Exercise 7

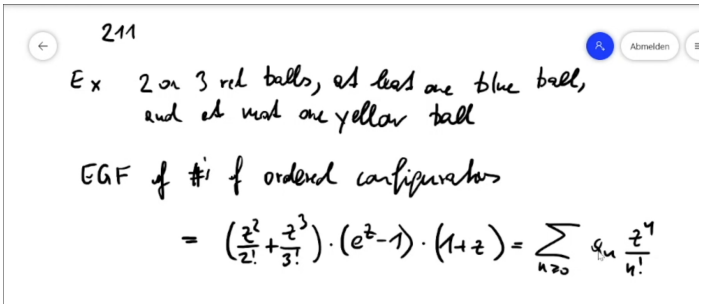
Discrete Mathematics

November 26, 2020

Exercise 61

Recall that given a sequence $a_0, a_1, a_2, \ldots, a_k, \ldots$ the function $\hat{A}(z) = \sum_{k \geq 0} a_k \frac{z^k}{k!}$ is called the exponential generating function (EGF) of the sequence.

First of all, we clarify what we are actually looking for. We're looking for *ordered* choices of *indistinguishable* balls. A similar example has been done in the lecture:



In this note $z^3/3!$ symbolises 3 red balls. The coefficient of it is 1, so there is exactly 1 possible way to choose 3 red balls. If they were labeled/distinguishable, there would be 3! choices. This would give the term $3!\frac{z^3}{3!} = z^3$.

The taylor series expansion of this equation even starts with exactly this term $3!\frac{z^3}{3!} = z^3$. Let $n = 3$. Denote red balls with r and blue balls with b. This means the balls are indistinguishable. This way, we get the 3 configurations rrg,rgr,grr which fulfill the requirement. We see that this is exactly the coefficient from the taylor series.

Consider the identities of sequence (left) and EGF (right)

$$1, 1, 1, 1, 1, 1, \ldots, 1, \ldots \qquad e^z = \sum_{n \geq 0} \frac{z^n}{n!}$$

$$1, 0, 1, 0, \ldots, 1, 0, \ldots \qquad \frac{1}{2}\left(e^z + e^{-z}\right) = \sum_{n \geq 0} \frac{1 + (-1)^n}{2} \frac{z^n}{n!} \tag{1}$$

For understanding the second identity, observe the first few terms of it have indeed its sequence as coefficients.

$$\sum_{n\geq 0} \frac{1+(-1)^n}{2}\frac{z^n}{n!} = \frac{1+(-1)^0}{2}\frac{z^0}{0!} + \frac{1+(-1)^1}{2}\frac{z^1}{1!} + \frac{1+(-1)^2}{2}\frac{z^2}{2!} + \frac{1+(-1)^3}{2}\frac{z^3}{3!}\cdots$$
$$= \frac{2}{2} + \frac{0}{2}\frac{z^1}{1!} + \frac{2}{2}\frac{z^2}{2!} + \frac{0}{2}\frac{z^3}{3!}\cdots$$

and that by the addition operation for EGF $A(z)+B(z) = \sum_{n\geq 0}(a_n+b_n)\frac{z^n}{n!}$ and the first identity, the second identity really holds

$$\sum_{n\geq 0} \frac{1+(-1)^n}{2}\frac{z^n}{n!} = \frac{1}{2}\sum_{n\geq 0}(1+(-1)^n)\frac{z^n}{n!} = \frac{1}{2}\left(\sum_{n\geq 0}\frac{z^n}{n!} + \sum_{n\geq 0}\frac{(-z)^n}{n!}\right) = \frac{1}{2}\left(e^z + e^{-z}\right)$$

This second identity 1 shows the number of green balls.

We can think of solving problems on n elements as imposing a certain structure on them, for example, the trivial structure of "being a set". To impose the trivial structure on a given set is to give the elements only that structure which they already have: the structure of a set. The point is, there is just one such structure on every set. Thus the number of trivial "being a set" structures on an n-element is $f(n=1)$ for every n. The EGF for this trivial structure is therefore

$$\hat{A}(x) = \sum_{n\geq 0}\frac{x^n}{n!} = e^x \tag{2}$$

This is the only restriction that we have for the set of blue balls. Consequently, 2 describes the blue balls.

The sequence with exactly $a_2 = 1$ and every other element 0 gives the EGF $\frac{x^2}{2!}$. We use an analog argument for $a_4 = 1$. This gives us EGF for the red balls.

