

Σειρά Προβλημάτων 4 – Λύσεις

Άσκηση 1

Να αποδείξετε την ορθότητα των πιο κάτω προδιαγραφών.

(α) $\models_{\text{tot}} \{m, n \geq 0\} P \{x = m \wedge y = n\}$ όπου ο κώδικας του P δίνεται πιο κάτω.

```
x := 0;
y := 0;
while (x < m || y < n){
  if x < m
    x := x + 1;
  else
    y := y + 1;
}
```

(β) $\models_{\text{tot}} \{m \geq 0 \wedge n \geq 0\} P \{s = (m+r) \cdot n + 3\}$ όπου ο κώδικας του P δίνεται πιο κάτω.

```
i := 1;
s := 3;
while (i <= n){
  s := s + r;
  j := 1;
  while (j <= m)
    s := s + 1;
  j := j + 1;
  i := i + 1;
}
```

Λύση:

(α) Αμετάβλητη συνθήκη για το while: $x \leq m \vee y \leq n$
Μεταβλητή έκφραση για το while: $(m-x)+(n-y)$

$\{m, n \geq 0\}$

$\{(0 \leq m \wedge \forall 0 \leq n) \wedge 0 \leq m+n\}$

Συνεπαγωγή

$x := 0;$

$\{(x \leq m \wedge 0 \leq n) \wedge 0 \leq (m-x)+n\}$

Αξ. Ανάθεσης

$y := 0;$

$\{(x \leq m \wedge y \leq n) \wedge 0 \leq (m-x)+(n-y)\}$

Αξ. Ανάθεσης

$\text{while } (x < m \vee y < n) \{$

$\{(x \leq m \wedge y \leq n) \wedge 0 \leq (m-x)+(n-y) = E_0 \wedge (x < m \wedge y < n)\}$

Αμ. Συνθ.+Μετ. Εκφρ.+Φρουρός

$\{[x < m \rightarrow (x+1 \leq m \wedge y \leq n) \wedge (0 \leq (m-x-1)+(n-y) < E_0)] \wedge [x \geq m \rightarrow (x \leq m \wedge y+1 \leq n) \wedge (0 \leq (m-x)+(n-y-1) < E_0)]\}$

Συνεπαγωγή

$\text{if } x < m$

$\{(x+1 \leq m \wedge y \leq n) \wedge (0 \leq (m-x-1)+(n-y) < E_0)\}$

$x := x + 1;$

$\{(x \leq m \wedge y \leq n) \wedge (0 \leq (m-x)+(n-y) < E_0)\}$

Αξ. Ανάθεσης

else

$\{(x \leq m \wedge y+1 \leq n) \wedge (0 \leq (m-x)+(n-y-1) < E_0)\}$

$y := y + 1;$

$\{(x \leq m \wedge y \leq n) \wedge (0 \leq (m-x)+(n-y) < E_0)\}$

Αξ. Ανάθεσης

$\}$

$\{(x \leq m \wedge y \leq n) \wedge (x \geq m \wedge y \geq n)\}$

Κανόνας total-while

$\{x = m \wedge y = n\}$

Συνεπαγωγή

(β) Αμετάβλητη συνθήκη για το εσωτερικό while:

$$s = (m + r) \cdot (i - 1) + r + 3 + j - 1 \wedge j \leq m + 1 \wedge i + 1 \leq n + 1 \wedge 0 \leq n - i - 1 < E_0$$

Μεταβλητή συνθήκη για το εσωτερικό while: $m - j$

Αμετάβλητη συνθήκη για το εξωτερικό while $s = (m + r) \cdot (i - 1) + 3 \wedge i \leq n + 1 \wedge 0 \leq m$

Μεταβλητή συνθήκη για το εξωτερικό while: $n - i$

$\{m \geq 0 \wedge n \geq 0\}$

$\{3 = (m + r) \cdot 0 + 3 \wedge 1 \leq n + 1 \wedge 0 \leq m\}$

Συνεπαγωγή

$i := 1;$

$\{3 = (m + r) \cdot (i - 1) + 3 \wedge i \leq n + 1 \wedge 0 \leq m\}$

Αξ. ανάθεσης

$s := 3;$

$\{s = (m + r) \cdot (i - 1) + 3 \wedge i \leq n + 1 \wedge 0 \leq m\}$

Αξ. ανάθεσης

while ($i \leq n$) {

$\{s = (m + r) \cdot (i - 1) + 3 \wedge 0 \leq m \wedge i \leq n + 1 \wedge i \leq n \wedge 0 \leq n - i = E_0\}$

Φρ. + Αμ. Συνθ. + Μετ. Εκφρ.

