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 descide 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

Supose 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 $f(x)$.

```
X           Y

o ------> o
          o
          o
o ------> o
```

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

Inverse Image Example

Given the function

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

defined by

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

The produced map is:

$$\begin{array}{ccc} \text{a} & \rightarrow & 1 \\ \text{a} & \rightarrow & 2 \\ \text{b} & & \\ \text{c} & \rightarrow & 3 \\ \text{d} & & \end{array} \tag{3}$$

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 $A \mapsto \{1, ..., n\}$ exists. *(This means that there a 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

```
+--------------+
|     |--|     |
|  A  |--|  B  |
|     |--|     |
+--------------+
```

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

```
  a   b
o---o---o
1   2   3
```

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 $100 * 99 * ...$

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

2) Let the perls be enumerated by 1 to 1. 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 these exists $(n-1)!$ possibilities

Slide 24

Example

A card game consists of 52 cards:

- Each car 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 exists 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:

$$\begin{aligned} p &= 13 * 12 * C(4,2) * C(4,3) && (17) \\ &= 3744 && (18) \end{aligned}$$

Slide 28

$$C(n, m_1) * C(n - m_1, m_2) * ... * C(m_k, m_k) \tag{19}$$

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

$$= \frac{n!}{m_1! * ... * m_k!} \tag{21}$$

Lecture 3 (24.10.2018)

Slide 35

The Stirling numbers$_{n,k}$ of first orders it 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

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

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

then

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

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

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

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

First we invert, then we order the first row

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

$$f \circ f^{-1} = id, f^{-1} \circ f = id \tag{28}$$

Slide 41

Example

Let f be

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

We take the cycles without repitition:

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:

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

Slide 42

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

$$\begin{aligned} f &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 5 & 9 & 2 & 6 & 10 & 3 & 7 & 11 & 4 & 8 & 12 \end{pmatrix} && (31) \\ &= (2, 5, 6, 10, 4) \circ (3, 9, 11, 8, 7) \ \textit{(starting the cycle at 2)} && (32) \end{aligned}$$

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:

$$\begin{aligned} f &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} && (33) \\ &= (1, 2, 3, 4) && (34) \\ &= (1, 4) \circ (1, 3) \circ (1, 2) && (35) \end{aligned}$$

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

$$f = (1, 4) \circ (4, 3) \circ (3, 4) \circ (1, 3) \circ (1, 2) \tag{36}$$

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:

$$U(x) = u_0 + u_1 x + u_2 x^2 + ... \tag{37}$$

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:

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

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

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

$$\begin{aligned}
f(x) &= (1+x)^n && (40)\\
&\Rightarrow f^{(k)}(x) && (41)\\
&= (n(1+x)^{n-1})^{(k-1)} && (42)\\
&= (n(n-1)(1+x)^{n-2})^{(k-2)} * ... && (43)\\
&= n(n-1) * (n(1+x)^{n-1})^{(k-1)} * ... && (44)\\
&\Rightarrow f^{(k)}(0) = n(n-1)(n-2) * ... * (n-(k-1)) && (45)
\end{aligned}$$

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

$$\langle f_0, f_1, ... \rangle = F(x) = f_0 x^0 + f_1 x^1 + f_2 x^2 + ... \tag{46}$$

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

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

$$c_k = a_0 b_k + a_1 b_{k-1} + ... + a_k b_0 \tag{48}$$

Example

Given

$$f(x) = 2 + 3x - 4x^2 \tag{49}$$

$$g(x) = 5 - x + x^3 \tag{50}$$

$$c_0 = a_0 b_0 = 2 * 5 = 10 \tag{51}$$

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

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

$$f(x) * g(x) = c_0 + c_1 x^1 + c_2 x^2 + ... \tag{54}$$

Slide 50

Example

Geometrical Series

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

$$= \sum_{k=0}^{\infty} x^k - \sum_{k=0}^{\infty} x^{k+1} \tag{56}$$

$$= 1 + \sum_{k=1}^{\infty} x^k - \sum_{k=1}^{\infty} x^k = 1 \tag{57}$$

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

Here are some more generating functions:

$$\sum_{k=0}^{\infty}(-1)^k x^k \tag{58}$$
$$= 1 - x + x^2 - x^3 + ... \tag{59}$$
$$\widehat{=}(1, -1, 1, -1, ...) \tag{60}$$

$$\sum_{k=0}^{\infty} x^2 k \tag{61}$$
$$= 1 + x^2 + x^4 + x^6 + ... \tag{62}$$
$$\widehat{=}(1, 0, 1, 0, 1, ...) \tag{63}$$

Slide 52

$$F_n = F_{n-1} + F_{n-2} \tag{64}$$

The above equation is a homogeneous (no constants) linear recursion equation of second order (going back 2 steps)

