Discrete Mathematics
Lecture 8

Liangfeng Zhang
School of Information Science and Technology
ShanghaiTech University

Summary of Lecture 7

Chinese Reminder Theorem: $n_1, \ldots., n_k \in \mathbb{Z}^+, \gcd(n_i, n_j) = 1$

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \vdots \\ x \equiv b_k \pmod{n_k} \end{cases}$$

always has a unique solution modulo $n = n_1 n_2 \cdots n_k$.

CRT Map $\theta: \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}; \theta: \mathbb{Z}_n^* \to \mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$

- θ is always a bijection: $\phi(n) = \phi(n_1) \cdots \phi(n_k)$
- $\phi\left(p_1^{e_1} \cdots p_k^{e_k}\right) = \phi\left(p_1^{e_1}\right) \cdots \phi\left(p_k^{e_k}\right)$

Group: $(G, \star)$, a set G and a binary operation $\star$

- Closure; Associative; Identity; Inverse
- $(\mathbb{Z}_n, +)$ is an additive group
- $(\mathbb{Z}_n^*, *)$ is a multiplicative group

Order

阶数 基数（元素个数）

DEFINITION: The **order** of a group G is the cardinality of G.

- $|\mathbb{Z}_n| = n, |\mathbb{Z}_p^*| = p - 1, |\mathbb{Z}| = \infty$

DEFINITION: when $|G| < \infty$, $\forall a \in G$, the **order** of a is defined as the least integer $l > 0$ s.t. $a^l = 1$ ($la = 0$ for additive group)

乘法

证一定存在

EXAMPLE: Determine the orders of all elements of $\mathbb{Z}_7^*$

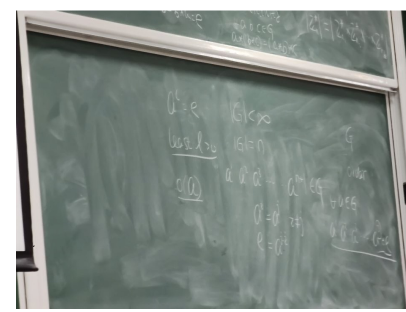
- $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$ $\quad a^l = e$
- $o(1) = 1, o(2) = 3, o(3) = 6, o(4) = 3, o(5) = 6, o(6) = 2$

EXAMPLE: Determine the orders of all elements of $\mathbb{Z}_6$

- $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ $\quad al = e$
- $o(0) = 1, o(1) = o(5) = 6, o(2) = o(4) = 3, o(3) = 2$

0 $\quad 1\times 6 = 6 \equiv 0$ $\quad 2\times 3 = 6 \equiv 0$ $\quad 3\times 2 = 6 \equiv 0$

$5\times 6 = 30 \equiv 0$ $\quad 4\times 3 = 12 \equiv 0$



Order of $a \in \mathbb{Z}_{11}^*$

a	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	$o(a)$
1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1	10
3	3	9	5	4	1	3	9	5	4	1	5
4	4	5	9	3	1	4	5	9	3	1	5
5	5	3	4	9	1	5	3	4	9	1	5
6	6	3	7	9	10	5	8	4	2	1	10
7	7	5	2	3	10	4	6	9	8	1	10
8	8	9	6	4	10	3	2	5	7	1	10
9	9	4	3	5	1	9	4	3	5	1	5
10	10	1	10	1	10	1	10	1	10	1	2

- $a^{10} = 1$ for every $a \in \mathbb{Z}_{11}^*$; $o(a)|10$ for every $a \in \mathbb{Z}_{11}^*$

Euler's Theorem

THEOREM: Let G be a multiplicative Abelian group of order m.

Then for any $a \in G$, $a^m = 1$. 加法群 $ma=0$

- $G = \{a_1, \dots, a_m\}$
  - If $i \neq j$, then $aa_i \neq aa_j$.
    - $aa_1 \cdot aa_2 \cdots aa_m = a_1 a_2 \cdots a_m \Rightarrow a^m = 1$

Euler's Theorem: Let $n > 1$ and $\alpha \in \mathbb{Z}_n^*$. Then $\alpha^{\phi(n)} = 1$.

- $\alpha^{\phi(n)}$, 1 are both residue classes modulo n
- Proof: a corollary of the previous theorem for $G = \mathbb{Z}_n^*$

Fermat's Little Theorem: If p is a prime and $\alpha \in \mathbb{Z}_p$.

Then $\alpha^p = \alpha$.

