Frobenius' number, semigroups and Möbius function

J. L. Ramírez Alfonsín

IMAG, Université de Montpellier

Universidade de São Paulo
Instituto de Matemática e Estatística
Departamento de Ciência da Computação
São Paulo, July 31st, 2018

Diophantine Frobenius Problem

Let $a_1, \ldots, a_n$ be positive integers with $\gcd(a_1, \ldots, a_n) = 1$, find the largest integer (called the Frobenius number and denoted by $g(a_1, \ldots, a_n)$) that is not representable as a nonnegative integer combination of $a_1, \ldots, a_n$.

Diophantine Frobenius Problem

Let $a_1, \ldots, a_n$ be positive integers with $\gcd(a_1, \ldots, a_n) = 1$, find the largest integer (called the Frobenius number and denoted by $g(a_1, \ldots, a_n)$) that is not representable as a nonnegative integer combination of $a_1, \ldots, a_n$.

Example: If $a_1 = 3$ and $a_2 = 8$ then

Diophantine Frobenius Problem

Let $a_1, \ldots, a_n$ be positive integers with $\gcd(a_1, \ldots, a_n) = 1$, find the largest integer (called the Frobenius number and denoted by $g(a_1, \ldots, a_n)$) that is not representable as a nonnegative integer combination of $a_1, \ldots, a_n$.

Example: If $a_1 = 3$ and $a_2 = 8$ then

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 $\cdots\cdots$

Diophantine Frobenius Problem

Let $a_1, \dots, a_n$ be positive integers with $\gcd(a_1, \dots, a_n) = 1$, find the largest integer (called the Frobenius number and denoted by $g(a_1, \dots, a_n)$) that is not representable as a nonnegative integer combination of $a_1, \dots, a_n$.

Example: If $a_1 = 3$ and $a_2 = 8$ then

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 $\cdots\cdots$

So, $g(3, 8) = 13$.

Some results

Theorem $g(a_1, \ldots, a_n)$ exists and it is finite.

Some results

Theorem $g(a_1, \ldots, a_n)$ exists and it is finite.

Theorem (Sylvester, 1882) $g(a_1, a_2) = a_1 a_2 - a_1 - a_2$.

Some results

Theorem $g(a_1, \ldots, a_n)$ exists and it is finite.

Theorem (Sylvester, 1882) $g(a_1, a_2) = a_1 a_2 - a_1 - a_2$.

Theorem (R.A., 1996) Computing $g(a_1, \ldots, a_n)$ is $\mathcal{NP}$-hard. (under Turing reductions)

Some results

Theorem $g(a_1, \ldots, a_n)$ exists and it is finite.

Theorem (Sylvester, 1882) $g(a_1, a_2) = a_1 a_2 - a_1 - a_2$.

Theorem (R.A., 1996) Computing $g(a_1, \ldots, a_n)$ is $\mathcal{NP}$-hard. (under Turing reductions)

Proof (sketch).

Some results

Theorem $g(a_1, \ldots, a_n)$ exists and it is finite.

Theorem (Sylvester, 1882) $g(a_1, a_2) = a_1 a_2 - a_1 - a_2$.

Theorem (R.A., 1996) Computing $g(a_1, \ldots, a_n)$ is $\mathcal{NP}$-hard. (under Turing reductions)

Proof (sketch).

[**IKP**] Input: positive integers $a_1, \ldots, a_n$ and t,

Question: do there exist integers $x_i \geq 0$,

with $1 \leq i \leq n$ such that $\sum_{i=1}^{n} x_i a_i = t$?

It is known that [**IKP**] is NP-complete.

Procedure

Find $g(a_1, \ldots, a_n)$

IF $t > g(a_1, \ldots, a_n)$ THEN **IKP** is answered affirmatively

ELSE

IF $t = g(a_1, \ldots a_n)$ THEN

IKP is answered negatively

ELSE

Find $g(\bar{a}_1, \ldots, \bar{a}_n, \bar{a}_{n+1})$, $\bar{a}_i = 2a_i$, $i = 1, \ldots, n$ and $\bar{a}_{n+1} = 2g(a_1, \ldots, a_n) + 1$ (note that $(\bar{a}_1, \ldots, \bar{a}_n, \bar{a}_{n+1}) = 1$)

Find $g(\bar{a}_1, \ldots, \bar{a}_n, \bar{a}_{n+1}, \bar{a}_{n+2})$, $\bar{a}_{n+2} = g(\bar{a}_1, \ldots, \bar{a}_n, \bar{a}_{n+1}) - 2t$

IKP is answered affirmatively if and only if $g(\bar{a}_1, \ldots, \bar{a}_{n+2}) < g(\bar{a}_1, \ldots, \bar{a}_{n+1})$

Methods

For $n = 3$

- Selmer and Bayer, 1978
- Rödseth, 1978
- Davison, 1994
- Scarf and Shallcross, 1993

Methods

For $n = 3$

- Selmer and Bayer, 1978
- Rödseth, 1978
- Davison, 1994
- Scarf and Shallcross, 1993

For $n \geq 4$

- Heap and Lynn, 1964
- Wilf, 1978
- Nijenhuis, 1979
- Greenberg, 1980
- Killingbergto, 2000
- Einstein, Lichtblau, Strzebonski and Wagon, 2007
- Roune, 2008

Kannan's method

Let P be a closed bounded convex set in $\mathbb{R}^n$ and let L be a lattice of dimension n also in $\mathbb{R}^n$.

Kannan's method

Let P be a closed bounded convex set in $\mathbb{R}^n$ and let L be a lattice of dimension n also in $\mathbb{R}^n$.

The least positive real t so that $tP + L$ equals $\mathbb{R}^n$ is called the covering radius of P with respect to L (denoted by $\mu(P, L)$).

Kannan's method

Let P be a closed bounded convex set in $\mathbb{R}^n$ and let L be a lattice of dimension n also in $\mathbb{R}^n$.

The least positive real t so that $tP + L$ equals $\mathbb{R}^n$ is called the covering radius of P with respect to L (denoted by $\mu(P, L)$).