$\{s + r = (m + r) \cdot (i - 1) + r + 3 \wedge 0 \leq m \wedge i + 1 \leq n + 1 \wedge 0 \leq n - i - 1 < E_0\}$

Συνεπαγωγή

$s := s + r;$

$\{s = (m + r) \cdot (i - 1) + r + 3 \wedge 1 \leq m + 1 \wedge i + 1 \leq n + 1 \wedge 0 \leq n - i - 1 < E_0\}$

Αξ. ανάθεσης

$j := 1;$

$\{s = (m + r) \cdot (i - 1) + r + 3 + j - 1 \wedge j \leq m + 1 \wedge 0 \leq m - j \wedge i + 1 \leq n + 1 \wedge 0 \leq n - i - 1 < E_0\}$

Αξ. Αν.

while ($j \leq m$) {

$\{s = (m + r) \cdot (i - 1) + r + 3 + j - 1 \wedge j \leq m + 1 \wedge 0 \leq m - j = F_0 \wedge i + 1 \leq n + 1 \wedge 0 \leq n - i - 1 < E_0 \wedge j \leq m\}$

Φρ. + Αμ. Συνθ. + Μετ. Εκφρ.

$\{s + 1 = (m + r) \cdot (i - 1) + r + 3 + j \wedge j + 1 \leq m + 1 \wedge 0 \leq m - j - 1 < F_0 \wedge i + 1 \leq n + 1 \wedge 0 \leq n - i - 1 < E_0\}$

Συνεπαγωγή

$s := s + 1;$

$\{s = (m + r) \cdot (i - 1) + r + 3 + j \wedge j + 1 \leq m + 1 \wedge 0 \leq m - j - 1 < F_0 \wedge i + 1 \leq n + 1 \wedge 0 \leq n - i - 1 < E_0\}$

Αξ. Ανάθεσης

$j := j + 1;$

$\{s = (m + r) \cdot (i - 1) + r + 3 + j - 1 \wedge j \leq m + 1 \wedge 0 \leq m - j < F_0 \wedge i + 1 \leq n + 1 \wedge 0 \leq n - i - 1 < E_0\}$

Αξ. Ανάθεσης

}

$\{s = (m + r) \cdot (i - 1) + r + 3 + j - 1 \wedge j \leq m + 1 \wedge i + 1 \leq n + 1 \wedge 0 \leq n - i - 1 < E_0 \wedge j > m\}$

Καν. tot-while

$\{s = (m + r) \cdot i + 3 \wedge i + 1 \leq n + 1 \wedge 0 \leq m \wedge 0 \leq n - i - 1 < E_0\}$

Συνεπαγωγή

$i := i + 1;$

$\{s = (m + r) \cdot (i - 1) + 3 \wedge i \leq n + 1 \wedge 0 \leq m \wedge 0 \leq n - i < E_0\}$

Αξ. Ανάθεσης

}

$\{s = (m + r) \cdot (i - 1) + 3 \wedge i \leq n + 1 \wedge i > n \wedge 0 \leq m\}$

Καν. tot-while

$\{s = (m + r) \cdot n + 3\}$

Συνεπαγωγή

Άσκηση 2

(α) Να αποδείξετε την ορθότητα της προδιαγραφής $\models_{\text{par}} \{n \geq 0\} C \{r = x^n\}$ όπου ο κώδικας του C δίνεται πιο κάτω.

```
r := 1; p := x; e := n;
while e > 0 {
  if (e mod 2) != 0
```

```

        r := r * p;
    else
        r := r;
        p := p * p;
        e := e div 2;
    }

```

(β) Να εξηγήσετε τις αλλαγές/προσθήκες που πρέπει να γίνουν στην απόδειξη από το μέρος (α) έτσι ώστε να αποδειχθεί η ολική ορθότητα της προδιαγραφής.

