# Large Subsets are Sumsets

### Benjamin Baily bmb2@williams.edu

This work was done jointly with the SMALL REU in 2015 and 2021.

With Justine Dell, Sophia Dever, Adam Dionne, Henry Fleischmann, Leo Goldmakher, Gal Gross, Faye Jackson, Steven J. Miller, Ethan Pesikoff, Huy Tuan Pham, Luke Reifenberg, and Vidya Venkatesh.

Williams College

May 24, 2022

# Set Addition

#### Definition

Given two sets  $A, B \subseteq \mathbb{Z}$ , we say that  $A + B = \{a + b \mid a \in A, b \in B\}$ .

# Set Addition

#### Definition

Given two sets  $A, B \subseteq \mathbb{Z}$ , we say that  $A + B = \{a + b \mid a \in A, b \in B\}$ .

### Example

$$\{0,1,2\}+\{0,1,2,4\}=\{0,1,2,3,4,5,6\}$$

# Set Addition

#### Definition

Given two sets  $A, B \subseteq \mathbb{Z}$ , we say that  $A + B = \{a + b \mid a \in A, b \in B\}$ .

#### Example

$$\{0,1,2\}+\{0,1,2,4\}=\{0,1,2,3,4,5,6\}$$

	0	1	2
0	0	1	2
1	1	2	3
2	2	3	4
4	4	5	6

#### Definition

A set  $S \subseteq \mathbb{Z}$  is **reducible** if S = A + B for two sets A, B such that  $|A|, |B| \ge 2$ . Otherwise, S is **irreducible**.

#### Definition

A set  $S \subseteq \mathbb{Z}$  is **reducible** if S = A + B for two sets A, B such that  $|A|, |B| \ge 2$ . Otherwise, S is **irreducible**.

### Example

For any set  $S \subset \mathbb{Z}$  and  $n \in \mathbb{Z}$ , we have  $S = (S + \{-n\}) + \{n\}$ , so it's important to require  $|A|, |B| \ge 2$ .

#### Definition

A set  $S \subseteq \mathbb{Z}$  is **reducible** if S = A + B for two sets A, B such that  $|A|, |B| \ge 2$ . Otherwise, S is **irreducible**.

### Example

For any set  $S \subset \mathbb{Z}$  and  $n \in \mathbb{Z}$ , we have  $S = (S + \{-n\}) + \{n\}$ , so it's important to require  $|A|, |B| \ge 2$ .

### Example

The set  $\{0, 1, 2\} = \{0, 1\} + \{0, 1\}$  is reducible.

#### Definition

A set  $S \subseteq \mathbb{Z}$  is **reducible** if S = A + B for two sets A, B such that  $|A|, |B| \ge 2$ . Otherwise, S is **irreducible**.

### Example

For any set  $S \subset \mathbb{Z}$  and  $n \in \mathbb{Z}$ , we have  $S = (S + \{-n\}) + \{n\}$ , so it's important to require  $|A|, |B| \ge 2$ .

### Example

The set  $\{0,1,2\} = \{0,1\} + \{0,1\}$  is reducible. In contrast,  $\{0,1,3\}$  is irreducible.

# Higher-Dimensional Irreducibility

#### Definition

Let  $S \subset \mathbb{Z}^d$ . S is **reducible** if S = A + B for  $A, B \subset \mathbb{Z}^d$  with  $|A|, |B| \geq 2$ . Otherwise, S is **irreducible**.

# Higher-Dimensional Irreducibility

#### Definition

Let  $S \subset \mathbb{Z}^d$ . S is **reducible** if S = A + B for  $A, B \subset \mathbb{Z}^d$  with  $|A|, |B| \geq 2$ . Otherwise, S is **irreducible**.

Let  $S = \{(0,0), (1,1), (2,2)\}$ . Then,

$$S = \{(0,0), (1,1)\} + \{(0,0), (1,1)\}$$

so S is reducible.

#### Definition

Let 
$$[n]^d = \underbrace{\{0, 1, \dots, n\} \times \{0, 1, \dots, n\} \cdots \{0, 1, \dots, n\}}_{d \ copies}$$
.

