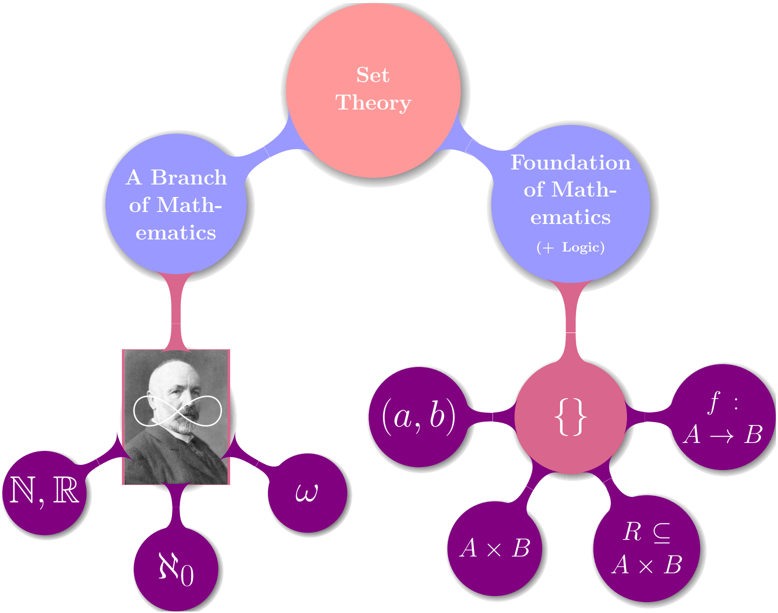
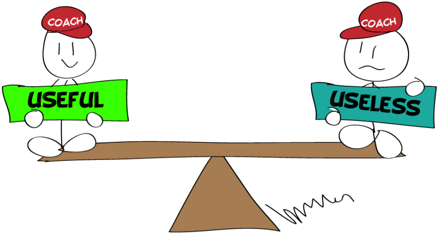
Functions

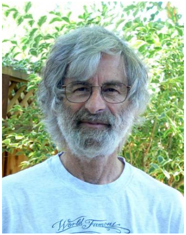
魏恒峰

hfwei@nju.edu.cn

2018 年 02 月 xx 日


Set Theory
A Branch of Math-ematics
Foundation of Math-ematics
(+ Logic)
$\mathbb{N}, \mathbb{R}$
$\aleph_0$
ω
(a, b)
$\{\}$
$f : A \to B$
$A \times B$
$R \subseteq A \times B$


COACH
USEFUL
COACH
USELESS



Time, Clocks, and the Ordering of Events in a Distributed System

Leslie Lamport
Massachusetts Computer Associates, Inc.

The concept of one event happening before another in a distributed system is examined, and is shown to define a partial ordering of the events. A distributed algorithm is given for synchronizing a system of logical clocks which can be used to totally order the events.

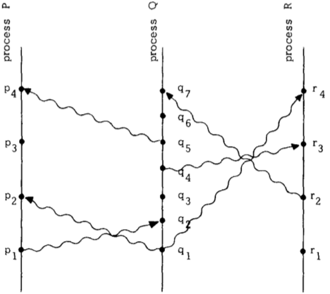


Figure 13. A selection of consistency axioms over an execution $(E, \mathsf{repl}, \mathsf{obj}, \mathsf{oper}, \mathsf{rval}, \mathsf{ro}, \mathsf{vis}, \mathsf{ar})$

Auxiliary relations

$\mathsf{sameobj}(e, f) \iff \mathsf{obj}(e) = \mathsf{obj}(f)$

Per-object causality (aka happens-before) order:

$\mathsf{hbo} = ((\mathsf{ro} \cap \mathsf{sameobj}) \cup \mathsf{vis})^+$

Causality (aka happens-before) order: $\mathsf{hb} = (\mathsf{ro} \cup \mathsf{vis})^+$

Axioms

EVENTUAL:

$\forall e \in E. \neg(\exists \text{ infinitely many } f \in E. \mathsf{sameobj}(e, f) \land \neg(e \xrightarrow{\mathsf{vis}} f))$

THINAIR: $\mathsf{ro} \cup \mathsf{vis}$ is acyclic

POCV (Per-Object Causal Visibility): $\mathsf{hbo} \subseteq \mathsf{vis}$

POCA (Per-Object Causal Arbitration): $\mathsf{hbo} \subseteq \mathsf{ar}$

COCV (Cross-Object Causal Visibility): $(\mathsf{hb} \cap \mathsf{sameobj}) \subseteq \mathsf{vis}$

COCA (Cross-Object Causal Arbitration): $\mathsf{hb} \cup \mathsf{ar}$ is acyclic

Figure 13. A selection of consistency axioms over an execution $(E, \mathsf{repl}, \mathsf{obj}, \mathsf{oper}, \mathsf{rval}, \mathsf{ro}, \mathsf{vis}, \mathsf{ar})$

