NOTES ON MÖBIUS INVERSION AND INCLUSION-EXCLUSION

MIKE ZABROCKI - NOVEMBER/DECEMBER 2017

This topic is covered in more detail (but perhaps more tersely) in [2, 3] and some of the ideas, definitions and presentation are taken from there. I also borrowed a number of ideas from [4].

In these notes what I plan to do is

- introduce Mobius inversion for integer sequences a_n and b_n related by $a_n = \sum_{d|n} b_d$
- Use this to give a formula for the Euler phi function
- Introduce posets
- Define Mobius inversion for posets
- Use that to introduce/prove inclusion-exclusion

We recently came across another example of a system of equations that is similar, but not the same. Consider

$$n = \sum_{d|n} \phi(d). \tag{1}$$

using the notation $d|n$ to represent the shorthand "d divides n" (that is, there exists an integer k such that $dk = n$). We gave a proof of this equation by looking at rotations of beads on a necklace and calculating the group of symmetries of rotations of those beads.

If $\sigma = (123\cdots n)$, then $\{\sigma^1, \sigma^2, \ldots, \sigma^n\}$ is the group of rotations on an n element set. We showed that the permutations σ^i such that $gcd(i, n) = d$ have exactly d cycles (each of length n/d). The number of permutations σ^i such that $gcd(i, n) = d$ is equal to $\phi(n/d)$. Since there are n permutations in the group, then $\sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d) = n$. (Note: This expression came up in context of applying Polya's theorem to count the number of necklaces and we concluded that the number of unique necklaces with n beads that have k different colors where you can rotate the necklace is equal to $\frac{1}{n}\sum_{d|n} \phi(n/d)k^d$.

One way to give a formula for the Euler phi function is to use the principle of inclusion-exclusion to show that

$$\phi(p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}) = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}(1-1/p_1)(1-1/p_2)\cdots(1-1/p_k) \ .$$

In these notes I am going to skip that proof (because in class I only did it directly for $\phi(p^aq^b) = p^aq^b - p^{a-1}q^b - p^aq^{b-1} + p^{a-1}q^{b-1}$ and I said that the more general case is similar). We will come up with a different type of formula for the Euler phi function using a "different" technique (actually it is the same, it is just in disguise it looks different).

I mentioned that we can use this system of equations (equation (1)) to solve for the values of $\phi(d)$.

$$
\begin{aligned}
1 &= \phi(1) & \phi(1) &= 1\\
2 &= \phi(1)+\phi(2) & \phi(2) &= 2-\phi(1) = 2-1 = 1\\
3 &= \phi(1)+\phi(3) & \phi(3) &= 3-\phi(1) = 3-1 = 2\\
4 &= \phi(1)+\phi(2)+\phi(4) & \phi(4) &= 2-\phi(2)-\phi(1) = 4-1-1 = 2\\
5 &= \phi(1)+\phi(5) & \phi(5) &= 5-\phi(1) = 5-1 = 4\\
6 &= \phi(1)+\phi(2)+\phi(3)+\phi(6) & \phi(6) &= 6-\phi(3)-\phi(2)-\phi(1) = 6-2-1-1 = 2\\
7 &= \phi(1)+\phi(7) & \phi(7) &= 7-\phi(1) = 7-1 = 6\\
8 &= \phi(1)+\phi(2)+\phi(4)+\phi(8) & \phi(8) &= 8-\phi(4)-\phi(2)-\phi(1) = 8-2-1-1 = 4\\
9 &= \phi(1)+\phi(3)+\phi(9) & \phi(9) &= 9-\phi(3)-\phi(1) = 9-2-1 = 6
\end{aligned}
$$

If we set up a system of equations of the form

$$a_n = \sum_{d|n} b_d, \tag{2}$$

then we can solve for b_n in terms of a_n.

$$
\begin{aligned}
a_1 &= b_1 & b_1 &= a_1\\
a_2 &= b_1+b_2 & b_2 &= a_2-b_1 = a_2-a_2\\
a_3 &= b_1+b_3 & b_3 &= a_3-b_1 = a_3-a_1\\
a_4 &= b_1+b_2+b_4 & b_4 &= a_4-b_2-b_1 = a_4-a_2\\
a_5 &= b_1+b_5 & b_5 &= a_5-b_1 = a_5-a_1\\
a_6 &= b_1+b_2+b_3+b_6 & b_6 &= a_6-b_3-b_2-b_1 = a_6-a_3-a_2+a_1\\
a_7 &= b_1+b_7 & b_7 &= a_7-b_1 = a_7-a_1\\
a_8 &= b_1+b_2+b_4+b_8 & b_8 &= a_8-b_4-b_2-b_1 = a_8-a_4\\
a_9 &= b_1+b_3+b_9 & b_9 &= a_9-b_3-b_1 = a_9-a_3
\end{aligned}
$$

The right hand side of the equation looks a bit hard to guess at (for instance, why is $b_9 = a_9 - a_3$ while $b_6 = a_6 - a_3 - a_2 + a_1$?), but there is an explicit formula for this expression. In this case

$$b_n = \sum_{d|n} \mu(d) a_{n/d} = \sum_{d|n} \mu(n/d) a_d \tag{3}$$

where

Definition 1.