### Definition

Let 
$$[n]^d = \underbrace{\{0, 1, \dots, n\} \times \{0, 1, \dots, n\} \cdots \{0, 1, \dots, n\}}_{\substack{d \text{ copies}}}.$$
  
For example,  $[5] = \{0, 1, 2, 3, 4, 5\}.$ 

#### Definition

Let 
$$[n]^d = \underbrace{\{0, 1, \dots, n\} \times \{0, 1, \dots, n\} \cdots \{0, 1, \dots, n\}}_{d \text{ copies}}$$
.  
For example,  $[5] = \{0, 1, 2, 3, 4, 5\}$ .

#### Definition

For  $d, n \geq 1$  we define  $f_d(n)$  as follows.

$$f_d(n) = \min_{S \subset [n]^d, Sirreducible} |[n]^d \setminus S|$$

#### Definition

Let 
$$[n]^d = \underbrace{\{0, 1, \dots, n\} \times \{0, 1, \dots, n\} \cdots \{0, 1, \dots, n\}}_{d \text{ copies}}.$$
  
For example,  $[5] = \{0, 1, 2, 3, 4, 5\}.$ 

#### Definition

For  $d, n \ge 1$  we define  $f_d(n)$  as follows.

$$f_d(n) = \min_{S \subset [n]^d, Sirreducible} |[n]^d \setminus S|$$

#### Theorem

For all d, we have have  $f_d(n) = \Theta(\log n)$ .

#### Lemma

Fix  $S \subset \mathbb{Z}^d$  such that  $|S| \geq 3$  and  $0 \in S$ . Let  $A = \{0, r\}$  for  $r \in \mathbb{Z}^d \setminus \{0\}$ . S = A + B for some  $B \subset S$  iff for all  $s \in S$ ,  $s - r \in S$  or  $s + r \in S$ .

#### Lemma

Fix  $S \subset \mathbb{Z}^d$  such that  $|S| \geq 3$  and  $0 \in S$ . Let  $A = \{0, r\}$  for  $r \in \mathbb{Z}^d \setminus \{0\}$ . S = A + B for some  $B \subset S$  iff for all  $s \in S$ ,  $s - r \in S$  or  $s + r \in S$ .

• We consider the minimum size of the complement of an irreducible subset of  $[n]^d$ .

#### Lemma

Fix  $S \subset \mathbb{Z}^d$  such that  $|S| \geq 3$  and  $0 \in S$ . Let  $A = \{0, r\}$  for  $r \in \mathbb{Z}^d \setminus \{0\}$ . S = A + B for some  $B \subset S$  iff for all  $s \in S$ ,  $s - r \in S$  or  $s + r \in S$ .

- We consider the minimum size of the complement of an irreducible subset of  $[n]^d$ .
- For each  $r \in [n]^d$ , in order for the set  $\{0, r\}$  to not be a summand of S, there must exist  $s \in S$  such that both  $r s, r + s \notin S$ .

#### Lemma

Fix  $S \subset \mathbb{Z}^d$  such that  $|S| \geq 3$  and  $0 \in S$ . Let  $A = \{0, r\}$  for  $r \in \mathbb{Z}^d \setminus \{0\}$ . S = A + B for some  $B \subset S$  iff for all  $s \in S$ ,  $s - r \in S$  or  $s + r \in S$ .

- We consider the minimum size of the complement of an irreducible subset of  $[n]^d$ .
- For each  $r \in [n]^d$ , in order for the set  $\{0, r\}$  to not be a summand of S, there must exist  $s \in S$  such that both  $r s, r + s \notin S$ .
- If  $|[n]^d \setminus S| \ll \log n$ , the complement of S is too small for this to hold for all  $r \in [n]^d$ .

# The Largest Irreducible Subset of $[n]^d$

#### Theorem

Let  $S \subseteq [n]^d$ . Let  $k = \lfloor [n]^d \setminus S \rfloor$ . Then, S is reducible if

$$\frac{k}{d}\log 2 + H_{\lceil \frac{k}{d} \rceil} + H_{\lceil \binom{k}{2} / d \rceil} < H_{n-1}$$

where  $H_n$  is the nth Harmonic number  $(H_n \approx \log(n))$ .