Auxiliary relations

$\mathsf{sameobj}(e, f) \iff \mathsf{obj}(e) = \mathsf{obj}(f)$

Per-object causality (aka happens-before) order:

$\mathsf{hbo} = ((\mathsf{ro} \cap \mathsf{sameobj}) \cup \mathsf{vis})^{+}$

Causality (aka happens-before) order: $\mathsf{hb} = (\mathsf{ro} \cup \mathsf{vis})^{+}$

Axioms

EVENTUAL:

$\forall e \in E.\, \neg(\exists \text{ infinitely many } f \in E.\, \mathsf{sameobj}(e, f) \wedge \neg(e \xrightarrow{\mathsf{vis}} f))$

THINAIR: $\mathsf{ro} \cup \mathsf{vis}$ is acyclic

POCV (Per-Object Causal Visibility): $\mathsf{hbo} \subseteq \mathsf{vis}$

POCA (Per-Object Causal Arbitration): $\mathsf{hbo} \subseteq \mathsf{ar}$

COCV (Cross-Object Causal Visibility): $(\mathsf{hb} \cap \mathsf{sameobj}) \subseteq \mathsf{vis}$

COCA (Cross-Object Causal Arbitration): $\mathsf{hb} \cup \mathsf{ar}$ is acyclic

Figure 17. Optimized state-based multi-value register and its simulation

$$
\begin{aligned}
\Sigma &= \mathsf{ReplicaID} \times \mathcal{P}(\mathbb{Z} \times (\mathsf{ReplicaID} \to \mathbb{N}_0))\\
\vec{\sigma}_0 &= \langle r, \emptyset \rangle\\
M &= \mathcal{P}(\mathbb{Z} \times (\mathsf{ReplicaID} \to \mathbb{N}_0))\\
\mathsf{do}(\mathtt{wr}(a), \langle r, V\rangle, t) &=\\
&\quad (\langle r, \{(a, (\lambda s.\, \text{if } s \neq r \text{ then } \max\{v(s) \mid (\_, v) \in V\}\\
&\qquad \text{else } \max\{v(s) \mid (\_, v) \in V\} + 1))\}\rangle, \bot)\\
\mathsf{do}(\mathtt{rd}, \langle r, V\rangle, t) &= (\langle r, V\rangle, \{a \mid (a, \_) \in V\})\\
\mathsf{send}(\langle r, V\rangle) &= (\langle r, V\rangle, V)\\
\mathsf{receive}(\langle r, V\rangle, V') &= \langle r, \{(a, v) \in V'' \mid\\
&\quad v \not\sqsubseteq \bigsqcup\{v' \mid \exists a'.\, (a', v') \in V'' \wedge a \neq a'\}\}\rangle,\\
\text{where } V'' &= \{(a, \bigsqcup\{v' \mid (a, v') \in V \cup V'\}) \mid (a, \_) \in V \cup V'\}
\end{aligned}
$$

$\langle s, V\rangle\, [\mathcal{R}_r]\, I \iff (r = s) \wedge (V\, [\mathcal{M}]\, I)$

$$
\begin{aligned}
&V\, [\mathcal{M}]\, ((E, \mathsf{repl}, \mathsf{obj}, \mathsf{oper}, \mathsf{rval}, \mathsf{ro}, \mathsf{vis}, \mathsf{ar}), \mathsf{info}) \iff\\
&\quad (\forall (a, v), (a', v') \in V.\, (a = a' \implies v = v')) \wedge\\
&\quad (\forall (a, v) \in V.\, \exists s.\, v(s) > 0) \wedge\\
&\quad (\forall (a, v) \in V.\, v \not\sqsubseteq \bigsqcup\{v' \mid \exists a'.\, (a', v') \in V \wedge a \neq a'\}) \wedge\\
&\quad \exists \text{ distinct } e_{s,k}.\\
&\quad (\{e \in E \mid \exists a.\, \mathsf{oper}(e) = \mathtt{wr}(a)\} = \{e_{s,k} \mid s \in \mathsf{ReplicaID} \wedge\\
&\qquad 1 \leq k \leq \max\{v(s) \mid \exists a.\, (a, v) \in V\}\}) \wedge\\
&\quad (\forall s, j, k.\, (\mathsf{repl}(e_{s,k}) = s) \wedge (e_{s,j} \xrightarrow{\mathsf{ro}} e_{s,k} \iff j < k)) \wedge\\
&\quad (\forall (a, v) \in V.\, \forall q.\, \{j \mid \mathsf{oper}(e_{q,j}) = \mathtt{wr}(a)\} \cup\\
&\qquad \{j \mid \exists s, k.\, e_{q,j} \xrightarrow{\mathsf{vis}} e_{s,k} \wedge \mathsf{oper}(e_{s,k}) = \mathtt{wr}(a)\} =\\
&\qquad \{j \mid 1 \leq j \leq v(q)\}) \wedge\\
&\quad (\forall e \in E.\, (\mathsf{oper}(e) = \mathtt{wr}(a) \wedge\\
&\qquad \neg\exists f \in E.\, \mathsf{oper}(f) = \mathtt{wr}(\_) \wedge e \xrightarrow{\mathsf{vis}} f) \implies (a, \_) \in V)
\end{aligned}
$$

