CrowdMath 2023: Minkowski Sum and Power Monoids

Easton Singer

Harvard University

2023 Summer Workshop on Factorization Theory

September 6, 2023

Outline

General Notation and Definitions

- $\mathbb{N} := \{1, 2, 3, \ldots\}$.
- $\mathbb{N}_0 := \{0\} \cup \mathbb{N} = \{0, 1, 2, \ldots\}$, which we will treat as a monoid with the operation of addition.
- Speaking of which, a monoid is a pair $(M, +)$ which satisfies the following axioms:
  - $a + (b + c) = (a + b) + c$ for all $a, b, c \in M$ (associativity).
  - $a + b = b + a$ for all $a, b \in M$ (commutativity).
  - There exists an element $0 \in M$ such that $a + 0 = 0 + a = a$ for all $a \in M$ (identity).
- Given a monoid $(M, +)$, a submonoid of $(M, +)$ is a monoid $(M', +)$ where M' is a subset of M that contains the identity of M, and M' is closed under the operation "$+$" as inherited from M.

Note: From now on, we will simply represent the monoid $(M, +)$ by M.

- For a monoid M, we will use $\mathcal{U}(M)$ to denote the set of invertible elements (or units) of M.

Note: All monoids in this talk will be written additively.

General Notation and Definitions cont.

Recall:

- In a monoid M, an element $a \in M$ is considered an atom if $a \notin \mathcal{U}(M)$ and $b + c = a$ implies that either $b \in \mathcal{U}(M)$ or $c \in \mathcal{U}(M)$.
- An element $a \in M$ is said to be atomic if it is either invertible or can be written as a finite sum of atoms. Such a decomposition is called a factorization.
- The monoid M itself is called atomic if every element of M is atomic.
- Furthermore, if M is atomic and every non-invertible element of M has a unique factorization into atoms (up to reordering and multiplication by units), then M is called a unique factorization monoid, or UFM.

Note: We will use $\mathcal{A}(M)$ to denote the set of atoms of M.

Here are some simple **examples**:

- The monoid $M = \mathbb{N}_0$ under addition has $\mathcal{U}(M) = \{0\}$ and $\mathcal{A}(M) = \{1\}$. It is easy to check that M is atomic and that M is a UFM.
- The monoid $M = \mathbb{N}_0 \setminus \{1\}$ is also a monoid under addition, but here, $\mathcal{U}(M) = \{0\}$ and $\mathcal{A}(M) = \{2, 3\}$. M is atomic but not a UFM, since $6 = 3 + 3 = 2 + 2 + 2$.

Introducing Power Monoids

For the following definitions, let M be any monoid.

- We will write $\mathcal{P}_{\mathrm{fin}}(M)$ and $\mathcal{P}_{\mathrm{fin},\times}(M)$ to denote the power monoid and restricted power monoid of M, respectively.
- The elements of $\mathcal{P}_{\mathrm{fin}}(M)$ are all nonempty finite subsets of M.
- The monoid operation on elements of $\mathcal{P}_{\mathrm{fin}}(M)$ is referred to as the Minkowski sum (written $+$) and is defined as follows:

$$A + B = \{a + b \mid a \in A, b \in B\}.$$

- $\mathcal{P}_{\mathrm{fin},\times}(M)$ is the submonoid of $\mathcal{P}_{\mathrm{fin}}(M)$ consisting only of the nonempty finite subsets of M which contain at least one invertible element of M.
  - In the special case where M is a reduced monoid (a monoid in which the only invertible element is the identity), the elements of $\mathcal{P}_{\mathrm{fin},\times}(M)$ are exactly all finite subsets of M containing the identity of M.

Today's Main Course: $\mathcal{P}_{\text{fin},0}(\mathbb{N}_0)$

Note: We will write $\mathcal{P}_{\text{fin},0}(\mathbb{N}_0)$ instead of $\mathcal{P}_{\text{fin},\times}(\mathbb{N}_0)$ to denote the restricted power monoid of $\mathbb{N}_0$.

Examples of elements in $\mathcal{P}_{\text{fin},0}(\mathbb{N}_0)$ include the following sets:

$$\{0\}, \{0,2\}, \{0,1,3\}, \{0,2,4\}, \{0,1000,1001,2000,2001\}.$$

To illustrate the Minkowski sum in a concrete example, we see that

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

We can make the following observations:

- Since the only invertible element of $\mathbb{N}_0$ is the identity, 0, the monoid $\mathcal{P}_{\text{fin},0}(\mathbb{N}_0)$ contains all finite sets of nonnegative integers including 0.
- $\{0\}$ is the identity of $\mathcal{P}_{\text{fin},0}(\mathbb{N}_0)$.
- Furthermore, it is easy to show that there are no invertible elements other than the identity, so $\mathcal{U}(\mathcal{P}_{\text{fin},0}(\mathbb{N}_0)) = \{\{0\}\}$.
- It is also not too difficult to show that $\mathcal{P}_{\text{fin},0}(\mathbb{N}_0)$ is an atomic monoid.

