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: $(q, G, g, h) \to x$
- CDH problem: $\left(q, G, g, g^a, g^b\right) \to g^{ab}$

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)

$a \leftarrow \mathbb{Z}_q$

$A = g^a$

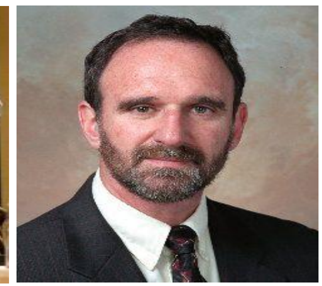
$\xrightarrow{(q, G, g, A)}$

$b \leftarrow \mathbb{Z}_q$

$B = g^b$

$\xleftarrow{B}$

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

Enumerative combinatorics

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

Designs and configurations

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

Graph theory

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

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, set builder; empty set $\emptyset$, universal set
- $A = B$; $A \subseteq B$; $A \subset B$; $A \cup B$; $A \cap B$; $\bar{A}$ 补集

全集

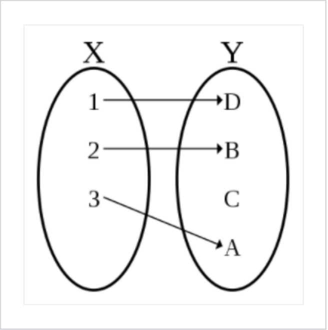
DEFINITION: Let $A, B \neq \emptyset$ be two sets. A **function (map)**

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

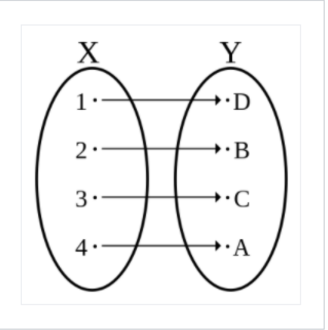
- **injective**单射: $f(a) = f(b) \Rightarrow a = b$
- **surjective**满射: $f(A) = B$
- **bijective**双射: injective and surjective

只有一个 $a \in A$，使……

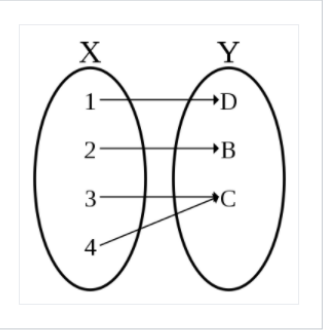
一一对应



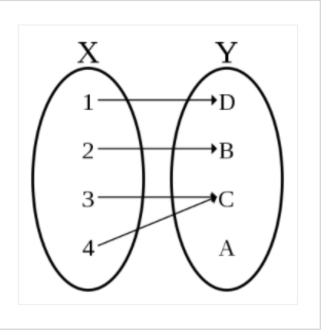
An injective non-surjective function (injection, not a bijection)



An injective surjective function (**bijection**)



A non-injective surjective function (surjection, not a bijection)



A non-injective non-surjective function (also not a bijection)

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: $\emptyset, \{1\}, \{x: x^2 - 2x - 3 = 0\}, \{a, b, c, \ldots, z\}$ 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

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

$\exists f(a) = f(b)$

$a \neq b$

来

数轴

Cardinality of Sets

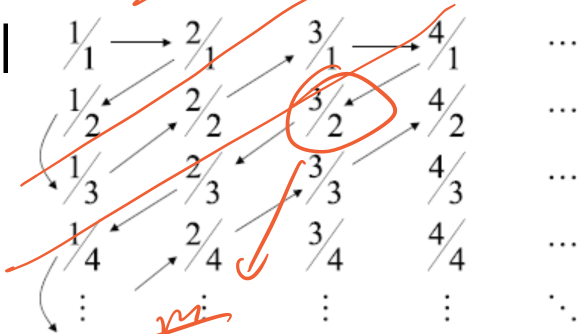
Z_2 Z_3 ...

