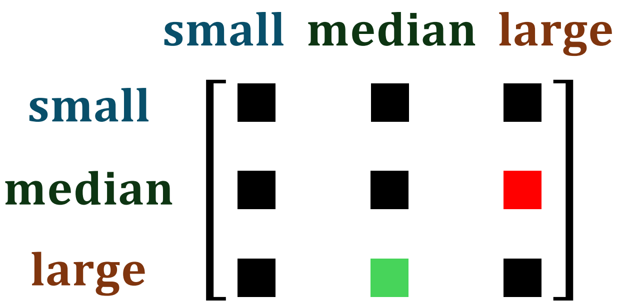
The SIS$^\infty$ problem

Linear dependence of
$\boldsymbol{R}$ vectors using coeffs $\pm\boldsymbol{B}$

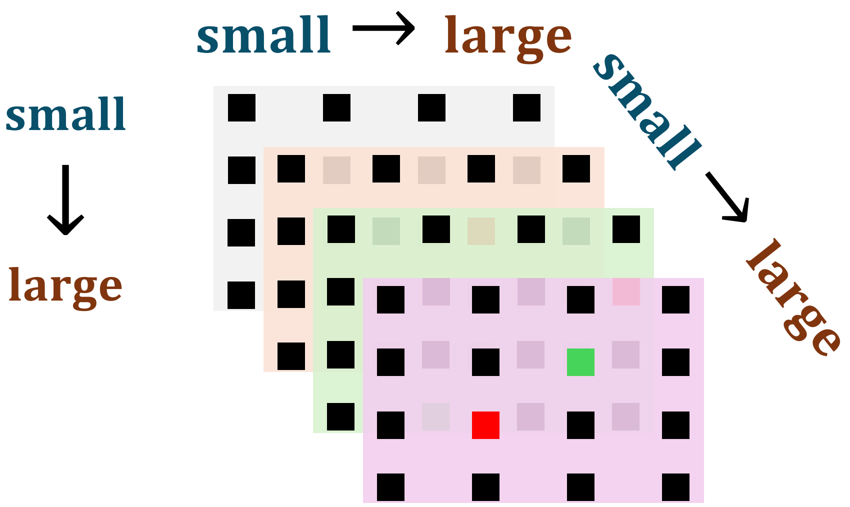
Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors
using coeffs in $\pm\boldsymbol{B}/\boldsymbol{k}$



$\boldsymbol{k = 2}$
$\boldsymbol{R}$ vectors



$\boldsymbol{k = 3}$
$\boldsymbol{R^2}$ vectors



$\boldsymbol{k = 4}$
$\boldsymbol{R^3}$ vectors

General $\boldsymbol{k}$

$(\boldsymbol{k-1})$-dim array

$\boldsymbol{R^{k-1}}$ vectors

Permutohedron

Algorithm overview

$\mathbf{F}_3^n$-Subset-Sum

Reducible vector

The SIS^∞ problem

Weight reduction

The $\boldsymbol{A}$-SIS problem

General reduction

The $\boldsymbol{A}$-SIS problem

Input: $\boldsymbol{v_1}, \dots, \boldsymbol{v_m} \in \mathbf{F}_{\boldsymbol{p}}^{\boldsymbol{n}}$ and $\boldsymbol{A} \subseteq \mathbf{F}_{\boldsymbol{p}}$

Output: linear dependence using coeffs in $\boldsymbol{A}$

The $\boldsymbol{A}$-SIS problem

Input: $\boldsymbol{v_1}, \ldots, \boldsymbol{v_m} \in \mathbf{F}_p^n$ and $\boldsymbol{A} \subseteq \mathbf{F}_p$

Output: linear dependence using coeffs in $\boldsymbol{A}$

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/3$

$$\begin{array}{cc} & \begin{array}{ccc} \text{small} & \text{median} & \text{large} \end{array} \\ \begin{array}{c} \text{small} \\ \text{median} \\ \text{large} \end{array} & \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \vec{0} \\ & = \vec{0} \end{array}$$

small $0 \sim B/3$
median $B/3 \sim 2B/3$
large $2B/3 \sim B$

The $\boldsymbol{A}$-SIS problem

Input: $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbf{F}_p^n$ and $\boldsymbol{A} \subseteq \mathbf{F}_p$