Λύση:

(α) Ακολουθεί η απόδειξη μερικής ορθότητας της προδιαγραφής. Χρησιμοποιούμε ως αμετάβλητη συνθήκη την

$$\eta = "r \cdot p^e = x^n \wedge e \geq 0"$$

$\{n \geq 0\}$

$\{x^n = x^n \wedge n \geq 0\}$

Συνεπαγωγή

$r := 1;$

$\{r \cdot x^n = x^n \wedge n \geq 0\}$

Αξ. Ανάθεσης

$p := x;$

$\{r \cdot p^n = x^n \wedge n \geq 0\}$

Αξ. Ανάθεσης

$e := n;$

$\{r \cdot p^e = x^n \wedge e \geq 0\}$

Αξ. Ανάθεσης

$\text{while } e > 0 \{$

$\{r \cdot p^e = x^n \wedge e \geq 0 \wedge e > 0\}$

Αμ. Συν. και Φρουρός

$\{[e \bmod 2 \neq 0 \rightarrow r \cdot p^{2 \cdot e \text{ div } 2 + 1} = x^n \wedge e \text{ div } 2 \geq 0]$

$\wedge [e \bmod 2 = 0 \rightarrow r \cdot p^{2 \cdot e \text{ div } 2} = x^n \wedge e \text{ div } 2 \geq 0]$

Συνεπαγωγή

$\text{if } (e \bmod 2) \neq 0$

$\{r \cdot p^{2 \cdot e \text{ div } 2} = x^n \wedge e \text{ div } 2 \geq 0\}$

$r := r * p;$

$\{r \cdot p^{2 \cdot e \text{ div } 2} = x^n \wedge e \text{ div } 2 \geq 0\}$

Αξ. Ανάθεσης

else

$\{r \cdot p^{2 \cdot e \text{ div } 2} = x^n \wedge e \text{ div } 2 \geq 0\}$

$r := r;$

$\{r \cdot p^{2 \cdot e \text{ div } 2} = x^n \wedge e \text{ div } 2 \geq 0\}$

Αξ. Ανάθεσης

$\{r \cdot p^{2 \cdot e \text{ div } 2} = x^n \wedge e \text{ div } 2 \geq 0\}$

Κανόνας if

$p := p * p;$

$\{r \cdot p^{e \text{ div } 2} = x^n \wedge e \text{ div } 2 \geq 0\}$

Αξ. Ανάθεσης

$e := e \text{ div } 2;$

$\{r \cdot p^e = x^n \wedge e \geq 0\}$

Αξ. Ανάθεσης

$\}$

$\{r \cdot p^e = x^n \wedge e \geq 0 \wedge e \leq 0\}$

Κανόνας while

$\{r = x^n\}$

Συνεπαγωγή

(β) Ακολουθεί η απόδειξη ολικής ορθότητας της προδιαγραφής. Ως μεταβλητή έκφραση χρησιμοποιείται η e .

$\{n \geq 0\}$	
$\{x^n = x^n \wedge n \geq 0\}$	Συνεπαγωγή
$r := 1;$	
$\{r \cdot x^n = x^n \wedge n \geq 0\}$	Αξ. Ανάθεσης
$p := x;$	
$\{r \cdot p^n = x^n \wedge n \geq 0\}$	Αξ. Ανάθεσης
$e := n;$	
$\{r \cdot p^e = x^n \wedge e \geq 0\}$	Αξ. Ανάθεσης
$\text{while } e > 0 \{$	
$\{r \cdot p^e = x^n \wedge e \geq 0 \wedge 0 \leq e = E_0\}$	Αμ. Συν., Μετ. Εκφρ. και Φρουρός
$[[e \bmod 2 \neq 0 \rightarrow r \cdot p^{2 \cdot e \div 2 + 1} = x^n \wedge 0 \leq e \div 2 < E_0]$	
$\wedge [e \bmod 2 = 0 \rightarrow r \cdot p^{2 \cdot e \div 2} = x^n \wedge 0 \leq e \div 2 < E_0]$	Συνεπαγωγή
$\text{if } (e \bmod 2) \neq 0$	
$\{r \cdot p \cdot p^{2 \cdot e \div 2} = x^n \wedge 0 \leq e \div 2 < E_0\}$	Προσυνθήκη if
$r := r * p;$	
$\{r \cdot p^{2 \cdot e \div 2} = x^n \wedge 0 \leq e \div 2 < E_0\}$	Αξ. Ανάθεσης
else	
$\{r \cdot p^{2 \cdot e \div 2} = x^n \wedge 0 \leq e \div 2 < E_0\}$	
$r := r;$	
$\{r \cdot p^{2 \cdot e \div 2} = x^n \wedge 0 \leq e \div 2 < E_0\}$	Αξ. Ανάθεσης
$\{r \cdot p^{2 \cdot e \div 2} = x^n \wedge 0 \leq e \div 2 < E_0\}$	Κανόνας if
$p := p * p;$	
$\{r \cdot p^{e \div 2} = x^n \wedge 0 \leq e \div 2 < E_0\}$	Αξ. Ανάθεσης
$e := e \div 2;$	
$\{r \cdot p^e = x^n \wedge 0 \leq e < E_0\}$	Αξ. Ανάθεσης
$\}$	
$\{r \cdot p^e = x^n \wedge e \geq 0 \wedge e \leq 0\}$	Καν. total-while
$\{r = x^n\}$	Συνεπαγωγή

