# Semigroups, Frobenius' number and Möbius function

J.L. Ramírez Alfonsín

IMAG, Université de Montpellier

**CombinatoireS Summer School**

Paris, June 29 - July 3 2015

## 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 $\cdots\cdots$

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

## 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 $\cdots\cdots$

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

## 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 $\cdots\cdots$

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

## 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 $\cdots\cdots$

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

## 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 $\cdots\cdots$

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

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

Proof (sketch). Since $\gcd(a_1, \ldots, a_n) = 1$ then $m_1 a_1 + \cdots + m_n a_n = 1$ for some $m_i \in \mathbb{N}$

Let $P$ and $-Q$ be the sum of positive and negative terms and so $P - Q = 1$.

Let $k \geq 0$ then $(a_1 - 1)Q + k = (a_1 - 1)Q + ha_1 + k'$ with $h \geq 0$ and $0 \leq k' < a_1$

So, $(a_1 - 1)Q + k = ha_1 + (a_1 - 1 - k')Q + k'P$.

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

**Proof (sketch).** Since $\gcd(a_1, \ldots, a_n) = 1$ then $m_1 a_1 + \cdots + m_n a_n = 1$ for some $m_i \in \mathbb{N}$

Let $P$ and $-Q$ be the sum of positive and negative terms and so $P - Q = 1$.

Let $k \geq 0$ then $(a_1 - 1)Q + k = (a_1 - 1)Q + ha_1 + k'$ with $h \geq 0$ and $0 \leq k' < a_1$

So, $(a_1 - 1)Q + k = ha_1 + (a_1 - 1 - k')Q + k'P$.

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

**Proof (sketch).** Since $\gcd(a_1, \ldots, a_n) = 1$ then $m_1 a_1 + \cdots + m_n a_n = 1$ for some $m_i \in \mathbb{N}$

Let $P$ and $-Q$ be the sum of positive and negative terms and so $P - Q = 1$.

Let $k \geq 0$ then $(a_1 - 1)Q + k = (a_1 - 1)Q + ha_1 + k'$ with $h \geq 0$ and $0 \leq k' < a_1$

So, $(a_1 - 1)Q + k = ha_1 + (a_1 - 1 - k')Q + k'P$.

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

Proof (sketch). Since $\gcd(a_1, \ldots, a_n) = 1$ then $m_1 a_1 + \cdots + m_n a_n = 1$ for some $m_i \in \mathbb{N}$

Let $P$ and $-Q$ be the sum of positive and negative terms and so $P - Q = 1$.

Let $k \geq 0$ then $(a_1 - 1)Q + k = (a_1 - 1)Q + ha_1 + k'$ with $h \geq 0$ and $0 \leq k' < a_1$

So, $(a_1 - 1)Q + k = ha_1 + (a_1 - 1 - k')Q + k'P$.

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

**Proof (sketch).** Since $\gcd(a_1, \ldots, a_n) = 1$ then $m_1 a_1 + \cdots + m_n a_n = 1$ for some $m_i \in \mathbb{N}$

Let $P$ and $-Q$ be the sum of positive and negative terms and so $P - Q = 1$.

Let $k \geq 0$ then $(a_1 - 1)Q + k = (a_1 - 1)Q + ha_1 + k'$ with $h \geq 0$ and $0 \leq k' < a_1$

So, $(a_1 - 1)Q + k = ha_1 + (a_1 - 1 - k')Q + k'P$.

Theorem (Sylvester, 1882) $g(a, b) = ab - a - b$

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

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 $\sum_{i=1}^{n} x_i a_i = t$?

Theorem (Sylvester, 1882) $g(a, b) = ab - a - b$

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

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 $\sum_{i=1}^{n} x_i a_i = t$?

Theorem (Sylvester, 1882) $g(a,b) = ab - a - b$

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

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 $\sum_{i=1}^{n} x_i a_i = t$?

Theorem (Sylvester, 1882) $g(a,b) = ab - a - b$

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

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 $\sum_{i=1}^{n} x_i a_i = t$?

## 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

When $n = 3$

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

When $n \geq 4$

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

## Methods

When $n = 3$

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

When $n \geq 4$

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

## Methods

When $n = 3$

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

When $n \geq 4$

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

## Kannan's result

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

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

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

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

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

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

Theorem (Kannan, 1992) Let

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

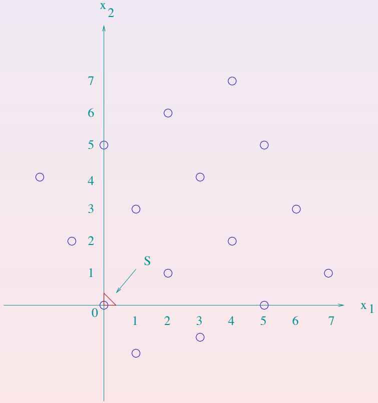
and

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

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

Example 1: Let $a_1 = 3, a_2 = 4$ and $a_3 = 5$.

