
Mathematical Logic for Computer Science **(Third Revised Edition)**

Springer, 2012

Mordechai (Moti) Ben-Ari

<http://www.weizmann.ac.il/sci-tea/benari/>

© 2012 by Springer.

Example 1.2: A half-adder

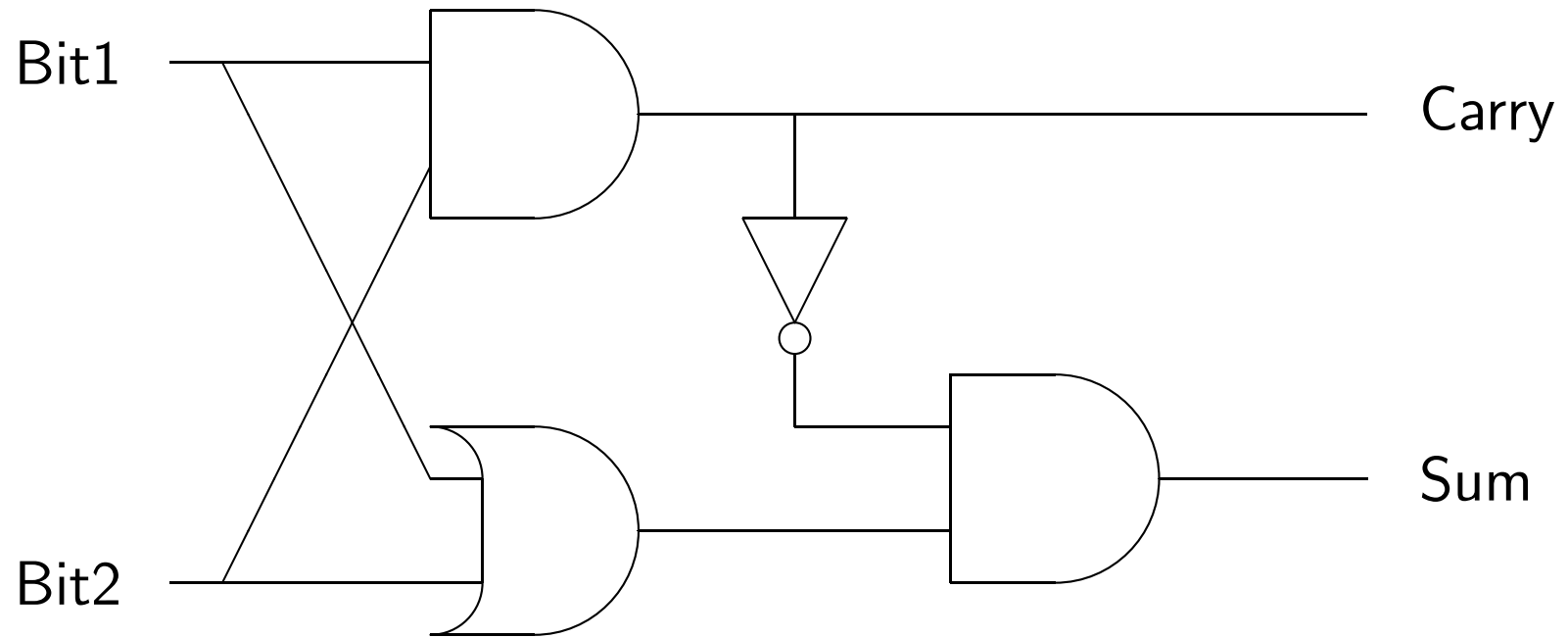
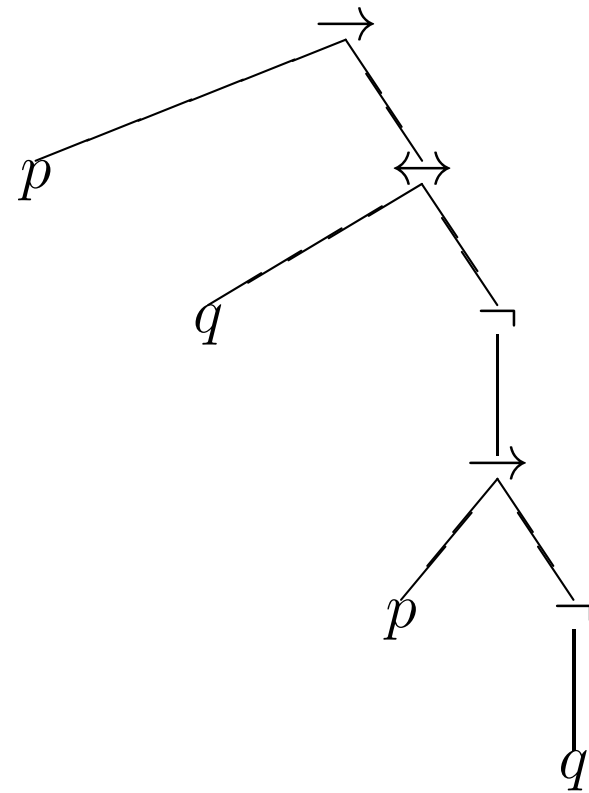
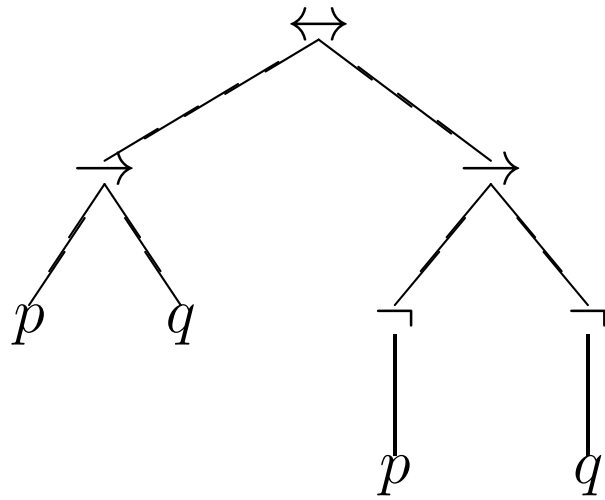


Figure 2.1: Two formulas



Notation

| Operator | Alternates | Java language |
|-------------------|------------------------------|---------------|
| \neg | \sim | ! |
| \wedge | $\&$ | $\&$, $\&\&$ |
| \vee | | , |
| \rightarrow | \supset , \Rightarrow | |
| \leftrightarrow | \equiv , \Leftrightarrow | |
| \oplus | \neq | \wedge |
| \uparrow | | |

Figure 2.2: Derivation tree for $p \rightarrow q \Leftrightarrow \neg p \rightarrow \neg q$

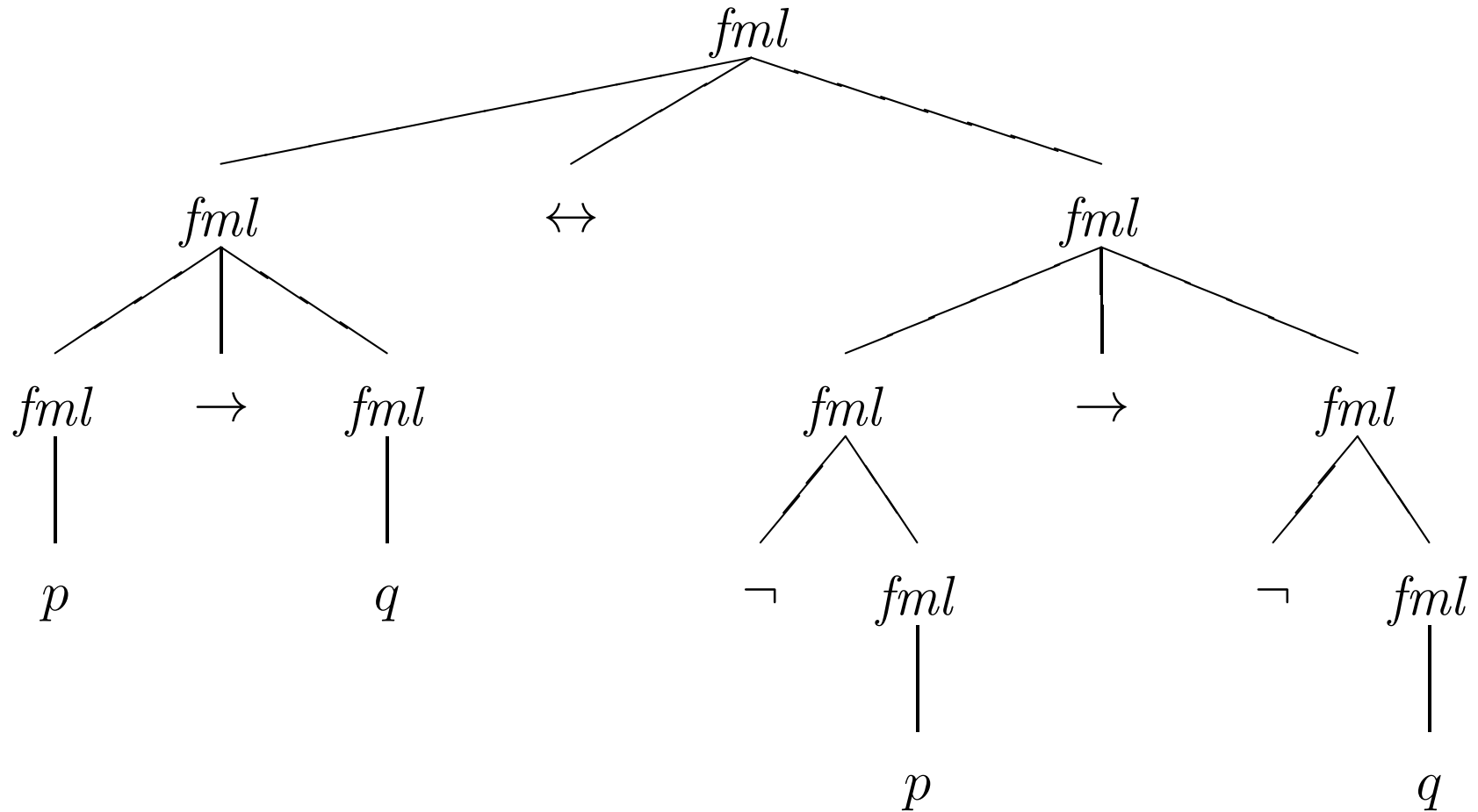


Figure 2.3: Truth values of formulas

| A | $v(A_1)$ | $v(A_2)$ | $v(A)$ |
|-----------------------|-----------|----------|--------|
| $\neg A_1$ | T | | F |
| $\neg A_1$ | F | | T |
| $A_1 \vee A_2$ | F | F | F |
| $A_1 \vee A_2$ | otherwise | | T |
| $A_1 \wedge A_2$ | T | T | T |
| $A_1 \wedge A_2$ | otherwise | | F |
| $A_1 \rightarrow A_2$ | T | F | F |
| $A_1 \rightarrow A_2$ | otherwise | | T |

| A | $v(A_1)$ | $v(A_2)$ | $v(A)$ |
|---------------------------|----------------------|----------|--------|
| $A_1 \uparrow A_2$ | T | T | F |
| $A_1 \uparrow A_2$ | otherwise | | T |
| $A_1 \downarrow A_2$ | F | F | T |
| $A_1 \downarrow A_2$ | otherwise | | F |
| $A_1 \leftrightarrow A_2$ | $v(A_1) = v(A_2)$ | | T |
| $A_1 \leftrightarrow A_2$ | $v(A_1) \neq v(A_2)$ | | F |
| $A_1 \oplus A_2$ | $v(A_1) \neq v(A_2)$ | | T |
| $A_1 \oplus A_2$ | $v(A_1) = v(A_2)$ | | F |

Example 2.21

| p | q | $p \rightarrow q$ |
|-----|-----|-------------------|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

Example 2.22

| p | q | $p \rightarrow q$ | $\neg p$ | $\neg q$ | $\neg q \rightarrow \neg p$ | $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$ |
|-----|-----|-------------------|----------|----------|-----------------------------|---|
| T | T | T | F | F | T | T |
| T | F | F | F | T | F | T |
| F | T | T | T | F | T | T |
| F | F | T | T | T | T | T |

Example 2.23

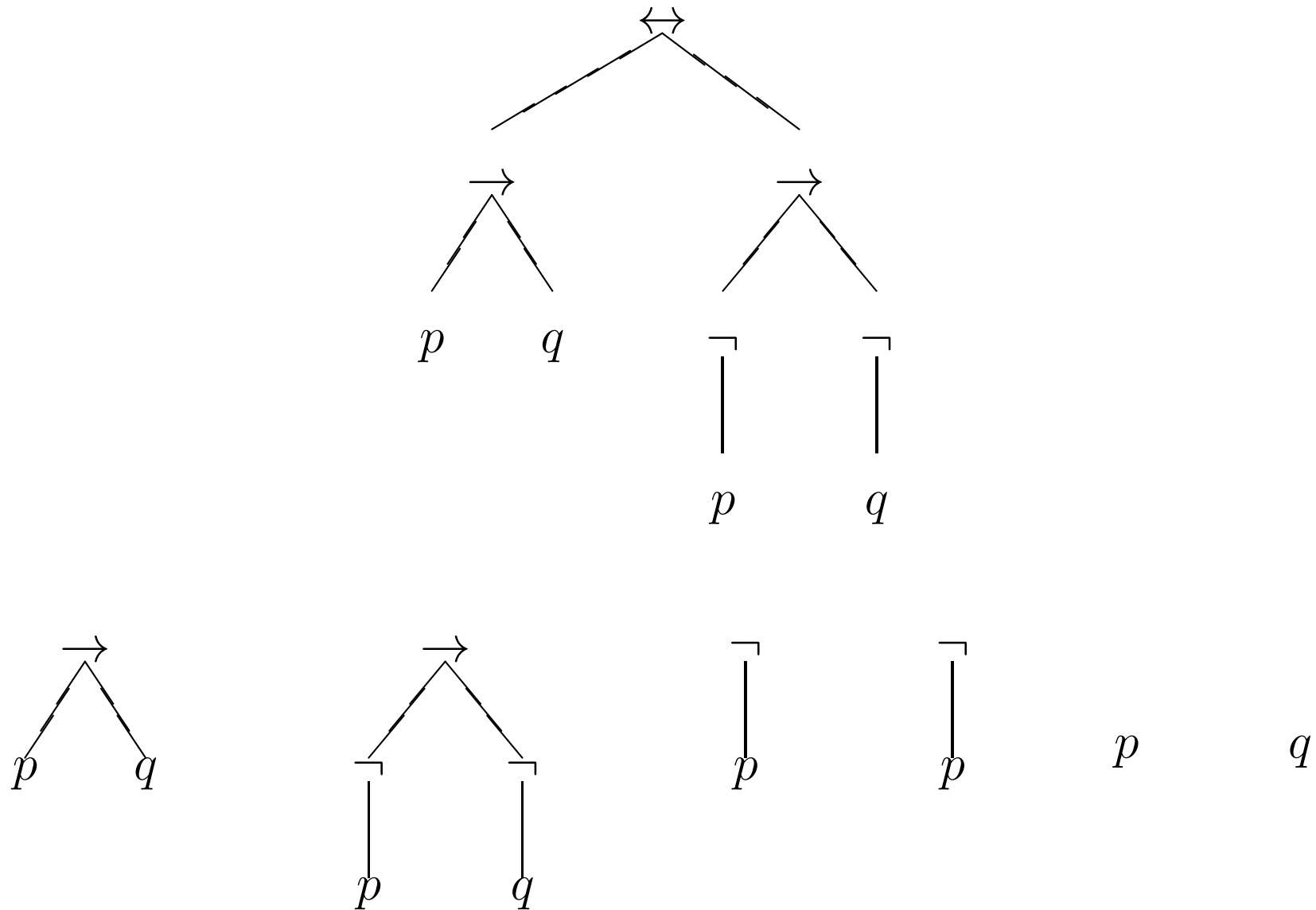
$$\begin{array}{ccccccc}
 (p \rightarrow q) & \leftrightarrow & (\neg q \rightarrow \neg p) \\
 T & F & F & T \\
 T & F & T & F & T \\
 T & F & T & F & F & T \\
 T & F & T & F & F & F & T \\
 T & F & F & T & F & F & F & T \\
 T & F & F & T & T & F & F & F & T
 \end{array}$$

| p | q | $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$ | | | | | | | |
|-----|-----|---|-----|-----|-----|-----|-----|-----|---------|
| T | T | T | T | T | T | F | T | T | F T |
| T | F | T | F | F | T | T | F | F | F T |
| F | T | F | T | T | T | F | T | T | T F |
| F | F | F | T | F | T | T | F | T | T F |

Example 2.27

| p | q | $v(p \vee q)$ | $v(q \vee p)$ |
|-----|-----|---------------|---------------|
| T | T | T | T |
| T | F | T | T |
| F | T | T | T |
| F | F | F | F |

Figure 2.4: Subformulas



Logically equivalent formulas (1)

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

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

$$A \rightarrow \text{true} \equiv \text{true}$$

$$A \rightarrow \text{false} \equiv \neg A$$

$$A \leftrightarrow \text{true} \equiv A$$

$$A \leftrightarrow \text{false} \equiv \neg A$$

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

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

$$\text{true} \rightarrow A \equiv A$$

$$\text{false} \rightarrow A \equiv \text{true}$$

$$A \oplus \text{true} \equiv \neg A$$

$$A \oplus \text{false} \equiv A$$

$$A \equiv \neg \neg A$$

$$A \equiv A \wedge A$$

$$A \vee \neg A \equiv \text{true}$$

$$A \rightarrow A \equiv \text{true}$$

$$A \leftrightarrow A \equiv \text{true}$$

$$\neg A \equiv A \uparrow A$$

$$A \equiv A \vee A$$

$$A \wedge \neg A \equiv \text{false}$$

$$A \oplus A \equiv \text{false}$$

$$\neg A \equiv A \downarrow A$$

Logically equivalent formulas (2)

$$A \vee B \equiv B \vee A$$

$$A \wedge B \equiv B \wedge A$$

$$A \leftrightarrow B \equiv B \leftrightarrow A$$

$$A \oplus B \equiv B \oplus A$$

$$A \uparrow B \equiv B \uparrow A$$

$$A \downarrow B \equiv B \downarrow A$$

$$A \vee (B \vee C) \equiv (A \vee B) \vee C$$

$$A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$$

$$A \leftrightarrow (B \leftrightarrow C) \equiv (A \leftrightarrow B) \leftrightarrow C$$

$$A \oplus (B \oplus C) \equiv (A \oplus B) \oplus C$$

$$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$$

$$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$$

Logically equivalent formulas (3)

$$A \leftrightarrow B \equiv (A \rightarrow B) \wedge (B \rightarrow A)$$

$$A \oplus B \equiv \neg(A \rightarrow B) \vee \neg(B \rightarrow A)$$

$$A \rightarrow B \equiv \neg A \vee B$$

$$A \rightarrow B \equiv \neg(A \wedge \neg B)$$

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

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

$$A \vee B \equiv \neg A \rightarrow B$$

$$A \wedge B \equiv \neg(A \rightarrow \neg B)$$

One-place operators

| x | \circ_1 | \circ_2 | \circ_3 | \circ_4 |
|-----|-----------|-----------|-----------|-----------|
| T | T | T | F | F |
| F | T | F | T | F |

Two-place operators

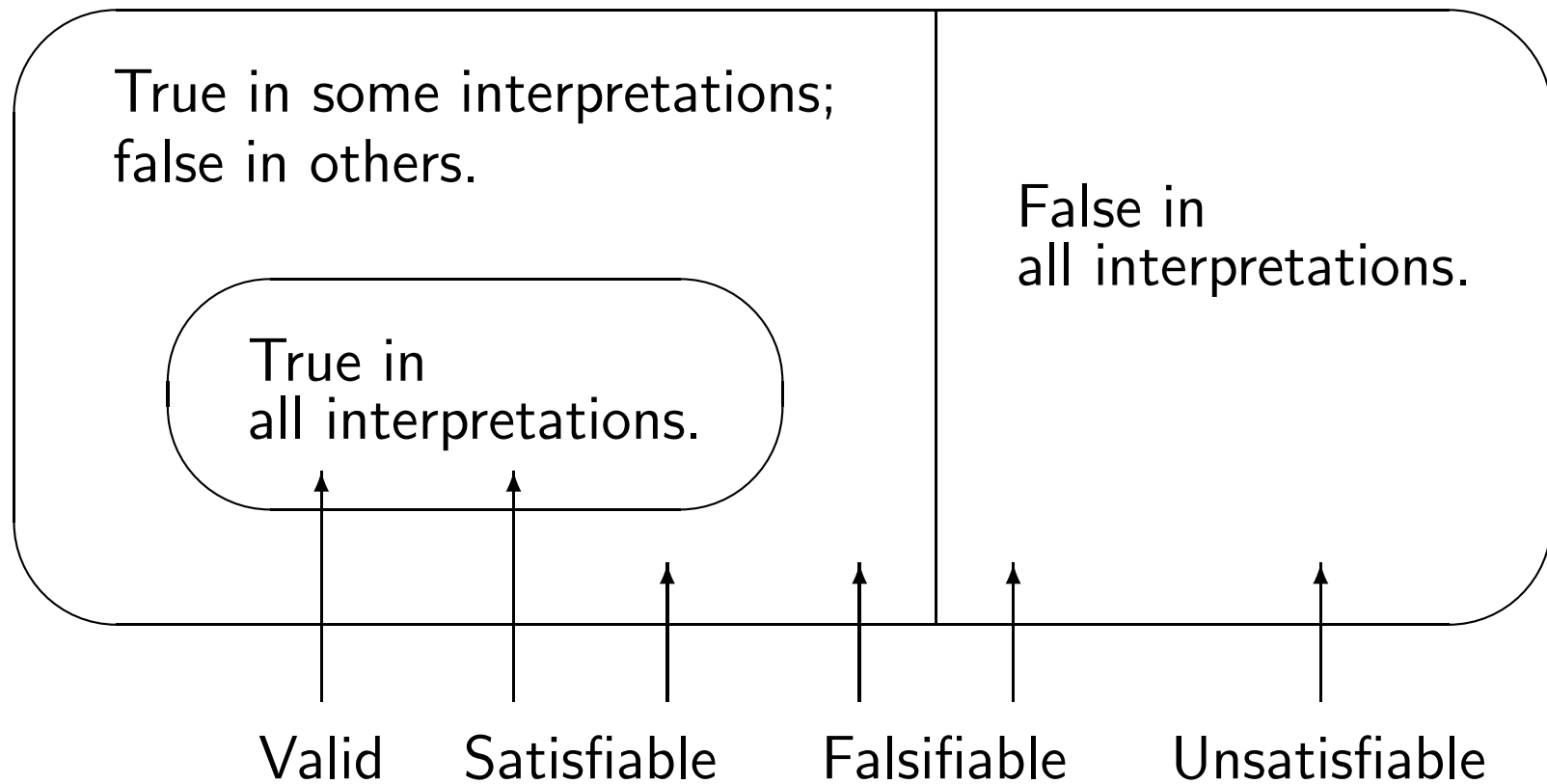
| x_1 | x_2 | \circ_1 | \circ_2 | \circ_3 | \circ_4 | \circ_5 | \circ_6 | \circ_7 | \circ_8 |
|-------|-------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| T | T | T | T | T | T | T | T | T | T |
| T | F | T | T | T | T | F | F | F | F |
| F | T | T | T | F | F | T | T | F | F |
| F | F | T | F | T | F | T | F | T | F |

| x_1 | x_2 | \circ_9 | \circ_{10} | \circ_{11} | \circ_{12} | \circ_{13} | \circ_{14} | \circ_{15} | \circ_{16} |
|-------|-------|-----------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|
| T | T | F | F | F | F | F | F | F | F |
| T | F | T | T | T | T | F | F | F | F |
| F | T | T | T | F | F | T | T | F | F |
| F | F | T | F | T | F | T | F | T | F |

Operator names

| op | name | symbol | op | name | symbol |
|-----------|---------------------|-------------------|--------------|--------------|--------------|
| \circ_2 | disjunction | \vee | \circ_{15} | nor | \downarrow |
| \circ_8 | conjunction | \wedge | \circ_9 | nand | \uparrow |
| \circ_5 | implication | \rightarrow | \circ_{12} | | |
| \circ_3 | reverse implication | \leftarrow | \circ_{14} | | |
| \circ_7 | equivalence | \leftrightarrow | \circ_{10} | exclusive or | \oplus |

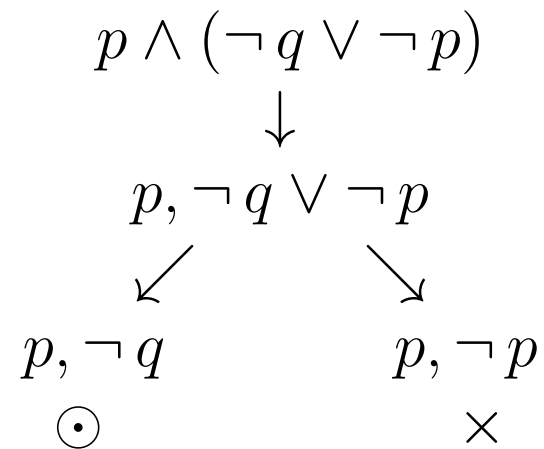
Valid, satisfiable, falsifiable and unsatisfiable formulas