Άσκηση 3

Θεωρήστε το μοντέλο Kripke $M=(W, R, L)$, όπου

$$W = \{r, s, t, u, v, w\}$$

$$R = \{(r, s), (s, s), (u, u), (u, v), (v, u), (w, v), (w, w), (w, t)\}, \text{ και}$$

$$L(r) = \{p, q\}, L(s) = \{p\}, L(u) = \{q\}, L(t) = \{\}, L(v) = \{p\} \text{ και } L(w) = \{p, q\}.$$

(α) Να παρουσιάσετε το μοντέλο M γραφικά.

(β) Για κάθε μια από τις πιο κάτω ιδιότητες να αποφασίσετε σε ποιους κόσμους του μοντέλου M ικανοποιείται.

i. $\Diamond \Box \perp$

ii. $\Box \Box q$

iii. $\Diamond \Box q$

iv. $\Diamond(q \vee \Box q)$

v. $\Diamond^n(q \vee \Box q)$, όπου το $\Diamond^n$ συμβολίζει η εφαρμογές του τελεστή $\Diamond$, $n \geq 0$

(γ) Να δώσετε μια εναλλακτική απονομή ατομικών προτάσεων στους κόμβους του μοντέλου M (συνάρτηση L) έτσι ώστε να ικανοποιούνται ταυτόχρονα όλες οι πιο κάτω ιδιότητες

i. $w \models \Diamond \Box p \rightarrow \Box p$

ii. $r \models \neg p \rightarrow \Diamond \Diamond q$

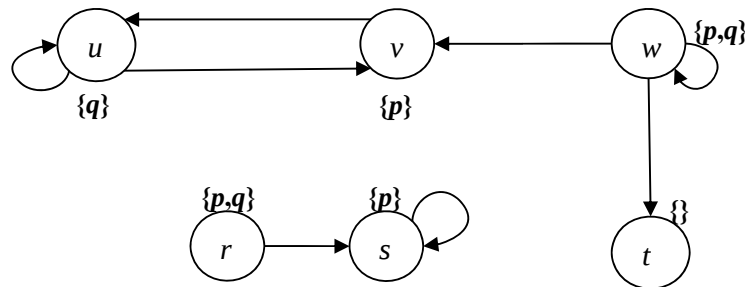
iii. $u \models \Box \Diamond \Box \neg q$

iv. $v \models p \rightarrow \Diamond p$

v. $s \models q \rightarrow \Box \neg q$

Λύση:

(α) Ακολουθεί το δοσμένο μοντέλο σε γραφική αναπαράσταση.



(β)

i. Η ιδιότητα $\Diamond \Box \perp$ με λόγια εκφράζει ότι «υπάρχει τουλάχιστον μια επόμενη κατάσταση κάθε επόμενης της οποίας ικανοποιεί το $\perp$ ». Αφού καμιά κατάσταση δεν ικανοποιεί το $\perp$ αυτό ισοδυναμεί με «υπάρχει τουλάχιστον μια επόμενη κατάσταση από την οποία δεν υπάρχει καμιά επόμενη». Επομένως, η μοναδική κατάσταση που ικανοποιεί την ιδιότητα είναι η w .