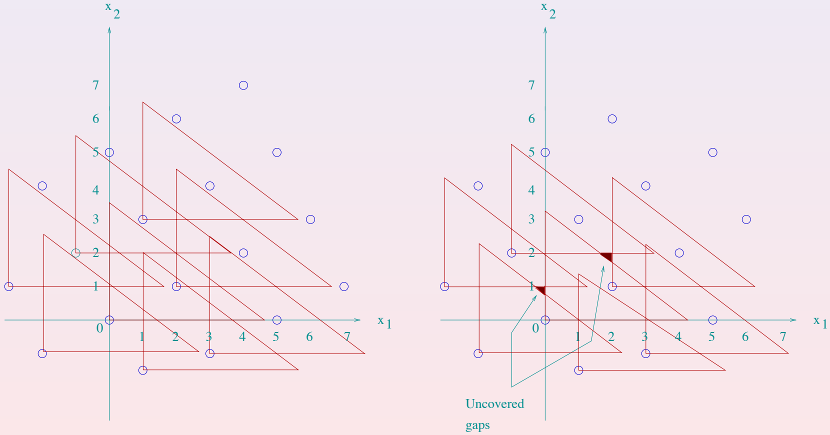
Example 1: Let $a_1 = 3, a_2 = 4$ and $a_3 = 5$.



Example 1 cont ... then, $g(3,4,5) = 2$ and thus $\mu(L,S) = 14$

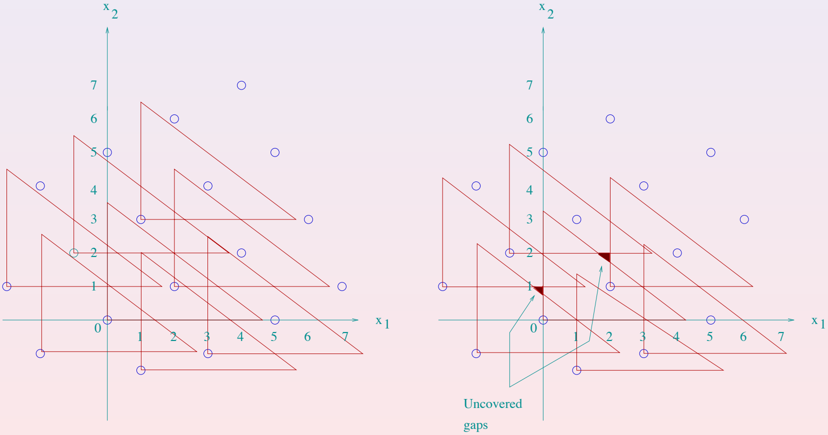
Notice that $(14)S$ covers the plane while $(13)S$ does not.

## Example 1 cont ... then, $g(3,4,5) = 2$ and thus $\mu(L, S) = 14$




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

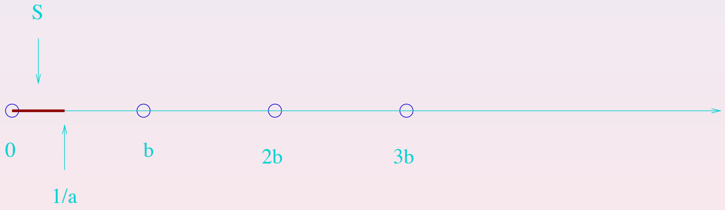
## Example 1 cont ... then, $g(3,4,5) = 2$ and thus $\mu(L, S) = 14$




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

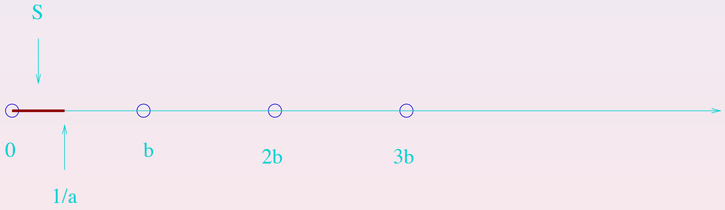
Example 2: Let $a_1, a_2$ be positive integers with $\gcd(a_1, a_2) = 1$.
Minimum integer $t$ such that $tS$ covers the interval $[0, b]$ is $ab$.
Thus, $g(a, b) = \mu(S, L) - a - b = ab - a - b$.

Example 2: Let $a_1, a_2$ be positive integers with $\gcd(a_1, a_2) = 1$.