Some More Structural Observations

- One strange property (or non-property) of $\mathcal{P}_{\text{fin},0}(\mathbb{N}_0)$ is that it is not cancellative: in other words, $A + C = B + C$ does NOT imply $A = B$.
- For example, $\{0, 2\} + \{0, 1\} = \{0, 1, 2, 3\} = \{0, 1, 2\} + \{0, 1\}$.

Corollary: $\mathcal{P}_{\text{fin},0}(\mathbb{N}_0)$ is not a UFM.

- By the previous example, we have $\{0, 2\} + \{0, 1\}$ as one factorization of $\{0, 1, 2, 3\}$ and $\{0, 1\} + \{0, 1\} + \{0, 1\}$ as another distinct factorization (we will prove later that $\{0, 2\}$ and $\{0, 1\}$ are in fact both atoms).
- One might expect the atoms of $\mathcal{P}_{\text{fin},0}(\mathbb{N}_0)$ to follow some simple pattern, but they have so far eluded any succinct description. Here are all of the atoms of $\mathcal{P}_{\text{fin},0}(\mathbb{N}_0)$ with maximum element at most 4:

$$\{0, 1\}, \{0, 2\}, \{0, 3\}, \{0, 4\}, \{0, 1, 3\}, \{0, 2, 3\},$$
$$\{0, 1, 4\}, \{0, 3, 4\}, \{0, 1, 2, 4\}, \{0, 2, 3, 4\}.$$

A Basic Class of Atoms in $\mathcal{P}_{\text{fin},0}(\mathbb{N}_0)$

While it can be difficult to determine if an arbitrary set in $\mathcal{P}_{\text{fin},0}(\mathbb{N}_0)$ is an atom or not, we can find a number of infinite classes of atoms.

Proposition (easy to prove)

For any positive integer $m \geq 1$, the set $\{0, m\}$ is an atom in $\mathcal{P}_{fin,0}(\mathbb{N}_0)$.

Proof:

- Suppose $B + C = \{0, m\}$ for some $B, C \neq \{0\}$.
- Then, there exist positive integers $b \in B \setminus \{0\}$ and $c \in C \setminus \{0\}$.
- However, we see that $0 + 0, b + 0$, and $b + c$ are all distinct numbers that are contained in $B + C$.
- Therefore, $|B + C| \geq 3$, but $|B + C| = |\{0, m\}| = 2$, so this is a contradiction. □

The idea of considering distinct numbers that are contained in a Minkowski sum gives us a much more general result that is useful to remember.

Theorem (easy to show)

If $A, B \in \mathcal{P}_{fin,0}(\mathbb{N}_0)$ are any sets, then $|A + B| \geq |A| + |B| - 1$.

Counting Atoms

In $\mathcal{P}_{\text{fin},0}(\mathbb{N}_0)$, we are motivated to find a way to count the number of atoms with certain properties. This turns our focus a little bit from algebra to combinatorics, which we can apply to get some interesting results.

Most of the rest of this presentation will be concerned with the following definitions:

$$S_{n,k} := \{S \in \mathcal{P}_{\text{fin},0}(\mathbb{N}_0) \mid \max S \leq n \text{ and } |S| = k\}.$$
$$A_{n,k} := \{A \in S_{n,k} \mid A \text{ is an atom.}\}.$$
$$\alpha_{n,k} := |A_{n,k}|.$$

- We claim that $|S_{n,k}| = \binom{n}{k-1}$, and that the set is nonempty when $1 \leq k \leq n+1$.
- This is because to obtain an arbitrary element in $S_{n,k}$, we must select $k-1$ positive integers from 1 to n and then append 0.

It's worth noting here that although we don't necessarily expect a simple closed form expression for $\alpha_{n,k}$, we can still ask and surprisingly answer some questions about the sequence $\alpha_{n,k}$ as a whole.

The Two Dimensional Sequence $\alpha_{n,k}$

$n=0$:	0						
$n=1$:	0	1					
$n=2$:	0	2	0				
$n=3$:	0	3	2	0			
$n=4$:	0	4	4	2	0		
$n=5$:	0	5	8	6	0	0	
$n=6$:	0	6	12	14	6	0	0

Table: First few rows of $\alpha_{n,k}$

- When we write the numbers $\alpha_{n,k}$ in a Pascal's triangle-like arrangement, we immediately see some similarities and differences between the two sequences.
- Since we know that $|S_{n,k}| = \binom{n}{k-1}$ and $A_{n,k} \subseteq S_{n,k}$, it's clear that $\alpha_{n,k} \leq \binom{n}{k-1}$, so all entries in this triangle are at most equal to the corresponding entry in Pascal's triangle.