ii. Η ιδιότητα $\Box \Box q$ με λόγια εκφράζει ότι «από κάθε επόμενη κατάσταση κάθε επόμενη ικανοποιεί το q ». Αυτό ισοδυναμεί με «κάθε μεθεπόμενη κατάσταση ικανοποιεί το q ». Η μοναδική κατάσταση που ικανοποιεί την ιδιότητα είναι η t .

iii. Η ιδιότητα $\Diamond \Box q$ με λόγια εκφράζει ότι «υπάρχει επόμενη κατάσταση κάθε επόμενης της οποίας ικανοποιεί το q ». Οι καταστάσεις που ικανοποιούν την ιδιότητα είναι οι u , w .

iv. Η ιδιότητα $\Diamond(q \vee \Box q)$ με λόγια εκφράζει ότι «υπάρχει επόμενη κατάσταση που είτε ικανοποιεί το q είτε κάθε επόμενη της ικανοποιεί το q ». Οι καταστάσεις που ικανοποιούν την ιδιότητα είναι οι u , v και w .

v. Η ιδιότητα $\Diamond^n(q \vee \Box q)$, όπου το $\Diamond^n$ συμβολίζει η εφαρμογές του τελεστή $\Diamond$, $n \geq 0$, εκφράζει ότι «μετά από n βήματα υπάρχει κατάσταση που είτε ικανοποιεί το q είτε κάθε επόμενη της ικανοποιεί το q ». Παρατηρούμε ότι για $n = 0$ η ιδιότητα ικανοποιείται από τις καταστάσεις u , v , r , και w . Για $n = 1$ έχουμε την περίπτωση της ιδιότητας στο σκέλος iv. Για $n > 1$ η ιδιότητα ικανοποιείται από τις καταστάσεις u , v , και w .

(γ) Εναλλακτική απονομή ατομικών προτάσεων στους κόμβους του μοντέλου M (συνάρτηση L) έτσι ώστε να ικανοποιούνται ταυτόχρονα οι δοσμένες ιδιότητες είναι:

$$L(r) = \{p\}, L(s) = \{\}, L(u) = \{p\}, L(t) = \{p\}, L(v) = \{p\} \text{ και } L(w) = \{\}.$$

Άσκηση 4

Ποιες από τις πιο κάτω προτάσεις του βασικού τροπικού λογισμού είναι έγκυρες; Να αποδείξετε τις απαντήσεις σας.

- (α) $\Diamond \perp$
- (β) $\Diamond \top$
- (γ) $\Box p \rightarrow \Diamond p$
- (δ) $(\Box \phi \wedge \Diamond \psi) \rightarrow \Diamond \phi$
- (ε) $(\Box(p \wedge q) \wedge \neg \Diamond p) \rightarrow \Box \neg q$

Λύση:

(α) Η πρόταση $\Diamond \perp$ δεν είναι έγκυρη. Αντιπαράδειγμα της μη εγκυρότητας αποτελεί οποιοδήποτε μοντέλο και με κατάσταση την οποία διαδέχεται κάποια επόμενη.

(β) Η πρόταση $\Diamond \perp$ δεν είναι έγκυρη. Αντιπαράδειγμα της μη εγκυρότητας αποτελεί οποιοδήποτε μοντέλο και με κατάσταση την οποία δεν διαδέχεται κάποια επόμενη.

(γ) Η πρόταση $\Box p \rightarrow \Diamond p$ δεν είναι έγκυρη. Αντιπαράδειγμα της μη εγκυρότητας αποτελεί οποιοδήποτε μοντέλο και με κατάσταση την οποία δεν διαδέχεται κάποια επόμενη.

(δ) Η πρόταση είναι έγκυρη. Η απόδειξη έχει ως εξής:

Έστω κόσμος w σε κάποιο μοντέλο Kripke M . Τότε, έστω

$w \Vdash (\Box \phi \wedge \Diamond \psi)$	αν και μόνο αν	$w \Vdash \Box \phi$ και $w \Vdash \Diamond \psi$
	αν και μόνο αν	$x \Vdash \phi$ για κάθε x τέτοιο ώστε $(w,x) \in R$ και
		$u \Vdash \psi$ για κάποιο u τέτοιο ώστε $(w,u) \in R$
	συνεπάγεται	$u \Vdash \phi$ για κάποιο u τέτοιο ώστε $(w,u) \in R$
	συνεπάγεται	$w \Vdash \Diamond \phi$

Αυτό ολοκληρώνει την απόδειξη.