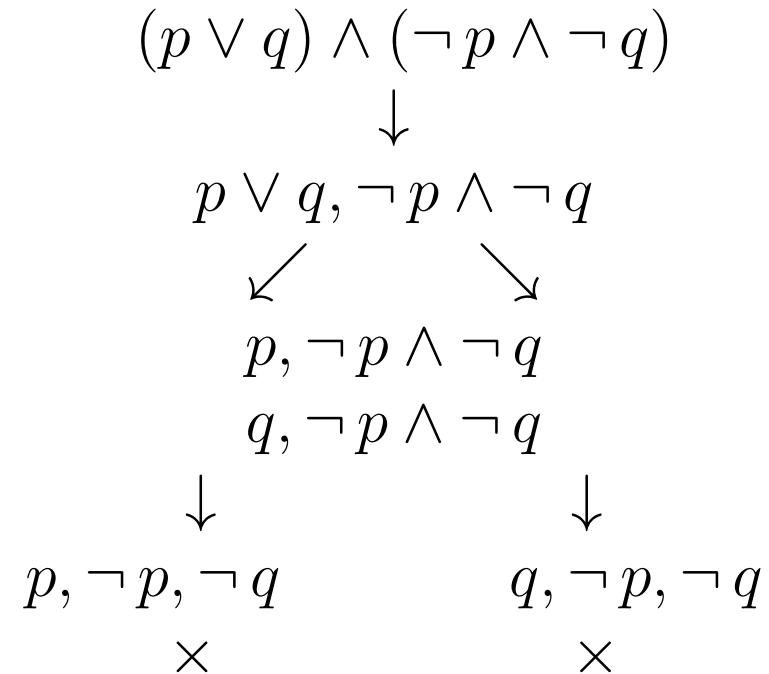
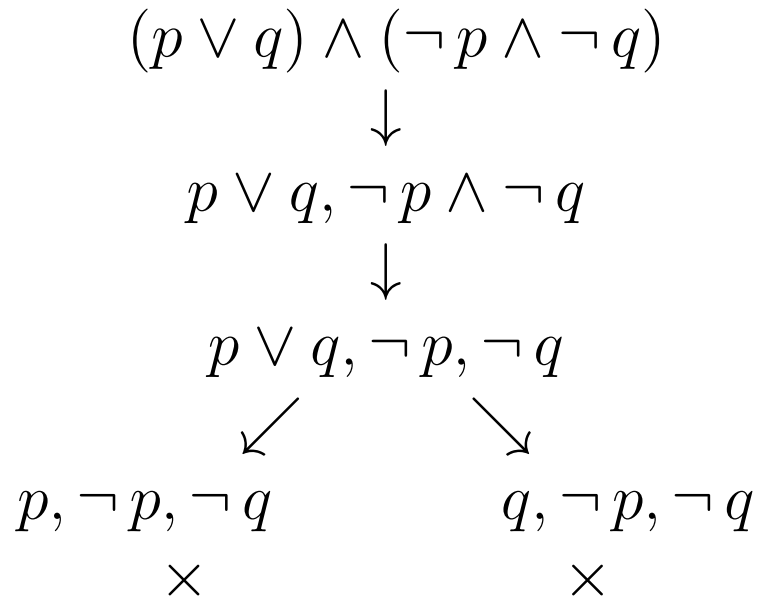
Example 2.41

| p | q | $p \vee q$ | $\neg p$ | $\neg q$ | $(p \vee q) \wedge \neg p \wedge \neg q$ |
|-----|-----|------------|----------|----------|--|
| T | T | T | F | F | F |
| T | F | T | F | T | F |
| F | T | T | T | F | F |
| F | F | F | T | T | F |

Semantic tableau for $p \wedge (\neg q \vee \neg p)$



Semantic tableaux $(p \vee q) \wedge (\neg p \wedge \neg q)$



α -formulas

| α | α_1 | α_2 |
|------------------------------|-----------------------|-----------------------|
| $\neg \neg A_1$ | A_1 | |
| $A_1 \wedge A_2$ | A_1 | A_2 |
| $\neg (A_1 \vee A_2)$ | $\neg A_1$ | $\neg A_2$ |
| $\neg (A_1 \rightarrow A_2)$ | A_1 | $\neg A_2$ |
| $\neg (A_1 \uparrow A_2)$ | A_1 | A_2 |
| $A_1 \downarrow A_2$ | $\neg A_1$ | $\neg A_2$ |
| $A_1 \leftrightarrow A_2$ | $A_1 \rightarrow A_2$ | $A_2 \rightarrow A_1$ |
| $\neg (A_1 \oplus A_2)$ | $A_1 \rightarrow A_2$ | $A_2 \rightarrow A_1$ |

β -formulas

| β | β_1 | β_2 |
|----------------------------------|------------------------------|------------------------------|
| $\neg (B_1 \wedge B_2)$ | $\neg B_1$ | $\neg B_2$ |
| $B_1 \vee B_2$ | B_1 | B_2 |
| $B_1 \rightarrow B_2$ | $\neg B_1$ | B_2 |
| $B_1 \uparrow B_2$ | $\neg B_1$ | $\neg B_2$ |
| $\neg (B_1 \downarrow B_2)$ | B_1 | B_2 |
| $\neg (B_1 \leftrightarrow B_2)$ | $\neg (B_1 \rightarrow B_2)$ | $\neg (B_2 \rightarrow B_1)$ |
| $B_1 \oplus B_2$ | $\neg (B_1 \rightarrow B_2)$ | $\neg (B_2 \rightarrow B_1)$ |

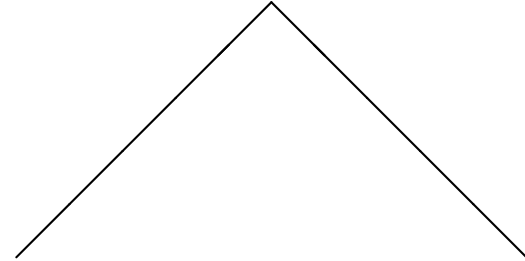
Section 2.7.1: Inductive step in proof of soundness

$$n : \{A_1 \wedge A_2\} \cup U_0$$



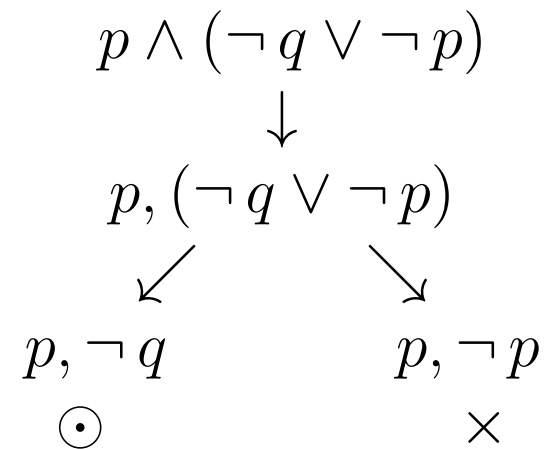
$$n' : \{A_1, A_2\} \cup U_0$$

$$n : \{B_1 \vee B_2\} \cup U_0$$



$$n' : \{B_1\} \cup U_0 \quad n'' : \{B_2\} \cup U_0$$

Example 2.73: Semantic tableau for $p \wedge (\neg q \vee \neg p)$



Example 2.74: Semantic tableau for $p \vee (q \wedge \neg q)$

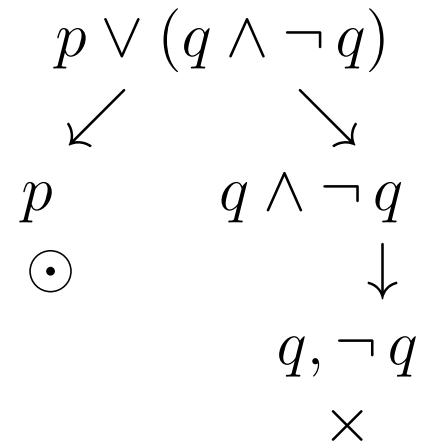


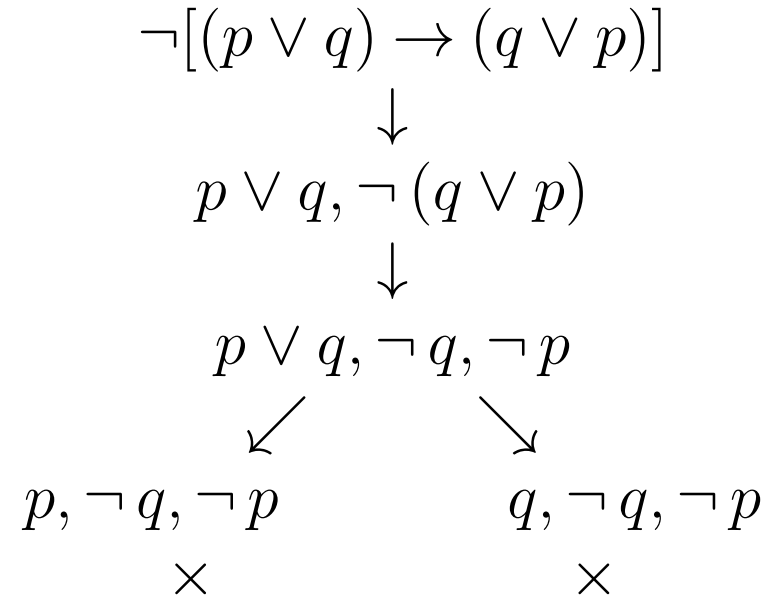
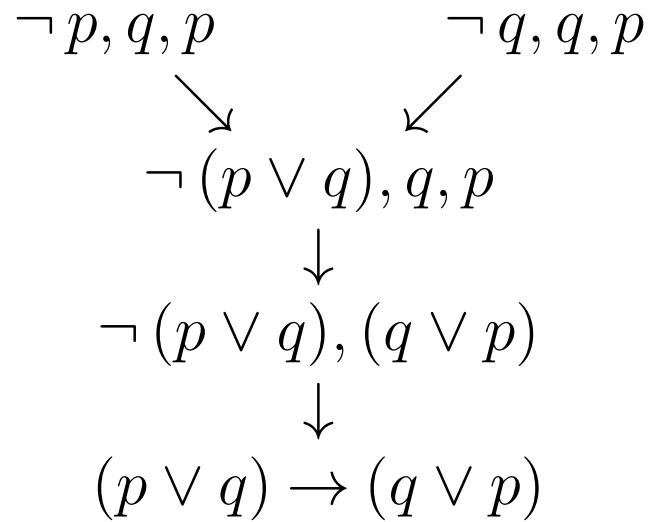
Figure 3.1: Classification of α -formulas

| α | α_1 | α_2 |
|---------------------------------|-----------------------------|-----------------------------|
| $\neg\neg A$ | A | |
| $\neg(A_1 \wedge A_2)$ | $\neg A_1$ | $\neg A_2$ |
| $A_1 \vee A_2$ | A_1 | A_2 |
| $A_1 \rightarrow A_2$ | $\neg A_1$ | A_2 |
| $A_1 \uparrow A_2$ | $\neg A_1$ | $\neg A_2$ |
| $\neg(A_1 \downarrow A_2)$ | A_1 | A_2 |
| $\neg(A_1 \leftrightarrow A_2)$ | $\neg(A_1 \rightarrow A_2)$ | $\neg(A_2 \rightarrow A_1)$ |
| $A_1 \oplus A_2$ | $\neg(A_1 \rightarrow A_2)$ | $\neg(A_2 \rightarrow A_1)$ |

Figure 3.1: Classification of β -formulas

| β | β_1 | β_2 |
|-----------------------------|-----------------------|-----------------------|
| $B_1 \wedge B_2$ | B_1 | B_2 |
| $\neg(B_1 \vee B_2)$ | $\neg B_1$ | $\neg B_2$ |
| $\neg(B_1 \rightarrow B_2)$ | B_1 | $\neg B_2$ |
| $\neg(B_1 \uparrow B_2)$ | B_1 | B_2 |
| $B_1 \downarrow B_2$ | $\neg B_1$ | $\neg B_2$ |
| $B_1 \leftrightarrow B_2$ | $B_1 \rightarrow B_2$ | $B_2 \rightarrow B_1$ |
| $\neg(B_1 \oplus B_2)$ | $B_1 \rightarrow B_2$ | $B_2 \rightarrow B_1$ |

Section 3.2.1: \mathcal{G} and semantic tableaux



Hilbert system \mathcal{H}

Axiom 1 $\vdash (A \rightarrow (B \rightarrow A)),$

Axiom 2 $\vdash (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)),$

Axiom 3 $\vdash (\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B).$

Modus ponens
$$\frac{\vdash A \qquad \vdash A \rightarrow B}{\vdash B}.$$

Derived rules of inference

Deduction

$$\frac{U \cup \{A\} \vdash B}{U \vdash A \rightarrow B}$$

Contrapositive

$$\frac{U \vdash \neg B \rightarrow \neg A}{U \vdash A \rightarrow B}$$

Transitivity

$$\frac{U \vdash A \rightarrow B \quad U \vdash B \rightarrow C}{U \vdash A \rightarrow C}$$

Exchange of antecedent

$$\frac{U \vdash A \rightarrow (B \rightarrow C)}{U \vdash B \rightarrow (A \rightarrow C)}$$

Double negation

$$\frac{U \vdash \neg \neg A}{U \vdash A}$$

Reductio ad absurdum

$$\frac{U \vdash \neg A \rightarrow \text{false}}{U \vdash A}$$

Theorem 3.37: Soundness of axioms 1 and 3

$$\neg[A \rightarrow (B \rightarrow A)]$$

↓

$$A, \neg(B \rightarrow A)$$

↓

$$A, B, \neg A$$

×

$$\neg[(\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)]$$

↓

$$\neg B \rightarrow \neg A, \neg(A \rightarrow B)$$

↓

$$\neg B \rightarrow \neg A, A, \neg B$$

↙

↘

$$\neg\neg B, A, \neg B$$

$$\neg A, A, \neg B$$

×

↓

$$B, A, \neg B$$

×

Figure 3.32: Rules of inference for sequents

| op | Introduction into consequent | Introduction into antecedent |
|---------------|---|--|
| \wedge | $\frac{U \Rightarrow V \cup \{A\} \quad U \Rightarrow V \cup \{B\}}{U \Rightarrow V \cup \{A \wedge B\}}$ | $\frac{U \cup \{A, B\} \Rightarrow V}{U \cup \{A \wedge B\} \Rightarrow V}$ |
| \vee | $\frac{U \Rightarrow V \cup \{A, B\}}{U \Rightarrow V \cup \{A \vee B\}}$ | $\frac{U \cup \{A\} \Rightarrow V \quad U \cup \{B\} \Rightarrow V}{U \cup \{A \vee B\} \Rightarrow V}$ |
| \rightarrow | $\frac{U \cup \{A\} \Rightarrow V \cup \{B\}}{U \Rightarrow V \cup \{A \rightarrow B\}}$ | $\frac{U \Rightarrow V \cup \{A\} \quad U \cup \{B\} \Rightarrow V}{U \cup \{A \rightarrow B\} \Rightarrow V}$ |
| \neg | $\frac{U \cup \{A\} \Rightarrow V}{U \Rightarrow V \cup \{\neg A\}}$ | $\frac{U \Rightarrow V \cup \{A\}}{U \cup \{\neg A\} \Rightarrow V}$ |

Figure 3.3: A natural deduction proof

| | | |
|-----|---|------------------------|
| 1. | $A \rightarrow \neg A$ | Assumption |
| 2. | $\neg \neg A$ | Assumption |
| 3. | A | Double neg. 2 |
| 4. | $\neg A$ | MP 1, 3 |
| 5. | $A \rightarrow (\neg A \rightarrow \text{false})$ | Theorem 3.21 |
| 6. | $\neg A \rightarrow \text{false}$ | MP 3, 5 |
| 7. | false | MP 4, 6 |
| 8. | $\neg \neg A \rightarrow \text{false}$ | Deduction 2, 7 |
| 9. | $\neg A$ | Reductio ad absurdum 8 |
| 10. | $(A \rightarrow \neg A) \rightarrow \neg A$ | Deduction 1, 9 |

Figure 4.1: Resolution refutation as a tree

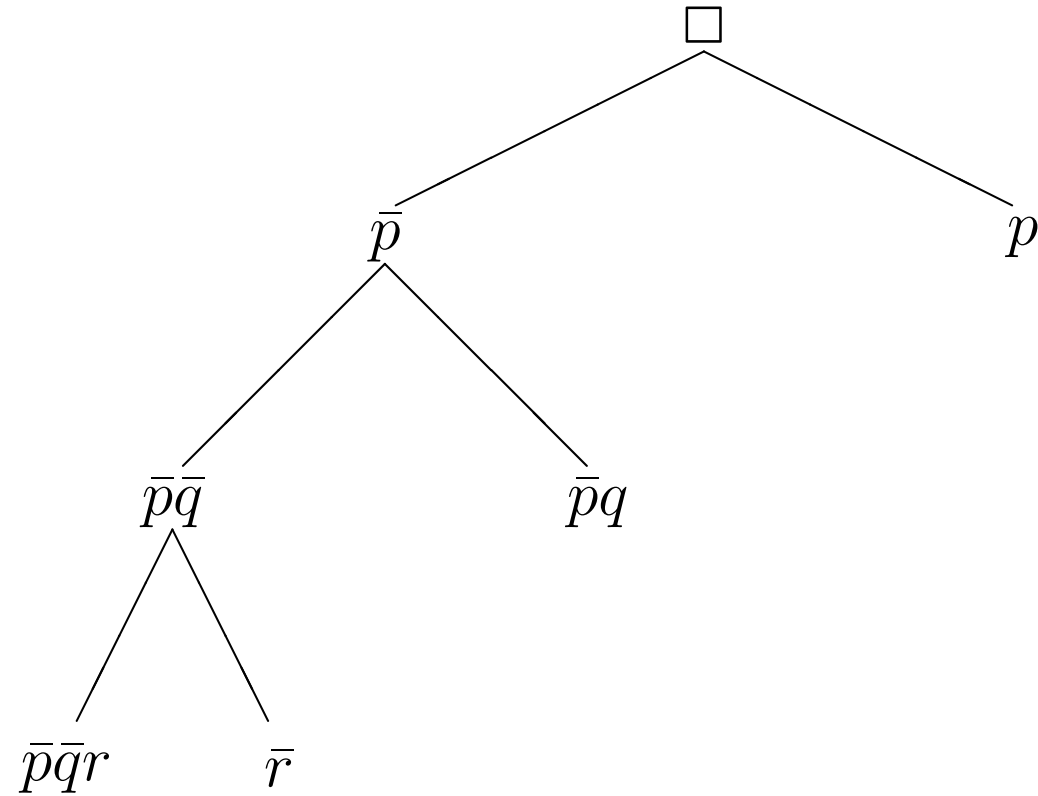


Figure 4.2: Incomplete resolution tree

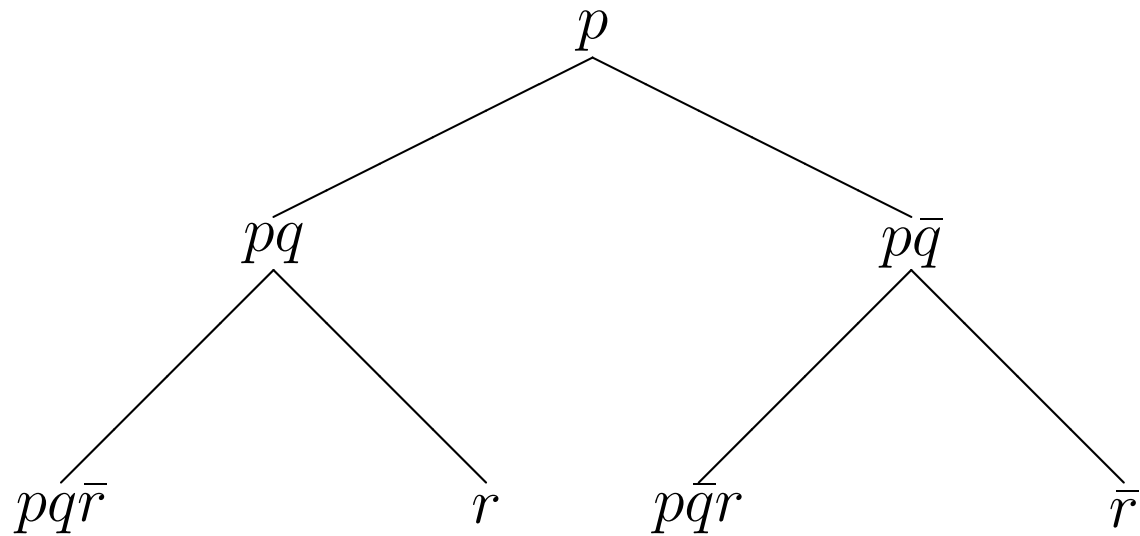


Figure 4.3: Semantic tree

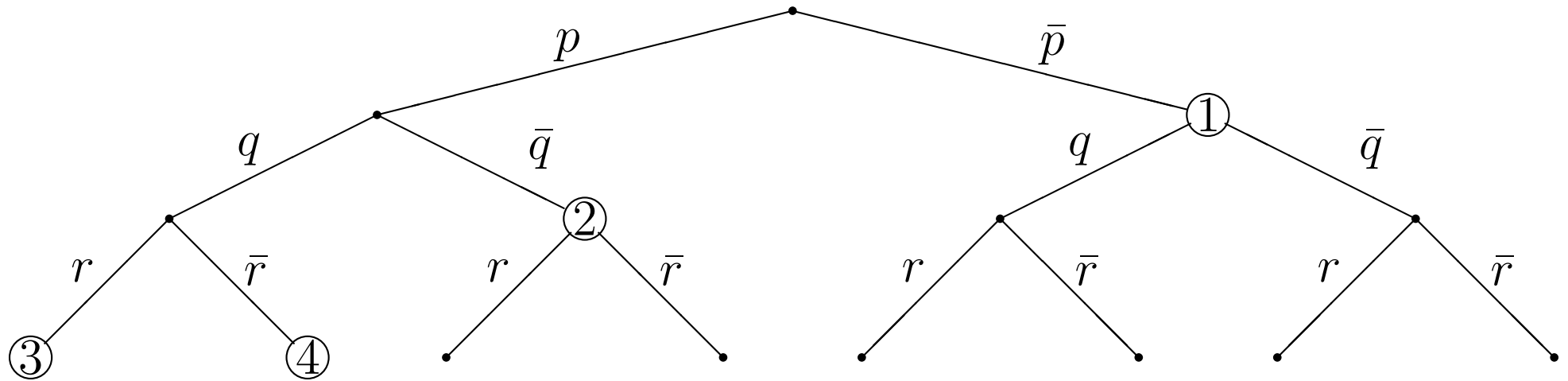
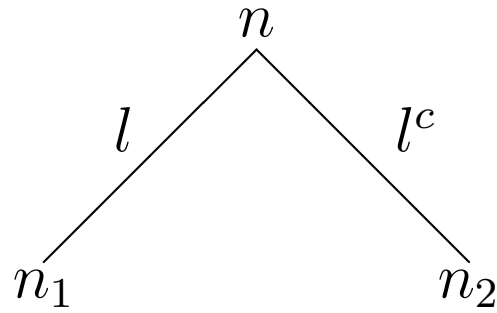
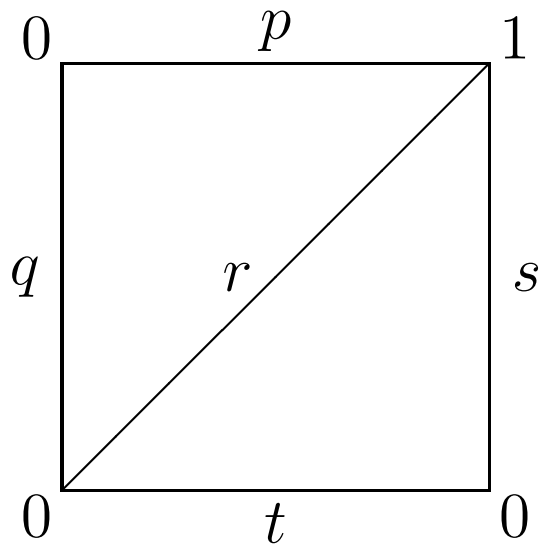


Figure 4.4: Inference and failure node



Section 4.5: Graph for Tseitin clauses



Section 5.1: Efficient truth table for $p \vee (q \wedge r)$

| p | q | r | $p \vee (q \wedge r)$ |
|-----|-----|-----|-----------------------|
| T | T | T | T |
| T | T | F | T |
| T | F | T | T |
| T | F | F | T |
| F | T | T | T |
| F | T | F | F |
| F | F | T | F |
| F | F | F | F |

| p | q | r | $p \vee (q \wedge r)$ |
|-----|-----|-----|-----------------------|
| T | T | * | T |
| T | F | * | T |

| p | q | r | $p \vee (q \wedge r)$ |
|-----|-----|-----|-----------------------|
| T | * | * | T |

