Factorizations in Evaluation Monoids

Sophie Zhu
*Mentor:* Felix Gotti

Preliminaries
Overview
Atomicity
ACCP, BFM, & FFM
Closing Remarks

MIT PRIMES 2021 Conference

October 16, 2021
Monoids

An (additive) monoid is a pair \((M, +)\), where \(M\) is a set and \(+\) is a binary operation on \(M\), such that

- \(+\) is both associative and commutative, and
- there exists \(0 \in M\) such that \(x + 0 = x\).

Examples

- \((\mathbb{Z}_{\geq 0}, +), (\mathbb{R}_{\geq 0}, +)\)
- \((\{0\} \cup \mathbb{Q}_{\geq 1}, +)\)
- \((\{0, 3, 6, 7, 9, 10, 11, 12, \ldots \}, +)\)
- every abelian group
Monoids

An (additive) **monoid** is a pair \((M, +)\), where \(M\) is a set and \(+\) is a binary operation on \(M\), such that

- \(+\) is both associative and commutative, and
- there exists \(0 \in M\) such that \(x + 0 = x\).

**Examples**

- \((\mathbb{Z}_{\geq 0}, +)\), \((\mathbb{R}_{\geq 0}, +)\)
- \((\{0\} \cup \mathbb{Q}_{\geq 1}, +)\)
- \((\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}, +)\)
- every abelian group
Monoids

An (additive) **monoid** is a pair \((M, +)\), where \(M\) is a set and \(+\) is a binary operation on \(M\), such that

- \(+\) is both associative and commutative, and
- there exists \(0 \in M\) such that \(x + 0 = x\).

**Examples**

- \((\mathbb{Z}_{\geq 0}, +)\), \((\mathbb{R}_{\geq 0}, +)\)
- \((\{0\} \cup \mathbb{Q}_{\geq 1}, +)\)
- \((\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}, +)\)
- every abelian group
Monoids

An (additive) monoid is a pair \((M, +)\), where \(M\) is a set and \(+\) is a binary operation on \(M\), such that
- \(+\) is both associative and commutative, and
- there exists \(0 \in M\) such that \(x + 0 = x\).

Examples
- \((\mathbb{Z}_{\geq 0}, +), (\mathbb{R}_{\geq 0}, +)\)
- \((\{0\} \cup \mathbb{Q}_{\geq 1}, +)\)
- \((\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}, +)\)
- every abelian group
Monoids

An (additive) **monoid** is a pair \((M, +)\), where \(M\) is a set and + is a binary operation on \(M\), such that

- + is both associative and commutative, and
- there exists \(0 \in M\) such that \(x + 0 = x\).

**Examples**

- \((\mathbb{Z}_{\geq 0}, +), (\mathbb{R}_{\geq 0}, +)\)
- \((\{0\} \cup \mathbb{Q}_{\geq 1}, +)\)
- \((\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}, +)\)
- every abelian group
For this talk, let \((M, +)\) be an additive monoid with a unique invertible element; namely, 0.

- An integer \(p \geq 2\) is a **prime** if \(p = a \cdot b\) for any \(a, b \in \mathbb{Z}_{\geq 1}\) implies \(a = 1\) or \(b = 1\).

- A nonzero element \(a\) in \((M, +)\) is an **atom** if the equality \(a = x + y\) for some \(x, y \in M\) implies \(x = 0\) or \(y = 0\).

We denote the set of atoms in \(M\) by \(A(M)\).

**Examples**

- \(A(\mathbb{Z}_{\geq 0}) = \{1\}\)
- \(A(M) = A(\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}) = \{3, 7, 11\}\). For instance, if \(7 = x + y\) for \(x, y \in M\), then \(x = 0\) or \(y = 0\) because \(3 + 3 = 6, 3 + 6 = 9,\) and \(6 + 6 = 12\).
Atoms

For this talk, let $(M, +)$ be an additive monoid with a unique invertible element; namely, 0.

- An integer $p \geq 2$ is a prime if $p = a \cdot b$ for any $a, b \in \mathbb{Z}_{\geq 1}$ implies $a = 1$ or $b = 1$.
- A nonzero element $a$ in $(M, +)$ is an atom if the equality $a = x + y$ for some $x, y \in M$ implies $x = 0$ or $y = 0$.

We denote the set of atoms in $M$ by $A(M)$.

