Discrete Mathematics
Lecture 9

Liangfeng Zhang
School of Information Science and Technology
ShanghaiTech University

Summary of Lecture 8

Group: $(G, \star)$, closure, associative, identity, inverse

- additive group; multiplicative group

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 $g \in G$
  - $\mathbb{Z}_p^*$ is a cyclic group for any prime p
    - $p = 2q + 1$ for a prime $q \Rightarrow \mathbb{Z}_p^*$ has a subgroup of order q

DLOG and CDH

DEFINITION: Let $G = \langle g \rangle$ be a cyclic group of order q with generator g. For every $h \in G$, there exists $x \in \{0,1,\ldots,q-1\}$ such that $h = g^x$. The integer x is called the **discrete logarithm of h with respect to g.**

- $x = \log_g h$

DLOG Problem: $G = \langle g \rangle$ is a cyclic group of order q **hard**

- **Input**: G and $h = g^x$ for $x \leftarrow \{0,1,\ldots,q-1\}$
- **Output**: $f_{\mathrm{DLOG}}(q, G, g; h) = \log_g h$

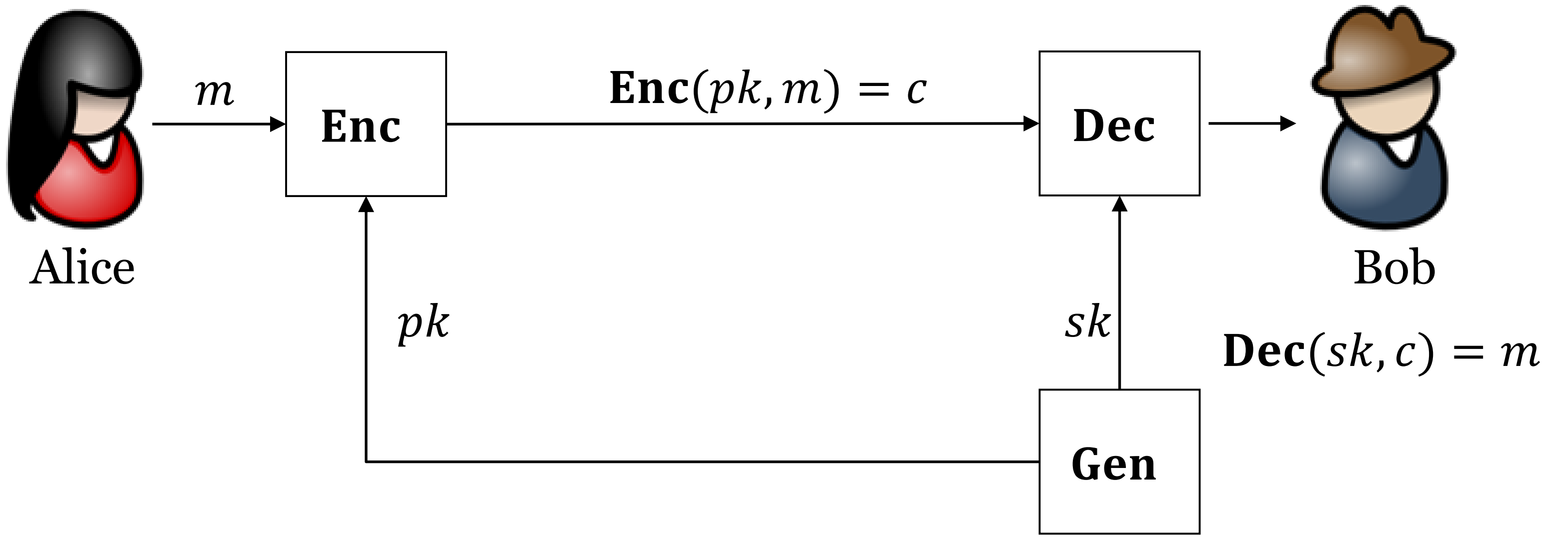
CDH Problem: computational Diffie-Hellman **hard**

- **Input**: $G = \langle g \rangle$ of order q and $A = g^a, B = g^b$ for $a, b \leftarrow \{0,1,\ldots,q-1\}$
- **Output**: $f_{\mathrm{CDH}}(q, G, g; A, B) = g^{ab}$ $a : A = g^a$ $g^{ab} = (B)^a$