Theorem (Kannan, 1992) Let

$$L = \{(x_1, \ldots, x_{n-1}) | x_i \text{ integers and } \sum_{i=1}^{n-1} a_i x_i \equiv 0 \; (mod \;\; a_n)$$

and

$$S = \{(x_1, \ldots, x_{n-1}) | x_i \geq 0 \text{ reals and } \sum_{i=1}^{n-1} a_i x_i \leq 1\}.$$

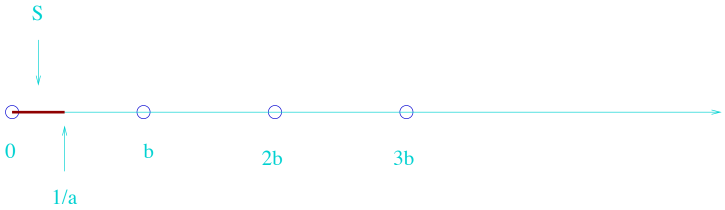
Then, $\mu(S, L) = g(a_1, \ldots, a_n) + a_1 + \cdots + a_n$.

Example 1

Let a_1, a_2 be positive integers with $\gcd(a_1, a_2) = 1$.

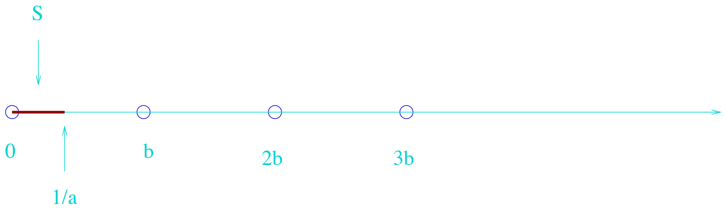
Example 1

Let a_1, a_2 be positive integers with $\gcd(a_1, a_2) = 1$.



Example 1

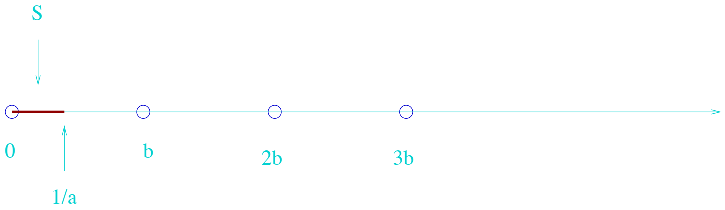
Let a_1, a_2 be positive integers with $\gcd(a_1, a_2) = 1$.



The minimum integer t such that tS covers the interval $[0, b]$ is ab.

Example 1

Let a_1, a_2 be positive integers with $\gcd(a_1, a_2) = 1$.



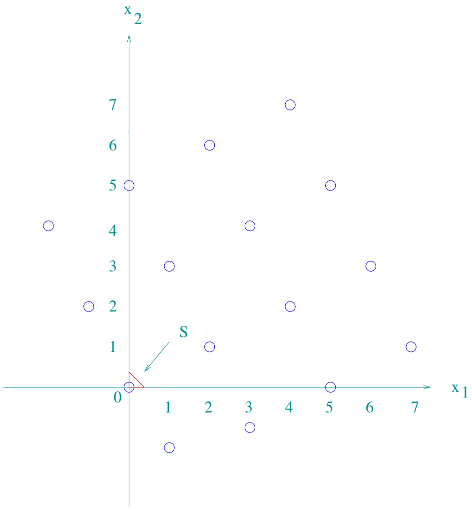
The minimum integer t such that tS covers the interval $[0, b]$ is ab.
Then, $g(a, b) = \mu(S, L) - a - b = ab - a - b$.

Example 2

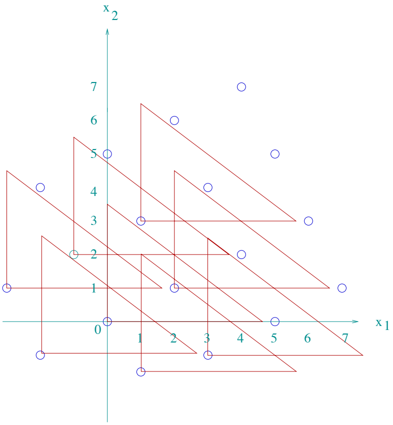
Let $a_1 = 3, a_2 = 4$ and $a_3 = 5.$

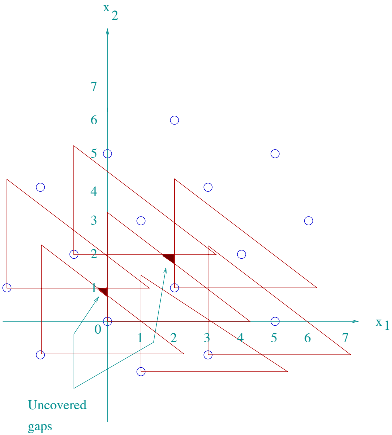
Example 2

Let $a_1 = 3$, $a_2 = 4$ and $a_3 = 5$.

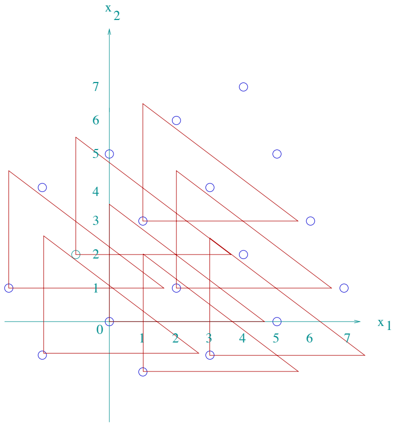


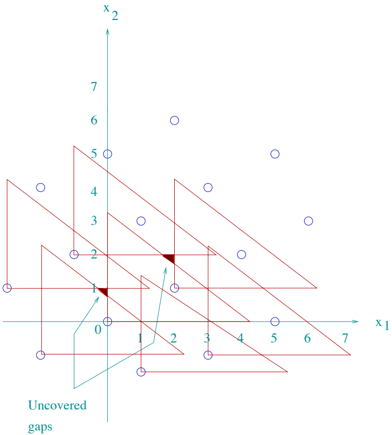
Notice that (14)S covers the plane while (13)S does not.





Notice that $(14)S$ covers the plane while $(13)S$ does not.





Then $\mu(S, L) = 14$ and thus $g(3, 4, 5) = \mu(S, L) - 3 - 4 - 5 = 2$.

Algorithms

Theorem (Kannan, 1992) There is a polynomial time algorithm to compute $g(a_1, \ldots, a_n)$ when $n \geq 2$ is fixed.

Theorem (Kannan, 1992) There is a polynomial time algorithm to compute $g(a_1, \dots, a_n)$ when $n \geq 2$ is fixed.

Theorem (Fukshansky, Robins, 2005) Relate the Frobenius number to a covering radius of a Euclidean ball with respect to a different lattices.