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

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

Q

20 21



$\frac{m}{n}$

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

表示 all $\frac{n}{m}$

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

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

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

- $2^X = \{\alpha | \alpha: X \to \{0,1\}\}$ the set of all functions from X to $\{0,1\}$

Q

- $\mathcal{P}(X) = \{A | A \subseteq X\}$: the power set of X
- $f: 2^X \to \mathcal{P}(X) \quad \alpha \mapsto A = \{x: \alpha(x) = 1\}$

P: Power set = { all Sub set of A }

[illegible]onilaztion

diag

Cardinality of Sets

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

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

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

保证 $b'_i \neq b_{ii}$

- Let $b_i = \begin{cases} 4, & b_{ii} \neq 4 \\ 5, & b_{ii} = 4 \end{cases}$ for $i = 1,2,3,\ldots$

降乱

- $b = 0.b_1b_2b_3b_4b_5b_6b_7b_8b_9\cdots$ is in $(0,1)$ but has no preimage
  - $b \neq f(i)$ for every $i = 1,2,\ldots$
- f cannot be a bijection

Cantor's Diagonal Argument

是个集合

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

The Diagonal Argument:

离 连

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:

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

- 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

x是构造出来的

Cantor's Theorem

$\mathcal{P}$

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

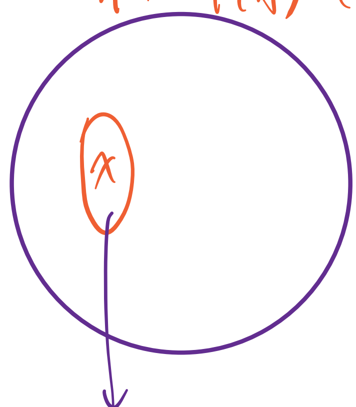
- $|A| \le |\mathcal{P}(A)|$ "$f(a) = f(b)$ $a = b$."
  - The function $f: A \to \mathcal{P}(A)$ defined by $f(a) = \{a\}$ is injective.
- $|A| \neq |\mathcal{P}(A)|$ since 满射.
  - Assume that there is a bijection $g: A \to \mathcal{P}(A)$
  - Define $X = \{a: a \in A \text{ and } a \notin g(a)\}$ "All the" 子集集
  - ***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

A, $P(A)$ (满射

X's

by def

$a = g(a')$



$a' \in X$

$a' \notin X$

$a' \notin \{g(a')\} = X$

$a \in g(x) = X$.

are some $g(a')$

$(a' \in \neg X)$

$\neg X := \{a : a \in A,\ a \in g(a)\}.$

The Halting Problem

breaks.

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

- 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**.

can compute

- Assume there is a Turing machine **HALT**

assumed machine

- Define a new Turing machine **Turing**(P) that runs on any Turing machine P
  - **If HALT**(P, P) = "halts“, loops forever
  - **If HALT**(P, P) = "loops forever“, halts
- **Turing**(**Turing**) loops forever⇒ **HALT**(**Turing**, **Turing**) = "halts"⇒**Turing(Turing) halts**
- **Turing**(**Turing**) halts ⇒ **HALT**(**Turing**, **Turing**) = "loops forever"⇒**Turing(Turing)** loops forever

Proof concept [edit]

Christopher Strachey outlined a proof by contradiction that the halting problem is not solvable.[26][27] The proof proceeds as follows: Suppose that there exists a total computable function *halts(f)* that returns true if the subroutine *f* halts (when run with no inputs) and returns false otherwise. Now consider the following subroutine:

```
def g():
    if halts(g):
        loop_forever()
```

halts(g) must either return true or false, because *halts* was assumed to be total. If *halts(g)* returns true, then *g* will call *loop_forever* and never halt, which is a contradiction. If *halts(g)* returns false, then *g* will halt, because it will not call *loop_forever* this is also a contradiction. Overall, *g* does the opposite of what *halts* says *g* should do, so *halts(g)* can

For example, in pseudocode, the program

```
while (true) continue
```

does not halt; rather, it goes on forever in an infinite loop. On the other hand, the program

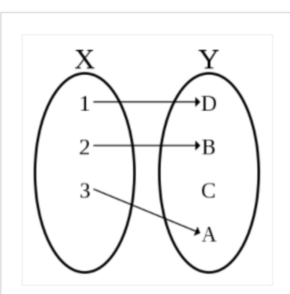
```
print "Hello, world!"
```

does halt.

