Exercise Sheet 6

Due date: 15:30, Dec 9th, to be submitted on COOL.

Working with your partner, you should try to solve all of the exercises below. You should then submit solutions to four of the problems, with each of you writing two, clearly indicating the author of each solution. Note that each problem is worth 10 points, and starred exercises represent problems that may be a little tougher, should you wish to challenge yourself. In case you have difficulties submitting on COOL, please send your solutions by e-mail.

Exercise 1 Recall that the Euler totient function $\phi(n)$ counts the numbers in $[n]$ that are relatively prime to n. Prove that $n = \sum_{d|n} \phi(d)$, where the sum is over all $d \in \mathbb{N}$ that divide n.

Solution: (張沂魁) We first claim that for a finite poset $(P, \leq)$ and $P \subseteq \mathbb{R}$, and real functions $f, g : P \to \mathbb{R}$, we have

$$g(y) = \sum_{x \leq y} f(x) \quad \forall y \in P \iff f(y) = \sum_{x \leq y} g(x)\mu(x, y) \quad \forall y \in P,$$

where μ is the mobius function, the inverse function of Zeta function. We first prove from left to right. Suppose $P = \{a_i\}_{i=1}^{n}$, and without lose of generality we can extend $\leq$ to $<$ so that $a_1 < a_2 < \cdots < a_n$. Note that if $a_i \leq a_j$ but $a_i \neq a_j$, then $a_i < a_j$. We define

$$G = \begin{pmatrix} g(a_1) \\ \vdots \\ g(a_n) \end{pmatrix}, \quad Z = (\zeta(a_i, a_j))_{n \times n} \in M_n(\mathbb{R}), \text{ and } F = \begin{pmatrix} f(a_1) \\ \vdots \\ f(a_n) \end{pmatrix},$$

and for every $y \in P$, then since we know

$$g(y) = \sum_{x \leq y} f(x) = \sum_{i=1}^{n} \zeta(a_i, y) f(a_i),$$

so we have

$$G = Z^t F.$$

Note that

$$Z = \begin{pmatrix} 1 & & & * \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix},$$

i.e. Z is upper triangular, so Z^t is lower triangular and thus invertible since $\det(Z^t) = 1$ (the product of the diagonal entries). Thus,

$$F = \left(Z^t\right)^{-1} G.$$

Note that $\zeta * \mu = \delta$, and converting this to the matrix representation we have

$$Z \cdot M_\mu = I \implies M_\mu^t \cdot Z^t = I.$$

Hence, we know $\left(Z^t\right)^{-1} = M_\mu^t$ since the inverse of a matrix is unique. Thus,

$$F = M_\mu^t G,$$

i.e.

$$f(a_i) = \sum_{k=1}^{n} \left(M_\mu^t\right)_{ik} g(a_k) = \sum_{k=1}^{n} \mu(a_k, a_i) g(a_k) = \sum_{k \leq i} \mu(a_k, a_i) g(a_k).$$

Now since this proof is invertible, so we know the if and only if statement holds. Now suppose $(P, \leq) = ([n], \cdot \mid \cdot)$, which is the division poset of $[n]$, where n is a fixed positive integer. Hence, we know

$$g(y) = \sum_{x \mid y} f(x) \quad \forall y \in [n] \iff f(y) = \sum_{x \mid y} g(x) \mu(x, y) \quad \forall y \in [n].$$

Note that for every fixed x, the construction of μ is

$$\mu(x, x) = 1, \quad \mu(x, y) = -\sum_{x \mid z \mid y, x \neq z} \mu(z, y) \text{ for } x \mid y, x \neq y.$$

Equivalently, we have

$$\sum_{x \mid z \mid y} \mu(z, y) = 0.$$

Thus, for every $x \mid y$, we have $\mu(x, y) = \mu\left(1, \frac{y}{x}\right)$. From now on, we refer $\mu(1, n)$ to $\mu(n)$. Thus, we have

$$\sum_{d \mid n} \mu(d) = 0, \quad \mu(1) = 1.$$

Hence, for prime n, we know

$$\mu(1) + \mu(n) = 0 \implies \mu(n) = -1.$$

Claim: $\mu\left(p^k\right) = 0$ for $k \geq 2$ and any prime p.

