Discrete Mathematics : 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.

Set Theory is pervasive in CS

$\because$ CS roots lie in Set Theory.

$\because$ CS needs mathematics.

$\because$ CS as a science of the artificial looks to Set Theory for inspiration: databases, logic programming, types, functions, grammars, …

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

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, Frænkel.

The re-invention of Logic to formalize all Mathematics.

1930's Gödel, Church, Turing

Proof as computation.
The birth of CS!

The course:

Ch. 1 Mathematical induction

Ch. 2 Sets & logic

Ch. 3 Relations, functions & size of sets

Ch. 4 Constructions on sets

Ch. 5 Inductive definitions

Ch. 6 Well-founded induction

Mini-Seminars

To help you do proofs, communicate proofs, engage with the course.
(See also 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.

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

$\mathcal{U}$ 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 $\forall x.\ x \in A \Rightarrow x \in B.$

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,

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

or

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

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 $P(x)$:

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

$\varepsilon \quad a \quad aa \quad ab \quad ba$

Exercise

Let S be the set of strings over symbols a, b (with $a \neq b$).

Describe the sets

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

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

$\varepsilon \quad a \quad aa \quad ab \quad ba$

Exercise

Let S be the set of strings over symbols a, b (with $a \neq b$).

Describe the sets

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

Proposition $\{x \in S \mid ax = xb\} = \emptyset$

Proof. By contradiction. Assume $\{x \in S \mid ax = xb\} \neq \emptyset$. Then there is a string x of least length s.t. ~~$ax=xb$~~.

$$ax = xb.$$

$\therefore \quad x = sb$ for some string s.

$$\therefore \quad asb = sbb$$

$$\therefore \quad as = sb$$

But s has smaller length than x.

$\rightarrow$ a contradiction.

$\therefore \quad \{x \in S \mid ax = xb\} = \emptyset \quad \square$

Operations on sets

Assume a set $\mathcal{U}$.

Let $A \subseteq \mathcal{U}$ and $B \subseteq \mathcal{U}$.

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

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

As Venn diagrams ...

Applying Venn diagrams, an example

In a class all students take one or more of

Arithmetic

Biology

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?

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

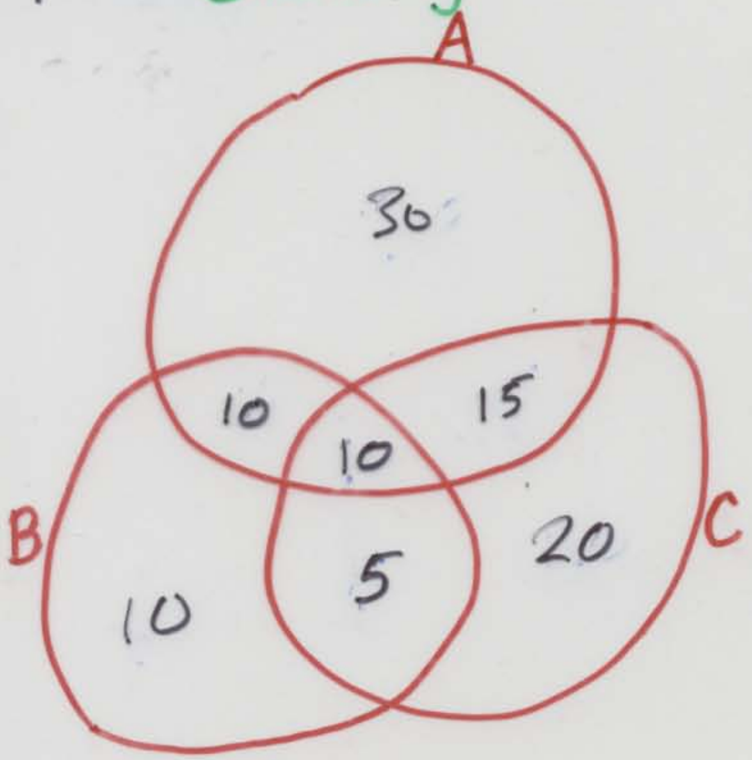
50 do Chem

20 do Arith & Bio

15 do Bio & Chem

25 do Chem & Arith

10 do Arith & Bio & Chem.



What is the no. of students?

John Venn

John Venn

Laws for sets, a sample.

Let $A, B, C \subseteq \mathcal{U}$.

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

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

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

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

$$A \cup A^c = \mathcal{U}$$

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

Augustus de Morgan

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.
- Entailment between properties corr. to inclusion 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

e.g.