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes} \\ 0 & \text{if there is a prime } p \text{ such that } p^2 \text{ divides } d \end{cases}.$$

In particular, since equation (1) has exactly the form (2) (with $a_n = n$ and $b_d = \phi(d)$), then equation (3) says that

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = \sum_{d|n} \mu(n/d) d\ . \tag{4}$$

Start with a lemma, namely:

Lemma 2. *For $n \geq 1$,*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

Proof. First we note that the sum over $d|n$ of $\mu(d)$ is really the sum over the square free divisors of n (because the ones that are not square free have $\mu(d) = 0$). Then assume that $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ where $k > 0$. Every divisor will be a product of some subset of the p_i. Therefore assuming $n > 1$ then $k > 0$ and

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{S \subseteq \{1,2,\ldots,k\}} \mu\left(\prod_{i \in S} p_i\right) = \sum_{r=0}^{k} \sum_{S \subseteq \{1,2,\ldots,k\} : |S| = r} \mu\left(\prod_{i \in S} p_i\right) \\ &= \sum_{r=0}^{k} (-1)^r \binom{k}{r} = (1-1)^k = 0 \ . \end{aligned}$$

□

From this property it follows that $a_n = \sum_{d|n} b_d$ implies equation (3).

Lemma 3. *If $a_n = \sum_{d|n} b_d$, then $b_n = \sum_{d|n} \mu(n/d) a_d$.*

Proof.

$$\sum_{d|n} \mu(n/d) a_d = \sum_{d|n} \sum_{c|d} b_c \mu(n/d) = \sum_{c|n} \sum_{c|d \text{ and } d|n} \mu(n/d) b_c = \sum_{c|n} \sum_{d'|(n/c)} \mu((n/c)/d') b_c$$

By Lemma 2, the inner sum $\sum_{d'|(n/c)} \mu((n/c)/d')$ is equal to 1 if $n/c = 1$ and 0 otherwise, hence the right hand side is b_n. □

The proof of the converse of Lemma 3 is similar. I will prove both directions more generally in the notes below (combine Theorem 13 and Example 15 and this shows Lemma 3 and its converse).

When we started the class we talked about telescoping sums and I gave several exercises where $a_n = \sum_{i=1}^{n} b_i$ and I said that we could prove this if we show $b_n = a_n - a_{n-1}$, then it follows that $\sum_{i=1}^{n} b_i = \sum_{i=2}^{n} (a_i - a_{i-1}) + a_1 = \sum_{i=1}^{n} a_i - \sum_{i=2}^{n} a_{i-1} = a_n$.

I want to organize three seemingly different systems of equations that and develop a technique in order to solve them:

$$\begin{array}{rcr} a_n = \sum_{i=1}^{n} b_i & \text{if and only if} & b_n = a_n - a_{n-1} \\ a_n = \sum_{d|n} b_d & \text{if and only if} & b_n = \sum_{d|n} \mu(n/d) a_d \\ a_S = \sum_{T \subset S} b_T & \text{if and only if} & b_S = \sum_{T \subset S} (-1)^{|S|-|T|} a_T \end{array}$$

The first of these is telescoping sums, the second is Möbius inversion, third one we haven't used yet in any obvious manner, but it is equivalent to inclusion-exclusion. I will next discuss a setup where there are many formulae that fit this pattern.

1. Partially ordered sets

A partially ordered set (*poset* for short) is a (countable or finite) set of objects, S, together with a binary relation $\leq$ satisfying

(1) $x \leq x$ for $x \in S$,
(2) if $x \leq y$ and $y \leq x$, then $x = y$,
(3) if $x \leq y$ and $y \leq z$, then $x \leq z$.

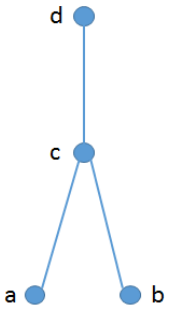
Note: this definition is kind of modeled on

A binary relation that satisfies (1) is called a *reflexive* relation. A binary relation that satisfies condition (3) is called *transitive*. If you have seen these definitions before it would have been likely that they would have come up in a discussion about 'equivalence relations' and every equivalence relation satisfies (1), (3) and a third relation that says if x is related to y, then y is related to x. A partial order satisfies a weaker condition so every equivalence relation is a partial order, but not every partial order is an equivalence relation.

A partial order is sort of a generalization of the notion of $\leq$ on the set of numbers.

For each poset there is a diagram, called a Hasse diagram, which encodes the information in the order and the set in a picture. The Hasse diagram for a poset $P = (S, \leq)$ has a point for each element x in S. If $x \leq y$ in the poset then x is placed lower in the diagram. If $x \leq y$ and there does not exists a z such that $x \leq z \leq y$ then a line is drawn between the two points representing x and y. If x and y are not comparable in the poset, then no edge is placed between x and y and there should be no upward path between x and y either.

Example 4. For example



is the Hasse diagram for a poset with three elements in the set and $a \leq c$ and $b \leq c$ while a and b are not comparable while a, b and c are all less than or equal to d.

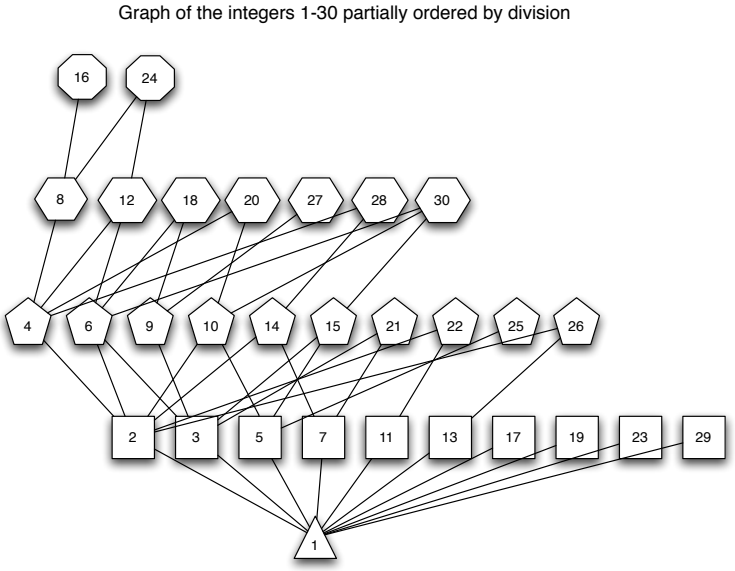
While that example explains a small example of a finite poset, below are four examples which provide us with infinite examples of posets.