Output: linear dependence using coeffs in $\boldsymbol{A}$

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm\boldsymbol{B}/\mathbf{3}$

$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$ is reducible

For example, if $\boldsymbol{c}$ is **large**, then

$$\begin{aligned}&\boldsymbol{c} \cdot \boldsymbol{u}\\ &= -\mathbf{small} \cdot \boldsymbol{d} + \mathbf{small} \cdot \boldsymbol{b}\\ &\quad +(\mathbf{median} - \mathbf{median}) \cdot \boldsymbol{e}\\ &\quad +(\boldsymbol{c} - \mathbf{large}) \cdot \boldsymbol{f} + (\mathbf{large} - \boldsymbol{c}) \cdot \boldsymbol{h}\end{aligned}$$

$$\begin{array}{cc} & \begin{array}{ccc}\mathbf{small} & \mathbf{median} & \mathbf{large}\end{array} \\ \begin{array}{c}\mathbf{small}\\ \mathbf{median}\\ \mathbf{large}\end{array} & \begin{bmatrix}\boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t}\\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f}\\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i}\end{bmatrix} = \vec{0} \\ & = \vec{0}\end{array}$$

$\mathbf{small}$ $\mathbf{0} \sim \boldsymbol{B}/\mathbf{3}$
$\mathbf{median}$ $\boldsymbol{B}/\mathbf{3} \sim \mathbf{2}\boldsymbol{B}/\mathbf{3}$
$\mathbf{large}$ $\mathbf{2}\boldsymbol{B}/\mathbf{3} \sim \boldsymbol{B}$

The $\boldsymbol{A}$-SIS problem

Input: $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbf{F}_p^n$ and $\boldsymbol{A} \subseteq \mathbf{F}_p$

Output: linear dependence using coeffs in $\boldsymbol{A}$

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \leq \boldsymbol{c} \leq \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/\mathbf{3}$

$$\begin{array}{cc} & \begin{array}{ccc} \mathbf{small} & \mathbf{median} & \mathbf{large} \end{array} \\ \begin{array}{c} \mathbf{small} \\ \mathbf{median} \\ \mathbf{large} \end{array} & \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \vec{0} \\ & = \vec{0} \end{array}$$

small $\mathbf{0} \sim \boldsymbol{B}/\mathbf{3}$
median $\boldsymbol{B}/\mathbf{3} \sim \mathbf{2}\boldsymbol{B}/\mathbf{3}$
large $\mathbf{2}\boldsymbol{B}/\mathbf{3} \sim \boldsymbol{B}$

$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$ is reducible

For example, if $\boldsymbol{c}$ is **large**, then

$$\begin{aligned} &\boldsymbol{c} \cdot \boldsymbol{u} \\ &= -\mathbf{small} \cdot \boldsymbol{d} + \mathbf{small} \cdot \boldsymbol{b} \\ &\quad +(\mathbf{median} - \mathbf{median}) \cdot \boldsymbol{e} \\ &\quad +(\boldsymbol{c} - \mathbf{large}) \cdot \boldsymbol{f} + (\mathbf{large} - \boldsymbol{c}) \cdot \boldsymbol{h} \end{aligned}$$

has coeffs in

- $\pm$**small**
- **median** $-$ **median**
- **large** $-$ **large**

The $\boldsymbol{A}$-SIS problem

Input: $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbf{F}_p^n$ and $\boldsymbol{A} \subseteq \mathbf{F}_p$

Output: linear dependence using coeffs in $\boldsymbol{A}$

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $-\boldsymbol{B} \le \boldsymbol{c} \le \boldsymbol{B}$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm \boldsymbol{B}/\mathbf{3}$

$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$ is reducible

$$\begin{array}{cc} & \begin{array}{ccc} \textbf{small} & \textbf{median} & \textbf{large} \end{array} \\ \begin{array}{c} \textbf{small} \\ \textbf{median} \\ \textbf{large} \end{array} & \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \vec{0} \\ & = \vec{0} \end{array}$$

small $\mathbf{0} \sim \boldsymbol{B}/\mathbf{3}$
median $\boldsymbol{B}/\mathbf{3} \sim \mathbf{2}\boldsymbol{B}/\mathbf{3}$
large $\mathbf{2}\boldsymbol{B}/\mathbf{3} \sim \boldsymbol{B}$