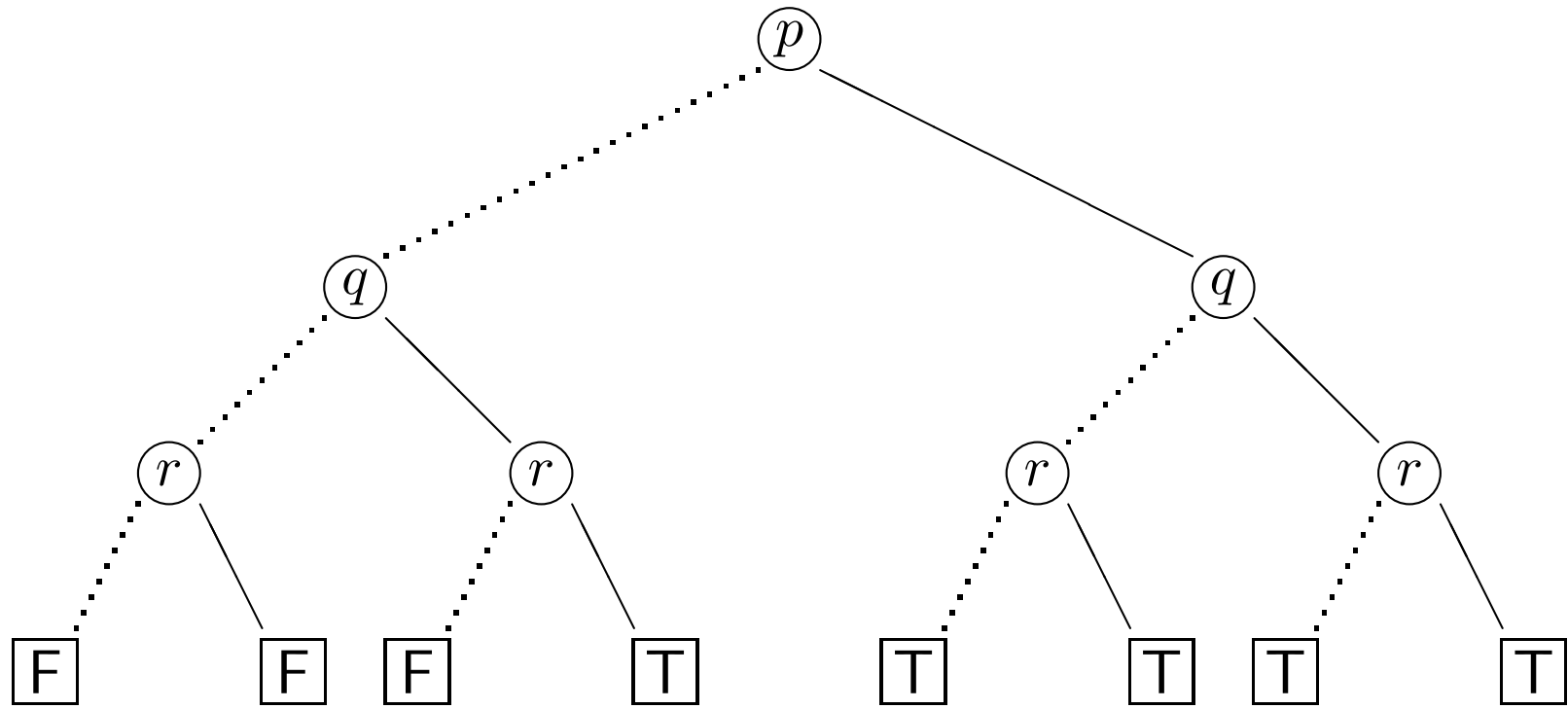
| p | q | r | $p \vee (q \wedge r)$ |
|-----|-----|-----|-----------------------|
| T | * | * | T |
| F | T | T | T |
| F | T | F | F |
| F | F | * | F |

Section 5.1: Efficient truth table for $p \oplus q \oplus r$

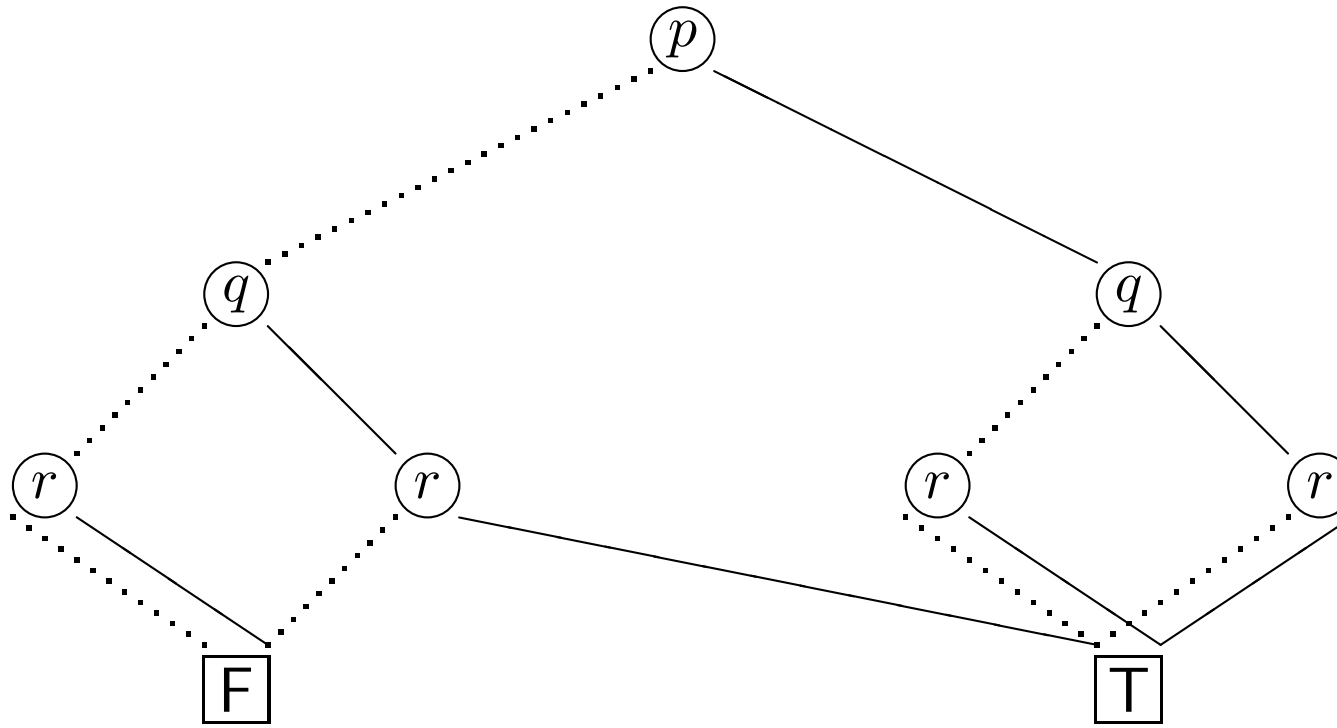
| p | q | r | $p \oplus q \oplus r$ |
|-----|-----|-----|-----------------------|
| T | T | T | T |
| T | T | F | F |
| T | F | T | F |
| T | F | F | T |
| F | T | T | F |
| F | T | F | T |
| F | F | T | T |
| F | F | F | F |

| p | q | r | $p \oplus q \oplus r$ |
|-----|-----|-----|-----------------------|
| T | T | T | T |
| T | T | F | F |
| T | F | T | F |
| T | F | F | T |
| F | T | * | (See rows 3 and 4.) |
| F | F | * | (See rows 1 and 2.) |

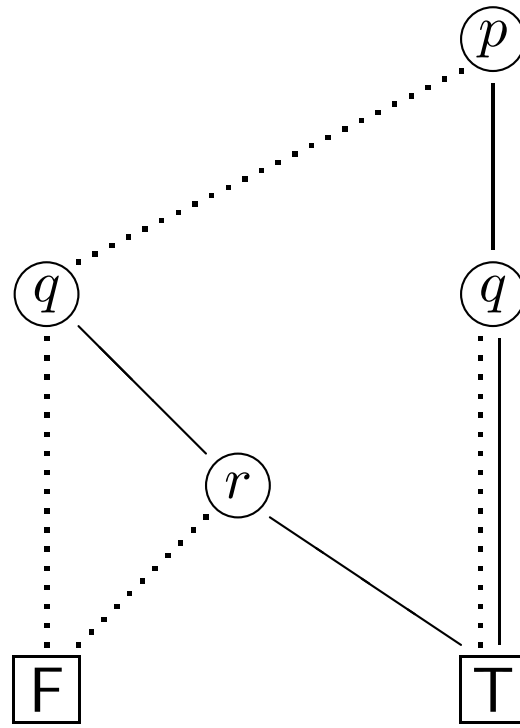
Figure 5.1: BDD for $p \vee (q \wedge r)$



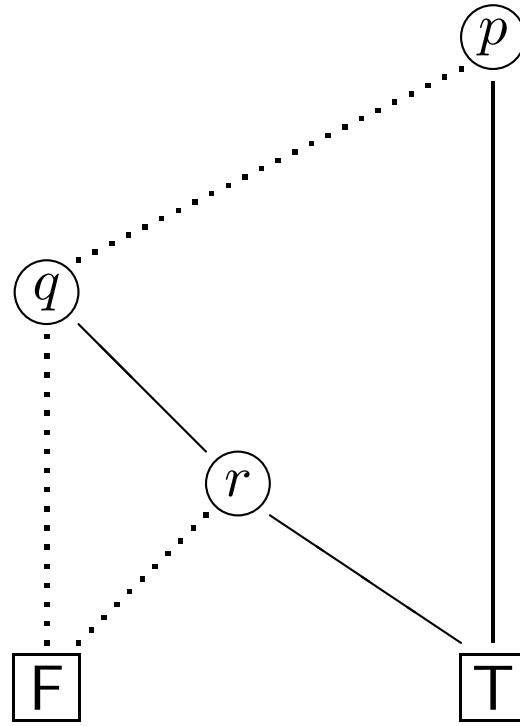
Example 5.6: First reduction of BDD for $p \vee (q \wedge r)$



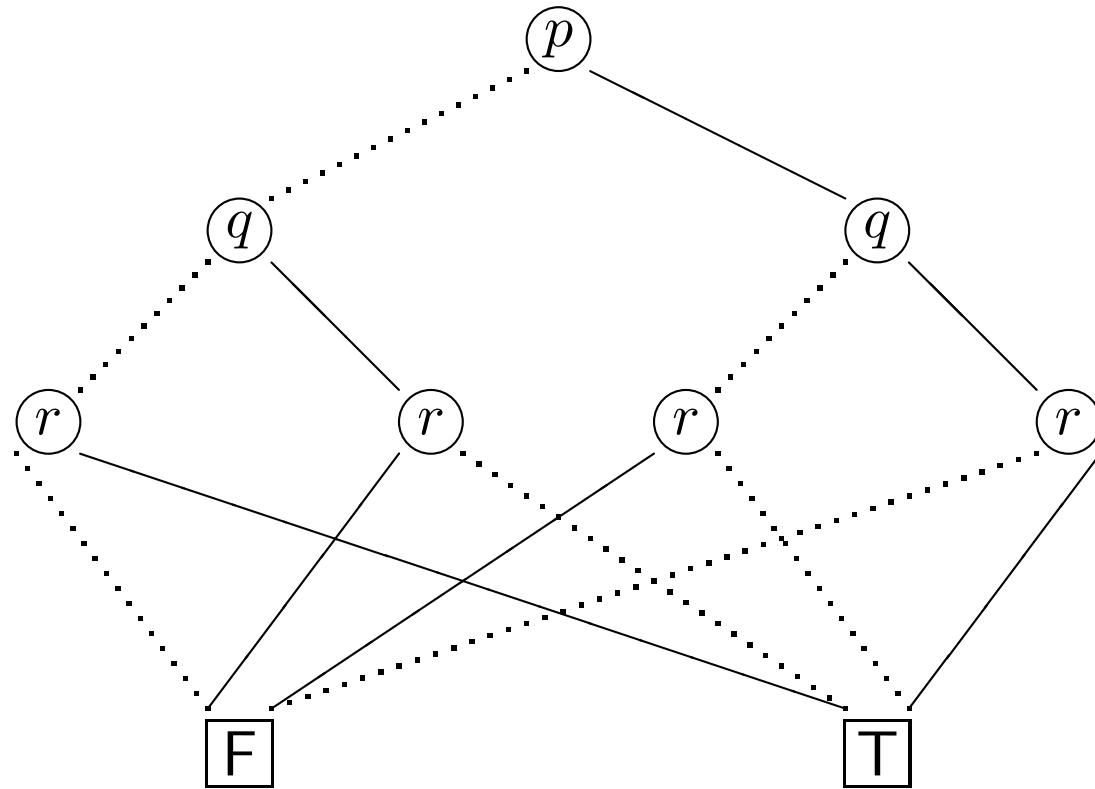
Example 5.6: Second reduction of BDD for $p \vee (q \wedge r)$



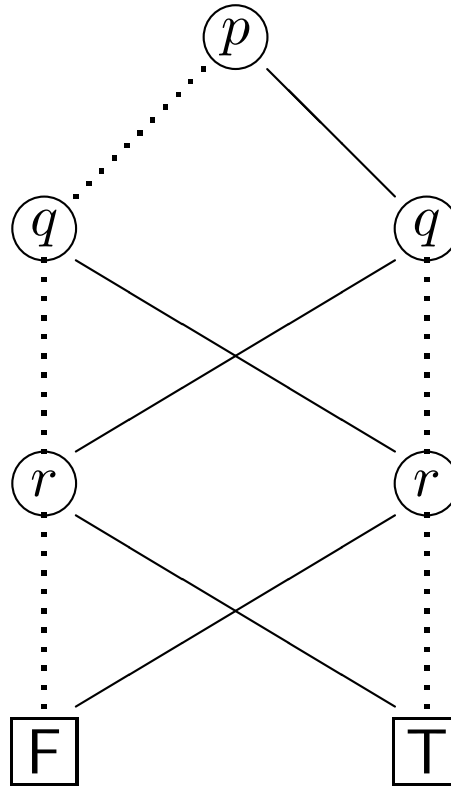
Example 5.6: Third reduction of BDD for $p \vee (q \wedge r)$



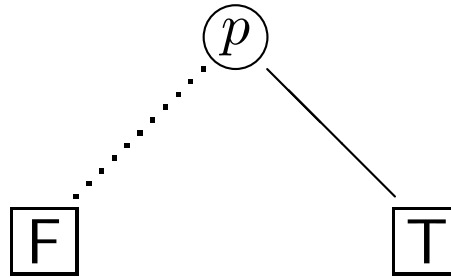
Example 5.7: BDD for $p \oplus q \oplus r$ after first reduction



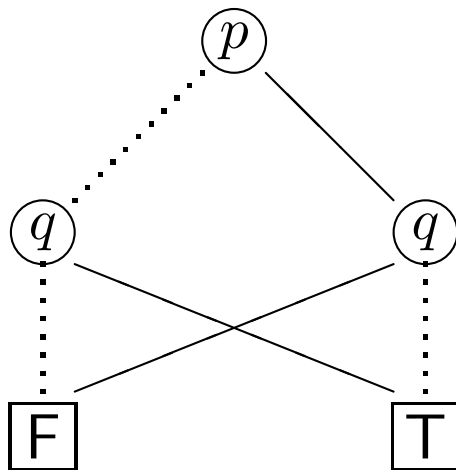
Example 5.6: BDD for $p \oplus q \oplus r$ after second reduction



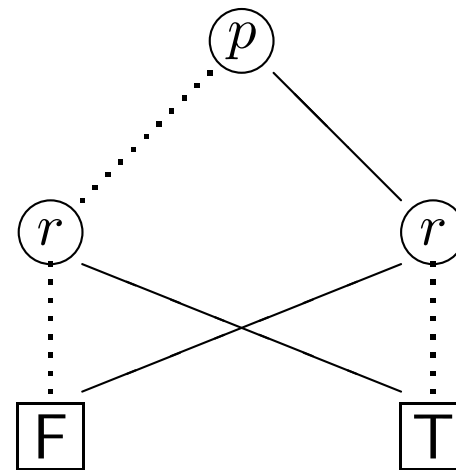
BDD for $(p \oplus q) \oplus (p \oplus r)$ from BDDs for $p \oplus q$ and $p \oplus r$



BDD for $p \oplus q$



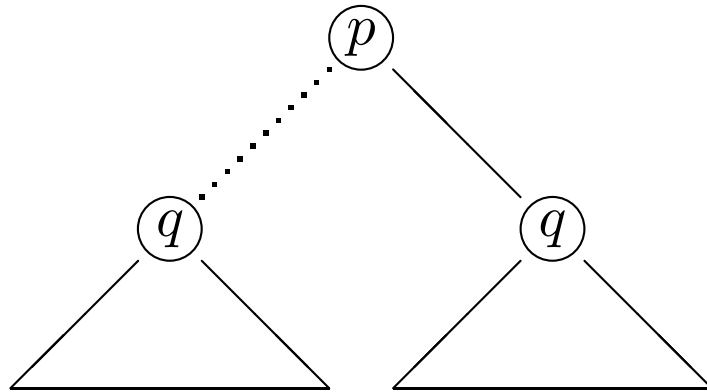
BDD for $p \oplus r$



\oplus

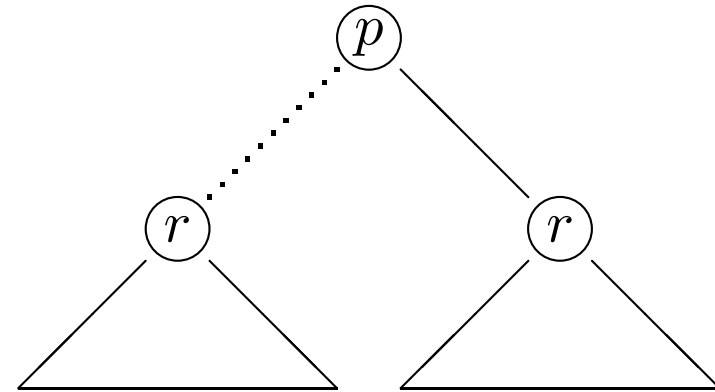
BDD for $(p \oplus q) \oplus (p \oplus r)$ from BDDs for $p \oplus q$ and $p \oplus r$

BDD for $p \oplus q$



\oplus

BDD for $p \oplus r$

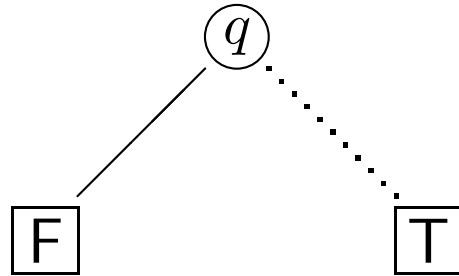


BDD for $F \oplus q$ BDD for $T \oplus q$

BDD for $F \oplus r$ BDD for $T \oplus r$

BDD for $(p \oplus q) \oplus (p \oplus r)$ from BDDs for $p \oplus q$ and $p \oplus r$

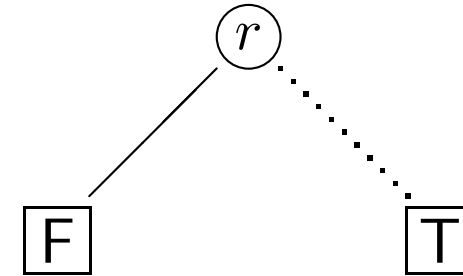
BDD for $\neg q$



BDD for $\neg T$

BDD for $\neg F$

BDD for $\neg r$



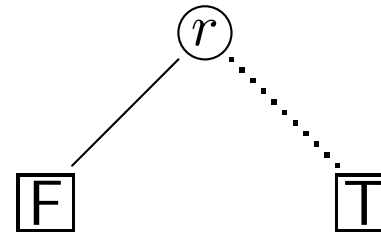
BDD for $\neg T$

BDD for $\neg F$

BDD for $\neg F$



BDD for $\neg r$



BDD for $\neg T$

BDD for $\neg F$

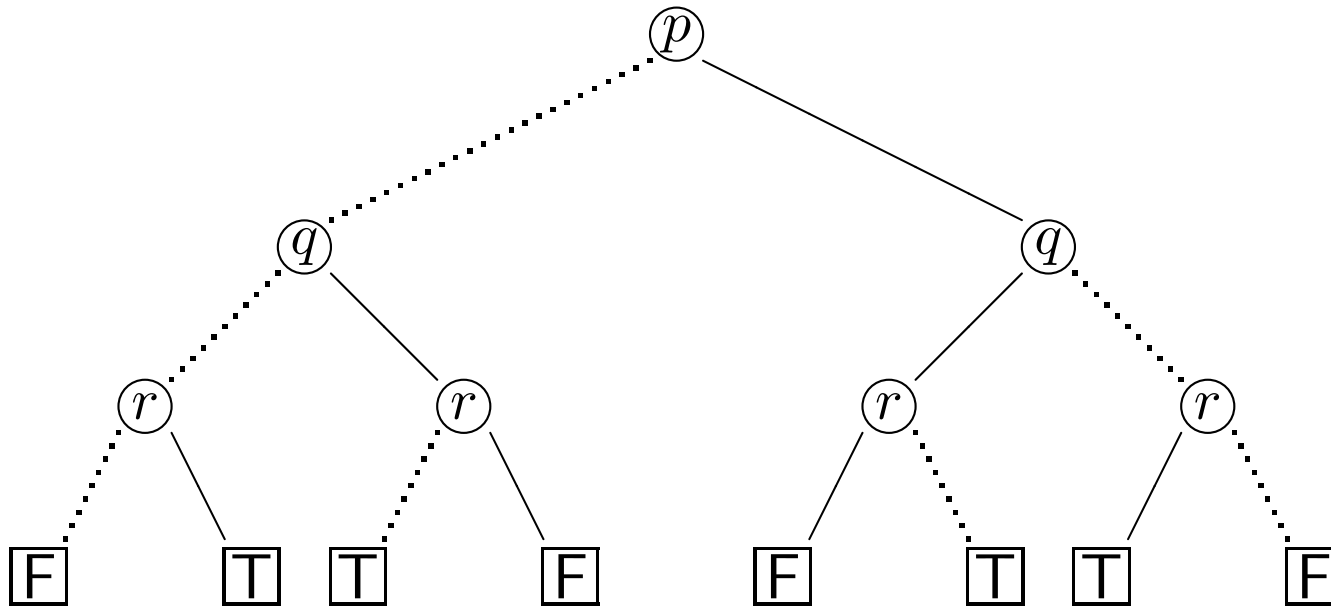
BDD for $(p \oplus q) \oplus (p \oplus r)$ from BDDs for $p \oplus q$ and $p \oplus r$

$$\begin{array}{ccccc} \text{BDD for } \neg F & & \text{BDD for } \neg T & & \text{BDD for } \neg F \oplus \neg T \\ \boxed{\text{T}} & \oplus & \boxed{\text{F}} & \equiv & \boxed{\text{T}} \end{array}$$

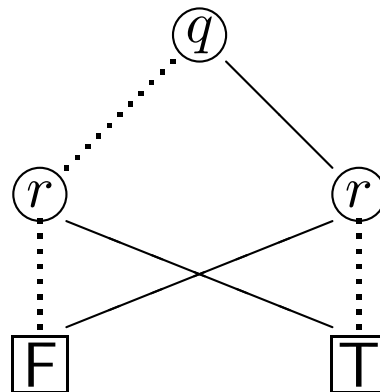
$$\begin{array}{ccccc} \text{BDD for } \neg F & & \text{BDD for } \neg F & & \text{BDD for } \neg F \oplus \neg F \\ \boxed{\text{T}} & \oplus & \boxed{\text{T}} & \equiv & \boxed{\text{F}} \end{array}$$

$$\begin{array}{ccccc} \text{BDD for } \neg F & & \text{BDD for } \neg r & & \text{BDD for } \neg F \oplus \neg r \\ \boxed{\text{T}} & \oplus & \begin{array}{c} \textcircled{r} \\ \swarrow \quad \searrow \\ \boxed{\text{F}} \quad \boxed{\text{T}} \end{array} & \equiv & \begin{array}{c} \textcircled{r} \\ \swarrow \quad \searrow \\ \boxed{\text{T}} \quad \boxed{\text{F}} \end{array} \end{array}$$

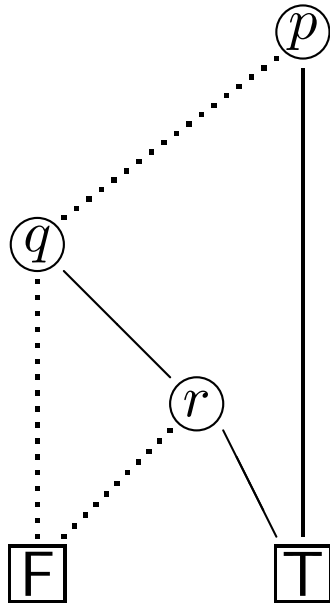
BDD for $(p \oplus q) \oplus (p \oplus r)$ from BDDs for $p \oplus q$ and $p \oplus r$



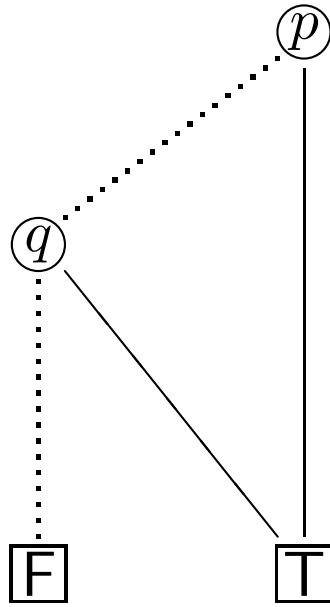
BDD for $q \oplus r$



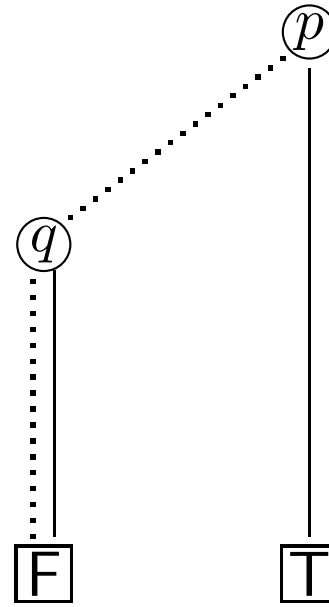
Example 5.21: Restriction



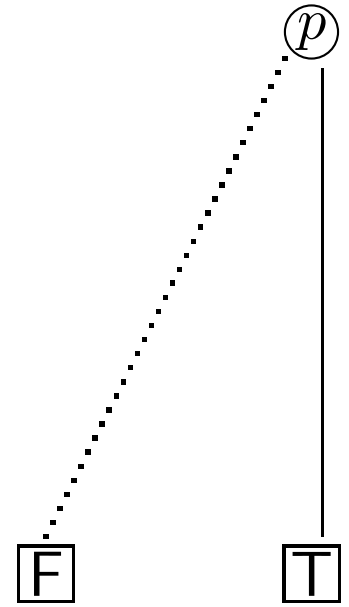
(a)



