# Logik för dataloger, DD1350
# Kurskompendium

Andreas Lundblad, Dilian Gurov, Karl Palmskog

Senast uppdaterat: 2013-05-30

# Innehåll

# Kapitel 1

# Lösningsförslag till utvalda övningar

## Exercises 1.1 (page 78)

1. Use $\neg$, $\rightarrow$, $\wedge$ and $\vee$ to express the following declarative sentences in propositional logic; in each case state what your respective propositional atoms $p$, $q$, etc. mean:

   (b) Robert was jealous of Yvonne, or he was not in a good mood.

$p \vee \neg q$

$p$: Robert was jealous of Yvonne.
$q$: Robert was in a good mood.

   (c) If the barometer falls, then either it will rain or it will snow.

$p \rightarrow q \vee r$

$p$: The barometer falls.
$q$: It will rain.
$r$: It will snow.

Alternative solution for exclusive or: $p \rightarrow (q \wedge \neg r) \vee (\neg q \wedge r)$

   (e) Cancer will not be cured unless its cause is determined and a new drug for cancer is found.

$\neg q \vee \neg r \rightarrow \neg p$

$p$: Cancer will be cured.
$q$: Its cause is determined.
$r$: A new drug for cancer is found.

   (f) If interest rates go up, share prices go down.

$p \rightarrow q$

$p$: Interests rates go up.
$q$: share prices go down.

(g) If Smith has installed central heating, then he has sold his car or he has not paid his mortgage.

$p \to (q \lor \neg r)$

$p$: Smith has installed central heating.
$q$: Smith has sold his car.
$r$: Smith has paid his mortgage.

## Exercises 1.2 (page 78)

1. Prove the validity of the following sequents:

(a) $p \to q \to r \vdash q \to p \to r$

| | | |
|---|---|---|
| 1 | $p \to q \to r$ | premise |
| 2 | $q$ | assumption |
| 3 | $p$ | assumption |
| 4 | $q \to r$ | $\to$e 3,1 |
| 5 | $r$ | $\to$e 2,4 |
| 6 | $p \to r$ | $\to$i 3-5 |
| 7 | $q \to p \to r$ | $\to$i 2-6 |

(b) $\vdash (p \to q) \to (p \to r) \to (q \to r \to s) \to p \to s$

| | | |
|---|---|---|
| 1 | $p \to q$ | assumption |
| 2 | $p \to r$ | assumption |
| 3 | $q \to r \to s$ | assumption |
| 4 | $p$ | assumption |
| 5 | $q$ | $\to$e 4,1 |
| 6 | $r$ | $\to$e 4,2 |
| 7 | $r \to s$ | $\to$e 5,3 |
| 8 | $s$ | $\to$e 6,7 |
| 9 | $p \to s$ | $\to$i 4-8 |
| 10 | $(q \to r \to s) \to (p \to s)$ | $\to$i 3-9 |
| 11 | $(p \to r) \to (q \to r \to s) \to p \to s$ | $\to$i 2-10 |
| 12 | $(p \to q) \to (p \to r) \to (q \to r \to s) \to p \to s$ | $\to$i 1-11 |

(d) $(p \land q) \land r, s \land t \vdash q \land s$

| | | |
|---|---|---|
| 1 | $(p \land q) \land r$ | premise |
| 2 | $s \land t$ | premise |
| 3 | $p \land q$ | $\land e_1$ 1 |
| 4 | $q$ | $\land e_2$ 3 |
| 5 | $s$ | $\land e_1$ 2 |
| 6 | $q \land s$ | $\land$i 4,5 |

(d) $p \to (p \to q), p \vdash q$

| | | |
|---|---|---|
| 1 | $p \to (p \to q)$ | premise |
| 2 | $p$ | premise |
| 3 | $p \to q$ | $\to$e 2,1 |
| 4 | $q$ | $\to$e 2,3 |

(g) $p \vdash q \to (p \wedge q)$

| | | |
|---|---|---|
| 1 | $p$ | premise |
| 2 | $q$ | assumption |
| 3 | $p \wedge q$ | $\wedge$i 1,2 |
| 4 | $q \to (p \wedge q)$ | $\to$i 2-3 |

(k) $p \to (q \to r), p \to q \vdash p \to r$

| | | |
|---|---|---|
| 1 | $p \to (q \to r)$ | premise |
| 2 | $p \to q$ | premise |
| 3 | $p$ | assumption |
| 4 | $q$ | $\to$e 3,2 |
| 5 | $q \to r$ | $\to$e 3,1 |
| 6 | $r$ | $\to$e 4,5 |
| 7 | $p \to r$ | $\to$i 3-6 |

(m) $p \vee q \vdash r \to (p \vee q) \wedge r$

| | | |
|---|---|---|
| 1 | $p \vee q$ | premise |
| 2 | $r$ | assumption |
| 3 | $(p \vee q) \wedge r$ | $\wedge$i 1, 2 |
| 4 | $r \to (p \vee q) \wedge r$ | $\to$i 2-3 |

(p) $p \to q \vdash ((p \land q) \to p) \land (p \to (p \land q))$

| | | |
|---|---|---|
| 1 | $p \to q$ | premise |
| 2 | $p \land q$ | assumption |
| 3 | $p$ | $\land e_1$ 2 |
| 4 | $(p \land q) \to p$ | $\to$i 2-3 |
| 5 | $p$ | assumption |
| 6 | $q$ | $\to$e 5,1 |
| 7 | $p \land q$ | $\land$i 5,6 |
| 8 | $p \to (p \land q)$ | $\to$i 5-7 |
| 9 | $((p \land q) \to p) \land (p \to (p \land q))$ | $\land$i 4,8 |

(q) $\vdash q \to (p \to (p \to (q \to p)))$

| | | |
|---|---|---|
| 1 | $q$ | assumption |
| 2 | $p$ | assumption |
| 3 | $p$ | assumption |
| 4 | $q$ | assumption |
| 5 | $p$ | copy 2 |
| 6 | $q \to p$ | $\to$i 4-5 |
| 7 | $p \to (q \to p)$ | $\to$i 3-6 |
| 8 | $p \to (p \to (q \to p))$ | $\to$i 2-7 |
| 9 | $q \to (p \to (p \to (q \to p)))$ | $\to$i 1-8 |

(s) $(p \to q) \land (p \to r) \vdash p \to q \land r$

| | | |
|---|---|---|
| 1 | $(p \to q) \land (p \to r)$ | premise |
| 2 | $p \to q$ | $\land e_1$ 1 |
| 3 | $p \to r$ | $\land e_2$ 1 |
| 4 | $p$ | assumption |
| 5 | $q$ | $\to$e 4,2 |
| 6 | $r$ | $\to$e 4,3 |
| 7 | $q \land r$ | $\land$i 5,6 |
| 8 | $p \to q \land r$ | $\to$i 4-7 |

(t) $\vdash (p \to q) \to ((r \to s) \to (p \wedge r \to q \wedge s))$

| | | |
|---|---|---|
| 1 | $p \to q$ | assumption |
| 2 | $r \to s$ | assumption |
| 3 | $p \wedge r$ | assumption |
| 4 | $p$ | $\wedge e_1$ 3 |
| 5 | $q$ | $\to$e 4,1 |
| 6 | $r$ | $\wedge e_2$ 3 |
| 7 | $s$ | $\to$e 6,2 |
| 8 | $q \wedge s$ | $\wedge$i 5,7 |
| 9 | $p \wedge r \to q \wedge s$ | $\to$i 3-8 |
| 10 | $(r \to s) \to (p \wedge r \to q \wedge s)$ | $\to$i 2-9 |
| 11 | $(p \to q) \to ((r \to s) \to (p \wedge r \to q \wedge s))$ | $\to$i 1-10 |

(v) $p \vee (p \wedge q) \vdash p$

| | | |
|---|---|---|
| 1 | $p \vee (p \wedge q)$ | premise |
| 2 | $p$ | assumption |
| 3 | $p$ | copy 2 |
| 4 | $p \wedge q$ | assumption |
| 5 | $p$ | $\wedge e_1$ 4 |
| 6 | $p$ | $\vee$e 1,2-3,4-5 |

(w) $r, p \to (r \to q) \vdash p \to (q \wedge r)$

| | | |
|---|---|---|
| 1 | $r$ | premise |
| 2 | $p \to (r \to q)$ | premise |
| 3 | $p$ | assumption |
| 4 | $r \to q$ | $\to$e 2,3 |
| 5 | $q$ | $\to$e 4,1 |
| 6 | $q \wedge r$ | $\wedge$i 5,1 |
| 7 | $p \to (q \wedge r)$ | $\to$i 3-6 |

2. For the sequents below, show which ones are valid and which ones aren't:

(b) $\neg p \vee \neg q \vdash \neg(p \wedge q)$

The sequent is valid. Proof:

| | | |
|---|---|---|
| 1 | $\neg p \lor \neg q$ | premise |
| 2 | $p \land q$ | assumption |
| 3 | $\neg p$ | assumption |
| 4 | $p$ | $\land e_1$ 2 |
| 5 | $\bot$ | $\neg$e 4,3 |
| 6 | $\neg q$ | assumption |
| 7 | $q$ | $\land e_2$ 2 |
| 8 | $\bot$ | $\neg$e 7,6 |
| 9 | $\bot$ | $\lor$e 1,3-5,6-8 |
| 10 | $\neg(p \land q)$ | $\neg$i 2-9 |

(d) $p \lor q, \neg q \lor r \vdash p \lor r$

The sequent is valid. Proof:

| | | |
|---|---|---|
| 1 | $p \lor q$ | premise |
| 2 | $\neg q \lor r$ | premise |
| 3 | $p$ | assumption |
| 4 | $p \lor r$ | $\lor i_1$ 3 |
| 5 | $q$ | assumption |
| 6 | $\neg q$ | assumption |
| 7 | $q$ | copy 5 |
| 8 | $\bot$ | $\neg$e 7,6 |
| 9 | $r$ | $\bot$e 8 |
| 10 | $r$ | assumption |
| 11 | $r$ | copy 10 |
| 12 | $r$ | $\lor$e 2,6-9,10-11 |
| 13 | $p \lor r$ | $\lor i_2$ 12 |
| 14 | $p \lor r$ | $\lor$e 1,3-4,5-13 |

(e) $p \to (q \lor r), \neg q, \neg r \vdash \neg p$ without using the MT rule

The sequent is valid. Proof:

| | | |
|---|---|---|
| 1 | $p \to (q \lor r)$ | premise |
| 2 | $\neg q$ | premise |
| 3 | $\neg r$ | premise |
| 4 | $p$ | assumption |
| 5 | $q \lor r$ | $\to$e 4, 1 |
| 6 | $q$ | assumption |
| 7 | $\bot$ | $\neg$e 6,2 |
| 8 | $r$ | assumption |
| 9 | $\bot$ | $\neg$e 8,3 |
| 10 | $\bot$ | $\lor$e 5, 6-7, 8-9 |
| 11 | $\neg p$ | $\neg$i 4-10 |

(f) $\neg p \wedge \neg q \vdash \neg(p \vee q)$

The sequent is valid. Proof:

| | | |
|---|---|---|
| 1 | $\neg p \wedge \neg q$ | premise |
| 2 | $p \vee q$ | assumption |
| 3 | $p$ | assumption |
| 4 | $\neg p$ | $\wedge e_1$ 1 |
| 5 | $\bot$ | $\neg e$ 3 4 |
| 6 | $q$ | assumption |
| 7 | $\neg q$ | $\wedge e_2$ 1 |
| 8 | $\bot$ | $\neg e$ 6 7 |
| 9 | $\bot$ | $\vee e$ 2,3-5,6-7 |
| 10 | $\neg(p \vee q)$ | $\neg i$ 2-9 |

