Discrete Mathematics II : Glynn Winskel

"Set Theory for Computer Science"

The concept of set (an unordered collection) is as universally important as the concept of number.

Originally intended as a foundation for Logic & Mathematics, Set Theory plays a fundamental role in design, understanding & reasoning in CS.

History

19c. Boole, de Morgan, Venn
Simple logic is simple set theory,
Properties, propositions as sets.

19c. Cantor
The power of sets,
Size of sets.

19c - 20c Frege, Russell & Whitehead ...
Zermelo, Fraenkel.
The re-invention of Logic to formalize all Mathematics.

1930's Gödel, Church, Turing
Proof as computation.
The birth of CS!

Set Theory is pervasive in C.S

∵ CS roots lie in Set Theory.

∵ CS needs mathematics.

∵ CS as a science of the artificial looks to Set Theory for inspiration: databases, logic programming, types, functions, grammars, ...

∵ Set Theory provides tools for describing & reasoning about processes of generation (inductive definitions).

The course:

Ch 1 Sets & Logic

Ch 2 Relations, functions & size of sets

Ch 3 Constructions on sets

Ch 4 Inductive definitions

Ch 5 Well-founded induction

Mini-Seminars

To help you do proofs, communicate proofs, engage with the course.
(See also introductory part of Ch. 1.)

Sets

A set is an (unordered) collection of elements.

Examples

$\emptyset$, or $\{\}$, the emptyset.

$\mathbb{N} = \{1, 2, 3, \cdots\}$ the set of natural numbers.

$\mathbb{N}_0 = \{0, 1, 2, 3, \cdots\}$.

U the set of students taking this course.

Fundamental Relations

Let A be a set.

$$x \in A$$

means x is an element of A, or
x is a member of A.

Let A, B be sets.

$A = B$ means A and B have the same elements, i.e.

$$\forall x.\ x \in A \Leftrightarrow x \in B.$$

$A \subseteq B$ means $\forall x.\ x \in A \Rightarrow x \in B.$

($\subseteq$: inclusion / subset)

Simple consequence:

$A = B$ iff $A \subseteq B$ and $B \subseteq A$.

('if and only if' $\Leftrightarrow$)

Defining sets by properties

We often describe a set by a property, for example,

$$\text{Even} = \{ x \mid x \in \mathbb{N} \;\&\; \exists y \in \mathbb{N}.\; x = 2y \},$$

or

$$\text{Even} = \{ x \in \mathbb{N} \mid \exists y \in \mathbb{N}.\; x = 2y \}.$$

The collection of all elements x satisfying a property $P(x)$:

$$\{ x \mid P(x) \}$$

The collection of all elements x of a set S satisfying property $P(x)$:

$$\{ x \in S \mid P(x) \}$$

Exercise

Let S be the set of strings over symbols a, b.

Describe the sets

$$\{x \in S \mid ax = xa\},$$

$$\{x \in S \mid ax = xb\}.$$

Operations on sets

Assume a set U.

Let $A \subseteq U$ and $B \subseteq U$.

Define

union

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$$

intersection

$$A \cap B = \{x \mid x \in A \ \& \ x \in B\}$$

complement

$$A^c = \{x \in U \mid x \notin A\}$$

As Venn diagrams ...