# The Largest Irreducible Subset of $[n]^d$

#### Theorem

Let 
$$S \subseteq [n]^d$$
. Let  $k = |[n]^d \setminus S|$ . Then, S is reducible if

$$\frac{k}{d}\log 2 + H_{\lceil \frac{k}{d} \rceil} + H_{\lceil \binom{k}{2} / d \rceil} < H_{n-1}$$

where  $H_n$  is the nth Harmonic number  $(H_n \approx \log(n))$ .

### Corollary

We have  $f_d(n) = \Omega(\log n)$ .

K. H. Kim and F. W. Roush showed in 2007 that the problem of determining if a set is irreducible is NP-complete.

K. H. Kim and F. W. Roush showed in 2007 that the problem of determining if a set is irreducible is NP-complete.

# Proposition (Local Irreducibility)

Suppose  $S \subset \mathbb{Z}^{\geq 0}$  with  $0 \in S$  satisfies the following.

- If m is the smallest nonzero element of S, then  $2m \notin S$ .
- **2** For each  $s \in S \setminus \{0, m\}$  there is some  $t \in S$  with t < s and  $s + t \notin S$ .

Then, S is irreducible.

K. H. Kim and F. W. Roush showed in 2007 that the problem of determining if a set is irreducible is NP-complete.

# Proposition (Local Irreducibility)

Suppose  $S \subset \mathbb{Z}^{\geq 0}$  with  $0 \in S$  satisfies the following.

- If m is the smallest nonzero element of S, then  $2m \notin S$ .
- **2** For each  $s \in S \setminus \{0, m\}$  there is some  $t \in S$  with t < s and  $s + t \notin S$ .

Then, S is irreducible.

• Local irreducibility is defined to be easily computer verifiable.

K. H. Kim and F. W. Roush showed in 2007 that the problem of determining if a set is irreducible is NP-complete.

## Proposition (Local Irreducibility)

Suppose  $S \subset \mathbb{Z}^{\geq 0}$  with  $0 \in S$  satisfies the following.

- If m is the smallest nonzero element of S, then  $2m \notin S$ .
- **2** For each  $s \in S \setminus \{0, m\}$  there is some  $t \in S$  with t < s and  $s + t \notin S$ .

Then, S is irreducible.

- Local irreducibility is defined to be easily computer verifiable.
- If  $S \subset [n]$ , then verification takes  $O(\max(|S|^2, ([n] \setminus S)^3))$  time.

K. H. Kim and F. W. Roush showed in 2007 that the problem of determining if a set is irreducible is NP-complete.

## Proposition (Local Irreducibility)

Suppose  $S \subset \mathbb{Z}^{\geq 0}$  with  $0 \in S$  satisfies the following.

- If m is the smallest nonzero element of S, then  $2m \notin S$ .
- **2** For each  $s \in S \setminus \{0, m\}$  there is some  $t \in S$  with t < s and  $s + t \notin S$ .

Then, S is irreducible.

- Local irreducibility is defined to be easily computer verifiable.
- If  $S \subset [n]$ , then verification takes  $O(\max(|S|^2, ([n] \setminus S)^3))$  time.
- Irreducibility follows by an iterative argument.

# Proposition (Local Irreducibility)

Suppose  $S \subset \mathbb{Z}^{\geq 0}$  with  $0 \in S$  satisfies the following.

- **1** If m is the smallest nonzero element of S, then  $2m \notin S$ .
- **2** For each  $s \in S \setminus \{0, m\}$  there is some  $t \in S$  with t < s and  $s + t \notin S$ .

Then, S is irreducible.

- WLOG,  $0 \in A, B$  and  $A, B \subset S$  by shifting the sets.
- 1 must be in A or B. Suppose  $1 \in B$ .
- Then, since  $1 + 1 \notin S$ ,  $1 \notin A$ .
- Since  $1+3 \notin S$ , we know  $3 \notin A$ .
- So,  $A = \{0\}$  and S is irreducible.

$$A = \{\} \qquad B = \{\}$$

# Proposition (Local Irreducibility)

Suppose  $S \subset \mathbb{Z}^{\geq 0}$  with  $0 \in S$  satisfies the following.

- **1** If m is the smallest nonzero element of S, then  $2m \notin S$ .
- **2** For each  $s \in S \setminus \{0, m\}$  there is some  $t \in S$  with t < s and  $s + t \notin S$ .

Then, S is irreducible.

