CS228 Logic for Computer Science 2021

Lecture 6: Substitution and equivalences

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2021-02-25

Simplifications for formulas

If we wish to develop algorithms for proof generation, we need more structure in our input.

For example, we simplify equations like $2x + 3 = 1 - x$, before solving them.

We will develop methods for simplifications or turning into normal forms.

Topic 6.1

Structural induction

Principle of structural induction

In order to prove theorems, we need to get used to the principle of structural induction.

Theorem 6.1

Every formula in P *has a property* Q *if*

- *Base case: every atomic formula has property* Q
- *induction steps: if* $F, G \in \mathrm{P}$ *have property* Q *so do* $\neg F$ *and* $(F \circ G)$, *where* $\circ$ *is a binary symbol*

Now we will see an important use of the structural induction.

Topic 6.2

Substitution theorems

Substitutions

Substitution is an important operation in logic.

Intuitively, we should be able to substitute equivalent subformulas without altering the truth values of formulas.

However, we need a proof to enable us.

In the following, we will prove three theorems.

Substitution theorem

Theorem 6.2

Let $F(p)$, G, and H be formulas. For some model m,

$$\textit{if} \quad m \models G \textit{ iff } m \models H \quad \textit{then} \quad m \models F(G) \textit{ iff } m \models F(H)$$

Proof.

Assume $m \models G$ iff $m \models H$.

We prove the theorem using structural induction over the structure of F.

base case:

$F(p)$ is atomic.

If $F(p) = p$, then $F(G) = G$ and $F(H) = H$. Therefore, hyp holds.

If $F(p) \neq p$, then $F(p) = F(G) = F(H)$. Again, hyp holds.

...

Substitution theorem (contd.)

Proof(contd.)

induction step:
Suppose $F(p) = F_1(p) \circ F_2(p)$ for some binary connective $\circ$.

Due to induction hypotheses, $m \models F_1(G)$ iff $m \models F_1(H)$, and $m \models F_2(G)$ iff $m \models F_2(H)$.

Due to the semantics of the propositional logic, $m \models F_1(G) \circ F_2(G)$ iff $m \models F_1(H) \circ F_2(H)$.

Therefore, $m \models F(G)$ iff $m \models F(H)$.

The negation case is symmetric. □

Equivalence generalization theorem

Theorem 6.3

If $F(p) \equiv G(p)$ then for each formula H, $F(H) \equiv G(H)$.

Proof.

Wlog, we assume p does not appear in H.(why?)

Commentary: If p occurs in H, we split the substitution in two steps. For a fresh q, we first substitute from p to $H[q/p]$ and subsequently q to p. Check if this trick works.

Consider a model m. Let $m' \triangleq \begin{cases} m[p \mapsto 1] & \text{if } m \models H \\ m[p \mapsto 0] & \text{if } m \not\models H. \end{cases}$

Due to the construction of m',

$$m' \models p \text{ iff } m' \models H.\text{(why?)} \qquad (*)$$

Now we will show that $m \models F(H)$ iff $m \models G(H)$. ...

Commentary: $p \notin \mathrm{Vars}(F(H))$ has a subtle assumption. Did $F(H)$ really replace all ps? If we define $F(z) = (z \lor p)$ and use in our theorem for $F(p)$. Then $F(r \lor q)$ has a p. There is a defining step for substitutions like $F(p)$ and the definition is appearing in the theorem.

Equivalence generalization theorem(contd.)

Proof(Contd.)

$$\begin{tikzcd}
m \models F(H) \arrow[d, Leftrightarrow, "p \notin \mathrm{Vars}(F(H))"] & & m \models G(H) \arrow[d, Leftrightarrow, "p \notin \mathrm{Vars}(G(H))"] \\
m' \models F(H) \arrow[d, Leftrightarrow, "\text{Thm 6.2 and } *"] & & m' \models G(H) \arrow[d, Leftrightarrow, "\text{Thm 6.2 and } *"] \\
m' \models F(p) \arrow[rr, Leftrightarrow, "\text{Due to lhs of this theorem } F(p) \equiv G(p)"'] & & m' \models G(p)
\end{tikzcd}$$

Therefore, $m \models F(H)$ iff $m \models G(H)$. Therefore, $F(H) \equiv G(H)$. □

Exercise 6.1

Can we extend the above argument for simultaneous substitutions?

Writing equivalences

The previous theorem allows us to first prove equivalences between formulas over variables then use it for arbitrary formulas.

We will state equivalences using variables instead of generic formulas.