Examples

- $A(\mathbb{Z}_{\geq 0}) = \{1\}$
- $A(M) = A(\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}) = \{3, 7, 11\}$. For instance, if $7 = x + y$ for $x, y \in M$, then $x = 0$ or $y = 0$ because $3 + 3 = 6, 3 + 6 = 9$, and $6 + 6 = 12$. 
Atoms

For this talk, let \((M, +)\) be an additive monoid with a unique invertible element; namely, 0.

- An integer \(p \geq 2\) is a \textit{prime} if \(p = a \cdot b\) for any \(a, b \in \mathbb{Z}_{\geq 1}\) implies \(a = 1\) or \(b = 1\).

- A nonzero element \(a\) in \((M, +)\) is an \textit{atom} if the equality \(a = x + y\) for some \(x, y \in M\) implies \(x = 0\) or \(y = 0\).

We denote the set of atoms in \(M\) by \(A(M)\).

Examples

- \(A(\mathbb{Z}_{\geq 0}) = \{1\}\)
- \(A(M) = A(\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}) = \{3, 7, 11\}\). For instance, if \(7 = x + y\) for \(x, y \in M\), then \(x = 0\) or \(y = 0\) because \(3 + 3 = 6\), \(3 + 6 = 9\), and \(6 + 6 = 12\).
Atoms

For this talk, let \((M, +)\) be an additive monoid with a unique invertible element; namely, 0.

- An integer \(p \geq 2\) is a **prime** if \(p = a \cdot b\) for any \(a, b \in \mathbb{Z}_{\geq 1}\) implies \(a = 1\) or \(b = 1\).
- A nonzero element \(a\) in \((M, +)\) is an **atom** if the equality \(a = x + y\) for some \(x, y \in M\) implies \(x = 0\) or \(y = 0\).

We denote the set of atoms in \(M\) by \(\mathcal{A}(M)\).

**Examples**

- \(\mathcal{A}(\mathbb{Z}_{\geq 0}) = \{1\}\)
- \(\mathcal{A}(M) = \mathcal{A}(\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}) = \{3, 7, 11\}\). For instance, if \(7 = x + y\) for \(x, y \in M\), then \(x = 0\) or \(y = 0\) because \(3 + 3 = 6, 3 + 6 = 9,\) and \(6 + 6 = 12\).
For this talk, let \((M, +)\) be an additive monoid with a unique invertible element; namely, 0.

- An integer \(p \geq 2\) is a prime if \(p = a \cdot b\) for any \(a, b \in \mathbb{Z}_{\geq 1}\) implies \(a = 1\) or \(b = 1\).

- A nonzero element \(a\) in \((M, +)\) is an atom if the equality \(a = x + y\) for some \(x, y \in M\) implies \(x = 0\) or \(y = 0\).

We denote the set of atoms in \(M\) by \(A(M)\).

**Examples**

- \(A(\mathbb{Z}_{\geq 0}) = \{1\}\)

- \(A(M) = A(\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}) = \{3, 7, 11\}\). For instance, if \(7 = x + y\) for \(x, y \in M\), then \(x = 0\) or \(y = 0\) because \(3 + 3 = 6\), \(3 + 6 = 9\), and \(6 + 6 = 12\).
Atoms

For this talk, let \((M, +)\) be an additive monoid with a unique invertible element; namely, 0.

- An integer \(p \geq 2\) is a **prime** if \(p = a \cdot b\) for any \(a, b \in \mathbb{Z}_{\geq 1}\) implies \(a = 1\) or \(b = 1\).

- A nonzero element \(a\) in \((M, +)\) is an **atom** if the equality \(a = x + y\) for some \(x, y \in M\) implies \(x = 0\) or \(y = 0\).

We denote the set of atoms in \(M\) by \(A(M)\).

**Examples**

- \(A(\mathbb{Z}_{\geq 0}) = \{1\}\)
- \(A(M) = A(\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}) = \{3, 7, 11\}\). For instance, if \(7 = x + y\) for \(x, y \in M\), then \(x = 0\) or \(y = 0\) because \(3 + 3 = 6\), \(3 + 6 = 9\), and \(6 + 6 = 12\).
Atomicity

- **Fundamental Theorem of Arithmetic**: Every $n \in \mathbb{Z}_{\geq 2}$ factors (uniquely) into primes.

- $(M, +)$ is atomic if every nonzero element can be written as a sum of atoms.