the former. The only non-trivial obligation is to show that if

$$V\, [\mathcal{M}]\, ((E, \mathsf{repl}, \mathsf{obj}, \mathsf{oper}, \mathsf{rval}, \mathsf{ro}, \mathsf{vis}), \mathsf{info}),$$

then

$$
\begin{aligned}
\{a \mid (a, \_) \in V\} \subseteq \{a \mid \exists e \in E.\, \mathsf{oper}(e) = \mathtt{wr}(a) \wedge&\\
\neg\exists f \in E.\, \exists a'.\, \mathsf{oper}(e) = \mathtt{wr}(a') \wedge e \xrightarrow{\mathsf{vis}} f\}& \quad (13)
\end{aligned}
$$

(the reverse inclusion is straightforwardly implied by $\mathcal{R}_r$).

Take $(a, v) \in V$. We have $\forall (a, v) \in V.\, \exists s.\, v(s) > 0$,

$$v \not\sqsubseteq \bigsqcup\{v' \mid \exists a'.\, (a', v') \in V \wedge a \neq a'\}$$

and

$$
\begin{aligned}
&\forall (a, v) \in V.\, \forall q.\, \{j \mid \mathsf{oper}(e_{q,j}) = \mathtt{wr}(a)\} \cup\\
&\quad \{j \mid \exists s, k.\, e_{q,j} \xrightarrow{\mathsf{vis}} e_{s,k} \wedge \mathsf{oper}(e_{s,k}) = \mathtt{wr}(a)\} =\\
&\quad \{j \mid 1 \leq j \leq v(q)\}.
\end{aligned}
$$

From this we get that for some $e \in E$

$$
\begin{aligned}
\mathsf{oper}(e) = \mathtt{wr}(a) \wedge \neg\exists f \in E.\, \exists a'.\, a' \neq a \wedge&\\
\mathsf{oper}(e) = \mathtt{wr}(a') \wedge e \xrightarrow{\mathsf{vis}} f.&
\end{aligned}
$$

Since vis is acyclic, this implies that for some $e' \in E$

$$\mathsf{oper}(e') = \mathtt{wr}(a) \wedge \neg\exists f \in E.\, \mathsf{oper}(e') = \mathtt{wr}(\_) \wedge e' \xrightarrow{\mathsf{vis}} f,$$

which establishes (13).

Let us now discharge RECEIVE. Let $\mathsf{receive}(\langle r, V\rangle, V') = \langle r, V'''\rangle$, where

$$
\begin{aligned}
V'' &= \{(a, \bigsqcup\{v' \mid (a, v') \in V \cup V'\}) \mid (a, \_) \in V \cup V'\};\\
V''' &= \{(a, v) \in V'' \mid v \not\sqsubseteq \bigsqcup\{(a', v') \in V'' \mid a \neq a'\}\}.
\end{aligned}
$$

Assume $\langle r, V\rangle\, [\mathcal{R}_r]\, I$, $V'\, [\mathcal{M}]\, J$ and

$$
\begin{aligned}
I &= ((E, \mathsf{repl}, \mathsf{obj}, \mathsf{oper}, \mathsf{rval}, \mathsf{ro}, \mathsf{vis}, \mathsf{ar}), \mathsf{info});\\
J &= ((E', \mathsf{repl}', \mathsf{obj}', \mathsf{oper}', \mathsf{rval}', \mathsf{ro}', \mathsf{vis}', \mathsf{ar}'), \mathsf{info}');\\
I \sqcup J &= ((E'', \mathsf{repl}'', \mathsf{obj}'', \mathsf{oper}'', \mathsf{rval}'', \mathsf{ro}'', \mathsf{vis}'', \mathsf{ar}''), \mathsf{info}'').
\end{aligned}
$$

