在线授课签到方法

1. 在线授课每次都要记录出席情况。
2. 助教在课程进行过程中随机选择一个时刻确定当次课出勤情况
3. 参会人员命名格式：姓名＋学号；非此格式有可能导致无出勤记录，当次出勤分数为0。
4. 若网络存在严重故障，请提前联系TA，否则由此导致无出勤记录的，当次出勤分数为0。
5. 若网络存在临时故障导致掉线，记录下掉线的时间，当天中午12:30前提交给TA。TA与其选定的时刻对照，如相符则进行补充登记。掉线次数理论上不应超过3次，每次不超过3分钟。对于每次课出勤结果，TA择时公布。

其他注意事项

1. 上课期间注意保持安静，麦克风静音，不得人为制造噪音。
2. 助教负责记录，违者当次课出勤分数为0；多次违反，整个学期出勤分数为0。
3. 关于课程内容的问题可在聊天区发表，助教全程记录留言内容，可随时回答问题。
4. 此区域不可发表与课程无关的内容，否则当次课出勤分数为0;多次发表与课程无关内容，整个学期出勤分数为0。

Discrete Mathematics
Lecture 9

Liangfeng Zhang
School of Information Science and Technology
ShanghaiTech University

Summary of Lecture 8

Order of a group G: the number of elements in G

Order of an element $a \in G$: the least $l > 0$ such that $a^l = 1$

- $a^{|G|} = 1$ for all $a \in G$
  - Euler's theorem, Fermat's little theorem

Subgroup: $H \subseteq G$ + $(H, \star)$ is also a group ($H \leq G$)

- $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$ is a subgroup of G for all $g \in G$
- Cyclic group: $G = \langle g \rangle$ for some $g \in G$

Discrete Logarithm: $G = \langle g \rangle = \{g^0. g^1, \ldots, g^{q-1}\}$

- $\forall h \in G, \exists x \in \{0,1, \ldots, q-1\}$ such that $h = g^x$
- Denote $x = \log_g h$
- DLOG problem: $(q, G, g, h) \rightarrow x$
- CDH problem: $\left(q, G, g, g^a, g^b\right) \rightarrow g^{ab}$

Diffie-Hellman Key Exchange

The Scheme: $G = \langle g \rangle$ is a cyclic group of prime order q

- Alice: $a \leftarrow \mathbb{Z}_q, A = g^a$; send (q, G, g, A) to Bob
- Bob: $b \leftarrow \mathbb{Z}_q, B = g^b$; send B to Alice; output $k = A^b$
- Alice: output $k = B^a$

Alice

Bob

(q, G, g)

$a \leftarrow \mathbb{Z}_q$

$A = g^a$

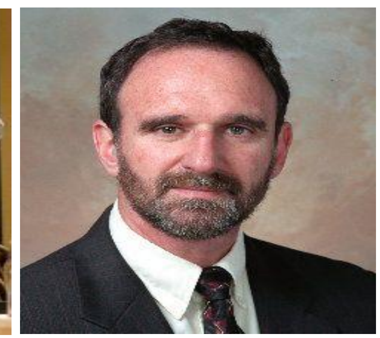
$\xrightarrow{(q, G, g, A)}$

$b \leftarrow \mathbb{Z}_q$

$B = g^b$

$\xleftarrow{B}$

output B^a | output A^b



Whitfield Diffie, Martin E. Hellman:
New directions in Cryptography,
IEEE Trans. Info. Theory, 1976
Turing Award 2015

Correctness: $A^b = g^{ab} = B^a$

Wiretapper: view $= (q, G, g, A, B)$

Security: view $\nrightarrow$ g^{ab}

Combinatorics

counting 计数

Enumerative combinatorics

- permutations, combinations, partitions of integers, generating functions, combinatorial identities, inequalities ......

Designs and configurations

区组 拉丁方 正交正列

- block designs, triple systems, Latin squares, orthogonal arrays, configurations, packing, covering, tiling ......

Graph theory 图论

$G=(V,E)$ 边集 顶点集

- graphs, trees, planarity, coloring, paths, cycles, ...

极值组合学

Extremal combinatorics

- extremal set theory, probabilistic method......

Algebraic combinatorics

- symmetric functions, group, algebra, representation, group actions......