Atomicity was first studied in the 1960s by Cohn in the context of commutative ring theory and, since then, has been systematically studied in the abstract context of commutative monoids.
Atomicity

- **Fundamental Theorem of Arithmetic**: Every $n \in \mathbb{Z}_{\geq 2}$ factors (uniquely) into primes.

- $\langle M, + \rangle$ is **atomic** if every nonzero element can be written as a sum of atoms.

Atomicity was first studied in the 1960s by Cohn in the context of commutative ring theory and, since then, has been systematically studied in the abstract context of commutative monoids.
Atomicity

- **Fundamental Theorem of Arithmetic**: Every $n \in \mathbb{Z}_{\geq 2}$ factors (uniquely) into primes.

- $(M, +)$ is **atomic** if every nonzero element can be written as a sum of atoms.

Atomicity was first studied in the 1960s by Cohn in the context of commutative ring theory and, since then, has been systematically studied in the abstract context of commutative monoids.
Examples of Atomic Monoids

- $\mathbb{Z}_{\geq 0}$ is atomic as $\mathcal{A}(\mathbb{Z}_{\geq 0}) = 1$ and $n = \underbrace{1 + 1 + \cdots + 1}_{n}$.

- For $M = \{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$, recall that $\mathcal{A}(M) = \{3, 7, 11\}$. One can verify that $M$ is atomic; for instance,
  - $6 = 3 + 3$,
  - $9 = 3 + 3 + 3$,
  - $10 = 3 + 7$, and
  - $12 = 3 + 3 + 3 + 3$.

For $A = \{a_i \mid i \in I\} \subseteq M$, we let $\langle A \rangle$, or $\langle a_i \mid i \in I \rangle$, denote the smallest monoid inside $M$ containing $A$.

- $M = \langle \frac{1}{2^k} \mid k \in \mathbb{Z}_{\geq 0} \rangle$ is not atomic because $\frac{1}{2^k} = \frac{1}{2^{k+1}} + \frac{1}{2^{k+1}}$ for each $k \in \mathbb{Z}_{\geq 0}$, and so $\mathcal{A}(M) = \emptyset$. 
Examples of Atomic Monoids

- \( \mathbb{Z}_{\geq 0} \) is atomic as \( A(\mathbb{Z}_{\geq 0}) = 1 \) and \( n = \underbrace{1 + 1 + \cdots + 1}_{n} \).
- For \( M = \{0, 3, 6, 7, 9, 10, 11, 12, \ldots \} \), recall that \( A(M) = \{3, 7, 11\} \). One can verify that \( M \) is atomic; for instance,
  - \( 6 = 3 + 3 \),
  - \( 9 = 3 + 3 + 3 \),
  - \( 10 = 3 + 7 \), and
  - \( 12 = 3 + 3 + 3 + 3 \).

For \( A = \{a_i \mid i \in I\} \subseteq M \), we let \( \langle A \rangle \), or \( \langle a_i \mid i \in I \rangle \), denote the smallest monoid inside \( M \) containing \( A \).

- \( M = \langle \frac{1}{2^k} \mid k \in \mathbb{Z}_{\geq 0} \rangle \) is not atomic because \( \frac{1}{2^k} = \frac{1}{2^{k+1}} + \frac{1}{2^{k+1}} \) for each \( k \in \mathbb{Z}_{\geq 0} \), and so \( A(M) = \emptyset \).
Examples of Atomic Monoids

- \( \mathbb{Z}_{\geq 0} \) is atomic as \( \mathcal{A}(\mathbb{Z}_{\geq 0}) = 1 \) and \( n = 1 + 1 + \cdots + 1 \).

- For \( M = \{0, 3, 6, 7, 9, 10, 11, 12, \ldots\} \), recall that \( \mathcal{A}(M) = \{3, 7, 11\} \). One can verify that \( M \) is atomic; for instance,
  - \( 6 = 3 + 3 \),
  - \( 9 = 3 + 3 + 3 \),
  - \( 10 = 3 + 7 \), and
  - \( 12 = 3 + 3 + 3 + 3 \).

For \( A = \{a_i \mid i \in I\} \subseteq M \), we let \( \langle A \rangle \), or \( \langle a_i \mid i \in I \rangle \), denote the smallest monoid inside \( M \) containing \( A \).

