From jugs of wine to the Möbius function of semigroup posets

J.L. Ramírez Alfonsín

IMAG, Université de Montpellier

Probabilistic Combinatorics:
A celebration of the work of Colin McDiarmid

Oxford, April 10th, 2016


PLEASE DO
NOT BRING
FOOD OR
DRINK
INTO THE
AUDITORIUM

Jugs of wine problem

There are three jugs with integral capacities, B, M and S respectively with $B = M + S$ and $M \geq S \geq 1$. Any jug may be poured into any other jug until either the first one is empty or the second is full. Initially jug B is full and the other two are empty.

We want to divide the wine equally, so that $\frac{1}{2}B$ gallons are in jugs B and M and jug S is empty, and we want to do so with a few pourings as possible

Jugs of wine problem

There are three jugs with integral capacities, B, M and S respectively with $B = M + S$ and $M \geq S \geq 1$. Any jug may be poured into any other jug until either the first one is empty or the second is full. Initially jug B is full and the other two are empty.

We want to divide the wine equally, so that $\frac{1}{2}B$ gallons are in jugs B and M and jug S is empty, and we want to do so with a few pourings as possible

The origine of this puzzle can be traced back at least as far as Tartaglia (16th century)

Jugs of wine problem

Theorem (McDiarmid, R.A., 1994) It is possible to share equally if and only if B is divisible by $2r$ where $r = \gcd(M, S)$. If this is the case the least number of pourings is $\frac{1}{r}B - 1$.

Jugs of wine problem

Theorem (McDiarmid, R.A., 1994) It is possible to share equally if and only if B is divisible by $2r$ where $r = \gcd(M, S)$. If this is the case the least number of pourings is $\frac{1}{r}B - 1$.

Moreover, we proposed an algorithm to achieve the unique optimal sequence of pourings.

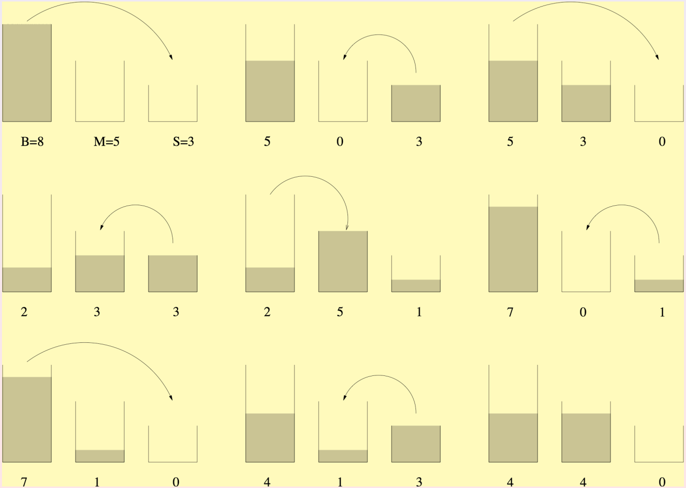
Jugs of wine problem

Theorem (McDiarmid, R.A., 1994) It is possible to share equally if and only if B is divisible by $2r$ where $r = \gcd(M, S)$. If this is the case the least number of pourings is $\frac{1}{r}B - 1$.

Moreover, we proposed an algorithm to achieve the unique optimal sequence of pourings.

Example : $B = 8$, $M = 5$ and $S = 3$

Jugs of wine problem



Colin's wise words

"Once you have
a result try to
take advantage
of it as much as
you can "

Stamp problem (Ian Stewart)

How hard can it be?

Deliver the solution to an everyday puzzle and you could win the biggest prize in mathematics, says **Ian Stewart**

EVER since a Babylonian scribe decided to teach his students arithmetic by setting them problems using the formula "I found a stone but did not weigh it..." mathematicians have celebrated the hidden depths of apparently everyday problems. They have found inspiration in slicing pies, tying knots and spinning coins. But even mathematicians have been surprised by the depth of the mystery that lurks behind an innocent question about postage stamps.