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

Example 2: Let $a_1, a_2$ be positive integers with $\gcd(a_1, a_2) = 1$.




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

## Hilbert series and Apéry set

Let $A[S] = K[z_1, \ldots, z_n]$ be the polynomial ring over $K$ (of characteristic 0) associated to the semigroup $S = \langle a_1, \ldots, a_n \rangle$. Then, de Hilbert series of $A[S]$ is

$$H(A[S], z) = \sum_{i \in S} z^s = \frac{Q(z)}{(1 - z^{a_1}) \cdots (1 - z^{a_n})}.$$

$$g(a_1, \ldots, a_n) = \text{degree of } H(A[S], z)$$

Theorem (Herzog 1970, Morales 1987) Formula for $H(A[S], z)$ when $S = \langle a, b, c \rangle$

## Hilbert series and Apéry set

Let $A[S] = K[z_1, \ldots, z_n]$ be the polynomial ring over $K$ (of characteristic 0) associated to the semigroup $S = \langle a_1, \ldots, a_n \rangle$. Then, de Hilbert series of $A[S]$ is

$$H(A[S], z) = \sum_{i \in S} z^s = \frac{Q(z)}{(1 - z^{a_1}) \cdots (1 - z^{a_n})}.$$

$$g(a_1, \ldots, a_n) = \text{degree of } H(A[S], z)$$

Theorem (Herzog 1970, Morales 1987) Formula for $H(A[S], z)$ when $S = \langle a, b, c \rangle$

## Hilbert series and Apéry set

Let $A[S] = K[z_1, \ldots, z_n]$ be the polynomial ring over $K$ (of characteristic 0) associated to the semigroup $S = \langle a_1, \ldots, a_n \rangle$. Then, de Hilbert series of $A[S]$ is

$$H(A[S], z) = \sum_{i \in S} z^s = \frac{Q(z)}{(1 - z^{a_1}) \cdots (1 - z^{a_n})}.$$

$$g(a_1, \ldots, a_n) = \text{degree of } H(A[S], z)$$

Theorem (Herzog 1970, Morales 1987) Formula for $H(A[S], z)$ when $S = \langle a, b, c \rangle$

The *Apéry* set of $S = \langle a_1, \ldots, a_n \rangle$ for $m \in S$ is

$$Ap(S;m) = \{s \in S \mid s - m \notin S\}$$

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

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

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

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

Remark: Contains the case $n = 3$ when $k = 1$ and $b = a + d$.

The *Apéry* set of $S = \langle a_1, \ldots, a_n \rangle$ for $m \in S$ is

$$Ap(S; m) = \{s \in S \mid s - m \notin S\}$$

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

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

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

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

Remark: Contains the case $n = 3$ when $k = 1$ and $b = a + d$.

The *Apéry* set of $S = \langle a_1, \ldots, a_n \rangle$ for $m \in S$ is

$$Ap(S;m) = \{s \in S \mid s - m \notin S\}$$

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

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

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

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

Remark: Contains the case $n = 3$ when $k = 1$ and $b = a + d$.

The *Apéry* set of $S = \langle a_1, \ldots, a_n \rangle$ for $m \in S$ is

$$Ap(S;m) = \{s \in S \mid s - m \notin S\}$$

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

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

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

where $s_v, s_{v+1}, P_v, P_{v+1}$ are some *particular* integers.
Remark: Contains the case $n = 3$ when $k = 1$ and $b = a + d$.

Input: $a, d, c, k, s_0$ Output: $s_v, s_{v+1}, P_v, P_{v+1}$

1. $r_{-1} = a, r_0 = s_0$
2. $r_{i-1} = \kappa_{i+1} r_i + r_{i+1}, \quad \kappa_{i+1} = \lfloor r_{i-1}/r_i \rfloor, \quad 0 = r_{\mu+1} < r_\mu < \cdots < r_{-1}$
3. $p_{i+1} = \kappa_{i+1} p_i + p_{i-1}, \quad p_{-1} = 0, \quad p_0 = 1$
4. $T_{i+1} = -\kappa_{i+1} T_i + T_{i-1}, \quad T_{-1} = a + kd, \quad T_0 = \frac{1}{a}((a+kd)r_0 - kc)$
5. IF there is a minimal $u$ such that $T_{2u+2} \leq 0$, THEN
$$\begin{pmatrix} s_v & P_v \\ s_{v+1} & P_{v+1} \end{pmatrix} = \begin{pmatrix} \gamma & 1 \\ \gamma - 1 & 1 \end{pmatrix} \begin{pmatrix} r_{2u+1} & -p_{2u+1} \\ r_{2u+2} & p_{2u+2} \end{pmatrix}, \gamma = \left\lfloor \frac{-T_{2u+2}}{T_{2u+1}} \right\rfloor + 1$$
6. ELSE $s_v = r_\mu, s_{v+1} = 0, P_v = p_\mu, P_{v+1} = p_{\mu+1}$.