Subgroup 子群

任何一个群都有{e}, G 2个平凡子群

DEFINITION: Let $(G,\star)$ be an Abelian group. A subset $H \subseteq G$ is called a **subgroup** of G if $(H,\star)$ is also a group. $(H \leq G)$

- Multiplicative: $G = \mathbb{Z}_6^* = \{1,5\}, H = \{1\}$ {1}/G G最大子群. ⇒ G
- Additive: $G = \mathbb{Z}_6 = \{0,1,2,3,4,5\}; H = \{0,2,4\}$ {0}/G

THEOREM: Let $(G,\cdot)$ be an Abelian group. Let $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$ be a subset of G, where $g \in G$. Then $\langle g \rangle \leq G$. 由g生成的子群

- Closure: $g^a \cdot g^b = g^{a+b} \in \langle g \rangle$
- Associative: $g^a \cdot (g^b \cdot g^c) = g^{a+b+c} = (g^a \cdot g^b) \cdot g^c$
- Identity element: $g^0 \cdot g^a = g^a \cdot g^0 = g^a$
- Inverse: $g^a \cdot g^{-a} = g^{-a} \cdot g^a = g^0$
- Communicative: $g^a \cdot g^b = g^{a+b} = g^{b+a} = g^b \cdot g^a$

Cyclic Group 循环群

eg. $(Z_n, +)$, $(Z_n^*, \times)$

$Z_n = \langle [1]_n \rangle$ $\qquad Z_5^* \langle [2]_5 \rangle$

DEFINITION: Let $(G,\cdot)$ be an Abelian group. G is said to be **cyclic** if there exists $g \in G$ such that $G = \langle g \rangle$.

- g is called a **generator** of G. 生成元

EXAMPLE: $\mathbb{Z}_{10}^* = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\} = \langle [3]_{10} \rangle$

- $g = [3]_{10}$
- $g^0 = [1]_{10}, g^1 = [3]_{10}, g^2 = [9]_{10}, g^3 = [27]_{10} = [7]_{10}$

REMARK: Let G be a finite group and let $g \in G$. Then $\langle g \rangle$ can be computed as $\{g^1, g^2, \dots\}$

Cyclic Group

EXAMPLE: $\mathbb{Z}_p^*$ is a cyclic group and $G = \langle g \rangle$ is a cyclic subgroup.

- p =179769313486231590772930519078902473361797697894230657273430081157732675805500963132708477322407536021120113879871393357658789768814416622492847430639474124377767893424865485276302219601246094119453082952085005768838150682342462881473913110540827237163350510684586298239947245938479716304835356329624227998859
  - p is a prime; $\mathbb{Z}_p^* = \langle 2 \rangle$ is a cyclic group of order $p - 1$
- q =898846567431157953864652595394512366808988489471153286367150405788663379027504815663542386612037680105600569399356966788293948844072083112464237153197370621888839467124327426381511098006230470597265414760425028844190753411712314407369565552704136185816752553422931491199736229692392858152417678164812113999429
  - $q = (p - 1)/2$ is a prime
  - $g = 3$
  - $G = \langle g \rangle$ is a subgroup of $\mathbb{Z}_p^*$ of order q

$P=11 \quad q = \frac{11-1}{2} = 5$

P: 安全素数

$\langle [3]_{11} \rangle = \{3, 9, 5, 4, 1, 3\}$

$\langle [2] \rangle = \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$

$\langle [3] \rangle$ 是5阶循环群

X order ≠ 5

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 $x \in \{0,1,\dots,q-1\}$ such that $h = g^x$. The integer x is called the **discrete logarithm of** h **with respect to** g.是h关于g的离散对数