(h) $p \to q, s \to t \vdash p \vee s \to q \wedge t$

The sequent is not valid. Consider for instance the following valuation:

$$\{p : F, s : T, q : F, t : T\}$$

3. Prove the validity of the sequents below:

(e) $\neg(p \to q) \vdash q \to p$

| | | |
|---|---|---|
| 1 | $\neg(p \to q)$ | premise |
| 2 | $q$ | assumption |
| 3 | $p$ | assumption |
| 4 | $q$ | copy 2 |
| 5 | $p \to q$ | $\to i$ 3-4 |
| 6 | $\bot$ | $\neg e$ 5,1 |
| 7 | $p$ | $\bot e$ 6 |
| 8 | $q \to p$ | $\to i$ 2-7 |

(g) $\vdash \neg p \vee q \rightarrow (p \rightarrow q)$

| | | |
|---|---|---|
| 1 | $\neg p \vee q$ | assumption |
| 2 | $\neg p$ | assumption |
| 3 | $p$ | assumption |
| 4 | $\bot$ | $\neg$e 3,2 |
| 5 | $q$ | $\bot$e 4 |
| 6 | $p \rightarrow q$ | $\rightarrow$i 3-5 |
| 7 | $q$ | assumption |
| 8 | $p$ | assumption |
| 9 | $q$ | copy 7 |
| 10 | $p \rightarrow q$ | $\rightarrow$i 8-9 |
| 11 | $p \rightarrow q$ | $\vee$e 1,2-6,7-10 |
| 12 | $\neg p \vee q \rightarrow (p \rightarrow q)$ | $\rightarrow$i 1-11 |

(i) $(c \wedge n) \rightarrow t, h \wedge \neg s, h \wedge \neg(s \vee c) \rightarrow p \vdash (n \wedge \neg t) \rightarrow p$

| | | |
|---|---|---|
| 1 | $(c \wedge n) \rightarrow t$ | premise |
| 2 | $h \wedge \neg s$ | premise |
| 3 | $h \wedge \neg(s \vee c) \rightarrow p$ | premise |
| 4 | $n \wedge \neg t$ | assumption |
| 5 | $h$ | $\wedge$e1 2 |
| 6 | $s \vee c$ | assumption |
| 7 | $s$ | assumption |
| 8 | $\neg s$ | $\wedge$e2 2 |
| 9 | $\bot$ | $\neg$e 7,8 |
| 10 | $c$ | assumption |
| 11 | $n$ | $\wedge$e1 4 |
| 12 | $c \wedge n$ | $\wedge$i 10,11 |
| 13 | $t$ | $\rightarrow$e 12,1 |
| 14 | $\neg t$ | $\wedge$e2 4 |
| 15 | $\bot$ | $\neg$e 13,14 |
| 16 | $\bot$ | $\vee$e 6,7-9,10-15 |
| 17 | $\neg(s \vee c)$ | $\neg$i 6-16 |
| 18 | $h \wedge \neg(s \vee c)$ | $\wedge$i 5,17 |
| 19 | $p$ | $\rightarrow$e 18,3 |
| 20 | $(n \wedge \neg t) \rightarrow p$ | $\rightarrow$i 4-19 |

## Exercises 1.4 (page 82)

2. Compute the complete truth table of the formula

   (d) $(p \wedge q) \rightarrow (p \vee q)$

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

   (e) $((p \rightarrow \neg q) \rightarrow \neg p) \rightarrow q$

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

   (f) $(p \rightarrow q) \wedge (p \rightarrow \neg q)$

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

   (g) $((p \rightarrow q) \rightarrow p) \rightarrow p$

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

   (h) $((p \vee q) \rightarrow r) \rightarrow ((p \rightarrow r) \vee (q \rightarrow r))$

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

(i) $(p \to q) \to (\neg p \to \neg q)$

| $p$ | $q$ | $\neg p$ | $\neg q$ | $p \to q$ | $\neg p \to \neg q$ | $(p \to q) \to (\neg p \to \neg q)$ |
|---|---|---|---|---|---|---|
| T | T | F | F | T | T | T |
| T | F | F | T | F | T | T |
| F | T | T | F | T | F | F |
| F | F | T | T | T | T | T |

7. These exercises let you practice proofs using mathematical induction. Make sure that you state your base case and inductive step clearly. You should also indicate where you apply the induction hypothesis.

(c) Use mathematical induction to show that $1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

Let $sqsum(n) = 1^2 + 2^2 + 3^2 + \ldots + n^2$.

**Basecase**

$$\begin{aligned} sqsum(1) &= 1 && \{\text{Def. } sqsum\} \\ &= \frac{1(1+1)(2 \cdot 1 + 1)}{6} && \{\text{arithmetics}\} \end{aligned}$$

**Induction step**
Assume

$$sqsum(k) = \frac{k(k+1)(2k+1)}{6} \qquad \text{(I.H.)}$$

$$\begin{aligned} sqsum(k+1) &= sqsum(k) + (k+1)^2 && \{\text{Def. } sqsum\} \\ &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 && \{\text{I.H.}\} \\ &= \frac{2k^3 + k^2 + 2k^2 + k + 6k^2 + 12k + 6}{6} && \{\text{arithmetics}\} \\ &= \frac{(k+1)(k+2)(2k+3)}{6} && \{\text{arithmetics}\} \\ &= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6} && \{\text{arithmetics}\} \end{aligned}$$

12. Show that the following sequents are not valid by finding a valuation in which the truth values of the formulas to the left of $\vdash$ are T and the truth value of the formula to the right of $\vdash$ is F.

(a) $\neg p \lor (q \to p) \vdash \neg p \land q$

$\{p : T,\ q : F\}$ yields $\underbrace{\neg p \lor \underbrace{(q \to p)}_{T}}_{T} \vdash \underbrace{\neg p \land \underbrace{q}_{F}}_{F}$

(b) $\neg r \to (p \lor q), r \land \neg q \vdash r \to q$

$\{p : T, q : F, r : T\}$ yields $\underbrace{\underbrace{\neg r}_{F} \to (p \lor q)}_{T}, \underbrace{\underbrace{r}_{T} \land \underbrace{\neg q}_{T}}_{T} \vdash \underbrace{r \to q}_{F}$

17. Does $\vDash \phi$ hold for the $\phi$ below? Please justify your answer.

(a) $(p \to q) \lor (q \to r)$

$\vDash (p \to q) \lor (q \to r)$ holds since either $q$ is true (in which case $p \to q$ is true), or $q$ is false (in which case $q \to r$ is true).

## Exercises 2.1 (page 157)

4. Let $F(x, y)$ mean that $x$ is the father of $y$; $M(x, y)$ denotes $x$ is the mother of $y$. Similarly, $H(x, y)$, $S(x, y)$, and $B(x, y)$ say that $x$ is the husband/sister/brother of $y$, respectively. You may also use constants to denote individuals, like 'Ed' and 'Patsy.' However, you are not allowed to use any predicate symbols other than the above to translate the following sentences into predicate logic:

(a) Everybody has a mother.

$\forall a\ \exists b\ M(b, a)$

(b) Everybody has a father and a mother.

$\forall a\ \exists b, c\ M(b, a) \land F(c, a)$

(c) Whoever has a mother has a father.

$\forall a\ (\exists b\ M(b, a) \to \exists c\ F(c, a))$

(d) Ed is a grandfather.

$$\exists a, b\ (F(Ed, a) \wedge (M(a, b) \vee F(a, b)))$$

(e) All fathers are parents.

$$\forall a\ ((\exists b\ F(a, b)) \rightarrow \exists b\ P(a, b))$$

where $P(x, y) = F(x, y) \vee M(x, y)$ means that "x is a parent of y".

(f) All husbands are spouses.

$$\forall a\ (\ \underbrace{(\exists b\ H(a, b))}_{a \text{ is a husband}}\ \rightarrow\ \underbrace{\exists b\ Q(a, b)}_{a \text{ is a spouse}}\ )$$

where $Q(x, y) = H(x, y) \vee H(y, x)$ means that "x is spouse of y".

(g) No uncle is an aunt.

An uncle is either the brother of a parent or the husband of a sister of a parent. A woman with an equivalent relationship is an aunt,

$$\forall a\ (\underbrace{(\exists b\ U(a, b))}_{a \text{ is an uncle}} \rightarrow \neg\ \underbrace{\exists b\ A(a, b)}_{a \text{ is an aunt}}\ )$$

where

$U(x, y) = \exists z\ P(z, y) \wedge (B(x, z) \vee \exists v\ S(v, z) \wedge H(x, v))$ means "$x$ is an uncle of $y$".
$A(x, y) = \exists z\ P(z, y) \wedge (S(x, z) \vee \exists v\ B(v, z) \wedge H(v, x))$ means "$x$ is an aunt of $y$".

(h) All brothers are siblings.

$$\forall a\ ((\exists b\ B(a, b)) \rightarrow \underbrace{(\exists b\ B(b, a) \vee S(b, a))}_{a \text{ is a sibbling}})$$

(i) Nobody's grandmother is anybody's father.

$$\forall a\ ((\exists b\ G(a, b)) \rightarrow \neg\exists b\ F(a, b))$$

where

$G(x, y) = \exists z\ (P(z, y) \wedge M(x, z))$ means "$x$ is a grandmother of $y$"
$P(x, y) = F(x, y) \vee M(x, y)$ means "x is a parent of y".

(j) Ed and Patsy are husband and wife.

$H(Ed, Patsy)$ or
$H(Ed, Patsy) \wedge W(Patsy, Ed)$ where $W(x, y) = H(y, x)$ means "$x$ is wife of $y$".

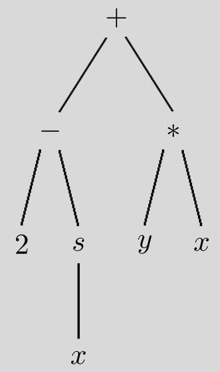
(k) Carl is Monique's brother-in-law.

A brother-in-law is one's sibling's husband, or one's spouse's brother.

$\exists a\ (S(a, Monique) \wedge H(Carl, a)) \vee \exists a\ (H(a, Monique) \wedge B(Carl, a))$

## Exercises 2.2 (page 158)

2. Draw the parse tree of the term $(2 - s(x)) + (y * x)$, considering that $-$, $+$, and $*$ are used in infix in this term. Compare your solution with the parse tree in Figure 2.14.




4. Let $\phi$ be $\exists x\ (P(y, z) \wedge (\forall y\ (\neg Q(y, x) \vee P(y, z))))$, where $P$ and $Q$ are predicate symbols with two arguments.

(c) Is there a variable in $\phi$ which has free and bound occurrences?

$y$ occurs both bound and free.

$$\phi = \exists x\ (P(\underbrace{y}_{free}, z) \wedge (\forall y\ (\neg Q(\underbrace{y}_{bound}, x) \vee P(\underbrace{y}_{bound}, z))))$$

(d) Consider the terms $w$ ($w$ is a variable), $f(x)$ and $g(y, z)$, where $f$ and $g$ are function symbols with arity 1 and 2, respectively.

i. Compute $\phi[w/x]$, $\phi[w/y]$, $\phi[f(x)/y]$, $\phi[g(y, z)/z]$

$\phi[w/x] = \phi$ (no free occurences of $x$.)

$\phi[w/y] = \exists x\ (P(w, z) \wedge (\forall y\ (\neg Q(y, x) \vee P(y, z))))$ (only first $y$ is free.)

$\phi[f(x)/y] = \exists x' \ (P(f(x), z) \wedge (\forall y \ (\neg Q(y, x') \vee P(y, z))))$ (avoid capturing $x$!)

$\phi[g(y,z)/z] = \exists x \ (P(y, g(y,z)) \wedge (\forall y' \ (\neg Q(y', x) \vee P(y', g(y,z)))))$ (avoid capturing $y$!)

ii. Which of $w$, $f(x)$ and $g(y,z)$ are free for $x$ in $\phi$?

$w$, $f(x)$, $g(y,z)$ (no free occurences of $x$!)

iii. Which of $w$, $f(x)$ and $g(y,z)$ are free for $y$ in $\phi$?