(b)



(c)



(b)

Section 6.4: 4-queens problem

| | | | | |
|---|---|---|---|---|
| 1 | | Q | | |
| 2 | | | | Q |
| 3 | Q | | | |
| 4 | | | Q | |
| | 1 | 2 | 3 | 4 |

Section 6.4.1: Encoding the 4-queens problem (1)

$$\begin{aligned}11 \vee 12 \vee 13 \vee 14, \\ 21 \vee 22 \vee 23 \vee 24, \\ 31 \vee 32 \vee 33 \vee 34, \\ 41 \vee 42 \vee 43 \vee 44.\end{aligned}$$

$$\begin{aligned}\overline{11} \vee \overline{12}, \quad \overline{11} \vee \overline{13}, \quad \overline{11} \vee \overline{14}, \quad \overline{12} \vee \overline{13}, \quad \overline{12} \vee \overline{14}, \quad \overline{13} \vee \overline{14}, \\ \overline{21} \vee \overline{22}, \quad \overline{21} \vee \overline{23}, \quad \overline{21} \vee \overline{24}, \quad \overline{22} \vee \overline{23}, \quad \overline{22} \vee \overline{24}, \quad \overline{23} \vee \overline{24}, \\ \overline{31} \vee \overline{32}, \quad \overline{31} \vee \overline{33}, \quad \overline{31} \vee \overline{34}, \quad \overline{32} \vee \overline{33}, \quad \overline{32} \vee \overline{34}, \quad \overline{33} \vee \overline{34}, \\ \overline{41} \vee \overline{42}, \quad \overline{41} \vee \overline{43}, \quad \overline{41} \vee \overline{44}, \quad \overline{42} \vee \overline{43}, \quad \overline{42} \vee \overline{44}, \quad \overline{43} \vee \overline{44},\end{aligned}$$

Section 6.4.1: Encoding the 4-queens problem (2)

$$\begin{array}{llllll} \overline{11} \vee \overline{21}, & \overline{11} \vee \overline{31}, & \overline{11} \vee \overline{41}, & \overline{21} \vee \overline{31}, & \overline{21} \vee \overline{41}, & \overline{31} \vee \overline{41}, \\ \overline{12} \vee \overline{22}, & \overline{12} \vee \overline{32}, & \overline{12} \vee \overline{42}, & \overline{22} \vee \overline{32}, & \overline{22} \vee \overline{42}, & \overline{32} \vee \overline{42}, \\ \overline{13} \vee \overline{23}, & \overline{13} \vee \overline{33}, & \overline{13} \vee \overline{43}, & \overline{23} \vee \overline{33}, & \overline{23} \vee \overline{43}, & \overline{33} \vee \overline{43}, \\ \overline{14} \vee \overline{24}, & \overline{14} \vee \overline{34}, & \overline{14} \vee \overline{44}, & \overline{24} \vee \overline{34}, & \overline{24} \vee \overline{44}, & \overline{34} \vee \overline{44}. \end{array}$$

$$\begin{array}{llllll} \overline{11} \vee \overline{22}, & \overline{11} \vee \overline{33}, & \overline{11} \vee \overline{44}, & \overline{12} \vee \overline{21}, & \overline{12} \vee \overline{23}, & \overline{12} \vee \overline{34}, \\ \overline{13} \vee \overline{22}, & \overline{13} \vee \overline{31}, & \overline{13} \vee \overline{24}, & \overline{14} \vee \overline{23}, & \overline{14} \vee \overline{32}, & \overline{14} \vee \overline{41}, \\ \overline{21} \vee \overline{32}, & \overline{21} \vee \overline{43}, & & \overline{22} \vee \overline{31}, & \overline{22} \vee \overline{33}, & \overline{22} \vee \overline{44}, \\ \overline{23} \vee \overline{32}, & \overline{23} \vee \overline{41}, & \overline{23} \vee \overline{34}, & \overline{24} \vee \overline{33}, & \overline{22} \vee \overline{42}, & \\ \overline{31} \vee \overline{42}, & & & \overline{32} \vee \overline{41}, & \overline{32} \vee \overline{43}, & \\ \overline{33} \vee \overline{42}, & \overline{33} \vee \overline{44}, & & \overline{34} \vee \overline{43}. & & \end{array}$$

Figure 7.1: Tree for $\forall x(\neg \exists y p(x, y) \vee \neg \exists y p(y, x))$

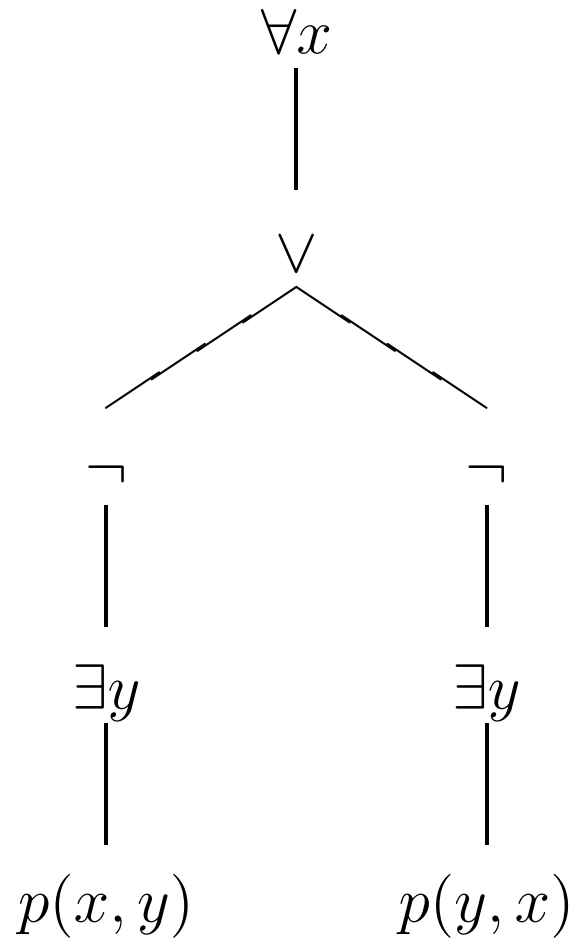


Figure 7.2: Global and local variables

```
class MyClass {  
    int x;  
    void p() {  
        int x;  
        x = 1;  
        // Print the value of x  
    }  
    void q() {  
        // Print the value of x  
    }  
    ... void main(...) {  
x = 5;  
p;  
q;  
}
```

Logically equivalent formulas (1)

$$\forall x A(x) \leftrightarrow \neg \exists x \neg A(x)$$

$$\exists x A(x) \leftrightarrow \neg \forall x \neg A(x)$$

$$\forall x \forall y A(x, y) \leftrightarrow \forall y \forall x A(x, y)$$

$$\exists x \exists y A(x, y) \leftrightarrow \exists y \exists x A(x, y)$$

$$\exists x \forall y A(x, y) \rightarrow \forall y \exists x A(x, y)$$

$$(\exists x A(x) \vee B) \leftrightarrow \exists x (A(x) \vee B) \quad (\forall x A(x) \vee B) \leftrightarrow \forall x (A(x) \vee B)$$

$$(B \vee \exists x A(x)) \leftrightarrow \exists x (B \vee A(x)) \quad (B \vee \forall x A(x)) \leftrightarrow \forall x (B \vee A(x))$$

$$(\exists x A(x) \wedge B) \leftrightarrow \exists x (A(x) \wedge B) \quad (\forall x A(x) \wedge B) \leftrightarrow \forall x (A(x) \wedge B)$$

$$(B \wedge \exists x A(x)) \leftrightarrow \exists x (B \wedge A(x)) \quad (B \wedge \forall x A(x)) \leftrightarrow \forall x (B \wedge A(x))$$

Logically equivalent formulas (2)

$$\forall x(A \rightarrow B(x)) \leftrightarrow (A \rightarrow \forall x B(x))$$

$$\forall x(A(x) \rightarrow B) \leftrightarrow (\exists x A(x) \rightarrow B)$$

$$(\exists x(A(x) \vee B(x))) \leftrightarrow (\exists x A(x) \vee \exists x B(x))$$

$$\forall x(A(x) \wedge B(x)) \leftrightarrow (\forall x A(x) \wedge \forall x B(x))$$

$$\forall x A(x) \vee \forall x B(x) \rightarrow \forall x(A(x) \vee B(x))$$

$$\exists x(A(x) \wedge B(x)) \rightarrow (\exists x A(x) \wedge \exists x B(x))$$

$$\forall x(A(x) \leftrightarrow B(x)) \rightarrow (\forall x A(x) \leftrightarrow \forall x B(x))$$

$$\forall x(A(x) \leftrightarrow B(x)) \rightarrow (\exists x A(x) \leftrightarrow \exists x B(x))$$

$$\exists x(A(x) \rightarrow B(x)) \leftrightarrow (\forall x A(x) \rightarrow \exists x B(x))$$

$$(\exists x A(x) \rightarrow \forall x B(x)) \rightarrow \forall x(A(x) \rightarrow B(x))$$

Logically equivalent formulas (3)

$$\forall x(A(x) \vee B(x)) \rightarrow (\forall x A(x) \vee \exists x B(x))$$

$$\forall x(A(x) \rightarrow B(x)) \rightarrow (\forall x A(x) \rightarrow \forall x B(x))$$

$$\forall x(A(x) \rightarrow B(x)) \rightarrow (\exists x A(x) \rightarrow \exists x B(x))$$

$$\forall x(A(x) \rightarrow B(x)) \rightarrow (\forall x A(x) \rightarrow \exists x B(x))$$

Figure 7.3: Semantic tableau for a satisfiable formula

$$\begin{array}{c} \neg (\forall x(p(x) \vee q(x)) \rightarrow (\forall x p(x) \vee \forall x q(x))) \\ \downarrow \\ \forall x(p(x) \vee q(x)), \neg (\forall x p(x) \vee \forall x q(x)) \\ \downarrow \\ \forall x(p(x) \vee q(x)), \neg \forall x p(x), \neg \forall x q(x) \\ \downarrow \\ \forall x(p(x) \vee q(x)), \neg \forall x p(x), \neg q(a) \\ \downarrow \\ \forall x(p(x) \vee q(x)), \neg p(a), \neg q(a) \\ \downarrow \\ p(a) \vee q(a), \neg p(a), \neg q(a) \\ \swarrow \quad \searrow \\ p(a), \neg p(a), \neg q(a) \quad q(a), \neg p(a), \neg q(a) \\ \times \qquad \qquad \qquad \times \end{array}$$

Figure 7.4: A tableau that should close, but doesn't

$$\begin{array}{c} \forall x \exists y p(x, y) \wedge \forall x (q(x) \wedge \neg q(x)) \\ \downarrow \\ \forall x \exists y p(x, y), \forall x (q(x) \wedge \neg q(x)) \\ \downarrow \\ \forall x \exists y p(x, y), \exists y p(a_1, y), \forall x (q(x) \wedge \neg q(x)) \\ \downarrow \\ \forall x \exists y p(x, y), p(a_1, a_2), \forall x (q(x) \wedge \neg q(x)) \\ \downarrow \\ \forall x \exists y p(x, y), p(a_1, a_2), \forall x (q(x) \wedge \neg q(x)) \\ \downarrow \\ \forall x \exists y p(x, y), \exists y p(a_2, y), p(a_1, a_2), \forall x (q(x) \wedge \neg q(x)) \\ \downarrow \\ \forall x \exists y p(x, y), p(a_2, a_3), p(a_1, a_2), \forall x (q(x) \wedge \neg q(x)) \end{array}$$

Rules for γ - and δ -formulas

| γ | $\gamma(a)$ |
|-----------------------|-------------|
| $\forall x A(x)$ | $A(a)$ |
| $\neg \exists x A(x)$ | $\neg A(a)$ |

| δ | $\delta(a)$ |
|-----------------------|-------------|
| $\exists x A(x)$ | $A(a)$ |
| $\neg \forall x A(x)$ | $\neg A(a)$ |

Figure 8.1: Semantic tableau in first-order logic

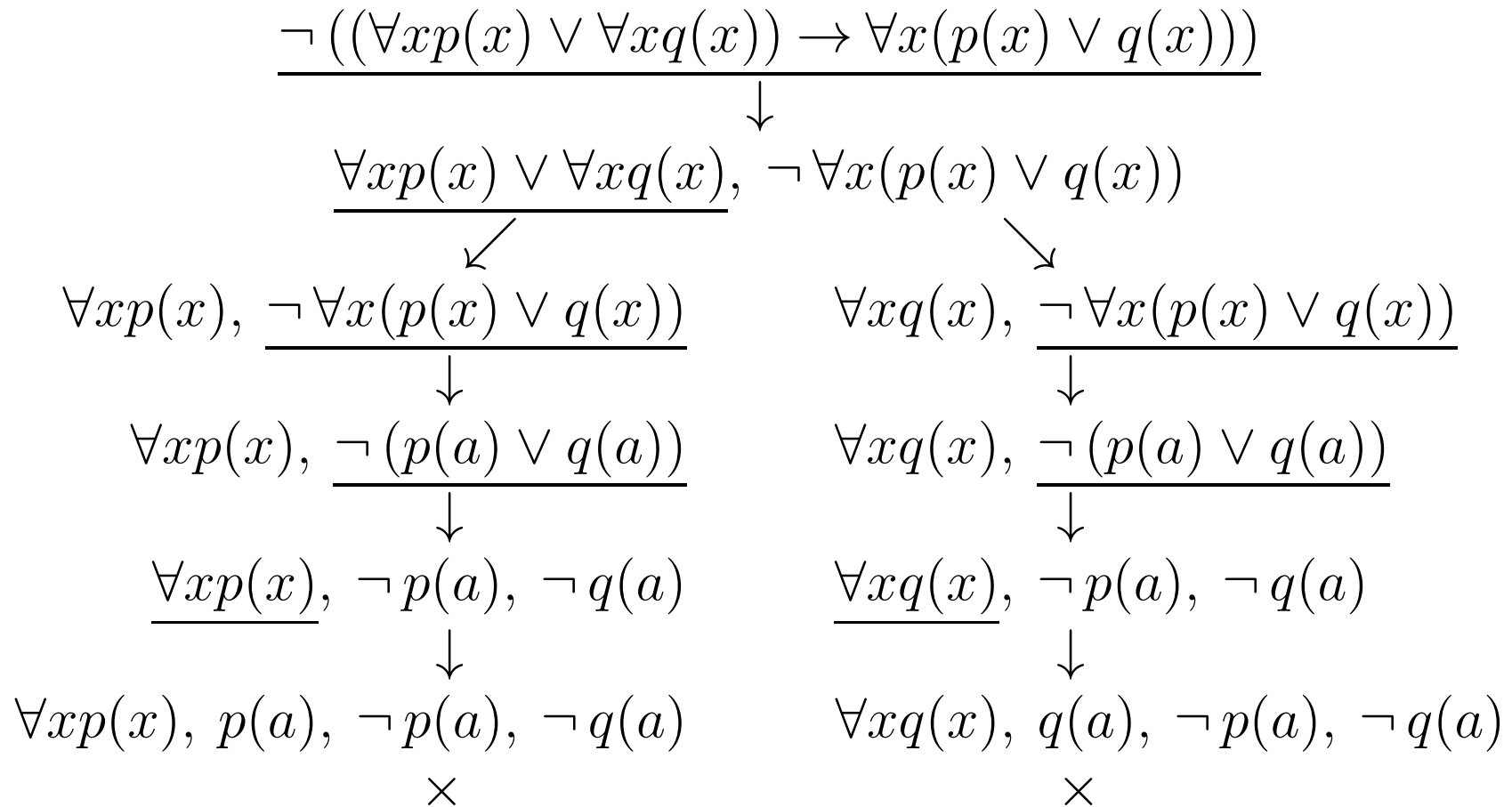
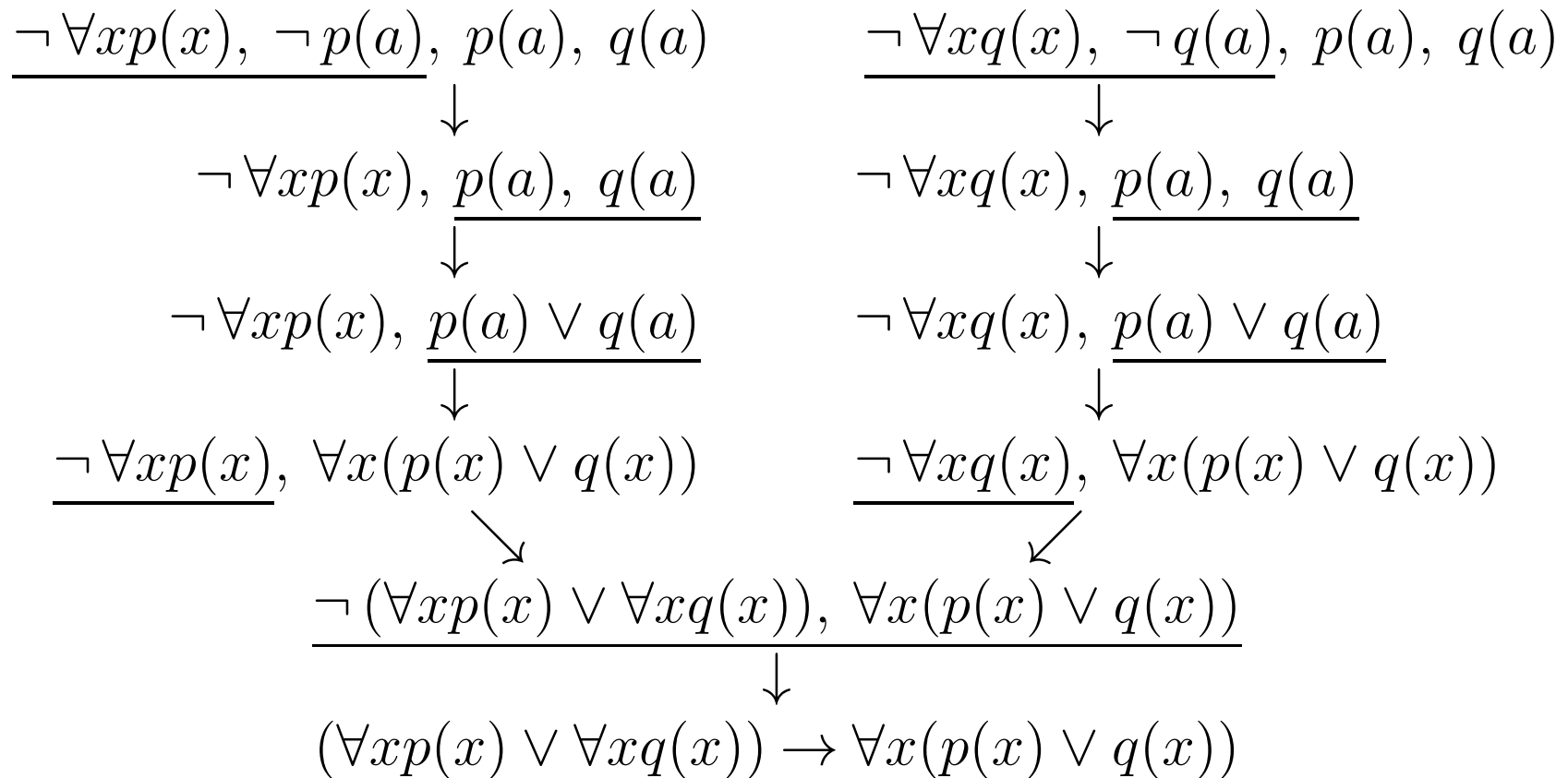


Figure 8.2: Gentzen proof tree in first-order logic



Rules for γ - and δ -formulas

$$\frac{U \cup \{\gamma, \gamma(a)\}}{U \cup \{\gamma\}}$$

$$\frac{U \cup \{\delta(a)\}}{U \cup \{\delta\}},$$

The rule for δ -formulas can be applied only if the constant a does not occur in any formula of U .

| γ | $\gamma(a)$ |
|-----------------------|-------------|
| $\exists x A(x)$ | $A(a)$ |
| $\neg \forall x A(x)$ | $\neg A(a)$ |

| δ | $\delta(a)$ |
|-----------------------|-------------|
| $\forall x A(x)$ | $A(a)$ |
| $\neg \exists x A(x)$ | $\neg A(a)$ |

Figure 8.3: δ -formulas follow γ -formulas

$$\begin{array}{c}
 \hline \neg \forall y p(a, y), \neg p(a, b), \neg p(a, a), \exists x p(x, b), p(a, b) \\
 \downarrow \\
 \hline \neg \forall y p(a, y), \neg p(a, a), \exists x p(x, b), p(a, b) \\
 \downarrow \\
 \neg \forall y p(a, y), \hline \exists x p(x, b), p(a, b) \\
 \downarrow \\
 \neg \forall y p(a, y), \hline \exists x p(x, b) \\
 \downarrow \\
 \hline \neg \forall y p(a, y), \forall y \exists x p(x, y) \\
 \downarrow \\
 \hline \neg \exists x \forall y p(x, y), \forall y \exists x p(x, y) \\
 \downarrow \\
 \exists x \forall y p(x, y) \rightarrow \forall y \exists x p(x, y)
 \end{array}$$

Hilbert system \mathcal{H}

Axiom 1 $\vdash (A \rightarrow (B \rightarrow A)),$

Axiom 2 $\vdash (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)),$

Axiom 3 $\vdash (\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B),$

Axiom 4 $\vdash \forall x A(x) \rightarrow A(a),$

Axiom 5 $\vdash \forall x (A \rightarrow B(x)) \rightarrow (A \rightarrow \forall x B(x)).$

Modus ponens
$$\frac{\vdash A \rightarrow B \quad \vdash A}{\vdash B}$$

Generalization
$$\frac{\vdash A(a)}{\vdash \forall x A(x)}.$$

In Axiom 5, $B(x)$ is a formula with a free variable x , while x is *not* a free variable of the formula A .

Derived rules of inference

Generalization $\frac{U \vdash A(a)}{U \vdash \forall x A(x)}$, a does not appear in U .

Deduction $\frac{U \cup \{A\} \vdash B}{U \vdash A \rightarrow B}$

Axiom 4 $\frac{U \vdash \forall x A(x)}{U \vdash A(a)}$

Generalization $\frac{\vdash A(a) \rightarrow B(a)}{\vdash \forall x A(x) \rightarrow \forall x B(x)}$

C-rule $\frac{U \vdash \exists x A(x)}{U \vdash A(a)}$, a does not appear in U or $\exists x A(x)$.