Sets and Functions

DEFINITION: A **set** is an unordered collection of **elements**

- $a \in A$; $a \notin A$); roster method 列举法, set builder 描述法; empty set $\emptyset$, universal set
- $A = B$; $A \subseteq B$; $A \subset B$; $A \cup B$; $A \cap B$; $\bar{A}$

DEFINITION: Let $A, B \neq \emptyset$ be two sets. A **function (map)**

$f: A \to B$ assigns a unique element $b \in B$ for all $a \in A$.

- **injective**单射: $f(a) = f(b) \Rightarrow a = b$
- **surjective**满射: $f(A) = B$
- **bijective**双射: injective and surjective

Cardinality of Sets

DEFINITION: Let A be a set. A is a **finite set** if it has finitely many elements; Otherwise, A is an **infinite set**.

- The **cardinality**基数 $|A|$ of a finite set A is the number of elements in A.

EXAMPLE: $\emptyset, \{1\}, \{x: x^2 - 2x - 3 = 0\}, \{a, b, c, \dots, z\}$ are all finite sets; $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all infinite sets

DEFINITION: Let A, B be any sets. We say that A, B **have the same cardinality**等势 ($|A| = |B|$) if there is a bijection $f: A \to B$

- We say that $|A| \leq |B|$ if there exists an injection $f: A \to B$.
  - If $|A| \leq |B|$ and $|A| \neq |B|$, we say that $|A| < |B|$

THEOREM: Let A, B, C be any sets. Then

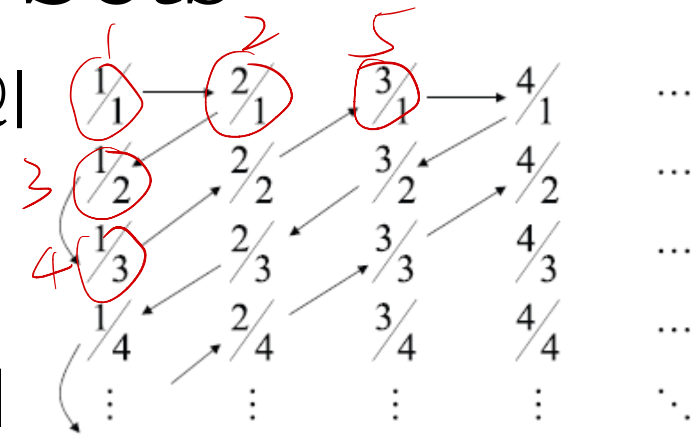
- $|A| = |A|$
- $|A| = |B| \Rightarrow |B| = |A|$
- $|A| = |B| \wedge |B| = |C| \Rightarrow |A| = |C|$

$f: A \to B$, $g: B \to C$

$h: A \to C$ $h(a) = g(f(a))$

Cardinality of Sets

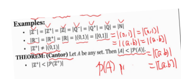
EXAMPLE: $|\mathbb{Z}^+| = |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}^+| = |\mathbb{Q}|$



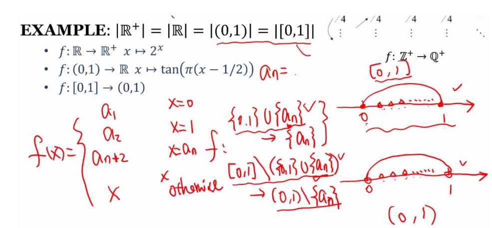
- $f: \mathbb{Z}^+ \to \mathbb{N} \quad x \mapsto x - 1$
- $f: \mathbb{Z} \to \mathbb{N} \quad f(x) = \begin{cases} 2x & x \geq 0 \\ -(2x+1) & x < 0 \end{cases}$

$f: \mathbb{Z}^+ \to \mathbb{Q}^+$

EXAMPLE: $|\mathbb{R}^+| = |\mathbb{R}| = |(0,1)| = |[0,1]|$



- $f: \mathbb{R} \to \mathbb{R}^+ \quad x \mapsto 2^x$
- $f: (0,1) \to \mathbb{R} \quad x \mapsto \tan\big(\pi(x - 1/2)\big)$
- $f: [0,1] \to (0,1)$
  - $f(1) = 2^{-1}, f(0) = 2^{-2}, f(2^{-n}) = 2^{-n-2}, n = 1,2,3,\ldots$
  - $f(x) = x$ for all other x