$w$, $g(y,z)$ (there is a free occurence of $y$ in the scope of $\exists x$, thus $f(x)$ is not free for $y$ in $\phi$.)

(e) What is the scope of $\exists x$ in $\phi$?

$$\exists x \ \underbrace{(P(y,z) \wedge (\forall y \ (\neg Q(y,x) \vee P(y,z))))}_{scope \ \ of \ \ \exists x}$$

## Exercises 2.3 (page 160)

1. Prove the validity of the following sequents using, among others, the rules =i and =e. Make sure that you indicate for each application of =e what the rule instances $\phi$, $t_1$ and $t_2$ are.

(a) $(y = 0) \wedge (y = x) \vdash 0 = x$

| | | |
|---|---|---|
| 1 | $(y = 0) \wedge (y = x)$ | premise |
| 2 | $y = 0$ | $\wedge e_1$ 1 |
| 3 | $y = x$ | $\wedge e_2$ 1 |
| 4 | $0 = x$ | =e 2,3 |

Where

$$\frac{t_1 = t_2 \quad \phi[t_1/x]}{\phi[t_2/x]} = e$$

$$\left.\begin{array}{l} t_1 \equiv y \\ t_2 \equiv 0 \\ \phi \equiv z = x \end{array}\right\} \begin{array}{ll} \phi[t_1/z] \equiv y = x & \text{(row 3)} \\ \phi[t_2/z] \equiv 0 = x & \text{(row 4)} \end{array}$$

9. Prove the validity of the following sequents in predicate logic, where $F$ , $G$, $P$, and $Q$ have arity 1, and $S$ has arity 0 (a 'propositional atom'):

(x) (not in the book) $\exists x\ (P(x) \rightarrow q) \vdash \forall x\ P(x) \rightarrow q$

| | | | |
|---|---|---|---|
| 1 | | $\exists x(P(x) \rightarrow q)$ | premise |
| 2 | | $\forall x P(x)$ | assumption |
| 3 | $x_0$ | $P(x_0) \rightarrow q$ | assumption |
| 4 | | $P(x_0)$ | ∀x e 2 |
| 5 | | $q$ | →e 4,3 |
| 6 | | $q$ | ∃x e 1, 3-5 |
| 7 | | $\forall x P(x) \rightarrow q$ | →i 2-6 |

(c) $\exists x\ P(x) \rightarrow q \vdash \forall x\ (P(x) \rightarrow q)$

| | | | |
|---|---|---|---|
| 1 | | $\exists x\ P(x) \rightarrow q$ | premise |
| 2 | $x_0$ | | |
| 3 | | $P(x_0)$ | assumption |
| 4 | | $\exists x P(x)$ | ∃x i 3 |
| 5 | | $q$ | →e 4,1 |
| 6 | | $P(x_0) \rightarrow q$ | →i 3-5 |
| 7 | | $\forall x(P(x) \rightarrow q)$ | ∀x i 2-6 |

(k) $\forall x\ (P(x) \wedge Q(x)) \vdash \forall x\ P(x) \wedge \forall x\ Q(x)$

| | | | |
|---|---|---|---|
| 1 | | $\forall x\ (P(x) \wedge Q(x))$ | premise |
| 2 | $x_0$ | | |
| 3 | | $P(x_0) \wedge Q(x_0)$ | ∀x e 1 |
| 4 | | $P(x_0)$ | $\wedge e_1$ 3 |
| 5 | | $\forall x\ P(x)$ | ∀x i 2-4 |
| 6 | $x_1$ | | |
| 7 | | $P(x_1) \wedge Q(x_1)$ | ∀x e 1 |
| 8 | | $Q(x_1)$ | $\wedge e_2$ 7 |
| 9 | | $\forall x\ Q(x)$ | ∀x i 6-8 |
| 10 | | $\forall x\ P(x) \wedge \forall x Q(x)$ | ∧i 5,9 |

(y) (not in book) $\exists x\ (P(x) \vee Q(x)) \vdash \exists x\ P(x) \vee \exists x\ Q(x)$

| | | | |
|---|---|---|---|
| 1 | | $\exists x(P(x) \vee Q(x))$ | premise |
| 2 | $x_0$ | $P(x_0) \vee Q(x_0)$ | assumption |
| 3 | | $P(x_0)$ | assumption |
| 4 | | $\exists x P(x)$ | ∃x i 3 |
| 5 | | $\exists x P(x) \vee \exists x Q(x)$ | ∨i1 4 |
| 6 | | $Q(x_0)$ | assumption |
| 7 | | $\exists x Q(x_0)$ | ∃x i 6 |
| 8 | | $\exists x P(x) \vee \exists x Q(x)$ | ∨i 2 7 |
| 9 | | $\exists x P(x) \vee \exists x Q(x)$ | ∨e 2, 3-5, 6-8 |
| 10 | | $\exists x P(x) \vee \exists x Q(x)$ | ∃x e 1,2-9 |

(r) $\neg\exists x\ P(x) \vdash \forall x\ \neg P(x)$

| | | | |
|---|---|---|---|
| 1 | | $\neg\exists x P(x)$ | premise |
| 2 | $x_0$ | | |
| 3 | | $P(x_0)$ | assumption |
| 4 | | $\exists x P(x)$ | ∃x i 3 |
| 5 | | $\bot$ | ¬e 4,1 |
| 6 | | $\neg P(x_0)$ | ¬i 3-5 |
| 7 | | $\forall x \neg P(x)$ | ∀x i 2-6 |

(z) (not in book) $\exists x\ \neg P(x) \vdash \neg\forall x\ P(x)$

| | | | |
|---|---|---|---|
| 1 | | $\exists x \neg P(x)$ | premise |
| 2 | | $\forall x P(x)$ | assumption |
| 3 | $x_0$ | $\neg P(x_0)$ | assumption |
| 4 | | $P(x_0)$ | ∀x e 2 |
| 5 | | $\bot$ | ¬e 4,3 |
| 6 | | $\bot$ | ∃x e 1,3-5 |
| 7 | | $\neg\forall x P(x)$ | ¬i 2-6 |

## Exercises 2.4 (page 163)

3. Let $P$ be a predicate with two arguments. Find a model which satisfies the sentence $\forall x\ \neg P(x,x)$; also find one which doesn't.

$\mathcal{M}_1 : A \stackrel{def}{=} \{a,b\} \quad P^{\mathcal{M}_1} \stackrel{def}{=} \{(a,b),(b,a)\}$

$$
\begin{aligned}
& \mathcal{M}_1 \models_l \forall x\ \neg P(x,x) \\
\Leftrightarrow\ & \mathcal{M}_1 \models_{l[x\mapsto a]} \neg P(x,x) \text{ and } \mathcal{M}_1 \models_{l[x\mapsto b]} \neg P(x,x) \\
\Leftrightarrow\ & \text{not } \mathcal{M}_1 \models_{l[x\mapsto a]} P(x,x) \text{ and not } \mathcal{M}_1 \models_{[x\mapsto b]} P(x,x) \\
\Leftrightarrow\ & \text{not } (a,a) \in P^{\mathcal{M}_1} \text{ and not } (b,b) \in P^{\mathcal{M}_1} \\
\Leftrightarrow\ & T \text{ (true)}
\end{aligned}
$$

$$
\mathcal{M}_2 : A \stackrel{def}{=} \{a,b\} \quad P^{\mathcal{M}_2} \stackrel{def}{=} \{(a,a),(a,b)\}
$$

$$
\begin{aligned}
& \mathcal{M}_2 \models_l \forall x\ \neg P(x,x) \\
\Leftrightarrow\ & ... \\
\Leftrightarrow\ & \text{not } (a,a) \in P^{\mathcal{M}_2} \text{ and not } (b,b) \in P^{\mathcal{M}_2} \\
\Leftrightarrow\ & F \text{ (false)}
\end{aligned}
$$

## Exercises 3.4 (page 247)

6. Consider the system $\mathcal{M}$ in Figure 3.40.

   (b) Determine whether $\mathcal{M}, s_0 \vDash \phi$ and $\mathcal{M}, s_2 \vDash \phi$ hold and justify your answer, where $\phi$ is the LTL or CTL formula:

   i. $\neg p \to r$

   $\mathcal{M}, s_0 \vDash \neg p \to r$ holds since $r$ holds in $s_0$.

   $\mathcal{M}, s_2 \vDash \neg p \to r$ holds since $r$ holds in $s_2$.

   iii. $\neg \mathsf{EG}\ r$

   $\mathcal{M}, s_0 \vDash \neg \mathsf{EG}\ r$ does not hold, since $\mathsf{EG}\ r$ holds in $s_0$ (take for instance $(s_0, s_0, s_0, \ldots)$).

   $\mathcal{M}, s_2 \vDash \neg \mathsf{EG}\ r$ does not hold, since $\mathsf{EG}\ r$ holds in $s_2$ (take for instance $(s_2, s_1, s_2, s_1, \ldots)$).

   vi. $\mathsf{EF}\ q$

   $\mathcal{M}, s_0 \vDash \mathsf{EF}\ q$ holds since $q$ holds in $s_0$.

   $\mathcal{M}, s_2 \vDash \mathsf{EF}\ q$ holds since $q$ holds in $s_2$.

   vii. $\mathsf{EG}\ r$

   Both $\mathcal{M}, s_0 \vDash \mathsf{EG}\ r$, $\mathcal{M}, s_2 \vDash \mathsf{EG}\ r$ hold. See (iii).

8. Consider the model $\mathcal{M}$ in Figure 3.41. Check whether $\mathcal{M}, s_0 \vDash \phi$ and $\mathcal{M}, s_2 \vDash \phi$ hold for the CTL formulas $\phi$:

   (a) $\mathsf{AF}\ q$

$$\dfrac{\dfrac{-}{\mathcal{M}, s_0 \vdash_{[]} q}\ p}{\mathcal{M}, s_0 \vdash_{[]} \mathsf{AF}\ q}\ \mathsf{AF}_1$$

$$\dfrac{\dfrac{\dfrac{-}{\mathcal{M}, s_0 \vdash_{[]} q}\ p}{\mathcal{M}, s_0 \vdash_{s_2} \mathsf{AF}\ q}\ \mathsf{AF}_1 \quad \dfrac{\dfrac{-}{\mathcal{M}, s_3 \vdash_{[]} q}\ p}{\mathcal{M}, s_3 \vdash_{s_2} \mathsf{AF}\ q}\ \mathsf{AF}_1}{\mathcal{M}, s_2 \vdash_{[]} \mathsf{AF}\ q}\ \mathsf{AF}_2$$

(b) $\mathsf{AG}\ (\mathsf{EF}\ (p \lor r))$

See Figure 1.1

(c) $\mathsf{EX}\ (\mathsf{EX}\ r)$

$$\dfrac{\dfrac{\dfrac{-}{\mathcal{M}, s_1 \vdash_{[]} r}\ p}{\mathcal{M}, s_1 \vdash_{[]} \mathsf{EX}\ r}\ \mathsf{EX}}{\mathcal{M}, s_0 \vdash_{[]} \mathsf{EX}(\mathsf{EX}\ r)}\ \mathsf{EX}$$

$$\dfrac{\dfrac{\dfrac{-}{\mathcal{M}, s_3 \vdash_{[]} r}\ p}{\mathcal{M}, s_0 \vdash_{[]} \mathsf{EX}\ r}\ \mathsf{EX}}{\mathcal{M}, s_2 \vdash_{[]} \mathsf{EX}(\mathsf{EX}\ r)}\ \mathsf{EX}$$

(d) $\mathsf{AG}\ (\mathsf{AF}\ q)$

$\mathcal{M}, s_0 \vDash \mathsf{AG}(\mathsf{AF}\ q)$ does not hold since $\mathsf{AF}\ q$ does not hold for $(s_0, s_1, s_1, s_1 \ldots)$.

