On the Goldbach Property for Group Semidomains

Eddy Li, Advaith Mopuri, and Charles Zhang
(Mentor: Harold Polo)

Summer Workshop for Intrepid Mathematicians

15 August 2024

Table of Contents

Notation

General notation used in this talk:

- $\mathbb{N} := \{1, 2, 3, \ldots\}$,
- $\mathbb{N}_0 := \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \ldots\}$,
- $\mathbb{P}$ denotes the set of primes.

Monoids

A pair $(M, +)$ of a set M and a binary operation $(+)$ is a monoid if

- M is closed under $(+)$, and
- $(+)$ is associative, commutative, and exhibits an identity element $e \in M$ such that $m + e = m$ for all $m \in M$.

Examples

- $(\mathbb{N}, \cdot)$ is clearly a monoid because $(\cdot)$ is associative and commutative and has identity 1.
- $(\mathbb{Z}/5\mathbb{Z}, +)$ is not only a monoid but is also closed under additive inverses.

Further, we say that a monoid M is an abelian group when every element of M has an additive inverse.

Monoids

Some monoids have specific properties.

- We say a monoid is <u>cancellative</u> if for $a, b, c \in M$, $a + c = b + c$ implies $a = b$.
- We say a monoid is <u>torsion-free</u> if for $a, b \in M$ and $n \in \mathbb{N}$, $na = nb$ (repeated addition) implies that $a = b$.
- We say a monoid is <u>linearly ordered</u> if there exists a binary relationship $\preceq$ that establishes a total order on M such that $b + d \preceq c + d$ for $b, c, d \in M$ where $b \preceq c$.

Examples

The monoid $(\mathbb{N}_0, +)$ is cancellative, torsion-free, and linearly ordered due to the properties of addition.

Theorem (Levi, 1913)

For a commutative monoid M, the following conditions are equivalent.

- M is cancellative and torsion-free.
- M can be turned into a linearly ordered monoid.

Rings

- A triple $(R, +, \cdot)$ is a ring if
  - $(R, +)$ is an abelian group, and
  - $(R \setminus \{0\}, \cdot)$ is a not necessarily cancellative monoid.
- $\mathbb{Z}, \mathbb{Z}/8\mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$ are all rings.
- A triple $(R, +, \cdot)$ is an integral domain if
  - $(R, +)$ is an abelian group, and
  - $(R \setminus \{0\}, \cdot)$ is a cancellative monoid. In other words, $(R \setminus \{0\}, \cdot)$ has no zero divisors.
- $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are examples of integral domains.
- A triple $(R, +, \cdot)$ is a semiring if
  - $(R, +)$ is a cancellative monoid, and
  - $(R \setminus \{0\}, \cdot)$ is a not necessarily cancellative monoid.
- $(\mathbb{N}_0, +, \cdot)$ is a semiring.
- In particular, we say that a subset R' of a semiring $(R, +, \cdot)$ is a subsemiring if $(R', +, \cdot)$ is a semiring when $+$ and $\cdot$ are restricted to the domain of R'.
- $(\mathbb{N}_0, +, \cdot)$ is a subsemiring of $(\mathbb{Z}, +, \cdot)$.

Semidomains

Definition

A semidomain is a subsemiring of an integral domain.

Throughout our presentation, we will refer to general semidomains as S. One example of a semidomain is $\mathbb{N}_0$. It may be helpful to think about the following definitions in the context of this semidomain.

Certain elements of semidomains have specific properties.

- An element $s \in S$ is an additive atom if $s = a + b$ for $a, b \in S$ implies that at least one of a or b is an additive unit.
- An element $s \in S$ is a multiplicative unit if there exists an $s^{-1} \in S$ such that $ss^{-1} = 1$.
- An element $s \in S$ is a multiplicative atom (multiplicative irreducible) if $s = ab$ for $a, b \in S$ implies that either a or b is a multiplicative unit (and s is also not a multiplicative unit).

We denote the sets of these elements as $\mathscr{A}_+(S)$, $S^\times$, and $\mathscr{A}(S)$, respectively.

Semidomains

There are some properties that the additive monoid of semidomains can satisfy.

