Derivation of Algorithms

Lecture 1
Propositional Calculus

COMP H 4018
Lecturer: Stephen Sheridan

Laws of the Calculus

Let P, Q, R be propositions

1. Constants

   $P \vee true \equiv true$

   $P \vee false \equiv P$

   $P \wedge true \equiv P$

   $P \wedge false \equiv false$

   $true \Rightarrow P \equiv P$

   $false \Rightarrow P \equiv true$

   $P \Rightarrow true \equiv true$

   $P \Rightarrow false \equiv \neg P$

2. Law of excluded middle : $P \vee \neg P \equiv true$

3. Law of contradiction: $P \wedge \neg P \equiv false$

4 Negation : $\neg\neg P \equiv P$

5. Associativity: $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$

   $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$

6. Commutativity: $P \vee Q \equiv Q \vee P$

   $P \wedge Q \equiv Q \wedge P$

7. Idempotency: $P \vee P \equiv P$

   $P \wedge P \equiv P$

8. De Morgan's laws : $\neg (P \wedge Q) \equiv \neg P \vee \neg Q$

   $\neg (P \vee Q) \equiv \neg P \wedge \neg Q$

9. Implication $P \Rightarrow Q \equiv \neg P \vee Q$

   $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$

   $(P \wedge Q) \Rightarrow R \equiv P \Rightarrow (Q \Rightarrow R)$

10. (If and only if) $\equiv$: $P \equiv Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$

11. Absorption: $[P \wedge (P \vee R) \equiv P]$

$[P \vee (P \wedge R) \equiv P]$

12. Laws of distribution: $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$

$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$

13. **Predicate Calculus**

Universal Quantification

$[(\forall x : P(x)) \wedge (\forall x : Q(x)) \equiv (\forall x : P(x) \wedge Q(x))]$
$[(\forall x: P(x)) \vee (\forall x : Q(x)) \Rightarrow (\forall x: P(x) \vee Q(x))]$
$[Q \vee (\forall x : P(x)) \equiv (\forall x: Q \vee P(x))]$, where x not free in Q
$[Q \wedge (\forall x: P(x)) \equiv (\forall x: Q \wedge P(x))]$, where x not free in Q

Existential Quantification

$[(\exists x: P(x) \wedge Q(x)) \Rightarrow (\exists x : P(x)) \wedge (\exists x : Q(x))]$
$[(\exists x : P(x)) \vee (\exists x: Q(x)) \equiv (\exists x: P(x) \vee Q(x))]$
$[Q \vee (\exists x: P(x)) \equiv (\exists x : Q \vee P(x))]$, where x not free in Q
$[Q \wedge (\exists x: P(x)) \equiv (\exists x : Q \wedge P(x))]$, where x not free in Q
$[(\exists x : P(x)) \equiv \neg(\forall x: \neg P(x))]$
$[(\neg\exists x : P(x)) \equiv (\forall x: \neg P(x))]$

14. **Universal Quantification over Ranges**

$[\forall i : R : P \equiv \forall i : \neg R \vee P]$ Trading
$[\forall i : false : P \equiv true]$
$[\forall i : i = x : P \equiv P(i := x)]$ One-point rule
$[(\forall i : R : P) \wedge (\forall i : R : Q) \equiv (\forall i : R : P \wedge Q)]$
$[(\forall i : R : P) \wedge (\forall i : S : P) \equiv (\forall i : R \vee S : P)]$
$[(\forall i : R : P) \vee (\forall i : R : Q) \Rightarrow (\forall i : R : P \vee Q)]$
$[Q \vee (\forall i : R : P) \equiv (\forall i : R : Q \vee P)]$
$[Q \wedge (\forall i : R : P) \equiv (\forall i : R : Q \wedge P)]$

15. **Existential Quantification over Ranges**

$[\exists i : R : P \equiv \exists i : R \wedge P]$ Trading
$[\exists i : false : P \equiv false]$

[$\exists$i : i = x : P $\equiv$ P(i := x)]   One-point rule
[($\exists$i : R : P $\wedge$ Q) $\Rightarrow$ ($\exists$i : R : P) $\wedge$ ($\exists$i : R : Q)]
[($\exists$i : R : P) $\vee$ ($\exists$i : R : Q) $\equiv$ ($\exists$i : R : P $\vee$ Q)]
[Q $\vee$ ($\exists$i : R : P) $\equiv$ ($\exists$i : R : Q $\vee$ P)]
[Q $\wedge$ ($\exists$i : R : P) $\equiv$ ($\exists$i : R : Q $\wedge$ P)]