Therefore, we finally get the EGF that describes required ordered choices of balls.

$$\hat{A}(z) = \sum_{k\geq 0} a_k \frac{z^k}{k!} = \left(\frac{z^2}{2!} + \frac{z^4}{4!}\right)\cdot\frac{1}{2}\left(e^z + e^{-z}\right)\cdot e^x \tag{3}$$

Using the identity $e^z = \sum_{n\geq 0} z^n/n!$

`https://math.stackexchange.com/a/3452283` `https://math.stackexchange.com/`

$$\begin{aligned}
\hat{A}(z) &= \left(\frac{x^2}{2!} + \frac{x^4}{4!}\right)\frac{1}{2}\left(e^x + e^{-x}\right)e^x \\
&= \left(\frac{x^2}{2!} + \frac{x^4}{4!}\right)\frac{1}{2}(e^{2x} + 1) \\
&= \frac{1}{2}\left(\frac{x^2}{2!} + \frac{x^4}{4!}\right) + \frac{1}{2}\left(\frac{x^2}{2!} + \frac{x^4}{4!}\right)e^{2x} \\
&= \frac{1}{2}\left(\frac{x^2}{2!} + \frac{x^4}{4!}\right) + \frac{1}{2}\left(\frac{x^2}{2!} + \frac{x^4}{4!}\right)\sum_{n=0}^{\infty}\frac{1}{n!}2^n x^n \\
&= \frac{1}{2}\left(\frac{x^2}{2!} + \frac{x^4}{4!}\right) + \frac{1}{2}\cdot\frac{x^2}{2!}\sum_{n=0}^{\infty}\frac{1}{n!}2^n x^n + \frac{1}{2}\cdot\frac{x^4}{4!}\sum_{n=0}^{\infty}\frac{1}{n!}2^n x^n \\
&= \frac{1}{2}\cdot\frac{x^2}{2!} + \frac{1}{2}\cdot\frac{x^4}{4!} + g(x) + h(x)
\end{aligned}$$

to keep equations short, we define

$$g(x) = \frac{1}{2}\cdot\frac{x^2}{2!}\sum_{n=0}^{\infty}\frac{1}{n!}2^n x^n$$

and

$$h(x) = \frac{1}{2}\cdot\frac{x^4}{4!}\sum_{n=0}^{\infty}\frac{1}{n!}2^n x^n$$

Then using the index shift $i = n + 2$

$$\begin{aligned}
g(x) &= \frac{1}{2}\cdot\frac{x^2}{2!}\sum_{n=0}^{\infty}\frac{1}{n!}2^n x^n \\
&= \frac{1}{4}\sum_{n=0}^{\infty}\frac{1}{n!}2^n x^{n+2} \\
&= \frac{1}{4}\sum_{i=2}^{\infty}\frac{1}{(i-2)!}2^{i-2}x^i \\
&= \frac{1}{4}\sum_{i=2}^{\infty}\frac{1}{(i-2)!}\cdot\frac{i(i-1)}{i(i-1)}\frac{2^i}{4}x^i \\
&= \frac{1}{16}\sum_{i=2}^{\infty}\frac{i(i-1)}{i!}2^i x^i
\end{aligned}$$

and using the index shift $j = n + 4$

$$\begin{aligned}
h(x) &= \frac{1}{2} \cdot \frac{x^4}{4!} \sum_{n=0}^{\infty} \frac{1}{n!} 2^n x^n \\
&= \frac{1}{48} \sum_{n=0}^{\infty} \frac{1}{n!} 2^n x^{n+4} \\
&= \frac{1}{48} \sum_{j=4}^{\infty} \frac{1}{(j-4)!} 2^{j-4} x^j \\
&= \frac{1}{48} \sum_{j=4}^{\infty} \frac{1}{(j-4)!} \cdot \frac{j(j-1)(j-2)(j-3)}{j(j-1)(j-2)(j-3)} \frac{2^j}{16} x^j \\
&= \frac{1}{768} \sum_{j=4}^{\infty} \frac{j(j-1)(j-2)(j-3)}{j!} 2^j x^j
\end{aligned}$$

changing i, j back to n and plugging $g(x), h(x)$ again into the equation for $\hat{A}(z)$ gives

$$\hat{A}(z) = \frac{1}{2} \cdot \frac{x^2}{2!} + \frac{1}{2} \cdot \frac{x^4}{4!} + \sum_{n=2}^{\infty} \frac{1}{16} 2^n n(n-1) \frac{x^n}{n!} + \sum_{n=4}^{\infty} \frac{1}{768} 2^n n(n-1)(n-2)(n-3) \frac{x^n}{n!}$$