Figure 9.1: Finite sequences of terms (1)

$$n = 1 \quad a$$

$$n = 2 \quad b$$

$$n = 3 \quad f(a), f(b), f(f(a)), f(f(b))$$

$$n = 4 \quad f(f(f(a))), f(f(f(b))),$$

$g(a, a), g(a, b), g(a, f(a)), g(a, f(b)), g(a, f(f(a))), g(a, f(f(b))),$
six similar terms with b as the first argument of g ,

$g(f(a), a), g(f(a), b), g(f(a), f(a)), g(f(a), f(b)),$
 $g(f(a), f(f(a))), g(f(a), f(f(b))),$
six similar terms with $f(b)$ as the first argument of g ,

Figure 9.1: Finite sequences of terms (2)

$g(f(f(a)), a), g(f(f(a)), b), g(f(f(a)), f(a)), g(f(f(a)), f(b)),$
 $g(f(f(a)), f(f(a))), g(f(f(a)), f(f(b))),$

six similar terms with $f(f(b))$ as the first argument of g ,

$f(g(a, a)), f(g(a, b)), f(g(a, f(a))), f(g(a, f(b))),$

twelve similar terms with $b, f(a), f(b)$ as the first argument of g ,

$f(f(g(a, a))), f(f(g(a, b))), f(f(g(b, a))), f(f(g(b, b))).$

Example 9.20: Hebrand universes

$$S_1 = \{pa \neg pbqz, \neg qz \neg pbqz\}$$

$$H_{S_1} = \{a, b\}$$

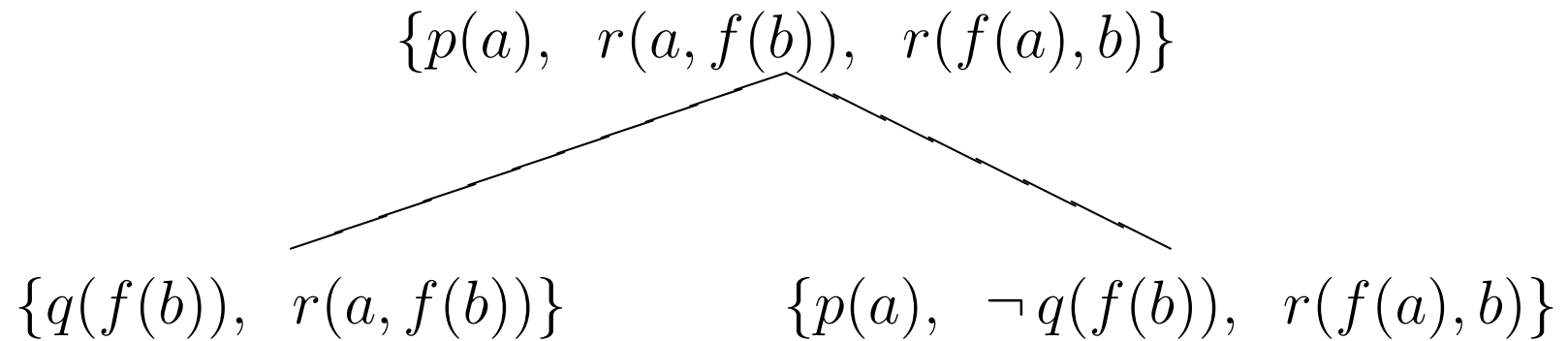
$$S_2 = \{\neg pxf(y), pwg(w)\}$$

$$H_{S_2} = \{a, f(a), g(a), \\ f(f(a)), g(f(a)), f(g(a)), g(g(a)), \dots\}$$

$$S_3 = \{\neg paf(x, y), pbf(x, y)\}$$

$$H_{S_3} = \{a, b, f(a, a), f(a, b), f(b, a), f(b, b), \\ f(a, f(a, a)), f(f(a, a), a), \dots\}$$

Example 10.2: Ground resolution



Example 10.7: Unification

$$\begin{array}{lllll} \langle & g(y) = x, & f(x, h(x), y) = f(g(z), w, z) & & \rangle \\ \langle & f(g(y), h(g(y)), y) = f(g(z), w, z), & x = g(y) & & \rangle \\ \langle & g(y) = g(z), & h(g(y)) = w, & y = z, & x = g(y) \rangle \\ \langle & y = z, & h(g(y)) = w, & y = z, & x = g(y) \rangle \\ \langle & h(g(z)) = w, & z = z, & x = g(z), & y = z \rangle \\ \langle & z = z, & x = g(z), & y = z, & w = h(g(z)) \rangle \\ \langle & x = g(z), & y = z, & w = h(g(z)) & \rangle \end{array}$$

Example 10.29: Resolution refutation (1)

1. $\neg p(x) \vee q(x) \vee r(x, f(x))$
2. $\neg p(x) \vee q(x) \vee s(f(x))$
3. $t(a)$
4. $p(a)$
5. $\neg r(a, y) \vee t(y)$
6. $\neg t(x) \vee \neg q(x)$
7. $\neg t(x) \vee \neg s(x)$

Example 10.29: Resolution refutation (2)

| | | | |
|-----|------------------------|---------------------|--------|
| 8. | $\neg q(a)$ | $x \leftarrow a$ | 3, 6 |
| 9. | $q(a) \vee s(f(a))$ | $x \leftarrow a$ | 2, 4 |
| 10. | $s(f(a))$ | | 8, 9 |
| 11. | $q(a) \vee r(a, f(a))$ | $x \leftarrow a$ | 1, 4 |
| 12. | $r(a, f(a))$ | | 8, 11 |
| 13. | $t(f(a))$ | $y \leftarrow f(a)$ | 5, 12 |
| 14. | $\neg s(f(a))$ | $x \leftarrow f(a)$ | 7, 13 |
| 15. | \square | | 10, 14 |

Example 10.30: Resolution refutation

| | | | |
|-------------|---|--|---------------------|
| 1. | $\neg p(x, y) \vee p(y, x)$ | | |
| 2. | $\neg p(x, y) \vee \neg p(y, z) \vee p(x, z)$ | | |
| 3. | $p(x, f(x))$ | | |
| 4. | $\neg p(x, x)$ | | |
| 3'. | $p(x', f(x'))$ | | Rename 3 |
| 5. | $p(f(x), x)$ | $\sigma_1 = \{y \leftarrow f(x), x' \leftarrow x\}$ | 1, 3' |
| 3''. | $p(x'', f(x''))$ | | Rename 3 |
| 6. | $\neg p(f(x), z) \vee p(x, z)$ | $\sigma_2 = \{y \leftarrow f(x), x'' \leftarrow x\}$ | 2, 3'' |
| 5'''. 7. | $p(f(x'''), x''')$ $p(x, x)$ | $\sigma_3 = \{z \leftarrow x, x''' \leftarrow x\}$ | Rename 5 6, 5''' |
| 4'''. 8. | $\neg p(x''', x''')$ \square | $\sigma_4 = \{x'''' \leftarrow x\}$ | Rename 4 7, 4''' |

Theorem 10.33: Lifting Lemma

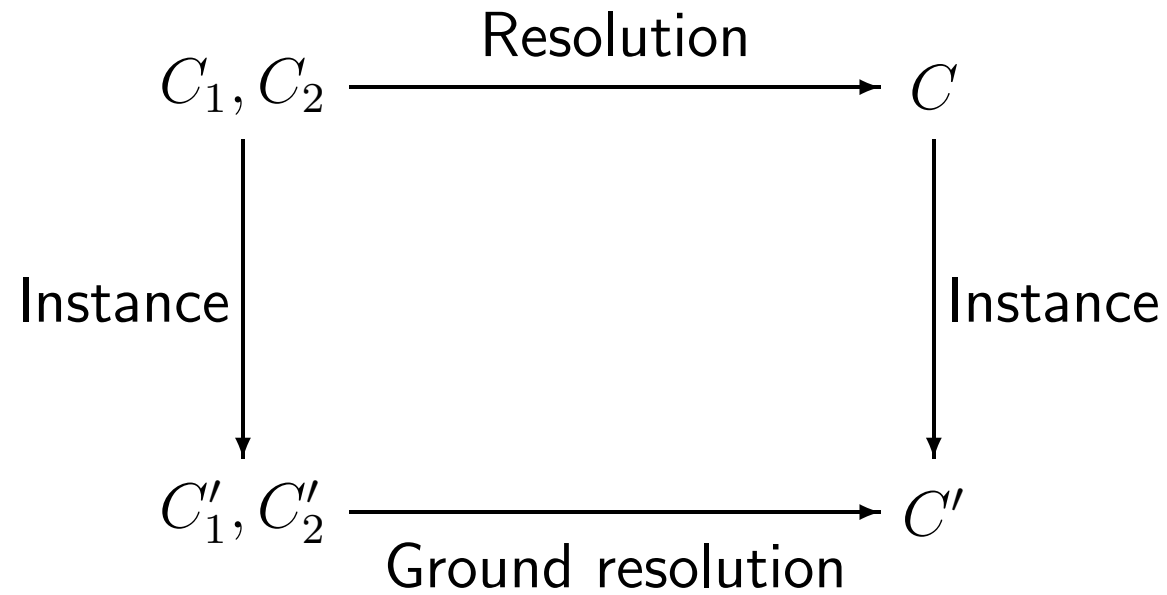


Figure 10.1: Example for the lifting lemma (1)

$$C_1 = \{p(x), p(f(y)), p(f(z)), q(x)\}$$

$$C_2 = \{\neg p(f(u)), \neg p(w), r(u)\}$$

$$\theta_1 = \{x \leftarrow f(a), y \leftarrow a, z \leftarrow a\}$$

$$\theta_2 = \{u \leftarrow a, w \leftarrow f(a)\}$$

$$C'_1 = C_1\theta_1 = \{p(f(a)), q(f(a))\}$$

$$C'_2 = C_2\theta_2 = \{\neg p(f(a)), r(a)\}$$

$$C' = Res(C_1, C_2) = \{q(f(a)), r(a)\}$$

Figure 10.1: Example for the lifting lemma (2)

$$L_1 = \{p(x), p(f(y)), p(f(z))\}$$

$$\lambda_1 = \{x \leftarrow f(y), z \leftarrow y\}$$

$$L_1\lambda_1 = \{p(f(y))\}$$

$$L_2 = \{\neg p(f(u)), \neg p(w)\}$$

$$\lambda_2 = \{w \leftarrow f(u)\}$$

$$L_2\lambda_2 = \{\neg p(f(u))\}$$

$$\lambda = \lambda_1 \cup \lambda_2 = \{x \leftarrow f(y), z \leftarrow y, w \leftarrow f(u)\}$$

$$L_1\lambda = \{p(f(y))\}$$

$$C_1\lambda = \{p(f(y)), q(f(y))\}$$

$$L_2\lambda = \{\neg p(f(u))\}$$

$$C_2\lambda = \{\neg p(f(u)), r(u)\}$$

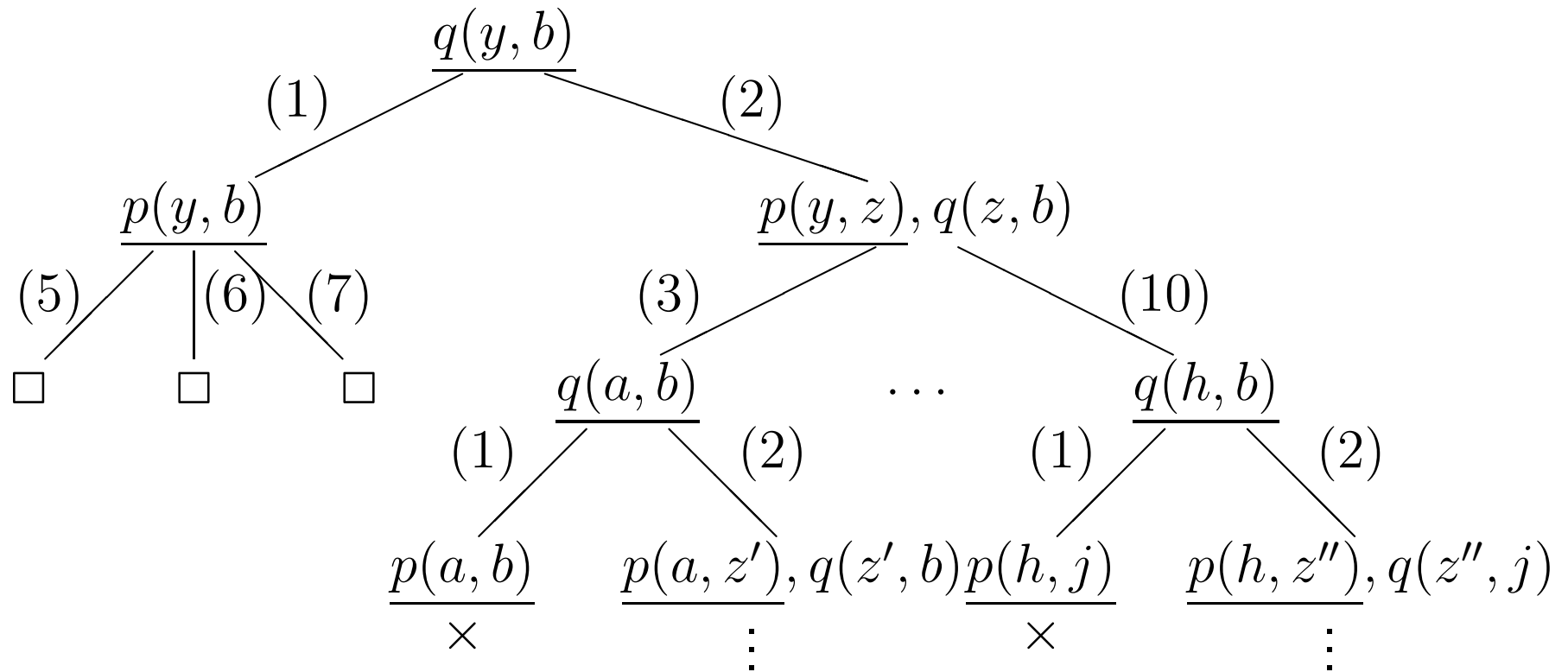
Figure 10.1: Example for the lifting lemma (3)

$$\begin{aligned}\sigma &= \{u \leftarrow y\} \\ C &= Res(C_1\lambda, C_2\lambda) = \{q(f(y)), r(y)\}, \text{ using } \sigma \\ \lambda\sigma &= \{x \leftarrow f(y), z \leftarrow y, w \leftarrow f(y), u \leftarrow y\} \\ C_1\lambda\sigma &= \{p(f(y)), q(f(y))\} \\ C_2\lambda\sigma &= \{\neg p(f(y)), r(y)\} \\ C &= Res(C_1, C_2) = \{q(f(y)), r(y)\}, \text{ using } \lambda\sigma\end{aligned}$$

$$\begin{aligned}\theta'_1 &= \{y \leftarrow a\} \\ C'_1 &= C_1\theta_1 = \{p(f(a)), q(f(a))\} = C_1\lambda\sigma\theta_1 \\ \theta'_2 &= \{y \leftarrow a\} \\ C'_2 &= C_2\theta_2 = \{\neg p(f(a)), r(a)\} = C_2\lambda\sigma\theta_2\end{aligned}$$

$$\begin{aligned}\theta' &= \{y \leftarrow a\} \\ C' &= Res(C'_1, C'_2) = \{q(f(a)), r(a)\}\end{aligned}$$

Figure 11.1: SLD-tree for selection of leftmost literal



Theorem 12.3: Church's Theorem

$$S_M = \left(\bigwedge_{i=0}^n S_i \wedge p_0(a, a) \right) \rightarrow \exists z_1 \exists z_2 p_n(z_1, z_2).$$

| L_i | S_i |
|--|--|
| $x = x + 1;$ | $\forall x \forall y (p_i(x, y) \rightarrow p_{i+1}(s(x), y))$ |
| $y = y + 1;$ | $\forall x \forall y (p_i(x, y) \rightarrow p_{i+1}(x, s(y)))$ |
| if $(x == 0)$ goto Lj; else $x = x - 1;$ | $\forall x (p_i(a, x) \rightarrow p_j(a, x)) \wedge$ $\forall x \forall y (p_i(s(x), y) \rightarrow p_{i+1}(x, y))$ |
| if $(y == 0)$ then goto Lj; else $y = y - 1;$ | $\forall x (p_i(x, a) \rightarrow p_j(x, a)) \wedge$ $\forall x \forall y (p_i(x, s(y)) \rightarrow p_{i+1}(x, y))$ |

Figure 13.1: State transition diagram

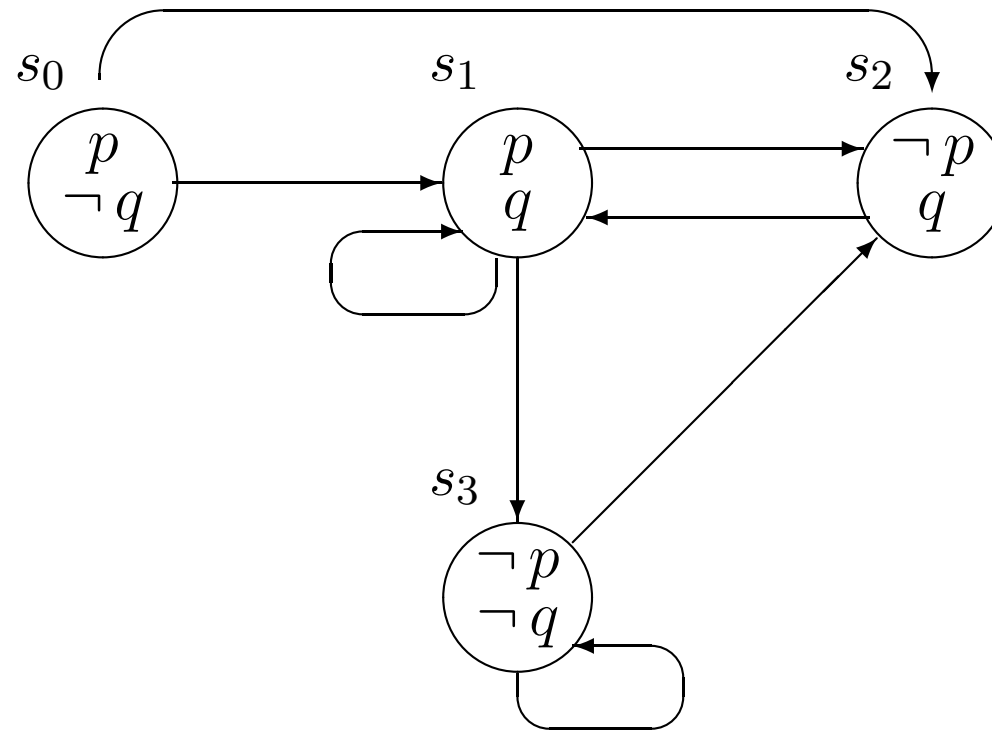
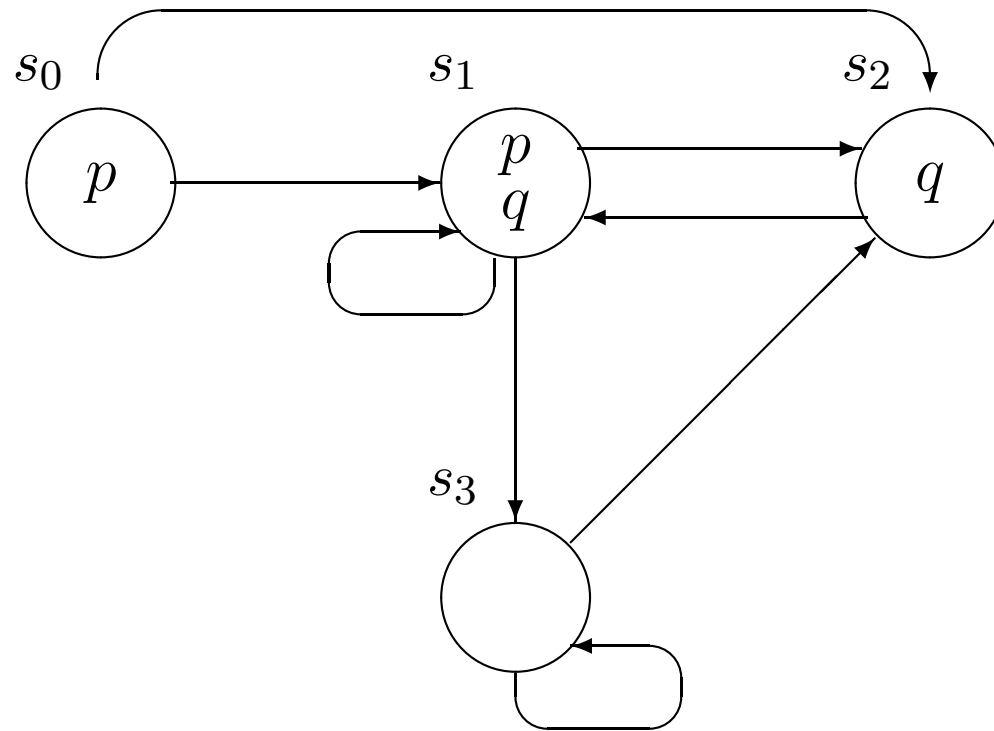
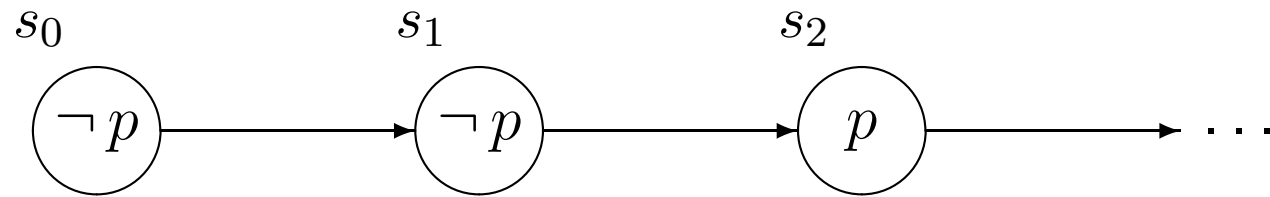


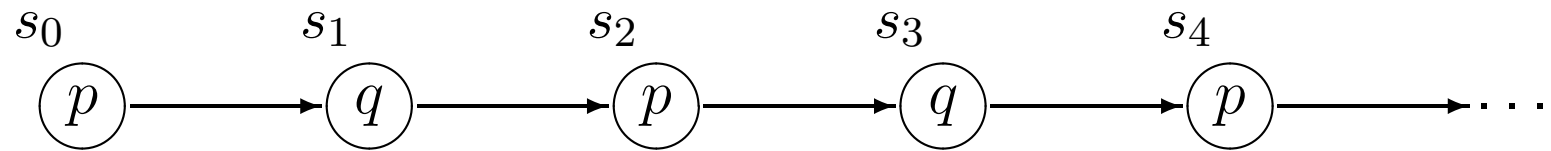
Figure 13.2: Alternate representation



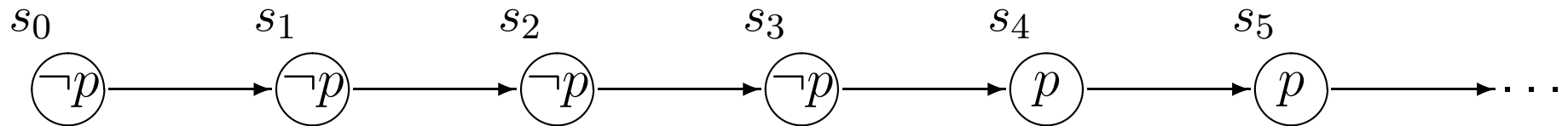
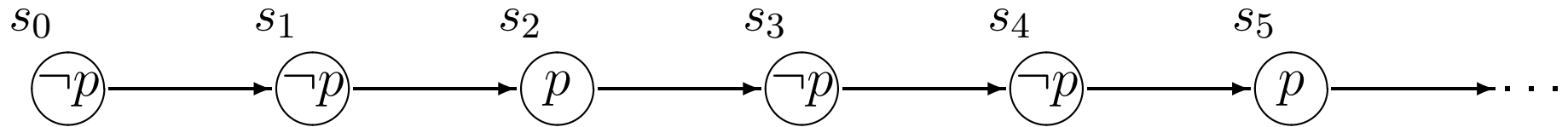
Definition 13.27: Linear temporal logic



Example 13.33



Commutativity



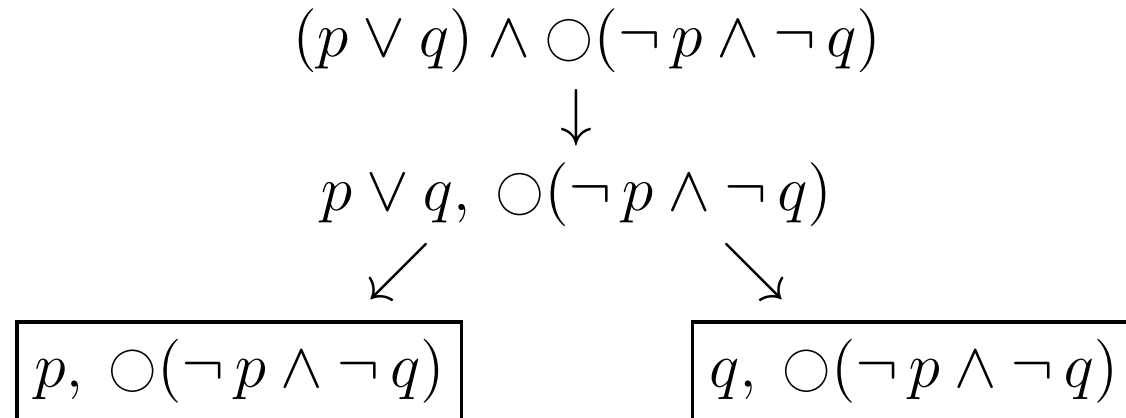
Section 13.51: Tableaux rules for LTL

| α | α_1 | α_2 |
|-------------------|------------|----------------------------|
| $\Box A$ | A | $\bigcirc \Box A$ |
| $\neg \Diamond A$ | $\neg A$ | $\neg \bigcirc \Diamond A$ |