- 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

$$
\begin{aligned}
A, B, \cdots ::= \; & a, b, c, \cdots \mid \\
& T \mid \\
& F \mid \\
& A \wedge B \mid \\
& A \vee B \mid \\
& \neg A
\end{aligned}
$$

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

Abbreviations

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

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

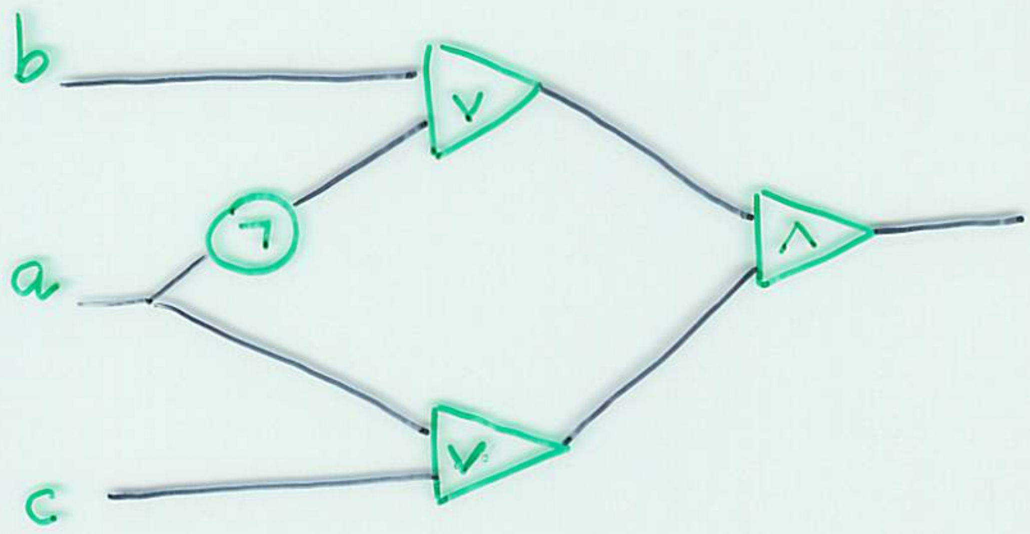
Boolean propositions realised as Boolean circuits

$a, b, c, \dots$ 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



Evaluating Boolean propositions - Truth tables

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

$\Rightarrow$ is 'material implication'

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	
F	T	T	F	
T	F	F	F	
T	T	F	T	

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

Boolean propositions as sets

Idea:

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

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

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

Example of a model S

Model S comprises

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

and the interpretation for which

$$[\![a]\!]_S = \{x \in \mathcal{U}_S \mid x \text{ is from Emma}\}$$

$$[\![b]\!]_S = \{x \in \mathcal{U}_S \mid x \text{ has a driving licence}\}$$

$$[\![c]\!]_S = \{x \in \mathcal{U}_S \mid x \text{ is from Churchill}\}$$

$$\vdots$$

$$[\![A \wedge B]\!]_S = [\![A]\!]_S \cap [\![B]\!]_S \qquad [\![T]\!]_S = \mathcal{U}_S$$

$$[\![A \vee B]\!]_S = [\![A]\!]_S \cup [\![B]\!]_S \qquad [\![F]\!]_S = \emptyset$$

$$[\![\neg A]\!]_S = [\![A]\!]_S^{\,c}$$

[Example of definition by structural induction.]

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

Label connection points on a circuit board $a, b, c, \ldots$

Model $\mathcal{H}$ comprises

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

and the interpretation for which

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

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

$$\vdots$$

A model $\mathcal{M}$ for Boolean propositions comprises
a set $\mathcal{U}_{\mathcal{M}}$, the universe of $\mathcal{M}$,
together with an interpretation

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

of all propositons A such that

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

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

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

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

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 $\models A \Rightarrow B$.

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 $\models A \Rightarrow B$ $\quad [\![\neg A \vee B]\!]_{\mathcal{M}} = \mathcal{U}_{\mathcal{M}}$

$[\![A]\!]_{\mathcal{M}} \subseteq [\![B]\!]_{\mathcal{M}}$ iff $[\![A]\!]_{\mathcal{M}}^{c} \cup [\![B]\!]_{\mathcal{M}} = \mathcal{U}_{\mathcal{M}}$.

Structural induction for Boolean propositions:

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

IH holds for all $a \in Var$, T, F.

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 $\neg A$.