

Discrete Mathematics Lecture Notes (WS18/19)

Created by Liang Chun

Lecture 1 (10.10.2018)

Prelude: Motivation

What is the aim of the lecture?

Learn basic frameworks used in all areas of mathematics:

- Mathematicians deal with statements
- Usually the statements are about numbers
- The statements may be true or false
- To decide whether a statement is true or false requires a proof
- Use this framework to acquire some knowledge about principles of counting
- Graph theory has a direct application in real world problems
- The basic knowledge about algebraic methods will be used in coding theory

Example:

1. 15 is a multiple of 3
2. 20 is a multiple of 3

Theorem: 15 is a multiple of 3

Proof: $15 = 3 * 5$

Chapter 1: Principles of Counting

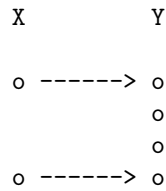
Basic Counting Problems

- Permutation: $\frac{n!}{(n-r)!}$
- Combinations: $\frac{n!}{(n-r)!r!}$

Definition 1.2.1

Remarks

Suppose that X and Y are sets. We say that we have a function/map from X to Y if for each $x \in X$ we can specify a unique element in Y , which we denote by $f(x)$.



- $f(x)$ is defined $\forall x \in X$
- these are just one such object $\forall x \in X$

Inverse Image Example

Given the function

$$f : \{1, 2, 3\}' \mapsto \{a, b, c, d\} \quad (1)$$

defined by

$$f(x) = \begin{cases} a, & \text{if } x = 1 \\ a, & \text{if } x = 2 \\ c, & \text{if } x = 3 \end{cases} \quad (2)$$

The produced map is:

$$\begin{array}{ccc}
 a & \rightarrow & 1 \\
 a & \rightarrow & 2 \\
 b & & \\
 c & \rightarrow & 3 \\
 d & &
 \end{array} \quad (3)$$

The image/inverse image of the following sets under f are:

1. set $\{2, 3\}$; image: $\{a, c\}$
2. set $\{a\}$; inverse image: $\{1, 2\}$
3. set $\{a, b\}$; inverse image: $\{1, 2\}$
4. set $\{b, d\}$; inverse image: \emptyset

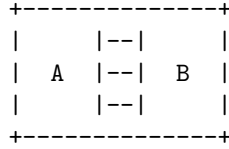
Definition 1.2.2 Cardinality

A set A is finite if a bijective mapping $A \mapsto \{1, \dots, n\}$ exists. (*This means that there is exactly n number of elements inside set A .*)

In this case n is called the **cardinality** of A and A has $|A| := n$ elements.

Two sets A, B are defined to have the same cardinality if a bijective mapping $A \mapsto B$ exists.

Not Disjoint Sets



1. $A = \{1, 2, 3, 4, 5\}, |A| = 5$
2. $B = \{3, 4, 5, 6, 7\}, |B| = 5$

$$|A \cup B| \tag{4}$$

$$= |1, 2, 3, 4, 5, 6, 7| \tag{5}$$

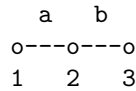
$$= 7 \tag{6}$$

$$\neq |A| + |B| \tag{7}$$

Counting Sets

1. $|X \cup Y| = |X| + |Y| - |X \cap Y|$
2. $|X \cup Y \cup Z| = |X| + |Y| + |Z| + (|X \cap Y| + |X \cap Z| + |Y \cap Z|) - |X \cap Y \cap Z|$

Double Counting Principle



1. $N = 1, 2, 3$, (nodes)
2. $E = a, b$ (edges)
3. $R =$ incidence

$$|R| \text{ (over the nodes)} \tag{8}$$

$$= |x \in E|1 \text{ is incident to } x| + |x \in E|2 \text{ is incident to } x| + |x \in E|3 \text{ is incident to } x| \tag{9}$$

$$= |a| + |a, b| + |b| \tag{10}$$

$$= 4 \tag{11}$$

$$|R| \text{ (over the edges)} \tag{12}$$

$$= |x \in N|x \text{ is incident to } a| + |x \in N|x \text{ is incident to } b| \tag{13}$$

$$= |1, 2| + |2, 3| \tag{14}$$

$$= 4 \tag{15}$$

Lecture 2 (17.10.2018)