## Fast Algorithms (computational algebraic methods)

Einstein, Lichtblau, Strzebonski and Wagon
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
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

Package
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/FrobeniusNumbe

## Fast Algorithms (computational algebraic methods)

Einstein, Lichtblau, Strzebonski and Wagon

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

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

Package

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/FrobeniusNumbe

## Fast Algorithms (computational algebraic methods)

Einstein, Lichtblau, Strzebonski and Wagon

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

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

Package

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/FrobeniusNumbe

## Applications

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

## Applications

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 and 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.

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 and 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.

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 and 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.

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

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

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

# 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.

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

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

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

# 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.

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

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

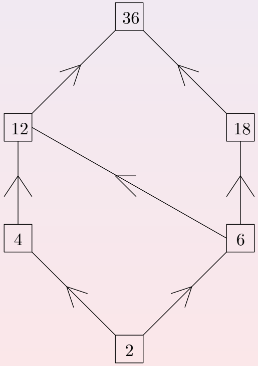
We denote by $c_l(a, b)$ the number of chains of length $l$ between $a$ and $b$.

The **Möbius function** $\mu_{\mathcal{P}}$ is the function

$$\mu_{\mathcal{P}} : \mathcal{P} \times \mathcal{P} \longrightarrow \mathbb{Z}$$
$$\mu_{\mathcal{P}}(a, b) = \sum_{l \geq 0} (-1)^l c_l(a, b).$$

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 $\left\{ \begin{array}{c} \{2,4,36\} \\ \{2,6,36\} \\ \{2,12,36\} \\ \{2,18,36\} \end{array} \right.$
- length 3 $\left\{ \begin{array}{c} \{2,4,12,36\} \\ \{2,6,12,26\} \\ \{2,6,18,36\} \end{array} \right.$




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

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

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

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

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

# Möbius classical arithmetic function

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 $\zeta$, $s \in \mathbb{C}, Re(s) > 0$

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

# Möbius classical arithmetic function

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 $\zeta$, $s \in \mathbb{C}, Re(s) > 0$

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

# Möbius classical arithmetic function

There are impressive results using $\mu$, 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 $36/2 = 18 = 2 \cdot 3^2$

# Möbius classical arithmetic function

There are impressive results using $\mu$, 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 $36/2 = 18 = 2 \cdot 3^2$

# Möbius inversion formula

**Theorem**

*Let* $(\mathcal{P}, \leq)$ *be a poset, let* $p$ *be an element of* $\mathcal{P}$ *and consider* $f : \mathcal{P} \to \mathbb{R}$ *a function such that* $f(x) = 0$ *for all* $x \not\geq p$*. Suppose that*

$$g(x) = \sum_{y \leq x} f(y) \text{ for all } x \in \mathcal{P}.$$

*Then,*

$$f(x) = \sum_{y \leq x} g(y)\, \mu_{\mathcal{P}}(y, x) \text{ for all } x \in \mathcal{P}.$$

Compute the Euler function $\phi(n)$ (the number of integers smaller or equal to $n$ and coprime with $n$)

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$$

Let $D$ be a finite set and consider the **poset** $(\mathcal{P}, \subset)$ **of multisets over** $D$ **ordered by inclusion**. Then, for all $A, B$ multisets over $D$ we have that

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

Compute the Euler function $\phi(n)$ (the number of integers smaller or equal to $n$ and coprime with $n$)

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$$

Let $D$ be a finite set and consider the **poset** $(\mathcal{P}, \subset)$ **of multisets over** $D$ **ordered by inclusion**. Then, for all $A, B$ multisets over $D$ we have that

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

# 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.,

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

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 $(\mathbb{N}^m, \leq_{\mathcal{S}})$.

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

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

## 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.,

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

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

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

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

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

# 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.,

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

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 $(\mathbb{N}^m, \leq_{\mathcal{S}})$.

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 $\mu_{\mathcal{S}}$

1. *Deddens* (1979).

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

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

2. *Chappelon and R.A.* (2013).
   - They 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.

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

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

1. *Deddens* (1979).

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

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

2. *Chappelon and R.A.* (2013).
   - They 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.