(ε) Η πρόταση είναι έγκυρη. Η απόδειξη έχει ως εξής:

Έστω κόσμος w σε κάποιο μοντέλο Kripke M . Τότε, έστω

$w \Vdash (\Box(p \wedge q) \wedge \neg \Diamond p)$	αν και μόνο αν	$w \Vdash \Box(p \wedge q)$ και $w \Vdash \neg \Diamond p$
	αν και μόνο αν	$x \Vdash p \wedge q$ για κάθε x τέτοιο ώστε $(w,x) \in R$
		και όχι υπάρχει u , $(w,u) \in R$, τέτοιο ώστε $u \Vdash p$
	συνεπάγεται	$x \Vdash p$ για κάθε x τέτοιο ώστε $(w,x) \in R$
		και όχι υπάρχει u , $(w,u) \in R$, τέτοιο ώστε $u \Vdash p$
	συνεπάγεται	όχι υπάρχει u τέτοιο ώστε $(w,u) \in R$
	συνεπάγεται	για κάθε u τέτοιο ώστε $(w,u) \in R$, $u \Vdash \neg q$
	συνεπάγεται	$w \Vdash \Box \neg q$

Αυτό ολοκληρώνει την απόδειξη.

Άσκηση 5

Να αποδείξετε τα πιο κάτω λογικά επακόλουθα του Τροπικού Λογισμού KT45.

- (α) $\vdash_K \Box(\phi \rightarrow \psi) \rightarrow (\Box \phi \rightarrow \Box \psi)$
- (β) $\Box(\phi \rightarrow \psi), \Diamond \phi \vdash_K \Diamond \psi$
- (γ) $\Box(\phi \vee \psi), \Box(\phi \rightarrow \chi), \Box(\psi \rightarrow \chi) \vdash_K \Box \chi$

Λύση:

(α)

1.	$\Box(\phi \rightarrow \psi)$	πρ. υπόθεση
2.	$\Box\phi$	πρ. υπόθεση
3.	$\phi \rightarrow \psi$	$\Box e 1$
4.	ϕ	$\Box e 2$
5.	ψ	MP 3, 4
6.	$\Box\psi$	$\Box i 3-5$
7.	$\Box\phi \rightarrow \Box\psi$	$\rightarrow i 3-6$

8. $\Box(\phi \rightarrow \psi) \rightarrow (\Box\phi \rightarrow \Box\psi) \quad \rightarrow i 1-7$

(β) Χρησιμοποιώντας τον ορισμό $\Diamond\phi = \neg\Box\neg\phi$, θα αποδείξουμε ότι $\Box(\phi \rightarrow \psi), \neg\Box\neg\phi \vdash_K \neg\Box\neg\psi$

1.	$\Box(\phi \rightarrow \psi)$	προϋπόθεση
2.	$\neg\Box\neg\phi$	προϋπόθεση
3.	$\Box\neg\psi$	πρ. υπ.
4.	$\neg\psi$	$\Box e 3$
5.	$\phi \rightarrow \psi$	$\Box e 1$
6.	$\neg\phi$	MT 5, 4
7.	$\Box\neg\phi$	$\Box i 4-6$
8.	$\perp$	$\neg e 2, 7$
9.	$\neg\Box\neg\psi$	RAA 3-8

(γ) $\Box(\phi \vee \psi), \Box(\phi \rightarrow \chi), \Box(\psi \rightarrow \chi) \vdash_K \Box\chi$

1.	$\Box(\phi \vee \psi)$	προϋπόθεση
2.	$\Box(\phi \rightarrow \chi)$	προϋπόθεση
3.	$\Box(\psi \rightarrow \chi)$	προϋπόθεση
4.	$\phi \vee \psi$	$\Box e 1$
5.	$\phi \rightarrow \chi$	$\Box e 2$
6.	$\psi \rightarrow \chi$	$\Box e 3$
7.	ϕ πρ. υπ.	ψ πρ. υπ.
8.	χ MP 5, 7	χ MP 6, 7
9.	χ	$\vee e 4, 7-8$
10.	$\Box\chi$	$\Box i 4-9$