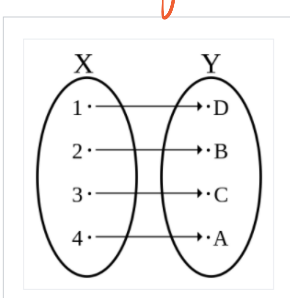
While deciding whether these programs halt is simple, more complex programs prove problematic. One approach to the problem might be to run the program for some number of steps and check if it halts. But if the program does not halt, it is unknown whether the program will eventually halt or run forever. Turing proved no algorithm exists that always correctly decides whether, for a given arbitrary program and input, the program halts when run with that input. The essence of Turing's proof is that any such algorithm can be made to contradict itself and therefore cannot be correct.

injection: 单　　surjection: 满

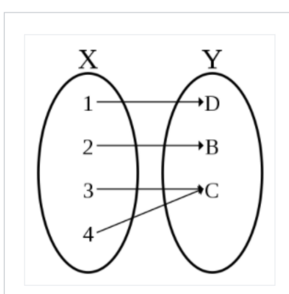
bijection: 双



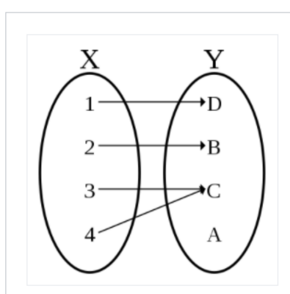
An injective non-surjective function (injection, not a bijection)



An injective surjective function (**bijection**)



A non-injective surjective function (surjection, not a bijection)



A non-injective non-surjective function (also not a bijection)

Countable and Uncountable

可列的

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

EXAMPLE:

- $\mathbb{Z}^-, \mathbb{Z}^+, \mathbb{Z}, \mathbb{Q}^-, \mathbb{Q}^+, \mathbb{Q}, \mathbb{N}, \mathbb{N} \times \mathbb{N}$, 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 $a_1, a_2, \ldots$

- 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 $i = 1,2,3 \ldots$

sign for all type jections

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?

∃ bijection

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

意为: ∃ injection

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

- $|(0,1)| \leq |[0,1)|$ $\quad x \to x$ 也可
  - $f: (0,1) \to [0,1)$ $\; x \to \frac{x}{2}$ is injective

单

$a = b$

$f(a) = f(b)$

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

trick

Schröder-Bernstein Theorem

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

- $|\mathcal{P}(\mathbb{Z}^+)| \le |[0,1)|$ $X \subseteq \mathbb{Z}^+$ ，位第a_i个为1，剩下为0.
  - $f: \mathcal{P}(\mathbb{Z}^+) \to [0,1)$ $\{a_1, a_2, \ldots\} \mapsto 0.\cdots 1_{a_1} \cdots 1_{a_2} \cdots$ is an injection.
- $|[0,1)| \le |\mathcal{P}(\mathbb{Z}^+)|$
  - $\forall x \in [0,1), x = 0.r_1 r_2 \cdots$ $(r_1, r_2, \cdots \in \{0, \ldots, 9\}, \text{no } \dot{9})$
    - $0 \leftrightarrow 0000, 1 \leftrightarrow 0001, \ldots, 9 \leftrightarrow 1001$ 二进制小数
    - x has a $\boxed{\text{binary}}$ representation $x = 0.b_1 b_2 \cdots$ 取所有1位值$\{b_i\}$
      - $f: [0,1) \to \mathcal{P}(\mathbb{Z}^+)$ $x \mapsto \{i : i \in \mathbb{Z}^+ \wedge b_i = 1\}$ is an injection $\in \mathbb{Z}^+$

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

$\aleph_0$ $2^{\aleph_0}$ $= c$! c

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

假设！

不存在基数"最大"的集合，因为任何集合可以做幂集

Basic Rules of Counting

odd $\cup$ even $= \mathbb{Z}$, odd $\cap$ even $= \phi$

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

- $\bigcup_{i=1}^{k} A_i = A$ and 全集=原集合.
- $A_i \cap A_j = \emptyset$ for all $i, j \in [k]$ with $i \neq j$. 两两不交

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 $n_1 + n_2 + \cdots + n_k$.