Algorithms

Theorem (Kannan, 1992) There is a polynomial time algorithm to compute $g(a_1, \ldots, a_n)$ when $n \geq 2$ is fixed.

Theorem (Fukshansky, Robins, 2005) Relate the Frobenius number to a covering radius of a Euclidean ball with respect to a different lattices.

Einstein, Lichtblau, Strzebonski and Wagon (algebraic method)
Find $g(a_1, \ldots, a_4)$ involving 100-digit numbers in about one second
Find $g(a_1, \ldots, a_{10})$ involving 10-digit numbers in two days

Algorithms

Theorem (Kannan, 1992) There is a polynomial time algorithm to compute $g(a_1, \ldots, a_n)$ when $n \geq 2$ is fixed.

Theorem (Fukshansky, Robins, 2005) Relate the Frobenius number to a covering radius of a Euclidean ball with respect to a different lattices.

Einstein, Lichtblau, Strzebonski and Wagon (algebraic method)
Find $g(a_1, \ldots, a_4)$ involving 100-digit numbers in about one second
Find $g(a_1, \ldots, a_{10})$ involving 10-digit numbers in two days

Roune (algebraic method)
Find $g(a_1, \ldots, a_4)$ involving 10 000-digit numbers in few second
Find $g(a_1, \ldots, a_{13})$ involving 10-digit numbers in few days

Algorithms

Theorem (Kannan, 1992) There is a polynomial time algorithm to compute $g(a_1, \ldots, a_n)$ when $n \geq 2$ is fixed.

Theorem (Fukshansky, Robins, 2005) Relate the Frobenius number to a covering radius of a Euclidean ball with respect to a different lattices.

Einstein, Lichtblau, Strzebonski and Wagon (algebraic method)
Find $g(a_1, \ldots, a_4)$ involving 100-digit numbers in about one second
Find $g(a_1, \ldots, a_{10})$ involving 10-digit numbers in two days

Roune (algebraic method)
Find $g(a_1, \ldots, a_4)$ involving 10 000-digit numbers in few second
Find $g(a_1, \ldots, a_{13})$ involving 10-digit numbers in few days

Packages
http://www.broune.com/frobby/
http://www.math.ruu.nl/people/beukers/frobenius/
http://cmup.fc.up.pt/cmup/mdelgado/numericalsgps/
http://reference.wolfram.com/mathematica/ref/FrobeniusNumber.html

A semigroup S is called symmetric if $S \cup (g - S) = \mathbb{Z}$.

A semigroup S is called symmetric if $S \cup (g - S) = \mathbb{Z}$.

(Bresinsky, 1979) Monomial curves
(Kunz, 1979, Herzog, 1970) Gorestein rings
(Apéry, 1945) Classification plane of algebraic branches
(Buchweitz, 1981) Weierstrass semigroups
(Pellikaan and Torres, 1999) Algebraic codes

Shell-sort method

Shell-sort method

3,2,7,9,8,1,1,5,2,6

Shell-sort method

3,2,7,9,8,1,1,5,2,6 (increment sequence: 7,3,1)

Shell-sort method

3,2,7,9,8,1,1,5,2,6 (increment sequence: 7,3,1)

7-sorted: 3,2,6,9,8,1,1,5,2,7

Shell-sort method

3,2,7,9,8,1,1,5,2,6 (increment sequence: 7,3,1)

7-sorted: 3,2,6,9,8,1,1,5,2,7

3-sorted: 1,2,1,3,5,2,7,8,6,9

Shell-sort method

3,2,7,9,8,1,1,5,2,6 (increment sequence: 7,3,1)

7-sorted: 3,2,6,9,8,1,1,5,2,7

3-sorted: 1,2,1,3,5,2,7,8,6,9

1-sorted: 1,1,2,2,3,5,6,7,8,9

Shell-sort method

Lemme (Incerpi and Sedgewick, 1985) The number of steps required to h_j-sort a set on N integers that is already $h_{j+1} - h_{j+2} - \cdots - h_t$-sorted is

$$O\left(\frac{Ng(h_{j+1}, h_{j+2}, \ldots, h_t)}{h_j}\right)$$

Shell-sort method

Lemme (Incerpi and Sedgewick, 1985) The number of steps required to h_j-sort a set on N integers that is already $h_{j+1} - h_{j+2} - \cdots - h_t$-sorted is

$$O\left(\frac{Ng(h_{j+1}, h_{j+2}, \ldots, h_t)}{h_j}\right)$$

Theorem (Incerpi, Sedgewick, 1985) The running time of Shell-sort is $O(N^{3/2})$ where N is the number of elements in the file (on average and in worst case).

Shell-sort method

Lemme (Incerpi and Sedgewick, 1985) The number of steps required to h_j-sort a set on N integers that is already $h_{j+1} - h_{j+2} - \cdots - h_t$-sorted is

$$O\left(\frac{Ng(h_{j+1}, h_{j+2}, \ldots, h_t)}{h_j}\right)$$

Theorem (Incerpi, Sedgewick, 1985) The running time of Shell-sort is $O(N^{3/2})$ where N is the number of elements in the file (on average and in worst case).

Conjecture (Gonnet, 1984)The asymptotic growth of the average case running time of Shell-sort is $O(N \log N \log\log N)$ where N is the number of elements in the file.

Basics on posets

Let $(\mathcal{P}, \leq)$ be a locally finite poset, i.e,

- the set $\mathcal{P}$ is partially ordered by $\leq$, and
- for every $a, b \in \mathcal{P}$ the set $\{c \in \mathcal{P} \mid a \leq c \leq b\}$ is finite.

Let $(\mathcal{P}, \leq)$ be a locally finite poset, i.e,

- the set $\mathcal{P}$ is partially ordered by $\leq$, and
- for every $a, b \in \mathcal{P}$ the set $\{c \in \mathcal{P} \mid a \leq c \leq b\}$ is finite.

A chain of length $l \geq 0$ between $a, b \in \mathcal{P}$ is

$$\{a = a_0 < a_1 < \cdots < a_l = b\} \subset \mathcal{P}.$$

We denote by $c_l(a, b)$ the number of chains of length l between a and b.

Let $(\mathcal{P}, \leq)$ be a locally finite poset, i.e,

- the set $\mathcal{P}$ is partially ordered by $\leq$, and
- for every $a, b \in \mathcal{P}$ the set $\{c \in \mathcal{P} \mid a \leq c \leq b\}$ is finite.