Slide 53

Example: Fibonacci Numbers

The main idea now is to expand the right series as a formal power series. To do this we factorize the denominator. We put:

$$1 - x - x^2 = (1 - ax)(1 - bx) \tag{65}$$

If we substitute $x = \frac{1}{y}$, equation (2) is equivalent to

$$1 - \frac{1}{y} - \frac{1}{y^2} = (1 - \frac{a}{y})(1 - \frac{b}{y}) \tag{66}$$
$$\Leftrightarrow y^2 - y - 1 \tag{67}$$
$$= (y - a)(y - b) \tag{68}$$

$$y_{1,2} = \frac{1}{2} + \sqrt{\frac{1}{4} + 1} \tag{69}$$
$$= \frac{1}{2} + \frac{\sqrt{5}}{2} \tag{70}$$

The zeroes of $y^2 - y - 1$ are:

$$a = \frac{1}{2} + \frac{\sqrt{5}}{2}, \quad b = \frac{1}{2} - \frac{\sqrt{5}}{2} \tag{71}$$

Now we decompose into partial fractions

$$\frac{1+x}{1-x-x^2} = \frac{\alpha}{(1-ax)} + \frac{\beta}{(1-bx)} \tag{72}$$

$$\begin{aligned}
1 + x &= \alpha(1-bx) + \beta(1-ax) && (73)\\
1 + x &= \alpha + \beta + (-\alpha b - \beta a)x && (74)\\
&\Rightarrow \alpha + \beta = 1, \quad -\alpha b - \beta a = 1 && (75)\\
&\Rightarrow \alpha = \frac{1+a}{-b+a} = \frac{1+a}{\sqrt{5}}, \quad \beta = 1 - \frac{1+a}{\sqrt{5}} = -\frac{1+b}{\sqrt{5}} && (76)
\end{aligned}$$

Each summand from the right hand side is now expanded by the sum rule for the geomtrical series:

$$\begin{aligned}
\Rightarrow \frac{1+x}{1-x-x^2} &= \frac{1+a}{\sqrt{5}(1-ax)} - \frac{1+b}{\sqrt{5}(1-bx)} && (77)\\
&= \frac{1+a}{\sqrt{5}} \sum_{k=0}^{\infty} a^k x^k - \frac{1+b}{\sqrt{5}} \sum_{k=0}^{\infty} b^k x^k && (78)\\
&= \sum_{k=0}^{\infty} \left[\frac{1+a}{\sqrt{5}} a^k - \frac{1+b}{\sqrt{5}} b^k \right] x^k && (79)\\
&\Rightarrow F_k = \frac{a^{k+2}}{\sqrt{5}} - \frac{b^{k+2}}{\sqrt{5}} \quad (1 + a = a^2, 1 + b = b^2) && (80)
\end{aligned}$$

We can then compute the specific numbers k in F_k:

$$\begin{aligned}
F_2 &= \frac{(\frac{1}{2} + \frac{\sqrt{5}}{2})^4}{\sqrt{5}} - \frac{(\frac{1}{2} + \frac{\sqrt{5}}{2})^4}{\sqrt{5}} && (81)\\
&= 3 && (82)
\end{aligned}$$

Slide 54

Special case: Fibonacci numbers

$$F_n = F_{n-1} + F_{n-2} \tag{83}$$

So we have $k = 0$, $h_k = 0$, $\beta_1 = -1$, $\beta_2 = -1$, $\beta_j = 0$ for $3 \leq j \leq n$

Slide 55

Remark on the proof 1.10.5

$$p_{n+k} = \sum_{j=0}^{n} a_{n+k-j}\beta_j = 0, \quad \forall k \geq 0 \tag{84}$$

$$\begin{aligned}
A(x) &= a_0 + a_1 x + a_2 x^2 + ... && (85)\\
A(x) &= \sum_{j=0}^{n} \beta_j x^j && (86)\\
&= a_0\beta_0 x^0 + (a_0\beta_1 + a_1\beta_0)x^1 + (a_0\beta_2 + a_1\beta_1 + a_2\beta_0)x^2 + ... && (87)\\
&= \underbrace{(a_0\beta_n + a_1\beta_{n-1} + ... + a_n\beta_0)}_{= 0 \text{ due to recursion formula}} x^n && (88)
\end{aligned}$$

At first we substitute in the equation $1 + \beta_1 x + \beta_2 x^2 + ... = 0$

After multiplication by y^n we get the auxiliary equation:

$$y^n + \beta_1 y^{n-1} + ... + \beta_n = 0 \tag{89}$$

According to the fundemental theorem of algebra, there exists numbers:

$$y_1, ..., y_5 \in \mathbb{C} \tag{90}$$

such that:

$$y^n + \beta_1 y^{n-1} + ... + \beta_n = (y - y_1)^{m_1}(y - y_2)^{m_2} \dot{...} (y - y_5)^{m_5} \tag{91}$$

and

$$\sum_{j=0}^{5} m_j = n \tag{92}$$

By back substituting, we have:

$$\begin{aligned}
1 + \beta_1 x + \beta_2 x^2 + ... + \beta_n x^n &= x^n (y^n + \beta_1 y^{n-1} + ... + \beta n) && (93)\\
&= x^n (y - y_1)^{m_1}(y - y_2)^{m_2}...(y - y_5)^{m_5} && (94)\\
&= x^n (\frac{1}{x} - y_1)^{m_1}(\frac{1}{x} - y_2)^{m_2}...(\frac{1}{x} - y_5)^{m_5} && (95)\\
&= (1 - y_1 x)^{m_1}(1 - y_2 x)^{m_2}...(1 - y_5)^{m_5} && (96)
\end{aligned}$$