Hardness: If G is the order q subgroup of $\mathbb{Z}_p^*$ $(p = 2q + 1)$

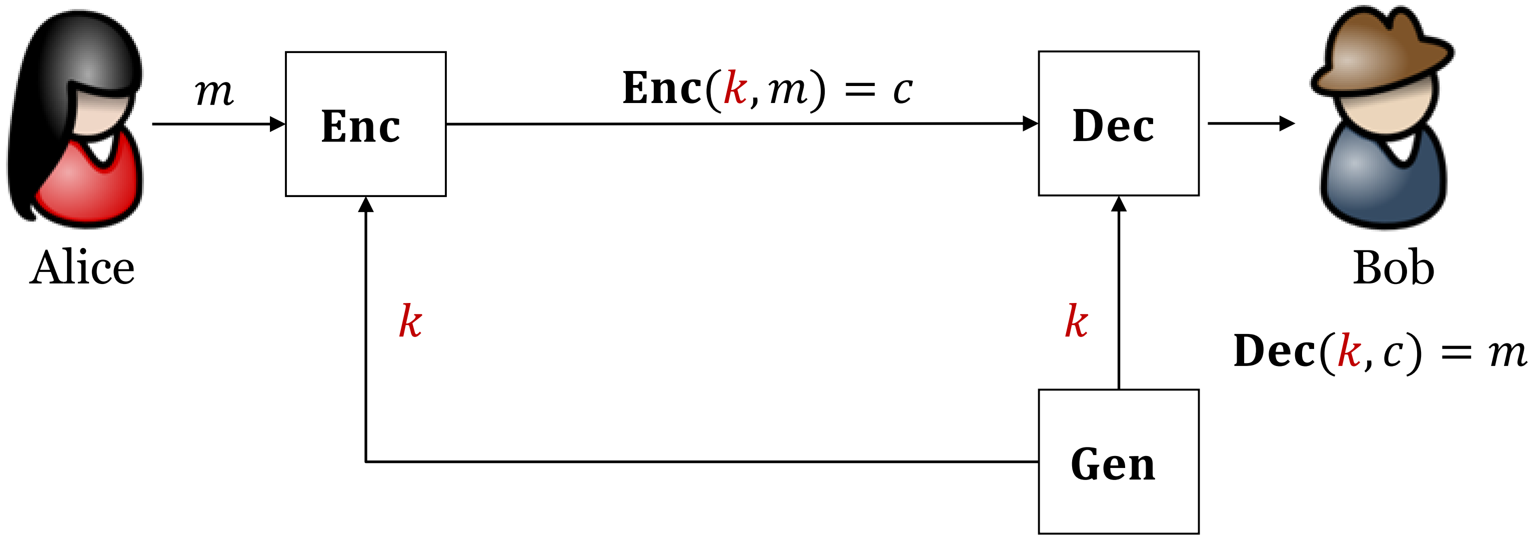
- The best known algorithm runs in $\exp\left(O\left(\sqrt{\ln q \ln\ln q}\right)\right)$

Public-Key Encryption



- **Gen**, **Enc**, **Dec**: key generation, encryption, decryption
- m, c, pk, sk: plaintext (message), ciphertext, public key, private key
- $\mathcal{M}, \mathcal{C}$: plaintext space, ciphertext space
- $\Pi = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec}) + \mathcal{M}, |\mathcal{M}| > 1$
  - **Correctness**: $\mathbf{Dec}\big(sk, \mathbf{Enc}(pk, m)\big) = m$ for any pk, sk, m
  - **Security**: if sk is not known, it's difficult to learn m from pk, c

Private-Key Encryption



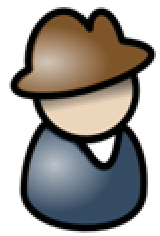
- **Gen**, **Enc**, **Dec**: key generation, encryption, decryption
- m, c, k: plaintext (message), ciphertext, secret key
- $\mathcal{M}, \mathcal{C}$: plaintext space, ciphertext space
- $\Pi = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec}) + \mathcal{M}, |\mathcal{M}| > 1$
  - **Correctness**: $\mathbf{Dec}\big(k, \mathbf{Enc}(k, m)\big) = m$ for any k, m
  - **Security**: if k is not known, it's difficult to learn m from c