- $x = \log_g h$ g,h很大时，log_g h是困难问题，无法多项式时间解决

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

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

人名

CDH Problem: computational Diffie-Hellman

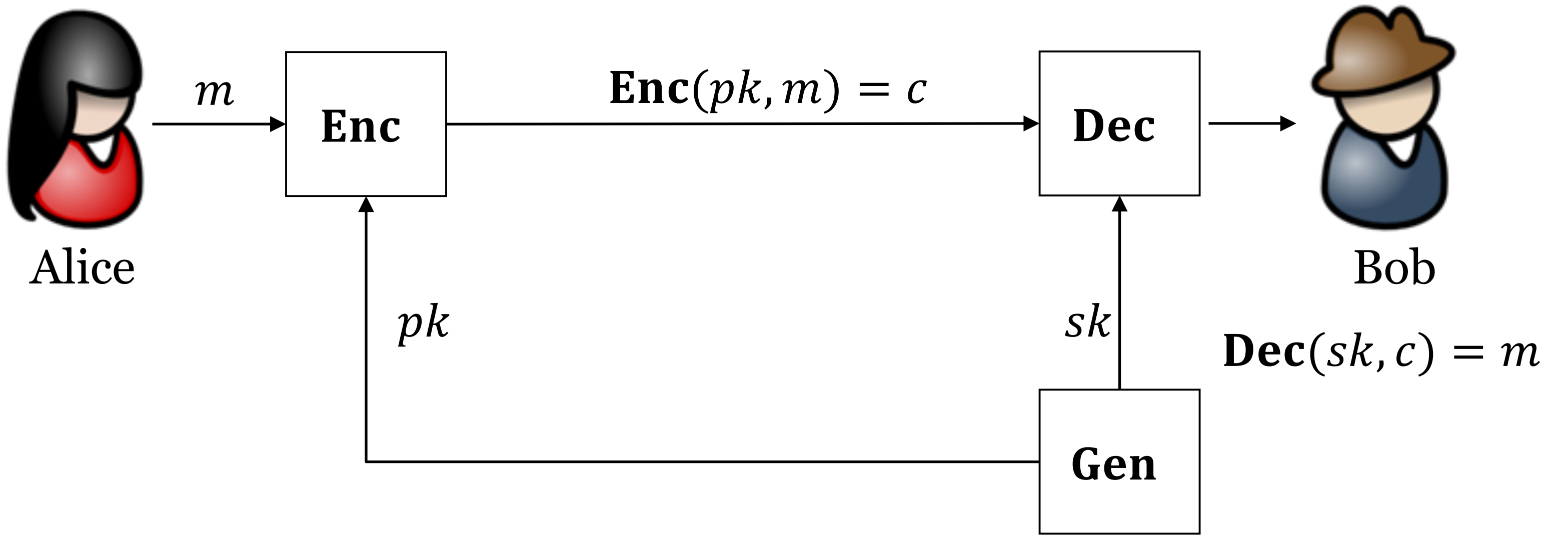
- **Input**: $G = \langle g \rangle$ of order q and $A = g^a, B = g^b$ for $a, b \leftarrow \{0,1,\dots,q-1\}$
- **Output**: $f_{\mathrm{CDH}}(q, G, g; A, B) = g^{ab}$

a,b不知道

无多项式时间做法

RSA

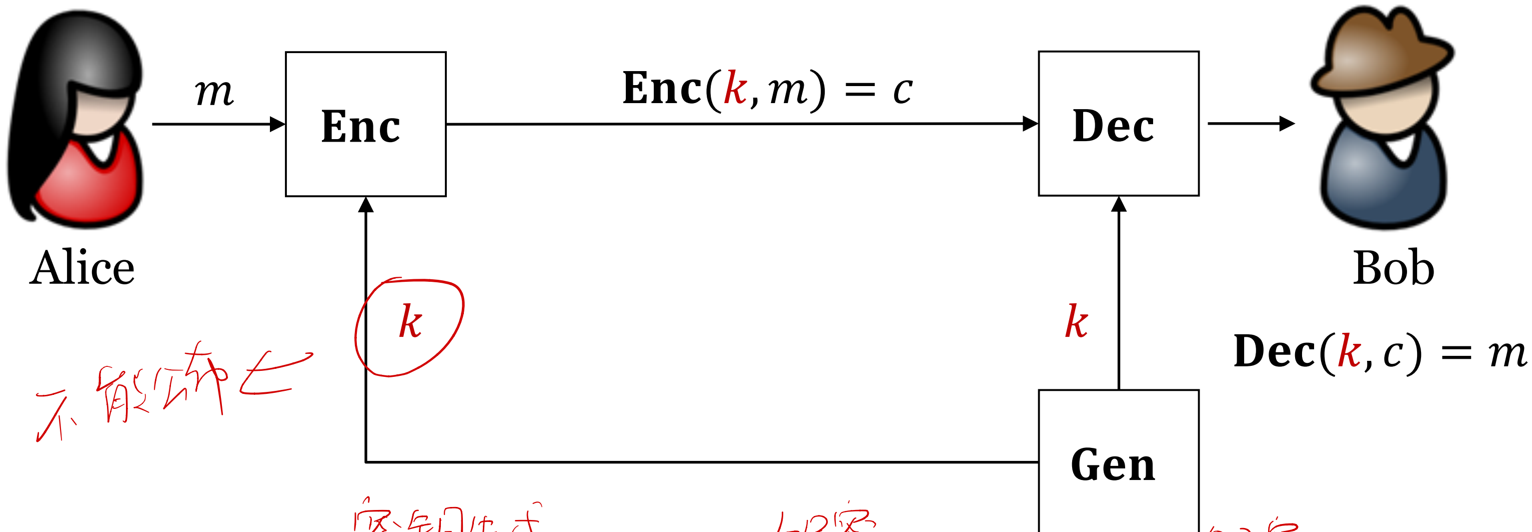
Public-Key Encryption



- $\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec}$: 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