Down+Right Diagonals

- In Pascal's triangle, the diagonals going down and to the right and the diagonals going down and to the left are the same (the table is centrally symmetric).
- But for the sequence $\alpha_{n,k}$, we'll see that the behavior of the two types of diagonals could not be more different.
- One of the first results of this year's CrowdMath project was the following theorem about the diagonals going down and right:

Theorem (CrowdMath 2023)

For any $k \in \{-1\} \cup \mathbb{N}_0$, there exists a positive integer N such that for all $n > N$, $\alpha_{n,n-k} = 0$ holds.

- Intuitively, this result says that if we "remove" a fixed number, $k+1$, elements from the set $\{0, 1, 2, \ldots, n\}$, then if we choose n large enough, no matter which elements are removed, the left over set will never be an atom (i.e. it will have enough structure that it can be decomposed as a nontrivial Minkowski sum).

The Example of k = 0

Let's see an actual example of this theorem in action, where we consider the numbers $\alpha_{n,n}$ ($k = 0$ in the theorem statement).

Proposition (easy to prove)

$\alpha_{n,n} = 0$ *if and only if* $n = 1$ *or* $n \geq 5$.

Proof:

- It's easy to check that $\alpha_{1,1} = 0$ and $\alpha_{2,2} = \alpha_{3,3} = \alpha_{4,4} = 2$.
- For example, $\alpha_{4,4} = 2$ because the two sets $\{0, 1, 2, 4\}$ and $\{0, 2, 3, 4\}$ are atoms.
- Now, suppose $n \geq 5$, and consider $S_{n,n}$ as consisting of all sets of the form $\{0, 1, 2, \ldots, n\} \setminus \{i\}$ for $1 \leq i \leq n$.
  - Case 1: $i = n$. $\{0, 1, 2, \ldots, n-1\} = \{0, 1\} + \{0, 1, \ldots, n-2\}$, so this is not an atom.
  - Case 2: $1 < i < n-1$. Here, we see that $\{0, 1, \ldots, i-1, i+1, \ldots, n\} = \{0, 1\} + \{0, 1, \ldots, i-2, i+1, \ldots, n-1\}$.
  - Case 3: $i = 1$ or $i = n-1$. We'll see the decomposition for $i = 1$ here: $\{0, 2, 3, \ldots, n\} = \{0, 2\} + \{0, 2, 3, \ldots, n-2\}$, which is where we use the requirement that $n \geq 5$.

□

Down+Left Diagonals

Question

The previous theorem concerned the numbers $\alpha_{n,n-k}$ for fixed k. What can we say about the numbers $\alpha_{n,k}$ for fixed k?

- Interestingly, in the case of "sparse" sets (where n is significantly greater than k), nearly every set *is* an atom.
- Specifically, we have this result:

Theorem (CrowdMath 2023)

For any $k \in \mathbb{N}_{\geq 2}$, the following limit holds:

$$\lim_{n \to \infty} \frac{\alpha_{n,k}}{\binom{n}{k-1}} = 1.$$

- The proof of this theorem makes heavy use of the inequality stated before that $|A + B| \geq |A| + |B| - 1$, which allows us to get a strong upper bound on the number of non-atoms in $S_{n,k}$.
- Then, we can show that the proportion of non-atoms in $S_{n,k}$ goes to zero, so the proportion of atoms must approach 1 as n goes to ∞.

Open Questions Page 1

- The study of the numbers $\alpha_{n,k}$ is relatively new, and thus there are many interesting questions we can propose seeing the results we've talked about today.
- For example, we can ask some direct follow-up quantitative questions to the "diagonal" observations, such as the following:

Question

We know that for all $k \in \{-1\} \cup \mathbb{N}_0$*, there exists an* N *such that for all* $n > N$*,* $\alpha_{n,n-k} = 0$*. For a given* k*, what is the smallest such* N *for which this holds?*

- Our proof of the first result gives a particular N for which the statement holds, which is $2^{\binom{k+1}{2}+(k+1)+2}$, but we expect that smaller values of N should be achievable.

Question

We know that for all $k \geq 2 \in \mathbb{N}$, $\lim_{n\to\infty} \frac{\alpha_{n,k}}{\binom{n}{k-1}} = 1$*. Could we prove a stronger statement like* $1 - F(n) \leq \frac{\alpha_{n,k}}{\binom{n}{k-1}} \leq 1$ *for all* n*, for some natural function* F *satisfying* $\lim_{n\to\infty} F(n) = 0$*?*

- Leaving the diagonal behavior behind, we can also ask questions about the center of the triangle, such as the following:

Question

Recall that $0 \le \alpha_{2n,n+1} \le \binom{2n}{n}$. *To which side does this lean, and can we describe in any reasonably interesting way the behavior of* $\alpha_{2n,n+1}$ *as n goes to infinity?*

- Similarly, we may wonder about the behavior of entire rows of the triangle.
- Define $A_n := \bigcup_{k=1}^{n+1} A_{n,k}$ and $\alpha_n := |A_n| = \sum_{k=1}^{n+1} \alpha_{n,k}$ for any n.