Proof: For $k = 2$, since

$$\mu(1) + \mu(p) + \mu\left(p^2\right) = 0,$$

and since $\mu(p) = -1$, so we're done. Now suppose for $k \leq \ell$ this is true, then since

$$0 = \sum_{d|p^{\ell+1}} \mu(d) = \mu(1) + \mu(p) + \cdots + \mu(p^\ell) + \mu\left(p^{\ell+1}\right) = \mu(1) + \mu(p) + \mu\left(p^{\ell+1}\right),$$

so we have $\mu\left(p^{\ell+1}\right) = 0$, and we're done.

Claim: If $\gcd(a,b) = 1$, then $\mu(ab) = \mu(a)\mu(b)$.

proof: We prove it by induction on ab. For $ab = 1$, then $a = 1, b = 1$, and since

$$1 = \mu(1) = \mu(1 \cdot 1) = \mu(1)^2,$$

so the base case is true. Now suppose for all $ab \leq k$ this is true. Then, for all $a'b' = k+1$ and $\gcd(a', b') = 1$, we have

$$\mu\left(a'b'\right) = - \sum_{\substack{d|a'b' \\ d \neq a'b'}} \mu(d) = - \sum_{\substack{e|a' \\ f|b' \\ ef \neq a'b'}} \mu(ef) = - \sum_{\substack{e|a' \\ f|b' \\ ef \neq a'b'}} \mu(e)\mu(f)$$

$$= - \sum_{e|a'} \mu(e) \sum_{\substack{f|b' \\ ef \neq a'b'}} \mu(f) = - \left(\sum_{e|a'} \mu(e) \sum_{f|b'} \mu(f) - \mu(a')\mu(b') \right)$$

$$= - \left(\sum_{ef|a'b'} \mu(e)\mu(f) - \mu(a')\mu(b') \right) = - \left(\sum_{ef|a'b'} \mu(ef) - \mu(a')\mu(b') \right)$$

$$= -(-\mu(a')\mu(b')) = \mu(a')\mu(b').$$

Hence, we can conclude that

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1; \\ (-1)^k, & \text{if } n = p_1 p_2 \ldots p_k \text{ where } p_i\text{'s are prime}; \\ 0, & \text{otherwise.} \end{cases}$$

For $n = 1$, it is trivial. As for $n = p_1 p_2 \ldots p_k$ where p_i's are all prime, since we know

$$\mu(n) = \mu(p_1)\mu(p_2) \ldots \mu(p_k) = (-1)^k,$$

so this is true. For the "otherwise" case, since we know $p^2 \mid n$ for some prime p and

$$\mu(n) = \mu\left(p^2\right) \mu\left(\frac{n}{p^2}\right) = 0 \cdot \mu\left(\frac{n}{p^2}\right) = 0,$$

so this is also true. By this, we know

$$g(y) = \sum_{x|y} f(x) \quad \forall y \in [n] \iff f(y) = \sum_{x|y} g(x)\mu\left(\frac{y}{x}\right) \quad \forall y \in [n],$$

and now we know the value of $\mu\left(\frac{y}{x}\right)$.