- WLOG,  $0 \in A, B$  and  $A, B \subset S$  by shifting the sets.
- 1 must be in A or B. Suppose  $1 \in B$ .
- Then, since  $1 + 1 \notin S$ ,  $1 \notin A$ .
- Since  $1+3 \notin S$ , we know  $3 \notin A$ .
- So,  $A = \{0\}$  and S is irreducible.

$$A = \{0\}$$
  $B = \{0\}$ 

# Proposition (Local Irreducibility)

Suppose  $S \subset \mathbb{Z}^{\geq 0}$  with  $0 \in S$  satisfies the following.

- **1** If m is the smallest nonzero element of S, then  $2m \notin S$ .
- **2** For each  $s \in S \setminus \{0, m\}$  there is some  $t \in S$  with t < s and  $s + t \notin S$ .

Then, S is irreducible.

- WLOG,  $0 \in A, B$  and  $A, B \subset S$  by shifting the sets.
- 1 must be in A or B. Suppose  $1 \in B$ .
- Then, since  $1 + 1 \notin S$ ,  $1 \notin A$ .
- Since  $1+3 \notin S$ , we know  $3 \notin A$ .
- So,  $A = \{0\}$  and S is irreducible.

$$A = \{0\}$$
  $B = \{0, 1\}$ 

# Proposition (Local Irreducibility)

Suppose  $S \subset \mathbb{Z}^{\geq 0}$  with  $0 \in S$  satisfies the following.

- **1** If m is the smallest nonzero element of S, then  $2m \notin S$ .
- **2** For each  $s \in S \setminus \{0, m\}$  there is some  $t \in S$  with t < s and  $s + t \notin S$ .

Then, S is irreducible.

- WLOG,  $0 \in A, B$  and  $A, B \subset S$  by shifting the sets.
- 1 must be in A or B. Suppose  $1 \in B$ .
- Then, since  $1 + 1 \notin S$ ,  $1 \notin A$ .
- Since  $1+3 \notin S$ , we know  $3 \notin A$ .
- So,  $A = \{0\}$  and S is irreducible.

$$A = \{0\}$$
  $B = \{0, 1, 3\}$ 

# Proposition (Local Irreducibility)

Suppose  $S \subset \mathbb{Z}^{\geq 0}$  with  $0 \in S$  satisfies the following.

- **1** If m is the smallest nonzero element of S, then  $2m \notin S$ .
- **2** For each  $s \in S \setminus \{0, m\}$  there is some  $t \in S$  with t < s and  $s + t \notin S$ .

Then, S is irreducible.

- WLOG,  $0 \in A, B$  and  $A, B \subset S$  by shifting the sets.
- 1 must be in A or B. Suppose  $1 \in B$ .
- Then, since  $1 + 1 \notin S$ ,  $1 \notin A$ .
- Since  $1+3 \notin S$ , we know  $3 \notin A$ .
- So,  $A = \{0\}$  and S is irreducible.

$$A = \{0\}$$
  $B = \{0, 1, 3\}$ 

# Local Irreducibility in Higher Dimensions

## Proposition (Local Irreducibility)

Suppose a set  $S \subset \mathbb{Z}^d_{\geq 0}$  with  $0 \in S$  satisfies the following.

- **1** If m is the lexicographically first nonzero element of S, then  $2m \notin S$ .
- **2** For each  $s \in S \setminus \{0, m\}$  there is some  $t \in S$  with  $t \prec s$  and  $s + t \notin S$ .

Then, S is irreducible.

• We construct explicit families of large locally irreducible subsets of  $\mathbb{Z}^{\geq 0}$ 

- We construct explicit families of large locally irreducible subsets of  $\mathbb{Z}^{\geq 0}$
- Use pseudo-greedy construction algorithm to construct the 1-dimensional set

- We construct explicit families of large locally irreducible subsets of  $\mathbb{Z}^{\geq 0}$
- Use pseudo-greedy construction algorithm to construct the 1-dimensional set
- In higher dimensions, place a copy of the 1-dimensional set along each axis of the cube

- We construct explicit families of large locally irreducible subsets of  $\mathbb{Z}^{\geq 0}$
- Use pseudo-greedy construction algorithm to construct the 1-dimensional set
- In higher dimensions, place a copy of the 1-dimensional set along each axis of the cube

# Proposition

For all n, d there exists an irreducible subset  $S \subset [n]^d$  such that  $|[n]^d \setminus S| = O(\log n)$ .

