Reducibility of Sets in Generalized Settings

Justine Dell[1], Henry Fleischmann[2], and Faye Jackson[2]
Mentors: Leo Goldmakher[3] and Steven J. Miller[3]

Haverford College[1], University of Michigan[2], Williams College[3]

August 21, 2021

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

Irreducibility

Definition

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

Irreducibility

Definition

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

Example

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

Irreducibility

Definition

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

Example

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

Higher Dimensional Irreducibility

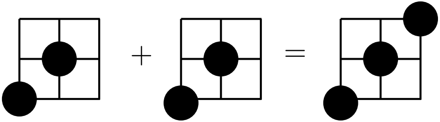
Definition

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

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

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

so S is reducible.



What is the largest size of an irreducible subset of $[n]^d$?

Definition

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

Lemma (BDGGPV 2021)

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 $[n]^d$.
- The above lemma shows that if $|[n^d] \setminus S|$ is too small then $S = A + B$ for some $A = \{0, r\}$.

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

Theorem (SMALL 2021)

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

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

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

- This tells us that the size of the complements of irreducible subsets of $[n]^d$ are $\Omega(d \log n)$.

How do you easily show a set is irreducible?

Proposition (Local Irreducibility)

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

1. $(M_S + M_S) \cap S = \varnothing$*, for* M_S *the set of minimal norm elements.*
2. *For each* $s \in S \setminus M_S$ *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.
- Irreducibility follows by an iterative contradiction argument.
- In 1-dimension, the minimum size of the complement is $\Theta(\log(n))$.

Local Irreducibility Example

Proposition (Local Irreducibility)

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

1. $(M_S + M_S) \cap S = \varnothing$, *for M_S the set of minimal norm elements.*
2. *For each $s \in S \setminus M_S$ there is some $t \in S$ with $|t| < |s|$ and $s + t \notin S$.*

Then, S is irreducible.

Suppose $S = \{0, 1, 3\} = A + B$.

- 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.

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

Local Irreducibility Example

Proposition (Local Irreducibility)

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

1. $(M_S + M_S) \cap S = \varnothing$, *for M_S the set of minimal norm elements.*
2. *For each $s \in S \setminus M_S$ there is some $t \in S$ with $|t| < |s|$ and $s + t \notin S$.*

Then, S is irreducible.

Suppose $S = \{0, 1, 3\} = A + B$.

- 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.

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

Local Irreducibility Example

Proposition (Local Irreducibility)

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

1. $(M_S + M_S) \cap S = \varnothing$, *for M_S the set of minimal norm elements.*
2. *For each $s \in S \setminus M_S$ there is some $t \in S$ with $|t| < |s|$ and $s + t \notin S$.*

Then, S is irreducible.

Suppose $S = \{0, 1, 3\} = A + B$.

- 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.

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

Local Irreducibility Example

Proposition (Local Irreducibility)

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

1. $(M_S + M_S) \cap S = \varnothing$, *for M_S the set of minimal norm elements.*
2. *For each $s \in S \setminus M_S$ there is some $t \in S$ with $|t| < |s|$ and $s + t \notin S$.*

Then, S is irreducible.

Suppose $S = \{0, 1, 3\} = A + B$.

- 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.

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

Local Irreducibility Example

Proposition (Local Irreducibility)

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

1. $(M_S + M_S) \cap S = \varnothing$, *for M_S the set of minimal norm elements.*
2. *For each $s \in S \setminus M_S$ there is some $t \in S$ with $|t| < |s|$ and $s + t \notin S$.*

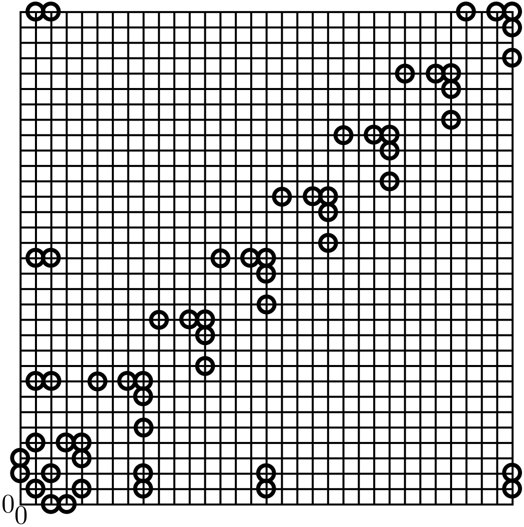
Then, S is irreducible.