- A semidomain S is additively reduced if 0 is the only additively invertible element of S.
- A semidomain S is additively atomic if $(S, +)$ is atomic – that is, every nonunit element is the sum of finitely many additive atoms.
- A semidomain S is additively Furstenberg if $(S, +)$ is Furstenberg – that is, every nonunit element is divisible by at least one additive atom.

Examples

- $\mathbb{N}_0$ is a semidomain with $\mathscr{A}_+(S) = \{1\}$, $S^\times = \{1\}$, and $\mathscr{A}(S) = \mathbb{P}$. Further, $\mathbb{N}_0$ is additively reduced, additively atomic, and additively Furstenberg.
- $\mathbb{N}_0[x^{\pm 1}]$ is a semidomain with $\mathscr{A}_+(S) = S^\times = \{x^k \mid k \in \mathbb{Z}\}$, while $\mathscr{A}(S)$ is very complicated. Further, $\mathbb{N}_0[x^{\pm 1}]$ is additively reduced, additively atomic, and additively Furstenberg.

History

- The Goldbach conjecture was initially presented in a letter from Christian Goldbach to Leonhard Euler in 1742. In modern terms, it hypothesizes that every even integer greater than 2 can be expressed as the sum of two positive prime numbers.
- This conjecture has yet to be proven, but progress has been made on analogues of the problem in different domains.
- The first such analogue was developed by Hayes (1965) on $\mathbb{Z}[x^{\pm 1}]$.
- Later, Pollack (2011) extended Hayes's result from $\mathbb{Z}$ to Noetherian rings with infinitely many maximal ideals.

History

- More recently, Liao and Polo (2023) have shown an analogue of the Goldbach conjecture over $\mathbb{N}_0[x^{\pm 1}]$.
- Kaplan and Polo (2024) have extended this result to more general additively atomic semidomains S satisfying $\mathscr{A}_+(S) = S^\times$.

Most of the work concerning variations of the Goldbach conjecture for polynomials has so far been focused on the possible coefficients for the polynomials.

For this talk, we concern ourselves with conjecture in the context of group semidomains, rather than just Laurent polynomial semidomains.

Liao and Polo

To begin, we properly define $\mathbb{N}_0[x^{\pm 1}]$ as

$$\mathbb{N}_0[x^{\pm 1}] = \left\{ \sum_{i=0}^{n} c_i x^{k_i} \;\middle|\; c_i \in \mathbb{N}_0, k_i \in \mathbb{Z} \right\}.$$

Liao and Polo showed the following theorem for $\mathbb{N}_0[x^{\pm 1}]$.

Theorem (Liao–Polo, 2023)

Every polynomial $f \in \mathbb{N}_0[x^{\pm 1}]$ such that $f(1) > 3$ and $|\mathrm{supp}(f)| > 1$ can be written as the sum of two irreducibles.

For example, let us consider decomposing the Laurent polynomial

$$f = 6x^7 + 3x^4 + 4x^3 + 7x + 5x^{-1} + 3x^{-4} + 8x^{-6}$$

into the sum of irreducible Laurent polynomials.

Liao and Polo

We begin by splitting f into hyper-monolithic summands as shown below:

$$f = 6x^7 + 3x^4 + 4x^3 + 7x + 5x^{-1} + 3x^{-4} + 8x^{-6}.$$

Here, we have $f = g + h$, where

$$g = 3x^4 + 4x^3 + 5x^{-1}$$

and

$$h = 6x^7 + 7x + 3x^{-4} + 8x^{-6}.$$

Next, we strategically move terms (or parts of terms) from h to g. The goal of this is to make g irreducible by making its coefficients sum to a prime.

Additionally, we also ensure that h stays irreducible by maintaining its hyper-monolithicity and making sure its coefficients are relatively prime.

Liao and Polo

In this case, we split h as

$$6x^7 + 7x + 3x^{-4} + (1 + 7)x^{-6}$$

so that our final values for g and h are

$$g = 3x^4 + 4x^3 + 5x^{-1} + x^{-6}$$

and

$$h = 6x^7 + 7x + 3x^{-4} + 7x^{-6}.$$

In particular, note how the coefficients of g sum to 13, a prime number.