By inserting n we can calculate some coefficients and get the identities

$$\sum_{n=2}^{\infty} \frac{1}{16} 2^n n(n-1) \frac{x^n}{n!} = \sum_{n=5}^{\infty} \left(\frac{1}{16} 2^n n(n-1) \frac{x^n}{n!} \right) + \frac{1}{2} \frac{x^2}{2!} + 3 \frac{x^3}{3!} + 12 \frac{x^4}{4!}$$

and

$$\sum_{n=4}^{\infty} \frac{1}{768} 2^n n(n-1)(n-2)(n-3) \frac{x^n}{n!} = \sum_{n=5}^{\infty} \left(\frac{1}{768} 2^n n(n-1)(n-2)(n-3) \frac{x^n}{n!} \right) + \frac{1}{2} \frac{x^4}{4!}$$

and by the addition law for EGF to

$$\hat{A}(z) = \frac{x^2}{2!} + 3 \frac{x^3}{3!} + 13 \frac{x^4}{4!} + \sum_{n=5}^{\infty} 2^n n(n-1) \left(\frac{1}{16} + \frac{1}{768} (n-2)(n-3) \right) \frac{x^n}{n!}$$

Hence

$$a_n = \begin{cases} 1, & n = 2 \\ 3, & n = 3 \\ 13, & n = 4 \\ 2^n n(n-1) \left(\frac{1}{16} + \frac{1}{768} (n-2)(n-3) \right), & n \geqslant 5. \end{cases}$$

Exercise 62

$M = \{1, 2, \ldots, n\}$ with the permutations form the symmetric group S_n.

Let T_n denote the number of solutions of $\pi \circ \pi = id_M$ in S_n, the symmetric group of degree n.

Lemma:

$$T_n = T_{n-1} + (n-1)T_{n-2} \tag{4}$$

Proof: Recall that the order of an element a of a group is the smallest positive integer m such that $a^m = id$. Recall that a transposition is an exchange of two elements while the others remain fixed. Recall that transpositions π, ϕ are disjoint if the elements that are moved by π are disjoint to those moved by ϕ.

The only, elements of order two in S_n are those which are the product of disjoint transpositions, and the identity element. The number of elements of order two which can be obtained from the permutations of the digits $1, 2, \ldots, n-1$ alone are T_{n-1}. The only other such elements are obtained from involving the digit n in a transposition with some other digit and multiplying by any other permutation of order two involving the remaining $n-2$ digits. Their number is $(n-1)T_{n-2}$. Thus the proof is complete and we obtain recurrence 4.

Example: Let $M = \{1, 2\}$.

$f = (12)$	$f(1) = 1$	$f(2) = 2$	$f^2(1) = 1$	$f^2(2) = 2$
$g = (21)$	$g(1) = 2$	$g(1) = 1$	$g(g(1)) = 1$	$g(g(2)) = 2$

We see that f^2, g^2 are just the identity permutation id. Let now $M' = \{1, 2, 3\}$. We now have to multiply transpositions involving 3 and some other digit by any other permutation of the remaining $3-2$ digits. There are exactly $(3-1) \cdot 1$ possibilities: $(31)(11)$ and $(32)(11)$. Therefore $T_2 = 4$. Let now $M'' = \{1, 2, 3, 4\}$. We now have to multiply transpositions involving 4 and some other digit by any other permutation of the remaining $4-2$ digits. There are exactly $(4-1) \cdot 4$ possibilities: $(41)(22)$, $(41)(33)$, $(41)(23)$, $(41)(32)$ and $(42)(11)$, $(42)(33)$, $(42)(13)$, $(42)(31)$ and $(43)(11)$, $(43)(22)$, $(43)(12)$, $(43)(21)$. Therefore, $T_3 = 10$.