$\mathcal{M}, s_2 \vDash \mathsf{AG}(\mathsf{AF}\ q)$ does not hold since $\mathsf{AF}\ q$ does not hold for $(s_2, s_0, s_1, s_1, s_1 \ldots)$.

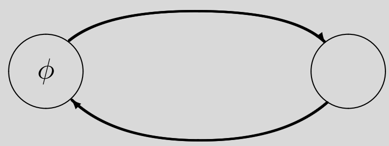
(x) (not in book) $\mathsf{EF}\ (\mathsf{EG}\ r)$

$$\dfrac{\dfrac{\dfrac{\dfrac{-}{\mathcal{M}, s_1 \vdash_{[]} r}\ p \qquad \dfrac{-}{\mathcal{M}, s_1 \vdash_{[s_1]} \mathsf{EG}\ r}\ \mathsf{EG}_1}{\mathcal{M}, s_1 \vdash_{[]} \mathsf{EG}\ r}\ \mathsf{EG}_2}{\mathcal{M}, s_1 \vdash_{[s_0]} \mathsf{EF}\ (\mathsf{EG}\ r)}\ \mathsf{EF}_1}{\mathcal{M}, s_0 \vdash_{[]} \mathsf{EF}\ (\mathsf{EG}\ r)}\ \mathsf{EF}_2$$

10. Which of the following pairs of CTL formulas are equivalent? For those which are not, exhibit a model of one of the pair which is not a model of the other:

(a) $\mathsf{EF}\ \phi$ and $\mathsf{EG}\ \phi$

$\mathsf{EF}\ \phi \not\equiv \mathsf{EG}\ \phi$



(b) $\mathsf{EF}\ \phi \vee \mathsf{EF}\ \psi$ and $\mathsf{EF}\ (\phi \vee \psi)$

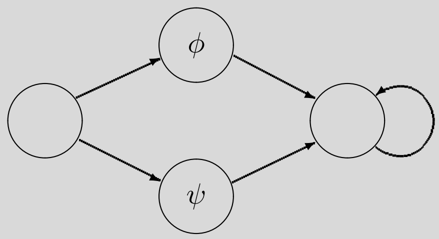
$\mathsf{EF}\ \phi \vee \mathsf{EF}\ \psi \equiv \mathsf{EF}(\phi \vee \psi)$

$\Rightarrow$: If $\mathsf{EF}\ \phi$ holds there is a path in which $\phi$ eventually holds, thus there is a path in which $\phi \vee \psi$ eventually holds. If $\mathsf{EF}\ \psi$ holds there is a path in which $\psi$ eventually holds, thus there is a path in which $\phi \vee \psi$ eventually holds. It follows that $\mathsf{EF}(\phi \vee \psi)$ holds. (Think of it as an or-elimination.)

$\Leftarrow$: If $\mathsf{EF}(\phi \vee \psi)$ holds there is a path in which $\phi$ eventually holds or in which $\psi$ eventually holds. In the former case, $\mathsf{EF}\ \phi$ holds, and in the latter case, $\mathsf{EF}\ \psi$ holds, thus $\mathsf{EF}\ \phi \vee \mathsf{EF}\ \psi$ holds. (Again, think of it as an or-elimination.)

(c) $\mathsf{AF}\ \phi \vee \mathsf{AF}\ \psi$ and $\mathsf{AF}\ (\phi \vee \psi)$

$\mathsf{AF}\ \phi \vee \mathsf{AF}\ \psi \not\equiv \mathsf{AF}(\phi \vee \psi)$



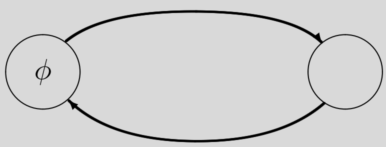

(d) $\mathsf{AF}\ \neg\phi$ and $\neg\mathsf{EG}\ \phi$

$\mathsf{AF}\ \neg\phi \equiv \neg\mathsf{EG}\ \phi$:

| | |
|---|---|
| Page 216 in the course book states that | $\neg\mathsf{AF}\ \phi \equiv \mathsf{EG}\ \neg\phi$ |
| By replacing $\phi$ with $\neg\phi$ we get | $\neg\mathsf{AF}\ \neg\phi \equiv \mathsf{EG}\ \neg\neg\phi$ |
| Negating both sides results in | $\neg\neg\mathsf{AF}\ \neg\phi \equiv \neg\mathsf{EG}\ \neg\neg\phi$ |
| Removing double negations gives: | $\mathsf{AF}\ \neg\phi \equiv \neg\mathsf{EG}\phi$ |

(e) $\mathsf{EF}\ \neg\phi$ and $\neg\mathsf{AF}\ \phi$

$\mathsf{EF}\ \neg\phi \not\equiv \neg\mathsf{AF}\ \phi$



# Exercises 4.3 (page 300)

5. Use the proof rule for assignment and logical implication as appropriate to show the validity of

   (a) $\vdash_{\mathsf{par}} (\!|x > 0|\!)\ \mathtt{y} = \mathtt{x} + \mathtt{1};\ (\!|y > 1|\!)$

$$\dfrac{\overset{\checkmark}{\vdash x > 0 \to x + 1 > 1} \qquad \dfrac{-}{(\!|x + 1 > 1|\!) y = x + 1; (\!|y > 1|\!)}\ \textit{Assignment}}{(\!|x > 0|\!) y = x + 1; (\!|y > 1|\!)}\ \text{Implied}$$

10. Prove the validity of the sequent $\vdash_{\mathsf{par}} (\!|\top|\!)\ P\ (\!|z = \min(x, y)|\!)$, where $\min(x, y)$ is the smalest number of $x$ and $y$ – e.g. $\min(7, 3) = 3$ – and the code of $P$ is given by

$$
\begin{array}{l}
\textbf{if } (x > y)\ \{ \\
\qquad z = y; \\
\}\ \textbf{else}\ \{ \\
\qquad z = x; \\
\}
\end{array}
$$

By proof tree:

$$\dfrac{\dfrac{\overset{\checkmark}{\vdash \mathit{true} \wedge x > y \to y = \mathit{min}(x, y)} \qquad \dfrac{-}{(\!|y = \mathit{min}(x, y)|\!) z = y; (\!|z = \mathit{min}(x, y)|\!)}\ \text{Assignment}}{(\!|\mathit{true} \wedge x > y|\!) z = y; (\!|z = \mathit{min}(x, y)|\!)}\ \text{Implied} \qquad A}{(\!|\mathit{true}|\!)\textbf{if } (x > y)\{z = y;\}\ \textbf{else}\ \{z = x;\}(\!|z = \mathit{min}(x, y)|\!)}\ \text{If}$$

$$\dfrac{\dfrac{\overset{\checkmark}{\vdash \mathit{true} \wedge \neg(x > 0) \to x = \mathit{min}(x, y)} \qquad \dfrac{-}{(\!|x = \mathit{min}(x, y)|\!) z = x; (\!|z = \mathit{min}(x, y)|\!)}\ \text{Assignment}}{(\!|\mathit{true} \wedge \neg(x > y)|\!) z = x; (\!|z = \mathit{min}(x, y)|\!)}\ \text{Implied}}{A}$$

By proof tableaux:

| | |
|---|---|
| $(\!|\mathit{true}|\!)$ | Precondition |
| **if** $(x > y)$ $\{$ | |
| $\quad (\!|\mathit{true} \wedge x > y|\!)$ | If |
| $\quad (\!|y = \mathit{min}(x, y)|\!)$ | Implied (✓) |
| $\quad z = y;$ | |
| $\quad (\!|z = \mathit{min}(x, y)|\!)$ | Assignment |
| $\}$ **else** $\{$ | |
| $\quad (\!|\mathit{true} \wedge \neg(x > y)|\!)$ | If |
| $\quad (\!|x = \mathit{min}(x, y)|\!)$ | Implied (✓) |
| $\quad z = x;$ | |
| $\quad (\!|z = \mathit{min}(x, y)|\!)$ | Assignment |
| $\}$ | |
| $(\!|z = \mathit{min}(x, y)|\!)$ | Postcondition |

13. Show that $\vdash_{\mathsf{par}} (\!|x \geq 0|\!)$ `Copy1` $(\!|x = y|\!)$ is valid, where `Copy1` denotes the code

```
a = x;
y = 0;
while (a != 0) {
    y = y + 1;
    a = a - 1;
}
```

The loop invariant is in this case $a + y = x$

Here is a proof tableaux

| | |
|---|---|
| $(\!\|x \geq 0\|\!)$ | Precondition |
| $(\!\|x + 0 = x\|\!)$ | Implied (✓) |
| $a = x;$ | |
| $(\!\|a + 0 = x\|\!)$ | Assignment |
| $y = 0;$ | |
| $(\!\|a + y = x\|\!)$ | Assignment |
| **while** $(a \mathrel{!}= 0)$ { | |
| $\quad(\!\|a + y = x \land a \neq 0\|\!)$ | Partial-while |
| $\quad(\!\|(a-1) + (y+1) = x\|\!)$ | Implied (✓) |
| $\quad y = y + 1;$ | |
| $\quad(\!\|(a-1) + y = x\|\!)$ | Assignment |
| $\quad a = a - 1;$ | |
| $\quad(\!\|a + y = x\|\!)$ | Assignment |
| } | |
| $(\!\|a + y = x \land \neg(a \neq 0)\|\!)$ | Partial-while |
| $(\!\|x = y\|\!)$ | Implied ✓ |

We get the following three proof obligations:

| | |
|---|---|
| $\vdash x \geq 0 \to x + 0 = x$ | holds since $x + 0 = 0$ |
| $\vdash a + y = x \land a \neq 0 \to (a-1) + (y+1) = x$ | holds since $(a-1) + (y+1) = a + y$ |
| $\vdash a + y = x \land \neg(a \neq 0) \to x = y$ | holds since $a + y = y$ when $a = 0$ |

14. Show that $\vdash_{\mathsf{par}} (\!|y \geq 0|\!)$ `Mult1` $(\!|z = x \cdot y|\!)$ is valid, where `Mult1` is:

```
a = 0;
z = 0;
while (a != y) {
    z = z + x;
    a = a + 1;
}
```

The proof tableaux is similar to the one in the previous solution, but with the invariant $z = a \cdot x$.