A chain of length $l \geq 0$ between $a, b \in \mathcal{P}$ is

$$\{a = a_0 < a_1 < \cdots < a_l = b\} \subset \mathcal{P}.$$

We denote by $c_l(a, b)$ the number of chains of length l between a and b. The Möbius function $\mu_{\mathcal{P}}$ is the function

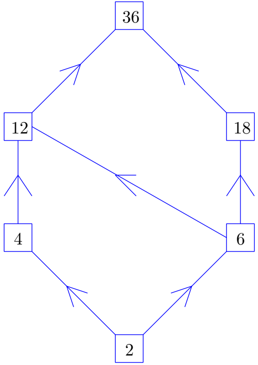
$$\mu_{\mathcal{P}} : \mathcal{P} \times \mathcal{P} \longrightarrow \mathbb{Z}$$

$$\mu_{\mathcal{P}}(a, b) = \sum_{l \geq 0} (-1)^l c_l(a, b)$$

Example

Consider the poset $(\mathbb{N}, |\,)$ of nonnegative integers ordered by divisibility, i.e., $a \mid b \iff a$ divides b. Let us compute $\mu_{\mathbb{N}}(2, 36)$. We observe that $\{c \in \mathbb{N};\ 2 \mid c \mid 36\} = \{2, 4, 6, 12, 18, 36\}$. Chains of

- length 1 $\rightarrow$ $\{2, 36\}$
- length 2 $\begin{cases} \{2, 4, 36\} \\ \{2, 6, 36\} \\ \{2, 12, 36\} \\ \{2, 18, 36\} \end{cases}$
- length 3 $\begin{cases} \{2, 4, 12, 36\} \\ \{2, 6, 12, 26\} \\ \{2, 6, 18, 36\} \end{cases}$



Thus,

$$\mu_{\mathbb{N}}(2, 36) = -c_1(2, 36) + c_2(2, 36) - c_3(2, 36) = -1 + 4 - 3 = 0.$$

Möbius classical arithmetic function

Given $n \in \mathbb{N}$ the Möbius arithmetic function $\mu(n)$ is defined as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n = p_1 \cdots p_k \text{ with } p_i \text{ distincts primes}, \\ 0 & \text{otherwise i.e; } n \text{ admits at least one square} \\ & \text{factor bigger than one.} \end{cases}$$

Möbius classical arithmetic function

Given $n \in \mathbb{N}$ the Möbius arithmetic function $\mu(n)$ is defined as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n = p_1 \cdots p_k \text{ with } p_i \text{ distincts primes,} \\ 0 & \text{otherwise i.e; } n \text{ admits at least one square} \\ & \text{factor bigger than one.} \end{cases}$$

Example : $\mu(2) = \mu(7) = -1, \mu(4) = \mu(8) = 0, \mu(6) = \mu(10) = 1.$

Möbius classical arithmetic function

Given $n \in \mathbb{N}$ the Möbius arithmetic function $\mu(n)$ is defined as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n = p_1 \cdots p_k \text{ with } p_i \text{ distincts primes,} \\ 0 & \text{otherwise i.e; } n \text{ admits at least one square} \\ & \text{factor bigger than one.} \end{cases}$$

Example : $\mu(2) = \mu(7) = -1, \mu(4) = \mu(8) = 0, \mu(6) = \mu(10) = 1.$

The inverse of the Riemann function ζ, $s \in \mathbb{C}, Re(s) > 0$

$$\zeta^{-1}(s) = \left(\sum_{n=1}^{+\infty} \frac{1}{n^s}\right)^{-1} = \prod_{p-prime} (1 - p^{-1}) = \sum_{n=1}^{+\infty} \frac{\mu(n)}{n^2}.$$

Möbius classical arithmetic function

There are impressive results using μ, for instance for an integer n

$$Pr(n \text{ do not contain a square factor }) = \frac{6}{\pi^2}$$

Möbius classical arithmetic function

There are impressive results using μ, for instance for an integer n

$$Pr(n \text{ do not contain a square factor }) = \frac{6}{\pi^2}$$

For $(\mathbb{N}, |\,)$ we have that for all $a, b \in \mathbb{N}$

$$\mu_{\mathbb{N}}(a,b) = \begin{cases} (-1)^r & \text{if } b/a \text{ is a product of } r \text{ distinct primes,} \\ 0 & \text{otherwise.} \end{cases}$$

$\mu_{\mathbb{N}}(2, 36) = 0$ because $36/2 = 18 = 2 \cdot 3^2$

Semigroup poset

Let $\mathcal{S} := \langle a_1, \ldots, a_n \rangle \subset \mathbb{N}^m$ denote the subsemigroup of $\mathbb{N}^m$ generated by $a_1, \ldots, a_n \in \mathbb{N}^m$, i.e.,

$$\mathcal{S} := \langle a_1, \ldots, a_n \rangle = \{x_1 a_1 + \cdots + x_n a_n \,|\, x_1, \ldots, x_n \in \mathbb{N}\}.$$

Semigroup poset

Let $\mathcal{S} := \langle a_1, \dots, a_n \rangle \subset \mathbb{N}^m$ denote the subsemigroup of $\mathbb{N}^m$ generated by $a_1, \dots, a_n \in \mathbb{N}^m$, i.e.,

$$\mathcal{S} := \langle a_1, \dots, a_n \rangle = \{x_1 a_1 + \cdots + x_n a_n \,|\, x_1, \dots, x_n \in \mathbb{N}\}.$$

The semigroup $\mathcal{S}$ induces an partial order $\leq_{\mathcal{S}}$ on $\mathbb{N}^m$ given by

$$x \leq_{\mathcal{S}} y \Longleftrightarrow y - x \in \mathcal{S}.$$

We denote by $\mu_{\mathcal{S}}$ the Möbius function associated to $(\mathbb{N}^m, \leq_{\mathcal{S}})$.

Let $\mathcal{S} := \langle a_1, \ldots, a_n \rangle \subset \mathbb{N}^m$ denote the subsemigroup of $\mathbb{N}^m$ generated by $a_1, \ldots, a_n \in \mathbb{N}^m$, i.e.,

$$\mathcal{S} := \langle a_1, \ldots, a_n \rangle = \{x_1 a_1 + \cdots + x_n a_n \,|\, x_1, \ldots, x_n \in \mathbb{N}\}.$$

The semigroup $\mathcal{S}$ induces an partial order $\leq_{\mathcal{S}}$ on $\mathbb{N}^m$ given by

$$x \leq_{\mathcal{S}} y \iff y - x \in \mathcal{S}.$$

We denote by $\mu_{\mathcal{S}}$ the Möbius function associated to $(\mathbb{N}^m, \leq_{\mathcal{S}})$.