EXAMPLE: $|2^X| = |\mathcal{P}(X)|$

- $2^X = \{\alpha \mid \alpha: X \to \{0,1\}\}$ the set of all functions from X to $\{0,1\}$
- $\mathcal{P}(X) = \{A \mid A \subseteq X\}$: the power set of X X的幂集
- $f: 2^X \to \mathcal{P}(X) \quad \alpha \mapsto A = \{x: \alpha(x) = 1\}$

Cardinality of Sets

THEOREM: $|(0,1)| \neq |\mathbb{Z}^+|$

- Suppose that $|(0,1)| = |\mathbb{Z}^+|$. Then there is a bijection $f: \mathbb{Z}^+ \to (0,1)$

$$f(1) = 0.b_{11}b_{12}b_{13}b_{14}b_{15}b_{16}b_{17}b_{18}b_{19}\cdots$$
$$f(2) = 0.b_{21}b_{22}b_{23}b_{24}b_{25}b_{26}b_{27}b_{28}b_{29}\cdots$$
$$f(3) = 0.b_{31}b_{32}b_{33}b_{34}b_{35}b_{36}b_{37}b_{38}b_{39}\cdots$$
$$f(4) = 0.b_{41}b_{42}b_{43}b_{44}b_{45}b_{46}b_{47}b_{48}b_{49}\cdots$$
$$f(5) = 0.b_{51}b_{52}b_{53}b_{54}b_{55}b_{56}b_{57}b_{58}b_{59}\cdots$$
$$f(6) = 0.b_{61}b_{62}b_{63}b_{64}b_{65}b_{66}b_{67}b_{68}b_{69}\cdots$$
$$\cdots$$
$$f(n) = 0.b_{n1}b_{n2}b_{n3}b_{n4}b_{n5}b_{n6}b_{n7}b_{n8}b_{n9}\cdots$$
$$\cdots$$

- Let $b_i = \begin{cases} 4, & b_{ii} \neq 4 \\ 5, & b_{ii} = 4 \end{cases}$ for $i = 1,2,3,\ldots$ $b_i \neq b_{ii}$ $\to b \neq f(i)$ 原像.
- $b = 0.b_1b_2b_3b_4b_5b_6b_7b_8b_9\cdots$ is in $(0,1)$ but has no preimage
  - $b \neq f(i)$ for every $i = 1,2,\ldots$
- f cannot be a bijection

康拓对角线法

Cantor's Diagonal Argument

Question: Show that $|A| \neq |\mathbb{Z}^+|$.

The Diagonal Argument:

1) Suppose that $|A| = |\mathbb{Z}^+|$. Then there is a bijection $f\colon \mathbb{Z}^+ \to A$
2) Represent the function f as a list:

$$
\begin{array}{c|l}
f(1) & a_1 \cdots\cdots\cdots\cdots \\
f(2) & a_2 \cdots\cdots\cdots\cdots \\
\vdots & \quad\vdots \\
f(i) & a_i \cdots\cdots\cdots\cdots \\
 & \qquad\qquad\qquad x \\
\vdots & \quad\vdots
\end{array}
$$

- Every element of $\mathbb{Z}^+$ appears once in the left-hand side
- Every element of A appears once in the right-hand side

3) Construct an element x by considering the diagonal of the list
4) Show that $x \neq a_i$ for all $i \in \mathbb{Z}^+$
5) Show that $x \in A$
6) 4) and 5) give a contradiction

Cantor's Theorem

THEOREM: (Cantor) Let A be any set. Then $|A| < |\mathcal{P}(A)|$.

- $|A| \leq |\mathcal{P}(A)|$
  - The function $f: A \to \mathcal{P}(A)$ defined by $f(a) = \{a\}$ is injective.
- $|A| \neq |\mathcal{P}(A)|$
  - Assume that there is a bijection $g: A \to \mathcal{P}(A)$
  - Define $X = \{a: a \in A \text{ and } a \notin g(a)\}$
  - ***X* should appear in the list**. It is clear that $X \subseteq A$ and hence $X \in \mathcal{P}(A)$
  - ***X* will not appear in the list**. Suppose that $X = g(x)$ for some $x \in A$
    - If $x \in X$, then $x \notin g(x) = X$
      - This gives a contradiction
    - If $x \notin X$, then $x \in g(x) = X$
      - This gives a contradiction

The Halting Problem

$$\mathbf{HALT}(P, I) = \begin{cases} \text{"halts"} & \text{if } P(I) \text{ halts;} \\ \text{"loops forever"} & \text{if } P(I) \text{ loops forever.} \end{cases}$$

- P: a program; I: an input to the program P.