Suppose that your post office sells stamps with just two values: 2 cents and 5 cents. By combining these values, you can make up almost any whole number of cents. For example, to post a letter costing 9¢, you could stick one 5¢ stamp and two 2¢ stamps on the envelope. Two values that you cannot achieve are 1¢ and 3¢ – and in fact these are the only impossible amounts. You can produce any even amount using 2¢ stamps – given a big enough envelope – and any odd value from 5¢ upwards, using one 5¢ stamp and multiple 2¢ stamps.

This example is typical. Given an unlimited supply of stamps, there is always some key value above which any total can be achieved by sticking the right combination of stamps on the envelope. This is also true if you have more than two denominations of stamp available.

But the million-dollar question is this: with *n* denominations of stamps available, what is that key value? The first person to consider a simple version of this question was James Joseph Sylvester in 1883 (to be precise, he was when dealing with just two denominations (see "Pushing the envelope", page 48).

In its general form, the postage-stamp problem really could be a million-dollar question: the Clay Mathematics Institute in Cambridge, Massachusetts, is offering exactly that amount to anyone who can solve a problem that is logically equivalent to it. We now have tantalising new hints that the postage-stamp problem – and therefore, perhaps, the related million-dollar enigma – might not be as daunting as it appears. So considering how to pay for posting our mail might lead to a breakthrough in one of the most significant mathematical problems of the 21st century.

It will never compute

The issue centres around the cost of solving a problem – not in dollars and cents, but in computational effort. We measure the difficulty of a calculation by the number of basic computational steps needed to complete it: for a particular size of problem – often measured in terms of the number of digits in the number to be crunched – what is the "running time" of the algorithm concerned? If the problem concerns 50-digit numbers rather than 25-digit numbers, say, how much longer does the algorithm take to get the answer? What about 100-digit numbers, or any number of digits? It should be noted that this running time is an abstract notion, related but not equivalent to the actual time

to look at it that way – if the running time grows in step with some fixed power of the number of digits required to pose the question. For example, an algorithm for testing a number *n* to see whether it is prime may have a running time linked to the sixth power of the number of digits of *n*.

Such algorithms are said to be "class P", where the "P" stands for "polynomial". Algorithms that run in polynomial time are relatively stable: they do not get wildly slower with small increases in the size of the input. In contrast, non-P algorithms are generally impractical – "inefficient"or "hard" – and become unmanageable with relatively small increases in input size. It's not quite that straightforward, because some non-P algorithms are pretty efficient until the input size gets very big indeed, while some P algorithms depend on a parameter which is so large that they couldn't actually run within a human lifetime. Nevertheless, the distinction between P and non-P seems to be the most basic and important distinction in problems about the efficiency of algorithms – a way to formalise the intuitive ideas of "easy to compute" versus "hard to compute".

Are there any such things as truly hard problems? Yes, several kinds. The obvious ones are hard for a simple reason, such as printing out the answer takes too long. A good example is "print all ways to rearrange this list of symbols". With the 52 symbols in a pack of cards, the list would contain 80,658,175,170, 943,878,571,660,636,856,403,766,975,289,505, 440,883,277,824,000,000,000,000 arrangements, and you'd have to print the lot. These types of problem have to be excluded, which we do by introducing another class of algorithm, confusingly called NP, which run in "nondeterministic polynomial" time. A problem is NP if any proposed solution can be checked to determine whether it is right or wrong, in polynomial time – that is, in reasonable time. A rough analogy is solving a jigsaw puzzle. However long it takes to work out how to fit the pieces together – the nondeterministic aspect – a brief glance at the result usually reveals whether it is correct.

All this classification has led to a rather fundamental question, and whoever cracks it

Stamp problem

Given n stamps of values $a_1, \ldots, a_n$, what is the largest integer from which any amount can be achieved by sticking the right combination of stamps on an (big enough) envelope ?

Stamp problem

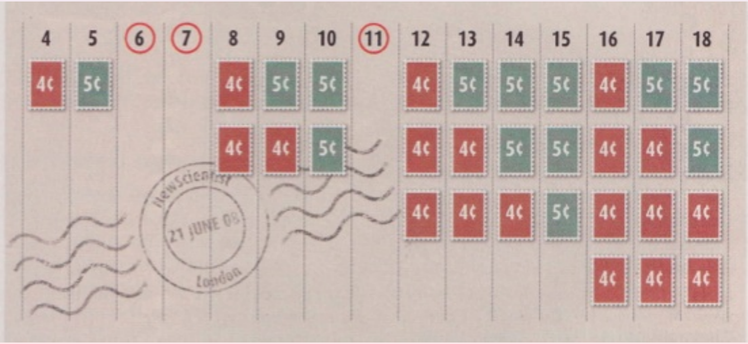
Given n stamps of values $a_1, \ldots, a_n$, what is the largest integer from which any amount can be achieved by sticking the right combination of stamps on an (big enough) envelope ?