It is easy to check that $\mu_{\mathcal{S}}(x, y) = 0$ if $y - x \notin \mathbb{N}^m$, or $\mu_{\mathcal{S}}(x, y) = \mu_{\mathcal{S}}(0, y - x)$ otherwise. Hence we shall only consider the reduced Möbius function $\mu_{\mathcal{S}} : \mathbb{N}^m \longrightarrow \mathbb{Z}$ defined by

$$\mu_{\mathcal{S}}(x) := \mu_{\mathcal{S}}(0, x) \quad \text{for all } x \in \mathbb{N}^m.$$

Known results about $\mu_{\mathcal{S}}$

Theorem (Deddens, 1979) For $\mathcal{S} = \langle a, b \rangle \subset \mathbb{N}$ where $a, b \in \mathbb{Z}^+$ are relatively prime:

$$\mu_{\mathcal{S}}(x) = \begin{cases} 1 & \text{if } x \equiv 0 \text{ or } a+b \pmod{ab}, \\ -1 & \text{if } x \equiv a \text{ or } b \pmod{ab}, \\ 0 & \text{otherwise.} \end{cases}$$

Known results about $\mu_{\mathcal{S}}$

Theorem (Deddens, 1979) For $\mathcal{S} = \langle a, b \rangle \subset \mathbb{N}$ where $a, b \in \mathbb{Z}^+$ are relatively prime:

$$\mu_{\mathcal{S}}(x) = \begin{cases} 1 & \textit{if } x \equiv 0 \textit{ or } a+b \ (\textit{mod } ab), \\ -1 & \textit{if } x \equiv a \textit{ or } b \ (\textit{mod } ab), \\ 0 & \textit{otherwise}. \end{cases}$$

Theorem (Chappelon, R.A., 2013) Provide a recursive formula for $\mu_{\mathcal{S}}$ when $\mathcal{S} = \langle a, a+d, \ldots, a+kd \rangle \subset \mathbb{N}$ for some $a, k, d \in \mathbb{Z}^+$, and a semi-explicit formula for $\mathcal{S} = \langle a, a+d, a+2d \rangle \subset \mathbb{N}$ where $a, d \in \mathbb{Z}^+$, $\gcd\{a, a+d, a+2d\} = 1$ and a is even.

Known results about $\mu_{\mathcal{S}}$

Theorem (Deddens, 1979) For $\mathcal{S} = \langle a, b \rangle \subset \mathbb{N}$ where $a, b \in \mathbb{Z}^+$ are relatively prime:

$$\mu_{\mathcal{S}}(x) = \begin{cases} 1 & \textit{if } x \equiv 0 \textit{ or } a+b \ (\textit{mod } ab), \\ -1 & \textit{if } x \equiv a \textit{ or } b \ (\textit{mod } ab), \\ 0 & \textit{otherwise}. \end{cases}$$

Theorem (Chappelon, R.A., 2013) Provide a recursive formula for $\mu_{\mathcal{S}}$ when $\mathcal{S} = \langle a, a+d, \ldots, a+kd \rangle \subset \mathbb{N}$ for some $a, k, d \in \mathbb{Z}^+$, and a semi-explicit formula for $\mathcal{S} = \langle a, a+d, a+2d \rangle \subset \mathbb{N}$ where $a, d \in \mathbb{Z}^+$, $\gcd\{a, a+d, a+2d\} = 1$ and a is even.

Remark In both papers the authors approach the problem by a thorough study of the intrinsic properties of each semigroup.

Hilbert series of a semigroup

Let $\mathcal{S} \subset \mathbb{N}^m$ be a semigroup and let k be a field of characteristic 0. A ring R is called affine semigroup ring associated to $\mathcal{S}$ if $R = k[\mathcal{S}]$ is the subring of $k[x_1, \ldots, x_n]$ with k-basis given by the monomials $\mathbf{x}^\lambda = x_1^{\lambda_1} \cdots x_n^{\lambda_n}$ for each element $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathcal{S}$.

Hilbert series of a semigroup

Let $\mathcal{S} \subset \mathbb{N}^m$ be a semigroup and let k be a field of characteristic 0. A ring R is called affine semigroup ring associated to $\mathcal{S}$ if $R = k[\mathcal{S}]$ is the subring of $k[x_1, \dots, x_n]$ with k-basis given by the monomials $\mathbf{x}^\lambda = x_1^{\lambda_1} \cdots x_n^{\lambda_n}$ for each element $\lambda = (\lambda_1, \dots, \lambda_n) \in \mathcal{S}$.

The multivariate Hilbert series associated to $\mathcal{S}$ is

$$\mathcal{H}_{\mathcal{S}}(\mathbf{t}) := \sum_{b \in \mathcal{S}} \mathbf{t}^b \in \mathbb{Z}[[t_1, \dots, t_m]]$$

where $\mathbf{t}^b := t_1^{b_1} \cdots t_m^{b_m}$ for each $b = (b_1, \dots, b_m) \in \mathbb{N}^m$.

Hilbert series of a semigroup

Let $\mathcal{S} \subset \mathbb{N}^m$ be a semigroup and let k be a field of characteristic 0. A ring R is called affine semigroup ring associated to $\mathcal{S}$ if $R = k[\mathcal{S}]$ is the subring of $k[x_1, \ldots, x_n]$ with k-basis given by the monomials $\mathbf{x}^\lambda = x_1^{\lambda_1} \cdots x_n^{\lambda_n}$ for each element $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathcal{S}$.

The multivariate Hilbert series associated to $\mathcal{S}$ is

$$\mathcal{H}_{\mathcal{S}}(\mathbf{t}) := \sum_{b \in \mathcal{S}} \mathbf{t}^b \in \mathbb{Z}[[t_1, \ldots, t_m]]$$

where $\mathbf{t}^b := t_1^{b_1} \cdots t_m^{b_m}$ for each $b = (b_1, \ldots, b_m) \in \mathbb{N}^m$.