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)

$a \leftarrow \mathbb{Z}_q$

$A = g^a$

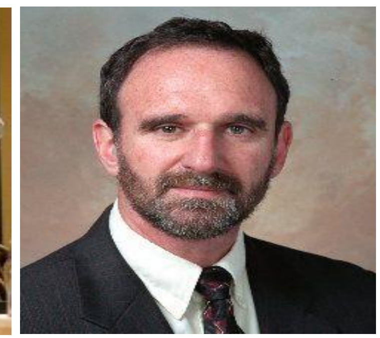
$\xrightarrow{(q, G, g, A)}$

$b \leftarrow \mathbb{Z}_q$

$B = g^b$

$\xleftarrow{B}$

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 $\nrightarrow g^{ab}$

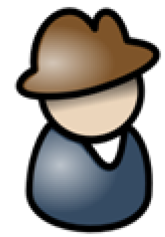
Diffie-Hellman Key Exchange

EXAMPLE: $p = 23;\ \mathbb{Z}_p^* = \langle 5 \rangle; G = \langle 2 \rangle, q = |G| = 11, g = 2$

Alice

$a = 3$

$A = g^a = 8$



Bob

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

$b = 7$

$B = g^b = 13$

$$\xleftarrow{B}$$

Alice: $k = 12$

Bob: $k = 12$

Adversary: $q = 11, p = 23, g = 2, A = 8, B = 13, k =?$

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
- $A = B; A \subseteq B; A \subset B; A \cup B; A \cap B; \bar{A}$

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

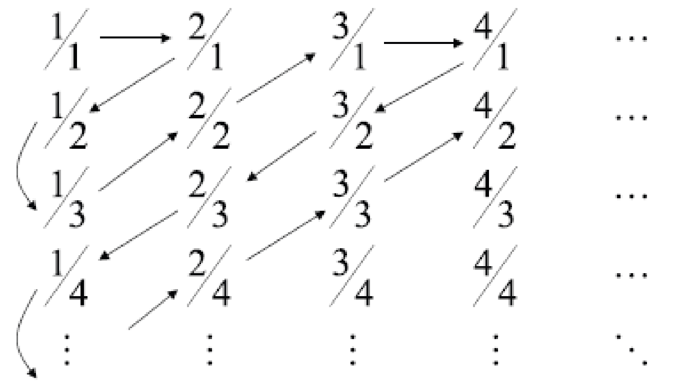
THEOREM: Let A, B, C be any sets. Then

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

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

- $f: \mathbb{R} \to \mathbb{R}^+ \quad x \mapsto 2^x$
- $f: (0,1) \to \mathbb{R} \quad x \mapsto \tan\left(\pi(x - 1/2)\right)$
- $f: [0,1] \to (0,1)$
  - $f(1) = 2^{-1}, f(0) = 2^{-2}, f(2^{-n}) = 2^{-n-2}, n = 1,2,3, \ldots$
  - $f(x) = x$ 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
- $f: 2^X \to \mathcal{P}(X) \quad \alpha \mapsto A = \{x: \alpha(x) = 1\}$

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 $i = 1,2,3,\ldots$
- $b = 0.b_1b_2b_3b_4b_5b_6b_7b_8b_9\cdots$ 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

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 $f: A \rightarrow \mathcal{P}(A)$ defined by $f(a) = \{a\}$ is injective.
- $|A| \neq |\mathcal{P}(A)|$
  - Assume that there is a bijection $g: A \rightarrow \mathcal{P}(A)$
  - 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 $\{0,1\}^*$
  - $\{0,1\}^* = \bigcup_{n\geq 0}\{0,1\}^n$: 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: $|A| = |\mathbb{Z}^+|$

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 $f: \mathbb{Z}^+ \to A$
- If $A = \{a_1, a_2, \ldots\}$, then the $f: \mathbb{Z}^+ \to A$ 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 $X = \{a_{i_1}, a_{i_2}, \dots\}$ $\quad X$ 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: $|\mathbb{Z}^+| < |\mathcal{P}(\mathbb{Z}^+)| = |[0,1)| = |(0,1)| = |\mathbb{R}|$

$\aleph_0 \qquad 2^{\aleph_0} \qquad c$

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 $\aleph_0 < |A| < c$.