- \( M = \langle \frac{1}{2^k} \mid k \in \mathbb{Z}_{\geq 0} \rangle \) is not atomic because \( \frac{1}{2^k} = \frac{1}{2^{k+1}} + \frac{1}{2^{k+1}} \) for each \( k \in \mathbb{Z}_{\geq 0} \), and so \( \mathcal{A}(M) = \emptyset \).
Examples of Atomic Monoids

- $\mathbb{Z}_{\geq 0}$ is atomic as $\mathcal{A}(\mathbb{Z}_{\geq 0}) = 1$ and $n = 1 + 1 + \cdots + 1$.
- For $M = \{0, 3, 6, 7, 9, 10, 11, 12, \ldots \}$, recall that $\mathcal{A}(M) = \{3, 7, 11\}$. One can verify that $M$ is atomic; for instance,
  - $6 = 3 + 3$,
  - $9 = 3 + 3 + 3$,
  - $10 = 3 + 7$, and
  - $12 = 3 + 3 + 3 + 3$.

For $A = \{a_i \mid i \in I\} \subseteq M$, we let $\langle A \rangle$, or $\langle a_i \mid i \in I \rangle$, denote the smallest monoid inside $M$ containing $A$.

- $M = \langle \frac{1}{2^k} \mid k \in \mathbb{Z}_{\geq 0} \rangle$ is not atomic because $\frac{1}{2^k} = \frac{1}{2^{k+1}} + \frac{1}{2^{k+1}}$ for each $k \in \mathbb{Z}_{\geq 0}$, and so $\mathcal{A}(M) = \emptyset$. 
A factorization of a nonzero $x \in M$ is a decomposition $x = a_1 + \cdots + a_\ell$, where $a_1, \ldots, a_\ell \in A(M)$, in which case $\ell$ is called a length of $x$.

Define $L(x)$ as the set of all possible lengths of $x$.

Examples

- In $\mathbb{Z}_{\geq 0}$, the decomposition $n = 1 + 1 + \cdots + 1$ is a factorization of $n$ of length $n$. This is unique, so $L(n) = \{n\}$ for all $n \geq 1$.
- In $\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$ the decompositions $10 = 3 + 7$ and $21 = 7 + 7 + 7$ are factorizations of 10 and 21 of lengths 2 and 3, resp. This factorization of 10 is unique, so $L(10) = \{2\}$, but $21 = 3 + \cdots + 3$ (7 times) is also a factorization of 21; indeed, $L(21) = \{3, 7\}$. 
Factorizations

- A **factorization** of a nonzero \( x \in M \) is a decomposition \( x = a_1 + \cdots + a_\ell \), where \( a_1, \ldots, a_\ell \in A(M) \), in which case \( \ell \) is called a **length** of \( x \).
- Define \( L(x) \) as the set of all possible lengths of \( x \).

**Examples**

- In \( \mathbb{Z}_{\geq 0} \), the decomposition \( n = 1 + 1 + \cdots + 1 \) is a factorization of \( n \) of length \( n \). This is unique, so \( L(n) = \{n\} \) for all \( n \geq 1 \).
- In \( \{0, 3, 6, 7, 9, 10, 11, 12, \ldots\} \) the decompositions \( 10 = 3 + 7 \) and \( 21 = 7 + 7 + 7 \) are factorizations of 10 and 21 of lengths 2 and 3, resp. This factorization of 10 is unique, so \( L(10) = \{2\} \), but \( 21 = 3 + \cdots + 3 \) (7 times) is also a factorization of 21; indeed, \( L(21) = \{3, 7\} \).
A factorization of a nonzero $x \in M$ is a decomposition $x = a_1 + \cdots + a_\ell$, where $a_1, \ldots, a_\ell \in A(M)$, in which case $\ell$ is called a length of $x$.

Define $L(x)$ as the set of all possible lengths of $x$.

**Examples**

- In $\mathbb{Z}_{\geq 0}$, the decomposition $n = 1 + 1 + \cdots + 1$ is a factorization of $n$ of length $n$. This is unique, so $L(n) = \{n\}$ for all $n \geq 1$.
- In $\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$ the decompositions $10 = 3 + 7$ and $21 = 7 + 7 + 7$ are factorizations of 10 and 21 of lengths 2 and 3, resp. This factorization of 10 is unique, so $L(10) = \{2\}$, but $21 = 3 + \cdots + 3$ (7 times) is also a factorization of 21; indeed, $L(21) = \{3, 7\}$. 
Examples of BFM$s$, FFM$s$, and UFM$s$

Let $M$ be an atomic monoid. Then

- $M$ is a **bounded factorization monoid** (BFM) if for each nonzero $x \in M$, the set $L(x)$ is bounded.
  - In a BFM, an element may have infinitely many factorizations.
    - $\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$ is a BFM. Since its elements lie in $\mathbb{Z}_{\geq 0}$, the length of a factorization of $n$ is always bounded above by $n$.