Suppose $S = \{0, 1, 3\} = A + B$.

- 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.

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

Constructive upper bound of $O(\sqrt{n})$



$\mathbb{Z}^2_{\geq 0}$ with $\circ$ denoting belonging to the set complement.

Lunar Numbers

- In 2011, David Applegate, Marc LeBrun, and Neil Sloane introduced *Lunar arithmetic* (originally called *Dismal arithmetic*), a system for arithmetic without carries.

Lunar Numbers

- In 2011, David Applegate, Marc LeBrun, and Neil Sloane introduced *Lunar arithmetic* (originally called *Dismal arithmetic*), a system for arithmetic without carries.
- To perform "lunar addition" on single digits, take the larger digit:

$$2 \oplus 6 = 6.$$

Lunar Numbers

- In 2011, David Applegate, Marc LeBrun, and Neil Sloane introduced *Lunar arithmetic* (originally called *Dismal arithmetic*), a system for arithmetic without carries.
- To perform "lunar addition" on single digits, take the larger digit:

$$2 \oplus 6 = 6.$$

- To perform "lunar multiplication" on single digits, take the smaller digit:

$$2 \otimes 6 = 2.$$

Arithmetic Without Carries

When we lunar add or multiply numbers with several digits, we will not have to perform any carries.

Arithmetic Without Carries

When we lunar add or multiply numbers with several digits, we will not have to perform any carries.

Example

$$\begin{array}{cccc} & 6 & 2 & 4 \\ \oplus & 3 & 8 & 1 \\ \hline \end{array}$$

Arithmetic Without Carries

When we lunar add or multiply numbers with several digits, we will not have to perform any carries.

Example

$$\begin{array}{cccc} & 6 & 2 & 4 \\ \oplus & 3 & 8 & 1 \\ \hline = & 6 & 8 & 4 \end{array}$$

Arithmetic Without Carries

When we lunar add or multiply numbers with several digits, we will not have to perform any carries.

Example

$$\begin{array}{cccc} & 6 & 2 & 4 \\ \oplus & 3 & 8 & 1 \\ \hline = & 6 & 8 & 4 \end{array}$$

$$\begin{array}{ccccc} & & 6 & 2 & 4 \\ \otimes & & 3 & 8 & 1 \\ \hline \end{array}$$

Arithmetic Without Carries

When we lunar add or multiply numbers with several digits, we will not have to perform any carries.

Example

$$
\begin{array}{rccc}
 & 6 & 2 & 4 \\
\oplus & 3 & 8 & 1 \\
\hline
= & 6 & 8 & 4
\end{array}
$$

$$
\begin{array}{rccc}
 & 6 & 2 & 4 \\
\otimes & 3 & 8 & 1 \\
\hline
= & 1 & 1 & 1
\end{array}
$$

Arithmetic Without Carries

When we lunar add or multiply numbers with several digits, we will not have to perform any carries.

Example

$$\begin{array}{rccc} & 6 & 2 & 4 \\ \oplus & 3 & 8 & 1 \\ \hline = & 6 & 8 & 4 \end{array}$$

$$\begin{array}{rcccc} & & 6 & 2 & 4 \\ \otimes & & 3 & 8 & 1 \\ \hline = & & 1 & 1 & 1 \\ & 6 & 2 & 4 & \end{array}$$

Arithmetic Without Carries

When we lunar add or multiply numbers with several digits, we will not have to perform any carries.

Example

$$\begin{array}{cccc} & 6 & 2 & 4 \\ \oplus & 3 & 8 & 1 \\ \hline = & 6 & 8 & 4 \end{array}$$

$$\begin{array}{cccccc} & & & 6 & 2 & 4 \\ \otimes & & & 3 & 8 & 1 \\ \hline = & & & 1 & 1 & 1 \\ & & 6 & 2 & 4 & \\ & 3 & 2 & 3 & & \\ \hline \end{array}$$

Arithmetic Without Carries

When we lunar add or multiply numbers with several digits, we will not have to perform any carries.