Example 5. Consider the poset $(\{1, 2, \ldots, n\}, \leq)$ where $a \leq b$ if $b - a$ is a non-negative integer. This is the normal order on integers and the poset looks like a chain.

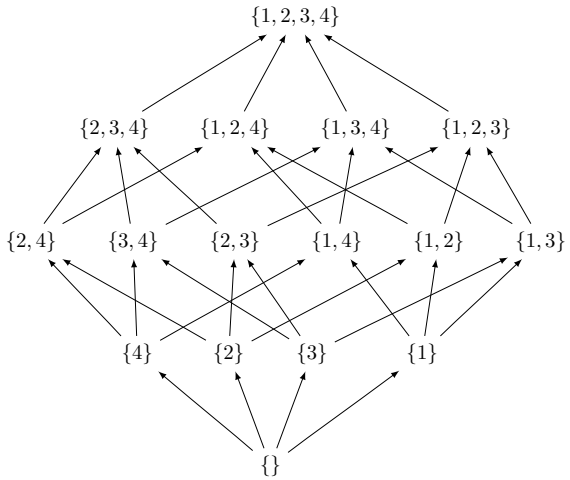
In this case, every pair of integers satisfies either $x \leq y$ or $y \leq x$ (or both if $x = y$). This is not typical of a poset and this is where the "partial" from phrase "partially ordered set" comes from. Typically a poset will have some elements x, y such that $x \not\leq y$ and $y \not\leq x$,

that is, there are pairs of elements which are not comparable. A poset where every pair of elements x, y has either $x \leq y$ or $y \leq x$ is referred to as a total order.

Example 6. The poset of integers $(\{1, 2, 3, \ldots), \leq_|)$ where the notation $a \leq_| b$ if a divides b. This is an infinite poset and so the Hasse diagram can only represent a portion of it. I had drawn this one in class and it has 1 as a minimal element (because 1 divides every integer). Then on a level above 1 there are all the primes with a line from 1 to each of those primes. On level k of this poset there are all the integers which are a product of k primes.



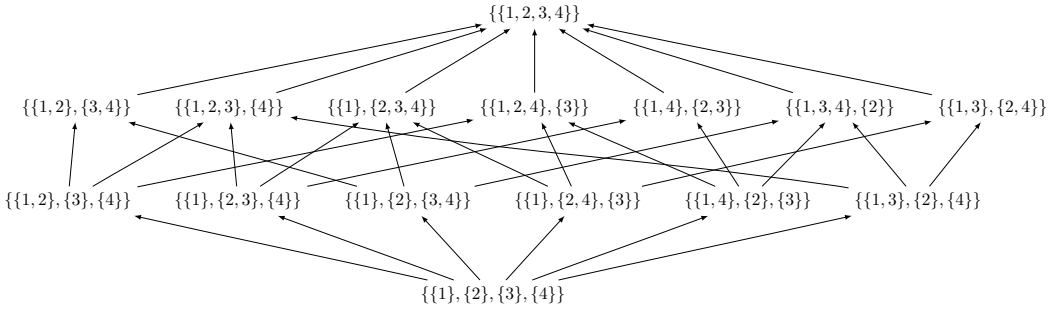
Example 7. Consider the set $B_n = \{S : S \subseteq \{1, 2, 3, \ldots, n\}\}$ and the order S is less than or equal to T if $S \subseteq T$. This is known as the Boolean poset. For every n, B_n has 2^n elements. The Boolean poset for $n = 4$ is shown below.



The picture above was created in Sage with the command `view(Poset((Subsets(4),lambda S,T: S.issubset(T))))` .

Example 8. Any set S with the relation $x = x$ is an equivalence relation and partial order $(S, =)$. The Hasse diagram looks like a sequence of points all at the same level and none of them are connected.

Example 9. The set partitions $\{1, 2, \ldots, n\}$ are the set of sets $\{S_1, S_2, \ldots, S_r\}$ where each $S_i \subseteq \{1, 2, \ldots, n\}$ such that $S_1 \cup S_2 \cup \cdots \cup S_r = \{1, 2, \ldots, n\}$ and all of the S_i are are all disjoint. We say that $\{S_1, S_2, \ldots, S_r\} \leq \{T_1, T_2, \ldots, T_d\}$ if for each $1 \leq i \leq r$, $S_i \subseteq T_j$ for some $1 \leq j \leq d$. An example of the Hasse diagram for this poset for $n = 4$ is shown below.



The image above was created with Sage using the command `view(Poset((SetPartitions(4), lambda A,B: A in B.refinements()))))` .

2. The Möbius function of a poset

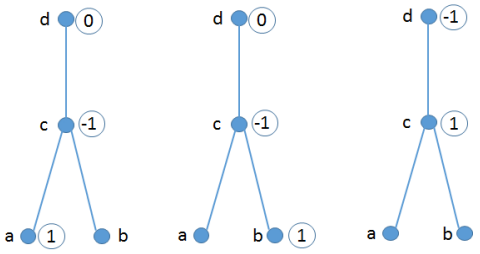
For any poset and any pair of elements x, y in the poset, define $\mu(x, y) = 0$ if $x \not\leq y$, $\mu(x, x) = 1$ and if $x \leq y$, then $\sum_{x \leq z \leq y} \mu(x, z) = 0$. Equivalently, $\mu(x, y) = -\sum_{x \leq z < y} \mu(x, z)$.