Example : Two stamps of 4¢ and 5¢

Stamp problem

Given n stamps of values $a_1, \ldots, a_n$, what is the largest integer from which any amount can be achieved by sticking the right combination of stamps on an (big enough) envelope ?

Example : Two stamps of 4¢ and 5¢



The Diophantine Frobenius problem

Let $a_1, \ldots, a_n$ positive integers. We say that an integer s is representable by $a_1, \ldots, a_n$ if there exist integers $x_i \geq 0$ such that

$$s = \sum_{i=1}^{n} x_i a_i.$$

The Diophantine Frobenius problem

Let $a_1, \ldots, a_n$ positive integers. We say that an integer s is representable by $a_1, \ldots, a_n$ if there exist integers $x_i \geq 0$ such that

$$s = \sum_{i=1}^{n} x_i a_i.$$

Let us suppose that $\gcd(a_1, \ldots, a_n) = 1$.

The Diophantine Frobenius problem

Let $a_1, \ldots, a_n$ positive integers. We say that an integer s is representable by $a_1, \ldots, a_n$ if there exist integers $x_i \geq 0$ such that

$$s = \sum_{i=1}^{n} x_i a_i.$$

Let us suppose that $\gcd(a_1, \ldots, a_n) = 1$. The so-called diophantine Frobenius problem ask to find the largest integer **no** representable by $a_1, \ldots, a_n$ (such a number is denoted by $g(a_1, \ldots, a_n)$ and is called Frobenius number).

The Diophantine Frobenius problem

Let $a_1, \ldots, a_n$ positive integers. We say that an integer s is representable by $a_1, \ldots, a_n$ if there exist integers $x_i \geq 0$ such that

$$s = \sum_{i=1}^{n} x_i a_i.$$

Let us suppose that $\gcd(a_1, \ldots, a_n) = 1$. The so-called diophantine Frobenius problem ask to find the largest integer **no** representable by $a_1, \ldots, a_n$ (such a number is denoted by $g(a_1, \ldots, a_n)$ and is called Frobenius number).

Example : $a_1 = 3$, $a_2 = 8$

The Diophantine Frobenius problem

Let $a_1, \ldots, a_n$ positive integers. We say that an integer s is representable by $a_1, \ldots, a_n$ if there exist integers $x_i \geq 0$ such that

$$s = \sum_{i=1}^{n} x_i a_i.$$

Let us suppose that $\gcd(a_1, \ldots, a_n) = 1$. The so-called diophantine Frobenius problem ask to find the largest integer **no** representable by $a_1, \ldots, a_n$ (such a number is denoted by $g(a_1, \ldots, a_n)$ and is called Frobenius number).

Example : $a_1 = 3$, $a_2 = 8$
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 $\cdots$

The Diophantine Frobenius problem

Let $a_1, \ldots, a_n$ positive integers. We say that an integer s is representable by $a_1, \ldots, a_n$ if there exist integers $x_i \geq 0$ such that

$$s = \sum_{i=1}^{n} x_i a_i.$$

Let us suppose that $\gcd(a_1, \ldots, a_n) = 1$. The so-called diophantine Frobenius problem ask to find the largest integer **no** representable by $a_1, \ldots, a_n$ (such a number is denoted by $g(a_1, \ldots, a_n)$ and is called Frobenius number).

Example : $a_1 = 3$, $a_2 = 8$

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 $\cdots$ Then $g(3, 8) = 13$.