$$
\dfrac{
\dfrac{\dfrac{\dfrac{-}{\mathcal{M}, s_0 \vdash_{[]} p}\;p}{\mathcal{M}, s_0 \vdash_{[]} p \vee r}\;\vee_1}{\mathcal{M}, s_0 \vdash \mathsf{EF}\;(p \vee r)}\;\mathsf{EF}_1
\qquad
\dfrac{
\dfrac{\dfrac{\dfrac{-}{\mathcal{M}, s_3 \vdash_{[]} r}\;p}{\mathcal{M}, s_3 \vdash_{[]} p \vee r}\;\vee_2}{\mathcal{M}, s_3 \vdash \mathsf{EF}\;(p \vee r)}\;\mathsf{EF}_1
\qquad
\dfrac{-}{\mathcal{M}, s_0 \vdash_{s_3, s_0} \mathsf{AG}\;(\mathsf{EF}\;(p \vee r))}\;\mathsf{AG}_1
}{\mathcal{M}, s_3 \vdash_{s_0} \mathsf{AG}\;(\mathsf{EF}\;(p \vee r))}\;\mathsf{AG}_2
\qquad A
}{\mathcal{M}, s_0 \vdash \mathsf{AG}\;(\mathsf{EF}\;(p \vee r))}\;\mathsf{AG}_2
$$

$$
\dfrac{
\dfrac{
\dfrac{\dfrac{\dfrac{-}{\mathcal{M}, s_1 \vdash_{[]} r}\;p}{\mathcal{M}, s_1 \vdash_{[]} p \vee r}\;\vee_2}{\mathcal{M}, s_1 \vdash \mathsf{EF}\;(p \vee r)}\;\mathsf{EF}_1
\quad
\dfrac{-}{\mathcal{M}, s_1 \vdash_{s_1, s_0} \mathsf{AG}\;(\mathsf{EF}\;(p \vee r))}\;\mathsf{AG}_1
\quad
\dfrac{
\dfrac{\dfrac{\dfrac{-}{\mathcal{M}, s_2 \vdash_{[]} p}\;p}{\mathcal{M}, s_2 \vdash_{[]} p \vee r}\;\vee_1}{\mathcal{M}, s_2 \vdash \mathsf{EF}\;(p \vee r)}\;\mathsf{EF}_1
\quad
\dfrac{-}{\mathcal{M}, s_0 \vdash_{s_2, s_1, s_0} \mathsf{AG}\;(\mathsf{EF}\;(p \vee r))}\;\mathsf{AG}_1
\quad
\dfrac{
\dfrac{\dfrac{\dfrac{-}{\mathcal{M}, s_3 \vdash_{[]} r}\;p}{\mathcal{M}, s_3 \vdash_{[]} p \vee r}\;\vee_2}{\mathcal{M}, s_3 \vdash \mathsf{EF}\;(p \vee r)}\;\mathsf{EF}_1
\quad
\dfrac{-}{\mathcal{M}, s_0 \vdash_{s_3, s_2, s_1, s_0} \mathsf{AG}\;(\mathsf{EF}\;(p \vee r))}\;\mathsf{AG}_1
}{\mathcal{M}, s_3 \vdash_{s_2, s_1, s_0} \mathsf{AG}\;(\mathsf{EF}\;(p \vee r))}\;\mathsf{AG}_2
}{\mathcal{M}, s_2 \vdash_{s_1, s_0} \mathsf{AG}\;(\mathsf{EF}\;(p \vee r))}\;\mathsf{AG}_2
}{\mathcal{M}, s_1 \vdash_{s_0} \mathsf{AG}\;(\mathsf{EF}\;(p \vee r))}\;\mathsf{AG}_2
}{A}
$$

Figur 1.1: Solution for exercise 3.4 8 (b).

# Kapitel 2

# Exempel på strukturell induktion: binära träd

## Definition av binära träd

Vi definierar den induktiva datatypen $BTree$ i BNF med en 0-ställig funktionssymbol $\mathsf{leaf}$ och en 2-ställig funktionssymbol $\mathsf{btree}$ enligt nedan.

$$BTree ::= \mathsf{leaf} \mid \mathsf{btree}(BTree, BTree)$$

Två exempel på $BTree$-termer är som följer.

$$\begin{array}{l} \mathsf{leaf} \\ \mathsf{btree}(\mathsf{leaf}, \mathsf{btree}(\mathsf{leaf}, \mathsf{leaf})) \end{array}$$

**Övning 2.1.** (A) Formulera en induktionsprincip för $BTree$-termer. Kvantifiera över alla enställiga predikat $P$ som tar en sådana termer som argument.

$$\forall P \left( P(\mathsf{leaf}) \land \left(\forall t_1 \, \forall t_2 \, (P(t_1) \land P(t_2)) \to P(\mathsf{btree}(t_1, t_2))\right)\right) \to \forall t \, P(t)$$

Tolkning:

För att visa $\forall t \, P(t)$:

- visa $P(\mathsf{leaf})$ (basfall)
- ta godtyckliga $t_1$ och $t_2$ (induktionssteg)
  antag $P(t_1)$ och $P(t_2)$ (induktionshypotes)
  visa $P(\mathsf{btree}(t_1, t_2))$

## Trädhöjd

Vi definierar en induktiv funktion **height** som tar en $BTree$-term som argument och returnerar höjden på det binära träd som termen representerar.

**Definition 2.1.**

$$\begin{aligned} \mathbf{height}(\mathsf{leaf}) &\stackrel{\mathsf{def}}{=} 0 \\ \mathbf{height}(\mathsf{btree}(t_1, t_2)) &\stackrel{\mathsf{def}}{=} 1 + \mathbf{max}(\mathbf{height}(t_1), \mathbf{height}(t_2)) \end{aligned}$$

**Övning 2.2.** (E) Bevisa genom att veckla ut definitionen för **height** att

$$\mathbf{height}(\mathsf{btree}(\mathsf{leaf}, \mathsf{btree}(\mathsf{leaf}, \mathsf{leaf}))) = 2$$

$$\begin{array}{ll}
\mathbf{height}(\mathsf{btree}(\mathsf{leaf}, \mathsf{btree}(\mathsf{leaf}, \mathsf{leaf}))) & \\
= 1 + \mathbf{max}(\mathbf{height}(\mathsf{leaf}), \mathbf{height}(\mathsf{btree}(\mathsf{leaf}, \mathsf{leaf}))) & \{\text{Def. } 2.1\} \\
= 1 + \mathbf{max}(0, 1 + \mathbf{max}(\mathbf{height}(\mathsf{leaf}), \mathbf{height}(\mathsf{leaf}))) & \{\text{Def. } 2.1\} \\
= 1 + \mathbf{max}(0, 1 + \mathbf{max}(0, 0)) & \{\text{Def. } 2.1\} \\
= 1 + \mathbf{max}(0, 1 + 0) & \{\text{Def. } \mathbf{max}\} \\
= 1 + 1 & \{\text{Def. } \mathbf{max},\ \text{Aritmetik}\} \\
= 2 & \{\text{Aritmetik}\}
\end{array}$$

## Lövantal

Vi definierar en induktiv funktion **numleaves** som tar en *BTree*-term som argument och returnerar antalet löv i det binära träd som termen representerar.

**Definition 2.2.**

$$\begin{aligned}
\mathbf{numleaves}(\mathsf{leaf}) &\overset{\mathsf{def}}{=} 1 \\
\mathbf{numleaves}(\mathsf{btree}(t_1, t_2)) &\overset{\mathsf{def}}{=} \mathbf{numleaves}(t_1) + \mathbf{numleaves}(t_2)
\end{aligned}$$

**Övning 2.3.** (E) Bevisa genom att veckla ut definitionen för **numleaves** att

$$\mathbf{numleaves}(\mathsf{btree}(\mathsf{leaf}, \mathsf{btree}(\mathsf{leaf}, \mathsf{leaf}))) = 3$$

$$\begin{array}{ll}
\mathbf{numleaves}(\mathsf{btree}(\mathsf{leaf}, \mathsf{btree}(\mathsf{leaf}, \mathsf{leaf}))) & \\
= \mathbf{numleaves}(\mathsf{leaf}) + \mathbf{numleaves}(\mathsf{btree}(\mathsf{leaf}, \mathsf{leaf})) & \{\text{Def. } 2.2\} \\
= 1 + \mathbf{numleaves}(\mathsf{leaf}) + \mathbf{numleaves}(\mathsf{leaf}) & \{\text{Def. } 2.2\} \\
= 1 + 1 + 1 & \{\text{Def. } 2.2\} \\
= 3 & \{\text{Aritmetik}\}
\end{array}$$

## Kompletta binära träd

Vi definierar ett induktivt predikat **complete** i form av en funktion som tar en *BTree*-term som argument och returnerar *true* om alla löv i det motsvarande binära trädet är på samma höjd, och *false* annars.

**Definition 2.3.**

$$\begin{aligned}
\mathbf{complete}(\mathsf{leaf}) &\overset{\mathsf{def}}{=} \mathit{true} \\
\mathbf{complete}(\mathsf{btree}(t_1, t_2)) &\overset{\mathsf{def}}{=} \mathbf{complete}(t_1) \land \mathbf{complete}(t_2) \land \mathbf{height}(t_1) = \mathbf{height}(t_2)
\end{aligned}$$

**Övning 2.4.** (A) Bevisa genom att använda strukturell induktion att

$$\forall t\ \mathbf{complete}(t) \rightarrow \mathbf{numleaves}(t) = 2^{\mathbf{height}(t)}$$

Låt $t$ vara en *BTree*-term. Vi gör induktion över strukturen för $t$.

- Fall $t = \mathsf{leaf}$.

  Vi har att $\mathbf{complete}(\mathsf{leaf})$ är *true* enligt Def. 2.3 och

  $$\begin{aligned} & \mathbf{numleaves}(\mathsf{leaf}) & \\ & = 1 & \{\text{Def. 2.2}\} \\ & = 2^0 & \{\text{Aritmetik}\} \\ & = 2^{\mathbf{height}(\mathsf{leaf})} & \{\text{Def. 2.1}\} \end{aligned}$$

- Fall $t = \mathsf{btree}(t_1, t_2)$ för $t_1$ och $t_2$ *BTree*-termer.

  Antag som första induktionshypotes ($\text{IH}_1$) att $\mathbf{complete}(t_1) \rightarrow \mathbf{numleaves}(t_1) = 2^{\mathbf{height}(t_1)}$ och som andra induktionshypotes ($\text{IH}_2$) att $\mathbf{complete}(t_2) \rightarrow \mathbf{numleaves}(t_2) = 2^{\mathbf{height}(t_2)}$. Antag sedan som hypotes (H) att $\mathbf{complete}(\mathsf{btree}(t_1, t_2))$ för att visa implikationen.

  $$\begin{aligned} & \mathbf{numleaves}(\mathsf{btree}(t_1, t_2)) & \\ & = \mathbf{numleaves}(t_1) + \mathbf{numleaves}(t_2) & \{\text{Def. 2.2}\} \\ & = 2^{\mathbf{height}(t_1)} + 2^{\mathbf{height}(t_2)} & \{\text{H, IH}_1,\ \text{IH}_2\} \\ & = 2^{1+\mathbf{max}(\mathbf{height}(t_1),\mathbf{height}(t_2))} & \{\text{H, Def. 2.3, Aritmetik}\} \\ & = 2^{\mathbf{height}(\mathsf{btree}(t_1,t_2))} & \{\text{Def. 2.1}\} \end{aligned}$$

# Kapitel 3

# Exempel på strukturell induktion: listor

## Introduktion

I detta kapitel presenteras en övning i användningen av strukturell induktion, i ett scenario som ibland förekommer i systemutveckling—en given funktion ska ersättas av en funktion med samma specifikation som är mer effektiv. Här ska dock bevisas att den nya funktionen har samma beteende som den ursprungliga och att den faktiskt är effektivare.

## Definition av listor

Vi börjar med att i BNF definiera den induktiva datatypen *List*, som tolkas som en lista av termer av typen *Letter*, bokstäver.

$$List ::= \mathsf{empty} \mid \mathsf{cons}(Letter, List)$$

**Övning 3.1.** (A) Formulera en induktionsprincip för *List*-termer. Kvantifiera över alla enställiga predikat $P$ som tar en sådana termer som argument.

$$\forall P \left( P(\mathsf{empty}) \wedge \left(\forall a\ \forall u'\ P(u') \rightarrow P(\mathsf{cons}(a, u'))\right)\right) \rightarrow \forall u\ P(u)$$

Tolkning:

För att visa $\forall u\ P(u)$:

- visa $P(\mathsf{empty})$ (basfall)
- ta godtyckliga $a$ och $u'$ (induktionssteg)
  antag $P(u')$ (induktionshypotes)
  visa $P(\mathsf{cons}(a, u'))$

### Listors längd

Vi definierar en induktiv funktion **length** från mängden av listor till de naturliga talen som ger en listas längd.

**Definition 3.1.**

$$\begin{aligned}\mathbf{length}(\mathsf{empty}) &\stackrel{\mathsf{def}}{=} 0\\ \mathbf{length}(\mathsf{cons}(a,u)) &\stackrel{\mathsf{def}}{=} 1+\mathbf{length}(u)\end{aligned}$$

**Övning 3.2.** (E) Bevisa stegvis genom att veckla ut definitionen för **length** att

$$\forall a\ \forall b\ \mathbf{length}(\mathsf{cons}(a,\mathsf{cons}(b,\mathsf{empty}))) = 2.$$

Låt $a$ och $b$ vara *Letter*-termer.

$$\begin{aligned}&\mathbf{length}(\mathsf{cons}(a,\mathsf{cons}(b,\mathsf{empty})))\\ &= 1+\mathbf{length}(\mathsf{cons}(b,\mathsf{empty})) && \{\text{Def. 3.1}\}\\ &= 1+1+\mathbf{length}(\mathsf{empty}) && \{\text{Def. 3.1}\}\\ &= 1+1+0 && \{\text{Def. 3.1}\}\\ &= 2 && \{\text{Aritmetik}\}\end{aligned}$$

### Konkatenering av listor

Vi definierar en konkateneringsfunktion **conc** som tar två listor som argument och returnerar en sammanslagen lista.