Now we can start to prove the problem. Suppose $s = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, where p_i's are prime, then we know

$$\phi(s) = s\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right)$$

$$= s\left(\sum_{I \subseteq [k]} \prod_{i \in I}\left(-\frac{1}{p_i}\right)\right) = s\sum_{I \subseteq [k]}(-1)^{|I|}\frac{1}{\prod_{i \in I} p_i} = s\sum_{d|s}\frac{\mu(d)}{d}$$

$$= \sum_{d|s}\frac{s}{d}\mu(d) = \sum_{e|s} e\mu\left(\frac{s}{e}\right).$$

Note that we let $e = \frac{s}{d}$ in the last step, and this statement is true for all $s \in [n]$. Now if we let $\phi = f$ and $g(x) = x$, then we know

$$g(y) = \sum_{x|y} f(x) \implies y = \sum_{x|y} \phi(x).$$

In particular, we can choose $y = n$ so that

$$n = \sum_{x|n} \phi(x),$$

and since this proof is true for all n, so we can conclude that

$$n = \sum_{d|n} \phi(d) \text{ for all } n \in \mathbb{N}.$$

Exercise 2 Recall that a chain C in a poset $(P, \leq)$ is a subset $C \subseteq P$ where every pair of elements $x, y \in C$ is comparable. Consider the infinite poset $(2^{\mathbb{N}}, \subseteq)$, where the elements are (possibly infinite) subsets of $\mathbb{N}$, ordered by inclusion.

(a) Show that this poset has a countably infinite[1] chain.

(b)* Is there an uncountable[2] chain in the poset?

---

[1]A set S is countably infinite if there is a bijection from S to $\mathbb{N}$. In other words, you can list the elements $S = \{s_1, s_2, s_3, s_4, \ldots\}$, with every element of S appearing within some finite number of terms.
[2]A set is uncountable if it is infinite, but not countably so. That is, there is no injection from S into $\mathbb{N}$.

Solution: (張沂魁)

(a) Consider
$$a_1 = \{1\}, a_{n+1} = a_n \cup \{n+1\} \text{ for all } n \geq 1,$$

so we know $C_1 = \{a_i\}_{i=1}^{\infty}$ is an infinite chain. Note that C_1 is countable since we can make a bijeciton from C_1 to $\mathbb{N}$ by f, where

$$f(a_i) = i \text{ for all } i \in \mathbb{N}.$$

(b) Since $\mathbb{Q}$ is countable, so we can enumerates $\mathbb{Q}$ as $(q_n)_{n=1}^{\infty}$. Now consider

$$S_x = \{n \in \mathbb{N} : q_n < x\} \quad \forall x \in \mathbb{R},$$

then we know

$$C_2 = \{S_x : x \in \mathbb{R}\}$$

is an infinite chain since for all $a, b \in C_2$, we know $a = S_x$ and $b = S_y$ for some $x, y \in \mathbb{R}$, and WLOG suppose $x \leq y$, then $S_x \subseteq S_y$ since $w \in S_x$ iff $q_w < x$, and this gives $q_w < x \leq y$, and thus $w \in S_y$. Hence, $a = S_x \subseteq S_y = b$. Note that there is a bijection g between C_2 and $\mathbb{R}$ by

$$g(S_x) = x \in \mathbb{R},$$

and since $\mathbb{R}$ is uncountable, so C_2 is also uncountable, and we're done.

Exercise 3 Let $n \geq 1$ be odd. For a family $\mathcal{F} \subseteq \binom{[n]}{k}$ of subsets of size k of a ground set $[n]$, we define its *shadow* $\partial \mathcal{F} = \{G \in \binom{[n]}{k-1} : \exists F \in \mathcal{F} \text{ such that } G \subset F\}$ to be the $(k-1)$-sets that are contained in some set of $\mathcal{F}$.

(a) Show that for every $\mathcal{F} \subseteq \binom{[n]}{\frac{n+1}{2}}$, we have $|\partial \mathcal{F}| \geq |\mathcal{F}|$.

(b) Prove that if $\mathcal{A} \subseteq 2^{[n]}$ is an antichain of size $\binom{n}{\frac{n+1}{2}}$ with $\mathcal{A} \notin \{\binom{[n]}{\frac{n-1}{2}}, \binom{[n]}{\frac{n+1}{2}}\}$, then there must be some non-empty $\mathcal{F} \subsetneq \binom{[n]}{\frac{n+1}{2}}$ with $|\partial \mathcal{F}| = |\mathcal{F}|$.