Applying Venn diagrams, an example

In a class all students take one or more of

$A = \{x \mid x \text{ does Arithmetic}\}$

$B = \{x \mid x \text{ does Biology}\}$

$C = \{x \mid x \text{ does Chemistry}\}$

so that

65 do Arith

35 do Bio

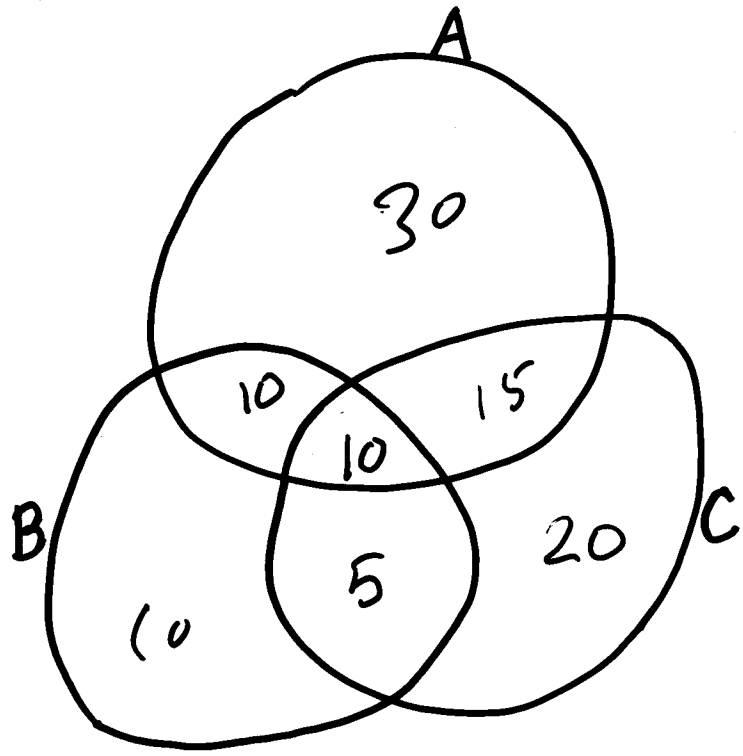
50 do Chem

20 do Arith & Bio

15 do Bio & Chem

25 do Chem & Arith

10 do Arith & Bio & Chem.



What is the no. of students?

Laws for sets, a sample.

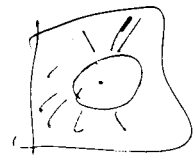
Let $A, B, C \subseteq U$.

$$A \cup (B \cup C) = (A \cup B) \cup C$$

$$A \cup B = B \cup A$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$(A^c)^c = A$$



$$A \cup A^c = U$$

$$(A \cup B)^c = A^c \cap B^c$$

The Boolean identities for sets: Let A, B range over subsets of U:

Associativity	$A \cup (B \cup C) = (A \cup B) \cup C$	$A \cap (B \cap C) = (A \cap B) \cap C$
Commutativity	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Idempotence	$A \cup A = A$	$A \cap A = A$
Empty set	$A \cup \emptyset = A$	$A \cap \emptyset = \emptyset$
Universal set	$A \cup U = U$	$A \cap U = A$
Distributivity	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Absorption	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
Complements	$A \cup A^c = U$	$A \cap A^c = \emptyset$
	$(A^c)^c = A$	
De Morgan's laws	$(A \cup B)^c = A^c \cap B^c$	$(A \cap B)^c = A^c \cup B^c$

Identities on sets allow us to deduce inclusions because

Proposition

$$A \subseteq B \quad \text{iff} \quad A \cap B = A.$$

$$A \subseteq B \quad \text{iff} \quad A \cup B = B.$$

Exercise

Let $A, B \subseteq U$. Then,

$$A \subseteq B \quad \text{iff} \quad A^c \cup B = U.$$

$$A \subseteq B \quad \text{iff} \quad A \cap B^c = \emptyset.$$

$A \subseteq B$ iff A

Properties as sets

Property	'Extension' as a set
$P(x)$	$\{x \in U \mid P(x)\}$
$Q(x)$ & $R(x)$	$\{x \in U \mid Q(x)\} \cap \{x \in U \mid R(x)\}$
$Q(x)$ or $R(x)$	$\{x \in U \mid Q(x)\} \cup \{x \in U \mid R(x)\}$
$\neg P(x)$	$\{x \in U \mid P(x)\}^c$
$Q(x) \Rightarrow R(x)$	$\{x \in U \mid Q(x)\}^c \cup \{x \in U \mid R(x)\}$

x is a man
x is a male homosapiens
} $\{x \mid x \text{ is a man}\}$

- Logical operations corr. to Boolean operations.
- Equivalence of properties corr. to equality of sets.

GEORGE BOOLE

'Laws of Thought'

Interpret

properties, eg. "x is an even no."

propositions, eg. "It's raining"

as sets.

Propositional Logic

The study of Boolean propositions

eg.

- It's sunny $\wedge$ Dave wears sunglasses
  $\wedge \neg$ (Lucy carries an umbrella.)

- Being a student of Emmanuel $\Rightarrow$
  Having a driving licence

- Wire g is high $\Rightarrow$ (Wire s is high $\Leftrightarrow$ Wire d is high.)

and the relations of equivalence and entailment between them.

Boolean propositions

$$A, B, \cdots ::= a, b, c, \cdots \mid \top \mid \bot \mid A \wedge B \mid A \vee B \mid \neg A$$

$a, b, c, \cdots \in \mathit{Var}$, a set of propositional variables.

