Friendly Introduction to the Factorization Theory of Numerical Semigroups

Felix Gotti
felixgotti@berkeley.edu

UC Berkeley

Residents Symposium, PURE Math 2015

Outline

Commutative Cancellative Monoid

Consider the pair $(S, +)$, where S is a nonempty set and $+ : S \times S \to S$ a binary operation.

- $(S, +)$ is *associative* if $a + (b + c) = (a + b) + c$ for all $a, b, c \in S$.
- $e \in S$ is called an *identity* if $e + a = a + e = a$ for all $a \in S$.

Definition (Monoid)

If the pair $(M, +)$ is associative and contains an identity, we say that $(M, +)$ is a *monoid*.

Commutative Cancellative Monoid

With notation as before:

- $(S, +)$ is *commutative* if $a + b = b + a$ for all $a, b, c \in S$.
- A commutative pair $(S, +)$ is *cancellative* if $c + a = c + b$ implies $a = b$ for all $a, b, c \in S$.

Remark: In Factorization Theory, we only study monoids that are commutative and cancellative, so we will omit to specify it.

Examples (Commutative Cancellative Monoid)

We have come across many monoids in elementary mathematics. For example:

Examples

- $(\mathbb{N}, +)$, whose identity is 0.
- $(\mathbb{N}^k, +)$, whose identity is $(0, \dots, 0)$.

There are certainly other less standard monoids, such as the Hilbert monoid.

Example (Hilbert Monoid)

Consider The set $\mathcal{H} := \{1 + 4n \mid n \in \mathbb{N}\}$. Define the addition operation on $\mathcal{H}$ to be
$(1 + 4n) + (1 + 4m) := (1 + 4n)(1 + 4m) = 1 + 4(n + m + 4nm)$.
The identity of $\mathcal{H}$ is 1.

Units and Irreducible Elements

Let M be a monoid.

- $u \in M$ is a *unit* if there exists $v \in M$ such that $u + v = e$. The set of units of M is denoted by $M^\times$.
- An element $a \in M \setminus M^\times$ is said to be *irreducible* or an *atom* if $a = u + v$ for some $u, v \in M$ implies that either u or v is a unit. The set of irreducible elements of M is denoted by $\mathcal{A}(M)$.
- M is said to be *atomic* if any element in $M \setminus M^\times$ can be written as the sum of irreducible elements.

Units and Irreducible Elements (Examples)

Example (1)

- The only unit of $(\mathbb{N}, +)$ is 0.
- The only irreducible element of $(\mathbb{N}, +)$ is 1.
- $(\mathbb{N}, +)$ is atomic.

Example (2)

- The only unit of $(\mathbb{N}^k, +)$ is $(0, \dots, 0)$.
- If $M = (\mathbb{N}^k, +)$ then $\mathcal{A}(M) = \{ e_i \mid 1 \le i \le k \}$, where e_i is the element of $\mathbb{N}^k$ with 1 in the i-th coordinate and zeroes elsewhere.
- $(\mathbb{N}^k, +)$ is atomic.

Numerical Semigroups

Definition (Numerical Semigroup)

An additive submonoid $M \subseteq \mathbb{N}$ is said to be a *numerical monoid* if $\mathbb{N} \setminus M$ is finite.

If a submonoid $M \subseteq \mathbb{N}$ is generated by $\{ a_1, \dots, a_k \}$ we write $M = \langle a_1, \dots, a_k \rangle$. We always assume that $a_1 < \cdots < a_k$. The following theorem hold.

Theorem

1. *Every numerical monoid is finitely generated.*
2. *A submonoid $M = \langle a_1, \dots, a_k \rangle$ of $\mathbb{N}$ is a numerical monoid if and only if $\gcd(a_1, \dots, a_k) = 1$.*

Numerical Semigroups (continuation)

Further definitions and notation:

1. A numerical monoid $M = \langle S \rangle$ is *minimally generated by S* if no proper subset of S generates M.
2. If $M = \langle a_1, \dots, a_k \rangle$ is minimally generated, then $\mathcal{A}(M) = \{ a_1, \dots, a_k \}$, and n is called the *embedding dimension* of M.
3. g is a *gap* of M if $g \in \mathbb{N} \setminus M$.
    - The set of gaps is denoted by $G(M)$.
    - The maximum of $G(M)$, denoted by $\mathcal{F}(M)$, is called the Frobenius number of M.