- We construct explicit families of large locally irreducible subsets of  $\mathbb{Z}^{\geq 0}$
- Use pseudo-greedy construction algorithm to construct the 1-dimensional set
- In higher dimensions, place a copy of the 1-dimensional set along each axis of the cube

## Proposition

For all n, d there exists an irreducible subset  $S \subset [n]^d$  such that  $|[n]^d \setminus S| = O(\log n)$ .

### Corollary

We have  $f_d(n) = \Theta(\log n)$ .

• Start with the set  $Q_0 = \{0, 1\}$ 

- Start with the set  $Q_0 = \{0, 1\}$
- After stage i of the process,  $Q_i$  has maximum element  $M_i$

- Start with the set  $Q_0 = \{0, 1\}$
- After stage i of the process,  $Q_i$  has maximum element  $M_i$
- Find the largest number N such that  $Q_i \cup \{M_i + 1, ..., N 1\}$  is locally irreducible

- Start with the set  $Q_0 = \{0, 1\}$
- After stage i of the process,  $Q_i$  has maximum element  $M_i$
- Find the largest number N such that  $Q_i \cup \{M_i + 1, ..., N 1\}$  is locally irreducible
- Set  $Q_{i+1} = Q_i \cup \{M_i + 1, \dots, N-1\}$

- Start with the set  $Q_0 = \{0, 1\}$
- After stage i of the process,  $Q_i$  has maximum element  $M_i$
- Find the largest number N such that  $Q_i \cup \{M_i + 1, ..., N 1\}$  is locally irreducible
- Set  $Q_{i+1} = Q_i \cup \{M_i + 1, \dots, N-1\}$

$$\mathcal{Q}_0 = \{0, 1\}$$

- Start with the set  $Q_0 = \{0, 1\}$
- After stage i of the process,  $Q_i$  has maximum element  $M_i$
- Find the largest number N such that  $Q_i \cup \{M_i + 1, ..., N 1\}$  is locally irreducible
- Set  $Q_{i+1} = Q_i \cup \{M_i + 1, \dots, N-1\}$

$$Q_1 = \{0, 1, 3\}$$

- Start with the set  $Q_0 = \{0, 1\}$
- After stage i of the process,  $Q_i$  has maximum element  $M_i$
- Find the largest number N such that  $Q_i \cup \{M_i + 1, ..., N 1\}$  is locally irreducible
- Set  $Q_{i+1} = Q_i \cup \{M_i + 1, \dots, N-1\}$

$$Q_2 = \{0, 1, 3, 5, 6, 7\}$$

- Start with the set  $Q_0 = \{0, 1\}$
- After stage i of the process,  $Q_i$  has maximum element  $M_i$
- Find the largest number N such that  $Q_i \cup \{M_i + 1, ..., N 1\}$  is locally irreducible
- Set  $Q_{i+1} = Q_i \cup \{M_i + 1, \dots, N-1\}$

$$Q_3 = \{0, 1, 3, 5, 6, 7, 9, 10\}$$

- Start with the set  $Q_0 = \{0, 1\}$
- After stage i of the process,  $Q_i$  has maximum element  $M_i$
- Find the largest number N such that  $Q_i \cup \{M_i + 1, ..., N 1\}$  is locally irreducible
- Set  $Q_{i+1} = Q_i \cup \{M_i + 1, \dots, N-1\}$

$$Q_4 = \{0, 1, 3, 5, 6, 7, 9, 10, 12, 13, 14, 15\}$$

• The set  $Q := \bigcup_{i=1}^{\infty} Q_i$  is locally irreducible by construction.

- The set  $Q := \bigcup_{i=1}^{\infty} Q_i$  is locally irreducible by construction.
- For each n, the set  $[n] \cap \mathcal{Q}$  is also locally irreducible.

- The set  $Q := \bigcup_{i=1}^{\infty} Q_i$  is locally irreducible by construction.
- For each n, the set  $[n] \cap \mathcal{Q}$  is also locally irreducible.
- **Problem:** Hard to estimate the size of  $[n] \cap \mathcal{Q}$ .