By agree we have $I \sqcup J \in \mathsf{IEx}$. Then

$$
\begin{aligned}
&(\forall (a, v), (a', v') \in V.\, (a = a' \implies v = v')) \wedge\\
&(\forall (a, v) \in V.\, \exists s.\, v(s) > 0) \wedge\\
&(\forall (a, v) \in V.\, v \not\sqsubseteq \bigsqcup\{v' \mid \exists a'.\, (a', v') \in V \wedge a \neq a'\}) \wedge\\
&\exists \text{ distinct } e_{s,k}.\\
&(\{e \in E \mid \exists a.\, \mathsf{oper}''(e) = \mathtt{wr}(a)\} = \{e_{s,k} \mid s \in \mathsf{ReplicaID} \wedge\\
&\quad 1 \leq k \leq \max\{v(s) \mid \exists a.\, (a, v) \in V\}\}) \wedge\\
&(\forall s, j, k.\, (\mathsf{repl}''(e_{s,k}) = s) \wedge (e_{s,j} \xrightarrow{\mathsf{ro}} e_{s,k} \iff j < k)) \wedge\\
&(\forall (a, v) \in V.\, \forall q.\, \{j \mid \mathsf{oper}''(e_{q,j}) = \mathtt{wr}(a)\} \cup\\
&\quad \{j \mid \exists s, k.\, e_{q,j} \xrightarrow{\mathsf{vis}} e_{s,k} \wedge \mathsf{oper}''(e_{s,k}) = \mathtt{wr}(a)\} =\\
&\quad \{j \mid 1 \leq j \leq v(q)\}) \wedge\\
&(\forall e \in E.\, (\mathsf{oper}''(e) = \mathtt{wr}(a) \wedge\\
&\quad \neg\exists f \in E.\, \mathsf{oper}''(f) = \mathtt{wr}(\_) \wedge e \xrightarrow{\mathsf{vis}} f) \implies (a, \_) \in V)
\end{aligned}
$$

and

$$
\begin{aligned}
&(\forall (a, v), (a', v') \in V'.\, (a = a' \implies v = v')) \wedge\\
&(\forall (a, v) \in V'.\, \exists s.\, v(s) > 0) \wedge\\
&(\forall (a, v) \in V'.\, v \not\sqsubseteq \bigsqcup\{v' \mid \exists a'.\, (a', v') \in V' \wedge a \neq a'\}) \wedge\\
&\exists \text{ distinct } e_{s,k}.\\
&(\{e \in E' \mid \exists a.\, \mathsf{oper}''(e) = \mathtt{wr}(a)\} = \{e_{s,k} \mid s \in \mathsf{ReplicaID} \wedge\\
&\quad 1 \leq k \leq \max\{v(s) \mid \exists a.\, (a, v) \in V'\}\}) \wedge\\
&(\forall s, j, k.\, (\mathsf{repl}''(e_{s,k}) = s) \wedge (e_{s,j} \xrightarrow{\mathsf{ro}'} e_{s,k} \iff j < k)) \wedge\\
&(\forall (a, v) \in V'.\, \forall q.\, \{j \mid \mathsf{oper}''(e_{q,j}) = \mathtt{wr}(a)\} \cup\\
&\quad \{j \mid \exists s, k.\, e_{q,j} \xrightarrow{\mathsf{vis}'} e_{s,k} \wedge \mathsf{oper}''(e_{s,k}) = \mathtt{wr}(a)\} =\\
&\quad \{j \mid 1 \leq j \leq v(q)\}) \wedge\\
&(\forall e \in E'.\, (\mathsf{oper}''(e) = \mathtt{wr}(a) \wedge\\
&\quad \neg\exists f \in E'.\, \mathsf{oper}''(f) = \mathtt{wr}(\_) \wedge e \xrightarrow{\mathsf{vis}'} f) \implies (a, \_) \in V').
\end{aligned}
$$

The agree property also implies

$$
\begin{aligned}
\forall s, k.\, 1 \leq k \leq \min\{&\max\{v(s) \mid \exists a.\, (a, v) \in V\},\\
&\max\{v(s) \mid \exists a.\, (a, v) \in V'\}\} \implies e_{s,k} = e'_{s,k}.
\end{aligned}
$$

Hence, there exist distinct

$$e''_{s,k} \text{ for } s \in \mathsf{ReplicaID},\ k = 1..(\max\{v(s) \mid \exists a.\, (a, v) \in V'''\}),$$

such that

$$
\begin{aligned}
&(\forall s, k.\, 1 \leq k \leq \max\{v(s) \mid \exists a.\, (a, v) \in V\} \implies e''_{s,k} = e_{s,k}) \wedge\\
&(\forall s, k.\, 1 \leq k \leq \max\{v(s) \mid \exists a.\, (a, v) \in V'\} \implies e''_{s,k} = e'_{s,k})
\end{aligned}
$$

and

$$
\begin{aligned}
&(\{e \in E \cup E' \mid \exists a.\, \mathsf{oper}''(e) = \mathtt{wr}(a)\} =\\
&\{e''_{s,k} \mid s \in \mathsf{ReplicaID} \wedge 1 \leq k \leq \max\{v(s) \mid \exists a.\, (a, v) \in V'''\}\})\\
&\wedge (\forall s, j, k.\, (\mathsf{repl}(e''_{s,k}) = s) \wedge (e''_{s,j} \xrightarrow{\mathsf{ro}''} e''_{s,k} \iff j < k)).
\end{aligned}
$$