Examples of Numerical Semigroups

Example (1)

- $M = \langle 8, 9, 19 \rangle$ is a numerical monoid because $\gcd(8, 9, 19) = 1$.
- M has embedding dimension 3.
- $\mathcal{F}(M) = 39$.

Example (2)

- $M_n = \langle n, n+3, n+5 \rangle$ is a numerical monoid for every $n \in \mathbb{N}$ since $\gcd(n, n+3, n+5) = 1$.
- M has embedding dimension 3.

Families of Numerical Semigroups

Arithmetic Monoid:

Definition

A numerical monoid $M = \langle a, a+d, \dots, a+kd \rangle$ where $a, k, d \in \mathbb{N}$ such that $1 \le k < a$ and $\gcd(a, d) = 1$ is called *arithmetic monoid*.

Examples (Arithmetic Monoid)

- $M = \langle 3, 8, 13 \rangle$. Here $a = 3$, $d = 5$, and $k = 2$.
- Any embedding dimension 2 numerical monoid $M = \langle x, y \rangle$ is an arithmetic monoid, where $d = y - x$ and $k = 1$
- An arithmetic monoid with $d = 1$ is called numerical monoid generated by an interval.

Families of Numerical Semigroups (continuation)

Generalized Arithmetic Monoid:

Definition

A numerical monoid $M = \langle a, ha + d, \ldots, ha + kd \rangle$ where $a, h, k, d \in \mathbb{N}$ such that $1 \leq k < a$ and $\gcd(a, d) = 1$ is called *generalized arithmetic monoid*.

Example (Generalized Arithmetic Monoid)

- $M = \langle 3, 8, 10 \rangle = \langle 3, 2 \cdot 3 + 2, 2 \cdot 3 + 2 \cdot 2 \rangle$. So $a = 3$, $h = 2$, $d = 2$, and $k = 2$.
- $\langle 5, 52, 59 \rangle = \langle 5, 5 \cdot 9 + 7, 5 \cdot 9 + 2 \cdot 7 \rangle$. So $a = 5$, $h = 9$, $d = 7$, and $k = 2$.
- Any arithmetic monoid is a generalized arithmetic monoid where $h = 1$.

Factorizations

Let $M = \langle a_1, \dots, a_k \rangle$ be a minimally generated numerical monoid.

- The *factorization map* of M is $\varphi : \mathbb{N}^k \to M$ defined by $\varphi(z_1, \dots, z_k) = z_1 a_1 + \dots + z_k a_k$.
- $z = (z_1, \dots, z_k) \in \mathbb{N}^k$ is said to be a *factorization* of $a \in M$ if $\varphi(z) = a$.
- The *set of factorizations* of $a \in M$ is defined by

$$\mathsf{Z}(a) := \varphi^{-1}(a) = \{\, (z_1, \dots, z_k) \mid \varphi(z_1, \dots, z_k) = a \,\}.$$

Example (Factorizations)

Let $M = \langle 3, 8, 13 \rangle$ and $30 \in M$.

- $30 = 10 \cdot 3 + 0 \cdot 8 + 0 \cdot 13$, then $z_1 = (10, 0, 0) \in \mathsf{Z}(30)$.
- $30 = 2 \cdot 3 + 3 \cdot 8 + 0 \cdot 13$, then $z_2 = (2, 3, 0) \in \mathsf{Z}(30)$.
- $30 = 3 \cdot 3 + 1 \cdot 8 + 1 \cdot 13$, then $z_3 = (3, 1, 1) \in \mathsf{Z}(30)$.
- Actually, $\mathsf{Z}(30) = \{\, z_1, z_2, z_3 \,\}$.

Length and Distance

Let $M = \langle a_1, \dots, a_k \rangle$ be a minimally generated numerical monoid.