Substitute $T_n = n!a_n$ in recurrence 4. The substitution gives

$$\begin{aligned} n!a_n &= (n-1)!a_{n-1} + (n-1)(n-2)!a_{n-2} \\ n!a_n &= (n-1)!a_{n-1} + (n-1)!a_{n-2} \\ na_n &= a_{n-1} + a_{n-2}; \quad a_0 = a_1 = 1 \end{aligned} \tag{5}$$

Consider the function $y = \sum_{i=0}^{\infty} a_i x^i$. We know from the lecture that $(a_{n-1})_{n\geq 1} \leftrightarrow xA(x)$ and $(na_n)_{n\geq 0} \leftrightarrow xA'(x)$. This yields the differential equation

$$x\, dy/dx = xy + x^2 y$$

We separate the variables, integrate both sides and use $a_0 = A = 1$.

$$\begin{aligned} x\,dy &= xy\,dx + x^2 y\,dx \\ dy/y &= dx + x\,dx \\ dy/y &= dx + x\,dx \\ dy/y &= dx(1+x) \\ \log(y) &= x + \frac{1}{2}x^2 + A' \\ y &= \exp(x + \frac{1}{2}x^2 + A') \\ y &= \exp(x + \frac{1}{2}x^2) \cdot A \\ y &= \exp(x + \frac{1}{2}x^2) \end{aligned}$$

This is OEIS A000085. These numbers are also called telephone numbers. There is a nice proof by Chowla, Herstein and Moore [1]. There is also a nice answer on Stackexchange.

Exercise 63

Wolfram Alpha

Reindex to get

$$a_{n+2} - 2(n+2)a_{n+1} + (n+2)(n+1)a_n = 2(n+2)(n+2)!$$

Multiply by $\frac{z^{n+2}}{(n+2)!}$ and sum over $n \geq 0$

$$\sum_{n\geq 0} a_{n+2}\frac{z^{n+2}}{(n+2)!} - \sum_{n\geq 0} 2(n+2)a_{n+1}\frac{zz^{n+1}}{(n+2)!} + \sum_{n\geq 0}(n+2)(n+1)a_n\frac{z^2 z^n}{(n+2)!} = \sum_{n\geq 0} 2(n+2)(n+2)!\frac{z^{n+2}}{(n+2)!}$$

Simplify and note that some parts are $\hat{A}(z) = \sum_{n\geq 0} a_n \frac{z^n}{n!}$ with some initial summands missing

$$\underbrace{\sum_{n\geq 0} a_{n+2}\frac{z^{n+2}}{(n+2)!}}_{\hat{A}(z) - a_0\frac{z^0}{0!} - a_1\frac{z^1}{1!}} - 2z\underbrace{\sum_{n\geq 0} a_{n+1}\frac{z^{n+1}}{(n+1)!}}_{\hat{A}(z) - a_0\frac{z^0}{0!}} + z^2\underbrace{\sum_{n\geq 0} a_n\frac{z^n}{n!}}_{\hat{A}(z)} = 2\underbrace{\sum_{n\geq 0}(n+2)z^{n+2}}_{\sum_{n\geq 0}(nz^n) - 0z^0 - 1z^1}$$

We know from the lecture that $(n \cdot a_n)_{n\geq 0} \leftrightarrow zA'(z)$ and we know the differentiation rule for OGF $A'(z) = \sum_{n\geq 0}(n+1)a_{n+1}z^n$ and from that we get $\sum_{n\geq 0} nz^n = z\left(\sum_{n\geq 0} z^n\right)' = z\left(\frac{1}{1-z}\right)' = \frac{z}{(1-z)^2}$.

Furthermore, we know $a_0 = a_1 = 1$ and $(z-1)^2 = (1-z)^2 = z^2 - 2z + 1$,

$$\begin{aligned}
\hat{A}(z) - 1 - z - 2z\hat{A}(z) + 2z + z^2\hat{A}(z) &= \frac{2z}{(1-z)^2} - 2z \\
\hat{A}(z)(1-z)^2 &= \frac{2z}{(1-z)^2} - 3z + 1 \\
\hat{A}(z) &= \frac{2z}{(1-z)^4} - \frac{3z}{(1-z)^2} + \frac{1}{(1-z)^2} \qquad (6)
\end{aligned}$$

using the binomial theorem $\sum_{n\geq 0}\binom{n+k-1}{k-1}z^n = \frac{1}{(1-z)^k}$, we see

$$\frac{1}{(1-z)^2} = \sum_{n\geq 0}\binom{n+1}{1}z^n = \sum_{n\geq 0}(n+1)z^n = \sum_{n\geq 0}(n+1)!\frac{z^n}{n!}$$

and (the binomial can be calculated by definition $n!/(k!(n-k)!)$)

$$\frac{1}{(1-z)^4} = \sum_{n\geq 0}\binom{n+3}{3}z^n = \sum_{n\geq 0}\frac{1}{6}(n+1)(n+2)(n+3)n!\frac{z^n}{n!}$$