By the definition of V'' and V''' we have

$$\forall (a, v), (a', v') \in V'''.\, (a = a' \implies v = v').$$

We also straightforwardly get

$$\forall (a, v) \in V'.\, \exists s.\, v(s) > 0$$

and

$$
\begin{aligned}
&(\forall (a, v) \in V''.\, \forall q.\, \{j \mid \mathsf{oper}''(e''_{q,j}) = \mathtt{wr}(a)\} \cup\\
&\quad \{j \mid \exists s, k.\, e''_{q,j} \xrightarrow{\mathsf{vis}''} e''_{s,k} \wedge \mathsf{oper}''(e''_{s,k}) = \mathtt{wr}(a)\} = \quad (14)\\
&\quad \{j \mid 1 \leq j \leq v(q)\}).
\end{aligned}
$$

Definition of Function

Definition (Function)

Let A and B be sets.
A **function** f from A to B is a *relation* f from A to B such that

$$\forall a \in A\ \exists! b \in B\ (a, b) \in f.$$

Definition (Function)

Let A and B be sets.
A **function** f from A to B is a *relation* f from A to B such that

$$\forall a \in A \; \exists! b \in B \; (a, b) \in f.$$

For Proof:

$$\forall$$

$$\exists! : \forall b, b' \in B, (a, b) \in f \wedge (a, b') \in f \implies b = b'.$$

Definition (Function)

Let A and B be sets.
A **function** f from A to B is a *relation* f from A to B such that

$$\forall a \in A \; \exists! b \in B \; (a, b) \in f.$$

For Proof:

$$\forall$$

$$\exists! : \forall b, b' \in B, (a, b) \in f \land (a, b') \in f \implies b = b'.$$

$$f : A \to B, \quad a \mapsto f(a) \qquad \Big(b = f(a)\Big)$$

$$A : \mathrm{dom}(f) \qquad B : \mathrm{cod}(f)$$

Definition (Function)

Let A and B be sets.
A **function** f from A to B is a *relation* f from A to B such that

$$\forall a \in A \; \exists! b \in B \; (a, b) \in f.$$

For Proof:

$$\forall$$

$$\exists! : \forall b, b' \in B, (a, b) \in f \land (a, b') \in f \implies b = b'.$$

$$f : A \to B, \quad a \mapsto f(a) \qquad \big(b = f(a)\big)$$

$$A : \mathrm{dom}(f) \qquad B : \mathrm{cod}(f)$$

$$\mathrm{ran}(f) = f(A) = \{f(a) \mid a \in A\} \subseteq B$$

A function $f : A \to B$ is a set.

$$f \subseteq A \times B$$

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

$$(a, b) = \{\{a\}, \{a, b\}\}$$

Definition (Axiom of Extensionality (集合的外延公理))

$$\forall A \forall B \forall x (x \in A \iff x \in B) \iff A = B.$$

Intensionality (内涵) *vs.* Extensionality (外延)

Definition (Axiom of Extensionality (集合的外延公理))

$$\forall A \forall B \forall x (x \in A \iff x \in B) \iff A = B.$$

Intensionality (内涵) *vs.* Extensionality (外延)

Definition (函数的外延性原则)

$$f = g \iff \mathrm{dom}(f) = \mathrm{dom}(g) \land (\forall x \in \mathrm{dom}(f) : f(x) = g(x))$$

Special Functions (*-jectivity*)

Definition (Injective (one-to-one; 1-1) 单射函数)

$$f : A \to B$$

$$\forall a_1, a_2 \in A : a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$$

Definition (Injective (one-to-one; 1-1) 单射函数)

$$f : A \to B \qquad f : A \rightarrowtail B$$

$$\forall a_1, a_2 \in A : a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$$

Definition (Injective (one-to-one; 1-1) 单射函数)

$$f : A \to B \qquad f : A \rightarrowtail B$$

$$\forall a_1, a_2 \in A : a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$$

For Proof:

- To prove that f *is* 1-1:

$$\forall a_1, a_2 \in A : f(a_1) = f(a_2) \implies a_1 = a_2$$

Definition (Injective (one-to-one; 1-1) 单射函数)

$$f : A \to B \qquad f : A \rightarrowtail B$$

$$\forall a_1, a_2 \in A : a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$$

For Proof:

- To prove that f *is* 1-1:

$$\forall a_1, a_2 \in A : f(a_1) = f(a_2) \implies a_1 = a_2$$

- To show that f *is not* 1-1:

$$\exists a_1, a_2 \in A : a_1 \neq a_2 \wedge f(a_1) = f(a_2)$$

Definition (Surjective (onto) 满射函数)

$$f : A \to B$$

$$\mathrm{ran}(f) = B$$

Definition (Surjective (onto) 满射函数)

$$f : A \to B \qquad f : A \twoheadrightarrow B$$

$$\mathsf{ran}(f) = B$$

Definition (Surjective (onto) 满射函数)

$$f : A \to B \qquad f : A \twoheadrightarrow B$$

$$\text{ran}(f) = B$$

For Proof:

- To prove that f *is* onto:

$$\forall b \in B \left(\exists a \in A : f(a) = b \right)$$

Definition (Surjective (onto) 满射函数)

$$f : A \to B \qquad f : A \twoheadrightarrow B$$

$$\mathrm{ran}(f) = B$$

For Proof:

- To prove that f *is* onto:

$$\forall b \in B \left(\exists a \in A : f(a) = b \right)$$

- To show that f *is not* onto:

$$\exists b \in B \left(\forall a \in A : f(a) \neq b \right)$$

Theorem (Cantor Theorem (ES Theorem 24.4))

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Proof.