Kaplan and Polo

- Kaplan and Polo extend the theorem shown by Liao and Polo into Laurent polynomial semidomains $S[x^{\pm 1}]$:

$$S[x^{\pm 1}] = \left\{ \sum_{i=0}^{n} s_i x^{k_i} \;\middle|\; s_i \in S, k_i \in \mathbb{Z} \right\}$$

- The proof by Liao and Polo which resolves $\mathbb{N}_0[x^{\pm 1}]$ does not apply generally to $S[x^{\pm 1}]$ due to requiring specific properties of the multiplicative irreducibles of $\mathbb{N}_0$, and thus would require properties for them in S.

Kaplan and Polo

- Instead, they explictly decompose polynomials of $S[x^{\pm 1}]$ in a wholly different way from Liao and Polo. In particular, in the case of $\mathbb{N}_0[x^{\pm 1}]$ for sake of example, they show that if one splits the following polynomial

$$6x^7 + 3x^4 + 4x^3 + 7x + 5x^{-1} + 3x^{-4} + 8x^{-6}$$

  into the following two polynomials,

$$\begin{aligned} &1x^7 + && + 5x^{-1} + 3x^{-4} + 7x^{-6} \text{ and} \\ &5x^7 + 3x^4 + 4x^3 + 7x && + 1x^{-6}, \end{aligned}$$

  that both of these are irreducible.
- Note this no longer requires knowledge of the multiplicative irreducibles of S.

Kaplan and Polo

Eddy Li, Advaith Mopuri, and Charles Zhang
(Mentor: Harold Polo)

Theorem (Kaplan–Polo, 2023)

Let S be an additively reduced and additively atomic semidomain. The following statements are equivalent.

1. $\mathscr{A}_+(S) = S^\times$.
2. Every $f \in S[x^{\pm 1}]$ with $|\mathrm{supp}(f)| > 1$ can be expressed as the sum of at most 2 irreducibles.
3. There exists $k \in \mathbb{N}$ such that every $f \in S[x^{\pm 1}]$ with $|\mathrm{supp}(f)| > 1$ can be expressed as the sum of at most k irreducibles.

Moreover, if any of the previous statements hold and $f \in S[x^{\pm 1}]$ does not have one of the following forms:

(a) $f = ax^{k_0} + bx^{k_1}$, where either $a \in S^\times$ or $b \in S^\times$, or

(b) $f = ax^{k_0} + bx^{k_1} + cx^{k_2}$, where $a, b, c \in S^\times$,

then f is the sum of exactly two irreducible polynomials in $S[x^{\pm 1}]$.

Group Semidomains

Eddy Li, Advaith Mopuri, and Charles Zhang
(Mentor: Harold Polo)

Definition

Let M be a cancellative and torsion-free monoid. We define the monoid semidomain $S[M]$ as containing all polynomial expressions of the form

$$f(x) = \sum_{i=0}^{n} s_i x^{m_i}$$

such that

- $\{s_i \mid 0 \leq i \leq n\} \subseteq S$,
- $\{m_i \mid 0 \leq i \leq n\} \subseteq M$, and
- $m_i < m_{i+1}$ for $0 \leq i \leq n$,

In particular, a group semidomain is a monoid semidomain $S[M]$ in which M is a group. We denote such semidomains as $S[G]$.

Group Semidomains

Examples

- Laurent polynomial semidomains are group semidomains with $S[x^{\pm 1}] = S[\mathbb{Z}]$.
- $\mathbb{N}_0[\mathbb{Q}]$ is a group semidomain because $\mathbb{Q}$ is a cancellative and torsion-free group.
- A Jones polynomial $V_L(x)$ of a link $L \in S^3$ can be expressed as a Laurent polynomial in $\sqrt{x}$ with integer coefficients. Thus, for all links L, we have $V_L(x) \in \mathbb{Z}[\frac{\mathbb{Z}}{2}]$.

Non-Example

- The domain $\mathbb{N}_0[(\mathbb{Z}/5\mathbb{Z}, +)]$ is not a group semidomain because $(\mathbb{Z}/5\mathbb{Z}, +)$, the group of integers modulo 5 under addition, is not torsion-free.