**Definition 3.2.**

$$\begin{aligned}\mathbf{conc}(\mathsf{empty},v) &\stackrel{\mathsf{def}}{=} v\\ \mathbf{conc}(\mathsf{cons}(a,u),v) &\stackrel{\mathsf{def}}{=} \mathsf{cons}(a,\mathbf{conc}(u,v))\end{aligned}$$

**Övning 3.3.** (E) Bevisa stegvis genom att veckla ut definitionen för **conc** att

$$\forall a\ \forall b\ \mathbf{conc}(\mathsf{cons}(a,\mathsf{empty}),\mathsf{cons}(b,\mathsf{empty})) = \mathsf{cons}(a,\mathsf{cons}(b,\mathsf{empty}))$$

Låt $a$ och $b$ vara *Letter*-termer.

$$\begin{aligned}&\mathbf{conc}(\mathsf{cons}(a,\mathsf{empty}),\mathsf{cons}(b,\mathsf{empty}))\\ &= \mathsf{cons}(a,\mathbf{conc}(\mathsf{empty},\mathsf{cons}(b,\mathsf{empty}))) && \{\text{Def. 3.2}\}\\ &= \mathsf{cons}(a,\mathsf{cons}(b,\mathsf{empty})) && \{\text{Def. 3.2}\}\end{aligned}$$

**Övning 3.4.** (C) Bevisa genom att använda strukturell induktion att

$$\forall u\ \mathbf{conc}(u,\mathsf{empty}) = u$$

Låt $u$ vara en *List*-term. Vi gör induktion över strukturen för $u$.

- Fall $u = \mathsf{empty}$.

$$\begin{aligned} &\mathbf{conc}(\mathsf{empty}, \mathsf{empty}) \\ &= \mathsf{empty} && \{\text{Def. } 3.2\} \end{aligned}$$

- Fall $u = \mathsf{cons}(a, u')$ för $a$ en *Letter*-term och $u'$ en *List*-term.

  Antag som induktionshypotes (IH) att $\mathbf{conc}(u', \mathsf{empty}) = u'$.

$$\begin{aligned} &\mathbf{conc}(\mathsf{cons}(a, u'), \mathsf{empty}) \\ &= \mathsf{cons}(a, \mathbf{conc}(u', \mathsf{empty})) && \{\text{Def. } 3.2\} \\ &= \mathsf{cons}(a, u') && \{\text{IH}\} \end{aligned}$$

**Övning 3.5.** (A) Bevisa genom att använda strukturell induktion att **conc** är associativ, dvs bevisa att

$$\forall u \; \forall v \; \forall w \; \mathbf{conc}(u, \mathbf{conc}(v, w)) = \mathbf{conc}(\mathbf{conc}(u, v), w)$$

Låt $u$ vara en *List*-term. Vi gör induktion över strukturen för $u$.

- Fall $u = \mathsf{empty}$.

  Låt $v$ och $w$ vara *List*-termer.

$$\begin{aligned} &\mathbf{conc}(\mathsf{empty}, \mathbf{conc}(v, w)) \\ &= \mathbf{conc}(v, w) && \{\text{Def. } 3.2\} \\ &= \mathbf{conc}(\mathbf{conc}(\mathsf{empty}, v), w) && \{\text{Def. } 3.2\} \end{aligned}$$

- Fall $u = \mathsf{cons}(a, u')$ för $a$ en *Letter*-term och $u'$ en *List*-term.

  Låt $v$ och $w$ vara *List*-termer och antag som induktionshypotes (IH) att $\forall v \; \forall w \; \mathbf{conc}(u', \mathbf{conc}(v, w)) = \mathbf{conc}(\mathbf{conc}(u', v), w)$.

$$\begin{aligned} &\mathbf{conc}(\mathsf{cons}(a, u'), \mathbf{conc}(v, w)) \\ &= \mathsf{cons}(a, \mathbf{conc}(u', \mathbf{conc}(v, w))) && \{\text{Def. } 3.2\} \\ &= \mathsf{cons}(a, \mathbf{conc}(\mathbf{conc}(u', v), w)) && \{\text{IH}\} \\ &= \mathbf{conc}(\mathsf{cons}(a, (\mathbf{conc}(u', v)), w) && \{\text{Def. } 3.2\} \\ &= \mathbf{conc}(\mathbf{conc}(\mathsf{cons}(a, u'), v), w) && \{\text{Def. } 3.2\} \end{aligned}$$

# Omvändning av listor

## En första omvändningsfunktion

Vi definierar en initial omvändningsfunktion **reverse**.

**Definition 3.3.**

$$\mathbf{reverse}(\mathsf{empty}) \stackrel{\text{def}}{=} \mathsf{empty}$$
$$\mathbf{reverse}(\mathsf{cons}(a, u)) \stackrel{\text{def}}{=} \mathbf{conc}(\mathbf{reverse}(u), \mathsf{cons}(a, \mathsf{empty}))$$

**Övning 3.6.** (E) Bevisa stegvis genom att veckla ut definitionen för **reverse** att

$$\forall a\ \forall b\ \mathbf{reverse}(\mathsf{cons}(a, \mathsf{cons}(b, \mathsf{empty}))) = \mathsf{cons}(b, \mathsf{cons}(a, \mathsf{empty}))$$

Låt $a$ och $b$ vara *Letter*-termer.

$$
\begin{aligned}
&\mathbf{reverse}(\mathsf{cons}(a, \mathsf{cons}(b, \mathsf{empty}))) \\
&= \mathbf{conc}(\mathbf{reverse}(\mathsf{cons}(b, \mathsf{empty})), \mathsf{cons}(a, \mathsf{empty})) && \{\text{Def. } 3.3\} \\
&= \mathbf{conc}(\mathbf{conc}(\mathbf{reverse}(\mathsf{empty}), \mathsf{cons}(b, \mathsf{empty})), \mathsf{cons}(a, \mathsf{empty})) && \{\text{Def. } 3.3\} \\
&= \mathbf{conc}(\mathbf{conc}(\mathsf{empty}, \mathsf{cons}(b, \mathsf{empty})), \mathsf{cons}(a, \mathsf{empty})) && \{\text{Def. } 3.2\} \\
&= \mathbf{conc}(\mathsf{cons}(b, \mathsf{empty}), \mathsf{cons}(a, \mathsf{empty})) && \{\text{Def. } 3.2\} \\
&= \mathsf{cons}(b, \mathbf{conc}(\mathsf{empty}, \mathsf{cons}(a, \mathsf{empty}))) && \{\text{Def. } 3.2\} \\
&= \mathsf{cons}(b, \mathsf{cons}(a, \mathsf{empty})) && \{\text{Def. } 3.2\}
\end{aligned}
$$

**Övning 3.7.** (A) Bevisa med strukturell induktion och resultaten från övning 3.4 och 3.5 att **reverse** distribuerar över **conc**, dvs att

$$\forall u\ \forall v\ \mathbf{reverse}(\mathbf{conc}(u, v)) = \mathbf{conc}(\mathbf{reverse}(v), \mathbf{reverse}(u))$$

Låt $u$ vara en *List*-term. Vi gör induktion över strukturen för $u$.

- Fall $u = \mathsf{empty}$.

  Låt $v$ vara en *List*-term.

$$
\begin{aligned}
&\mathbf{reverse}(\mathbf{conc}(\mathsf{empty}, v)) \\
&= \mathbf{reverse}(v) && \{\text{Def. } 3.2\} \\
&= \mathbf{conc}(\mathbf{reverse}(v), \mathsf{empty}) && \{\text{Övn. } 3.4\} \\
&= \mathbf{conc}(\mathbf{reverse}(v), \mathbf{reverse}(\mathsf{empty})) && \{\text{Def. } 3.3\}
\end{aligned}
$$

- Fall $u = \mathsf{cons}(a, u')$ för $a$ en *Letter*-term och $u'$ en *List*-term.

  Antag som induktionshypotes (IH) att $\forall v\ \mathbf{reverse}(\mathbf{conc}(u', v)) = \mathbf{conc}(\mathbf{reverse}(v), \mathbf{reverse}(u'))$, och låt $v$ vara en *List*-term.

$$
\begin{aligned}
&\mathbf{reverse}(\mathbf{conc}(\mathsf{cons}(a, u'), v)) \\
&= \mathbf{reverse}(\mathsf{cons}(a, \mathbf{conc}(u', v))) && \{\text{Def. } 3.2\} \\
&= \mathbf{conc}(\mathbf{reverse}(\mathbf{conc}(u', v)), \mathsf{cons}(a, \mathsf{empty})) && \{\text{Def. } 3.3\} \\
&= \mathbf{conc}(\mathbf{conc}(\mathbf{reverse}(v), \mathbf{reverse}(u')), \mathsf{cons}(a, \mathsf{empty})) && \{\text{IH}\} \\
&= \mathbf{conc}(\mathbf{reverse}(v), \mathbf{conc}(\mathbf{reverse}(u'), \mathsf{cons}(a, \mathsf{empty}))) && \{\text{Övn. } 3.5\} \\
&= \mathbf{conc}(\mathbf{reverse}(v), \mathbf{reverse}(\mathsf{cons}(a, u'))) && \{\text{Def. } 3.3\}
\end{aligned}
$$

### En effektivare omvändningsfunktion?

Vi definierar en funktion **rev** som en hjälpfunktion till en ny omvändningsfunktion **reverse**′.

**Definition 3.4.**

$$\mathbf{rev}(\mathsf{empty}, v) \stackrel{\mathsf{def}}{=} v$$
$$\mathbf{rev}(\mathsf{cons}(a, u), v) \stackrel{\mathsf{def}}{=} \mathbf{rev}(u, \mathsf{cons}(a, v))$$
$$\mathbf{reverse}'(u) \stackrel{\mathsf{def}}{=} \mathbf{rev}(u, \mathsf{empty})$$

**Övning 3.8.** (E) Bevisa stegvis genom att veckla ut definitionen för **reverse**′ att

$$\forall a\ \forall b\ \mathbf{reverse}'(\mathsf{cons}(a, \mathsf{cons}(b, \mathsf{empty}))) = \mathsf{cons}(b, \mathsf{cons}(a, \mathsf{empty}))$$

Låt $a$ och $b$ vara *Letter*-termer.

$$\begin{aligned}
&\mathbf{reverse}'(\mathsf{cons}(a, \mathsf{cons}(b, \mathsf{empty}))) \\
&= \mathbf{rev}(\mathsf{cons}(a, \mathsf{cons}(b, \mathsf{empty})), \mathsf{empty}) && \{\text{Def. } 3.4\} \\
&= \mathbf{rev}(\mathsf{cons}(b, \mathsf{empty}), \mathsf{cons}(a, \mathsf{empty})) && \{\text{Def. } 3.4\} \\
&= \mathbf{rev}(\mathsf{empty}, \mathsf{cons}(b, \mathsf{cons}(a, \mathsf{empty}))) && \{\text{Def. } 3.4\} \\
&= \mathsf{cons}(b, \mathsf{cons}(a, \mathsf{empty})) && \{\text{Def. } 3.4\}
\end{aligned}$$

**Övning 3.9.** (A) Bevisa med strukturell induktion och resultatet från övning 3.5 att

$$\forall u\ \forall v\ \mathbf{conc}(\mathbf{reverse}'(u), v) = \mathbf{rev}(u, v)$$

Låt $u$ vara en *List*-term. Vi gör induktion över strukturen för $u$.