# of entry

Basic Rules of Counting

PP: n step: $n_1 \times n_2 \cdots$

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 $|A| = |B|$.

不重复

一一对应[illegible] 双射：不重漏

Basic Rules of Counting

大数因子数

EXAMPLE: Find # of all/composite divisors of $N = 2^{100} \times 3^{200}$.

- $A = \{n \in \mathbb{Z}^+ : n|N\}$: the # of all divisors of N is $|A|$
  - $n|N$ must have the form $n = 2^a 3^b, 0 \leq a \leq 100, 0 \leq b \leq 200$
  - $|A|$ = # of ways of constructing an integer of the form $2^a 3^b$
  - step 1 $D_1 = \{2^0, 2^1, \ldots, 2^{100}\}; D_2 = \{3^0, 3^1, \ldots, 3^{200}\}$
  - step 2 $|A| = |D_1 \times D_2| = |D_1| \times |D_2| = 101 \times 201$ product rule
- $A_1 = \{n \in A : n \text{ is prime}\}$ 质; $A_2 = \{n \in A : n \text{ is composite}\}$ 合; $A_3 = \{1\}$
  - # of composite divisors of N is $|A_2|$
  - $\{A_1, A_2, A_3\}$ is a partition of A.
    - $|A| = |A_1| + |A_2| + |A_3|$ Sum rule
      - $|A_2| = |A| - |A_1| - |A_3|$
      - $|A_1| = 2, |A_3| = 1$
      - $|A_2| = 101 \times 201 - 2 - 1 = 20298$

$\{2,3\}$.

$r=n$：全排列

Permutations of Set

$1 \le r \le n, r \in Z^+$　　选排列

DEFINITION: Let $A = \{a_1, \dots, a_n\}$ and $r \in [n]$. An **r-permutation** of A is a sequence of r distinct elements of A.

a中取r个元素再排列.

- An n-permutation of A is simply called a **permutation** of A.
    - The 2-permutations of $A = \{1,2,3\}$ are 1,2; 1,3; 2,1; 2,3; 3,1; 3,2

THEOREM: An n-element set has $P(n,r) = n!/(n-r)!$ Different r-permutations.

可重复

DEFINITION: Let $A = \{a_1, \dots, a_n\}$ and $r \in [n]$. An **r-permutation** of A **with repetition** is a sequence of r elements of A.

- The 2-permutations of $A = \{1,2,3\}$ with repetition are
    - 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.

$P(n,r)=n^r$
repetition

(both the production rule)

考题

集合元素互异

Multiset

元素的重复

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

重数：{1,1,2,3}

1: 2

2: 1

3: 1

- An element $x \in A$ has **multiplicity** m if it appears m times in A.
- A multiset A is called an ***n*-multiset** 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 元素数
  - a_i has multiplicity n_i for all $i \in [n]$.
- $T = \{t_1 \cdot a_1, t_2 \cdot a_2, \ldots, t_k \cdot a_k\}$ is called an ***r*-subset** of A if
  - $0 \le t_i \le n_i$ for every $i \in [k]$, and
  - $t_1 + t_2 + \cdots + t_k = r$

r子集 元素数!

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

{2a, b, c}

{a, a, b, c}

排列

Permutations of Multiset

{a b a c

DEFINITION: Let $A = \{n_1 \cdot a_1, \ldots, n_k \cdot a_k\}$ be an n-multiset. A **permutation** of A is 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
  - $A = \{1 \cdot \mathrm{a}, 2 \cdot \mathrm{b}, 3 \cdot \mathrm{c}\}$
  - a, b, c, b, c, c is a permutation (全) of A; bcb is a 3-permutation of A;

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

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

→ 当成不同

→ 去重复

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

- r-permutation of A ~~w/o~~ without repetition: r-permutation of $\{1 \cdot a_1, \ldots, 1 \cdot a_n\}$.
- r-permutation of A with repetition: r-permutation of $\{\infty \cdot a_1, \ldots, \infty \cdot a_n\}$.

因a1重复造成的多倍.

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
  - $A = \{1 \cdot \mathrm{a}, 2 \cdot \mathrm{b}, 3 \cdot \mathrm{c}\}$
  - 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.