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

# Main objectives

1. Provide **general tools** to study $\mu_{\mathcal{S}}$ for every semigroup $\mathcal{S} \subset \mathbb{N}^m$.

2. Provide **explicit formulas** for certain families of semigroups $\mathcal{S} \subset \mathbb{N}^m$.

# Main objectives

1. Provide **general tools** to study $\mu_{\mathcal{S}}$ for every semigroup $\mathcal{S} \subset \mathbb{N}^m$.

2. Provide **explicit formulas** for certain families of semigroups $\mathcal{S} \subset \mathbb{N}^m$.

## $\mathcal{S}$-graded Hilbert series

Let $k$ be a field. A semigroup $\mathcal{S} = \langle a_1, \ldots, a_n \rangle \subset \mathbb{N}^m$ induces a **grading** in the **ring of polynomials** $k[x_1, \ldots, x_n]$ by assigning $\deg_{\mathcal{S}}(x_i) := a_i$ for all $i \in \{1, \ldots, n\}$.

For all $b \in \mathbb{N}^m$, we denote by $k[x_1, \ldots, x_n]_b$ the $k$-vector space formed by all polynomials $\mathcal{S}$-homogeneous of $\mathcal{S}$-degree $b$.

Consider $I \subset k[\mathbf{x}]$ an ideal generated by $\mathcal{S}$-homogeneous polynomials. For all $b \in \mathbb{N}^m$ we denote by $I_b$ the $k$-vector space formed by the $\mathcal{S}$-homogeneous polynomials of $I$ of $\mathcal{S}$-degree $b$.

# $\mathcal{S}$-graded Hilbert series

Let $k$ be a field. A semigroup $\mathcal{S} = \langle a_1, \dots, a_n \rangle \subset \mathbb{N}^m$ induces a **grading** in the **ring of polynomials** $k[x_1, \dots, x_n]$ by assigning $\deg_{\mathcal{S}}(x_i) := a_i$ for all $i \in \{1, \dots, n\}$.

For all $b \in \mathbb{N}^m$, we denote by $k[x_1, \dots, x_n]_b$ the $k$-vector space formed by all polynomials $\mathcal{S}$-homogeneous of $\mathcal{S}$-degree $b$.

Consider $I \subset k[\mathbf{x}]$ an ideal generated by $\mathcal{S}$-homogeneous polynomials. For all $b \in \mathbb{N}^m$ we denote by $I_b$ the $k$-vector space formed by the $\mathcal{S}$-homogeneous polynomials of $I$ of $\mathcal{S}$-degree $b$.

# $\mathcal{S}$-graded Hilbert series

Let $k$ be a field. A semigroup $\mathcal{S} = \langle a_1, \ldots, a_n \rangle \subset \mathbb{N}^m$ induces a **grading** in the **ring of polynomials** $k[x_1, \ldots, x_n]$ by assigning $\deg_{\mathcal{S}}(x_i) := a_i$ for all $i \in \{1, \ldots, n\}$.

For all $b \in \mathbb{N}^m$, we denote by $k[x_1, \ldots, x_n]_b$ the $k$-vector space formed by all polynomials $\mathcal{S}$-homogeneous of $\mathcal{S}$-degree $b$.

Consider $I \subset k[\mathbf{x}]$ an ideal generated by $\mathcal{S}$-homogeneous polynomials. For all $b \in \mathbb{N}^m$ we denote by $I_b$ the $k$-vector space formed by the $\mathcal{S}$-homogeneous polynomials of $I$ of $\mathcal{S}$-degree $b$.

The $\mathcal{S}$-**graded Hilbert function** of $M := k[x_1, \ldots, x_n]/I$ is

$$HF_M : \mathbb{N}^m \longrightarrow \mathbb{N},$$

where $HF_M(b) := \dim_k(k[x_1, \ldots, x_n]_b) - \dim_k(I_b)$ for all $b \in \mathbb{N}^m$.

We define the $\mathcal{S}$-**graded Hilbert series** of $M$ as the formal power series in $\mathbb{Z}[[t_1, \ldots, t_m]]$:

$$\mathcal{H}_M(\mathbf{t}) := \sum_{b \in \mathbb{N}^m} HF_M(b)\ \mathbf{t}^b$$

The $\mathcal{S}$-**graded Hilbert function** of $M := k[x_1, \ldots, x_n]/I$ is

$$HF_M : \mathbb{N}^m \longrightarrow \mathbb{N},$$

where $HF_M(b) := \dim_k(k[x_1, \ldots, x_n]_b) - \dim_k(I_b)$ for all $b \in \mathbb{N}^m$.