Example

$$
\begin{array}{rrrr}
 & 6 & 2 & 4 \\
\oplus & 3 & 8 & 1 \\
\hline
= & 6 & 8 & 4
\end{array}
$$

$$
\begin{array}{rrrrrr}
 & & & 6 & 2 & 4 \\
\otimes & & & 3 & 8 & 1 \\
\hline
= & & & 1 & 1 & 1 \\
 & & 6 & 2 & 4 & \\
 & 3 & 2 & 3 & & \\
\hline
= & 3 & 6 & 3 & 4 & 1
\end{array}
$$

Why study Lunar Numbers?

Base 2 numbers correspond to subsets of the natural numbers, with lunar multiplication corresponding to set addition (Gal Gross, 2019).

Why study Lunar Numbers?

Base 2 numbers correspond to subsets of the natural numbers, with lunar multiplication corresponding to set addition (Gal Gross, 2019).

Example

The set $\{0, 1, 3\}$ corresponds to the base 2 number 1101, and $\{0, 2\}$ corresponds to 101.

Why study Lunar Numbers?

Base 2 numbers correspond to subsets of the natural numbers, with lunar multiplication corresponding to set addition (Gal Gross, 2019).

Example

The set $\{0, 1, 3\}$ corresponds to the base 2 number 1101, and $\{0, 2\}$ corresponds to 101. Their lunar product is

$$\begin{array}{ccccccc} & & & 1 & 1 & 0 & 1 \\ \otimes & & & & 1 & 0 & 1 \\ \hline = & 1 & 1 & 1 & 1 & 0 & 1 \end{array}$$

This corresponds to the set $\{0, 1, 2, 3, 5\}$, which is $\{0, 1, 3\} + \{0, 2\}$.

Why study Lunar Numbers?

Base 2 numbers correspond to subsets of the natural numbers, with lunar multiplication corresponding to set addition (Gal Gross, 2019).

Example

The set $\{0,1,3\}$ corresponds to the base 2 number 1101, and $\{0,2\}$ corresponds to 101. Their lunar product is

$$\begin{array}{ccccccc} & & & 1 & 1 & 0 & 1 \\ \otimes & & & & 1 & 0 & 1 \\ \hline = & 1 & 1 & 1 & 1 & 0 & 1 \end{array}$$

This corresponds to the set $\{0,1,2,3,5\}$, which is $\{0,1,3\}+\{0,2\}$.

Lunar multiplication in arbitrary base can thus be thought of as a generalization of set addition.

Lunar Primes

- We say that a lunar number n is *irreducible* if all of its possible (lunar) factorizations include a number containing only one non-zero digit.
    - In the base 2 case, n is irreducible if and only if its corresponding set is irreducible.

Lunar Primes

- We say that a lunar number n is *irreducible* if all of its possible (lunar) factorizations include a number containing only one non-zero digit.
  - In the base 2 case, n is irreducible if and only if its corresponding set is irreducible.
- If n is base b lunar number, we say that n is *prime* if its only possible factorization is $(b-1) \otimes_b n$.
  - $(b-1)$ is the unit for lunar multiplication.

Lunar Primes

- We say that a lunar number n is *irreducible* if all of its possible (lunar) factorizations include a number containing only one non-zero digit.
  - In the base 2 case, n is irreducible if and only if its corresponding set is irreducible.
- If n is base b lunar number, we say that n is *prime* if its only possible factorization is $(b-1) \otimes_b n$.
  - $(b-1)$ is the unit for lunar multiplication.
- A base b lunar number is prime if and only if it is irreducible, contains the digit $b-1$, and has non-zero final digit.
  - We call lunar numbers which contain the digit $b-1$ and have a non-zero final digit *candidates for primality*.

How many Lunar Primes are there?

Theorem (SMALL 2021)

The proportion of base b, length k candidates for primality which are irreducible (and thus prime) tends to 1 as $k \to \infty$.

How many Lunar Primes are there?

Theorem (SMALL 2021)

The proportion of base b, length k candidates for primality which are irreducible (and thus prime) tends to 1 as $k \to \infty$.

- Conjectured by Applegate et al. in their paper on lunar arithmetic.

How many Lunar Primes are there?

Theorem (SMALL 2021)

The proportion of base b, length k candidates for primality which are irreducible (and thus prime) tends to 1 as $k \to \infty$.