(c) Deduce that the only maximum antichains in $2^{[n]}$ are $\binom{[n]}{\frac{n-1}{2}}$ and $\binom{[n]}{\frac{n+1}{2}}$.

Exercise 4 Let $\mathcal{B}_n = (2^{[n]}, \subseteq)$ be the Boolean poset of all subsets of $[n]$, ordered by inclusion. A symmetric chain in $\mathcal{B}_n$ is a chain $S_k \subseteq S_{k+1} \subseteq \ldots \subseteq S_{n-k}$ such that $|S_i| = i$ for all i. Prove that for all $n \geq 1$, $\mathcal{B}_n$ can be partitioned into symmetric chains.

Solution: (黃子恆) See last few pages.

Exercise 5 A family $\mathcal{F} = \{F_1, F_2, \ldots, F_m\}$ of subsets of $[n]$ is said to be *separating* if for any two elements $1 \le i < j \le n$, there is some set $F \in \mathcal{F}$ such that $|F \cap \{i, j\}| = 1$; that is, the set F differentiates between i and j.

(a) Prove that the smallest separating family has size $\lceil \log_2 n \rceil$.

The family is said to be *strongly separating* if even more is true: for every $1 \le i < j \le n$, there are sets $F, G \in \mathcal{F}$ such that $F \cap \{i, j\} = \{i\}$ and $G \cap \{i, j\} = \{j\}$.

(b) Prove that the smallest strongly separating family has size m, where m is the smallest natural number satisfying $\binom{m}{\lceil m/2 \rceil} \ge n$.[3]

Exercise 6 Consider the poset $(P, \le)$ whose Hasse diagram is given in Figure 1.

(a) For every pair $i, j \in [6]$, determine value of the Möbius function $\mu(i, j)$.

(b) Prove that for any finite poset $(P, \le)$ and all $x, y \in P$, $\mu(x, y)$ is always an integer.
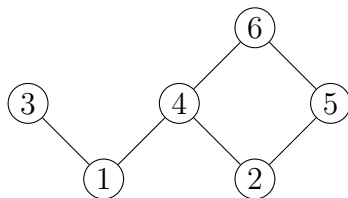

Figure 1: The Hasse diagram of a poset.

Solution: (黃子恆) See last few pages.

---

[3]When n is large, we have $m = \log_2 n + \frac{1}{2} \log_2 \log_2 n + O(1)$.

4. We'll prove it by induction.

As $n=1$, $\phi \subseteq \{1\}$ is a symmetry chain partition of B_1.

As $n=k$, say $B_k = C_1 \dot\cup C_2 \dot\cup \cdots \dot\cup C_m$, where C_i is a symmetry chain $\forall i \in [m]$. Now, as $n=k+1$, we will construct two kinds of symmetry chain.

For any $i \in [m]$, say $C_i = \{S_{i,\hat{j}}, S_{i,\hat{j}+1}, \cdots, S_{i,k-\hat{j}}\}$, where $|S_{i,\ell}| = \ell$ for all ℓ and $S_{i,\hat{j}} \subseteq S_{i,\hat{j}+1} \subseteq \cdots \subseteq S_{i,k-\hat{j}}$.

Now we start our construction.

- First kind: $C_i' = C_i \cup \{S_{i,k-\hat{j}} \cup \{k+1\}\}$.

  Since $S_{i,k-\hat{j}} \subseteq S_{i,k-\hat{j}} \cup \{k+1\}$ and $|S_{i,k-\hat{j}} \cup \{k+1\}| = (k+1) - \hat{j}$, $C_{\hat{j}}'$ is also a symmetry chain.