Group Semidomains

Definition

For any $f = \sum_{i=0}^{n} s_i x^{g_i} \in S[G]$, define its support $\operatorname{supp}(f)$ as

$$\operatorname{supp}(f) := \{g_i \mid s_i \neq 0, 0 \leq i \leq n\}.$$

For all $f \in S[G]$, f has $|\operatorname{supp}(f)|$ terms.

Definition

For any $f \in S[G]$, we say that f is monolithic if having $f = gh$ for $g, h \in S[G]$ implies that at least one of g and h is a monomial.

Group Semidomains

Examples

In $\mathbb{N}_0[x^{\pm 1}]$, the polynomial

$$f = 1 + x + 2x^2 + x^4$$

is irreducible and has $\operatorname{supp}(f) = \{0, 1, 2, 4\}$. Meanwhile

$$2f = 2 + 2x + 4x^2 + 2x^4$$

is monolithic but not irreducible, as we may write $2f = 2(1 + x + 2x^2 + x^4)$ and neither 2 nor $1 + x + 2x^2 + x^4$ are multiplicative units. Note that we still have $\operatorname{supp}(f) = \operatorname{supp}(2f) = \{0, 1, 2, 4\}$.

Our First Main Result

Eddy Li, Advaith Mopuri, and Charles Zhang
(Mentor: Harold Polo)

Theorem (L–M–Z, 202?)

Let S be an additively reduced and additively Furstenberg semidomain. The following statements are equivalent.

1. $\mathscr{A}_+(S) = S^\times$.
2. Every $f \in S[G]$ with $|\mathrm{supp}(f)| > 1$ can be expressed as the sum of at most two irreducibles.
3. There exists $k \in \mathbb{N}$ such that every $f \in S[G]$ with $|\mathrm{supp}(f)| > 1$ can be expressed as the sum of at most k irreducibles.

Moreover, if any of the previous statements hold and $f \in S[G]$ is not of one of the following forms:

(a) $f = s_0 x^{g_0} + s_1 x^{g_1}$, where either $s_0 \in S^\times$ or $s_1 \in S^\times$, or

(b) $f = s_0 x^{g_0} + s_1 x^{g_1} + s_2 x^{g_2}$, where either $s_0, s_1, s_2 \in S^\times$,

then f can be decomposed into exactly two irreducible summands in $S[G]$.

Group Series Semidomains

Definition

Let M be a cancellative and torsion-free monoid. We define the monoid series semidomain $S[\![M]\!]$ as containing all series of the form

$$f(x) = \sum_{i=0}^{\infty} s_i x^{m_i}$$

such that

- $\{s_i \mid i \in \mathbb{N}_0\} \subseteq S$,
- $\{m_i \mid i \in \mathbb{N}_0\} \subseteq M$,
- $m_i < m_{i+1}$ for all $i \in \mathbb{N}_0$, and
- $\{m_i \mid i \in \mathbb{N}_0\} \cap \{m \in M \mid m < 0\}$ is finite.

In particular, a group series semidomain is a monoid series semidomain $S[\![M]\!]$ in which M is a group. We denote such semidomains as $S[\![G]\!]$.

Group Series Semidomains

Examples

- For all semidomains S and torsion-free abelian groups G, note the inclusion $S[G] \subset S[\![G]\!]$.
  - If S is additively reduced, then $S[G]$ is a divisor-closed subsemidomain of $S[\![G]\!]$.
  - The above may not be true if S is not additively reduced. For instance, $(1-x)(\sum_{i=0}^{\infty} x^i) = 1$ in $\mathbb{Z}[\![\mathbb{Z}]\!]$.
- Laurent series semidomains are group series semidomains with $G = \mathbb{Z}$, since $S[\![x^{\pm 1}]\!] = S[\![\mathbb{Z}]\!]$.
- By Laurent's Theorem, any analytic function $f : \mathbb{C} \setminus \{0\} \to \mathbb{C}$ can be represented as a series $p \in \mathbb{C}[\![x^{\pm 1}]\!] = \mathbb{C}[\![\mathbb{Z}]\!]$.
- The multivariate Laurent series semidomain $S[\![x_1^{\pm 1}, x_2^{\pm 1}, \dots, x_n^{\pm 1}]\!]$ is isomorphic to the group series semidomain $S[\![\mathbb{Z}^n]\!]$ via the mapping

$$\varphi\left(\sum_{i=0}^{\infty} s_i x_1^{a_{i1}} x_2^{a_{i2}} \dots x_n^{a_{in}}\right) := \sum_{i=0}^{\infty} s_i x^{(a_{i1}, a_{i2}, \dots, a_{in})}.$$