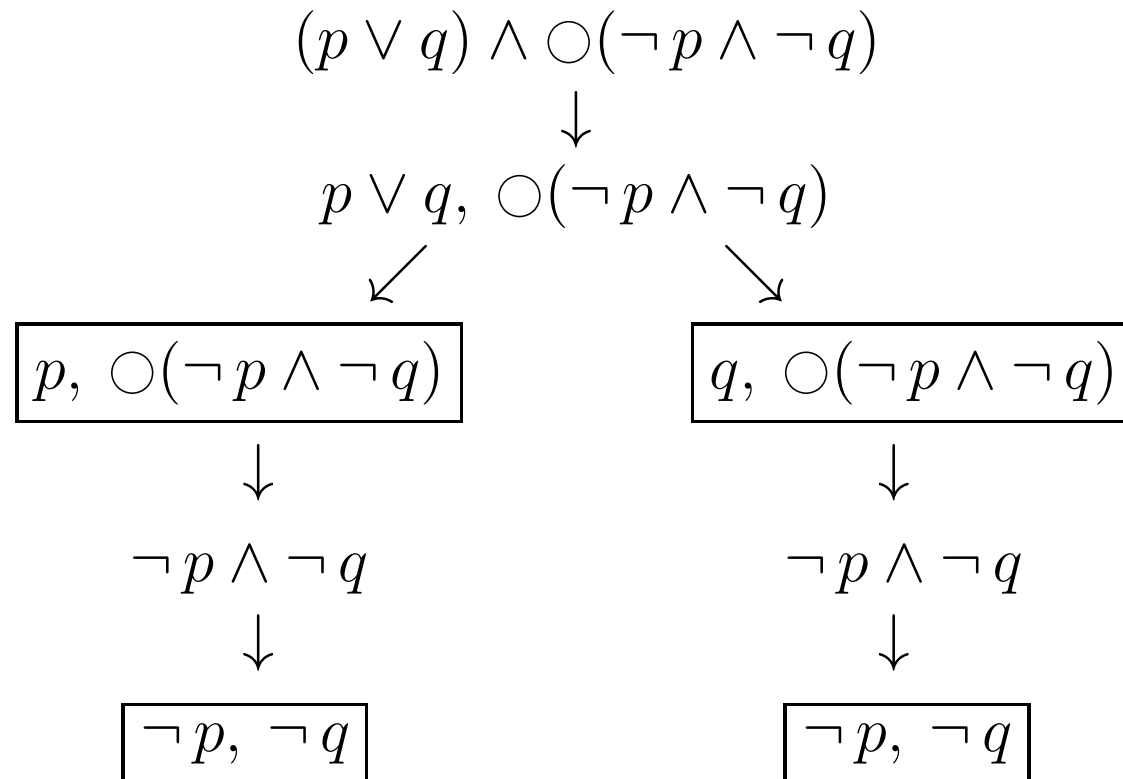
| β | β_1 | β_2 |
|---------------|-----------|------------------------|
| $\Diamond A$ | A | $\bigcirc \Diamond A$ |
| $\neg \Box A$ | $\neg A$ | $\neg \bigcirc \Box A$ |

| X | X_1 |
|-------------------|----------|
| $\bigcirc A$ | A |
| $\neg \bigcirc A$ | $\neg A$ |

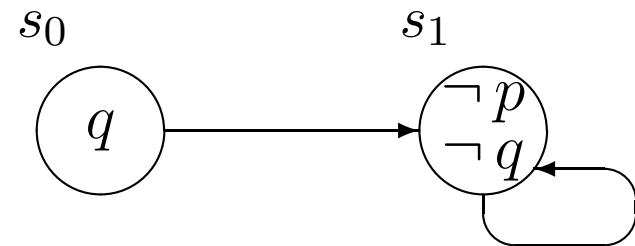
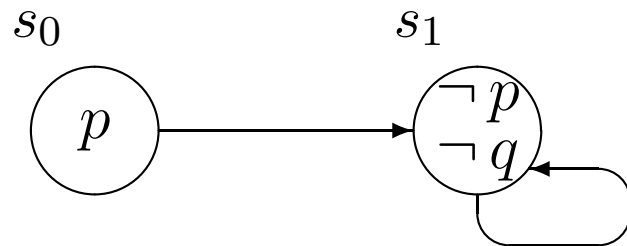
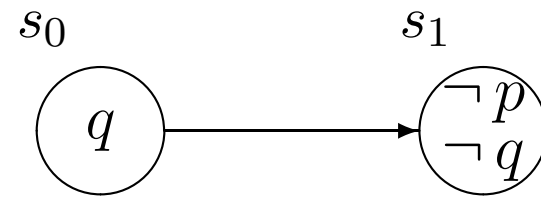
The rule for next formulas (1)



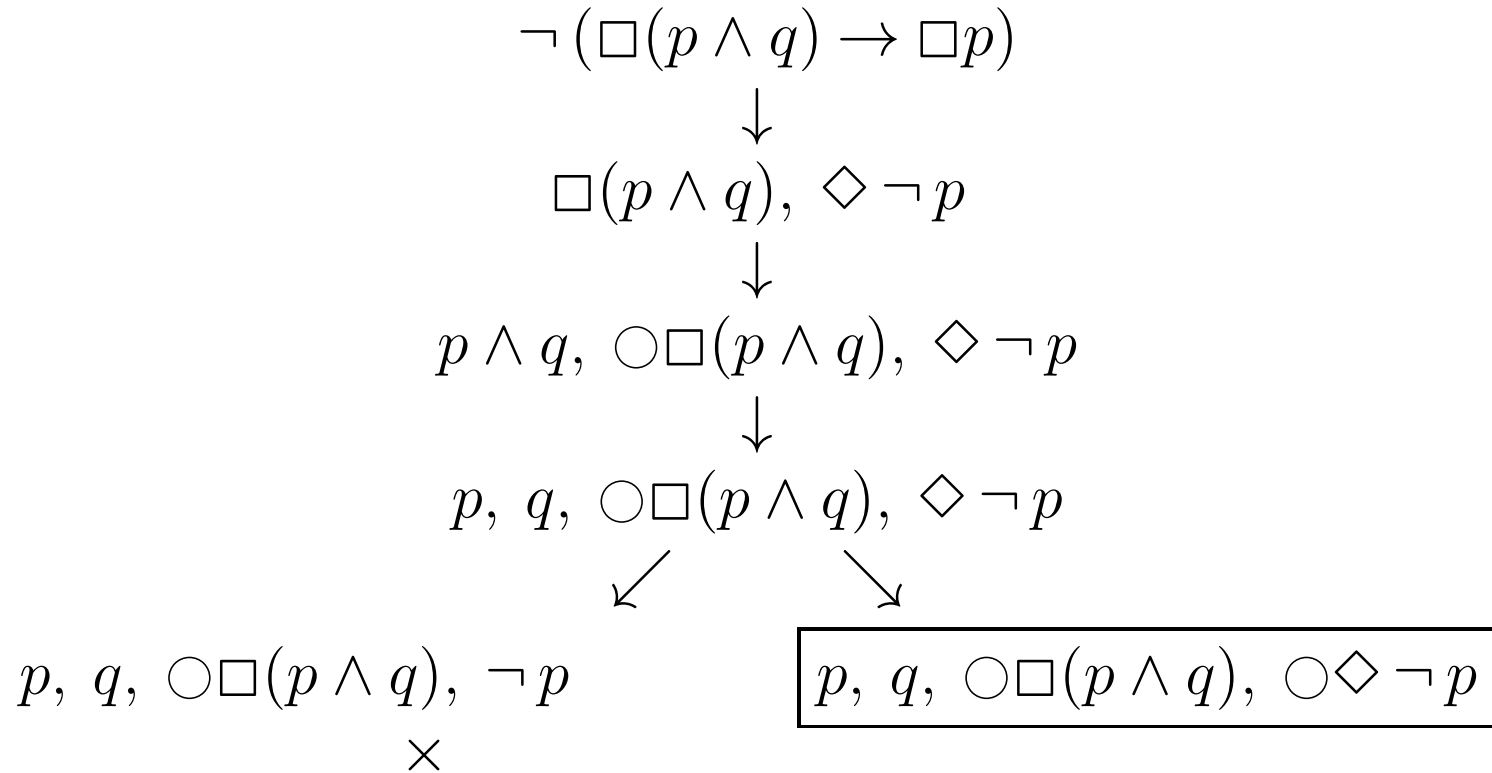
The rule for next formulas (2)



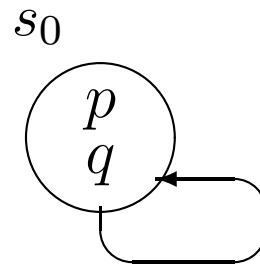
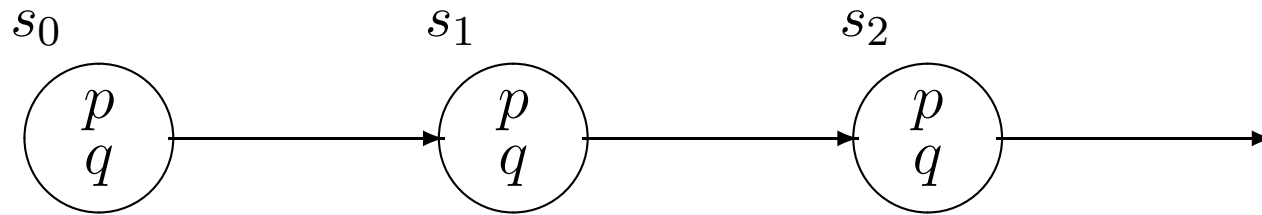
The rule for next formulas (3)



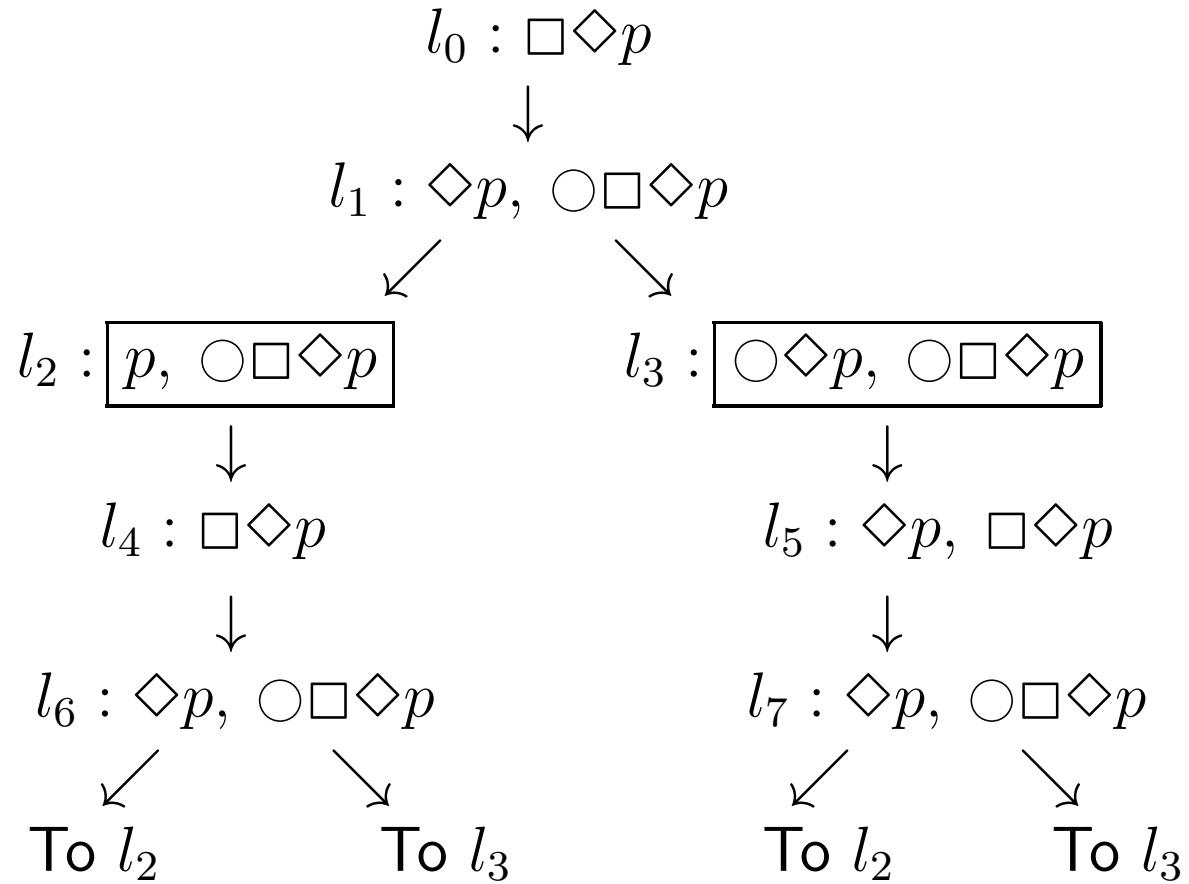
Semantic tableau for $\neg (\Box(p \wedge q) \rightarrow \Box p)$



Interpretations for $\neg (\Box(p \wedge q) \rightarrow \Box p)$



Example 13.38



Example 13.43

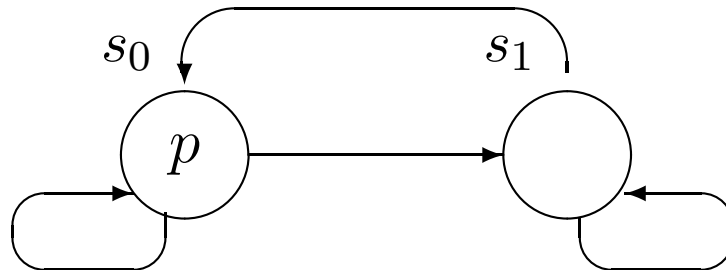
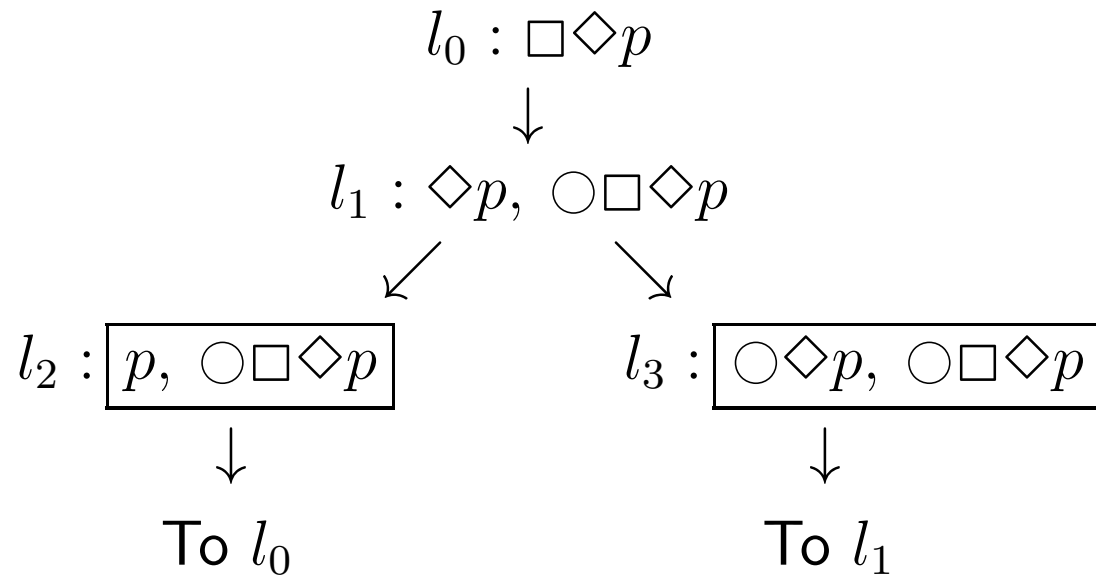
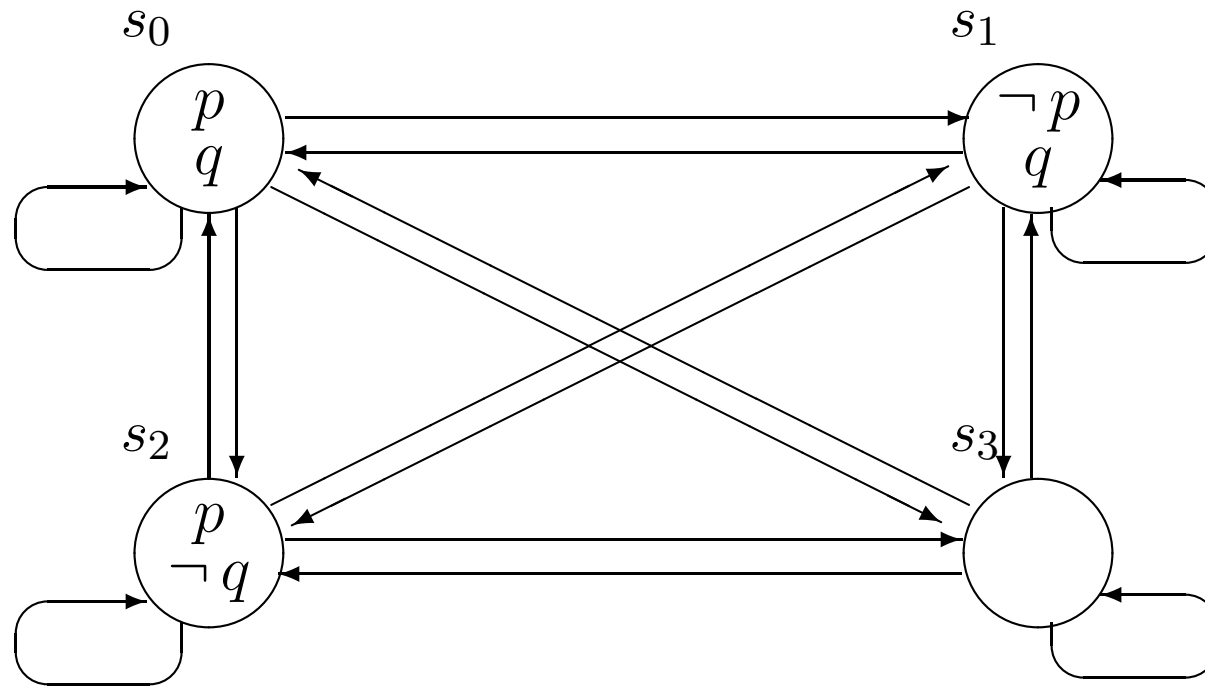


Figure 13.3: $\Box(\Diamond(p \wedge q) \wedge \Diamond(\neg p \wedge q) \wedge \Diamond(p \wedge \neg q))$



Section 13.5.4: A linear, fulfilling Hintikka structure

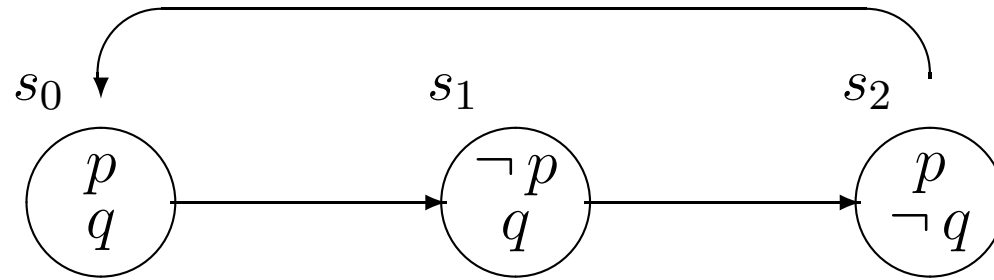


Figure 13.4: Strongly connected components

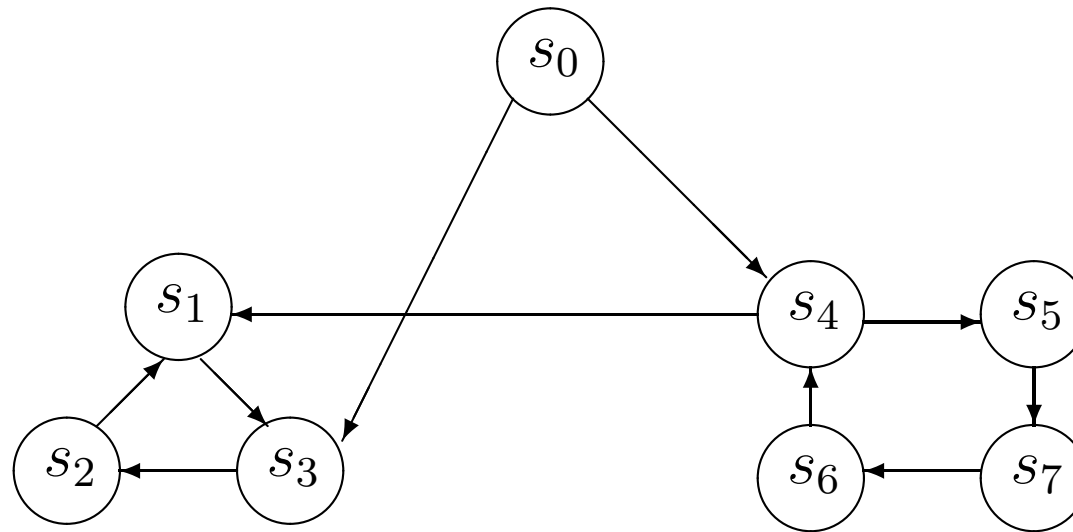


Figure 13.5: Component graph

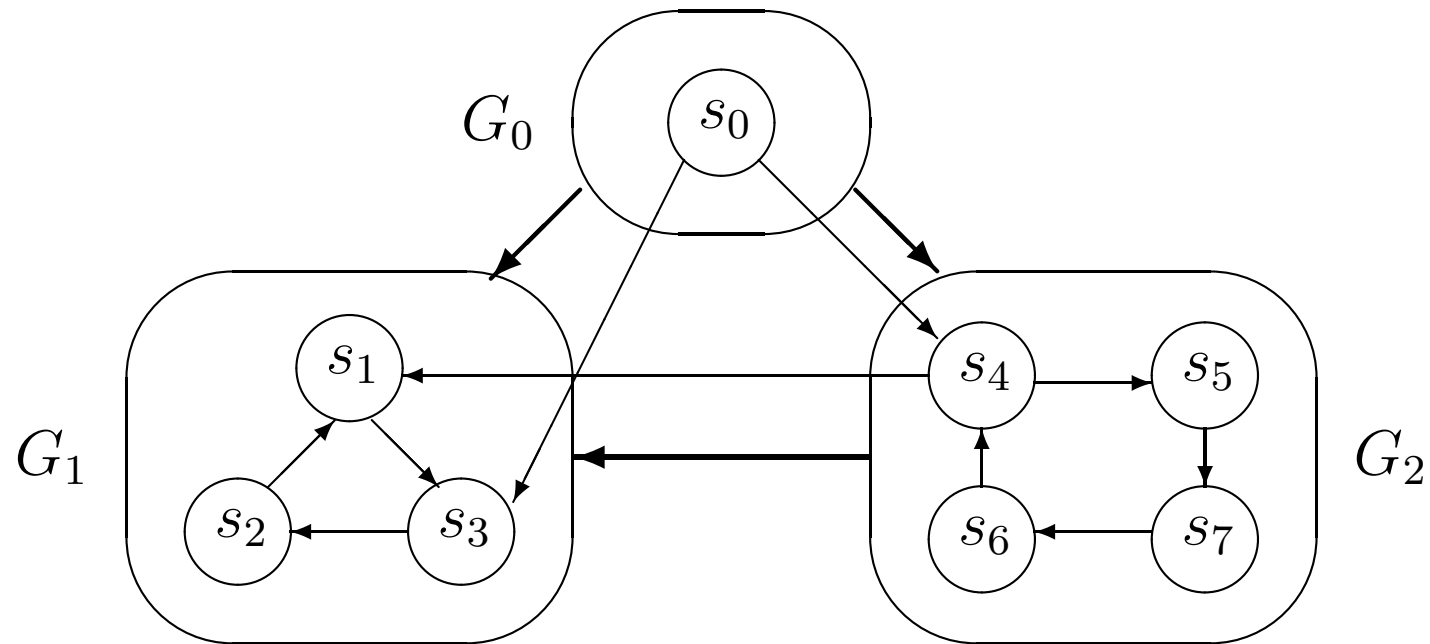
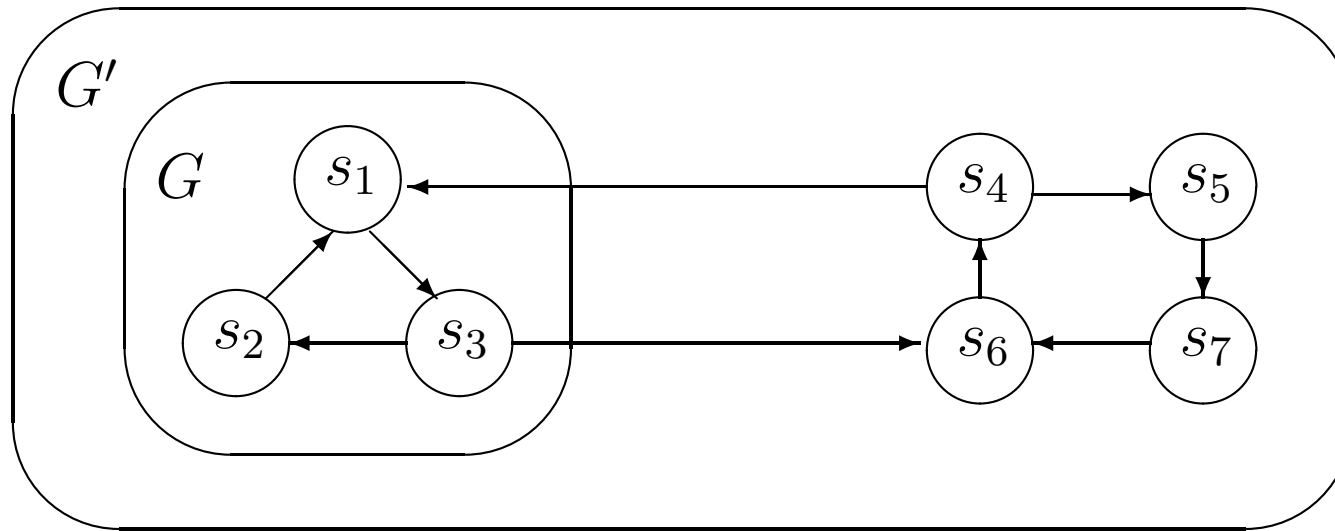
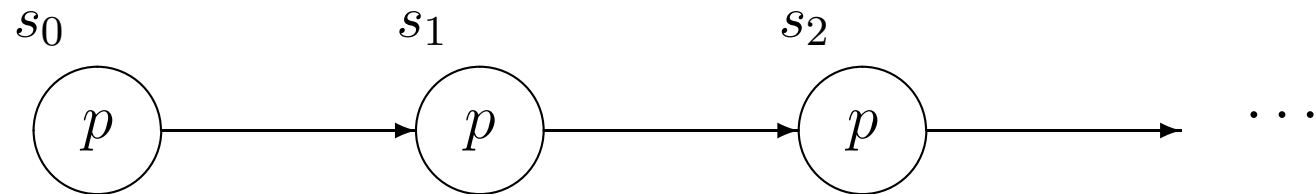