- $M$ is a **finite factorization monoid** (FFM) if each nonzero $x \in M$ has finitely many factorizations.
  - $\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$ is also an FFM.

- $M$ is a **unique factorization monoid** (UFM) if each nonzero $x \in M$ has exactly one factorization.
  - $\mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM and FFM).
  - $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM & FFM), where $\mathcal{A}(\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}) = \{(1, 0), (0, 1)\}$.
Examples of BFM$s$, FFM$s$, and UFM$s$

Let $M$ be an atomic monoid. Then

- $M$ is a **bounded factorization monoid** (BFM) if for each nonzero $x \in M$, the set $L(x)$ is bounded.
  - In a BFM, an element may have infinitely many factorizations.
  - $\{0, 3, 6, 7, 9, 10, 11, 12, \ldots \}$ is a BFM. Since its elements lie in $\mathbb{Z}_{\geq 0}$, the length of a factorization of $n$ is always bounded above by $n$.

- $M$ is a **finite factorization monoid** (FFM) if each nonzero $x \in M$ has finitely many factorizations.
  - $\{0, 3, 6, 7, 9, 10, 11, 12, \ldots \}$ is also an FFM.

- $M$ is a **unique factorization monoid** (UFM) if each nonzero $x \in M$ has exactly one factorization.
  - $\mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM and FFM).
  - $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM & FFM), where $A(\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}) = \{(1, 0), (0, 1)\}$. 
Examples of BFMss, FFMss, and UFMss

Let $M$ be an atomic monoid. Then

- $M$ is a **bounded factorization monoid** (BFM) if for each nonzero $x \in M$, the set $L(x)$ is bounded.
  - In a BFM, an element may have infinitely many factorizations.
  - $\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$ is a BFM. Since its elements lie in $\mathbb{Z}_{\geq 0}$, the length of a factorization of $n$ is always bounded above by $n$.

- $M$ is a **finite factorization monoid** (FFM) if each nonzero $x \in M$ has finitely many factorizations.
  - $\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$ is also an FFM.

- $M$ is a **unique factorization monoid** (UFM) if each nonzero $x \in M$ has exactly one factorization.
  - $\mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM and FFM).
  - $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM & FFM), where $\mathcal{A}(\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}) = \{(1, 0), (0, 1)\}$.
Examples of BFM$s$, FFM$s$, and UFM$s$

Let $M$ be an atomic monoid. Then

- $M$ is a **bounded factorization monoid** (BFM) if for each nonzero $x \in M$, the set $L(x)$ is bounded.
  - In a BFM, an element may have infinitely many factorizations.
  - $\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$ is a BFM. Since its elements lie in $\mathbb{Z}_{\geq 0}$, the length of a factorization of $n$ is always bounded above by $n$.

- $M$ is a **finite factorization monoid** (FFM) if each nonzero $x \in M$ has finitely many factorizations.
  - $\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$ is also an FFM.

- $M$ is a **unique factorization monoid** (UFM) if each nonzero $x \in M$ has exactly one factorization.
  - $\mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM and FFM).
  - $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM & FFM), where $\mathcal{A}(\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}) = \{(1, 0), (0, 1)\}$.
Examples of BFM$s$, FFM$s$, and UFM$s$

Let $M$ be an atomic monoid. Then

- $M$ is a **bounded factorization monoid** (BFM) if for each nonzero $x \in M$, the set $L(x)$ is bounded.
  - In a BFM, an element may have infinitely many factorizations.
  - $\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$ is a BFM. Since its elements lie in $\mathbb{Z}_{\geq 0}$, the length of a factorization of $n$ is always bounded above by $n$.

- $M$ is a **finite factorization monoid** (FFM) if each nonzero $x \in M$ has finitely many factorizations.
  - $\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$ is also an FFM.