- Fall $u = \mathsf{empty}$.

  Låt $v$ vara en *List*-term.

$$\begin{aligned}
&\mathbf{conc}(\mathbf{reverse}'(\mathsf{empty}), v) \\
&= \mathbf{conc}(\mathbf{rev}(\mathsf{empty}, \mathsf{empty}), v) && \{\text{Def. } 3.4\} \\
&= \mathbf{conc}(\mathsf{empty}, v) && \{\text{Def. } 3.4\} \\
&= v && \{\text{Def. } 3.2\} \\
&= \mathbf{rev}(\mathsf{empty}, v) && \{\text{Def. } 3.4\}
\end{aligned}$$

- Fall $u = \mathsf{cons}(a, u')$ för $a$ en *Letter*-term och $u'$ en *List*-term.

  Antag som induktionshypotes (IH) att $\forall v\ \mathbf{conc}(\mathbf{reverse}'(u'), v) = \mathbf{rev}(u', v)$, och låt $v$ vara en *List*-term.

$$\begin{aligned}
&\mathbf{conc}(\mathbf{reverse}'(\mathsf{cons}(a, u')), v) \\
&= \mathbf{conc}(\mathbf{rev}(u', \mathsf{cons}(a, \mathsf{empty})), v) && \{\text{Def. } 3.4\} \\
&= \mathbf{conc}(\mathbf{conc}(\mathbf{rev}(u', \mathit{empty}), \mathsf{cons}(a, \mathit{empty})), v) && \{\text{IH, Def. } 3.4\} \\
&= \mathbf{conc}(\mathbf{rev}(u', \mathsf{empty}), \mathbf{conc}(\mathsf{cons}(a, \mathsf{empty}), v)) && \{\text{Övn. } 3.5\} \\
&= \mathbf{conc}(\mathbf{reverse}'(u'), \mathsf{cons}(a, v)) && \{\text{Def. } 3.4,\ \text{Def. } 3.2\} \\
&= \mathbf{rev}(\mathsf{cons}(a, u'), v) && \{\text{IH, Def. } 3.4\}
\end{aligned}$$

**Övning 3.10.** (C) Bevisa med hjälp av resultatet från övning 3.9 och strukturell induktion att

$$\forall u \; \mathbf{reverse}(u) = \mathbf{reverse}'(u)$$

Låt $u$ vara en *List*-term. Vi gör induktion över strukturen för $u$.

- Fall $u = \mathsf{empty}$.

$$\begin{aligned} & \mathbf{reverse}(\mathsf{empty}) \\ & = \mathsf{empty} && \{\text{Def. } 3.3\} \\ & = \mathbf{rev}(\mathsf{empty}, \mathsf{empty}) && \{\text{Def. } 3.4\} \\ & = \mathbf{reverse}'(\mathsf{empty}) && \{\text{Def. } 3.4\} \end{aligned}$$

- Fall $u = \mathsf{cons}(a, u')$ för $a$ en *Letter*-term och $u'$ en *List*-term.

  Antag som induktionshypotes (IH) att $\mathbf{reverse}(u') = \mathbf{reverse}'(u')$.

$$\begin{aligned} & \mathbf{reverse}(\mathsf{cons}(a, u')) \\ & = \mathbf{conc}(\mathbf{reverse}(u'), \mathsf{cons}(a, \mathsf{empty})) && \{\text{Def. } 3.3\} \\ & = \mathbf{conc}(\mathbf{reverse}'(u'), \mathsf{cons}(a, \mathsf{empty})) && \{\text{IH}\} \\ & = \mathbf{reverse}'(\mathsf{cons}(a, u')) && \{\text{Övn. } 3.9\} \end{aligned}$$

# Effektivitetsanalys

## Effektivitetsmått

För att uttrycka funktioners effektivitet kan man låta dem returnera tuplar, där den ena delen är ett effektivitetsmått och den andra delen är det önskade resultatet. De olika delarna görs sedan åtkomliga med tilläggsfunktioner enligt följande.

**Definition 3.5.**

$$\begin{aligned} \mathbf{cost}(\langle s, d \rangle) &\stackrel{\text{def}}{=} s \\ \mathbf{result}(\langle s, d \rangle) &\stackrel{\text{def}}{=} d \end{aligned}$$

## Mätbara varianter av funktioner

Betrakta en mätbar variant av funktionen **conc**.

**Definition 3.6.**

$$\begin{aligned} \mathbf{mconc}(\mathsf{empty}, v) &\stackrel{\text{def}}{=} \langle 0, v \rangle \\ \mathbf{mconc}(\mathsf{cons}(a, u'), v) &\stackrel{\text{def}}{=} \mathbf{let}\ r = \mathbf{mconc}(u', v)\ \mathbf{in} \\ & \quad\ \langle 1 + \mathbf{cost}(r), \mathsf{cons}(a, \mathbf{result}(r)) \rangle \end{aligned}$$

**Övning 3.11.** (C) Bevisa genom att använda strukturell induktion att **conc** och resultatdelen av **mconc** sammanfaller för alla listor, dvs att

$$\forall u \, \forall v \; \mathbf{result}(\mathbf{mconc}(u, v)) = \mathbf{conc}(u, v)$$

Låt $u$ vara en *List*-term. Vi gör induktion över strukturen för $u$.

- Fall $u = \mathsf{empty}$.

  Låt $v$ vara en *List*-term.

$$\begin{aligned}
&\mathbf{result}(\mathbf{mconc}(\mathsf{empty}, v)) \\
&= \mathbf{result}(\langle 0, v\rangle) && \{\text{Def. 3.6}\} \\
&= v && \{\text{Def. 3.5}\} \\
&= \mathbf{conc}(\mathsf{empty}, v) && \{\text{Def. 3.2}\}
\end{aligned}$$

- Fall $u = \mathsf{cons}(a, u')$ för $a$ en *Letter*-term och $u'$ en *List*-term.

  Antag som induktionshypotes (IH) att $\forall v\ \mathbf{result}(\mathbf{mconc}(u', v)) = \mathbf{conc}(u', v)$, och låt $v$ vara en *List*-term.

$$\begin{aligned}
&\mathbf{result}(\mathbf{mconc}(\mathsf{cons}(a, u'))) \\
&= \mathsf{cons}(a, \mathbf{result}(\mathbf{mconc}(u', v))) && \{\text{Def. 3.6, Def. 3.5}\} \\
&= \mathsf{cons}(a, \mathbf{conc}(u', v)) && \{\text{IH}\} \\
&= \mathbf{conc}(\mathsf{cons}(a, u'), v) && \{\text{Def. 3.2}\}
\end{aligned}$$

**Övning 3.12.** (A) Bevisa genom att använda strukturell induktion att resultatdelen av **mconc** har den sammanlagda längden av båda argumenten, dvs att

$$\forall u\ \forall v\ \mathbf{length}(\mathbf{result}(\mathbf{mconc}(u, v))) = \mathbf{length}(u) + \mathbf{length}(v)$$

Låt $u$ vara en *List*-term. Vi gör induktion över strukturen för $u$.

- Fall $u = \mathsf{empty}$.

  Låt $v$ vara en *List*-term.

$$\begin{aligned}
&\mathbf{length}(\mathbf{result}(\mathbf{mconc}(\mathsf{empty}, v))) \\
&= \mathbf{length}(\mathbf{result}(\langle 0, v\rangle)) && \{\text{Def. 3.6}\} \\
&= \mathbf{length}(v) && \{\text{Def. 3.5}\} \\
&= 0 + \mathbf{length}(v) && \{\text{Aritmetik}\} \\
&= \mathbf{length}(\mathsf{empty}) + \mathbf{length}(v) && \{\text{Def. 3.1}\}
\end{aligned}$$

- Fall $u = \mathsf{cons}(a, u')$ för $a$ en *Letter*-term och $u'$ en *List*-term.

  Antag som induktionshypotes (IH) att $\forall v\ \mathbf{length}(\mathbf{result}(\mathbf{mconc}(u', v))) = \mathbf{length}(u') + \mathbf{length}(v)$, och låt $v$ vara en *List*-term.

$$\begin{aligned}
&\mathbf{length}(\mathbf{result}(\mathbf{mconc}(\mathsf{cons}(a, u'), v))) \\
&= \mathbf{length}(\mathsf{cons}(a, \mathbf{result}(\mathbf{mconc}(u', v)))) && \{\text{Def. 3.6, Def. 3.5}\} \\
&= 1 + \mathbf{length}(\mathbf{result}(\mathbf{mconc}(u', v))) && \{\text{Def. 3.1}\} \\
&= 1 + \mathbf{length}(u') + \mathbf{length}(v) && \{\text{IH}\} \\
&= \mathbf{length}(\mathsf{cons}(a, u')) + \mathsf{length}(v) && \{\text{Def. 3.1}\}
\end{aligned}$$

**Övning 3.13.** (C) Bevisa att kostnadsdelen av **mconc** är precis längden av det första argumentet, dvs att

$$\forall u\ \forall v\ \mathbf{cost}(\mathbf{mconc}(u, v)) = \mathbf{length}(u)$$

Låt $u$ vara en *List*-term. Vi gör induktion över strukturen för $u$.

- Fall $u = \mathsf{empty}$.

  Låt $v$ vara en *List*-term.

$$\begin{aligned} & \mathbf{cost}(\mathbf{mconc}(\mathsf{empty}, v)) & \\ & = \mathbf{cost}(\langle 0, v \rangle) & \{\text{Def. } 3.6\} \\ & = 0 & \{\text{Def. } 3.5\} \\ & = \mathbf{length}(\mathsf{empty}) & \{\text{Def. } 3.1\} \end{aligned}$$

- Fall $u = \mathsf{cons}(a, u')$ för $a$ en *Letter*-term och $u'$ en *List*-term.

  Antag som induktionshypotes (IH) att $\forall v\ \mathbf{cost}(\mathbf{mconc}(u', v)) = \mathbf{length}(u')$, och låt $v$ vara en *List*-term.

$$\begin{aligned} & \mathbf{cost}(\mathbf{mconc}(\mathsf{cons}(a, u'), v)) & \\ & = 1 + \mathbf{cost}(\mathbf{mconc}(u', v)) & \{\text{Def. } 3.6,\ \text{Def. } 3.5\} \\ & = 1 + \mathbf{length}(u') & \{\text{IH}\} \\ & = \mathbf{length}(\mathsf{cons}(a, u')) & \{\text{Def. } 3.1\} \end{aligned}$$

Betrakta nu en mätbar variant av funktionen **reverse**.

**Definition 3.7.**

$$\begin{aligned} \mathbf{mreverse}(\mathsf{empty}) & \stackrel{\text{def}}{=} \langle 0, \mathsf{empty} \rangle \\ \mathbf{mreverse}(\mathsf{cons}(a, u')) & \stackrel{\text{def}}{=} \mathbf{let}\ rr = \mathbf{mreverse}(u')\ \mathbf{in} \\ & \quad\ \ \mathbf{let}\ rc = \mathbf{mconc}(\mathbf{result}(rr), \mathsf{cons}(a, \mathsf{empty}))\ \mathbf{in} \\ & \quad\ \ \langle 1 + \mathbf{cost}(rc) + \mathbf{cost}(rr), \mathbf{result}(rc) \rangle \end{aligned}$$

**Övning 3.14.** (C) Bevisa genom att använda strukturell induktion och resultatet från övning 3.11 att **reverse** och resultatdelen av **mreverse** sammanfaller för alla listor, dvs att

$$\forall u\ \mathbf{result}(\mathbf{mreverse}(u)) = \mathbf{reverse}(u)$$

Låt $u$ vara en *List*-term. Vi gör induktion över strukturen för $u$.