Substituting

$$\hat{A}(z) = 2z\sum_{n\geq 0}\frac{1}{6}(n+1)(n+2)(n+3)n!\frac{z^n}{n!} - 3z\sum_{n\geq 0}(n+1)!\frac{z^n}{n!} + \sum_{n\geq 0}(n+1)!\frac{z^n}{n!}$$

moving the constants in, applying index multiply $zA(z) = \sum_{n\geq 0} na_{n-1}\frac{z^n}{n!}$ and applying addition rule

$$\begin{aligned}
\hat{A}(z) &= \sum_{n\geq 0}\frac{1}{3}n^2(n+1)(n+2)n!\frac{z^n}{n!} - \sum_{n\geq 0}3nn!\frac{z^n}{n!} + \sum_{n\geq 0}(n+1)!\frac{z^n}{n!} \\
&= \sum_{n\geq 0}\frac{1}{3}n^2(n+1)(n+2)n! - 3nn! + (n+1)!\frac{z^n}{n!} \\
&= \sum_{n\geq 0} n!\left(\frac{1}{3}n^2(n+1)(n+2) - 2n + 1\right)\frac{z^n}{n!}
\end{aligned}$$

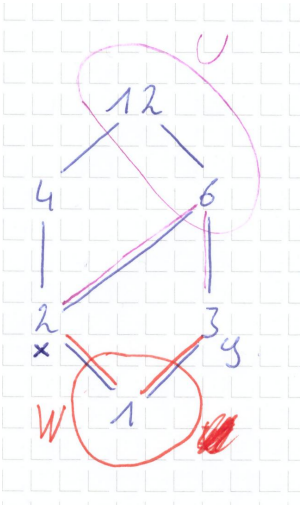
Exercise 66

We should have calculated all values, like 67.

Then $P = \{1, 2, 3, 4, 6, 12\}$.

We see that $\forall x \in P : 1 \mid x$ holds, therefore 1 is the zero-element. We see that $\forall x \in P : x \mid 12$ holds, therefore 12 is the one-element.

Recall from the lecture that $x \wedge y$ ("meet") is the unique maximal element of all common lower elements of x, y if it exists. For example, $W = \{u \in P : u \mid 2 \wedge u \mid 3\} = \{1\}$. As $|W| = 1$, 1 is unique, therefore $2 \wedge 3 = 1$. Recall from the lecture that $x \vee y$ ("join") is the unique minimal element of all common upper bounds of x, y if it exists. For example, $U = \{u \in P : 2 \mid u \wedge 3 \mid u\} = \{6, 12\}$. 6 is the unique minimal element in U, therefore $2 \vee 3 = 6$.



By exhaustively trying, we see that for all $x, y \in P$ there is $x \wedge y$ and $x \vee y$. Therefore $(P, |)$ is a lattice. We know from the lecture, that the Möbius function can be computed for lattices more easily.

> Theorem from the lecture: Suppose L is a finite lattice with 0 and 1-element. Suppose $b \in L \setminus \{1\}$. Then the Möbius function can be computed by $\mu_L(0, 1) = -\sum_{x \neq 0 \text{ and } x \wedge b = 0} \mu_L(x, 1)$

That means we have to consider only those x for which $x \wedge b$ is the zero-element. As $(P, |)$ is a finite lattice with 0 and 1-element, we can use the theorem. Let $b = 4$.

x	W	$x \wedge b$
2	1,2,4	4
3	1	1
4	1,2,4	4
6	1,2	2
12	1,2,4	4

As 1 is our zero-element and 12 our one-element, by applying the theorem we get

$$\mu(0, 1) = -\mu(3, 12) \tag{7}$$

Definition from the lecture: Let $(P, \leq)$ be a locally finite poset. Then the Möbius function $\mu : P \times P \to \mathbb{R}$ on P is defined as

$$\forall x, y \in P : \sum_{z \in [x,y]} \mu(z, y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases} \tag{8}$$