In summary,

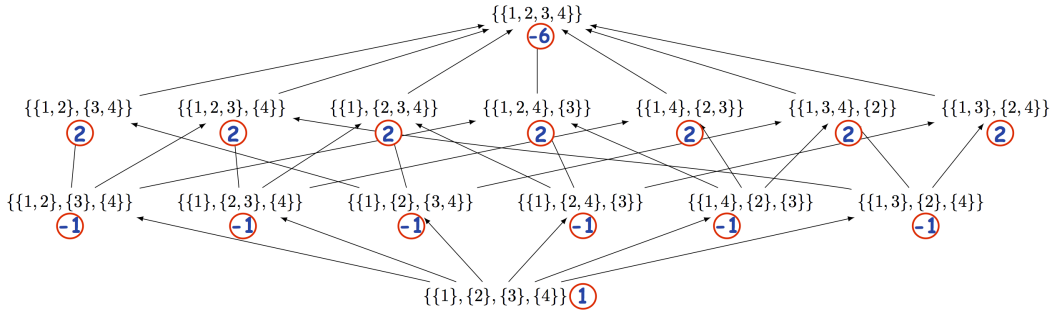
$$\mu(x,y) = \begin{cases} 0 & \text{if } x \not\leq y \\ 1 & \text{if } x = y \\ -\sum_{x \leq z < y} \mu(x,z) & \text{if } x < y \end{cases} . \tag{5}$$

We need only compute this Möbius function on all intervals $x \leq y$. In order to compute the value of the function $\mu(x,y)$ we set the value $\mu(x,x)$ and then for each y in the poset, we let $\mu(x,y)$ be the value so that the sum of all the values $\mu(x,z)$ where $x \leq z \leq y$ sum to 0.

Example 10. Below we compute the Möbius value of the poset for the three non-trivial intervals of the small example with 4 vertices above.



Example 11. The Möbius function for the poset of set partitions of 4 of the form $\mu(\{\{1\},\{2\},\{3\},\{4\}\},\pi)$ where π is a set partition of 4.



The reason for this definition of the M"obius function is that it is a combinatorial means to do linear algebra. If we have a system of linear equations indexed by the elements of a poset such as $a_x = \sum_{y \leq x} b_y$, then these unknowns are related by $b_x = \sum_{y \leq x} \mu(y,x) a_y$. We saw this relationship between equation (2) and (3). In this case the Möbius function for the poset of integers ordered by division is $\mu(d,n) = \mu(n/d)$ where on the left hand side of the equation $\mu(d,n)$ is given by equation (5) and on the right hand side $\mu(n/d)$ is given by Definition 1.

Define a function on pairs x, y in the poset by

$$\zeta(x,y) = \begin{cases} 1 & \text{if } x \leq y \\ 0 & \text{if } x \not\leq y \end{cases} \tag{6}$$

It follows that we can express any sum like

$$a_x = \sum_{y \leq x} b_y = \sum_y \zeta(y,x) b_y \tag{7}$$

in terms of the coefficients of the function $\zeta(y,x)$

Let P be a finite poset with n elements. First order our elements in the poset with a total order $\{x_1, x_2, \ldots, x_n\}$ so that the smaller elements come first, then we can define a matrix

$$Z = [\zeta(x,y)]_{x,y \in P} = \begin{pmatrix} \zeta(x_1,x_1) & \zeta(x_1,x_2) & \cdots & \zeta(x_1,x_n) \\ \zeta(x_2,x_1) & \zeta(x_2,x_2) & \cdots & \zeta(x_2,x_n) \\ \vdots & \vdots & \ddots & \vdots \\ \zeta(x_n,x_1) & \zeta(x_n,x_2) & \cdots & \zeta(x_n,x_n) \end{pmatrix} .$$

This matrix allows us to express the set of equations in (7) in matrix notation

(8)

$$\begin{pmatrix} a_{x_1} & a_{x_2} & \cdots & a_{x_n} \end{pmatrix} = \begin{pmatrix} b_{x_1} & b_{x_2} & \cdots & b_{x_n} \end{pmatrix} \begin{pmatrix} \zeta(x_1,x_1) & \zeta(x_1,x_2) & \cdots & \zeta(x_1,x_n) \\ \zeta(x_2,x_1) & \zeta(x_2,x_2) & \cdots & \zeta(x_2,x_n) \\ \vdots & \vdots & \ddots & \vdots \\ \zeta(x_n,x_1) & \zeta(x_n,x_2) & \cdots & \zeta(x_n,x_n) \end{pmatrix} .$$

Notice that if we list the elements in order where the smallest elements are first then $\mu(x_j, x_i) = 0$ if $j > i$ and so the matrix Z will be upper triangular (actually the fact that you can do this is a consequence of property (2) and (3) of the definition of a poset). Moreover since $\mu(x_i, x_i) = 1$ for all $1 \leq i \leq n$ we have that Z is upper unitriangular. Therefore $Z = I_{n \times n} + N$ where $I_{n \times n}$ is the $n \times n$ identity matrix and N is a nilpotent matrix (a matrix such that N^n is the zero matrix). Note that the reason that N is a nilpotent matrix is that it has 0's on and below the main diagonal so N^r will have 0's on the first r diagonals and N^n will have nothing but 0 entries.