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

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

Theorem (Sylvester, 1883)
$g(a_1, a_2) = a_1 a_2 - a_1 - a_2$

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

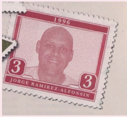
Theorem (Sylvester, 1883)
$g(a_1, a_2) = a_1 a_2 - a_1 - a_2$

Theorem (Kannan, 1992) There exists a polinomial time algorithm that determine $g(a_1, \ldots, a_n)$ when $n \geq 2$ is fixed

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

Theorem (Sylvester, 1883)
$g(a_1, a_2) = a_1 a_2 - a_1 - a_2$

Theorem (Kannan, 1992) There exists a polinomial time algorithm that determine $g(a_1, \ldots, a_n)$ when $n \geq 2$ is <u>fixed</u>



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

Others...

- Frobenius number of Fibonacci semigroups
- Gaps in semigroups
- Numerical semigroups : Apéry set and Hilbert series
- A tiling problem and the Frobenius number
- Two-generator semigroups and Fermat and Marsenne numbers
- On the number of numerical semigroups of prime power genus
- Möbius function of poset associated to semigroup

Basic 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.

Basic 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.

Basic 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

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

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

Basic Posets

Consider the poset $(\mathbb{N}, |)$ of nonnegative integers ordered by divisibility, i.e., $a \mid b \iff a$ divides b. Let us compute $\mu_{\mathbb{N}}(2, 36)$.

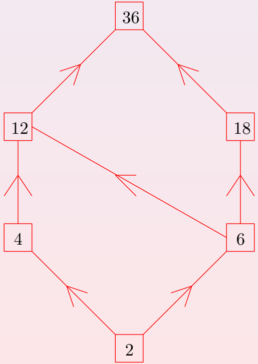
Basic Posets

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 $\{c \in \mathbb{N};\ 2 \mid c \mid 36\} = \{2, 4, 6, 12, 18, 36\}$.

Basic Posets

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 $\begin{cases} \{2,4,12,36\} \\ \{2,6,12,26\} \\ \{2,6,18,36\} \end{cases}$



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

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

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 $\mathcal{S} := \langle a_1, \ldots, a_n \rangle \subset \mathbb{N}^m$ 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 $(\mathbb{N}^m, \leq_{\mathcal{S}})$.

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

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

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 and R.A., 2013)

- **recursive formula** for $\mu_{\mathcal{S}}$ when $\mathcal{S} = \langle a, a+d, \ldots, a+kd \rangle \subset \mathbb{N}$ for some $a, k, d \in \mathbb{Z}^+$.
- **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 and R.A., 2013)

- **recursive formula** for $\mu_{\mathcal{S}}$ when $\mathcal{S} = \langle a, a+d, \ldots, a+kd \rangle \subset \mathbb{N}$ for some $a, k, d \in \mathbb{Z}^+$.
- **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.

Our approach was by a thorough study of the intrinsic properties of each semigroup.

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

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

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

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

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

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

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

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

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: Consider $\{e_1, \ldots, e_m\}$ the canonical basis of $\mathbb{N}^m$, i.e., $e_1 = (1, 0, \ldots, 0), \ldots, e_m = (0, \ldots, 0, 1) \in \mathbb{N}^m$.
For $\mathcal{S} = \mathbb{N}^m$, we have that

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

Möbius function via Hilbert series

Assume that

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

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

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

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

Theorem 1 (Chappelon, Garcia, Montejano, 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: $\mathcal{S} = \langle 2, 3 \rangle$

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

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 clearly have that $\mu_{\mathcal{S}}(0) = 1$ and adirect 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

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

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 (Chappelon, Garcia, Montejano, R.A., 2015)

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

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

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

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,

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

Unique Betti element

When $\mathcal{S} = \langle a_1, \ldots, a_n \rangle \subset \mathbb{N}$ is a semigroup with a unique Betti element 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 $i \in \{1, \ldots, n\}$.

Unique Betti element

When $\mathcal{S} = \langle a_1, \ldots, a_n \rangle \subset \mathbb{N}$ is a semigroup with a unique Betti element 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 $i \in \{1, \ldots, n\}$.

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

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

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 $\alpha(x)\, a_1 \equiv x \pmod{d}$.

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 $x = \sum_{i=1}^{k} x_i b_i$.

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 $x = \sum_{i=1}^{k} x_i b_i$.

$\mathcal{S} = \langle a_1, a_2, a_3 \rangle$ is complete intersection if $\gcd(a_i, a_j) a_k \in \langle a_i, a_j \rangle$.