- $M$ is a **unique factorization monoid** (UFM) if each nonzero $x \in M$ has exactly one factorization.
  - $\mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM and FFM).
  - $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM & FFM), where $A(\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}) = \{(1, 0), (0, 1)\}$. 
The phenomenon of non-uniqueness of factorizations naturally appears in algebraic number theory (for instance, the ring of integers $\mathbb{Z}[\sqrt{-5}]$ is not a UFD) and has been the main motivation for the development of factorization theory in the abstract context of commutative monoids. As a crucial part of this development, BFM s and FFM s were introduced in 1992.

Question

What can we say about the existence and non-uniqueness of factorizations in monoids in general?

The following follows directly from the definitions.

$$\text{UFM} \Rightarrow \text{FFM} \Rightarrow \text{BFM} \Rightarrow \text{atomicity}$$
The phenomenon of non-uniqueness of factorizations naturally appears in algebraic number theory (for instance, the ring of integers $\mathbb{Z}[\sqrt{-5}]$ is not a UFD) and has been the main motivation for the development of factorization theory in the abstract context of commutative monoids. As a crucial part of this development, BFM and FFMs were introduced in 1992.

Question

What can we say about the existence and non-uniqueness of factorizations in monoids in general?

The following follows directly from the definitions.

\[ UFM \Rightarrow FFM \Rightarrow BFM \Rightarrow \text{atomicity} \]
The phenomenon of non-uniqueness of factorizations naturally appears in algebraic number theory (for instance, the ring of integers $\mathbb{Z}[\sqrt{-5}]$ is not a UFD) and has been the main motivation for the development of factorization theory in the abstract context of commutative monoids. As a crucial part of this development, BFM\text{s} and FFM\text{s} were introduced in 1992.

**Question**

What can we say about the existence and non-uniqueness of factorizations in monoids in general?

The following follows directly from the definitions.

$$\text{UFM} \Rightarrow \text{FFM} \Rightarrow \text{BFM} \Rightarrow \text{atomicity}$$
Overview

**Definition**

For $\alpha \in \mathbb{R}_{>0}$, the (Laurent) evaluation monoid of $\alpha$ is

$$M_{\alpha} := \{ f(\alpha) \mid f(x) \in \mathbb{Z}_{\geq 0}[x, x^{-1}] \} = \{ f(\alpha) \mid f(x) = c_{-n}x^{-n} + \cdots + c_{n}x^{n}, c_{i} \in \mathbb{Z}_{\geq 0} \}.$$

We discuss the following classes of $M_{\alpha}$.

1. Atomic monoids
2. Bounded and finite factorization monoids (in connection with the ascending chain condition on principal ideals)
3. A class of FFM$s$ that are not UFMs
Overview

Definition

For $\alpha \in \mathbb{R}_{>0}$, the (Laurent) evaluation monoid of $\alpha$ is

$$M_\alpha := \{ f(\alpha) \mid f(x) \in \mathbb{Z}_{\geq 0}[x, x^{-1}] \}$$

$$= \{ f(\alpha) \mid f(x) = c_{-n}x^{-n} + \cdots + c_n x^n, c_i \in \mathbb{Z}_{\geq 0} \}.$$

We discuss the following classes of $M_\alpha$.

1. Atomic monoids

2. Bounded and finite factorization monoids (in connection with the ascending chain condition on principal ideals)

3. A class of FFMs that are not UFM
Overview

Definition

For $\alpha \in \mathbb{R}_{>0}$, the (Laurent) evaluation monoid of $\alpha$ is

$$M_\alpha := \{ f(\alpha) \mid f(x) \in \mathbb{Z}_{\geq 0}[x, x^{-1}] \} = \{ f(\alpha) \mid f(x) = c_{-n}x^{-n} + \cdots + c_nx^n, c_i \in \mathbb{Z}_{\geq 0} \}.$$

We discuss the following classes of $M_\alpha$.

1. Atomic monoids
2. Bounded and finite factorization monoids (in connection with the ascending chain condition on principal ideals)
3. A class of FFMs that are not UFM}s
Overview

Definition

For $\alpha \in \mathbb{R}_{>0}$, the (Laurent) evaluation monoid of $\alpha$ is

$$M_\alpha := \{f(\alpha) \mid f(x) \in \mathbb{Z}_{\geq 0}[x, x^{-1}]\}$$

$$= \{f(\alpha) \mid f(x) = c_{-n}x^{-n} + \cdots + c_nx^n, c_i \in \mathbb{Z}_{\geq 0}\}.$$ 

We discuss the following classes of $M_\alpha$.