As a consequence, we have that

$$Z^{-1} = I - N + N^2 - \cdots + (-1)^{n-1} N^{n-1}$$

since

$$\begin{aligned}(I+N)(I - N + N^2 - \cdots + (-1)^{n-1} N^{n-1}) &= I - N + N^2 - \cdots + (-1)^{n-1} N^{n-1} \\ &\quad + N - N^2 + N^3 - \cdots + (-1)^{n-1} N^n = I .\end{aligned}$$

If we define

$$M = \begin{pmatrix} \mu(x_1,x_1) & \mu(x_1,x_2) & \cdots & \mu(x_1,x_n) \\ \mu(x_2,x_1) & \mu(x_2,x_2) & \cdots & \mu(x_2,x_n) \\ \vdots & \vdots & \ddots & \vdots \\ \mu(x_n,x_1) & \mu(x_n,x_2) & \cdots & \mu(x_n,x_n) \end{pmatrix}$$

then M is also upper unitriangular since $\mu(x_j, x_i) = 0$ if $j > i$ and $\mu(x_i, x_i) = 1$.

Recall that if we have two matrices A and B which are indexed by the elements of the poset then the (x_i, x_j) entry of $AB = \sum_y A_{x_i,y} B_{y,x_j}$. Hence if we take the (x_i, x_j) entry of MZ, then this is equal to

$$\sum_y \mu(x_i, y)\zeta(y, x_j) = \sum_{y \leq x_j} \mu(x_i, y) = \sum_{x_i \leq y \leq x_j} \mu(x_i, y)$$

which is equal to 1 if $x_i = x_j$ and it is equal to 0 otherwise. In other words, $MZ = I$ and $M = Z^{-1}$ and for any x, z in the poset,

$$\sum_{z \leq y \leq x} \mu(z, y) = \begin{cases} 1 & \text{if } z = x \\ 0 & \text{if } z \neq x \end{cases} \tag{9}$$

Since M is the left inverse of Z then it is also it's right inverse so the (x_i, x_j) entry of ZM is

$$\sum_y \zeta(x_i, y)\mu(y, x_j) = \sum_{x_i \leq y \leq x_j} \mu(y, x_j) = \begin{cases} 1 & \text{if } x_i = x_j \\ 0 & \text{if } x_i \neq x_j \end{cases} \tag{10}$$

where the second equality happens because $ZM = I$. Hence we also have for x, z in the poset,

$$\sum_{z \leq y \leq x} \mu(y, x) = \begin{cases} 1 & \text{if } z = x \\ 0 & \text{if } z \neq x \end{cases} . \tag{11}$$

Example 12. Lets do a simple example to make sure it is clear what is happening in each of these formula. Consider the running example from Examples 4 and Example 10. We will label the rows and columns of the matrices Z and M by the poset entries $\{a, b, c, d\}$ in that order. Then we have

$$Z = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad M = \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{12}$$

You can quickly check that Z and M are inverses of each other and Z can be computed from the picture in Example 4 and M can be computed from the three pictures in Example 10. Moreover if we let

$$N = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{13}$$

(since $N = Z - I$), then you can also check that $M = I - N + N^2 - N^3$.

We can use this formula to prove that the Möbius function is there to help us do linear algebra. It gives us a relatively explicit formula for inverting a system of equations like $a_x = \sum_{y \leq x} b_y$.

Theorem 13. *Let P be a finite poset with relation $\leq$, then*

$$a_x = \sum_{y \leq x} b_y \text{ iff } b_x = \sum_{y \leq x} \mu(y,x) a_y$$

and

$$a_x = \sum_{y \geq x} b_y \text{ iff } b_x = \sum_{y \geq x} \mu(x,y) a_y \ .$$

Proof. Assume that $a_x = \sum_{y \leq x} b_y$ for all elements $x \in P$ (or as we will use this equation, $a_y = \sum_{z \leq y} b_z$), then

$$\sum_{y \leq x} \mu(y,x) a_y = \sum_{y \leq x} \sum_{z \leq y} \mu(y,x) b_z = \sum_{z \leq x} \sum_{z \leq y \leq x} \mu(y,x) b_z = b_x$$

where the last equality follows from equation (9). The second equality holds by interchanging the order of the sum. I did this in a video

`https://www.youtube.com/watch?v=5stHeMbYghY`

Now to prove the "only if" part of the first statement, assume that $b_y = \sum_{z \leq y} \mu(z,y) a_z$, then

$$\sum_{y \leq x} b_y = \sum_{y \leq x} \sum_{z \leq y} \mu(z,y) a_z = \sum_{z \leq x} = \sum_{z \leq y \leq x} \mu(z,y) a_z = a_x$$

where the last equality follows from equation (10).

These two calculations show the first "if and only if", the second statement in the theorem has an almost identical proof which I leave to the reader as an exercise. □

Example 14. The poset of positive integers ordered by the order in Example 5 has a Möbius function

$$\mu(i,j) = \begin{cases} 1 & \text{if } j = i \\ -1 & \text{if } j = i+1 \\ 0 & \text{otherwise} \end{cases} \tag{14}$$

This follows because we can easily check that $\sum_{a \leq b \leq c} \mu(a,b) = 0$ if $a \neq c$.

Theorem 13 says in the case of the positive integers that if

$$a_n = b_1 + b_2 + \cdots + b_n$$

for all $n \geq 1$, then

$$b_n = a_n - a_{n-1} \ .$$

This is called the method of telescoping sums (I had created a youtube video on the subject at `https://www.youtube.com/watch?v=H6MmDRtuiNw`).

Example 15. Lets come back to the poset in Example 6. The poset of positive integers order by division is where this topic began because we had a system of linear equations where $a_n = \sum_{d|n} b_d$ (see equation (2)) and I showed that there was a formula for b_n in terms

of the a_n, namely, $b_n = \sum_{d|n} \mu(n/d)a_d$ where the Möbius function is defined in Definition 1.