- Conjectured by Applegate et al. in their paper on lunar arithmetic.
- The base 2 case was proven in 2014 by Yaroslav Shitov.

How many Lunar Primes are there?

Theorem (SMALL 2021)

The proportion of base b, length k candidates for primality which are irreducible (and thus prime) tends to 1 as $k \to \infty$.

- Conjectured by Applegate et al. in their paper on lunar arithmetic.
- The base 2 case was proven in 2014 by Yaroslav Shitov.
- The $b = 2$ case implies that the proportion of subsets of $\{0, 1, \ldots, k\}$ containing 0 and k which are irreducible tends to 1 as $k \to \infty$.

Lunar Digit Strings

- It is useful to extend our definition of lunar numbers to include possibly infinitely long strings of digits equipped with lunar operations.

Lunar Digit Strings

- It is useful to extend our definition of lunar numbers to include possibly infinitely long strings of digits equipped with lunar operations.
- We call these (possibly infinitely long) strings of digits *lunar digit strings*.

Lunar Digit Strings

- It is useful to extend our definition of lunar numbers to include possibly infinitely long strings of digits equipped with lunar operations.
- We call these (possibly infinitely long) strings of digits *lunar digit strings*.
- In the base 2 case, lunar digit strings correspond to sets with a (possibly infinite) number of elements.

Example

The set of even natural numbers corresponds to the string 101010101....

Asymptotic Irreducibility

Definition

A set $S \subseteq \mathbb{N}$ is ***asymptotically irreducible*** *if adding and removing any finite number of elements of S results in an irreducible set.*

Asymptotic Irreducibility

Definition

A set $S \subseteq \mathbb{N}$ is ***asymptotically irreducible*** *if adding and removing any finite number of elements of S results in an irreducible set.*

Definition

A lunar digit string n is ***asymptotically irreducible*** *if changing any finite number of the digits of n results in an irreducible lunar digit string.*

These definitions correspond in the base 2 case.

Wirsing's Result and our Generalization

Theorem (Eduard Wirsing, 1953)

The proportion of subsets of $\mathbb{N}$ *which are asymptotically irreducible is 1.*

Wirsing's Result and our Generalization

Theorem (Eduard Wirsing, 1953)

The proportion of subsets of $\mathbb{N}$ which are asymptotically irreducible is 1.

- Implies that the proportion of base 2 lunar strings which are asymptotically irreducible is 1.

Wirsing's Result and our Generalization

Theorem (Eduard Wirsing, 1953)

The proportion of subsets of $\mathbb{N}$ *which are asymptotically irreducible is 1.*

- Implies that the proportion of base 2 lunar strings which are asymptotically irreducible is 1.
- Although Wirsing's result far predates lunar numbers, his proof actually relies heavily on the correspondence between sets and base 2 digit strings.

Wirsing's Result and our Generalization

Theorem (Eduard Wirsing, 1953)

The proportion of subsets of $\mathbb{N}$ which are asymptotically irreducible is 1.

- Implies that the proportion of base 2 lunar strings which are asymptotically irreducible is 1.
- Although Wirsing's result far predates lunar numbers, his proof actually relies heavily on the correspondence between sets and base 2 digit strings.

Theorem (SMALL 2021)

For $b \geq 2$, the proportion of base b lunar digit strings which are asymptotically irreducible is 1.

Acknowledgments

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

Special thanks to our co-researchers Ben Baily, Ethan Pesikoff, and Luke Reifenberg, and Professors Leo Goldmakher and Steven J. Miller for their mentorship.

References

- B. Baily, S. Dever, L. Goldmakher, G. Gross, H. Pham, and C. Venkatesh, Large Sets are Sumsets, in preparation.
- D. Applegate, M. LeBrun, N.J.A Sloane, Dismal Arithmetic, *Journal of Integer Sequences*, Vol.14, 2011.
- G. Gross, Maximally additively reducible subsets of the integers, preprint, https://arxiv.org/abs/1908.05220.
- Y. Shitov, How many Boolean polynomials are irreducible?, *International Journal of Algebra and Computation*, 2014.
- E. Wirsing, Ein metrischer Satz über Mengen ganzer Zahlen, *Archiv der Mathematik*, Vol.4, 1953.