- Fall $u = \mathsf{empty}$.

$$\begin{aligned} & \mathbf{result}(\mathbf{mreverse}(\mathsf{empty})) & \\ & = \mathbf{result}(\langle 0, \mathsf{empty} \rangle) & \{\text{Def. } 3.7\} \\ & = \mathsf{empty} & \{\text{Def. } 3.5\} \\ & = \mathbf{reverse}(\mathsf{empty}) & \{\text{Def. } 3.3\} \end{aligned}$$

- Fall $u = \mathsf{cons}(a, u')$ för $a$ en *Letter*-term och $u'$ en *List*-term.

  Antag som induktionshypotes (IH) att $\mathbf{result}(\mathbf{mreverse}(u')) = \mathbf{reverse}(u')$.

$$
\begin{aligned}
&\mathbf{result}(\mathbf{mreverse}(\mathsf{cons}(a, u'))) \\
&= \mathbf{result}(\mathbf{mconc}(\mathbf{result}(\mathbf{mreverse}(u')), \mathsf{cons}(a, \mathsf{empty}))) && \{\text{Def. 3.6}\} \\
&= \mathbf{conc}(\mathbf{result}(\mathbf{mreverse}(u')), \mathsf{cons}(a, \mathsf{empty})) && \{\text{Övn. 3.11}\} \\
&= \mathbf{conc}(\mathbf{reverse}(u'), \mathsf{cons}(a, \mathsf{empty})) && \{\text{IH}\} \\
&= \mathbf{reverse}(\mathsf{cons}(a, u')) && \{\text{Def. 3.3}\}
\end{aligned}
$$

**Övning 3.15.** (A) Bevisa genom att använda strukturell induktion och resultatet från övning 3.12 att resultatdelen av **mreverse** är längden av argumentet, dvs att

$$\forall u\ \mathbf{length}(\mathbf{result}(\mathbf{mreverse}(u))) = \mathbf{length}(u)$$

Låt $u$ vara en *List*-term. Vi gör induktion över strukturen för $u$.

- Fall $u = \mathsf{empty}$.

$$
\begin{aligned}
&\mathbf{length}(\mathbf{result}(\mathbf{mreverse}(\mathsf{empty}))) \\
&= \mathbf{length}(\mathbf{result}(\langle 0, \mathsf{empty}\rangle)) && \{\text{Def. 3.7}\} \\
&= \mathbf{length}(\mathsf{empty}) && \{\text{Def. 3.5}\}
\end{aligned}
$$

- Fall $u = \mathsf{cons}(a, u')$ för $a$ en *Letter*-term och $u'$ en *List*-term.

  Antag som induktionshypotes (IH) att $\mathbf{length}(\mathbf{result}(\mathbf{mreverse}(u'))) = \mathbf{length}(u')$.

$$
\begin{aligned}
&\mathbf{length}(\mathbf{result}(\mathbf{mreverse}(\mathsf{cons}(a, u')))) \\
&= \mathbf{length}(\mathbf{result}(\mathbf{mconc}(\mathbf{result}(\mathbf{mreverse}(u')), \mathsf{cons}(a, \mathsf{empty})))) && \{\text{Def. 3.7}\} \\
&= \mathbf{length}(\mathbf{result}(\mathbf{mreverse}(u'))) + \mathbf{length}(\mathsf{cons}(a, \mathsf{empty})) && \{\text{Övn. 3.12}\} \\
&= 1 + \mathbf{length}(\mathbf{result}(\mathbf{mreverse}(u'))) && \{\text{Aritmetik}\} \\
&= 1 + \mathbf{length}(u') && \{\text{IH}\} \\
&= \mathbf{length}(\mathsf{cons}(a, u')) && \{\text{Def. 3.1}\}
\end{aligned}
$$

**Övning 3.16.** (A) Bevisa genom att använda strukturell induktion och resultaten från övning 3.13 och 3.15 att dubbla kostnadsdelen av **mreverse** är lika med kvadraten av argumentets längd plus argumentets längd, dvs att

$$\forall u\ 2 \times \mathbf{cost}(\mathbf{mreverse}(u)) = \mathbf{length}(u) \times \mathbf{length}(u) + \mathbf{length}(u)$$

Låt $u$ vara en *List*-term. Vi gör induktion över strukturen för $u$.

- Fall $u = \mathsf{empty}$.

$$
\begin{aligned}
&2 \times \mathbf{cost}(\mathbf{mreverse}(\mathsf{empty})) \\
&= 2 \times \mathbf{cost}(\langle 0, \mathsf{empty} \rangle) && \{\text{Def. 3.7}\} \\
&= 0 && \{\text{Def. 3.5}\} \\
&= 0 \times 0 + 0 && \{\text{Aritmetik}\} \\
&= \mathbf{length}(\mathsf{empty}) \times \mathbf{length}(\mathsf{empty}) + \mathbf{length}(\mathsf{empty}) && \{\text{Def. 3.1}\}
\end{aligned}
$$

- Fall $u = \mathsf{cons}(a, u')$ för $a$ en *Letter*-term och $u'$ en *List*-term.

  Antag som induktionshypotes (IH) att $2 \times \mathbf{cost}(\mathbf{mreverse}(u')) = \mathbf{length}(u') \times \mathbf{length}(u') + \mathbf{length}(u')$.

$$
\begin{aligned}
&2 \times \mathbf{cost}(\mathbf{mreverse}(\mathsf{cons}(a, u'))) \\
&= 2 \times (1 + \mathbf{length}(\mathbf{result}(\mathbf{mreverse}(u'))) + \mathbf{cost}(\mathbf{mreverse}(u'))) && \{\text{Def. 3.7, Övn. 3.13}\} \\
&= 2 \times (1 + \mathbf{length}(u') \; + \mathbf{cost}(\mathbf{mreverse}(u'))) && \{\text{Övn. 3.15}\} \\
&= 2 \times (1 + \mathbf{length}(u')) + 2 \times \mathbf{cost}(\mathbf{mreverse}(u')) && \{\text{Aritmetik}\} \\
&= 2 \times (1 + \mathbf{length}(u')) + \mathbf{length}(u') \times \mathbf{length}(u') + \mathbf{length}(u') && \{\text{IH}\} \\
&= (1 + \mathbf{length}(u')) \times (1 + \mathbf{length}(u')) + (1 + \mathbf{length}(u')) && \{\text{Aritmetik}\} \\
&= \mathbf{length}(\mathsf{cons}(a, u')) \times \mathbf{length}(\mathsf{cons}(a, u')) + \mathbf{length}(\mathsf{cons}(a, u')) && \{\text{Def. 3.7}\}
\end{aligned}
$$

Betrakta nu mätbara varianter av funktionerna **rev** och **reverse′**.

**Definition 3.8.**

$$
\begin{aligned}
\mathbf{mrev}(\mathsf{empty}, v) &\stackrel{\text{def}}{=} \langle 0, v \rangle \\
\mathbf{mrev}(\mathsf{cons}(a, u')) &\stackrel{\text{def}}{=} \mathbf{let}\ r = \mathbf{mrev}(u', \mathsf{cons}(a, v))\ \mathbf{in} \\
&\quad\ \langle 1 + \mathbf{cost}(r), \mathbf{result}(r) \rangle \\
\mathbf{mreverse}'(u) &\stackrel{\text{def}}{=} \mathbf{mrev}(u, \mathsf{empty})
\end{aligned}
$$

**Övning 3.17.** (C) Bevisa genom att använda strukturell induktion att resultatet av **rev** och resultatdelen av **mrev** sammanfaller för alla listor, dvs att

$$\forall u\ \forall v\ \mathbf{result}(\mathbf{mrev}(u, v)) = \mathbf{rev}(u, v)$$

Låt $u$ vara en *List*-term. Vi gör induktion över strukturen för $u$.

- Fall $u = \mathsf{empty}$.

  Låt $v$ vara en *List*-term.

$$
\begin{aligned}
&\mathbf{result}(\mathbf{mrev}(\mathsf{empty}, v)) \\
&= \mathbf{result}(\langle 0, v \rangle) && \{\text{Def. 3.8}\} \\
&= v && \{\text{Def. 3.5}\} \\
&= \mathbf{rev}(\mathsf{empty}, v) && \{\text{Def. 3.4}\}
\end{aligned}
$$

- Fall $u = \mathsf{cons}(a, u')$ för $a$ en *Letter*-term och $u'$ en *List*-term.

  Antag som induktionshypotes (IH) att $\forall v\ \mathbf{result}(\mathbf{mrev}(u', v)) = \mathbf{rev}(u', v)$, och låt $v$ vara en *List*-term.

$$
\begin{aligned}
&\mathbf{result}(\mathbf{mrev}(\mathsf{cons}(a, u'), v)) && \\
&= \mathbf{result}(\mathbf{mrev}(u', \mathsf{cons}(a, v))) && \{\text{Def. 3.8}\} \\
&= \mathbf{rev}(u', \mathsf{cons}(a, v)) && \{\text{IH}\}
\end{aligned}
$$

**Övning 3.18.** (E) Bevisa genom att använda resultatet från övning 3.17 att $\mathbf{reverse}'$ och resultatdelen av $\mathbf{mreverse}'$ och sammanfaller för alla listor, dvs att

$$\forall u\ \mathbf{result}(\mathbf{mreverse}'(u)) = \mathbf{reverse}'(u)$$

Låt $u$ vara en *List*-term.

$$
\begin{aligned}
&\mathbf{result}(\mathbf{mreverse}'(u)) && \\
&= \mathbf{rev}(u, \mathsf{empty}) && \{\text{Övn. 3.17}\} \\
&= \mathbf{reverse}'(u) && \{\text{Def 3.4}\}
\end{aligned}
$$

**Övning 3.19.** (A) Bevisa genom att använda strukturell induktion att kostnadsdelen av **mrev** är lika med första argumentets längd, dvs att

$$\forall u\ \forall v\ \mathbf{cost}(\mathbf{mrev}(u, v)) = \mathbf{length}(u)$$

Låt $u$ vara en *List*-term. Vi gör induktion över strukturen för $u$.

- Fall $u = \mathsf{empty}$.

  Låt $v$ vara en *List*-term.

$$
\begin{aligned}
&\mathbf{cost}(\mathbf{mrev}(\mathsf{empty}, v)) && \\
&= \mathbf{cost}(\langle 0, v \rangle) && \{\text{Def. 3.8}\} \\
&= 0 && \{\text{Def. 3.5}\} \\
&= \mathbf{length}(\mathsf{empty}) && \{\text{Def. 3.1}\}
\end{aligned}
$$

- Fall $u = \mathsf{cons}(a, u')$ för $a$ en *Letter*-term och $u'$ en *List*-term.

  Antag som induktionshypotes (IH) att $\forall v\ \mathbf{cost}(\mathbf{mrev}(u', v)) = \mathbf{length}(u')$, och låt $v$ vara en *List*-term.

$$
\begin{aligned}
&\mathbf{cost}(\mathbf{mrev}(\mathsf{cons}(a, u'), v) && \\
&= 1 + \mathbf{cost}(\mathbf{mrev}(u', \mathsf{cons}(a, v))) && \{\text{Def. 3.8, Def. 3.5}\} \\
&= 1 + \mathbf{length}(u') && \{\text{IH}\} \\
&= \mathbf{length}(\mathsf{cons}(a, u')) && \{\text{Def. 3.1}\}
\end{aligned}
$$

**Övning 3.20.** (E) Bevisa genom att använda resultatet från övning 3.19 att kostnadsdelen av **mreverse′** är lika med argumentets längd, dvs att

$$\forall u\ \mathbf{cost}(\mathbf{mreverse}'(u)) = \mathbf{length}(u)$$

Låt $u$ vara en *List*-term.

$$\begin{aligned}
&\mathbf{cost}(\mathbf{mreverse}'(u)) \\
&= \mathbf{cost}(\mathbf{mrev}(u, \mathsf{empty})) && \{\text{Def 3.8}\} \\
&= \mathbf{length}(u) && \{\text{Övn. 3.19}\}
\end{aligned}$$