16. **Argument Forms**

Modus Ponens: $P \Rightarrow Q, P \therefore Q$
Modus Tollens: $P \Rightarrow Q, \neg Q \therefore \neg P$
Hypothetical Syllogism: $P \Rightarrow Q, Q \Rightarrow R \therefore P \Rightarrow R$
Disjunctive Syllogism: $P \vee Q, \neg P \therefore Q$
Simplification: $P \wedge Q \therefore P$
Conjunction: $P, Q \therefore P \wedge Q$
Addition: $P \therefore P \vee Q$
Constructive Dilemma: $(P \Rightarrow Q) \wedge (R \Rightarrow S), P \vee R \therefore Q \vee S$
Destructive Dilemma: $(P \Rightarrow Q) \wedge (R \Rightarrow S), \neg Q \vee \neg S \therefore \neg P \vee \neg R$

Propositional Calculus

Def Proposition

Any statement which is either true or false

e.g. 2 is odd $\equiv$ false
$7 > 4$ $\equiv$ true
$21 + 6 < 7$ $\equiv$ false

Operators

Negation	:	$\neg$
And	:	$\wedge$
Or	:	$\vee$
Implication	:	$\Rightarrow$
Equivalence	:	$\equiv$

Truth Tables

These are tables listing all possible truth values.

Let x, y be any propositions. The following table lists each operator together with their associated truth values.

x	y	$x \wedge y$	$x \vee y$	$x \Rightarrow y$	$x \equiv y$	$\neg x$
t	t	T	t	t	t	f
t	f	F	t	f	f	f
f	t	F	t	t	f	t
f	f	F	f	t	t	t

Order of precedence : $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\equiv$

Note on implication

$A \Rightarrow B \equiv \neg A \vee B$
$\downarrow$ $\searrow$
Antecedent Consequent

This equivalence is proved with the following truth table

A	B	$\neg$ A	$\neg A \vee B$	$A \Rightarrow B \equiv \neg A \vee B$	$A \Rightarrow B$
T	t	F	t	**t**	t
T	f	F	f	**t**	f
F	t	T	t	**t**	t
F	f	T	t	**t**	t

Examples

Ex 1 : Evaluate the truth or falsity of

(i) $(A \Rightarrow B) \Rightarrow C$
(ii) $(A \equiv B) \equiv [(A \Rightarrow B) \wedge (B \Rightarrow A)]$
for A = B = true and C = false.

(i) $(A \Rightarrow B) \Rightarrow C$
$\equiv$ { substitution }
$(\underline{true} \Rightarrow \underline{true}) \Rightarrow \underline{false}$
$\equiv \{ \Rightarrow \}$
$\underline{true} \Rightarrow \underline{false}$
$\equiv \{ \Rightarrow \}$
$\underline{false}$

(ii) $(A \equiv B) \equiv [(A \Rightarrow B) \wedge (B \Rightarrow A)]$
$\equiv$ { substitution }
$(\underline{true} \equiv \underline{true}) \equiv [(\underline{true} \Rightarrow \underline{true}) \wedge (\underline{true} \Rightarrow \underline{true})]$
$\equiv \{ \equiv, \Rightarrow \}$
$\underline{true} \equiv [\underline{true} \wedge \underline{true}]$
$\equiv \{ \wedge \}$
$\underline{true} \equiv \underline{true}$
$\equiv \{ \equiv \}$
$\underline{true}$

Def : Tautology

A Tautology is a proposition that is true for all possible truth values.

Ex1 : Prove $p \vee \neg p$ is a tautology

p	¬ p	p ∨ ¬ p
t	f	**t**
f	t	**t**

Ex2 : Prove that $(P \Rightarrow R) \Rightarrow \neg (P \wedge \neg R)$ is a tautology

P	R	¬R	P ⇒ R	P ∧ ¬ R	¬ (P ∧ ¬ R)	(P ⇒ R) ⇒ ¬ (P ∧ ¬ R)
t	t	f	t	f	t	**t**
t	f	t	f	t	f	**t**
f	t	f	t	f	t	**t**
f	f	t	t	f	t	**t**

Ex3 : Prove $P \wedge (P \vee Q) \Rightarrow (P \vee Q)$ is a tautology.

Exercise.

Def : Contradiction

A contradiction is a proposition which is false for all possible truth values.

Example: Prove $p \wedge \neg p$ is a contradiction

p	$\neg p$	$p \wedge \neg p$
t	f	**f**
f	t	**f**

Valid Arguments

Def : An argument is valid if and only if

1: it is impossible for the premises to be true and the conclusion false.
or
2: its associated implication is a tautology.

It can be shown that these two definitions are equivalent,
i.e. $\neg (P \wedge \neg Q) \equiv P \Rightarrow Q$

Proof

Note: An invalid argument is one where a false conclusion is drawn from true premises.

One way to determine the validity or invalidity of an argument is to draw a truth table showing all possible truth values and check if any row has true premises and a false conclusion.