Warning: I am using the symbol μ in two different ways here. One is $\mu(n)$, with one argument, and this is the function which is defined in Definition 1. The other is $\mu(a, d)$, with two arguments, and this is the Möbius function of the poset of integers ordered by division which is defined by equation (5). These functions are related by $\mu(a, d) = \mu(d/a)$ if a divides d and $\mu(a, d) = 0$ otherwise. We will use Lemma 2 and the matrix notation that we built up previously to show why.

We will work with a finite poset and consider only those in the set $\{1, 2, \ldots, n\}$. The Möbius function that is defined by equation (5) (as the function defined by the $\sum_{a|d}$ and $_{d|n} \mu(a, d) = 0$ if $a \neq n$) are the entries $\mu(a, d)$ in the $n \times n$ matrix M which is the inverse of the matrix Z. By defining a matrix

$$M' = \left[\begin{cases} \mu(d/a) & \text{if } a|d \\ 0 & \text{otherwise} \end{cases} \right]_{1 \leq a,d \leq n}$$

we can then apply Lemma 2 to show that M' is also the inverse of Z. Therefore we conclude that $M = M'$ and

$$\mu(a, d) = \begin{cases} \mu(d/a) & \text{if } a|d \\ 0 & \text{otherwise} \end{cases}.$$

Example 16. The poset of subsets of $\{1, 2, \ldots, n\}$ that we introduced in Example 7 is called the Boolean poset. The Möbius function for this poset is

$$\mu(S, T) = \begin{cases} (-1)^{|T|-|S|} & \text{if } S \subseteq T \\ 0 & \text{otherwise} \end{cases}. \tag{15}$$

As an exercise, I asked you to prove the very Lemma that you need to to show that $\mu(S, T)$ has this formula, namely,

Lemma 17. *For fixed subsets U and T,*

$$\sum_{U \subseteq S \subseteq T} (-1)^{|T|-|S|} = \begin{cases} 1 & \textit{if } U = T \\ 0 & \textit{otherwise} \end{cases}$$

As in our previous example, this Lemma would show that the matrix whose rows and columns are indexed by the subsets of $\{1, 2, \ldots, n\}$ and whose entries are $(-1)^{|T|-|S|}$ if $S \subseteq T$ and 0 otherwise is the inverse of the matrix Z whose entries are 1 if $S \subseteq T$ and 0 otherwise. This proves that (15) is the Möbius function for this poset.

3. Inclusion-Exclusion

I think a typical topic that we would include in a combinatorics class is that of inclusion-exclusion but I don't always cover it because I think of it is a specialized technique with

limited applications. The addition principle that we started this class with says that if there are disjoint sets $A_1, A_2, \ldots, A_k$, then

$$|A_1 \cup A_2 \cup \cdots \cup A_k| = |A_1| + |A_2| + \cdots + |A_k| \ .$$

The formula for inclusion-exclusion says how to calculate $|A_1 \cup A_2 \cup \cdots \cup A_k|$ in the case when the sets A_i are not disjoint. It says

$$|A_1 \cup A_2 \cup \cdots \cup A_k| = \sum_{\emptyset \subset I \subseteq \{1,2,\ldots k\}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right| \tag{16}$$

or in less terse notation

$$\begin{aligned} |A_1 \cup A_2 \cup \cdots \cup A_k| &= |A_1| + |A_2| + \cdots + |A_k| - |A_1 \cap A_2| - |A_1 \cap A_3| - \cdots - |A_{k-1} \cap A_k| \\ &\quad + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + \cdots + |A_{k-2} \cap A_{k-1} \cap A_k| - \cdots \\ &\quad + (-1)^{k-1} |A_1 \cap A_2 \cap \cdots \cap A_k| \ . \end{aligned}$$

The reason it is a useful formula is that it can be used to count the number of elements in a union of sets when we can't easily separate them into disjoint pieces but we can enumerate the intersections. A simple example is counting the number of hands of cards where at least one of the suits is not included (see Example 20 below). If you try to count this set there are two ways of going about it: addition principle and inclusion-exclusion. The reference [4] also develops Inclusion-Exclusion using Möbius inversion and the development here is very similar to that presentation.

Although there are many ways to prove the inclusion-exclusion formula, we will use Möbius inversion. Typically it is proved using a sign reversing involution, induction or other method. For example, the book [2] presents several different proofs of Inclusion-Exclusion and presents Möbius inversion in the section on "Inclusion-Exclusion and Related Techniques."

Theorem 18. *(Inclusion-Exclusion formula) Let S be a finite set and $A_1, A_2, \ldots, A_k$ be subsets of S, then*

$$|S| - |A_1 \cup A_2 \cup \cdots \cup A_k| = \sum_{J \subseteq \{1,2,\ldots k\}} (-1)^{|J|} \left| \bigcap_{j \in J} A_j \right| \tag{17}$$

The sum on the right hand side of this equation is over subsets J of $\{1, 2, \ldots, k\}$ and, in particular, when J is the empty the term $\bigcap_{j \in J} A_j = S$. Note that equation (16) is equivalent to this statement by isolating $|A_1 \cup A_2 \cup \cdots \cup A_k|$ on one side of the equation.