Example 6.1

Since $\neg\neg p \equiv p$, *we can deduce* $\neg\neg(q \oplus r) \equiv (q \oplus r)$

Subformula replacement theorem

Theorem 6.4

Let G,H and F(p) be formulas. If $G \equiv H$ then $F(G) \equiv F(H)$.

Proof.

Due to Thm 6.2, straight forward. □

The above theorem allows us to use known equivalences to modify formulas.

Example 6.2

Since we know $\neg\neg(q \oplus r) \equiv (q \oplus r)$, $(\neg\neg(q \oplus r) \Rightarrow (r \land q)) \equiv ((q \oplus r) \Rightarrow (r \land q))$

Exercise 6.2

a. Complete the arguments in the above proof.

b. extend the argument for simultaneous substitutions.

Commentary: We had proven theorem 6.4 in the previous lecture using derivation rules. Now we have proven the theorems 6.2- 6.4 again using semantics instead of the derivation rules. There is nothing wrong in doing this. Can we prove theorem 6.3 using derivation rules?

Topic 6.3

Equivalences

Equivalences

- Let us go over a list of useful and easy equivalences for simplification of formulas
- We need to prove their correctness using truth tables. However, we will not present the truth tables in the slides in this lecture.

Commentary: We have seen a few truth tables in the earlier lectures illustrating equivalences. In the exams, you will be expected to illustrate the equivalences using truth tables.

Constant connectives

- $\neg\top \equiv \bot$
- $\top \land p \equiv p$
- $\top \lor p \equiv \top$
- $\top \oplus p \equiv \neg p$
- $\top \Rightarrow p \equiv p$
- $p \Rightarrow \top \equiv \top$
- $\top \Leftrightarrow p \equiv p$

- $\neg\bot \equiv \top$
- $\bot \land p \equiv \bot$
- $\bot \lor p \equiv p$
- $\bot \oplus p \equiv p$
- $\bot \Rightarrow p \equiv \top$
- $p \Rightarrow \bot \equiv \neg p$
- $\bot \Leftrightarrow p \equiv \neg p$

Exercise 6.3

Simplify, the following formulas using the above equivalences

- $\top \Rightarrow \bot$
- $(\top \oplus \top) \oplus \top$
- $p \Rightarrow (\bot \Rightarrow q)$

Exercise 6.4

Prove $\neg\top \equiv \bot$. *Hint: use semantics.*

Negation and the other connectives

- $\neg\neg p \equiv p$
- $\neg(p \vee q) \equiv \neg p \wedge \neg q$ (DeMorgan's Law)
- $\neg(p \wedge q) \equiv \neg p \vee \neg q$ (DeMorgan's Law)
- $\neg(p \Rightarrow q) \equiv p \wedge \neg q$
- $\neg(p \oplus q) \equiv \neg p \oplus q \equiv p \Leftrightarrow q$
- $\neg(p \Leftrightarrow q) \equiv p \oplus q$

Exercise 6.5

Show that the above equivalences are derivable. For example, $\emptyset \vdash \neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$

Expanded DeMorgan

Theorem 6.5

$$\neg(\bigvee_{i=0}^{m} p_i) \equiv \bigwedge_{i=0}^{m} \neg p_i$$

Proof.

We prove it by induction over m.

base case:

If $m = 0$, there is nothing to prove because both sides are same.

induction step:

Let us assume $\neg(\bigvee_{i=0}^{m} p_i) \equiv \bigwedge_{i=0}^{m} \neg p_i$

Now consider

$$\neg(\bigvee_{i=0}^{m+1} p_i) \equiv \neg(\bigvee_{i=0}^{m} p_i \vee p_{m+1}) \underbrace{\equiv \neg \bigvee_{i=0}^{m} p_i \wedge \neg p_{m+1}}_{\text{Binary DeMorgan Rule}} \underbrace{\equiv \bigwedge_{i=0}^{m} \neg p_i \wedge \neg p_{m+1}}_{\text{Subsitution theorem}} \equiv \bigwedge_{i=0}^{m+1} \neg p_i \qquad \square$$

Associativity

$\wedge$, $\vee$, $\oplus$ are associative

- $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$
- $p \vee (q \vee r) \equiv (p \vee q) \vee r$
- $p \oplus (q \oplus r) \equiv (p \oplus q) \oplus r$

Due to associativity, we do not need parentheses in the following formulas

- $p_1 \wedge \dots \wedge p_k = \bigwedge_{i=1}^{k} p_i$
- $p_1 \vee \dots \vee p_k = \bigvee_{i=1}^{k} p_i$
- $p_1 \oplus \ldots \oplus p_k = \bigoplus_{i=1}^{k} p_i$

The drop of parentheses is called flattening.