Hilbert has proved that

$$\mathcal{H}_{\mathcal{S}}(\mathbf{t}) = \frac{Q(\mathbf{t})}{(1 - \mathbf{t}^{c_1}) \cdots (1 - \mathbf{t}^{c_k})}$$

for some $c_1, \ldots, c_k \in \mathbb{N}^m$

Hilbert series

If $\mathcal{S} = \langle a_1, \ldots, a_n \rangle$ then $\mathcal{H}_{\mathcal{S}}(t) = \frac{Q(t)}{(1-t^{a_1})\cdots(1-t^{a_n})}$
and $g(a_1, \ldots, a_n) =$ degree of $\mathcal{H}_{\mathcal{S}}(t)$.

Hilbert series

If $\mathcal{S} = \langle a_1, \ldots, a_n \rangle$ then $\mathcal{H}_{\mathcal{S}}(t) = \frac{Q(t)}{(1-t^{a_1})\cdots(1-t^{a_n})}$
and $g(a_1, \ldots, a_n) =$ degree of $\mathcal{H}_{\mathcal{S}}(t)$.

The Apéry set of $\mathcal{S}$ for $m \in \mathcal{S}$ is $Ap(\mathcal{S}; m) = \{s \in \mathcal{S} \mid s - m \notin \mathcal{S}\}$.

Hilbert series

If $\mathcal{S} = \langle a_1, \ldots, a_n \rangle$ then $\mathcal{H}_{\mathcal{S}}(t) = \frac{Q(t)}{(1-t^{a_1})\cdots(1-t^{a_n})}$
and $g(a_1, \ldots, a_n) =$ degree of $\mathcal{H}_{\mathcal{S}}(t)$.

The Apéry set of $\mathcal{S}$ for $m \in \mathcal{S}$ is $Ap(\mathcal{S}; m) = \{s \in \mathcal{S} \mid s - m \notin \mathcal{S}\}$.

$$\mathcal{S} = Ap(\mathcal{S}; m) + m\mathbb{Z}_{\geq 0}, \quad \mathcal{H}_{\mathcal{S}}(t) = \frac{1}{1-t^m} \sum_{w \in Ap(\mathcal{S};m)} t^w$$

Hilbert series

If $\mathcal{S} = \langle a_1, \ldots, a_n \rangle$ then $\mathcal{H}_\mathcal{S}(t) = \frac{Q(t)}{(1-t^{a_1})\cdots(1-t^{a_n})}$
and $g(a_1, \ldots, a_n) =$ degree of $\mathcal{H}_\mathcal{S}(t)$.

The Apéry set of $\mathcal{S}$ for $m \in \mathcal{S}$ is $Ap(\mathcal{S}; m) = \{s \in \mathcal{S} \mid s - m \notin \mathcal{S}\}$.

$$\mathcal{S} = Ap(\mathcal{S}; m) + m\mathbb{Z}_{\geq 0}, \quad \mathcal{H}_\mathcal{S}(t) = \frac{1}{1-t^m} \sum_{w \in Ap(\mathcal{S};m)} t^w$$

Theorem (R.A., Rödseth, 2008) For $\mathcal{S} = \langle a, a+d, \ldots, a+kd, c \rangle$

$$\mathcal{H}_\mathcal{S}(t) = \frac{F_{s_v}(a;t)(1 - t^{c(P_{v+1}-P_v)}) + F_{s_v - s_{v+1}}(a;t)(t^{c(P_{v+1}-P_v)} - t^{cP_{v+1}})}{(1-t^a)(1-t^d)(1-t^{a+kd})(1-t^c)}$$

where $s_v, s_{v+1}, P_v, P_{v+1}$ are some *particular* integers.

Example 1

For $\mathcal{S} = \langle 2, 3 \rangle \subset \mathbb{N}$, we have that $\mathcal{S} = \{0, 2, 3, 4, 5 \ldots\}$

$$\mathcal{H}_{\mathcal{S}}(t) = 1 + t^2 + t^3 + t^4 + t^5 + \cdots$$

Example 1

For $\mathcal{S} = \langle 2, 3 \rangle \subset \mathbb{N}$, we have that $\mathcal{S} = \{0, 2, 3, 4, 5 \ldots\}$

$$\mathcal{H}_{\mathcal{S}}(t) = 1 + t^2 + t^3 + t^4 + t^5 + \cdots$$

$$t^2 \mathcal{H}_{\mathcal{S}}(t) = t^2 + t^4 + t^5 + \cdots$$

Then, $(1 - t^2)\,\mathcal{H}_{\mathcal{S}}(t) = 1 + t^3$, and

$$\mathcal{H}_{\mathcal{S}}(t) = \frac{1 + t^3}{1 - t^2}$$

Example 2

For $\mathcal{S} = \mathbb{N}^m$, we have that

$$
\begin{aligned}
\mathcal{H}_{\mathcal{S}}(\mathbf{t}) &= \sum_{b \in \mathbb{N}^m} \mathbf{t}^b \\
&= \sum_{(b_1,\ldots,b_m)\in\mathbb{N}^m} t_1^{b_1} \cdots t_m^{b_m} \\
&= (1 + t_1 + t_1^2 + \cdots) \cdots (1 + t_m + t_m^2 + \cdots) \\
&= \frac{1}{(1-t_1)} \cdots \frac{1}{(1-t_m)} \\
&= \frac{1}{(1-t_1)\cdots(1-t_m)}.
\end{aligned}
$$

Möbius function via Hilbert series

Assume that one can write

$$\mathcal{H}_{\mathcal{S}}(\mathbf{t}) = \frac{\sum_{b \in \Delta} f_b \, \mathbf{t}^b}{(1 - \mathbf{t}^{c_1}) \cdots (1 - \mathbf{t}^{c_k})}$$

for some finite set $\Delta \subset \mathbb{N}^m$ and some $c_1, \ldots, c_k \in \mathbb{N}^m$.

Möbius function via Hilbert series

Assume that one can write

$$\mathcal{H}_{\mathcal{S}}(\mathbf{t}) = \frac{\sum_{b\in\Delta} f_b\, \mathbf{t}^b}{(1-\mathbf{t}^{c_1})\cdots(1-\mathbf{t}^{c_k})}$$

for some finite set $\Delta \subset \mathbb{N}^m$ and some $c_1, \ldots, c_k \in \mathbb{N}^m$.

Theorem 1 (Chappelon, Montejano, Garcia Marco, R.A., 2015)

$$\sum_{b\in\Delta} f_b\ \mu_{\mathcal{S}}(x-b) = 0$$

for all $x \notin \{\sum_{i\in A} c_i \,|\, A \subset \{1,\ldots,k\}\}$.