By this equation, we see that

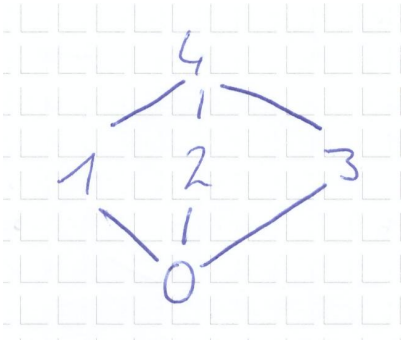
- for $x = y = 12$ we have $\mu(12, 12) = 1$
- for $x = 6, y = 12$ it holds $\mu(6, 12) + \mu(12, 12) = 0$. As we know $\mu(12, 12) = 1$, we get $\mu(6, 12) = -1$.
- for $x = 3, y = 12$ it holds $\mu(3, 12) + \mu(6, 12) + \mu(12, 12) = 0$. Therefore we get $\mu(3, 12) = 0$

By equation 7 we get our final result

$$\mu(0, 1) = 0.$$

Exercise 67

The relations yield the following Hasse diagram:



See Möbius equation 8. For all $x \in P$ holds $\mu(x, x) = 1$ by definition.
First:

- For $x = 0, y = 1$ holds $\mu(0, 1) + \mu(1, 1) = 0$. Therefore we get $\mu(0, 1) = -1$.
- For $x = 0, y = 2$ holds $\mu(0, 2) + \mu(2, 2) = 0$. Therefore we get $\mu(0, 2) = -1$.
- For $x = 0, y = 3$ holds $\mu(0, 3) + \mu(3, 3) = 0$. Therefore we get $\mu(0, 3) = -1$.

Second:

- For $x = 1, y = 4$ holds $\mu(1, 4) + \mu(4, 4) = 0$. Therefore we get $\mu(1, 4) = -1$.

- For $x = 2, y = 4$ holds $\mu(2,4) + \mu(4,4) = 0$. Therefore we get $\mu(2,4) = -1$.
- For $x = 3, y = 4$ holds $\mu(3,4) + \mu(4,4) = 0$. Therefore we get $\mu(3,4) = -1$.

Third, for $x = 0, y = 4$ holds $\mu(0,4) + \mu(1,4) + \mu(4,4) = 0$. Therefore we get $\mu(0,4) = 0$.

This is actually wrong:

Remark: The definition of the interval $[x,y] = \{z \in P : x \leq z \leq y\}$ holds also in equation 8 and allows choosing any of the elements $1, 2, 3$ to get $\mu(0,4)$. In other words, we could have also used $\mu(0,4) + \mu(2,4) + \mu(4,4) = 0$ or $\mu(0,4) + \mu(3,4) + \mu(4,4) = 0$ to get the same result.

All other x, y are not related. Consequently, $\mu(x,y) = 0$ for those.

Exercise 68

By definition an interval $[(a,x),(b,y)]$ in the partial order P is equal to the cartesian product of intervals in the first and second partial order $[a,b]_{\leq 1} \times [x,y]_{\leq 2}$.

If we can show that in the sum

$$\sum_{(z_1,z_2)\in[(a,x),(b,y)]} \mu_{P_1}(a,b) \cdot \mu_{P_2}(x,y)$$

the product $\mu_{P_1}(a,b) \cdot \mu_{P_2}(x,y)$ is 1 if and only if $(a,b) = (x,y)$ then we know that the product is the Möbius function.

Because of the first observation on cartesian product of intervals we get the identity

$$\sum_{(z_1,z_2)\in[(a,x),(b,y)]} \mu_{P_1}(z_1,x) \cdot \mu_{P_2}(z_2,y) = \sum_{z_1\in[a,b]_{\leq 1}} \mu_{P_1}(z_1,x) \cdot \sum_{z_2\in[x,y]_{\leq 2}} \mu_{P_2}(z_2,y)$$

We know that the condition 1 if and only if $x = y$ (from the Möbius equation 8) is called Kronecker delta $\delta_{x,y}$. The left and the right factor are both Möbius functions: $\delta_{a,b}$ and $\delta_{x,y}$. Therefore, the product is 1 if and only if $a = x \wedge b = y$. As a result, we get

$$\sum_{(z_1,z_2)\in[(a,x),(b,y)]} \mu_{P_1}(z_1,b) \cdot \mu_{P_2}(z_2,y) = \delta_{a,b} \cdot \delta_{x,y} = S_{(a,x),(b,y)}$$

This means that the product $\mu_{P_1}(a,b) \cdot \mu_{P_2}(x,y)$ has to be the Möbius function, which is exactly what we wanted to show.