- If $z = (z_1, \dots, z_k)$ is a factorization of a, the *length* of z is $|z| = z_1 + \cdots + z_k$. The set of all lengths of a is defined $\mathsf{L}(a)$.
- For $z = (z_1, \dots, z_k)$, $z' = (z'_1, \dots, z'_k) \in \mathsf{Z}(a)$ we set $\gcd(z, z') = (\min\{z_1, z'_1\}, \dots, \min\{z_p, z'_p\})$.
- The *distance* between z and z is defined by $d(z, z') = \max\{\, |z - \gcd(z, z')|, |z' - \gcd(z, z')| \,\}$.

Examples (Length and Distance)

Let $M = \langle 3, 8, 13 \rangle$ and $30 \in M$.

- $\mathsf{Z}(30) = \{\, z_1 = (10, 0, 0), z_2 = (2, 3, 0), z_3 = (3, 1, 1) \,\}$
- $|z_1| = 10$, $|z_2| = 5$, and $|z_3| = 5$.
- $\gcd(z_1, z_2) = (2, 0, 0)$ and $\gcd(z_2, z_3) = (2, 1, 0)$.
- $d(z_1, z_2) = 8$ and $d(z_2, z_3) = 2$.

Set of Lengths

Definition (Set of Lengths)

Let M be a minimally generated numerical monoid. The *set of lengths* of $a \in M$ is the set

$$\mathsf{L}(a) = \{\, |z| \mid z \in \mathsf{Z}(a) \,\}.$$

Example (Set of Lengths)

For $M = \langle 3, 8, 13 \rangle$ and $30 \in M$, we have seen that

$$\mathsf{Z}(30) = \{\, (10,0,0), (2,3,0), (3,1,1) \,\}.$$

Therefore

$$\mathsf{L}(30) = \{\, 5, 10 \,\}.$$

Catenary Degree

Let M be a numerical monoid, and let $a \in M$.
Given $z, z' \in \mathsf{Z}(a)$ and $N \geq 1$, an *N-chain* from z to z' is a sequence $z_0, \dots, z_n \in \mathsf{Z}(a)$ of factorizations of a such that $z_0 = z$, $z_n = z'$, and $d(z_{i-1}, z_i) \leq N$ for every $i = 1, \dots, n$.

Definition (Catenary Degree)

The *catenary degree* of a, denoted $\mathsf{c}(a)$, is the smallest non-negative integer N such that there exists an N-chain between any two factorizations of a. The *catenary degree* of M is the number

$$\mathsf{c}(M) = \sup\{\, \mathsf{c}(a) \mid a \in M \,\}.$$

Computing Catenary Degree

Let $M = \langle 3, 8, 10 \rangle$ and $a = 36$.

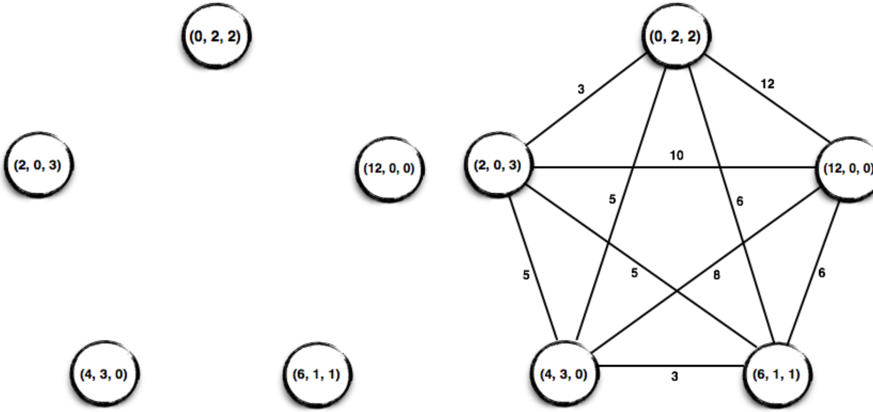

Figure: Catenary Graph of $a = 36$

Betti Elements

Let M be a numerical monoid.

Definition (Betti Graph)

For each nonzero $a \in M$ consider the graph ∇_a whose set of vertices is $\mathsf{Z}(a)$, in which two vertices z, $z' \in \mathsf{Z}(a)$ share an edge if $\gcd(z, z') \neq 0$.

Definition (Betti Element)

Let $\beta \in M$. If ∇_β is not connected, then β is called a *Betti element* of M. We write

$$\text{Betti}(M) = \{\, \beta \in M \mid \nabla_\beta \text{ is disconnected} \,\}$$

for the set of Betti elements of M.