We define the $\mathcal{S}$-**graded Hilbert series** of $M$ as the formal power series in $\mathbb{Z}[[t_1, \ldots, t_m]]$:

$$\mathcal{H}_M(\mathbf{t}) := \sum_{b \in \mathbb{N}^m} HF_M(b)\ \mathbf{t}^b$$

We denote by $I_{\mathcal{S}}$ the **toric ideal** of $\mathcal{S}$, i.e., the kernel of the homomorphism of $k$-algebras

$$\varphi : k[x_1, \ldots, x_n] \longrightarrow k[t_1, \ldots, t_m]$$

induced by $\varphi(x_i) = \mathbf{t}^{a_i}$ for all $i \in \{1, \ldots, n\}$.

It is well known that $I_{\mathcal{S}}$ is generated by $\mathcal{S}$-homogeneous polynomials.

**Proposition:**

$$\mathcal{H}_{k[x_1,\ldots,x_n]/I_{\mathcal{S}}}(\mathbf{t}) = \mathcal{H}_{\mathcal{S}}(\mathbf{t})$$

We denote by $I_{\mathcal{S}}$ the **toric ideal** of $\mathcal{S}$, i.e., the kernel of the homomorphism of $k$-algebras

$$\varphi : k[x_1, \ldots, x_n] \longrightarrow k[t_1, \ldots, t_m]$$

induced by $\varphi(x_i) = \mathbf{t}^{a_i}$ for all $i \in \{1, \ldots, n\}$.

It is well known that $I_{\mathcal{S}}$ is generated by $\mathcal{S}$-homogeneous polynomials.

**Proposition:**

$$\mathcal{H}_{k[x_1,\ldots,x_n]/I_{\mathcal{S}}}(\mathbf{t}) = \mathcal{H}_{\mathcal{S}}(\mathbf{t})$$

## Hilbert series of a semigroup

For every $b = (b_1, \ldots, b_m) \in \mathbb{N}^m$, we denote $\mathbf{t}^b := t_1^{b_1} \cdots t_m^{b_m}$.

Let $\mathcal{S} \subset \mathbb{N}^m$ be a semigroup, the **Hilbert series of** $\mathcal{S}$ is

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

**Examples: (1)** For $\mathcal{S} = \langle 2, 3 \rangle \subset \mathbb{N}$, we have that $\mathcal{S} = \{0, 2, 3, 4, 5 \ldots\}$

$$\begin{array}{rccccccccccc} \mathcal{H}_{\mathcal{S}}(t) = & 1 & + & t^2 & + & t^3 & + & t^4 & + & t^5 & + \cdots \\ t^2\,\mathcal{H}_{\mathcal{S}}(t) = & & & t^2 & + & & & t^4 & + & t^5 & + \cdots \end{array}$$

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

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

## Hilbert series of a semigroup

For every $b = (b_1, \ldots, b_m) \in \mathbb{N}^m$, we denote $\mathbf{t}^b := t_1^{b_1} \cdots t_m^{b_m}$.

Let $\mathcal{S} \subset \mathbb{N}^m$ be a semigroup, the **Hilbert series of** $\mathcal{S}$ is

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

**Examples: (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

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

# Hilbert series of a semigroup

For every $b = (b_1, \ldots, b_m) \in \mathbb{N}^m$, we denote $\mathbf{t}^b := t_1^{b_1} \cdots t_m^{b_m}$.

Let $\mathcal{S} \subset \mathbb{N}^m$ be a semigroup, the **Hilbert series of** $\mathcal{S}$ is

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

**Examples: (1)** For $\mathcal{S} = \langle 2, 3 \rangle \subset \mathbb{N}$, we have that $\mathcal{S} = \{0, 2, 3, 4, 5 \ldots\}$

$$\begin{array}{rccccccccccc} \mathcal{H}_{\mathcal{S}}(t) = & 1 & + & t^2 & + & t^3 & + & t^4 & + & t^5 & + \cdots \\ t^2\,\mathcal{H}_{\mathcal{S}}(t) = & & & t^2 & + & & & t^4 & + & t^5 & + \cdots \end{array}$$

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

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

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

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

# 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 $c_1, \ldots, c_k \in \mathbb{N}^m$.

**Theorem (1)**

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

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

# 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)**

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

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

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

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

It is evident that $\mu_{\mathcal{S}}(0) = 1$. A direct computation yields $\mu_{\mathcal{S}}(2) = -1$.

Hence

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

# 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 $x \notin \{0, 2\}$.

It is evident that $\mu_{\mathcal{S}}(0) = 1$. A direct computation yields $\mu_{\mathcal{S}}(2) = -1$.

Hence

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

## Möbius function via Hilbert series

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)**

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

# 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,

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

## 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,

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

### Definition

We say that a semigroup $\mathcal{S} = \langle a_1, \ldots, a_n \rangle \subset \mathbb{N}^m$ is a **complete intersection semigroup** if its corresponding toric ideal $I_{\mathcal{S}}$ is a complete intersection.