私钥加密
/对称加密

Private-Key Encryption



密钥生成 加密 解密

- **Gen, Enc, Dec**: key generation, encryption, decryption
- m, c, k: plaintext 明文 (message), ciphertext 密文, secret key 密钥
- $\mathcal{M}, \mathcal{C}$: 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

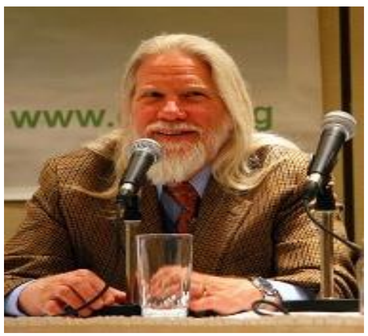
Alice: (q, G, g), $a \leftarrow \mathbb{Z}_q$, $A = g^a$

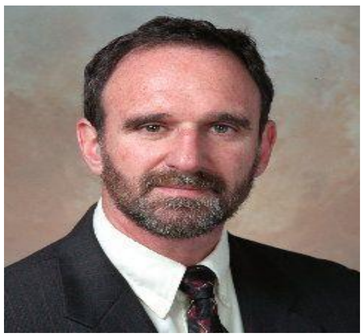
Alice $\xrightarrow{(q, G, g, A)}$ Bob

Bob: $b \leftarrow \mathbb{Z}_q$, $B = g^b$

Alice $\xleftarrow{B}$ Bob

Alice: output B^a — Bob: 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

2, 4, 8, 16, 9, 18, 13, 3, 6, 12,

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

Alice

Bob

128

$a = 3$
$A = g^a = 8$

$(q, G, g, A) \rightarrow$

23
×5
115

$b = 7$
$B = g^b = 13$

$\leftarrow B$

$k = 12$ $k = 12$

敌手

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

$23 = 2 \times 11 + 1$

安全

Security

Algorithms for DLOG, CDH: solving the DLOG problem first

- $\boldsymbol{G}$: **the group $\mathbb{Z}_p^*$ of order $q = p - 1$**
  - The best known algorithm runs in $\exp\left(O\left(\sqrt{\ln q \ln\ln q}\right)\right)$
  - $|G| = 2^{1024}$ has been used for many years; now not very safe
  - $|G| = 2^{2048}$ is recommended for today's application
- $\boldsymbol{G}$: **an order q subgroup of $\mathbb{Z}_p^*$, where $p = 2q + 1$ is a safe prime**
  - The best known algorithm runs in $\exp\left(O\left(\sqrt{\ln q \ln\ln q}\right)\right)$
- For specific group G of order q, the best known algorithm runs in
  - $\exp\left(O\left(\sqrt{(\ln q)^{1/3}(\ln\ln q)^{2/3}}\right)\right)$ //multiplicative group $\mathbb{F}_{p^k}^*$
- For specific group G of order q, the best algorithm runs in
  - $O(\sqrt{q})$ // elliptic curves

Combinatorics 组合

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)**

$f: A \rightarrow B$ 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 $|A| < |B|$

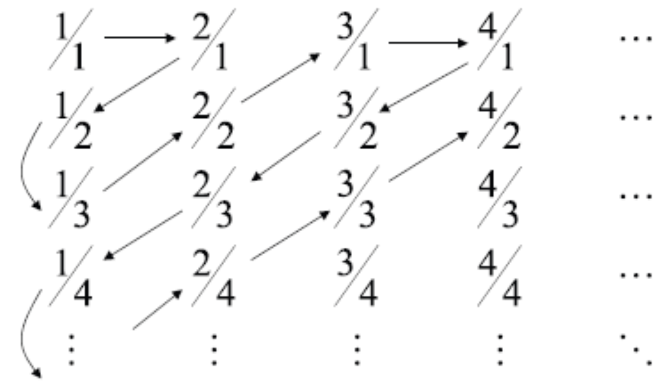
THEOREM: Let A, B, C be any sets. Then

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

Cardinality of Sets

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

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



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

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

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

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:

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

- 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

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 $\{0,1\}^*$
  - $\{0,1\}^* = \bigcup_{n\geq 0}\{0,1\}^n$: 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 $f\colon \mathbb{Z}^+ \to A$
- 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 $X = \{a_{i_1}, a_{i_2}, \dots\}$ $\quad X$ 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: $|\mathbb{Z}^+| < |\mathcal{P}(\mathbb{Z}^+)| = |[0,1)| = |(0,1)| = |\mathbb{R}|$

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

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 $\aleph_0 < |A| < c$.