Betti Elements (continuation)

The following theorems give evidence of the importance of the set of Betti elements.

Theorem

If M is a numerical monoid then $\mathrm{Betti}(M)$ *is finite.*

Theorem

If M is a numerical monoid then the following hold.

- *There exists* $\beta \in \mathrm{Betti}(M)$ *such that* $\mathrm{c}(\beta) = \mathrm{c}(M)$.
- *There exists* $\beta' \in \mathrm{Betti}(M)$ *such that* $\mathrm{c}(\beta') \le \mathrm{c}(a)$ *for every* $a \in M$.

Testing Betti Elements

Let $M = \langle 5, 18, 21, 24, 27 \rangle$ and $a = 54$. It is a Betti element.

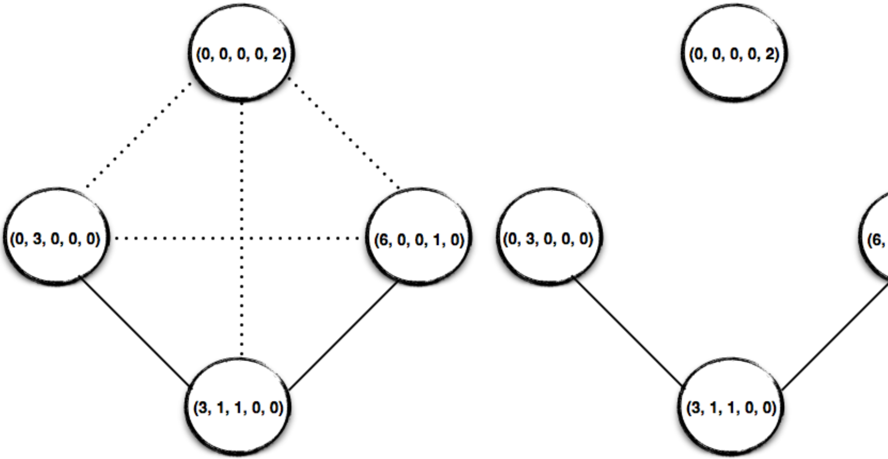

Figure: Betti Graph of $a = 54$

Testing Betti Elements

Let $M = \langle 5, 18, 21, 24, 27 \rangle$ and $a = 60$. It is NOT a Betti element.

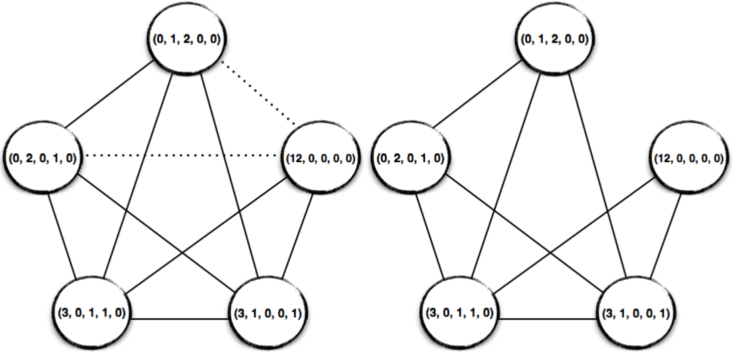

Figure: Betti Graph of $a = 60$

References

- P. A. Garcia-Sanchez and J. C. Rosales. *Numerical Semigroups*.
- S. Chapman, N. Kaplan, T. Lemburg, A. Niles, C. Zlogar. *Shifts of Generators and Delta Sets of Numerical Semigroup*.
- S. Chapman, P. Garcia-Sanchez, D. Llena, V. Ponomarenko, J. Rosales. *The Catenary and Tame Degree in Finitely Generated Commutative Cancellative Monoids*. Manuscripta Math. 120 (2006), no. 3, 253–264.
- A. Geroldinger and F. Halter-Koch. *Non-Unique Factorizations: Algebraic, Combinatorial, and Analytic Theory*. Chapman & Hall/CRC, Boca Raton, 2006.
- T. Barron, C. O'Neill, and R. Pelayo. *On the Set of Elasticities in Numerical Monoids*, 2015, arXiv:1409.3425v2.