The notation is quite terse, so it is worth trying the formula for the first few values of k. In the case that $k = 1$ and it says $|S| - |A_1| = |S| - |A_1|$ which is not very interesting. For $k = 2$ the expression is

$$|S| - |A_1 \cup A_2| = |S| - |A_1| - |A_2| + |A_1 \cap A_2|$$

and for $k = 3$, it says

$$|S| - |A_1 \cup A_2 \cup A_3| = |S| - |A_1| - |A_2| - |A_3| + |A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3| - |A_1 \cap A_2 \cap A_3| \ .$$

Proof. For a subset $I \subseteq \{1, 2, \ldots, k\}$, let

$$a_I = \left| \bigcap_{i \in I} A_i \right|$$

and

$$b_I = \left| \bigcap_{i \in I} A_i - \bigcup_{J \supset I} \bigcap_{j \in J} A_j \right| .$$

Lemma 19 (below) says that

$$a_I = \sum_{I \subseteq J \subseteq \{1,2,\ldots,k\}} b_J$$

and Theorem 13 says that

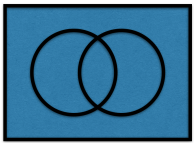
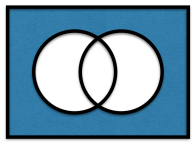
$$b_I = \sum_{I \subseteq J \subseteq \{1,2,\ldots,k\}} \mu(I, J) a_J \ .$$

In particular $b_\emptyset = |S| - |A_1 \cup A_2 \cup \cdots \cup A_k|$ because the empty intersection is S and $\bigcup_{J \supset \emptyset} \bigcap_{j \in J} A_j = A_1 \cup A_2 \cup \cdots \cup A_k$ and by Example 16, $\mu(\emptyset, J) a_J = (-1)^{|J|} \left| \bigcap_{j \in J} A_j \right|$ so equation (17) holds. □

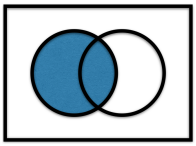
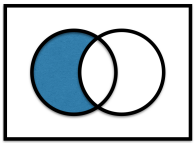
That was a terse proof because all of the work was done by Möbius inversion and in the setup of the sets representing the a_I and b_I (and all of that work is in Lemma 19). It might be a little disorienting that the final expression for inclusion-exclusion is just $b_\emptyset$ and we didn't need all of the other b_I (but then that means the expression for b_I is a more general result than just inclusion-exclusion alone).

What is probably not clear is the use of b_I as the cardinality of the sets $\bigcap_{i \in I} A_i - \bigcup_{J \supset I} \bigcap_{j \in J} A_j$. It is worth showing how the general formulas work with $k = 2$ using Venn diagrams in order to see how this is Möbius inversion in disguise.

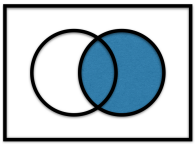
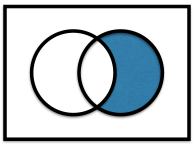
By the definitions of the a_I and b_I, we have

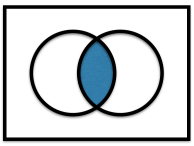
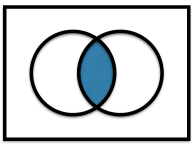
$$a_\emptyset = |S| \qquad b_\emptyset = |S - A_1 \cup A_2 \cup (A_1 \cap A_2)|$$

$$a_{\{1\}} = |A_1| \qquad b_{\{1\}} = |A_1 - A_1 \cap A_2|$$

$$a_{\{2\}} = |A_2| \qquad b_{\{2\}} = |A_2 - A_1 \cap A_2|$$

$$a_{\{1,2\}} = |A_1 \cap A_2| \qquad b_{\{1,2\}} = |A_1 \cap A_2|$$

From the pictures it is not hard to see a detail in the proof that I left as a Lemma. You can easily see in the pictures (and this is just an example), that

$$\begin{aligned} a_\emptyset &= b_\emptyset + b_{\{1\}} + b_{\{2\}} + b_{\{1,2\}} \\ a_{\{1\}} &= b_{\{1\}} + b_{\{1,2\}} \\ a_{\{2\}} &= b_{\{2\}} + b_{\{1,2\}} \\ a_{\{1,2\}} &= b_{\{1,2\}} \end{aligned}$$

The next lemma explains why the a_I are a sum of b_J over J subsets of $\{1, 2, \ldots, k\}$ which contain I.

Lemma 19. *For subsets $A_1, A_2, \ldots, A_k$ of S and for $I \subseteq \{1, 2, \ldots, k\}$, if $a_I = \left|\bigcap_{i\in I} A_i\right|$ and $b_I = \left|\bigcap_{i\in I} A_i - \bigcup_{J\supset I} \bigcap_{j\in J} A_j\right|$, then*

$$a_I = \sum_{I\subseteq J\subseteq\{1,2,\ldots,k\}} b_J \ .$$

Proof. In English, the description of b_I are the elements x which are in the intersections of A_i for i is in I such that x is not in any of the other A_j where j is not in I.

Let

$$B_I = \bigcap_{i\in I} A_i - \bigcup_{J\supset I} \bigcap_{j\in J} A_j,$$

then $b_I = |B_I|$. I will show that $\cap_{i\in I} A_i = \bigcup_{I\subseteq J\subseteq\{1,2,\ldots,k\}} B_J$ and the subsets B_J are all disjoint.