Group Series Semidomains

Definition

For any $f = \sum_{i=0}^{\infty} s_i x^{g_i} \in S[\![G]\!]$, define its support $\operatorname{supp}(f)$ as

$$\operatorname{supp}(f) := \{g_i \mid s_i \neq 0, i \in \mathbb{N}_0\}.$$

The series f has $|\operatorname{supp}(f)|$ terms.

Definition

For any $f \in S[\![G]\!]$, we say that f is monolithic if having $f = gh$ for $g, h \in S[\![G]\!]$ implies that at least one of g and h is a monomial.

Group Series Semidomains

Examples

- In $\mathbb{N}_0[\![x^{\pm 1}]\!]$, the series

$$f = \sum_{i=0}^{\infty} x^{2^i} = 1 + x + x^2 + x^4 + x^8 + \dots$$

  is irreducible and has $\mathrm{supp}(f) = \{0, 1, 2, 4, 8, \dots\}$, while

$$2f = 2\sum_{i=0}^{\infty} x^{2^i} = 2 + 2x + 2x^2 + 2x^4 + 2x^8 + \dots$$

  is monolithic but not irreducible with $\mathrm{supp}(f) = \mathrm{supp}(2f)$.
- If S is additively reduced, any monolithic $f \in S[G]$ is automatically monolithic in $S[\![G]\!]$.

Generalizing from Laurent Series

Eddy Li, Advaith Mopuri, and Charles Zhang
(Mentor: Harold Polo)

Theorem (Kaplan–Polo, 2024)

Let S be an additively reduced and additively atomic semidomain. The following statements are equivalent.

1. $\mathscr{A}_+(S) = S^\times$.
2. Every $f \in S[\![x^{\pm 1}]\!]$ with $|\text{supp}(f)| > 1$ can be expressed as the sum of at most 3 irreducibles.
3. There exists $k \in \mathbb{N}$ such that every $f \in S[\![x^{\pm 1}]\!]$ with $|\text{supp}(f)| > 1$ can be expressed as the sum of at most k irreducibles.

Can we generalize the above from $S[\![x^{\pm 1}]\!]$ onto $S[\![G]\!]$ for certain torsion-free abelian groups G?

Generalizing from Laurent Series

Fixing any additively reduced and additively Furstenberg semidomain S, we observe the following.

- If S satisfies $\mathscr{A}_+(S) = S^\times$, then $\mathscr{A}_+(S[\![\mathbb{Z}]\!]) = (S[\![\mathbb{Z}]\!])^\times$.
- For any $n \in \mathbb{N}$, the map φ given by

$$\varphi\left(\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} s_j x^{(a_{ij1}, a_{ij2}, \dots, a_{ijn})}\right) x^{k_i}\right) = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} s_j x^{(a_{ij1}, a_{ij2}, \dots, a_{ijn}, k_i)}$$

  entails a semidomain isomorphism $(S[\![\mathbb{Z}^n]\!])[\![\mathbb{Z}]\!] \cong S[\![\mathbb{Z}^{n+1}]\!]$.
- Inducting on n by repeatedly combining the previous theorem with the above observations allows for the extension of weak Goldbach for group series semidomains from $S[\![\mathbb{Z}]\!] = S[\![x^{\pm 1}]\!]$ to $S[\![\mathbb{Z}^n]\!]$ for general $n \in \mathbb{N}$.
- By folklore, any finitely-generated torsion-free abelian group G is isomorphic to $\mathbb{Z}^n$ for some n.

Our Second Main Result

We therefore arrive at our second major result.

Theorem (L–M–Z, 202?)

Let S be an additively reduced and additively Furstenberg semidomain. Let G be a finitely-generated torsion-free abelian group. The following are equivalent.

1. $\mathscr{A}_+(S) = S^\times$.
2. Every $f \in S[\![G]\!]$ with $|\mathrm{supp}(f)| > 1$ can be expressed as the sum of at most 3 irreducibles.
3. There exists $k \in \mathbb{N}$ such that every $f \in S[\![G]\!]$ with $|\mathrm{supp}(f)| > 1$ can be expressed as the sum of at most k irreducibles.