Figure 13.6: An SCC is contained in an MSCC



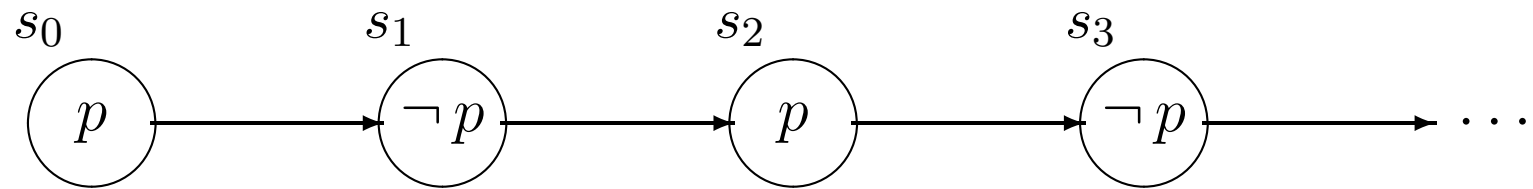
Example 13.68



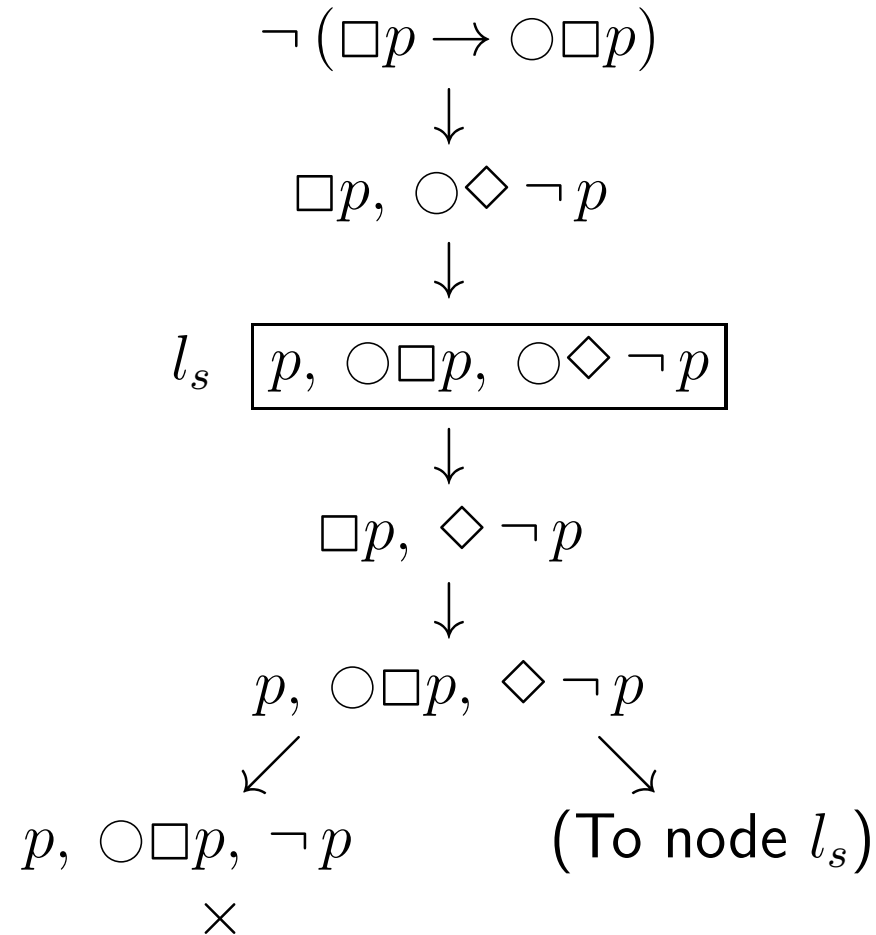
Deductive system \mathcal{L}

| | | |
|-----------------------|--|---|
| Axiom 0 | Prop | Any substitution instance of a valid propositional formula. |
| Axiom 1 | Distribution of \Box | $\vdash \Box(A \rightarrow B) \rightarrow (\Box A \rightarrow \Box B).$ |
| Axiom 2 | Distribution of \bigcirc | $\vdash \bigcirc(A \rightarrow B) \rightarrow (\bigcirc A \rightarrow \bigcirc B).$ |
| Axiom 3 | Expansion of \Box | $\vdash \Box A \rightarrow (A \wedge \bigcirc A \wedge \bigcirc \Box A).$ |
| Axiom 4 | Induction | $\vdash \Box(A \rightarrow \bigcirc A) \rightarrow (A \rightarrow \Box A).$ |
| Axiom 5 | Linearity | $\vdash \bigcirc A \leftrightarrow \neg \bigcirc \neg A.$ |
| Modus ponens | | $\frac{\vdash A \qquad \vdash A \rightarrow B}{\vdash B}.$ |
| Generalization | | $\frac{\vdash A}{\vdash \Box A}.$ |

Example 14.9



Semantic tableau for the negation of $\Box p \rightarrow \bigcirc \Box p$



Section 14.4: Axioms for binary temporal operators

Axiom 6 Expansion of \mathcal{U} $\vdash A\mathcal{U}B \leftrightarrow (B \vee (A \wedge \bigcirc(A\mathcal{U}B)))$.

Axiom 7 Eventuality $\vdash A\mathcal{U}B \rightarrow \Diamond B$.

Definition 15.8: \mathcal{HL} (1)

Domain axioms

Every true formula over the domain(s) of the program variables.

Assignment axiom

$$\vdash \{p(x)\{x \leftarrow t\}\} x := t \{p(x)\}.$$

Composition rule

$$\frac{\vdash \{p\} S1 \{q\} \qquad \vdash \{q\} S2 \{r\}}{\vdash \{p\} S1 ; S2 \{r\}}.$$

Definition 15.8: \mathcal{HL} (2)

Alternative rule

$$\frac{\vdash \{p \wedge B\} S1 \{q\} \quad \vdash \{p \wedge \neg B\} S2 \{q\}}{\vdash \{p\} \text{ if } B \text{ then } S1 \text{ else } S2 \{q\}}.$$

Loop rule

$$\frac{\vdash \{p \wedge B\} S \{p\}}{\vdash \{p\} \text{ while } B \text{ do } S \{p \wedge \neg B\}}.$$

Consequence rule

$$\frac{\vdash p_1 \rightarrow p \quad \vdash \{p\} S \{q\} \quad \vdash q \rightarrow q_1}{\vdash \{p_1\} S \{q_1\}}.$$

Section 15.3: Program to be verified

```
{true}
x := 0;
{x = 0}
y := b;
{x = 0 ∧ y = b}
while y <> 0 do
    {x = (b - y) · a}
    begin x := x + a; y := y - 1 end;
{x = a · b}
```

Section 15.4.1: Solution 1 (outline)

```
{0 ≤ a}  
x = E1(x,a);  
while (B(x,a))  
    {0 ≤ x2 ≤ a}  
    x = E2(x,a);  
{0 ≤ x2 ≤ a < (x + 1)2}.
```

Section 15.4.1: Solution 1 (final)

$\{0 \leq a\}$

$x = 0;$

while $((x+1)*(x+1) \leq a)$

$\{0 \leq x^2 \leq a\}$

$x = x + 1;$

$\{0 \leq x^2 \leq a < (x+1)^2\}.$

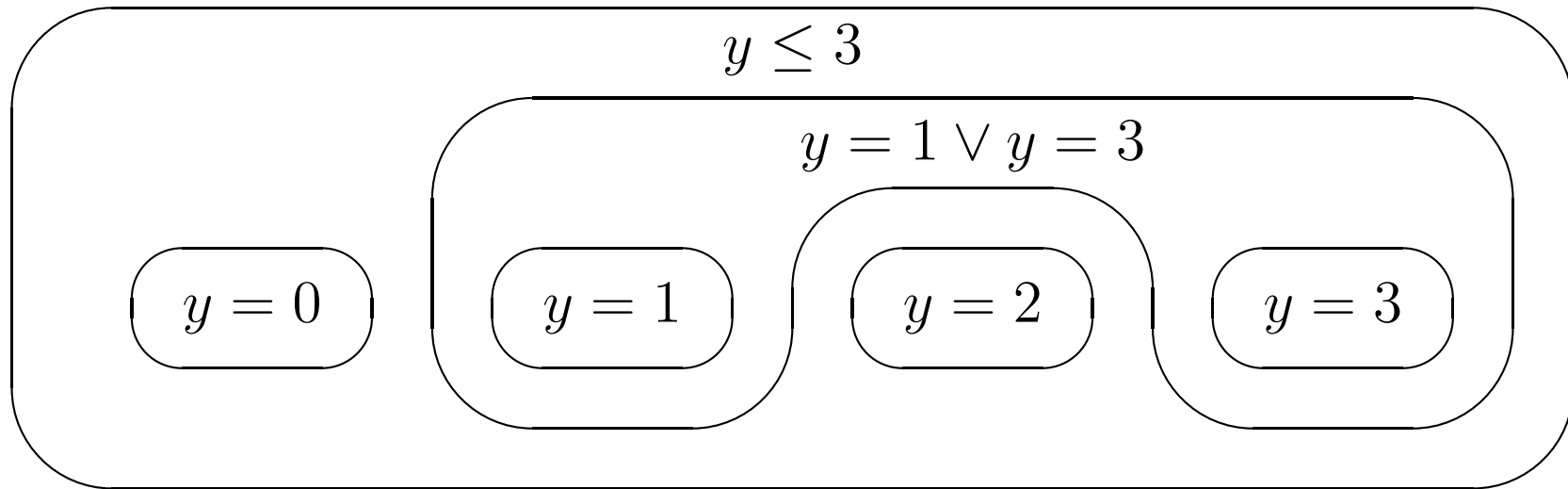
Section 15.4.1: Solution 2 (outline)

```
{0 ≤ a}  
x = 0;  
y = a+1;  
while (y != x+1)  
    {(0 ≤ x2 ≤ a < y2) ∧ (x < y ≤ a + 1)}  
    E(x,y,a);  
{0 ≤ x2 ≤ a < (x + 1)2}.
```

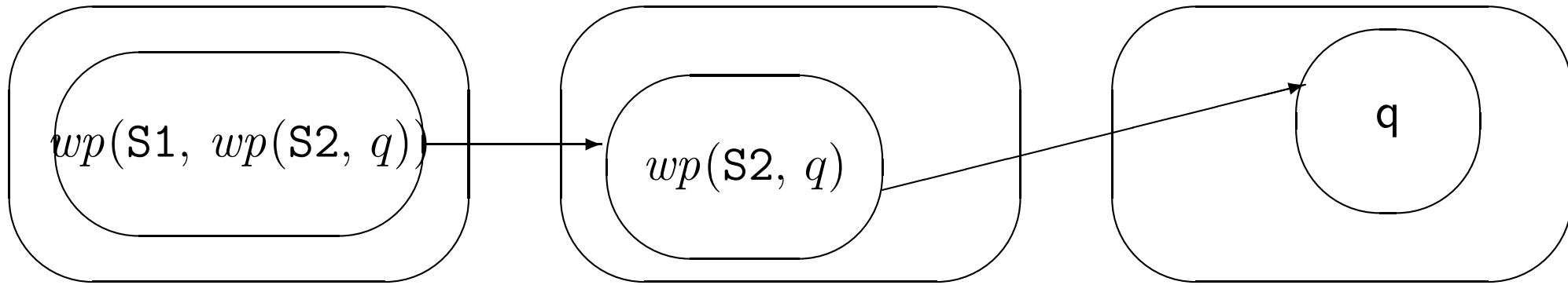
Section 15.4.1: Solution 2 (final)

```
{0 ≤ a}
x = 0;
y = a+1;
while (y != x+1)
    {0 ≤ x2 ≤ a < y2 ∧ x < y ≤ a + 1}
    {
        z = (x+y) / 2;
        if (z*z ≤ a)
            x = z;
        else
            y = z;
    }
{0 ≤ x2 ≤ a < (x + 1)2}.
```

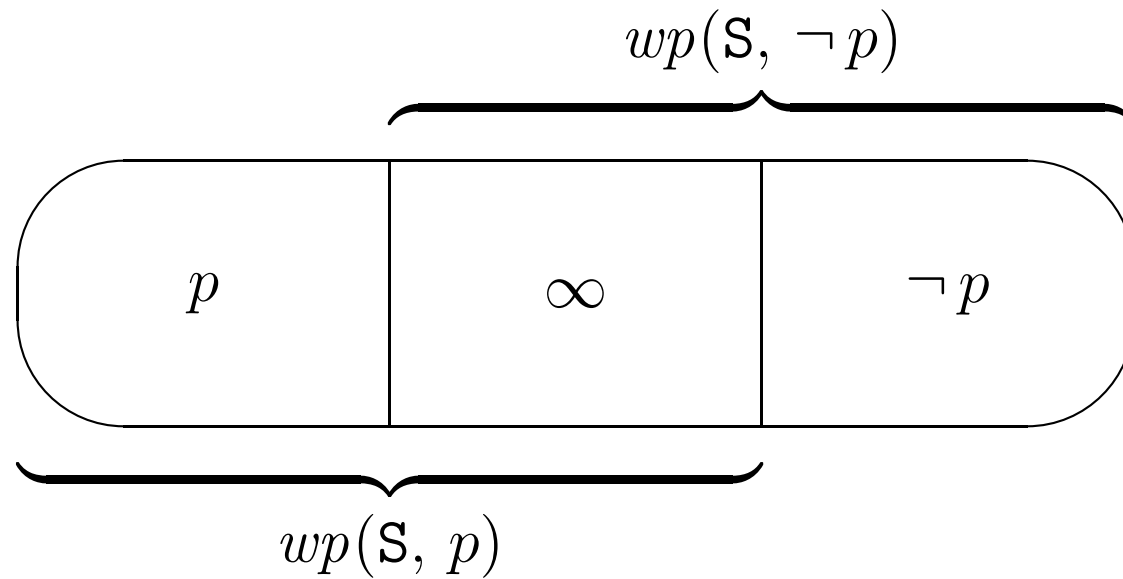
Example 15.15: Weaker conditions



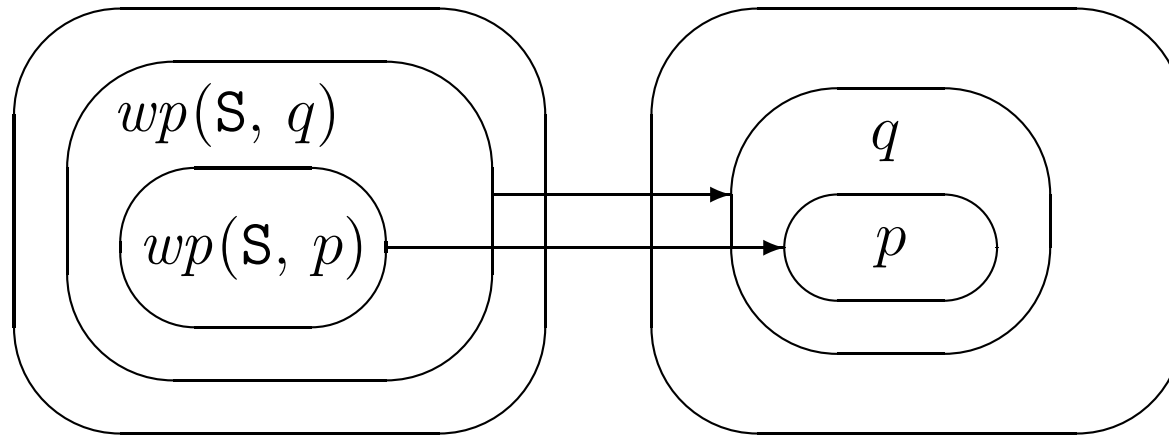
Definition 15.21: Sequential composition



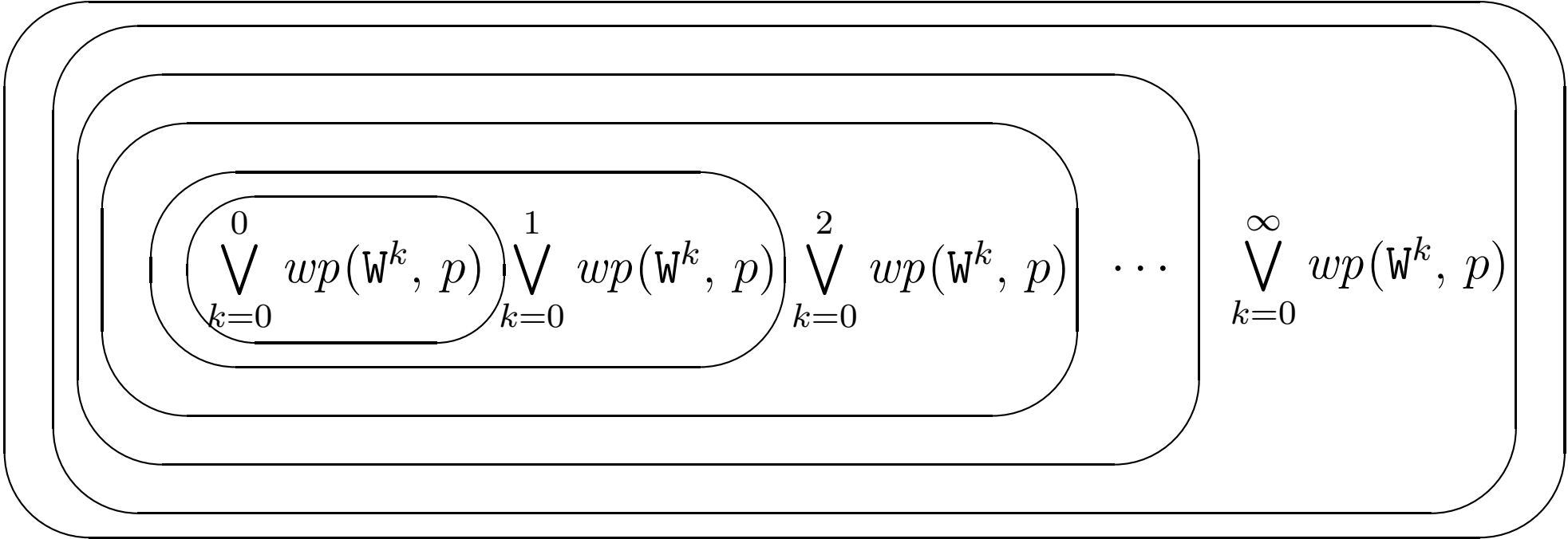
Corollary 9.26: Excluded miracle



Theorem 9.28: Monotonicity



Lemma 15.37


$$\bigvee_{k=0}^0 wp(W^k, p) \bigvee_{k=0}^1 wp(W^k, p) \bigvee_{k=0}^2 wp(W^k, p) \dots \bigvee_{k=0}^{\infty} wp(W^k, p)$$

Example 16.2

| int n = 0 | |
|--------------|--------------|
| Process p | Process q |
| 1: n = n + 1 | 1: n = n + 1 |
| 2: n = n + 1 | 2: n = n + 1 |
| end: | end: |

Atomic operations

| int n = 0 | |
|----------------------|----------------------|
| Process p | Process q |
| 1: n = n + 1 end: | 1: n = n + 1 end: |

| int n = 0 | |
|--|--|
| Process p | Process q |
| int temp = 0 1: temp = n 2: temp = temp + 1 3: n = temp end: | int temp = 0 1: temp = n 2: temp = temp + 1 3: n = temp end: |

Peterson's algorithm

| <pre>boolean wantp = false, wantq = false int turn = 1</pre> | |
|--|--|
| Process p | Process q |
| <pre>while (true) { non-critical-section wantp = true turn = 1 wait until (!wantq or turn == 2) critical-section wantp = false }</pre> | <pre>while (true) { non-critical-section wantq = true turn = 2 wait until (!wantp or turn == 1) critical-section wantq = false }</pre> |

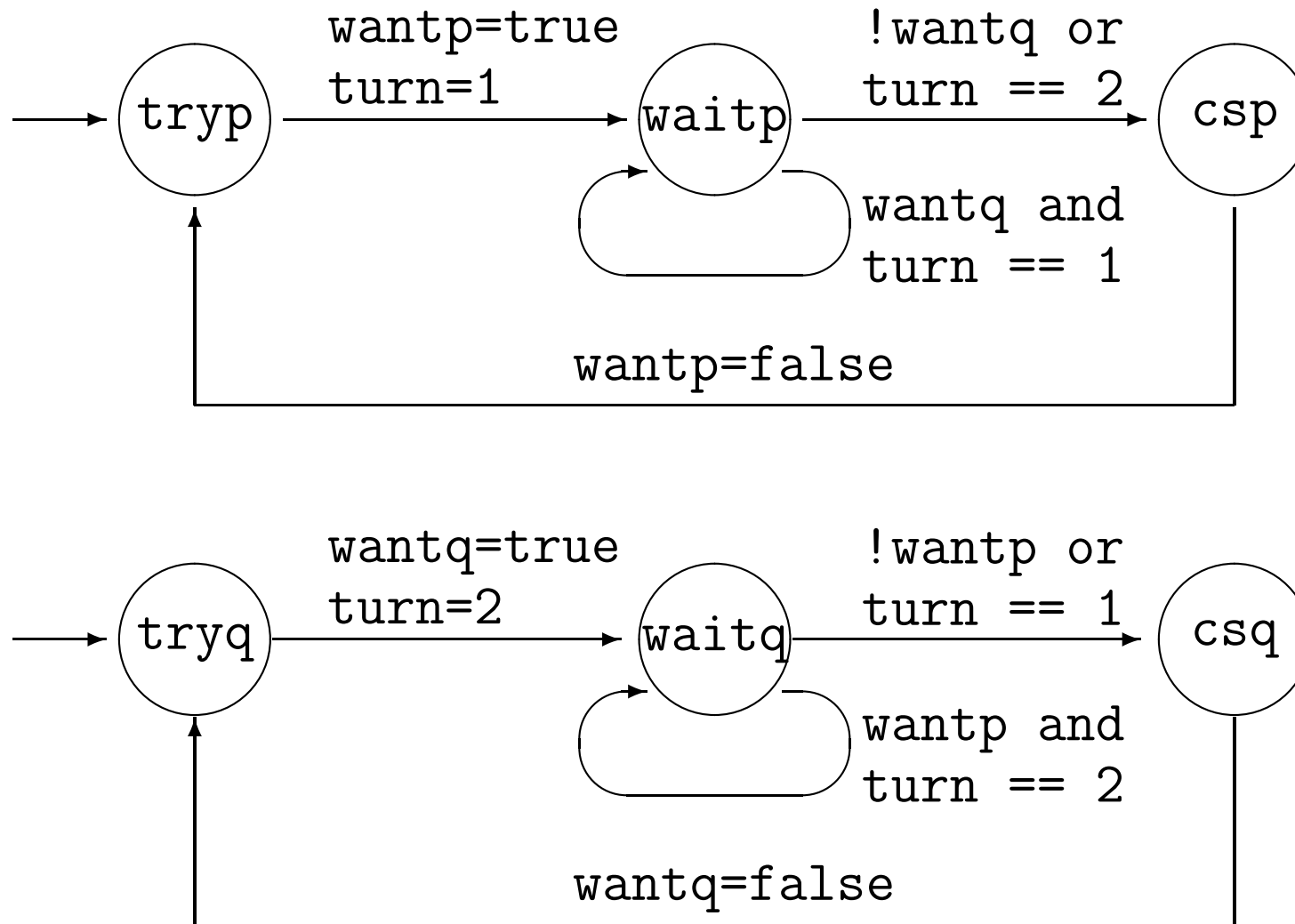
Abbreviated algorithm

| <pre>boolean wantp = false, wantq = false int turn = 1</pre> | |
|--|--|
| Process p | Process q |
| <pre>while (true) { tryp: wantp=true; turn=1 waitp: wait until (!wantq or turn == 2) csp: wantp = false }</pre> | <pre>while (true) { tryq: wantq=true; turn=2 waitq: wait until (!wantp or turn == 1) csq: wantq = false }</pre> |

Progress axioms

| Statement | Progress axioms |
|---|--|
| li: $v := \text{expression}$ li+1: | $\vdash l_i \rightarrow \Diamond l_{i+1}$ |
| li: if B then lt: S1 else lf: S2 | $\vdash l_i \rightarrow \Diamond(l_t \vee l_f)$ $\vdash (l_i \wedge \Box B) \rightarrow \Diamond l_t$ $\vdash (l_i \wedge \Box \neg B) \rightarrow \Diamond l_f$ |
| li: while B do lt: S1; lf: | $\vdash l_i \rightarrow \Diamond(l_t \vee l_f)$ $\vdash (l_i \wedge \Box B) \rightarrow \Diamond l_t$ $\vdash (l_i \wedge \Box \neg B) \rightarrow \Diamond l_f$ |