For example, if $\boldsymbol{c}$ is **large**, then

$$\begin{aligned} &\boldsymbol{c} \cdot \boldsymbol{u} \\ &= -\mathbf{small} \cdot \boldsymbol{d} + \mathbf{small} \cdot \boldsymbol{b} \\ &\quad + (\mathbf{median} - \mathbf{median}) \cdot \boldsymbol{e} \\ &\quad + (\boldsymbol{c} - \mathbf{large}) \cdot \boldsymbol{f} + (\mathbf{large} - \boldsymbol{c}) \cdot \boldsymbol{h} \end{aligned}$$

has coeffs in

- $\pm$**small**
- **median** $-$ **median**
- **large** $-$ **large**

All in $\pm \boldsymbol{B}/\mathbf{3}$

The $\boldsymbol{A}$-SIS problem

Input: $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in \mathbf{F}_p^n$ and $\boldsymbol{A} \subseteq \mathbf{F}_p$

Output: linear dependence using coeffs in $\boldsymbol{A}$

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $\boldsymbol{c} \in \pm(\mathbf{small} \cup \mathbf{median} \cup \mathbf{large})$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm$**small** $\cup$ (**median** $-$ **median**) $\cup$ (**large** $-$ **large**)

$$\begin{array}{c|c} & \begin{array}{ccc} \mathbf{small} & \mathbf{median} & \mathbf{large} \end{array} \\ \begin{array}{c} \mathbf{small} \\ \mathbf{median} \\ \mathbf{large} \end{array} & \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \vec{0} \\ & = \vec{0} \end{array}$$

small $\mathbf{0} \sim \boldsymbol{B}/\mathbf{3}$
median $\boldsymbol{B}/\mathbf{3} \sim \mathbf{2}\boldsymbol{B}/\mathbf{3}$
large $\mathbf{2}\boldsymbol{B}/\mathbf{3} \sim \boldsymbol{B}$

$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$ is reducible

For example, if $\boldsymbol{c}$ is **large**, then

$$\begin{aligned} &\boldsymbol{c} \cdot \boldsymbol{u} \\ &= -\mathbf{small} \cdot \boldsymbol{d} + \mathbf{small} \cdot \boldsymbol{b} \\ &\quad + (\mathbf{median} - \mathbf{median}) \cdot \boldsymbol{e} \\ &\quad + (\boldsymbol{c} - \mathbf{large}) \cdot \boldsymbol{f} + (\mathbf{large} - \boldsymbol{c}) \cdot \boldsymbol{h} \end{aligned}$$

has coeffs in

$$\left.\begin{array}{l} \bullet\ \pm\text{small} \\ \bullet\ \text{median} - \text{median} \\ \bullet\ \text{large} - \text{large} \end{array}\right\} \text{All in } \pm\boldsymbol{B}/\mathbf{3}$$

The $\boldsymbol{A}$-SIS problem

Input: $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbf{F}_p^n$ and $\boldsymbol{A} \subseteq \mathbf{F}_p$

Output: linear dependence using coeffs in $\boldsymbol{A}$

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $\boldsymbol{c} \in \pm(\boldsymbol{H}_0 \cup \boldsymbol{H}_1 \cup \boldsymbol{H}_2)$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm\boldsymbol{H}_0 \cup (\boldsymbol{H}_1 - \boldsymbol{H}_1) \cup (\boldsymbol{H}_2 - \boldsymbol{H}_2)$

$$\begin{array}{cc} & \begin{array}{ccc} \boldsymbol{H}_0 & \boldsymbol{H}_1 & \boldsymbol{H}_2 \end{array} \\ \begin{array}{c} \boldsymbol{H}_0 \\ \boldsymbol{H}_1 \\ \boldsymbol{H}_2 \end{array} & \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \vec{0} \\ & = \vec{0} \end{array}$$

$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$ is reducible

For example, if $\boldsymbol{c}$ is in $\boldsymbol{H}_2$, then

$$\begin{aligned} &\boldsymbol{c} \cdot \boldsymbol{u} \\ &= -\boldsymbol{H}_0 \cdot \boldsymbol{d} + \boldsymbol{H}_0 \cdot \boldsymbol{b} \\ &\quad +(\boldsymbol{H}_1 - \boldsymbol{H}_1) \cdot \boldsymbol{e} \\ &\quad +(\boldsymbol{c} - \boldsymbol{H}_2) \cdot \boldsymbol{f} + (\boldsymbol{H}_2 - \boldsymbol{c}) \cdot \boldsymbol{h} \end{aligned}$$

has coeffs in

- $\pm\boldsymbol{H}_0$
- $\boldsymbol{H}_1 - \boldsymbol{H}_1$
- $\boldsymbol{H}_2 - \boldsymbol{H}_2$