Example: $S = \langle 2, 3 \rangle$

We know that,

$$\mathcal{H}_S(t) = \frac{1+t^3}{1-t^2}.$$

Example: $\mathcal{S} = \langle 2, 3 \rangle$

We know that,

$$\mathcal{H}_{\mathcal{S}}(t) = \frac{1 + t^3}{1 - t^2}.$$

By Theorem 1 we have that

$$\mu_{\mathcal{S}}(x) + \mu_{\mathcal{S}}(x - 3) = 0$$

for all $x \notin \{0, 2\}$.

We know that,

$$\mathcal{H}_{\mathcal{S}}(t) = \frac{1+t^3}{1-t^2}.$$

By Theorem 1 we have that

$$\mu_{\mathcal{S}}(x) + \mu_{\mathcal{S}}(x-3) = 0$$

for all $x \notin \{0, 2\}$. It is evident that $\mu_{\mathcal{S}}(0) = 1$ and a direct computation yields $\mu_{\mathcal{S}}(2) = -1$.

Hence,

$$\mu_{\mathcal{S}}(x) = \begin{cases} 1 & \textit{if } x \equiv 0 \textit{ or } 5 \ (\textit{mod } 6), \\ -1 & \textit{if } x \equiv 2 \textit{ or } 3 \ (\textit{mod } 6), \\ 0 & \textit{otherwise}. \end{cases}$$

We consider $\mathcal{G}_{\mathcal{S}}$ the generating function of the Möbius function, which is

$$\mathcal{G}_{\mathcal{S}}(\mathbf{t}) := \sum_{b \in \mathbb{N}^m} \mu_{\mathcal{S}}(b)\,\mathbf{t}^b.$$

We consider $\mathcal{G}_{\mathcal{S}}$ the generating function of the Möbius function, which is

$$\mathcal{G}_{\mathcal{S}}(\mathbf{t}) := \sum_{b \in \mathbb{N}^m} \mu_{\mathcal{S}}(b)\, \mathbf{t}^b.$$

Theorem 2 (Chappelon, Montejano, Garcia Marco, R.A., 2015)

$$\mathcal{H}_{\mathcal{S}}(\mathbf{t})\ \mathcal{G}_{\mathcal{S}}(\mathbf{t}) = 1.$$

Example: $S = \mathbb{N}^m$

We denote $\{e_1, \ldots, e_m\}$ the canonical basis of $\mathbb{N}^m$, i.e., $e_1 = (1, 0, \ldots, 0), \ldots, e_m = (0, \ldots, 0, 1) \in \mathbb{N}^m$.

Example: $\mathcal{S} = \mathbb{N}^m$

We denote $\{e_1, \ldots, e_m\}$ the canonical basis of $\mathbb{N}^m$, i.e., $e_1 = (1, 0, \ldots, 0), \ldots, e_m = (0, \ldots, 0, 1) \in \mathbb{N}^m$.

We know that

$$\mathcal{H}_{\mathbb{N}^m}(\mathbf{t}) = \frac{1}{(1 - t_1)\cdots(1 - t_m)}$$

Example: $\mathcal{S} = \mathbb{N}^m$

We denote $\{e_1, \dots, e_m\}$ the canonical basis of $\mathbb{N}^m$, i.e.,
$e_1 = (1, 0, \dots, 0), \dots, e_m = (0, \dots, 0, 1) \in \mathbb{N}^m$.

We know that

$$\mathcal{H}_{\mathbb{N}^m}(\mathbf{t}) = \frac{1}{(1-t_1)\cdots(1-t_m)}$$

By Theorem 2 we have that

$$\mathcal{G}_{\mathbb{N}^m}(\mathbf{t}) = (1-t_1)\cdots(1-t_m) = \sum_{A \subset \{1,\dots,m\}} (-1)^{|A|} \, \mathbf{t}^{\sum_{i \in A} e_i}.$$

Example: $\mathcal{S} = \mathbb{N}^m$

We denote $\{e_1, \ldots, e_m\}$ the canonical basis of $\mathbb{N}^m$, i.e., $e_1 = (1, 0, \ldots, 0), \ldots, e_m = (0, \ldots, 0, 1) \in \mathbb{N}^m$.

We know that

$$\mathcal{H}_{\mathbb{N}^m}(\mathbf{t}) = \frac{1}{(1 - t_1) \cdots (1 - t_m)}$$

By Theorem 2 we have that

$$\mathcal{G}_{\mathbb{N}^m}(\mathbf{t}) = (1 - t_1) \cdots (1 - t_m) = \sum_{A \subset \{1, \ldots, m\}} (-1)^{|A|}\, \mathbf{t}^{\sum_{i \in A} e_i}.$$

Hence,

$$\mu_{\mathbb{N}^m}(x) = \begin{cases} (-1)^{|A|} & \textit{if } x = \sum_{i \in A} e_i \textit{ for some } A \subset \{1, \ldots, m\} \\ 0 & \textit{otherwise.} \end{cases}$$

Explicit formulas for $\mu_{\mathcal{S}}$

A semigroup $\mathcal{S} \subset \mathbb{N}^m$ is said to be a semigroup with a unique Betti element $b \in \mathbb{N}^m$ if $I_{\mathcal{S}}$ is generated by $\mathcal{S}$-homogeneous polynomials of $\mathcal{S}$-degree b.

A semigroup $\mathcal{S} \subset \mathbb{N}^m$ is said to be a semigroup with a unique Betti element $b \in \mathbb{N}^m$ if $I_{\mathcal{S}}$ is generated by $\mathcal{S}$-homogeneous polynomials of $\mathcal{S}$-degree b.

Theorem (Chappelon, Montejano, Garcia Marco, R.A., 2015) Set $r := \dim(\mathbb{Q}\{a_1, \ldots, a_n\})$. Then,

$$\mu_{\mathcal{S}}(x) = \sum_{j=1}^{t} (-1)^{|A_j|} \binom{k_j + n - r - 1}{k_j},$$

if $x = \sum_{i \in A_1} a_i + k_1\, b = \cdots = \sum_{i \in A_t} a_i + k_t\, b$ for $k_1, \ldots, k_t \in \mathbb{N}$.

Application

Let $D = \{d_1, \ldots, d_m\}$ be a finite set and let us consider $(\mathcal{P}, \subset)$, the poset of all multisets of D ordered by inclusion.