1. Atomic monoids
2. Bounded and finite factorization monoids (in connection with the ascending chain condition on principal ideals)
3. A class of FFMs that are not UFM
Overview

Definition

For $\alpha \in \mathbb{R}_{>0}$, the (Laurent) evaluation monoid of $\alpha$ is

$$M_{\alpha} := \{ f(\alpha) \mid f(x) \in \mathbb{Z}_{\geq 0}[x, x^{-1}] \} = \{ f(\alpha) \mid f(x) = c_{-n}x^{-n} + \cdots + c_n x^n, c_i \in \mathbb{Z}_{\geq 0} \}.$$

We discuss the following classes of $M_{\alpha}$.

1. Atomic monoids
2. Bounded and finite factorization monoids (in connection with the ascending chain condition on principal ideals)
3. A class of FFMs that are not UFM
Atomicity

Proposition (Z., 2021)

For each $\alpha \in \mathbb{R}_{>0}$, the following statements are equivalent.

(a) $1 \in A(M_\alpha)$.

(b) $A(M_\alpha) = \{\alpha^n \mid n \in \mathbb{Z}\}$.

(c) $M_\alpha$ is atomic.

If $\alpha \in \mathbb{R}_{>0}$ is transcendental, then $M_\alpha$ is atomic.

Example ($M_\alpha$ not atomic)

Consider the monic irreducible polynomial $m(x) = x^3 - 2x^2 + 3x - 7$, which has a real root $\alpha \in (2, 3)$. As $m(x)(x + 2) = x^4 - x^2 - x - 14$, we note $\alpha^4 = \alpha^2 + \alpha + 14$. Then $\alpha$ is not an atom in $M$, implying $M_\alpha$ is not atomic.
Proposition (Z., 2021)

For each $\alpha \in \mathbb{R}_{>0}$, the following statements are equivalent.

(a) $1 \in \mathcal{A}(M_\alpha)$.

(b) $\mathcal{A}(M_\alpha) = \{\alpha^n \mid n \in \mathbb{Z}\}$.

(c) $M_\alpha$ is atomic.

If $\alpha \in \mathbb{R}_{>0}$ is transcendental, then $M_\alpha$ is atomic.

Example ($M_\alpha$ not atomic)

Consider the monic irreducible polynomial $m(x) = x^3 - 2x^2 + 3x - 7$, which has a real root $\alpha \in (2, 3)$. As $m(x)(x + 2) = x^4 - x^2 - x - 14$, we note $\alpha^4 = \alpha^2 + \alpha + 14$. Then $\alpha$ is not an atom in $M$, implying $M_\alpha$ is not atomic.
One of the most relevant classes of atomic monoids are those satisfying the ACCP.

A monoid \((M, +)\) satisfies the **ascending chain condition on principal ideals** (ACCP) if every sequence \(\{x_n\}_{n \in \mathbb{Z}_{>0}} \subseteq M\) satisfying \(x_n - x_{n+1} \in M\) for each \(n \in \mathbb{N}\), is constant after some point.

**Example** (\(M_{\alpha}\) does not satisfy ACCP)

\[
\alpha = \frac{2}{3}. \text{ Take the sequence } \{x_n\}_{n \in \mathbb{Z}_{>0}} \text{ defined by } x_n = 2 \cdot (2/3)^n: \quad x_n - x_{n+1} = 2 \cdot (2/3)^n - 2 \cdot (2/3)^{n+1} = (2/3)^{n+1} \in M \text{ for each } n \in \mathbb{Z}_{\geq 0}, \text{ so the sequence does not become constant. Hence, it does not satisfy the ACCP.}
\]
One of the most relevant classes of atomic monoids are those satisfying the ACCP.

A monoid \((M, +)\) satisfies the \textbf{ascending chain condition on principal ideals} (ACCP) if every sequence \(\{x_n\}_{n \in \mathbb{Z}_>0} \subseteq M\) satisfying \(x_n - x_{n+1} \in M\) for each \(n \in \mathbb{N}\), is constant after some point.

\textbf{Example} (\(M_\alpha\) does not satisfy ACCP)

\[\alpha = 2/3.\] Take the sequence \(\{x_n\}_{n \in \mathbb{Z}_>0}\) defined by \(x_n = 2 \cdot (2/3)^n: x_n - x_{n+1} = 2 \cdot (2/3)^n - 2 \cdot (2/3)^{n+1} = (2/3)^{n+1} \in M\) for each \(n \in \mathbb{Z}_>0\), so the sequence does not become constant. Hence, it does not satisfy the ACCP.
The following result is well-known.