- The set  $Q := \bigcup_{i=1}^{\infty} Q_i$  is locally irreducible by construction.
- For each n, the set  $[n] \cap \mathcal{Q}$  is also locally irreducible.
- **Problem:** Hard to estimate the size of  $[n] \cap \mathcal{Q}$ .
- Solution: After constructing  $Q_9$ , change the construction.

- The set  $Q := \bigcup_{i=1}^{\infty} Q_i$  is locally irreducible by construction.
- For each n, the set  $[n] \cap \mathcal{Q}$  is also locally irreducible.
- **Problem:** Hard to estimate the size of  $[n] \cap \mathcal{Q}$ .
- Solution: After constructing  $Q_9$ , change the construction.
- For  $0 \le i \le 9$ , set  $\mathcal{P}_i := \mathcal{Q}_i$ , and for each  $0 \le i \le 9$ , set  $N_i = \max(\mathcal{P}_i) + 1$ .

- The set  $Q := \bigcup_{i=1}^{\infty} Q_i$  is locally irreducible by construction.
- For each n, the set  $[n] \cap \mathcal{Q}$  is also locally irreducible.
- **Problem:** Hard to estimate the size of  $[n] \cap \mathcal{Q}$ .
- Solution: After constructing  $Q_9$ , change the construction.
- For  $0 \le i \le 9$ , set  $\mathcal{P}_i := \mathcal{Q}_i$ , and for each  $0 \le i \le 9$ , set  $N_i = \max(\mathcal{P}_i) + 1$ .
- For  $i \ge 10$ , set  $N_i = N_{i-2} + N_{i-3}$  and let

$$\mathcal{P}_i = \mathcal{P}_{i-1} \cup \{N_{i-1} + 1, \dots, N_i - 1\}$$

• Let  $\mathcal{P} := \bigcup_{i=1}^{\infty} \mathcal{P}_i$ .

- Let  $\mathcal{P} := \bigcup_{i=1}^{\infty} \mathcal{P}_i$ .
- For each n, the set  $[n] \cap \mathcal{P}$  is locally irreducible and its complement in [n] is (up to finitely many edits) a linear recurrence sequence.

- Let  $\mathcal{P} := \bigcup_{i=1}^{\infty} \mathcal{P}_i$ .
- For each n, the set  $[n] \cap \mathcal{P}$  is locally irreducible and its complement in [n] is (up to finitely many edits) a linear recurrence sequence.
- We are able to estimate the number of terms in a linear recurrence sequence up to n.

- Let  $\mathcal{P} := \bigcup_{i=1}^{\infty} \mathcal{P}_i$ .
- For each n, the set  $[n] \cap \mathcal{P}$  is locally irreducible and its complement in [n] is (up to finitely many edits) a linear recurrence sequence.
- We are able to estimate the number of terms in a linear recurrence sequence up to n.
- Let  $\lambda$  denote the largest complex root of the polynomial  $x^3 x 1 = 0$ .

#### Proposition

Let  $\lambda = 1.325...$  denote the largest complex root of the polynomial  $x^3 - x - 1 = 0$ . Then  $|[n] \setminus \mathcal{P}| \sim \log_{\lambda} n$ .

## Recap

- We let  $f_d(n)$  denote the minimum size complement of an irreducible subset of  $[n]^d$ .
- **2** By showing that every sufficiently large subset  $S \subset [n]^d$  admits a factorization of the form S = A + B with  $A = \{0, r\}$ , we proved that  $f_d(n) = \Omega(\log n)$ .
- **3** Define **local irreducibility**, a strong condition on a subset of  $\mathbb{Z}^d$  such that every locally irreducible set is also irreducible.
- **1** Construct large locally irreducible subsets of  $[n]^d$  to prove that  $f_d(n) = O(\log n)$ .
- **6** Conclude that  $f_d(n) = \Theta(\log n)$ .

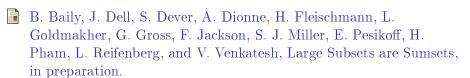
# Acknowledgments

This research was done as part of the SMALL REU program and was funded by NSF grant number 1947438.

Special thanks to Professors Leo Goldmakher and Steven J. Miller for their mentorship.



#### References



https://oeis.org/A349775