Proof. Let A be a set and let $f : A \to 2^A$. To show that f is not onto, we must find a $B \in 2^A$ (i.e., $B \subseteq A$) for which there is no $a \in A$ with $f(a) = B$. In other words, B is a set that f "misses." To this end, let

$$B = \{x \in A : x \notin f(x)\}.$$

We claim there is no $a \in A$ with $f(a) = B$.

Suppose, for the sake of contradiction, there is an $a \in A$ such that $f(a) = B$. We ponder: Is $a \in B$?

- If $a \in B$, then, since $B = f(a)$, we have $a \in f(a)$. So, by definition of B, $a \notin f(a)$; that is, $a \notin B$. $\Rightarrow\Leftarrow$
- If $a \notin B = f(a)$, then, by definition of B, $a \in B$. $\Rightarrow\Leftarrow$

Both $a \in B$ and $a \notin B$ lead to contradictions, and hence our supposition [there is an $a \in A$ with $f(a) = B$] is false, and therefore f is not onto. ■

□

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Theorem (Cantor Theorem)

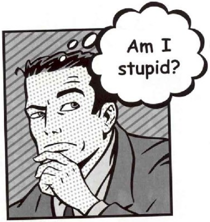
Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.



Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Understanding this problem:

$$A = \{1, 2, 3\}$$

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Understanding this problem:

$$A = \{1, 2, 3\}$$

2^A

$$2^A = \Big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\Big\}$$

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Understanding this problem:

$$A = \{1, 2, 3\}$$

2^A

$$2^A = \Big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\Big\}$$

Onto

$$\forall B \in 2^A \ \Big(\exists a \in A \ f(a) = B\Big).$$

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Understanding this problem:

$$A = \{1, 2, 3\}$$

2^A

$$2^A = \Big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\Big\}$$

Onto

$$\forall B \in 2^A \left(\exists a \in A \ f(a) = B\right).$$

Not Onto

$$\exists B \in 2^A \left(\forall a \in A \ f(a) \neq B\right).$$

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Proof.

$\square$

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Proof.

- Constructive proof ($\exists$):

$$B = \{x \in A \mid x \notin f(x)\}.$$

$\square$

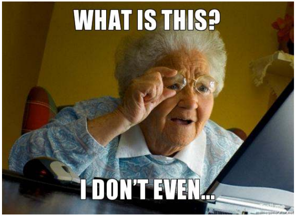
Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

Proof.

- Constructive proof ($\exists$):

$$B = \{x \in A \mid x \notin f(x)\}.$$



$\square$

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

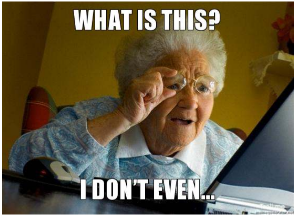
Proof.

- Constructive proof ($\exists$):

$$B = \{x \in A \mid x \notin f(x)\}.$$

- By contradiction ($\forall$):

$$\exists a \in A : f(a) = B.$$



$\square$

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

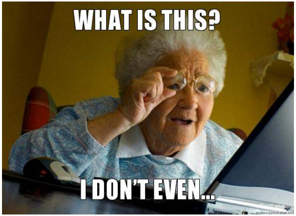
Proof.

- Constructive proof ($\exists$):

$$B = \{x \in A \mid x \notin f(x)\}.$$

- By contradiction ($\forall$):

$$\exists a \in A : f(a) = B.$$



$Q : a \in B?$

$\square$

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

对角线论证 (Cantor's diagonal argument) .

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

对角线论证 (Cantor's diagonal argument) .

a	$f(a)$					
	1	2	3	4	5	$\cdots$
1	1	1	0	0	1	$\cdots$
2	0	0	0	0	0	$\cdots$
3	1	0	0	1	0	$\cdots$
4	1	1	1	1	1	$\cdots$
5	0	1	0	1	0	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ldots$

□

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

对角线论证 (Cantor's diagonal argument) .

a	$f(a)$					
	1	2	3	4	5	$\cdots$
1	1	1	0	0	1	$\cdots$
2	0	0	0	0	0	$\cdots$
3	1	0	0	1	0	$\cdots$
4	1	1	1	1	1	$\cdots$
5	0	1	0	1	0	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ldots$

$\square$

Theorem (Cantor Theorem)

Let A be a set.
If $f : A \to 2^A$, then f is not onto.