Abbreviations

$$A \Rightarrow B \equiv (\neg A) \vee B$$

$$A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$$

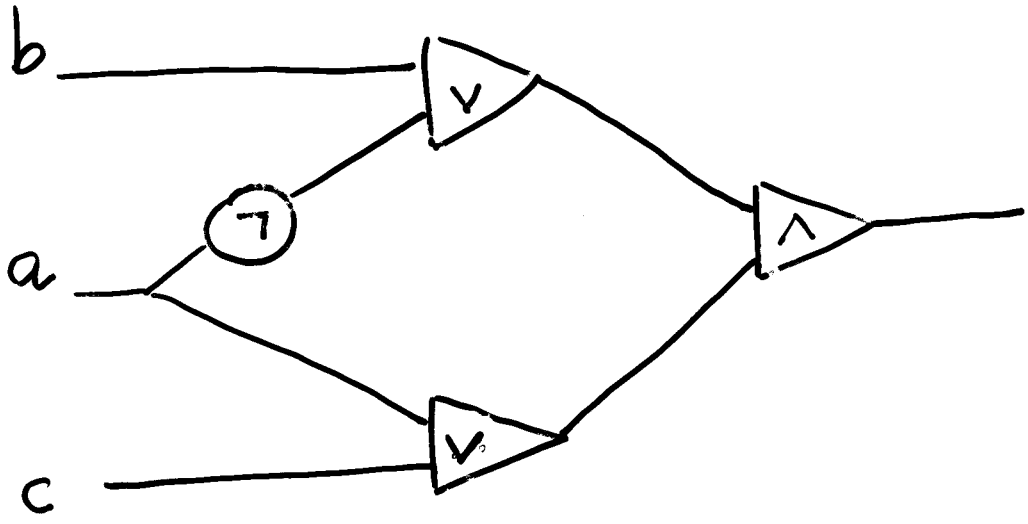
Boolean propositions realised as Boolean circuits

a, b, c, $\cdots$ correspond to input wires which can either be high (T) or low (F).

For example,

$$(\neg a \vee b) \wedge (a \vee c)$$

is realised as



An example, $(a \wedge b) \vee \neg a$

a	b	$\neg a$	$a \wedge b$	$(a \wedge b) \vee \neg a$
F	F	T	F	**T**
F	T	T	F	**T**
T	F	F	F	**F**
T	T	F	T	**T**

Evaluating Boolean propositions – Truth tables

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$\neg A \vee B$ $A \Rightarrow B$
F	F	T	F	F	T
F	T	T	F	T	T
T	F	F	F	F	F
T	T	F	T	T	T

So

'Pigs can fly $\Rightarrow$ I'm a professor' and

'Pigs can fly $\Rightarrow$ I'm the king of France'

are both true!

$\Rightarrow$ 'material implication'

Boolean propositions as sets

Idea:

Regard a Boolean proposition as a property of situations / states / individuals / things within some set of possibilities $\mathcal{U}$.

An interpretation of Boolean propositions should

- fix the interpretation of $a, b, c \ldots$ as sets $[\![a]\!], [\![b]\!], [\![c]\!], \ldots \subseteq \mathcal{U}$
- respect the intended meaning of $\mathsf{T}, \mathsf{F}, \wedge, \vee, \neg$.

Eg.

$\mathcal{U}$ = set of students at this class, ...

A model $\mathcal{M}$ for Boolean propositions comprises

a set $U_{\mathcal{M}}$, the universe of $\mathcal{M}$,

together with an interpretation

$$[\![A]\!]_{\mathcal{M}} \subseteq U_{\mathcal{M}}$$

of all propositions A such that

$$[\![T]\!]_{\mathcal{M}} = U_{\mathcal{M}} \qquad [\![F]\!]_{\mathcal{M}} = \emptyset$$

$$[\![A \wedge B]\!]_{\mathcal{M}} = [\![A]\!]_{\mathcal{M}} \cap [\![B]\!]_{\mathcal{M}}$$

$$[\![A \vee B]\!]_{\mathcal{M}} = [\![A]\!]_{\mathcal{M}} \cup [\![B]\!]_{\mathcal{M}}$$

$$[\![\neg A]\!]_{\mathcal{M}} = [\![A]\!]_{\mathcal{M}}^{c}.$$

Example of a model $\mathcal{S}$

Model $\mathcal{S}$ comprises

$U_{\mathcal{S}}$ = set of students of this class,

and the interpretation for which

$$[\![a]\!]_{\mathcal{S}} = \{x \in U_{\mathcal{S}} \mid x \text{ is from Enuma}\}$$

$$[\![b]\!]_{\mathcal{S}} = \{x \in U_{\mathcal{S}} \mid x \text{ has a driving licence}\}$$

$$[\![c]\!]_{\mathcal{S}} = \{x \in U_{\mathcal{S}} \mid x \text{ is from Churchill}\}$$

$$\vdots$$

$$[\![A \wedge B]\!]_{\mathcal{S}} = [\![A]\!]_{\mathcal{S}} \cap [\![B]\!]_{\mathcal{S}} \qquad [\![T]\!]_{\mathcal{S}} = U_{\mathcal{S}}$$

$$[\![A \vee B]\!]_{\mathcal{S}} = [\![A]\!]_{\mathcal{S}} \cup [\![B]\!]_{\mathcal{S}} \qquad [\![F]\!]_{\mathcal{S}} = \emptyset$$

$$[\![\neg A]\!]_{\mathcal{S}} = [\![A]\!]_{\mathcal{S}}^{c}$$

[Example of definition by Structural induction P.22]

Example of a model $\mathcal{H}$.

