Discrete Mathematics (Cont)

Glynn Winskel

Lent 2005.

This part : Set theory

Originally intended as a foundation for Mathematics, Set Theory plays a basic role in formalising and reasoning about CS.

History : Boole, de Morgan, Venn ...
Peano, Cantor, Frege, Russell & Whitehead, ...
Gödel, Church, Turing ...

Sets

A set is an (unordered) collection A

Basic judgement $x \in A$ "member of"
"element of"

$$A = B \quad \text{iff} \quad \forall x.\ x \in A \Leftrightarrow x \in B$$

$$A \subseteq B \quad \text{iff} \quad \forall x.\ x \in A \Rightarrow x \in B$$

$\rightsquigarrow$ ways to show two sets are equal.

Examples of sets:

$\{a, b, c\}$

$\emptyset$ or $\{\}$ empty set

$\mathbb{N} = \{1, 2, 3, \cdots\}$ an infinite set!

$$\text{Primes} = \{x \in \mathbb{N} \mid x > 1 \ \& \ \forall y.\ 1 < y < x \Rightarrow \text{hcf}(x,y) = 1\}$$

Sets and Properties

Often describe a set by a property:

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

a property

Russell

Set X is called the extension of property $P(x)$.

A safe way to build sets:

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

a set

[This pre-supposes sufficiently big sets like $\mathbb{N}$, or ways to construct them Ch.3]

Most often, can work within some suff. big set "the universe of discourse" $\mathcal{U}$.

For $A, B \subseteq \mathcal{U}$

have basic operations:

<u>union</u> $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$

intersection $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$

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

From which derive

(set) difference $A \setminus B = A \cap B^c$

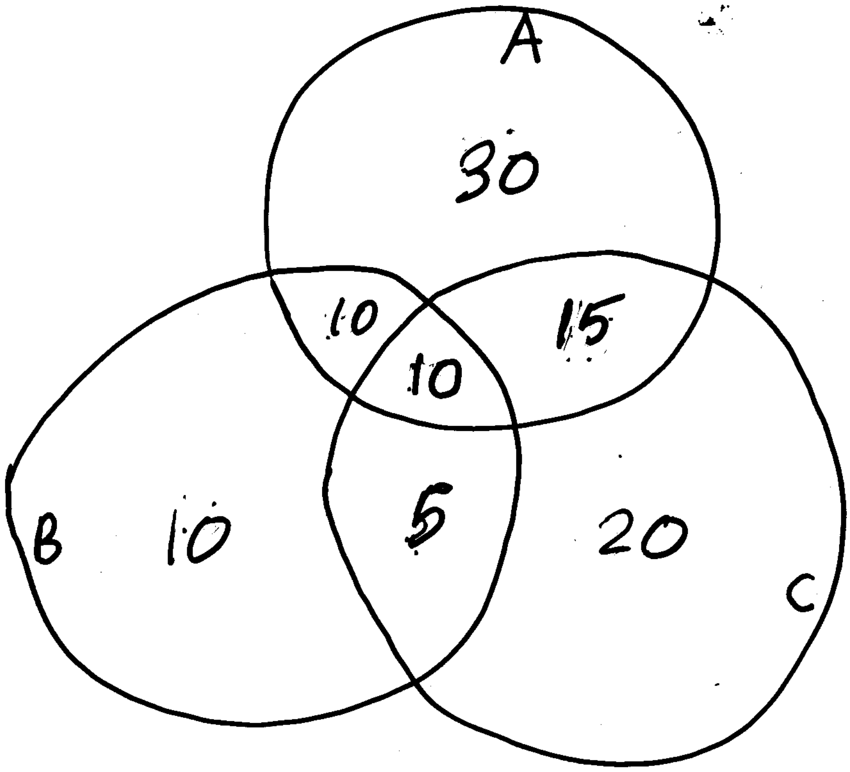
[symmetric difference $A \triangle B = (A \setminus B) \cup (B \setminus A)$]

Picture as Venn diagrams

An example applying Venn diagrams

Students take one or more of

Arithmetic	A
Biology	B
Chemistry	C



65 A

35 B

50 C

20 A & B

15 B & C

25 C & A

10 A & B & C

No. of students? 100

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

Recap: Sets & laws:

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

[cf. $A \times (B + C) = (A \times B) + (A \times C)$]

Eg. can derive

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

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

Laws for set operations $\cap$, $\cup$, $(\cdot)^c$ transfer to logical operations $\wedge$, $\vee$, $\neg$.

Boolean Propositions

$$A, B, \ldots ::= a, b, c, \ldots$$ propositional variables

$$\mid \text{true} \mid \text{false}$$

$$\mid A \wedge B \mid A \vee B \mid \neg A$$

conjunction disjunction negation

$A \Rightarrow B$ abbreviates $\neg A \vee B$

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

Truth table for $\neg, \wedge, \vee$.

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

a	b	$\neg b$	$a \wedge \neg b$
F	F	T	F
F	T	F	F
T	F	T	T
T	T	F	F

An interpretation (model):

$\mathcal{U}$ = school students

a attend arithmetic

b ·· biology

c ·· chemistry

Models for Boolean propositions

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

- a set $\mathcal{U}_{\mathcal{M}}$ of "states", universe of $\mathcal{M}$
- an interpretation $[\![A]\!]_{\mathcal{M}} \subseteq \mathcal{U}_{\mathcal{M}}$ of propositions A satisfying

$$[\![\mathrm{true}]\!]_{\mathcal{M}} = \mathcal{U}_{\mathcal{M}}$$

$$[\![\mathrm{false}]\!]_{\mathcal{M}} = \emptyset$$

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

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

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

[A model fixes the interpretation of propositional variables]

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 1.11 $A \models B$ iff $\models A \Rightarrow B$.

Structural induction for Boolean propositions:

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

IH holds for $a \in Var$, true, false.

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 $\neg A$.

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 τA

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

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

$$[\![\mathit{true}]\!]_{\tau A} = U_{\tau A} \qquad [\![\mathit{false}]\!]_{\tau A} = \emptyset$$

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

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

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

A definition by structural induction [P.20]

Lemma 1.12 $\models A$ 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,

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

We prove this by structural induction on propositions A. [P. 20-21] . . . $\square$

Corollary 1.13

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

Proposition 1.14

$\models A$ iff A is a tautology

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

Proof idea [P.23]:

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

A truth assignment

$t = \{aT, \ bF, \ cT, \ \dots\}$

corresponds to a row in truth table:

a	b	c	...	A
⋮	⋮	⋮		⋮
T	F	T	...	T
⋮	⋮	⋮		⋮

$\square$

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