Ex Show that $(P \vee Q) \wedge P \Rightarrow \neg Q$ is invalid.

Laws of Natural Deduction

Truth tables are fine if the number of variables is small. However, their use becomes impractical when their number grows. It would be nicer if we had rules that would allow the manipulation of logical formulae. The following set of laws, allow the simplification of logical expressions and may be proved with the use of truth tables.

(i) Constants

$P \vee \text{true} \equiv \text{true}$

$P \vee \text{false} \equiv P$

$P \wedge \text{true} \equiv P$

$P \wedge \text{false} \equiv \text{false}$

$\text{true} \Rightarrow P \equiv P$

$\text{false} \Rightarrow P \equiv \text{true}$

$P \Rightarrow \text{true} \equiv \text{true}$

$P \Rightarrow \text{false} \equiv \neg P$

(ii) Law of excluded middle : $P \vee \neg P \equiv \text{true}$

(iii) Law of contradiction : $P \wedge \neg P \equiv \text{false}$

(iv) Negation : $\neg\neg P \equiv P$

(v) Associativity : $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$

$P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$

(vi) Commutativity : $P \vee Q \equiv Q \vee P$

$P \wedge Q \equiv Q \wedge P$

(vii) Idempotency : $P \vee P \equiv P$

$P \wedge P \equiv P$

(viii) De Morgan's laws : $\neg (P \wedge Q) \equiv \neg P \vee \neg Q$

$\neg (P \vee Q) \equiv \neg P \wedge \neg Q$

(ix) Implication : $P \Rightarrow Q \equiv \neg P \vee Q$

$$P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$$

$$(P \wedge Q) \Rightarrow R \equiv P \Rightarrow (Q \Rightarrow R)$$

(x) (If and only if) ≡ : $P \equiv Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$

(xi) Absorption: $[P \wedge (P \vee R) \equiv P]$

$[P \vee (P \wedge R) \equiv P]$

(xii) Laws of distribution : $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$

$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$

Ex 1 : Prove De Morgan's Laws

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P \vee \neg Q$	$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$
t	t	t	f	f	t
t	f	f	t	t	t
f	t	f	t	t	t
f	f	f	t	t	t

P	Q	$P \vee Q$	$\neg(P \vee Q)$	$\neg P \wedge \neg Q$	$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$
t	t	t	f	f	t
t	f	t	f	f	t
f	t	t	f	f	t
f	f	f	t	t	t

Ex. 2 : Using the laws of Natural Deduction prove the following tautologies :

(1) $P \wedge Q \Rightarrow P$
(2) $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$
(3) $P \Rightarrow P \vee Q$
(4) $P \wedge (P \Rightarrow Q) \Rightarrow Q$
(5) $P \wedge (P \vee Q) \Rightarrow P \vee Q$
(6) $(P \wedge Q) \Rightarrow (P \Rightarrow Q)$

(1)

$(P \wedge Q) \Rightarrow P$
$\equiv \{ \Rightarrow \}$
$\neg (P \wedge Q) \vee P$
$\equiv$ { De Morgan }
$\neg P \vee \neg Q \vee P$
$\equiv$ { Associativity }
$\neg P \vee P \vee \neg Q$
$\equiv$ { Excluded middle }
$\underline{\text{true}} \vee \neg Q$
$\equiv$ { Constant }
$\underline{\text{true}}$

(2)

$(P \wedge (P \Rightarrow Q)) \Rightarrow Q$
$\equiv \{ \Rightarrow \}$
$(P \wedge (\neg P \vee Q)) \Rightarrow Q$
$\equiv$ {Distribution}
$(P \wedge \neg P \vee P \wedge Q) \Rightarrow Q$

$\equiv$ {Contradiction }
$(\text{false} \lor P \land Q) \Rightarrow Q$
$\equiv$ {Constant}
$(P \land Q) \Rightarrow Q$
$\equiv$ {Implication}
$\neg (P \land Q) \lor Q$
$\equiv$ {De Morgan }
$\neg P \lor \neg Q \lor Q$
$\equiv$ {Excluded middle }
$\neg P \lor \underline{\text{true}}$
$\equiv$ {Constant}
$\underline{\text{true}}$

Ex : Prove $(p \Rightarrow \neg q) \land (p \Rightarrow \neg r) \equiv \neg (p \land (q \lor r)$

Proof : $(p \Rightarrow \neg q) \land (p \Rightarrow \neg r)$
$\equiv$ {implication }
$(\neg p \lor \neg q) \land (\neg p \lor r)$
$\equiv$ {Distribution }
$\neg p \lor (\neg q \land \neg r)$
$\equiv$ {De Morgan }
$\neg p \lor \neg (q \lor r)$
$\equiv$ {De Morgan }
$\neg (p \land (q \lor r)$