对角线论证 (Cantor's diagonal argument) .

a	$f(a)$					
	1	2	3	4	5	$\cdots$
1	1	1	0	0	1	$\cdots$
2	0	0	0	0	0	$\cdots$
3	1	0	0	1	0	$\cdots$
4	1	1	1	1	1	$\cdots$
5	0	1	0	1	0	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$

$$B = \{0, 1, 1, 0, 1\}$$

□

Theorem (Cantor Theorem)

Let A be a set.
If $f: A \to 2^A$, then f is not onto.

对角线论证 (Cantor's diagonal argument) (以下仅适用于可数集合 A).

a	$f(a)$					
	1	2	3	4	5	$\cdots$
1	1	1	0	0	1	$\cdots$
2	0	0	0	0	0	$\cdots$
3	1	0	0	1	0	$\cdots$
4	1	1	1	1	1	$\cdots$
5	0	1	0	1	0	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$

$$B = \{0, 1, 1, 0, 1\}$$

Definition (Bijective (one-to-one correspondence) 一一对应)

$$f : A \to B \qquad f : A \quad B$$

1-1 & onto

cardinality

proof examples

Operations on Functions

Definition (Intersection, Union)

$$f_1, f_2 : A \to B$$

(i) Q : Is $f_1 \cup f_2$ a function from A to B?

(ii) Q : Is $f_1 \cap f_2$ a function from A to B?

Definition (Composition)

$$f : A \to B \qquad g : C \to D$$

$$\text{ran}(f) \subseteq C$$

The composition function

$$g \circ f : A \to D$$

$$(g \circ f)(x) = g(f(x))$$

Definition (Composition)

$$f : A \to B \qquad g : C \to D$$

$$\text{ran}(f) \subseteq C$$

The composition function

$$g \circ f : A \to D$$

$$(g \circ f)(x) = g(f(x))$$

Non-commutative:

$$f \circ g \neq g \circ f$$

Theorem (Associative Property for Composition)

$$f : A \to B \quad g : B \to C \quad h : C \to D$$

$$h \circ (g \circ f) = (h \circ g) \circ f$$

Theorem (Associative Property for Composition)

$$f : A \to B \quad g : B \to C \quad h : C \to D$$

$$h \circ (g \circ f) = (h \circ g) \circ f$$

Proof.

(i)

$$\mathsf{dom}(h \circ (g \circ f)) = \mathsf{dom}((h \circ g) \circ f)$$

(ii)

$$(h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)$$

□

Theorem (Properties of Composition (UD Theorem 15.7))

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

(i) *If f, g are injective, then $g \circ f$ is injective.*

(ii) *If f, g are surjective, then $g \circ f$ is surjective.*

(iii) *If f, g are bijective, then $g \circ f$ is bijective.*

Theorem (Properties of Composition (UD Theorem 15.7))

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

(i) *If* f, g *are injective, then* $g \circ f$ *is injective.*
(ii) *If* f, g *are surjective, then* $g \circ f$ *is surjective.*
(iii) *If* f, g *are bijective, then* $g \circ f$ *is bijective.*

Proof for (i).

$$\forall a_1, a_2 \in A \Big((g \circ f)(a_1) = (g \circ f)(a_2) \implies a_1 = a_2 \Big)$$

$\square$

Theorem (Properties of Composition (UD Theorem 15.8))

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

(i) *If $g \circ f$ is injective, then f is injective.*
(ii) *If $g \circ f$ is surjective, then g is surjective.*
(iii) *If $g \circ f$ is bijective, then f is injective and g is surjective.*

Cancellation Property for Composition (Problem 15.11)

$$f : A \to B \qquad g_1, g_2 : B \to A$$

$$f \circ g_1 = f \circ g_2 \land f \text{ is bijective} \implies g_1 = g_2$$

Cancellation Property for Composition (Problem 15.11)

$$f : A \to B \qquad g_1, g_2 : B \to A$$

$$f \circ g_1 = f \circ g_2 \land f \text{ is bijective} \implies g_1 = g_2$$

Proof.

f is one-to-one.

□

Definition (Inverse)

Let $f : A \to B$ be a bijective function.
The inverse of f is the function $f^{-1} : B \to A$ defined by

$$f^{-1}(b) = a \iff f(a) = b.$$

"Bijective" Requirement of f^{-1}:

$$f : A \to B \quad f \subseteq A \times B$$

Definition (Inverse)

Let $f : A \to B$ be a bijective function.
The inverse of f is the function $f^{-1} : B \to A$ defined by

$$f^{-1}(b) = a \iff f(a) = b.$$

"Bijective" Requirement of f^{-1}:

$$f : A \to B \quad f \subseteq A \times B$$

$$f^{-1} \subseteq B \times A \quad \text{(as a relation)}$$

Definition (Inverse)