Application

Let $D = \{d_1, \ldots, d_m\}$ be a finite set and let us consider $(\mathcal{P}, \subset)$, the poset of all multisets of D ordered by inclusion.

For the semigroup $\mathcal{S} = \mathbb{N}^m$, we consider the map

$$\begin{array}{rccc} \psi : & (\mathcal{P}, \subset) & \longrightarrow & (\mathbb{N}^m, \leq_{\mathbb{N}^m}) \\ & A & \mapsto & (m_A(d_1), \ldots, m_A(d_m)), \end{array}$$

where $m_A(d_i)$ denotes the number of times that d_i belongs to A.

Application

Let $D = \{d_1, \ldots, d_m\}$ be a finite set and let us consider $(\mathcal{P}, \subset)$, the poset of all multisets of D ordered by inclusion.

For the semigroup $\mathcal{S} = \mathbb{N}^m$, we consider the map

$$\begin{array}{rccc} \psi : & (\mathcal{P}, \subset) & \longrightarrow & (\mathbb{N}^m, \leq_{\mathbb{N}^m}) \\ & A & \mapsto & (m_A(d_1), \ldots, m_A(d_m)), \end{array}$$

where $m_A(d_i)$ denotes the number of times that d_i belongs to A.

ψ is an poset isomorphism (an order preserving and order reflecting bijection).

Application

Let $D = \{d_1, \ldots, d_m\}$ be a finite set and let us consider $(\mathcal{P}, \subset)$, the poset of all multisets of D ordered by inclusion.

For the semigroup $\mathcal{S} = \mathbb{N}^m$, we consider the map

$$\begin{array}{rccc} \psi : & (\mathcal{P}, \subset) & \longrightarrow & (\mathbb{N}^m, \leq_{\mathbb{N}^m}) \\ & A & \mapsto & (m_A(d_1), \ldots, m_A(d_m)), \end{array}$$

where $m_A(d_i)$ denotes the number of times that d_i belongs to A.

ψ is an poset isomorphism (an order preserving and order reflecting bijection). Hence,

$$\mu_{\mathcal{P}}(A, B) = \mu_{\mathbb{N}^m}(\psi(A), \psi(B)),$$

Let $D = \{d_1, \ldots, d_m\}$ be a finite set and let us consider $(\mathcal{P}, \subset)$, the poset of all multisets of D ordered by inclusion.

For the semigroup $\mathcal{S} = \mathbb{N}^m$, we consider the map

$$\begin{array}{rccc} \psi: & (\mathcal{P}, \subset) & \longrightarrow & (\mathbb{N}^m, \leq_{\mathbb{N}^m}) \\ & A & \mapsto & (m_A(d_1), \ldots, m_A(d_m)), \end{array}$$

where $m_A(d_i)$ denotes the number of times that d_i belongs to A.

ψ is an poset isomorphism (an order preserving and order reflecting bijection). Hence,

$$\mu_{\mathcal{P}}(A, B) = \mu_{\mathbb{N}^m}(\psi(A), \psi(B)),$$

We can obtain the formula for $\mu_{\mathcal{P}}$ by means of $\mu_{\mathbb{N}^m}$.

$$\mu_{\mathcal{P}}(A, B) = \begin{cases} (-1)^{|B \setminus A|} & \textit{if } A \subset B \textit{ and } B \setminus A \textit{ is a set}, \\ 0 & \textit{otherwise}. \end{cases}$$

Application more

Let $p_1, \ldots, p_m$ be m distinct prime numbers, and consider

$$\mathbb{N}_m := \{p_1^{\alpha_1} \cdots p_m^{\alpha_m} \mid \alpha_1, \ldots, \alpha_m \in \mathbb{N}\} \subset \mathbb{N}.$$

Application more

Let $p_1, \ldots, p_m$ be m distinct prime numbers, and consider

$$\mathbb{N}_m := \{p_1^{\alpha_1} \cdots p_m^{\alpha_m} \mid \alpha_1, \ldots, \alpha_m \in \mathbb{N}\} \subset \mathbb{N}.$$

Let us consider the poset $(\mathbb{N}_m, |)$, i.e., $\mathbb{N}_m$ partially ordered by divisibility.

Application more

Let $p_1, \ldots, p_m$ be m distinct prime numbers, and consider

$$\mathbb{N}_m := \{p_1^{\alpha_1} \cdots p_m^{\alpha_m} \mid \alpha_1, \ldots, \alpha_m \in \mathbb{N}\} \subset \mathbb{N}.$$

Let us consider the poset $(\mathbb{N}_m, |)$, i.e., $\mathbb{N}_m$ partially ordered by divisibility.

For the semigroup $\mathcal{S} = \mathbb{N}^m$, we consider the order isomorphism

$$\begin{array}{rccc} \psi : & (\mathbb{N}_m, |) & \longrightarrow & (\mathbb{N}^m, \leq_{\mathbb{N}^m}) \\ & p_1^{\alpha_1} \cdots p_m^{\alpha_m} & \mapsto & (\alpha_1, \ldots, \alpha_m). \end{array}$$

Application more

Let $p_1, \dots, p_m$ be m distinct prime numbers, and consider

$$\mathbb{N}_m := \{p_1^{\alpha_1} \cdots p_m^{\alpha_m} \,|\, \alpha_1, \dots, \alpha_m \in \mathbb{N}\} \subset \mathbb{N}.$$

Let us consider the poset $(\mathbb{N}_m, |)$, i.e., $\mathbb{N}_m$ partially ordered by divisibility.

For the semigroup $\mathcal{S} = \mathbb{N}^m$, we consider the order isomorphism

$$\begin{array}{rccc} \psi : & (\mathbb{N}_m, |) & \longrightarrow & (\mathbb{N}^m, \leq_{\mathbb{N}^m}) \\ & p_1^{\alpha_1} \cdots p_m^{\alpha_m} & \mapsto & (\alpha_1, \dots, \alpha_m). \end{array}$$

Hence, $\mu_{\mathbb{N}_m}(a, b) = \mu_{\mathbb{N}^m}(\psi(a), \psi(b))$, and we can recover the formula for $\mu_{\mathbb{N}_m}$ by means of $\mu_{\mathbb{N}^m}$.

$$\mu_{\mathbb{N}_m}(a, b) = \begin{cases} (-1)^r & \textit{if } b/a \textit{ is a product of } r \textit{ distinct primes}, \\ 0 & \textit{otherwise}. \end{cases}$$