QUESTION: Is there a Turing machine **HALT**?

- Turing machine: can be represented as a an element of $\{0,1\}^*$
  - $\{0,1\}^* = \cup_{n \geq 0} \{0,1\}^n$: the set of all finite bit strings

THEOREM: There is no Turing machine **HALT**.

- Assume there is a Turing machine **HALT**
- Define a new Turing machine $\mathbf{Turing}(P)$ that runs on any Turing machine P
  - **If** $\mathbf{HALT}(P, P) =$ "halts“, loops forever
  - **If** $\mathbf{HALT}(P, P) =$ "loops forever“, halts
- $\mathbf{Turing}(\mathbf{Turing})$ loops forever$\Rightarrow$ $\mathbf{HALT}(\mathbf{Turing}, \mathbf{Turing}) =$ "halts"$\Rightarrow$**Turing(Turing) halts**
- $\mathbf{Turing}(\mathbf{Turing})$ halts $\Rightarrow$ $\mathbf{HALT}(\mathbf{Turing}, \mathbf{Turing}) =$ "loops forever"$\Rightarrow$**Turing(Turing)** loops forever

Countable and Uncountable

DEFINITION: A set A is **countable**可数，可列 if $|A| < \infty$ or $|A| = |\mathbb{Z}^+|$;
otherwise, it is said to be **uncountable**不可数，不可列.

- countably infinite: $|A| = |\mathbb{Z}^+|$

可列无穷集合

EXAMPLE:

可列集的笛卡尔积还是可列集

- $\mathbb{Z}^-, \mathbb{Z}^+, \mathbb{Z}, \mathbb{Q}^-, \mathbb{Q}^+, \mathbb{Q}, \mathbb{N}, \mathbb{N} \times \mathbb{N}$, are countable
- $\mathbb{R}^-, \mathbb{R}^+, \mathbb{R}, (0,1), [0,1], (0,1], [0,1), (a, b), [a, b]$ are uncountable

THEOREM: A set A is countably infinite iff its elements can be arranged as a sequence $a_1, a_2, \ldots$

$\Leftrightarrow$

- If A is countably infinite, then there is a bijection $f\colon \mathbb{Z}^+ \to A$
- If $A = \{a_1, a_2, \ldots\}$, then the $f\colon \mathbb{Z}^+ \to A$ defined by $f(i) = a_i$ is a bijection
  - $a_i = f(i)$ for every $i = 1,2,3 \ldots$

Countable and Uncountable

THEOREM: Let A be countably infinite, then any infinite subset $X \subseteq A$ is countable.

- Let $A = \{a_1, a_2, \dots\}$. Then $X = \{a_{i_1}, a_{i_2}, \dots\}$ X is countable

THEOREM: Let A be uncountable, then any set $X \supseteq A$ is uncountable.

- If X is countable, then A is finite or countably infinite

THEOREM: If A, B are countably infinite, then so is $A \cup B$

- $A = \{a_1, a_2, a_3, \dots\}, B = \{b_1, b_2, b_3, \dots\}$
- $A \cup B = \{a_1, b_1, a_2, b_2, a_3, b_3, \dots\}$ //no elements will be included twice
  - application: the set of irrational numbers is uncountable

THEOREM: If A, B are countably infinite, then so is $A \times B$

- $A = \{a_1, a_2, a_3, \dots\}, B = \{b_1, b_2, b_3, \dots\}$
- $A \times B = \{(a_1, b_1), (a_1, b_2), (a_2, b_1), (a_1, b_3), (a_2, b_2), (a_3, b_1), (a_1, b_4), \dots\}$

Schröder-Bernstein Theorem

QUESTION: How to compare the cardinality of sets in general?