Exercise 6.6

Prove/Disprove $\Leftrightarrow$ is associative.

Commutativity

$\wedge$, $\vee$, $\oplus$, $\Leftrightarrow$ are commutative

- $(p \wedge q) \equiv (q \wedge p)$
- $(p \vee q) \equiv (q \vee p)$
- $(p \oplus q) \equiv (q \oplus p)$
- $(p \Leftrightarrow q) \equiv (q \Leftrightarrow p)$

Absorption law

- $p \wedge p \Leftrightarrow p$
- $p \vee p \Leftrightarrow p$

Due to associativity, commutativity and absorption law, we define the following notation with a clear meaning

- $\bigwedge\{p_1, \dots, p_k\} \triangleq p_1 \wedge \dots \wedge p_k$
- $\bigvee\{p_1, \dots, p_k\} \triangleq p_1 \vee \dots \vee p_k$

Distributivity

$\wedge$, $\vee$ distribute over each other

- $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
- $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

Exercise 6.7

Prove/Disprove the following equivalences

- $p \oplus (q \wedge r) \equiv (p \oplus q) \wedge (p \oplus r)$
- $p \Leftrightarrow (q \wedge r) \equiv (p \Leftrightarrow q) \wedge (p \Leftrightarrow r)$
- $p \Rightarrow (q \wedge r) \equiv (p \Rightarrow q) \wedge (p \Rightarrow r)$
- $p \Rightarrow (q \vee r) \equiv (p \Rightarrow q) \vee (p \Rightarrow r)$
- $(p \wedge q) \Rightarrow r \equiv (p \Rightarrow r) \wedge (q \Rightarrow r)$
- $(p \vee q) \Rightarrow r \equiv (p \Rightarrow r) \vee (q \Rightarrow r)$

Exercise: prove extended distributivity

Exercise 6.8

Using induction and the distributivity property, show the following

$$\bigvee_{i=0}^{m} \bigwedge_{j=0}^{n_i} p_{ij} \equiv \bigwedge_{j_0=0}^{n_0} \dots \bigwedge_{j_m=0}^{n_m} \bigvee_{i=0}^{m} p_{ij_i}$$

Properties of $\oplus$

- $\top \oplus p \equiv \neg p$
- $\bot \oplus p \equiv p$
- $p \oplus p \equiv \bot$
- $p \oplus \neg p \equiv \top$
- $(p \oplus q) \equiv (p \lor q) \land (\neg p \lor \neg q)$
- $(p \Leftrightarrow q) \equiv (p \lor \neg q) \land (q \lor \neg p)$

Simplify

- All tools include a simplify procedure using the presented equivalences
- $\oplus$ and $\Leftrightarrow$ are difficult connectives, because they result in larger formula if one aims to remove them. We will learn soon how to deal with the operators.

Topic 6.4

Problems

Simplifications

Exercise 6.9

Show $p_1 \oplus \ldots \oplus p_n$ *count odd number of one's in* $p_1, .., p_n$.

Exercise 6.10

Similar to the above problem characterize the following.

$$\underbrace{p_1 \Leftrightarrow \ldots \Leftrightarrow p_n}_{n}$$

Exercise 6.11

Simplify

$$\underbrace{p \oplus \ldots \oplus p}_{n} \oplus \underbrace{\neg p \oplus \ldots \oplus \neg p}_{k} \equiv ?$$

Exercise 6.12

Simplify

$$(p \lor (p \oplus y)) \Rightarrow (p \land q) \land (r \land \neg p)$$

Encoding if-then-else

Some propositional logic may also include a ternary operator $ite(p, q, r)$, which encodes that if p is true then q is true, otherwise r is true.

Exercise 6.13

Show the following two encodings of $ite(p, q, r)$ *are equivalent.*

1. $(p \land q) \lor (\neg p \land r)$
2. $(p \Rightarrow q) \land (\neg p \Rightarrow r)$

Simplify

Exercise 6.14

Let $G(x)$ be a formula. Show that the following equivalences hold.

- $F \vee G(F) \equiv F \vee G(\bot)$
- $F \wedge G \equiv F \wedge G(\top)$
- $F \Rightarrow G(F) \equiv F \Rightarrow G(\top)$

Commentary: **Solution:** Let us the solve first. If $m \models F$, then $m \models F \vee G(F)$ and $m \models F \vee G(\bot)$.
If $m \not\models F$, then $m \not\models F$ and $m \not\models \bot$. Therefore due to theorem 6.2, $m \models G(F)$ iff $m \models G(\bot)$. Therefore, $m \models F \vee G(F)$ iff $m \models F \vee G(\bot)$.

End of Lecture 6