Moreover, $I_{\mathcal{S}}$ is a **complete intersection** if there exists a system of $s = n - \dim(\mathbb{Q}\{a_1, \ldots, a_n\})$ $\mathcal{S}$-homogeneous polynomials $f_1, \ldots, f_s$ such that

$$I_{\mathcal{S}} = (f_1, \ldots, f_s).$$

Whenever $I_{\mathcal{S}}$ is a complete intersection generated $\mathcal{S}$-homogeneous polynomials of $\mathcal{S}$-degrees $b_1, \ldots, b_s \in \mathbb{N}^m$, then

$$\mathcal{H}_{\mathcal{S}}(\mathbf{t}) = \frac{(1 - \mathbf{t}^{b_1}) \cdots (1 - \mathbf{t}^{b_s})}{(1 - \mathbf{t}^{a_1}) \cdots (1 - \mathbf{t}^{a_n})}$$

## Definition

We say that a semigroup $\mathcal{S} = \langle a_1, \ldots, a_n \rangle \subset \mathbb{N}^m$ is a **complete intersection semigroup** if its corresponding toric ideal $I_{\mathcal{S}}$ is a complete intersection.

Moreover, $I_{\mathcal{S}}$ is a **complete intersection** if there exists a system of $s = n - \dim(\mathbb{Q}\{a_1, \ldots, a_n\})$ $\mathcal{S}$-homogeneous polynomials $f_1, \ldots, f_s$ such that

$$I_{\mathcal{S}} = (f_1, \ldots, f_s).$$

Whenever $I_{\mathcal{S}}$ is a complete intersection generated $\mathcal{S}$-homogeneous polynomials of $\mathcal{S}$-degrees $b_1, \ldots, b_s \in \mathbb{N}^m$, then

$$\mathcal{H}_{\mathcal{S}}(\mathbf{t}) = \frac{(1 - \mathbf{t}^{b_1}) \cdots (1 - \mathbf{t}^{b_s})}{(1 - \mathbf{t}^{a_1}) \cdots (1 - \mathbf{t}^{a_n})}$$

# 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 $b$.

**Theorem**

*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 $k_1, \ldots, k_t \in \mathbb{N}$.*

# 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 $b$.

## Theorem

*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* $k_1, \ldots, k_t \in \mathbb{N}$.

When $\mathcal{S} = \langle a_1, \ldots, a_n \rangle \subset \mathbb{N}$ is a **semigroup with a unique Betti element** and $\gcd\{a_1, \ldots, a_n\} = 1$, It is known that there exist pairwise relatively prime different integers $b_1, \ldots, b_n \geq 2$ such that $a_i := \prod_{j \neq i} b_j$ for all $i \in \{1, \ldots, n\}$.

In this setting we can refine the previous Theorem.

**Corollary**

*Set $b := \prod_{i=1}^{n} b_i$, then*

$$\mu_{\mathcal{S}}(x) = \begin{cases} (-1)^{|A|} \binom{k+n-2}{k} & \text{if } x = \sum_{i \in A} a_i + k\, b \\ & \text{for some } A \subset \{1, \ldots, n\}, k \in \mathbb{N} \\ 0 & \text{otherwise} \end{cases}$$

When $\mathcal{S} = \langle a_1, \ldots, a_n \rangle \subset \mathbb{N}$ is a **semigroup with a unique Betti element** and $\gcd\{a_1, \ldots, a_n\} = 1$, It is known that there exist pairwise relatively prime different integers $b_1, \ldots, b_n \geq 2$ such that $a_i := \prod_{j \neq i} b_j$ for all $i \in \{1, \ldots, n\}$.

In this setting we can refine the previous Theorem.

## Corollary

*Set* $b := \prod_{i=1}^{n} b_i$, *then*

$$\mu_{\mathcal{S}}(x) = \begin{cases} (-1)^{|A|} \binom{k+n-2}{k} & \text{if } x = \sum_{i \in A} a_i + k\, b \\ & \text{for some } A \subset \{1, \ldots, n\}, k \in \mathbb{N} \\ 0 & \text{otherwise} \end{cases}$$

# $\mathcal{S} = \langle a_1, a_2, a_3 \rangle \subset \mathbb{N}$ complete intersection

For every $x \in \mathbb{Z}$ we denote by $\alpha(x)$ the only integer such that $0 \leq \alpha(x) \leq d - 1$ and $\alpha(x)\, a_1 \equiv x \pmod{d}$.