Recall: $|S_{n,k}| = \binom{n}{k-1}$, so $\sum_{k=1}^{n+1} |S_{n,k}| = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$.

Conjecture (Gotti 2023)

$$\lim_{n\to\infty} \frac{\alpha_n}{2^n} \text{ exists and equals } 1.$$

Open Questions Page 3

- This year's CrowdMath project was largely motivated by one open problem, which we will look at now. It was actually work towards this result that led to the theorems we discussed previously.
- In general, we say that a sequence $a_1, a_2, \ldots, a_n$ of real numbers is unimodal if there exists $1 \leq t \leq n$ such that $a_1 \leq a_2 \leq \cdots \leq a_t$ and $a_t \geq a_{t+1} \geq \cdots \geq a_n$.
- For example, the sequence $1, 2, 3, 4, 4$ is unimodal, but the sequence $1, 2, 3, 2, 5$ is not.
- Also, many famous sequences in combinatorics and elsewhere in mathematics are unimodal, including the rows of Pascal's triangle (each row is unimodal).

Question

Is it true that for any n, the following sequence is unimodal?

$$\alpha_{n,1}, \alpha_{n,2}, \ldots, \alpha_{n,n+1}.$$

Definitions of Atomic-Related Properties

Recall: A monoid is atomic if every element of the monoid is atomic, which means it is either invertible or has a factorization into atoms.

Now, we will define a few related terms that we will need.

- A Puiseux monoid is any submonoid of $\mathbb{Q}_{\geq 0}$, the monoid consisting of nonnegative rational numbers under addition.
- Given a nonempty subset N of a monoid M, we say that d is a maximal common divisor of N if the following conditions hold:
  - $d \mid n$ for all $n \in N$ (d is a common divisor of N).
  - For all $c \in M$ that are common divisors of N, $d \mid c$ only if $c = d + u$ for some unit $u \in \mathcal{U}(M)$.
- We call a monoid M an MCD monoid if every nonempty subset $N \subset M$ has a maximal common divisor (MCD).
- A monoid M is called almost atomic if for every non-invertible element $b \in M$, there exists an atomic element $c \in M$ such that $b + c$ has at least one factorization into atoms.
- Similarly, a monoid M is called nearly atomic if there exists an element $c \in M$ such that for every non-invertible element $b \in M$, $b + c$ has at least one factorization into atoms.

Ascending Properties

Theorem (CrowdMath 2023)

Suppose M is an atomic Puiseux monoid. Then, if M is also an MCD monoid, $\mathcal{P}_{fin}(M)$ is atomic.

Note: Participants in CrowdMath 2023 also managed to construct an atomic Puiseux monoid that is NOT an MCD monoid, so atomicity may not always ascend to the power monoid.

Question (CrowdMath 2023)

Let M be a Puiseux monoid.
(a) Is $\mathcal{P}_{fin}(M)$ nearly atomic when M is nearly atomic?
(b) Is $\mathcal{P}_{fin}(M)$ almost atomic when M is almost atomic?

References

- D. D. Anderson, D. F. Anderson, and M. Zafrullah: *Factorizations in integral domains*, J. Pure Appl. Algebra **69** (1990) 1–19.
- A. A. Antoniou and S. Tringali: *On the arithmetic of power monoids and sumsets in cyclic groups*, Pacific Journal of Mathematics **312** (2021), No. 2, 279–308.
- P. Bienvenu, A. Geroldinger: *On algebraic properties of power monoids of numerical monoids*. Preprint available on arXiv: https://arxiv.org/abs/2205.00982
- S. T. Chapman, F. Gotti, and M. Gotti: *When is a Puiseux monoid atomic?*, Amer. Math. Monthly **128** (2021) 186–212.
- CrowdMath 2023: *Arithmetic of power monoids*, https://artofproblemsolving.com/polymath/mitprimes2023/f

References

Y. Fan and S. Tringali: *Power Monoids: A bridge between factorization theory and arithmetic combinatorics*, Journal of Algebra **512** (2018) 252–294.

F. Gotti and E. Singer: *The Minkowski sum in numerical semigroups*, CrowdMath 2023 (under preparation).

A. Geroldinger and Q. Zhong: *Factorization theory in commutative monoids*, Semigroup Forum **100** (2020) 22–51.

N. Lebowitz-Lockard: *On domains with properties weaker than atomicity*, Communications in Algebra **47** (2019), No. 5, 1862–1868.

End of Presentation

Thanks for listening!