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 $x = \sum_{i=1}^k x_i b_i$.

$\mathcal{S} = \langle a_1, a_2, a_3 \rangle$ is complete intersection if $\gcd(a_i, a_j) a_k \in \langle a_i, a_j \rangle$.

Theorem If $\mathcal{S} = \langle a_1, a_2, a_3 \rangle$ is complete intersection with $da_1 \in \langle a_2, a_3 \rangle$ then
$\mu_{\mathcal{S}}(x) = 0$ if $\alpha(x) \geq 2$, or
$\mu_{\mathcal{S}}(x) = (-1)^{\alpha} (d_B(x') - d_B(x' - a_2) - d_B(x' - a_3) + d_B(x' - a_2 - a_3))$
otherwise, where $x' := x - \alpha(x)\, a_1$ and $B := (da_1, a_2\, a_3/d)$.

Posets - isomorphism

Question Is a given poset $\mathcal{P}$ isomorphic to a poset associated to a semigroup $\mathcal{S}$?

Posets - isomorphism

Question Is a given poset $\mathcal{P}$ isomorphic to a poset associated to a semigroup $\mathcal{S}$?

Observation In such a case, one might be able to calculate $\mu_{\mathcal{P}}$ by computing $\mu_{\mathcal{S}}$ instead.

Posets - isomorphism

Question Is a given poset $\mathcal{P}$ isomorphic to a poset associated to a semigroup $\mathcal{S}$?

Observation In such a case, one might be able to calculate $\mu_{\mathcal{P}}$ by computing $\mu_{\mathcal{S}}$ instead.

Theorem (Chappelon, Garcia, Montejano, R.A., 2015) Let $\mathcal{P}$ be a locally finite poset and let $x \in \mathcal{P}$. Then $(\mathcal{P}_x, \leq)$ is isomorphic to $(\mathcal{S}, \leq_{\mathcal{S}})$ for some pointed semigroup $\mathcal{S} \subset \mathbb{Z}^m$ if and only if $\mathcal{P}_x$ is autoequivalelnt $l_I(x)$ is finite and $L_{\mathcal{P}} = Sat(L_{\mathcal{P}})$.

Example 1: poset of multisets

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.

Example 1: poset of multisets

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).

Example 1: poset of multisets

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,

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

Example 1: poset of multisets

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,

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

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

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

Example 2: divisibility poset

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 $(\mathbb{N}_m, |)$, i.e., $\mathbb{N}_m$ partially ordered by divisibility.

Example 2: divisibility poset

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 $(\mathbb{N}_m, |)$, i.e., $\mathbb{N}_m$ partially ordered by divisibility.
For the semigroup $\mathcal{S} = \mathbb{N}^m$, we consider the order isomorphism

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

Example 2: divisibility poset

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 $(\mathbb{N}_m, |)$, 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, $\mu_{\mathbb{N}_m}(a, b) = \mu_{\mathbb{N}^m}(\psi(a), \psi(b))$,

Example 2: divisibility poset

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

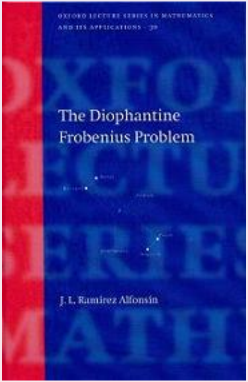
$$\mathbb{N}_m := \{p_1^{\alpha_1} \cdots p_m^{\alpha_m} \mid \alpha_1, \ldots, \alpha_m \in \mathbb{N}\} \subset \mathbb{N}.$$

Let us consider the $(\mathbb{N}_m, |)$, 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 $\mu_{\mathbb{N}^m}$.

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



Acknowledgements

I first started to work on **FP** while doing my D.Phil. supervised by Colin McDiarmid. At that time, Colin introduced me to knapsack-type problems that naturally lead me to consider **FP**. Colin has always encouraged and motivated me in different mathematical (and other) aspects that have certainly impacted in my academic career. In particular, Colin's enthusiasm gave me a first stimulus to write this manuscript. I wish to express my gratitude to Colin not only for his continuous support and generosity but also for a number of insightful mathematical discussions. I thank D. Welsh for many interesting conversations.

Thanks Colin