- Second kind: $C_i'' = \{S \cup \{k+1\} : S \in C_i \setminus \{S_{i,k-\hat{j}}\}\}$.

  Let we first assume C_i'' is nonempty (i.e. $|C_i| > 1$).

  Since $S_{i,\hat{j}} \cup \{k+1\} \subseteq S_{i,\hat{j}+1} \cup \{k+1\} \subseteq \cdots \subseteq S_{i,k-1-\hat{j}} \cup \{k+1\}$ and $|S_{i,\ell} \cup \{k+1\}| = \ell+1$ for $\ell = \hat{j}, \hat{j}+1, \cdots, k-1-\hat{j}$, C_i'' is also a symmetry chain (the size are $\hat{j}+1, \hat{j}+2, \cdots, k-\hat{j} = (k+1)-(\hat{j}+1)$).

Now, W.L.O.G, say $C_1'', C_2'', \cdots, C_r''$ are nonempty, $r \leq m$. Since $C_i \cap C_j = \phi \ \forall i,j$, by our construction, for all i,j, we have $C_i' \cap C_j' = C_i' \cap C_j'' = C_i'' \cap C_j'' = \phi$.

Also, for any $A \in B_k$, $A \in C_i$ for unique i by the induction hypothesis. For A and $A \cup \{k+1\} \in B_{k+1}$, consider our construction, if A is not the maximum element of C_i, then $A \in C_i'$ and $A \cup \{k+1\} \in C_i''$; if A is the maximum element of C_i, then $A, A \cup \{k+1\} \in C_i'$. Hence, $B_{k+1} = \left(\dot{\bigcup}_{i \in [m]} C_i'\right) \dot\cup \left(\dot{\bigcup}_{j \in [r]} C_j''\right)$.

By induction, B_n can be partitioned into symmetry chains for any positive integer n.

6. (a) Let's consider M_ζ first.

Recall that $\zeta_P(x,y) = \begin{cases} 1 & \text{if } x \leq y \\ 0 & \text{if } x \not\leq y \end{cases}$. By the Hasse

diagram, we have

$$M_\zeta = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{pmatrix} \overset{1}{1} & \overset{2}{0} & \overset{3}{1} & \overset{4}{1} & \overset{5}{0} & \overset{6}{1} \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Since $M_\zeta \times M_\mu = M_\delta = I$, by computing the inverse of M_ζ, we have

$$M_\mu = M_\zeta^{-1} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{pmatrix} \overset{1}{1} & \overset{2}{0} & \overset{3}{-1} & \overset{4}{-1} & \overset{5}{0} & \overset{6}{1} \\ 0 & 1 & 0 & -1 & -1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Hence, we have

$\mu(i,j) = 0 \quad \forall i \not\leq j$, $\mu(k,k) = 1 \quad \forall k \in [6]$,

$\mu(1,3) = \mu(1,4) = \mu(2,4) = \mu(2,5) = \mu(4,6) = \mu(5,6) = -1$,

and $\mu(1,6) = \mu(2,6) = 1$.

(b) Since M_ζ is an upper triangular matrix, its determinant is the product of its diagonal entries.

$\Rightarrow \det M_\zeta = \prod_{i \in P} \zeta(i,i) = \prod_{i \in P} 1 = 1$

$\Rightarrow M_\mu = \dfrac{1}{\det M_\zeta} \cdot \text{adj } M_\zeta = \text{adj } M_\zeta$.

Note that $(\text{adj } M_\zeta)_{ij} := (-1)^{i+j} \cdot M_{ji}$, where M_{ji} is the determinant of the $(n-1) \times (n-1)$ matrix obtained by removing the j-th row and the i-th column of M_ζ. Since the entries of M_ζ are neither 0 or 1, M_{ji} is an integer.

Hence, $M_\mu = \text{adj } M_\zeta$ are the matrix with all entries being integers. That is, $\mu(i,j) \in \mathbb{Z} \quad \forall i, j \in P$.