# Combinatorics

Lecture 4

Harbin, 2023

Let $\mu(n)$ be the **Möbius function** defined for $n \in \mathbb{N}$ by:

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & \text{if } n \text{ is not squarefree} \\ (-1)^s & \text{if } n = p_1 \cdots p_s \text{ is the product of } t \text{ distinct primes.} \end{cases}$$

Examples. $\mu(1) = 1$, $\mu(2) = -1$, $\mu(10) = 1$, $\mu(9) = 0$, $\mu(50) = 0$.

**Lemma 1.**

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1 \\ 0, & n \geq 2 \end{cases}$$

Proof. Let $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$. Then $d|n$ can be represented as

$$d = p_1^{l_1} p_2^{l_2} \dots p_s^{l_s},$$

where $0 \leq l_1 \leq k_1$, ..., $0 \leq l_s \leq k_s$.

Note that $\mu(d) = 0$, if at least one $l_i \geq 2$. Now in $\sum_{d|n} \mu(d)$ we are only interested in the terms in the expansion of which each $l_i$ equals either zero or one. Such terms are exactly $2^s$.

$$\sum_{d|n} \mu(d) = \mu(1) + s(-1) + C_s^2(-1)^2 + C_s^3(-1)^3 + \ldots + C_s^s(-1)^s$$

The sum on the right is equal to zero, whence we obtain the required assertion. ■

Definition. An arithmetic function $f$ is called multiplicative if $f(mn) = f(m)f(n)$ where $m$ and $n$ are relatively prime positive integers.

**Proposition 2.**

The function $\mu(n)$ is multiplicative.

Proof. We will prove that $\mu(mn) = \mu(m)\mu(n)$ whenever $m$ and $n$ are relatively prime numbers. First, we consider $m$ and $n$ are square-free numbers. We assume that $m = p_1 \dots p_k$, where $p_1, \dots, p_k$ are distinct primes, and $n = q_1 \dots q_s$, where $q_1, \dots, q_s$ are distinct primes. From the definition of $\mu(n)$, we write that $\mu(m) = (-1)^k$ and $\mu(n) = (-1)^s$, and $mn = p_1 \dots p_k q_1 \dots q_s$, again using the definition of $\mu(n)$, we write $\mu(mn) = (-1)^{k+s}$. Hence

$$\mu(mn) = (-1)^{k+s} = (-1)^k(-1)^s = \mu(m)\mu(n).$$

Now suppose at least one of $m$ and $n$ is divisible by a square of a prime, then $mn$ is also divisible by the square of a prime. So $\mu(mn) = 0$ and $\mu(m)$ or $\mu(n)$ is equal to zero. Now it is clear to see that the product of $\mu(m)$ and $\mu(n)$ is equal to zero. So $\mu(mn) = \mu(m)\mu(n)$ ■

**Theorem 3 (Möbius Inversion Formula).**

If $g$ is any arithmetic function and $f(n) = \sum_{d|n} g(d)$, then $g(n) = \sum_{d|n} f(d)\mu(\frac{n}{d}) = \sum_{d|n} \mu(d)f(\frac{n}{d})$

Proof. If $d|n$, we write $n = ed$, then the previous sum can be written as

$$\sum_{n=de} f(d)\mu(e)$$

and it is possible to write the last sum as,

$$\sum_{n=de} f(e)\mu(d)$$

Using equality below

$$f(\frac{n}{d}) = \sum_{e|\frac{n}{d}} g(e)$$

we write that

$$\sum_{d|n} \mu(d) f(\frac{n}{d}) = \sum_{d|n} \left(\mu(d) \sum_{e|\frac{n}{d}} g(e)\right)$$

Since $e$ divides $\frac{n}{d}$, then $e$ divides $n$. Inversely, each divisor of $n$ is $e$ which divides $\frac{n}{d}$ if and only if $d$ divides $\frac{n}{e}$. So $d$ divides $n$. As have seen, the coefficent of $g(e)$ is $\sum_{d|\frac{n}{e}} \mu(n)$ can be written as

$$\sum_{d|\frac{n}{e}} \mu(n) = \begin{cases} 1, & \frac{n}{e} = 1 \\ 0, & \frac{n}{e} > 1 \end{cases}$$

That implies $g(n)$ has only one coefficient $g(e)$ which is not equal to zero. So $g(e) = 1$. Then $g(n) = \sum_{d|n} f(\frac{n}{d})\mu(d)$ ■

## Proposition 4.

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

Proof. Note that Lemma 1 can be rewritten as $\sum_{d|n} \mu(d) = \lfloor \frac{1}{n} \rfloor$.

Then

$$\phi(n) = \sum_{k=1}^{n} \lfloor \frac{1}{gcd(n,k)} \rfloor = \sum_{k=1}^{n} \Big( \sum_{d|gcd(n,k)} \mu(d) \Big) =$$

$$= \sum_{k=1}^{n} \sum_{d|n,d|k} \mu(d) = \sum_{d|n} \sum_{q=1}^{\frac{n}{d}} \mu(d) = \sum_{d|n} \mu(d) (\sum_{q=1}^{\frac{n}{d}} 1) =$$

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

Example. Let $g(n) = 2^n$, where $n = 12$, and $f(n) = \sum_{d|n} g(d)$.
Thus $f(12) = 2 + 2^2 + 2^3 + 2^4 + 2^6 + 2^{12} = 4190$.
According to the inversion formula

$$g(12) = \mu(1)f(\frac{12}{1}) + \mu(2)f(\frac{12}{2}) + \mu(3)f(\frac{12}{3}) + \mu(4)f(\frac{12}{4}) +$$

$$+\mu(6)f(\frac{12}{6}) + \mu(12)f(\frac{12}{12}) = 4096$$

Let the set $X = \{b_1, \ldots, b_r\}$ be an alphabet, and make a directed cycle from its letters. We want to find $T_r(n)$ – number of all possible cyclic words of length $n$ composed of arbitrary letters (with repeats) from the alphabet $X$.