The $\boldsymbol{A}$-SIS problem

Input: $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbf{F}_p^n$ and $\boldsymbol{A} \subseteq \mathbf{F}_p$

Output: linear dependence using coeffs in $\boldsymbol{A}$

Def (reducible vector).
$\boldsymbol{u}$ is reducible if for any $\boldsymbol{c} \in \pm(\boldsymbol{H}_0 \cup \boldsymbol{H}_1 \cup \boldsymbol{H}_2)$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm\boldsymbol{H}_0 \cup (\boldsymbol{H}_1 - \boldsymbol{H}_1) \cup (\boldsymbol{H}_2 - \boldsymbol{H}_2)$

$$\begin{array}{cc} & \begin{array}{ccc} \boldsymbol{H}_0 & \boldsymbol{H}_1 & \boldsymbol{H}_2 \end{array} \\ \begin{array}{c} \boldsymbol{H}_0 \\ \boldsymbol{H}_1 \\ \boldsymbol{H}_2 \end{array} & \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{t} \\ \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \\ \boldsymbol{g} & \boldsymbol{h} & \boldsymbol{i} \end{bmatrix} = \vec{0} \\ & = \vec{0} \end{array}$$

$\boldsymbol{u} = \boldsymbol{f} - \boldsymbol{h}$ is reducible

For example, if $\boldsymbol{c}$ is in $\boldsymbol{H}_2$, then

$$\begin{aligned} &\boldsymbol{c} \cdot \boldsymbol{u} \\ &= -\boldsymbol{H}_0 \cdot \boldsymbol{d} + \boldsymbol{H}_0 \cdot \boldsymbol{b} \\ &\quad +(\boldsymbol{H}_1 - \boldsymbol{H}_1) \cdot \boldsymbol{e} \\ &\quad +(\boldsymbol{c} - \boldsymbol{H}_2) \cdot \boldsymbol{f} + (\boldsymbol{H}_2 - \boldsymbol{c}) \cdot \boldsymbol{h} \end{aligned}$$

has coeffs in

- $\pm\boldsymbol{H}_0$
- $\boldsymbol{H}_1 - \boldsymbol{H}_1$
- $\boldsymbol{H}_2 - \boldsymbol{H}_2$

The $\boldsymbol{A}$-SIS problem

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_p^n$ and $\boldsymbol{A} \subseteq \mathbf{F}_p$

Output: linear dependence using coeffs in $\boldsymbol{A}$

Def (reducible vector).

$\boldsymbol{u}$ is reducible if for any $\boldsymbol{c} \in \pm(\boldsymbol{H_0} \cup \boldsymbol{H_1} \cup \boldsymbol{H_2})$,
$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs
in $\pm\boldsymbol{H_0} \cup (\boldsymbol{H_1} - \boldsymbol{H_1}) \cup (\boldsymbol{H_2} - \boldsymbol{H_2})$

Theorem.

If $\boldsymbol{m} = \boldsymbol{R}$ suffices for $\boldsymbol{A} = \pm(\boldsymbol{H_0} \cup \boldsymbol{H_1} \cup \boldsymbol{H_2})$,
then reducible vector exists given $\boldsymbol{R}^2$ vectors

The $\boldsymbol{A}$-SIS problem

Input: $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in \mathbf{F}_p^n$ and $\boldsymbol{A} \subseteq \mathbf{F}_p$

Output: linear dependence using coeffs in $\boldsymbol{A}$

Def (reducible vector).

$\boldsymbol{u}$ is reducible if for any $\boldsymbol{c} \in \pm(\boldsymbol{H}_0 \cup \boldsymbol{H}_1 \cup \boldsymbol{H}_2)$,

$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs in $\pm\boldsymbol{H}_0 \cup (\boldsymbol{H}_1 - \boldsymbol{H}_1) \cup (\boldsymbol{H}_2 - \boldsymbol{H}_2)$

Theorem.

If $\boldsymbol{m} = \boldsymbol{R}$ suffices for $\boldsymbol{A} = \pm(\boldsymbol{H}_0 \cup \boldsymbol{H}_1 \cup \boldsymbol{H}_2)$,

then reducible vector exists given $\boldsymbol{R}^2$ vectors

Therefore $\boldsymbol{m} = \boldsymbol{R}^3$ suffices for $\boldsymbol{A} = \pm\boldsymbol{H}_0 \cup (\boldsymbol{H}_1 - \boldsymbol{H}_1) \cup (\boldsymbol{H}_2 - \boldsymbol{H}_2)$

The $\boldsymbol{A}$-SIS problem

Input: $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbf{F}_p^n$ and $\boldsymbol{A} \subseteq \mathbf{F}_p$

Output: linear dependence using coeffs in $\boldsymbol{A}$

Def (reducible vector).