Slide 21

Examples

- 1) The first person may choose among 100 seats, the second among 99 etc.
So we have $100 * 99 * \dots$

$$\frac{100!}{(100 - 95)!}, (n)_k \quad (16)$$

- 2) Let the pearls be enumerated by 1 to n . Then we cut the necklace at the part with number 1. So each assignment of pearls is bijectively mapped to an n -list, where the first element of the list always is the pearl with numbers 1. So there exists $(n - 1)!$ possibilities

Slide 24

Example

A card game consists of 52 cards:

- Each card has a suit out of {I, II, III, IV}
- Each card has a value out of {2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K, A}
- 2 cards form a pair, if they have the same value

How many possibilities exist so that we have among 5 arbitrary cards one pair and 3 cards with each the same value (but other than the pair)?

Solution

- 1) Choose the value of the pairs (13 possibilities)
- 2) Choose the value of the three cards (12 possibilities)
- 3) Choose the suit of the pair ($4C2 = 6$ possibilities)
- 4) Choose the suit of the other three cards ($4C3 = 4$ possibilities)

Therefore, we need the product rule:

$$p = 13 * 12 * C(4, 2) * C(4, 3) \quad (17)$$

$$= 3744 \quad (18)$$

Slide 28

$$C(n, m_1) * C(n - m_1, m_2) * \dots * C(m_k, m_k) \quad (19)$$

$$= \frac{n!}{(n - m_1)!m_1!} * \frac{(n - m_1)!}{(n - m_1 - m_2)!m_2!} * \dots * \frac{m_k!}{m_k!(m_k - m_k!)} \quad (20)$$

$$= \frac{n!}{m_1! * \dots * m_k!} \quad (21)$$

Lecture 3 (24.10.2018)

Slide 35

The Stirling numbers $s_{n,k}$ of first order is the number of permutation of a n -set with exactly k cycles

Theorem 1.8.4

$S(n, 1) = 1, S(n, n) = 1$ denotes from set n , choosing 1 partition or n partitions results in only one element

Slide 39

Let f, g be the permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \quad (22)$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 1 \end{pmatrix} \quad (23)$$

then

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 3 & 2 \end{pmatrix} \quad (24)$$

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \quad (25)$$

This example shows that in general the composition of permutation is not commutative since a permutation is bijective, also the inverse function is a permutation.

Let f be

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \quad (26)$$

First we invert, then we order the first row

$$f^{-1} = \begin{pmatrix} 2 & 1 & 4 & 5 & 3 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix} \quad (27)$$

$$f \circ f^{-1} = id, f^{-1} \circ f = id \quad (28)$$

Slide 41

Example

Let f be

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 8 & 1 & 5 & 9 & 3 & 7 & 6 \end{pmatrix} \quad (29)$$

We take the cycles without repetition:

- i. 1: $1 \mapsto 2 \mapsto 4 \mapsto 1$. The cycle is $(1, 2, 4)$
- ii. 3: $3 \mapsto 8 \mapsto 7 \mapsto 3$. The cycle is $(3, 8, 7)$
- iii. 5: $5 \mapsto 5$. The cycle is (5)
- iv. 6: $6 \mapsto 9 \mapsto 6$. The cycle is $(6, 9)$

The cycle representation of f is:

$$f = (1, 2, 4) \circ (3, 8, 7) \circ (5) \circ (6, 9) \quad (30)$$

Slide 42

Let f be the permutation which describes the change of sorting:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 5 & 9 & 2 & 6 & 10 & 3 & 7 & 11 & 4 & 8 & 12 \end{pmatrix} \quad (31)$$

$$= (2, 5, 6, 10, 4) \circ (3, 9, 11, 8, 7) \text{ (starting the cycle at 2)} \quad (32)$$

Since the two cycles have length 5, the cards are back to its original position after 5 procedures.