**Solution:** We call the period of a cyclic word $mind \geq 1$ such that after $d$ cyclic shifts by 1 symbol, the word goes into itself.

Lemma A. Any period $d$ divides $n$.

Proof. Let's assume that $n = dq + r$, where $0 < r < d$. Then we shift our word $q$ times by $d$ symbols. It has passed into itself. Now let's shift the word by $r$ symbols. Since we have shifted the word by $n$ symbols in total, it has moved into itself, which means that $r$ is the minimum number after which the word moves into itself – contradiction with the definition of a period.■

Observation. Any cyclic sequence of length $n$ and period $d$ has the form $A = a_1 \dots a_d a_1 \dots a_d a_1 \dots a_d$ , i.e. consists of $\frac{n}{d}$ repeating blocks of length $d$ — ehit follows from the previous lemma and the fact that after $d$ shifts, the letter $a_i$ goes into $a_{d+i}$.

Let $V$ be the set of all linear sequences (i.e. not cyclic) of length $n$. Let's $d_1, \dots, d_s$ are all divisors of $n$. Then $V = V_1 \bigsqcup V_2 \bigsqcup \dots \bigsqcup V_s$, where $V_i$ is the set of linear sequences with period $d_i$.

Let $W_i$ be the set of all linear sequences of length $d_i$ and period $d_i$. From the observation above $|V_i| = |W_i|$. Let $U_i$ be the set of cyclic sequences that are obtained from sequences $W_i$ by a cyclic shift. Then $d|U_i| = |W_i|$.

Next consider the function $m : \mathbb{N} \to \mathbb{N}$ given by $m(d_i) = |U_i|$. It satisfies the equality $d_i m(d_i) = |W_i|$ whence

$$r^n = \sum_{i=1}^{s} d_i m(d_i) = \sum_{d|n} dm(d)$$

Consider the functions $f(n) = r^n$, $g(n) = n \cdot m(n)$ and apply the Möbius inversion formula to them. Then

$$n \cdot m(n) = \sum_{d|n} \mu(d) r^{\frac{n}{d}} \Rightarrow m(n) = \frac{1}{n} \sum_{d|n} \mu(d) r^{\frac{n}{d}}$$

By Observation, cyclic sequences of length $n$ and period $d$ are identified with sequences of length $d$ and period $d$, and hence

$$T_r(n) = \sum_{d|n} m(d) = \sum_{d|n} \frac{1}{d} \Big( \sum_{d'|d} \mu(d') r^{\frac{d}{d'}} \Big) =$$

$$= \sum_{\substack{d|n \\ d'|d}} \frac{r^{\frac{d}{d'}} \mu(d')}{\frac{d}{d'} d'} \overset{k:=\frac{d}{d'}}{=} \sum_{d'k|n} \frac{r^k \mu(d')}{kd'} =$$

$$= \sum_{k|n} \frac{r^k}{k} \sum_{d'|\frac{n}{k}} \frac{\mu(d')}{d'} \overset{Prop.4}{=} \sum_{k|n} \frac{r^k \phi(\frac{n}{k})}{k \frac{n}{k}} = \frac{1}{n} \sum_{k|n} r^k \phi(\frac{n}{k}) \blacksquare$$

# Möbius function of a poset

Let $P$ be a poset. We define a map $\mu : P \times P \to \mathbb{Z}$ by induction.

$$\mu(x,x) = 1, \text{ for all } x \in P$$

$$\mu(x,y) = -\sum_{x \le z < y} \mu(x,z), \text{ for all } x < y \text{ in } P$$

**Proposition 5.**

Let $P$ be a finite poset. (In fact this Proposition holds in more generality but we will not need this.) Let $f, g : P \to \mathbb{C}$. Then $g(x) = \sum_{y \ge x} f(y)$ for all $x \in P$ if and only if $f(x) = \sum_{y \ge x} g(y)\mu(x,y)$ for all $x \in P$.

Proof. See Proposition 3.7.1 of R.P. Stanley, Enumerative Combinatorics, Vol 1, 2nd edition.

## Proposition 6.

Let $P$ and $Q$ be finite posets, and let $P \times Q$ be their direct product. If $(x, y) \leq (x', y')$ in $P \times Q$, then

$$\mu_{P\times Q}((x, y), (x', y')) = \mu_P(x, x')\mu_Q(y, y').$$

Proof. We have

$$\sum_{(x,y)\leq(u,v)\leq(x',y')} \mu_P(x, u)\mu_Q(y, v) = (\sum_{x\leq u\leq x'} \mu_P(x, u))(\sum_{y\leq v\leq y'} \mu_Q(y, v))$$

■

Remark (for those familiar with finite fields).
Let $\mathbb{F}_q$ denote the finite field of $q$ elements. Then in general, the number of monic irreducible polynomials of degree $n$ over the finite field $\mathbb{F}_q$ is given by Gauss's formula

$$M(q,n) := \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d$$

There is a wide generalization of polynomials of this kind - the so-called necklace polynomials, see
A.Kerber, "Algebraic Combinatorics Via Finite Group Actions" (1991)

Exercise 1. For any positive integer $n$, we let $D_n$ be the poset of all divisors of $n$. Show that for this poset $\mu(1, d) = \mu(d)$ for all $d$ dividing $n$.

Exercise 2. Let $X$ be a set with $n$ elements, and let $P = (\mathcal{P}(X), \subseteq)$. Prove that $\mu(\emptyset, S) = (-1)^k$, where $S \subseteq X$, and $|S| = k$.