$\boldsymbol{u}$ is reducible if for any $\boldsymbol{c} \in \pm(\boldsymbol{H}_0 \cup \boldsymbol{H}_1 \cup \cdots \cup \boldsymbol{H}_k)$,

$\boldsymbol{c} \cdot \boldsymbol{u}$ is a linear comb of the given vectors using coeffs

in $\pm\boldsymbol{H}_0 \cup (\boldsymbol{H}_1 - \boldsymbol{H}_1) \cup \cdots \cup (\boldsymbol{H}_k - \boldsymbol{H}_k)$

Theorem.

If $\boldsymbol{m} = \boldsymbol{R}$ suffices for $\boldsymbol{A} = \pm(\boldsymbol{H}_0 \cup \boldsymbol{H}_1 \cup \cdots \cup \boldsymbol{H}_k)$,

then reducible vector exists given $\boldsymbol{R}^k$ vectors

Therefore $\boldsymbol{m} = \boldsymbol{R}^{k+1}$ suffices for $\boldsymbol{A} = \pm\boldsymbol{H}_0 \cup (\boldsymbol{H}_1 - \boldsymbol{H}_1) \cup \cdots \cup (\boldsymbol{H}_k - \boldsymbol{H}_k)$

The $\boldsymbol{A}$-SIS problem

Input: $\boldsymbol{v_1, \ldots, v_m} \in \mathbf{F}_p^n$ and $\boldsymbol{A} \subseteq \mathbf{F}_p$

Output: linear dependence using coeffs in $\boldsymbol{A}$

Theorem.
If $\boldsymbol{m} = \boldsymbol{R}$ suffices for $\boldsymbol{A} = \pm(\boldsymbol{H_0} \cup \boldsymbol{H_1} \cup \cdots \cup \boldsymbol{H_k})$,
then $\boldsymbol{m} = \boldsymbol{R}^{\boldsymbol{k}+1}$ suffices for $\boldsymbol{A} = \pm \boldsymbol{H_0} \cup (\boldsymbol{H_1} - \boldsymbol{H_1}) \cup \cdots \cup (\boldsymbol{H_k} - \boldsymbol{H_k})$

The A-SIS problem

Input: $v_1, \ldots, v_m \in \mathbf{F}_p^n$ and $A \subseteq \mathbf{F}_p$

Output: linear dependence using coeffs in A

Theorem.
If $m = R$ suffices for $A = \pm(H_0 \cup H_1 \cup \cdots \cup H_k)$,
then $m = R^{k+1}$ suffices for $A = \pm H_0 \cup (H_1 - H_1) \cup \cdots \cup (H_k - H_k)$

Fact. If $A = \mathbf{F}_p$, then $m = n + 1$ suffices

The $\boldsymbol{A}$-SIS problem

Input: $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in \mathbf{F}_p^n$ and $\boldsymbol{A} \subseteq \mathbf{F}_p$

Output: linear dependence using coeffs in $\boldsymbol{A}$

Theorem.
If $\boldsymbol{m} = \boldsymbol{R}$ suffices for $\boldsymbol{A} = \pm(\boldsymbol{H}_0 \cup \boldsymbol{H}_1 \cup \cdots \cup \boldsymbol{H}_k)$,
then $\boldsymbol{m} = \boldsymbol{R}^{k+1}$ suffices for $\boldsymbol{A} = \pm \boldsymbol{H}_0 \cup (\boldsymbol{H}_1 - \boldsymbol{H}_1) \cup \cdots \cup (\boldsymbol{H}_k - \boldsymbol{H}_k)$

Fact. If $\boldsymbol{A} = \mathbf{F}_p$, then $\boldsymbol{m} = \boldsymbol{n} + \mathbf{1}$ suffices

Partition $\mathbf{F}_p = \pm(\boldsymbol{H}_0 \cup \boldsymbol{H}_1 \cup \cdots \cup \boldsymbol{H}_k)$
to obtain general $\boldsymbol{A}$