Slide 42

Let f be a composition of transpositions:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad (33)$$

$$= (1, 2, 3, 4) \quad (34)$$

$$= (1, 4) \circ (1, 3) \circ (1, 2) \quad (35)$$

But also adding $(3, 4)$ and $(4, 3)$ doesn't change the identity:

$$f = (1, 4) \circ (4, 3) \circ (3, 4) \circ (1, 3) \circ (1, 2) \quad (36)$$

Slide 43

Further Remarks

Generalization of polynomials, where the number of terms is allowed to be infinite. The solution of a combinatorial problem can often be expressed as a sequence u_n . In such cases it is often appropriate to use methods based on the representation of u_n as a power series:

$$U(x) = u_0 + u_1x + u_2x^2 + \dots \quad (37)$$

where $U(x)$ is called the generating function for the sequence u_n

Slide 47

Taylor Series

The n-th Taylor polynomial is defined as:

$$T_n f(x, a) = \sum_{k=0}^n \frac{f^{(k)}(a)}{k!} (x - a)^k \quad (38)$$

$$= f(a) + f'(a)(x - a) + \frac{f''(a)}{2}(x - a)^2 + \dots \quad (39)$$

In the special case where $a = 0$, then the Taylor series is called McLaurin series.

$$f(x) = (1 + x)^n \quad (40)$$

$$\Rightarrow f^{(k)}(x) \quad (41)$$

$$= (n(1 + x)^{n-1})^{(k-1)} \quad (42)$$

$$= (n(n-1)(1 + x)^{n-2})^{(k-2)} * \dots \quad (43)$$

$$= n(n-1) * (n(1 + x)^{n-1})^{(k-1)} * \dots \quad (44)$$

$$\Rightarrow f^{(k)}(0) = n(n-1)(n-2) * \dots * (n - (k-1)) \quad (45)$$

This is to compute the sequence of coefficients from the generating function. The other way round, given a sequence and then compute the function is easy: sequence

$$\langle f_0, f_1, \dots \rangle = F(x) = f_0x^0 + f_1x^1 + f_2x^2 + \dots \quad (46)$$

$$F(x) = (1 + x)^n = \binom{n}{0} + (n, 1)x + (n, 2)x^2 + \dots \quad (47)$$

can be regarded as saying the the generating function for the sequence defined by $u_n = (n, k)$ for any given integer n is $F(x) = (1 + x)^n$

Slide 48

Convolution definition

$$c_k = a_0 b_k + a_1 b_{k-1} + \dots + a_k b_0 \quad (48)$$

\

Example

Given

$$f(x) = 2 + 3x - 4x^2 \quad (49)$$

$$g(x) = 5 - x + x^3 \quad (50)$$

$$c_0 = a_0 b_0 = 2 * 5 = 10 \quad (51)$$

$$c_1 = a_0 b_1 + a_1 b_0 = (2 * -1) + (3 * 5) = 13 \quad (52)$$

$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 = (2 * 0) + (3 * -1) + (-4 * 5) = -23 \quad (53)$$

$$f(x) * g(x) = c_0 + c_1 x^1 + c_2 x^2 + \dots \quad (54)$$

Slide 50

Example

Geometrical Series

$$(1 - x) \sum_{k=0}^{\infty} x^k \quad (55)$$

$$= \sum_{k=0}^{\infty} x^k - \sum_{k=0}^{\infty} x^{k+1} \quad (56)$$

$$= 1 + \sum_{k=1}^{\infty} x^k - \sum_{k=1}^{\infty} x^k = 1 \quad (57)$$

So $(1 - x)$ is inverse to the geometrical series and we get $\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}$