So:

$$A(x) = \frac{P(x)}{(1-y_1x)^{m_1}(1-y_2x)^{m_2}...(1-y_5)^{m_5}} \tag{97}$$

According to the theorem of partial fraction decomposition, it holds:

$$A(x) = \sum_{k=1}^{5} \frac{H_k(x)}{(1-y_kx)^{m_k}} \tag{98}$$

with polynomial H_k and $deg(H_k) < m_k$.

Futhermore for each summand holds (omitting index k) due to partial fraction decomposition:

$$\frac{H(x)}{(1-\beta x)^m} = \sum_{j=1}^{m} \frac{\gamma_j}{(1-\beta x)^j}, \quad \gamma_j \in \mathbb{R} \tag{99}$$

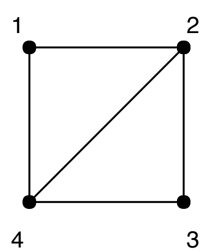
Each summand on the right hand sind can now be expanded by means of the geometrical series into a power series.

Slide 57

TBD

Slide 66

Example double counting principle



v\E	{1, 2}	{1, 4}	{4, 3}	{3, 2}	{4, 2}	countSum
1	x	x				2
2	x			x	x	3
3			x	x		2
4		x	x		x	3
	2	2	2	2	2	10

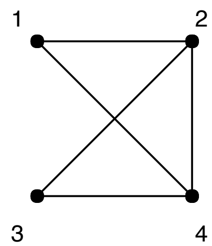
Slide 67

Remark to proof 2.1.4

$|V_0|$ has to be even because:

t	even	odd
even	even	odd
odd	odd	even

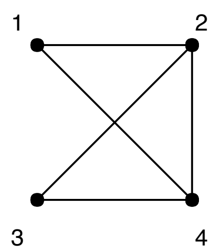
Slide 69



1	2	3	4
2	1	2	1
4	3	4	2
	4		3

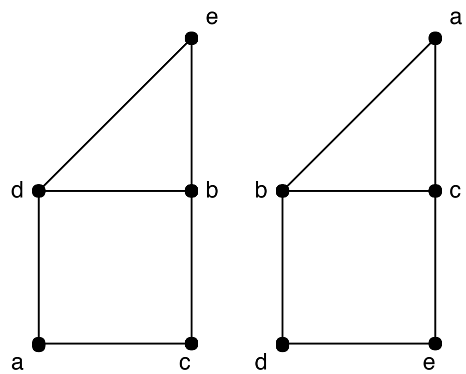
Slide 70

Example adjacency matrix



$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \tag{100}$$

Another adjacency matrix



A1 A2

$$A_1 = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix} \tag{101}$$

$$A_2 = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \tag{102}$$

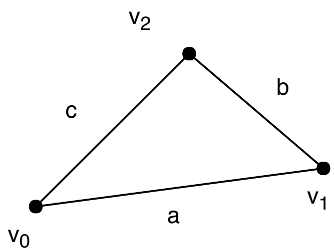
Slide 77

Remarks to the Proof 2.3.3 (No. 2)

- Here we have the case $\{u, v\} \in E$. So $\{3, 2\} \in E, G' = (V', E')$, $V' = V \cup \{a\}$, $E' = E \cup \{\{2, a\}, \{3, a\}\}$ and a closed Euler line is $(1, 2, a, 3, 4, 2, 3, 1)$
- Here we have the case $\{u, v\} \notin E$. So $\{1, 3\} \notin E$, $G' = (V, E')$, $E' = E \cup \{\{1, 3\}\}$ and a closed Euler line is $(1, 3, 5, 4, 3, 2, 1)$

Slide 78

Example



a. $w = v_0, \quad F = E = \{a, b, c\}$
b. $deg(v_0, F) = 2 \quad \Rightarrow v_1$ with $\{v_0, v_1\} \in F, W = (v_0, v_1), F = \{b, c\}$
c. $deg(v_1, F) = 1 \quad \Rightarrow v_2$ with $\{v_2, v_1\} \in F, W = (v_0, v_1, v_2), F = \{c\}$
d. $deg(v_2, F) = 1 \quad \Rightarrow v_0$ with $\{v_2, v_0\} \in F, W = (v_0, v_1, v_2, v_0), F = \emptyset$
e. $deg(v_0, F) = 0 \quad \Rightarrow$ STOP