Additionally, we show that P is indeed a partial ordered set. Using the definition $(a,x) \leq (b,y) \Leftrightarrow a \leq_1 b \wedge x \leq_2 y$, the three conditions follow directly

1. Reflexivity: We know that $\forall a \in P_1 : a \leq_1 a$ and $\forall x \in P_2 : x \leq_2 x$, therefore $\forall (a,x) \in P : (a,x) \leq (a,x)$.
2. Antisymmetry: We know that $\forall a,b \in P_1 : a \leq_1 b \wedge b \leq_1 a \implies a = b$ and $\forall x,y \in P_2 : x \leq_2 y \wedge y \leq_2 x \implies x = b$, therefore $\forall (a,x),(b,y) \in P : (a,x) \leq (b,y) \wedge (b,y) \leq (a,x) \implies (a,x) = (b,y)$

3. Transitivity: We know that $\forall a, b, c \in P_1 : a \leq_1 b \wedge b \leq_1 c \implies a \leq c$ and $\forall x, y, z \in P_2 : x \leq_2 y \wedge y \leq_2 z \implies x \leq z$, therefore $\forall (a, x), (b, y), (c, z) \in P : (a, x) \leq (b, y) \wedge (b, y) \leq (c, z) \implies (a, x) \leq (c, z)$

Therefore, (P, μ_P) is a locally finite poset with zero-element and it holds that $\mu_P((a, x), (b, y)) = \mu_{P_1}(a, b) \cdot \mu_{P_2}(x, y)$

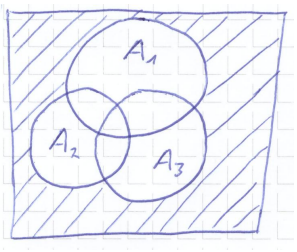
Exercise 69

Let $A_1, A_2, \ldots, A_m \subseteq M$. Say $\bar{A}_j = M \setminus A_j$. The principle of inclusion-exclusion is

$$\left| M \setminus \bigcup_{j=1}^{m} A_j \right| = \left| \bigcap_{j=1}^{m} \bar{A}_j \right| = \sum_{I \subseteq \{1,2,\ldots,m\}} (-1)^n \cdot |\cap_{i \in I} A_i| \tag{9}$$

Considering that the intersection of the empty set is the universe , we get for $m = 3$

$$\begin{aligned}
|M \setminus (A_1 \cup A_2 \cup A_3)| &= \left|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3\right| \\
&= (-1)^0 |\{\}| \\
&+ (-1)^1 |A_1| + (-1)^1 |A_2| + (-1)^1 |A_3| \\
&+ (-1)^2 |A_1 \cap A_2| + (-1)^2 |A_1 \cap A_3| + (-1)^2 |A_2 \cap A_3| \\
&+ (-1)^3 |A_1 \cap A_2 \cap A_3| \\
&= |M| \\
&- |A_1| - |A_2| - |A_3| \\
&+ |A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3| \\
&- |A_1 \cap A_2 \cap A_3|
\end{aligned}$$



We can get this by the Möbius-Inversion formula by introducing a proper partial order. We consider it to be $\left(2^{\{1,2,\ldots,m\}}, \supseteq\right)$. We now have to define a proper function. Suppose we have an element $I \subseteq \{1, 2, \ldots, m\}$ of the partial order, then we define

$$f(I) = \left| \bigcap_{i \in I} A_i \cap \bigcap_{j \notin I} \bar{A}_j \right| \tag{10}$$

For example, then $f(\{1\}) = \left|A_1 \cap \bar{A}_2 \cap \bar{A}_3\right|$ and $f(\{2,3\} = \left|\bar{A}_1 \cap A_2 \cap A_3\right|$.

We now define

$$s_f(I) = \sum_{J \supseteq I} f(I) = \left| \bigcap_{i \in I} A_i \right| \tag{11}$$

For example

$$\begin{aligned} s_f(\{1\}) &= f(\{1\}) + f(\{1,2\}) + f(\{1,3\}) + f(\{1,2,3\}) \\ &= |A_1 \cap \bar{A}_2 \cap \bar{A}_3| + |A_1 \cap A_2 \cap \bar{A}_3| + |A_1 \cap \bar{A}_2 \cap A_3| + |A_1 \cap A_2 \cap A_3| \\ &= |A_1| \end{aligned}$$

We see that in the second line A_1 is always there.