**Proposition**

Every BFM satisfies the ACCP.

Therefore,

\[
\text{UFM} \implies \text{FFM} \implies \text{BFM} \implies \text{ACCP} \implies \text{atomicity}
\]

We established the following main result for the class of Laurent evaluation monoids \(M_\alpha\).

**Theorem (Z., 2021)**

For \(\alpha \in \mathbb{R}_{>0}\), the following holds for \(M_\alpha\).

\[
\text{FFM} \iff \text{BFM} \iff \text{ACCP}
\]
Nested Classes of Atomic Monoids

The following result is well-known.

**Proposition**

*Every BFM satisfies the ACCP.*

Therefore,

\[ \text{UFM} \Rightarrow \text{FFM} \Rightarrow \text{BFM} \Rightarrow \text{ACCP} \Rightarrow \text{atomicity} \]

We established the following main result for the class of Laurent evaluation monoids \( M_\alpha \).

**Theorem (Z., 2021)**

*For \( \alpha \in \mathbb{R}_{>0} \), the following holds for \( M_\alpha \).*

\[ \text{FFM} \iff \text{BFM} \iff \text{ACCP} \]
A Class of FFM\s that are not UFM\s

Theorem (Z., 2021)

Suppose that $\alpha_1$ and $\alpha_2$ are the roots of an irreducible quadratic polynomial in $\mathbb{Q}[x]$ such that $0 < \alpha_1 < 1 < \alpha_2$. Then $M_{\alpha_1}$ is an FFM and, therefore, satisfies the ACCP.

Example ($M_{\alpha}$ is FFM but not UFM)
Consider the polynomial $p(x) := x^2 - 2x + \frac{1}{2}$. It is irreducible, with roots $\alpha_1 := 1 - \frac{\sqrt{2}}{2}$ and $\alpha_2 := 1 + \frac{\sqrt{2}}{2}$. Since $0 < \alpha_1 < 1 < \alpha_2$, the Theorem implies $M_{\alpha}$ is an FFM. However, it is not a UFM: since $M_{\alpha}$ is atomic, we have $1, \alpha, \alpha^2 \in A(M_{\alpha})$. Then the two sides of the equality $4\alpha_1 = 2\alpha_2^2 + 1$ yield distinct factorizations of the same element in $M_{\alpha}$. 
A Class of FFMs that are not UFM

**Theorem (Z., 2021)**

Suppose that $\alpha_1$ and $\alpha_2$ are the roots of an irreducible quadratic polynomial in $\mathbb{Q}[x]$ such that $0 < \alpha_1 < 1 < \alpha_2$. Then $M_{\alpha_1}$ is an FFM and, therefore, satisfies the ACCP.

**Example (M is FFM but not UFM)**

Consider the polynomial $p(x) := x^2 - 2x + \frac{1}{2}$. It is irreducible, with roots $\alpha_1 := 1 - \frac{\sqrt{2}}{2}$ and $\alpha_2 := 1 + \frac{\sqrt{2}}{2}$. Since $0 < \alpha_1 < 1 < \alpha_2$, the Theorem implies $M_{\alpha}$ is an FFM. However, it is not a UFM: since $M_{\alpha}$ is atomic, we have $1, \alpha, \alpha^2 \in A(M_{\alpha})$. Then the two sides of the equality $4\alpha_1 = 2\alpha_2^2 + 1$ yield distinct factorizations of the same element in $M_{\alpha}$. 
Diagram Summarizing Our Results

\[ \text{[UFM} \iff \text{HFM} \iff \text{LFM]} \]
\[ \downarrow \]
\[ \text{[FFM} \iff \text{BFM} \iff \text{ACCP]} \]
\[ \downarrow \]
\[ \text{atomicity} \]
References


Many thanks go to

- my mentor Dr. Felix Gotti (MIT) for his invaluable guidance, feedback, and encouragement.
- Dr. Pavel Etingof, Dr. Slava Gerovitch, Dr. Tanya Khovanova, the MIT Math Department, and the MIT PRIMES program, for providing us with the opportunity to work on this project.
- my mother for her constant support.
- you for listening.