Does the analogous result hold for groups G that are not finitely-generated?

It Doesn't Work!

We don't know yet.

The key ingredient in proving the previous result is that any strictly increasing sequence in $\mathbb{Z}$ must be unbounded. However, this does not generalize to all torsion-free abelian groups G that are not finitely-generated.

Example

For $G \in \{\mathbb{Q}, \mathbb{R}\}$, the sequence $(\frac{2^n-1}{2^n})_{n\in\mathbb{N}}$ increases but is strictly bounded in the interval $(0, 1)$.

Observe that both $\mathbb{Q}$ and $\mathbb{R}$ are not finitely-generated.

It Doesn't Work!

Open Question

Let S be an additively reduced and additively Furstenberg semidomain. Let G be a torsion-free abelian group. Can we decompose every $f \in S[\![G]\!]$ with $|\mathrm{supp}(f)| > 1$ as the sum of at most 3 irreducibles when

(a) $G = \mathbb{Q}$?

(b) $G = \mathbb{R}$?

Furstenbergness and Atomicity

- S is additively atomic if $(S, +)$ is atomic, so that all nonunit elements $s \in S$ can additively be factorized into atoms.
- S is additively Furstenberg if $(S, +)$ is Furstenberg, so that all nonunit elements $s \in S$ has some atom $a \in \mathscr{A}_+(S)$ additively dividing it.

Additive atomicity automatically implies Additive Furstenbergness, but are they truly different criteria?

- A construction of Lin–Rabinovitz–Zhang yields a monoid that is Furstenberg but not atomic.
- Constructions of Gotti–Polo and Fox–Goel–Liao yield semidomains that are multiplicatively Furstenberg but not multiplicatively atomic.

The above suggests that additive Furstenbergness would be strictly weaker than additive atomicity. However, this is only intuition, rather than rigorous proof.

Concluding Remarks on Furstenbergness

We construct an infinite class of semidomains which are additively Furstenberg but not additively atomic.

Proposition (L–M–Z, 202?)

For primes $p, q \in \mathbb{P}_{\geq 3}$ satisfying $\frac{q}{p} > \frac{1+\sqrt{5}}{2}$, set

$$(\kappa_{p,q}, \lambda_{p,q}) := \left(\frac{q}{p+q}, \frac{q^2}{p^2 + pq} \right).$$

Then the semidomain $S_{p,q} := \mathbb{N}_0 \left[\kappa_{p,q}, \lambda_{p,q} \right]$ is additively Furstenberg but not additively atomic. In particular, $\mathscr{A}_+(S_{p,q}) = \{\kappa_{p,q}^n : n \in \mathbb{N}_0\}$.

Examples

$S_{3,5} = \mathbb{N}_0[\frac{5}{8}, \frac{25}{24}]$ and $S_{7,13} = \mathbb{N}_0[\frac{13}{20}, \frac{169}{140}]$ are additively Furstenberg but not additively atomic. Observe that p and q can become arbitrarily large. For example, putting $S_{457,977} = \mathbb{N}_0[\frac{977}{1434}, \frac{954529}{655338}]$ works too.

References

H. Fox, A. Goel, and S. Liao: *Arithmetic of Semisubtractive Semidomains*, arXiv:https://arxiv.org/pdf/2311.07060.

F. Gotti and H. Polo: *On the arithmetic of polynomial semidomains*, Forum Math. (2023) **35** 1179–1197.

D. R. Hayes: *A Goldbach theorem for polynomials with integral coefficients*, Amer. Math. Monthly **72** (1965) 45–46.

N. Kaplan and H. Polo: *A Goldbach theorem for Laurent series semidomains*, arXiv:https://arxiv.org/abs/2312.14888.

S. Liao and H. Polo: *A Goldbach theorem for Laurent polynomials with positive integer coefficients*, Amer. Math. Monthly (to appear).

A. Lin, H. Rabinovitz, and Q. Zhang: *The Furstenberg property in Puiseux monoids*, arXiv:https://arxiv.org/abs/2309.12372.

End of Presentation

THANK YOU!