For every $x \in \mathbb{Z}$ and every $B = (b_1, \ldots, b_k) \subset (\mathbb{Z}^+)^k$, the **Sylvester denumerant** $d_B(x)$ is the number of non-negative integer solutions $(x_1, \ldots, x_k) \in \mathbb{N}^k$ to the equation $x = \sum_{i=1}^k x_i b_i$.

For $\mathcal{S} = \langle a_1, a_2, a_3 \rangle$ complete intersection and $\gcd\{a_1, a_2, a_3\} = 1$, we have the following result.

**Theorem**

*$\mu_{\mathcal{S}}(x) = 0$ if $\alpha(x) \geq 2$, or*

$$\mu_{\mathcal{S}}(x) = (-1)^{\alpha} \left(d_B(x') - d_B(x' - a_2) - d_B(x' - a_3) + d_B(x' - a_2 - a_3)\right)$$

*otherwise, where $x' := x - \alpha(x)\, a_1$ and $B := (da_1, a_2\, a_3/d)$.*

## $\mathcal{S} = \langle a_1, a_2, a_3 \rangle \subset \mathbb{N}$ complete intersection

For every $x \in \mathbb{Z}$ we denote by $\alpha(x)$ the only integer such that $0 \leq \alpha(x) \leq d-1$ and $\alpha(x)\, a_1 \equiv x \pmod{d}$.

For every $x \in \mathbb{Z}$ and every $B = (b_1, \ldots, b_k) \subset (\mathbb{Z}^+)^k$, the **Sylvester denumerant** $d_B(x)$ is the number of non-negative integer solutions $(x_1, \ldots, x_k) \in \mathbb{N}^k$ to the equation $x = \sum_{i=1}^k x_i b_i$.

For $\mathcal{S} = \langle a_1, a_2, a_3 \rangle$ complete intersection and $\gcd\{a_1, a_2, a_3\} = 1$, we have the following result.

**Theorem**

$\mu_{\mathcal{S}}(x) = 0$ *if* $\alpha(x) \geq 2$, *or*

$\mu_{\mathcal{S}}(x) = (-1)^{\alpha} \left(d_B(x') - d_B(x' - a_2) - d_B(x' - a_3) + d_B(x' - a_2 - a_3)\right)$

*otherwise, where* $x' := x - \alpha(x)\, a_1$ *and* $B := (da_1, a_2\, a_3/d)$.

# $\mathcal{S} = \langle a_1, a_2, a_3 \rangle \subset \mathbb{N}$ complete intersection

For every $x \in \mathbb{Z}$ we denote by $\alpha(x)$ the only integer such that $0 \leq \alpha(x) \leq d - 1$ and $\alpha(x)\, a_1 \equiv x \pmod{d}$.

For every $x \in \mathbb{Z}$ and every $B = (b_1, \ldots, b_k) \subset (\mathbb{Z}^+)^k$, the **Sylvester denumerant** $d_B(x)$ is the number of non-negative integer solutions $(x_1, \ldots, x_k) \in \mathbb{N}^k$ to the equation $x = \sum_{i=1}^k x_i b_i$.

For $\mathcal{S} = \langle a_1, a_2, a_3 \rangle$ complete intersection and $\gcd\{a_1, a_2, a_3\} = 1$, we have the following result.

**Theorem**

$\mu_{\mathcal{S}}(x) = 0$ *if* $\alpha(x) \geq 2$, *or*

$$\mu_{\mathcal{S}}(x) = (-1)^{\alpha} \left( d_B(x') - d_B(x' - a_2) - d_B(x' - a_3) + d_B(x' - a_2 - a_3) \right)$$

*otherwise, where* $x' := x - \alpha(x)\, a_1$ *and* $B := (da_1, a_2\, a_3/d)$.

# Examples of semigroup posets

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 $A$.

$\psi$ is an **poset isomorphism** (an order preserving and order reflecting bijection). Hence,

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

and we can recover the formula for $\mu_{\mathcal{P}}$ by means of $\mu_{\mathbb{N}^m}$.

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

# Examples of semigroup posets

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

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

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

$\psi$ is an **poset isomorphism** (an order preserving and order reflecting bijection). Hence,

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

and we can recover the formula for $\mu_{\mathcal{P}}$ by means of $\mu_{\mathbb{N}^m}$.

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

# Examples of semigroup posets

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 $A$.

$\psi$ is an **poset isomorphism** (an order preserving and order reflecting bijection). Hence,

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

and we can recover the formula for $\mu_{\mathcal{P}}$ by means of $\mu_{\mathbb{N}^m}$.

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

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

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

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 $\mu_{\mathbb{N}^m}$.

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

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**

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

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 $\mu_{\mathbb{N}^m}$.

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

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

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

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**

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

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 $\mu_{\mathbb{N}^m}$.

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