Let $f : A \to B$ be a bijective function.
The inverse of f is the function $f^{-1} : B \to A$ defined by

$$f^{-1}(b) = a \iff f(a) = b.$$

"Bijective" Requirement of f^{-1}:

$$f : A \to B \quad f \subseteq A \times B$$

$$f^{-1} \subseteq B \times A \quad \text{(as a relation)}$$

$$f^{-1} : X \ (\subseteq B) \to A \quad \text{(as a function to } A\text{)}$$

Definition (Inverse)

Let $f : A \to B$ be a bijective function.
The inverse of f is the function $f^{-1} : B \to A$ defined by

$$f^{-1}(b) = a \iff f(a) = b.$$

"Bijective" Requirement of f^{-1}:

$$f : A \to B \quad f \subseteq A \times B$$

$$f^{-1} \subseteq B \times A \quad \text{(as a relation)}$$

$$f^{-1} : X\ (\subseteq B) \to A \quad \text{(as a function to } A\text{)}$$

$$f^{-1} : B \to A \quad \text{(as a function from } B \text{ to } A\text{)}$$

Theorem ((UD Theorem 15.4 (ii)))

$$f : A \to B \textit{ is bijective} \implies f^{-1} \textit{ is bijective.}$$

Theorem (Solving Equations (UD Theorem 15.4))

$$f : A \to B \text{ is bijective}$$

(i) $f \circ f^{-1} = i_B$

(ii) $g : B \to A \wedge f \circ g = i_B \implies g = f^{-1}$

(iii) $f^{-1} \circ f = i_A$

(iv) $g : B \to A \wedge g \circ f = i_A \implies g = f^{-1}$

Theorem (Solving Equations (UD Theorem 15.4))

$$f : A \to B \textit{ is bijective}$$

(i) $f \circ f^{-1} = i_B$

(ii) $g : B \to A \land f \circ g = i_B \implies g = f^{-1}$

(iii) $f^{-1} \circ f = i_A$

(iv) $g : B \to A \land g \circ f = i_A \implies g = f^{-1}$

Solving the equations:

$$f \circ g = i_B \qquad g \circ f = i_A$$

Bijective $\Longrightarrow$ Inverse:

$$f : A \to B \text{ is bijective}$$

$$\Longrightarrow$$

$$\exists g : B \to A \left(f \circ g = i_B \land g \circ f = i_A \right)$$

Bijective $\implies$ Inverse:

$$f : A \to B \text{ is bijective}$$

$$\implies$$

$$\exists g : B \to A \left(f \circ g = i_B \land g \circ f = i_A \right) \land g = f^{-1}$$

Bijective $\implies$ Inverse:

$$f : A \to B \text{ is bijective}$$

$$\implies$$

$$\exists g : B \to A \left(f \circ g = i_B \land g \circ f = i_A \right) \land g = f^{-1}$$

Theorem (Inverse $\implies$ Bijective (UD Theorem 15.8 (iii)))

$$\exists g : B \to A \left(g \circ f = i_A \land f \circ g = i_B \right)$$

$$\implies$$

$f : A \to B$ is bijective

Bijective $\implies$ Inverse:

$$f : A \to B \text{ is bijective}$$

$$\implies$$

$$\exists g : B \to A \left(f \circ g = i_B \land g \circ f = i_A\right) \land g = f^{-1}$$

Theorem (Inverse $\implies$ Bijective (UD Theorem 15.8 (iii)))

$$\exists g : B \to A \left(g \circ f = i_A \land f \circ g = i_B\right)$$

$$\implies$$

$$f : A \to B \textit{ is bijective} \land g = f^{-1}$$

Theorem (Inverse of Composition (UD Theorem 15.6))

$$f : A \to B, g : B \to C \text{ are bijective}$$

(i) $g \circ f$ *is bijective*

(ii) $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

Proof for (ii).

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = i_A$$

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = i_B$$

□

Definition (Symmetric Group)

Let A be a set.
Consider all bijective functions on A and the composition ($\circ$) operator.

(i) $f \circ g$ is a bijective function on A

(ii) $h \circ (\circ g \circ f) = (h \circ g) \circ f$

(iii) $f \circ id_A = f = id_A \circ f$

(iv) $f \circ f^{-1} = id_A = f^{-1} \circ f$

$$f : X \to Y \quad A \subseteq X \quad B \subseteq Y$$

Definition (Image)

The image of A under f is the set

$$f(A) = \{f(a) \mid a \in A\}.$$

Definition (Inverse Image)

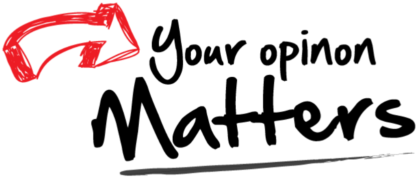
The inverse image of B under f is the set

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}.$$

$$Q_1 : A \textit{ vs. } f^{-1}(f(A))$$

$$Q_2 : B \textit{ vs. } f(f^{-1}(B))$$


Thank
You!



Office 302

Mailbox: H016

hfwei@nju.edu.cn