Take an element x in $\cap_{i\in I} A_i$, then x is in the intersection of some set of A_j for $j \in J$ where $I \subseteq J \subseteq \{1, 2, \ldots, k\}$. Let J be the largest set of indices with this property then

$x \in \bigcap_{j\in J} A_j$ and $x \notin \bigcup_{K\supset J} \bigcap_{j\in K} A_j$. This implies that $x \in B_J$ and (since x was arbitrary),

$$\cap_{i\in I} A_i \subseteq \bigcup_{I\subseteq J\subseteq\{1,2,\ldots,k\}} B_J \ .$$

It follows since $B_J \subseteq \cap_{i\in I} A_i$ that

$$\cap_{i\in I} A_i = \bigcup_{I\subseteq J\subseteq\{1,2,\ldots,k\}} B_J \ .$$

Next I claim that the B_J are also disjoint. That is, if $J \neq K$ then $B_J \cap B_K = \emptyset$. Take two sets $J \neq K$ and order them so that $J \neq J \cup K$. If we take an $x \in B_J \cap B_K$, then $x \in \bigcap_{k\in K} A_k$ and $x \in \bigcap_{j\in J} A_j$, hence it is in $\bigcap_{j\in J\cup K} A_j$, and since $J \neq J \neq K$ $x \notin B_J$ by definition, but this is a contradiction. Hence $B_J \cap B_K$ must be empty.

Therefore we have by the addition principle that

$$a_I = |\cap_{i\in I} A_i| = \sum_{I\subseteq J\subseteq\{1,2,\ldots,k\}} |B_J| = \sum_{I\subseteq J\subseteq\{1,2,\ldots,k\}} b_J \ .$$

□

Example 20. Say that we want to compute the number of 5 cards hands are there were every suit appears at least once (or equivalently the number of 5 card hands where at least one suit does not appear and subtract this result from $\binom{52}{5}$ the total number of 5 card hands).

Since there are 4 suits, exactly one of the 4 will have to appear twice. A 5 card hand where every suit appears at least once is determined by choosing a suit which appears twice, two cards from that suit and one card from each of the remaining suits. By the multiplication principle there are $4 \cdot \binom{13}{2} \cdot 13^3$ such hands.

Now lets try to count the same value using the inclusion-exclusion formula. For a set of suits I, let A_I be the set of 5 card hands that do not contain the suits in I. For instance $A_{\{\heartsuit,\diamondsuit\}}$ is the set of 5 card hands that don't contain either hearts or diamonds. Let S represent the set of all 5 card hands, then to compute the number of 5 card hands where every suit appears at least once we are looking for the cardinality of $S - A_{\{\heartsuit\}} \cup A_{\{\diamondsuit\}} \cup A_{\{\clubsuit\}} \cup A_{\{\spadesuit\}}$.

By the principle of inclusion exclusion, this is

$$\sum_{J\subseteq\{\heartsuit,\diamondsuit,\clubsuit,\spadesuit\}} (-1)^{|J|} |A_J| \ .$$

But the cardinality of A_J is equal to $\binom{13\cdot(4-|J|)}{5}$ and since there are $\binom{4}{k}$ subsets J of size k of $\{\heartsuit,\diamondsuit,\clubsuit,\spadesuit\}$, then the number of 5 card hands where every suit appears at least once is

$$\binom{52}{5} - 4\cdot\binom{39}{5} + 6\cdot\binom{26}{5} - 4\cdot\binom{13}{5} \ .$$

This expression is equal to $4 \cdot \binom{13}{2} \cdot 13^3 = 685464$.

In that example inclusion-exclusion was not the tool that we wanted to use because it was much easier to count the hands that contained all of the suits at least once by the multiplication principle than set up an inclusion-exclusion. But there are other examples where an application of inclusion-exclusion is the best way to count a quantity.

Example 21. Say that there are cereal boxes, essentially identical, with one of k different possible prizes and we want to estimate how many boxes of cereal that we need to buy to have a probability that we have at least one of each of the prizes. To do this we will compute the number of ways of picking n boxes of cereal such that all of the k prizes appear.

For a set $\{1, 2, \ldots, k\}$, let A_I represent the ways of picking n boxes of cereal such i^{th} prize for $i \in I$ does not occur. By the multiplication principle $|A_I| = (k - |I|)^n$. If we let S represent the set of choices of n cereal boxes then the number of possible prize sequences is $|S| = k^n$ and we wish to compute $|S - A_{\{1\}} \cup A_{\{2\}} \cup \cdots \cup A_{\{k\}}|$. We apply inclusion exclusions to conclude that it is equal to

$$\sum_{I \subseteq \{1,2,\ldots k\}} (-1)^k |A_I| = \sum_{r=0}^{k} (-1)^k \binom{k}{r} (k-r)^n \ .$$

So then if we try to compute the probability of picking n boxes and getting all k prizes, we would divide by the total number of sequences of prizes of length n and this implies

$$P(\text{all } k \text{ prizes occur in } n \text{ choices of cereal boxes}) = \sum_{r=0}^{k} (-1)^k \binom{k}{r} \frac{(k-r)^n}{k^n}$$

The most common application of inclusion-exclusion is to compute the number of "derangements" of the numbers $\{1, 2, \ldots, n\}$. These are the permutations π of $\{1, 2, \ldots, n\}$ such that $\pi(i) \neq i$ for all $1 \leq i \leq n$. This application is explained almost everywhere so I will refer the reader to any one of the references: [1, Theorem 4.4], [2, Section 4.5], [5], [6].

References

[1] R.B.J.T. Allenby, A. Slomson, *How to Count: an introduction to combinatorics*, Second Edition, CRC Press, 2011.

[2] N. A. Loehr, *Bijective Combinatorics*, CRC Press, 2011.

[3] R. Staneley, *Enumerative Combinatorics, Vol 1*, Wadsworth & Brooks/Cole, 1986.

[4] Erin Stuhlsatz, Möbius Inversion Formula, notes:
`https://www.whitman.edu/Documents/Academics/Mathematics/stuhlsatz.pdf`

[5] Wikipedia entry on derangements, `https://en.wikipedia.org/wiki/Derangement`

[6] Dennis White, Inclusion-Exclusion and Derangements, notes:
`http://www-users.math.umn.edu/~reiner/Classes/Derangements.pdf`