Label connection points on a circuit board a, b, c, ...

Model $\mathcal{H}$ comprises

$\mathcal{U}_{\mathcal{H}}$ = set of assignments of 'high' or 'low' to connection points,

and the interpretation for which

$$[\![a]\!]_{\mathcal{H}} = \{ V \in \mathcal{U}_{\mathcal{H}} \mid V_a = \text{'high'} \}$$

$$[\![b]\!]_{\mathcal{H}} = \{ V \in \mathcal{U}_{\mathcal{H}} \mid V_b = \text{'high'} \}$$

$$\vdots$$

Validity & Entailment

Let A, B be Boolean propositions.

A is valid in $\mathcal{M}$

iff $[\![A]\!]_{\mathcal{M}} = U_{\mathcal{M}}$.

A entails B in $\mathcal{M}$

iff $[\![A]\!]_{\mathcal{M}} \subseteq [\![B]\!]_{\mathcal{M}}$.

A is valid, $\models A$,

iff A is valid in all models $\mathcal{M}$.

A entails B, $A \models B$,

iff A entails B in all models $\mathcal{M}$.

$A = B$ iff $A \models B$ and $B \models A$.

Proposition $A \models B$ iff $\models A \Rightarrow B$.

Truth assignments

A truth assignment is an assignment of a unique truth value T F to each propositional variable.

E.g. $\{aT, bF, cT, \dots\}$.

The model τ_A

$U_{\tau A}$ = set of all truth assignments

$[\![a]\!]_{\tau A} = \{t \in U_{\tau A} \mid aT \in t\}$

$[\![T]\!]_{\tau A} = U_{\tau A}$ $\quad$ $[\![F]\!]_{\tau A} = \emptyset$

$[\![A \wedge B]\!]_{\tau A} = [\![A]\!]_{\tau A} \cap [\![B]\!]_{\tau A}$

$[\![A \vee B]\!]_{\tau A} = [\![A]\!]_{\tau A} \cup [\![B]\!]_{\tau A}$

$[\![\neg A]\!]_{\tau A} = [\![A]\!]^{c}_{\tau A}$

A definition by structural induction [P.22]

Structural induction for Boolean propositions:

To show IH holds for all Boolean propositions, it suffices to show

IH holds for all $a \in Var$, $\top$, $\bot$.

If IH holds for A and B, then IH holds for $A \vee B$.

If IH holds for A and B, then IH holds for $A \wedge B$.

If IH holds for A, then IH holds for $\neg A$.

Lemma 1.12 $\vdash A$ iff A is valid in $\mathcal{TA}$.

Proof: "only if": As $\mathcal{TA}$ is a particular model.

"if": Let $\mathcal{M}$ be a model.

For $u \in \mathcal{U}_{\mathcal{M}}$ define $t(u) \in \mathcal{U}_{\mathcal{TA}}$ by

$$t(u) = \{aT \mid a \in Var \;\&\; u \in [\![a]\!]_{\mathcal{M}}\} \cup \{aF \mid a \in Var \;\&\; u \notin [\![a]\!]_{\mathcal{M}}\}.$$

Claim: For all propositions A,

$$u \in [\![A]\!]_{\mathcal{M}} \text{ iff } t(u) \in [\![A]\!]_{\mathcal{TA}}. \quad \text{(IH)}$$

We prove this by structural induction on propositions A. [P. 22-23] ... □

Corollary 1.13

$$A \vdash B \text{ iff } [\![A]\!]_{\mathcal{TA}} \subseteq [\![B]\!]_{\mathcal{TA}}.$$

Proposition 1.14

$\models A$ iff A is a tautology

[ie. truth table for A yields T for all truth assignments to propl. variables]

Proof idea [P.25]:

$\models A$ iff A is valid in $\mathcal{I}A$

A truth assignment

$t = \{aT, \quad bF, \quad cT, \quad \cdots\}$

corresponds to a row in truth table:

a	b	c	⋯	A
⋮	⋮	⋮		⋮
T	F	T	⋯	T
⋮	⋮	⋮		⋮

□

↝
- A tautology is valid in all models
- Can simplify Boolean expressions using laws of sets (reading $\vee, \wedge, \neg$ as $\cup, \cap, (\,)^c$).