- $|\mathbb{Z}^-| = |\mathbb{Z}^+| = |\mathbb{Z}| = |\mathbb{Q}^-| = |\mathbb{Q}^+| = |\mathbb{Q}| = |\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$
- $|\mathbb{R}^-| = |\mathbb{R}^+| = |\mathbb{R}| = |(0,1)| = |[0,1]| = |(0,1]| = |[0,1)|$
- $|\mathbb{Z}^+| \neq |(0,1)|$: hence, $|\mathbb{Z}^+| \neq |\mathbb{R}|$, and in fact $|\mathbb{Z}^+| < |\mathbb{R}|$
- $|\mathbb{Z}^+| < |\mathcal{P}(\mathbb{Z}^+)|$
- $|\mathbb{R}|?\ |\mathcal{P}(\mathbb{Z}^+)|$: which set has more elements?

THEOREM: If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

EXAMPLE: Show that $|(0,1)| = |[0,1)|$

- $|(0,1)| \leq |[0,1)|$
  - $f: (0,1) \to [0,1)\ \ x \to \frac{x}{2}$ is injective
- $|[0,1)| \leq |(0,1)|$
  - $g: [0,1) \to (0,1)\ \ x \to \frac{x}{4} + \frac{1}{2}$ is injective

Schröder-Bernstein Theorem

EXAMPLE: $|\mathcal{P}(\mathbb{Z}^+)| = |[0,1)| = (|\mathbb{R}|)$

- $|\mathcal{P}(\mathbb{Z}^+)| \leq |[0,1)|$
  - $f: \mathcal{P}(\mathbb{Z}^+) \to [0,1) \quad \{a_1, a_2, \dots\} \mapsto 0.\cdots 1_{a_1} \cdots 1_{a_2} \cdots$ is an injection.
- $|[0,1)| \leq |\mathcal{P}(\mathbb{Z}^+)|$
  - $\forall x \in [0,1), x = 0.r_1 r_2 \cdots \ \left(r_1, r_2, \cdots \in \{0, \dots, 9\}, \text{no } \dot{9}\right)$
    - $0 \leftrightarrow 0000, 1 \leftrightarrow 0001, \dots, 9 \leftrightarrow 1001$
    - x has a binary representation $x = 0.b_1 b_2 \cdots$
      - $f: [0,1) \to \mathcal{P}(\mathbb{Z}^+) \ \ x \mapsto \{i: i \in \mathbb{Z}^+ \wedge b_i = 1\}$ is an injection

THEOREM: $|\mathbb{Z}^+| < |\mathcal{P}(\mathbb{Z}^+)| = |[0,1)| = |(0,1)| = |\mathbb{R}|$

阿列夫0 $\aleph_0$ $2^{\aleph_0}$ c

The continuum hypothesis连续统$\boxed{\text{假设}}$**:** There is no cardinal number between $\aleph_0$ and c, i.e., there is no set A such that $\aleph_0 < |A| < c$.

$|\mathbb{R}|$
$||$
$|\mathbb{Z}^+| < |P(\mathbb{Z}^+)| < |P(P(\mathbb{Z}^+))| \cdots$

Parenthesization

加括号

PROBLEM: Let $a_1, a_2, \dots, a_n, a_{n+1}$ be $n+1$ numbers. Let $*$ be any binary operator. Let C_n be the number of different ways of parenthesizing

$$a_1 * a_2 * \cdots * a_n * a_{n+1}$$

such that the calculation is not ambiguous. What is C_n?

- $n = 4$: there are 5 different ways
  - $((a_1 * a_2) * a_3) * a_4$
  - $(a_1 * a_2) * (a_3 * a_4)$
  - $(a_1 * (a_2 * a_3)) * a_4$
  - $a_1 * ((a_2 * a_3) * a_4)$
  - $a_1 * (a_2 * (a_3 * a_4))$
- $n = 100$?

Combinatorial Counting Techniques Required

Basic Rules of Counting

DEFINITION: Let A be a finite set. A **partition**划分 of set A is a family $\{A_1, A_2, \dots, A_k\}$ of nonempty subsets of A such that $\neq \phi$

- $\bigcup_{i=1}^{k} A_i = A$ and
- $A_i \cap A_j = \emptyset$ for all $i, j \in [k]$ with $i \neq j$.

The Sum Rule加法原则: Let A be a finite set. Let $\{A_1, A_2, \dots, A_k\}$ be a partition of A. Then $|A| = |A_1| + |A_2| + \cdots + |A_k|$.