Figure 16.3: Finite automata for Peterson's algorithm



Product automaton for Peterson's algorithm

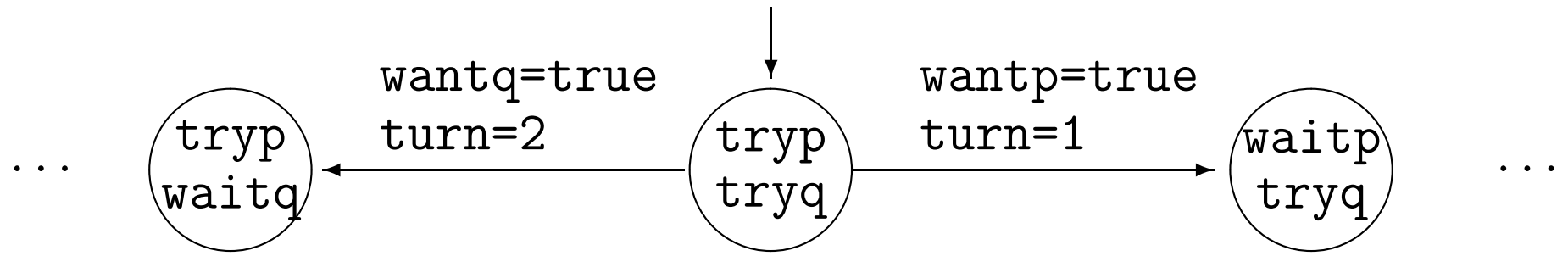
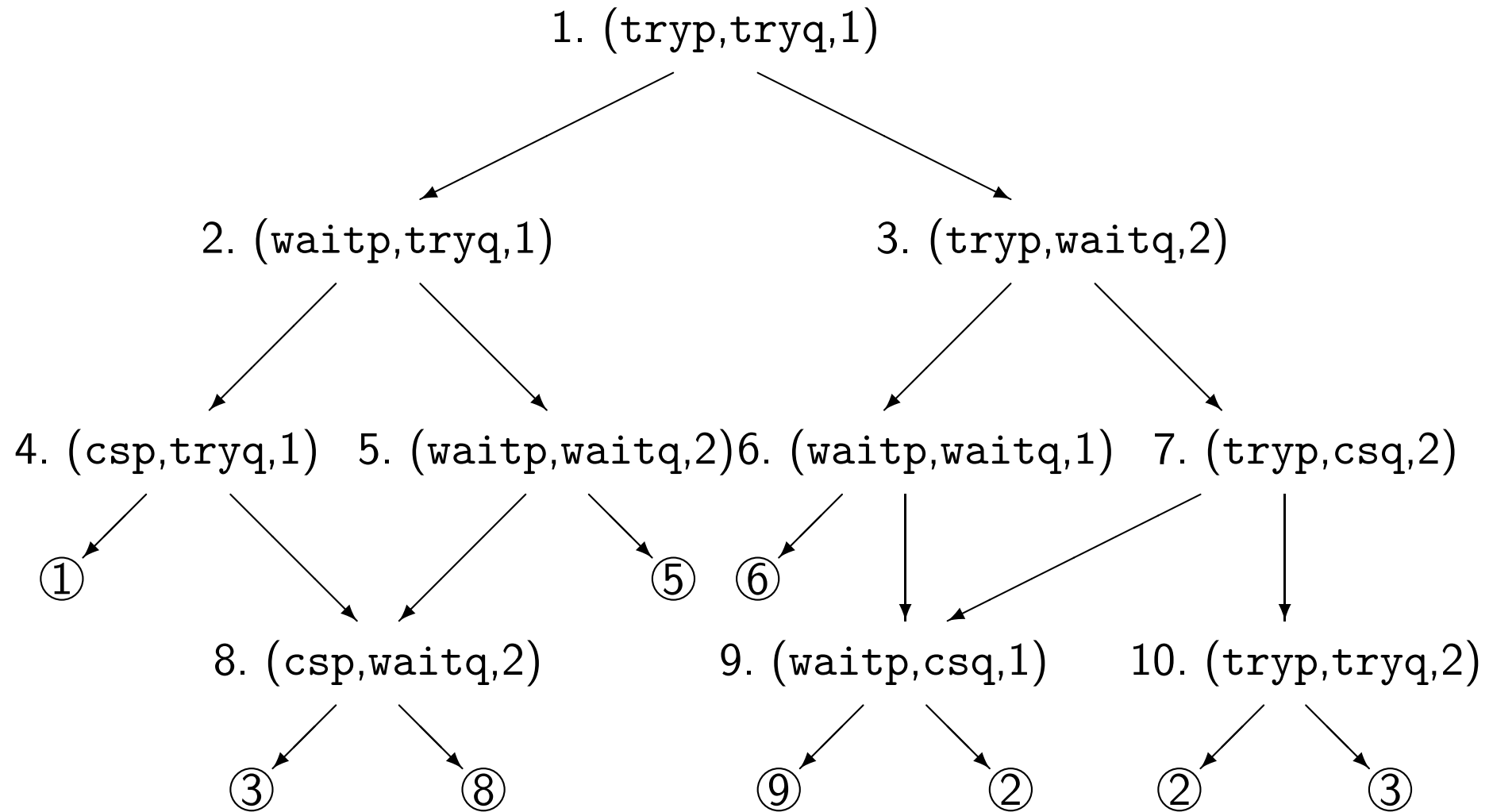


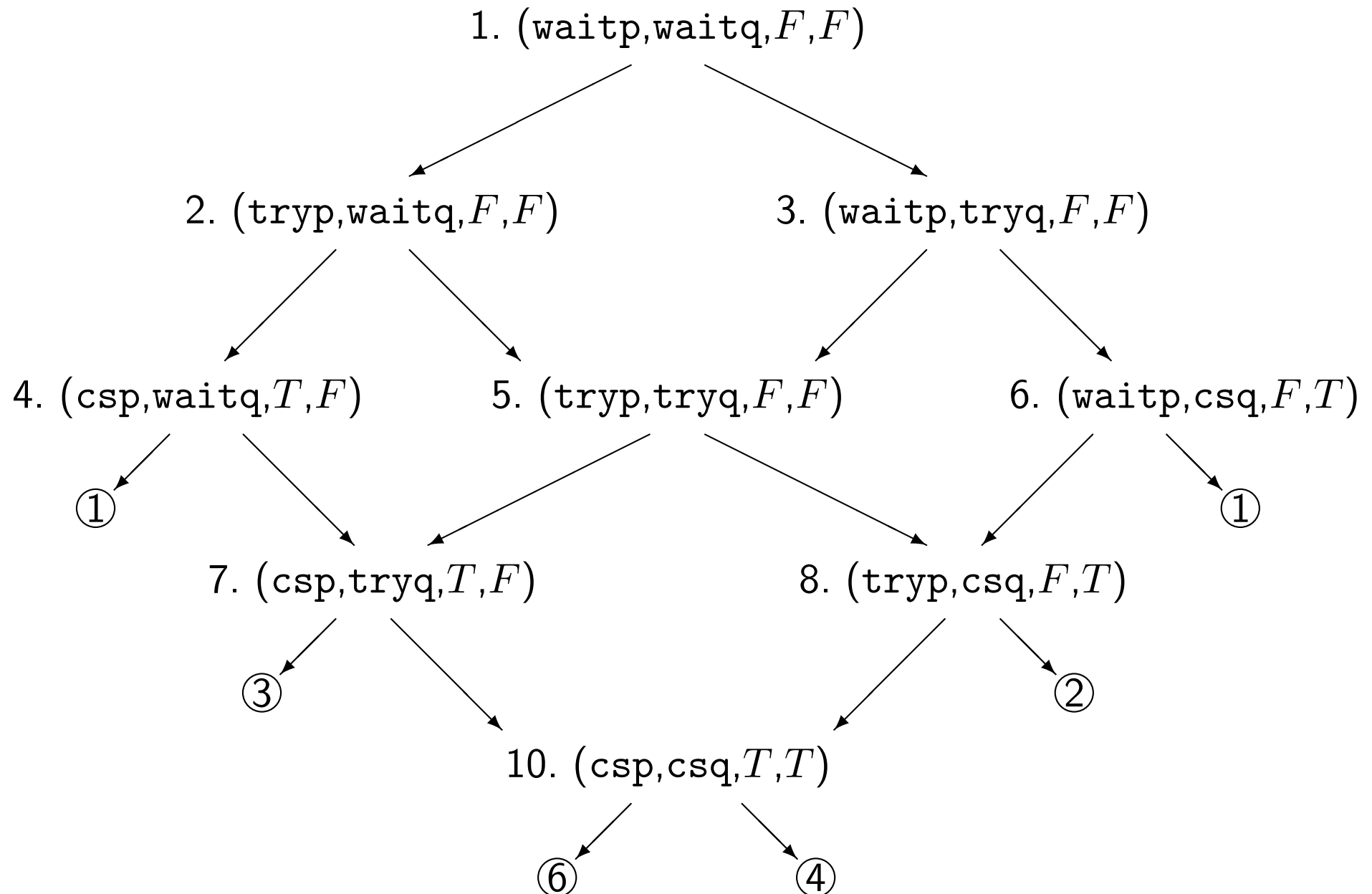
Figure 16.2: State space for Peterson's algorithm



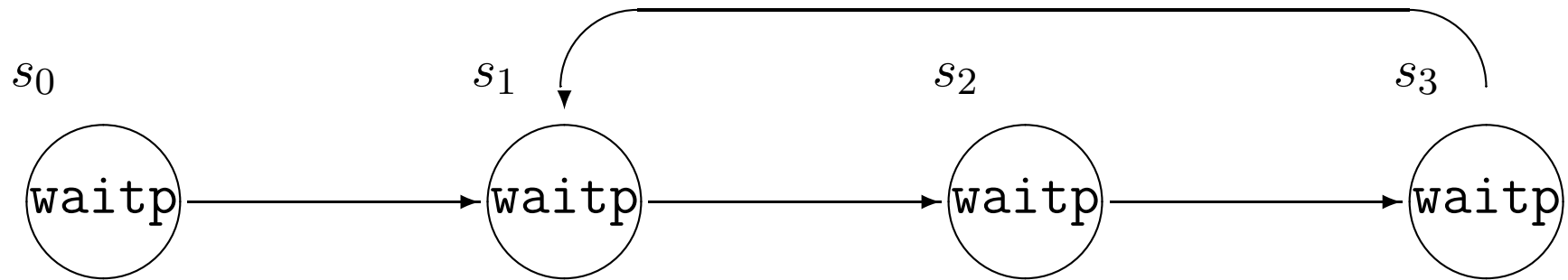
Section 16.5.2: Dijkstra's second attempt

| | |
|---|---|
| boolean wantp = false, wantq = false | |
| Process p | Process q |
| while (true) { waitp: wait until !wantq tryp: wantp = true csp: wantp = false } | while (true) { waitq: wait until !wantp tryq: wantq = true csq: wantq = false } |

Figure 16.3: State space for the second attempt



Section 16.6



Section 16.6.1

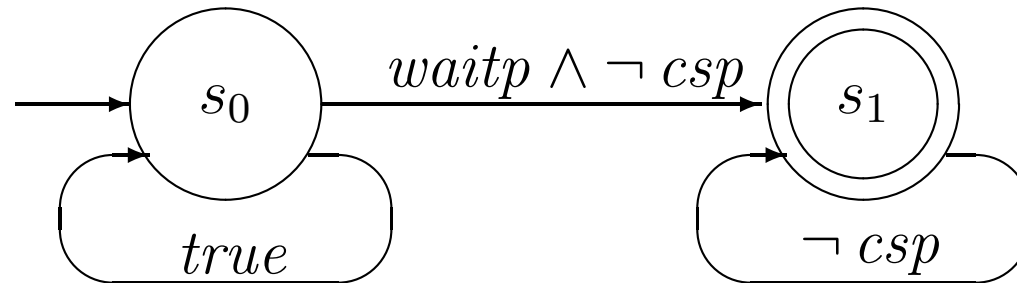
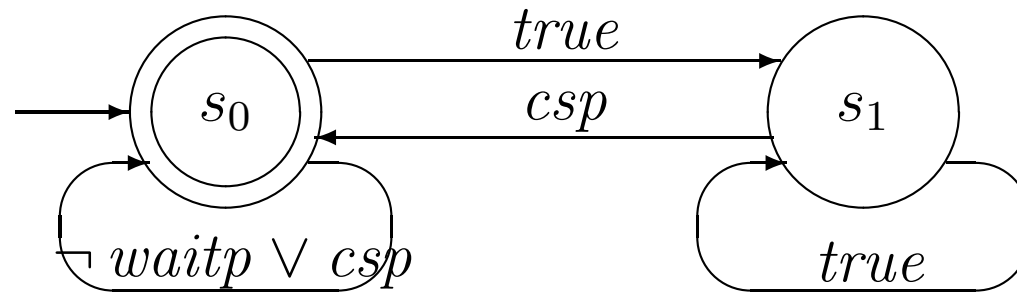


Figure 16.4: Model checking liveness

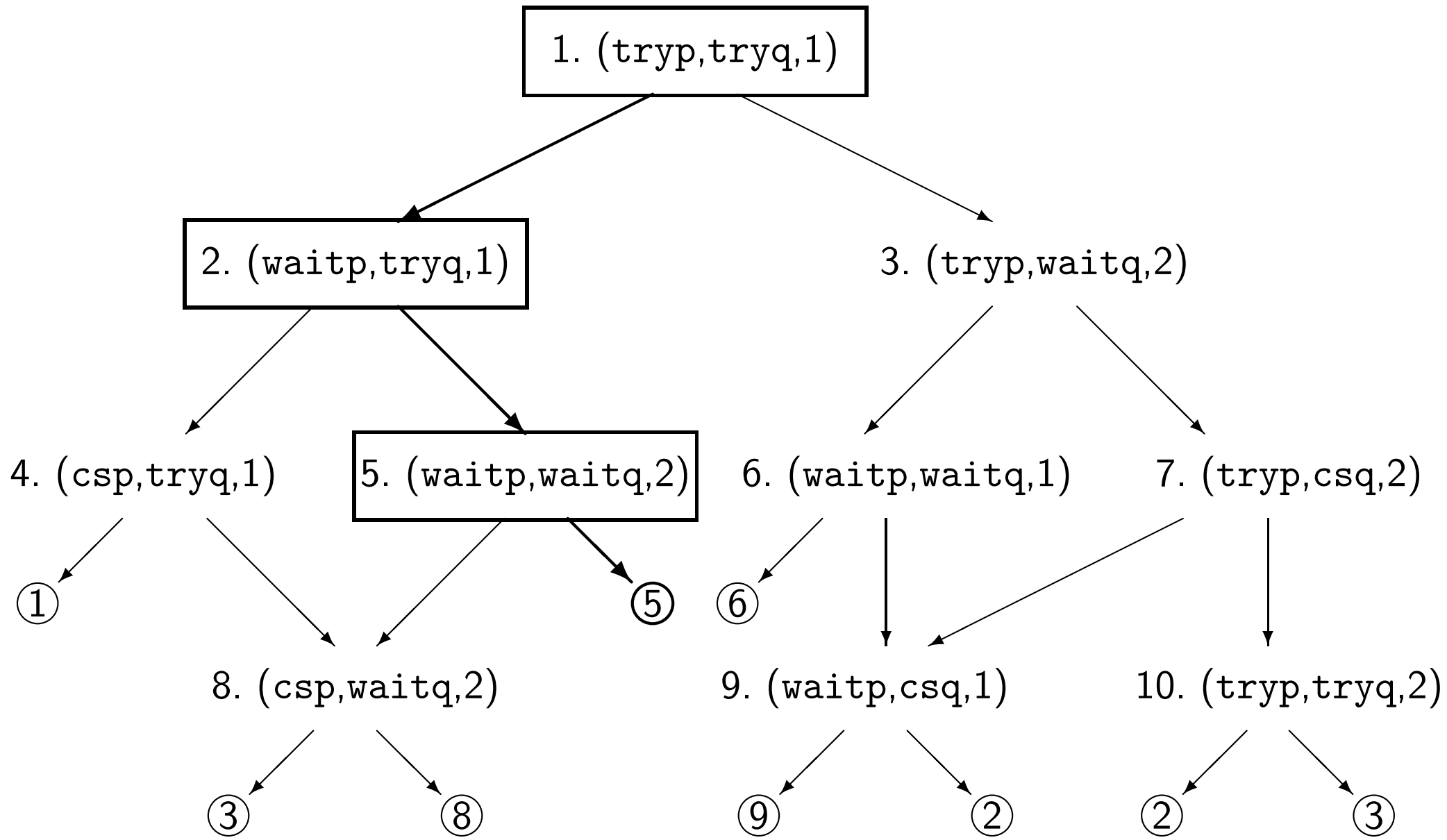


Figure 16.5: The state space as a tree

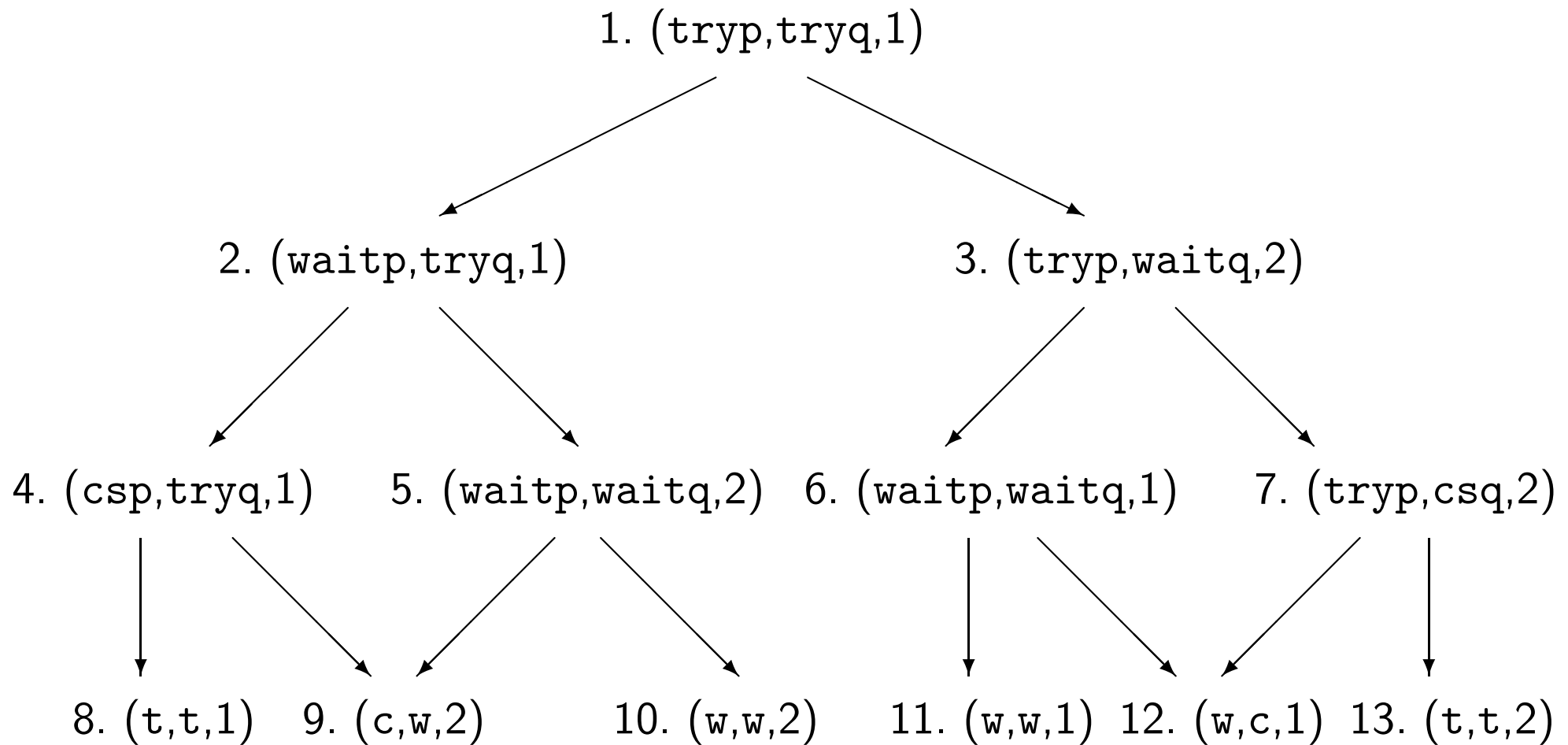
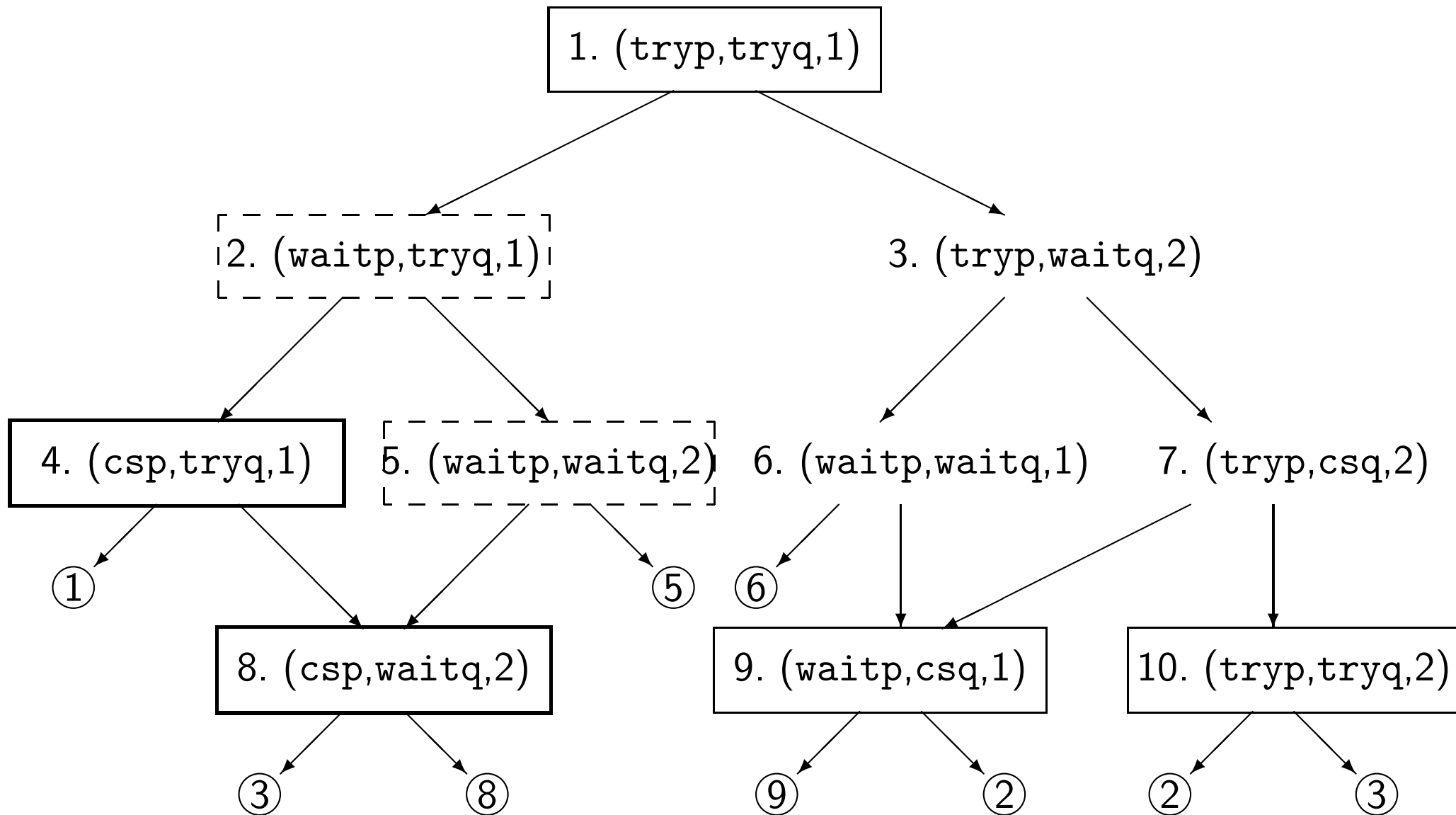
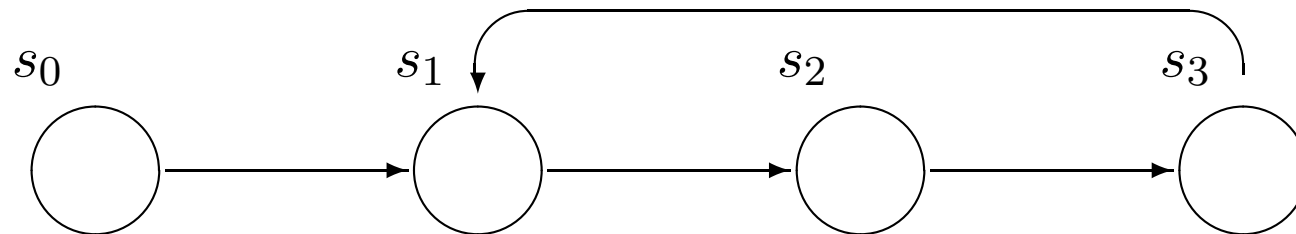


Figure 16.6: CTL model checking



Section 16.8: Symbolic model checking

| | | | |
|-------|-----------------------|-------|-----------------------|
| tryp | $p_0 \wedge p_1$ | tryq | $q_0 \wedge q_1$ |
| waitp | $\neg p_0 \wedge p_1$ | waitq | $\neg q_0 \wedge q_1$ |
| csp | $p_0 \wedge \neg p_1$ | csq | $q_0 \wedge \neg q_1$ |



Venn diagrams