By application of the theorem of Möbius-Inversion and considering that $\mu(J,I) = (-1)^{|J|-|I|}$ we get

$$f(I) = \sum_{J \supseteq I} s_f(J) \cdot \mu(J,I) = \sum_{J \supseteq I} (-1)^{|J|-|I|} |\bigcap_{j \in J} A_j| \tag{12}$$

This gives us a very general version of the principle of Inclusion-Exclusion.

For example, using $I = \{\}$

$$f(\{\}) = \left| \bigcap_{j=1}^{n} \bar{A}_j \right| = \sum_{J \subseteq \{1,2,\ldots,m\}} (-1)^{|J|} \left| \bigcap_{j \in J} A_j \right|$$

Exercise 70

Informally

φ counts the positive integers up to a given integer n that are relatively prime to n.

$$\varphi(20) = \varphi(2^2 5) = 20(1 - \frac{1}{2})(1 - \frac{1}{5}) = 20 \cdot \frac{1}{2} \cdot \frac{4}{5} = 8$$

In words: the distinct prime factors of 20 are 2 and 5; half of the twenty integers from 1 to 20 are divisible by 2, leaving ten; a fifth of those are divisible by 5, leaving eight numbers coprime to 20; these are: 1, 3, 7, 9, 11, 13, 17, 19. More generally, this gives

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

which is known as Euler's totient function. Using $m = pqr$ yields

$$\varphi(m) = pqr \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right) \left(1 - \frac{1}{r}\right)$$

More formally

https://en.wikipedia.org/wiki/Euler%27s_totient_function#Computing_Euler's_totient_function Euler's totient function φ counts the positive integers up to a given integer n that are relatively prime to n. For $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, where $p_1, p_2, \dots, p_r$ are the distinct primes diving n the function is

$$\varphi(n) = p_1^{k_1-1}(p_1 - 1)p_2^{k_2-1}(p_2 - 2) \dots p_r^{k_r-1}(p_r - 1)$$

Remark: This is known as Euler's product formula and equivalent to the formulation in the informal argument above.

For all x in $\{p, q, r\}$ holds: x is prime. Therefore, the only factor in its factorization is x itself. As for all numbers, the prime factorization of m is unique (Fundamental theorem of arithmetic). Hence, p, q, r are the distinct primes of m and $p^1 q^1 r^1$ is the only factorization of m.

Consequently, there are

$$\varphi(m) = p^{1-1}(p-1)q^{1-1}(q-1)r^{1-1}(r-1) = (p-1)(q-1)(r-1)$$

numbers in the range $1, 2, \dots, m$ that are relatively prime to m.

Proof of the used functions

Lemma: φ is a multiplicative function. This means that if $\gcd(m, n) = 1$ then $\varphi(m)\varphi(n) = \varphi(mn)$.

Proof outline: Let A, B, C be sets of positive integers which are coprime to and less than m, n, mn, respectively, so that $|A| = \varphi(m)$ etc. Then there is a bijection between $A \times B$ and C by the Chinese remainder theorem that we saw in the lecture.

Lemma: If p is prime and $k \geq 1$, then $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

Proof: Since p is prime, the only possible values of $\gcd(p^k, m)$ are $1, p, p^2, \dots, p^k$ and the only way to have $\gcd(p^k, m) > 1$ is if m is a multiple of p, i.e. $m = p, 2p, 3p, \dots, p^{k-1} = p^k$ and there are p^{k-1} such multiples less than p^k. Therefore, other other $p^k - p^{k-1}$ numbers are all relatively prime to p^k.

Proof of Euler's product formula: By the fundamental theorem of arithmetic, if $n > 1$ then there is a unique expression $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, where $p_1 < p_2 < \dots < p_3$ are prime numbers and each $k_i \geq 1$. Using the multiplicative property of ϕ and the formula for $\phi(p^k)$ gives

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \dots \varphi(p_r^{k_r}) \\ &= p_1^{k_1-1}(p_1 - 1)p_2^{k_2-1}(p_2 - 2) \dots p_r^{k_r-1}(p_r - 1)\end{aligned}$$

Remark: We could continue this proof to show the informal formulation above

References

[1] S. Chowla, I. N. Herstein, and W. K. Moore. "On Recursions Connected With Symmetric Groups I". In: *Canadian Journal of Mathematics* 3 (1951), pp. 328–334. DOI: 10.4153/CJM-1951-038-3.