- Suppose that a task can be done in one of n_1 ways, in one of n_2 ways, . . . , or in one of n_k ways, where none of the set of n_i ways of doing the task is the same as any of the set of n_j ways, for all pairs i and j with $1 \leq i < j \leq k$. Then the number of ways to do the task is $n_1 + n_2 + \cdots + n_k$.

Basic Rules of Counting

The Product Rule乘法原则: Let $A_1, A_2, \dots, A_k$ be finite sets. Then

$$|A_1 \times A_2 \times \cdots \times A_k| = |A_1| \times |A_2| \times \cdots \times |A_k|. \ (*)$$

- Suppose that a procedure is carried out by performing the tasks $T_1, T_2, \dots, T_k$ in sequence. If each task T_i $(i = 1,2, \dots, k)$ can be done in n_i ways, regardless of how the previous tasks were done, then there are $n_1 n_2 \cdots n_k$ ways to carry out the procedure.

EXAMPLE: # of composite divisors of $N = 2^{100} \times 3^{200} \times 5^{1000}$.

- $A = \{n \in \mathbb{Z}^+ : n|N\}$; $|A| = 101 \times 201 \times 1001$ //product rule $n = 2^a 3^b 5^c$
- $A_1 = \{n \in A : n \text{ is prime}\}$; $A_2 = \{n \in A : n \text{ is composite}\}$; $A_3 = \{1\}$
  - $\{A_1, A_2, A_3\}$ is a partition of A.
  - $|A| = |A_1| + |A_2| + |A_3| \Rightarrow |A_2| = |A| - |A_1| - |A_3|$
  - $|A_1| = 3, |A_3| = 1; |A_2| = 101 \times 201 \times 1001 - 3 - 1 = 20321297.$

The Bijection Rule一一对应原则、相等原则: Let A and B be two finite sets. If there is a bijection $f: A \to B$, then $|A| = |B|$.

Permutations of Set

DEFINITION: Let A be a finite set of n elements. Let $r \in [n]$.

- **r-permutation** of A: a sequence $a_1, a_2, \cdots, a_r$ of r distinct elements of A.
  - An n-permutation of A is simply called a **permutation** of A
    - Example: $A = \{1,2,3\}$
      - 2-Permutations of A: 1,2; 1,3; 2,1; 2,3; 3,1; 3,2
  - $P(n, r)$: the number of different r-permutations of an n-element set

THEOREM: $P(n, r) = n!/(n-r)!$ for all $n \in \mathbb{Z}^+$ and $r \in [n]$.

DEFINITION: Let A be a finite set of n elements.

- **r-permutation** of A **with repetition**: a sequence $a_1, a_2, \cdots, a_r$ of r elements of A.

  2可重复排列
  - Example: $A = \{1,2,3\}$; 2-Permutations of A with repetition:
    - 1,1; 1,2; 1,3; 2,1; 2,2; 2,3; 3,1; 3,2; 3,3

THEOREM: An n-element set has n^r different r-permutations with repetition.

Multiset

可重

DEFINITION: A **multiset**多重集 is a collection of elements which are not necessarily different from each other.

- An element $x \in A$ has **multiplicity**重数 m if it appears m times in A.
- A multiset A is called an ***n*-multiset***n*-多重集 if it has n elements.
- $A = \{n_1 \cdot a_1, n_2 \cdot a_2, \ldots, n_k \cdot a_k\}$: an $(n_1 + n_2 + \cdots + n_k)$-multiset where the elements $a_1, a_2, \ldots, a_k$ has multiplicities $n_1, n_2, \ldots, n_k$, respectively.
- $T = \{t_1 \cdot a_1, t_2 \cdot a_2, \ldots, t_k \cdot a_k\}$ is called an ***r*-subset** of A if
  - $0 \leq t_i \leq n_i$ for every $i \in [k]$, and　　r-子集
  - $t_1 + t_2 + \cdots + t_k = r$

EXAMPLE: $A = \{1 \cdot \mathrm{a}, 2 \cdot \mathrm{b}, 3 \cdot \mathrm{c}, 100 \cdot \mathrm{z}\}, T = \{1 \cdot \mathrm{b}, 98 \cdot \mathrm{z}\}$

- A is a 106-multiset; the multiplicities of a, b, c, z are 1,2,3,100, resp.
- T is a 99-subset of A

Permutations of Multiset

DEFINITION: Let $A = \{n_1 \cdot a_1, \dots, n_k \cdot a_k\}$ be an n-multiset.