The A-SIS problem

Input: $v_1, \dots, v_m \in \mathbf{F}_p^n$ and $A \subseteq \mathbf{F}_p$

Output: linear dependence using coeffs in A

Theorem.
If $m = R$ suffices for $A = \pm(H_0 \cup H_1 \cup \cdots \cup H_k)$,
then $m = R^{k+1}$ suffices for $A = \pm H_0 \cup (H_1 - H_1) \cup \cdots \cup (H_k - H_k)$

Fact. If $A = \mathbf{F}_p$, then $m = n + 1$ suffices

Partition $\mathbf{F}_p = \pm(H_0 \cup H_1 \cup \cdots \cup H_k)$
to obtain general A

Example.
$p = 11$ and $\mathbf{F}_p = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5\}$
$H_0 = \{0, 3, 4, 5\}$, $H_1 = \{1\}$, and $H_2 = \{2\}$

The $\boldsymbol{A}$-SIS problem

Input: $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in \mathbf{F}_p^n$ and $\boldsymbol{A} \subseteq \mathbf{F}_p$

Output: linear dependence using coeffs in $\boldsymbol{A}$

Theorem.
If $\boldsymbol{m} = \boldsymbol{R}$ suffices for $\boldsymbol{A} = \pm(\boldsymbol{H}_0 \cup \boldsymbol{H}_1 \cup \cdots \cup \boldsymbol{H}_k)$,
then $\boldsymbol{m} = \boldsymbol{R}^{k+1}$ suffices for $\boldsymbol{A} = \pm\boldsymbol{H}_0 \cup (\boldsymbol{H}_1 - \boldsymbol{H}_1) \cup \cdots \cup (\boldsymbol{H}_k - \boldsymbol{H}_k)$

Fact. If $\boldsymbol{A} = \mathbf{F}_p$, then $\boldsymbol{m} = \boldsymbol{n} + \mathbf{1}$ suffices

Partition $\mathbf{F}_p = \pm(\boldsymbol{H}_0 \cup \boldsymbol{H}_1 \cup \cdots \cup \boldsymbol{H}_k)$
to obtain general $\boldsymbol{A}$

Example.
$\boldsymbol{p} = \mathbf{11}$ and $\mathbf{F}_p = \{\mathbf{0}, \pm\mathbf{1}, \pm\mathbf{2}, \pm\mathbf{3}, \pm\mathbf{4}, \pm\mathbf{5}\}$
$\boldsymbol{H}_0 = \{\mathbf{0}, \mathbf{3}, \mathbf{4}, \mathbf{5}\}$, $\boldsymbol{H}_1 = \{\mathbf{1}\}$, and $\boldsymbol{H}_2 = \{\mathbf{2}\}$

Then $\boldsymbol{A} = \{\mathbf{0}, \pm\mathbf{3}, \pm\mathbf{4}, \pm\mathbf{5}\}$
And $\boldsymbol{m} \approx \boldsymbol{n}^3$ suffices

Summary

Classical algorithms matching/improving previous quantum algorithms on Short-Integer-Solution-related problem

- $\mathbf{F}_3^n$-Subset-Sum
- SIS^∞
- $\boldsymbol{A}$-SIS

Summary

Classical algorithms matching/improving previous quantum algorithms on Short-Integer-Solution-related problem

- $\mathbf{F}_3^n$-Subset-Sum
- SIS^∞
- $\boldsymbol{A}$-SIS

No quantum speedup for these problems anymore

Summary

Classical algorithms matching/improving previous quantum algorithms on Short-Integer-Solution-related problem

$$\left.\begin{array}{l}\mathbf{F}_3^n\text{-Subset-Sum} \\ \mathrm{SIS}^\infty \\ \boldsymbol{A}\text{-SIS}\end{array}\right\}\ \text{We do not break any crypto assumption}$$

No quantum speedup for these problems anymore

Summary

Classical algorithms matching/improving previous quantum algorithms on Short-Integer-Solution-related problem

$\mathbf{F}_3^n$-Subset-Sum
SIS^∞
$\boldsymbol{A}$-SIS

We do not break any crypto assumption

No quantum speedup for these problems anymore

Candidate quantum speedup still exists for quantum algorithms similarly based on Regev's reduction

Summary

Classical algorithms matching/improving previous quantum algorithms on Short-Integer-Solution-related problem

- $\mathbf{F}_3^n$-Subset-Sum
- SIS^∞
- $\boldsymbol{A}$-SIS

We do not break any crypto assumption

No quantum speedup for these problems anymore

Candidate quantum speedup still exists for quantum algorithms similarly based on Regev's reduction

Thank you!