- **permutation of** A: a sequence $x_1, x_2, \cdots, x_n$ of n elements, where a_i appears exactly n_i times for every $i \in [k]$.
- r**-permutation of** A: a permutation of some r-subset of A
  - $A = \{1 \cdot \mathrm{a}, 2 \cdot \mathrm{b}, 3 \cdot \mathrm{c}\}$ r排列 A的r子集的排列
  - a, b, c, b, c, c is a permutation of A; bcb is a 3-permutation of A;
  - bcb is a permutation of the subset $\{2 \cdot \mathrm{b}, 1 \cdot \mathrm{c}\}$

REMARK: Let $A = \{a_1, a_2, \dots, a_n\}$ be a set of n elements.

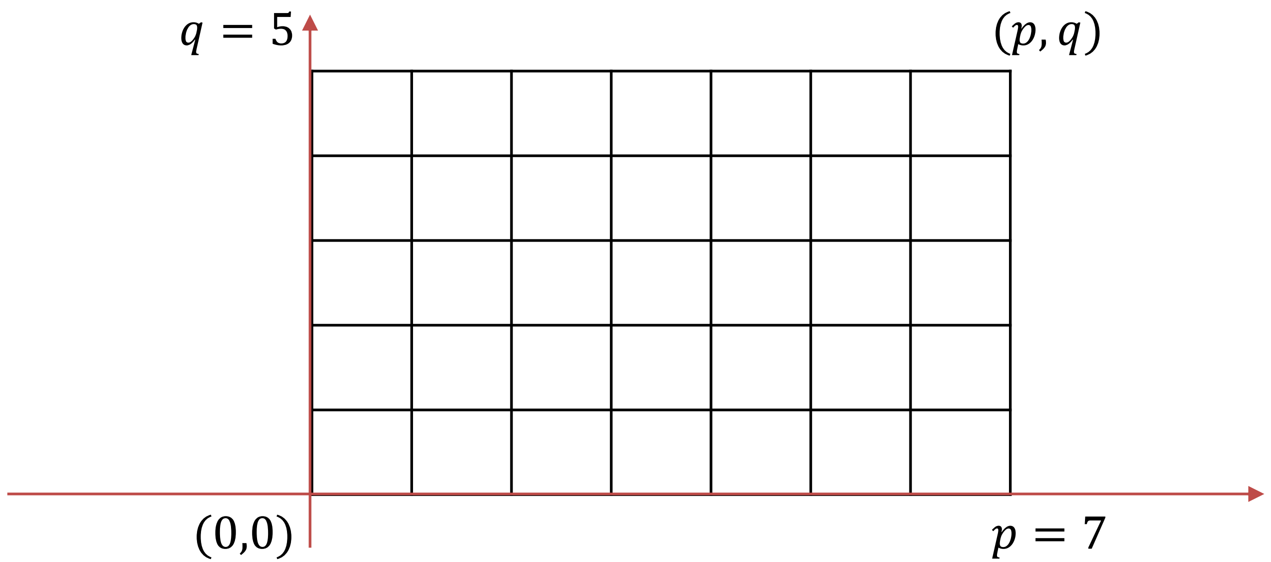
- For every $r \in [n]$, an r-permutation of A without repetition is an r-permutation of $\{1 \cdot a_1, 1 \cdot a_2, \dots, 1 \cdot a_n\}$.
- For every $r \geq 1$, an $r-$permutation of A with repetition is an $r-$permutation of $\{\infty \cdot a_1, \infty \cdot a_2, \dots, \infty \cdot a_n\}$.

THEOREM: Let $A = \{n_1 \cdot a_1, n_2 \cdot a_2, \dots, n_k \cdot a_k\}$ be a multiset.

Then A has exactly $\frac{(n_1+n_2+\cdots+n_k)!}{n_1!n_2!\cdots n_k!}$ permutations.

Shortest Path

DEFINITION: A $\boldsymbol{p \times q}$**-grid** is a collection of pq squares of side length 1, organized as a rectangle of side length p and q.



THEOREM: # of shortest paths from (0,0) to (p, q) is $\frac{(p+q)!}{p!q!}$.

- Let $A = \{p \cdot \rightarrow, q \cdot \uparrow\}$ be a $(p + q)$-multiset.
- # of shortest paths=# of permutations of A.