

Γλώσσες Προγραμματισμού II

<http://courses.softlab.ntua.gr/p12/>

Κωστής Σαγώνας

`kostis@cs.ntua.gr`

Νίκος Παπασπύρου

`nickie@softlab.ntua.gr`



Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχ. και Μηχ. Υπολογιστών

Εργαστήριο Τεχνολογίας Λογισμικού

Πολυτεχνειούπολη, 15780 Ζωγράφου.

Αξιοματική σημασιολογία (i)

- Τεχνική ή λογική των Floyd και Hoare
- Απόδειξη ορθότητας προγραμμάτων
- Απλή **προστακτική** γλώσσα

```
C ::= skip
    | i := E
    | C0; C1
    | while B do C
    | if B then C0 else C1
```

Αξιωματική σημασιολογία (ii)

- Τριάδα Hoare (Hoare triple) ή προδιαγραφές

$$\{P\}C\{Q\}$$

- C πρόγραμμα
- P και Q λογικές εκφράσεις
(προσυνθήκη – μετασυνθήκη)
- στις P και Q μπορούν να εμφανίζονται οι μεταβλητές του C

Αξιωματική σημασιολογία (iii)

- $\{P\}C\{Q\}$ αληθής \Leftrightarrow αν το C εκτελείται σε μια αρχική κατάσταση που ικανοποιεί την P και η εκτέλεσή του τερματίζει, τότε στην τελική κατάσταση ικανοποιείται η Q

- Παραδείγματα

$$\{X=1\}X:=X+1\{X=2\}$$
$$\{X=x \wedge Y=y\}R:=X; X:=Y; Y:=R\{X=y \wedge Y=x\}$$

- Μερική ορθότητα (partial correctness): ο τερματισμός του προγράμματος δεν εξασφαλίζεται από τις προδιαγραφές

Αξιωματική σημασιολογία (iv)

- Παραδείγματα (συνέχεια)

- Αληθής προσυνθήκη

$$\{\text{true}\}C\{Q\}$$

αληθής \Leftrightarrow αν το πρόγραμμα C τερματίζει,
τότε ικανοποιείται η Q

- Αληθής μετασυνθήκη

$$\{P\}C\{\text{true}\}$$

αληθής πάντοτε

Αξιωματική σημασιολογία (v)

■ Παραδείγματα (συνέχεια)

- Ψευδής προσυνθήκη

$$\{\text{false}\}C\{Q\}$$

αληθής πάντοτε

- Ψευδής μετασυνθήκη

$$\{P\}C\{\text{false}\}$$

αληθής \Leftrightarrow αν η αρχική κατάσταση ικανοποιεί την P, τότε το πρόγραμμα C δεν τερματίζει

Αξιοματική σημασιολογία (vi)

- Αξίωμα του *skip*

$$\{P\} \text{skip} \{P\}$$

- Αξίωμα της *ανάθεσης*

$$\{P [E/V]\} V := E \{P\}$$

- Παραδείγματα

$$\begin{aligned} & \{42=42\} X := 42 \{X=42\} \\ & \{X+1=n+1\} X := X+1 \{X=n+1\} \end{aligned}$$

Αξιωματική σημασιολογία (vii)

- Κανόνας ενδυνάμωσης της προσυνθήκης

$$\frac{P \Rightarrow R \quad \{R\}C\{Q\}}{\{P\}C\{Q\}}$$

- Παράδειγμα

$$\frac{X=n \Rightarrow X+1=n+1 \quad \{X+1=n+1\}X:=X+1\{X=n+1\}}{\{X=n\}X:=X+1\{X=n+1\}}$$

Αξιοματική σημασιολογία (viii)

- Κανόνας αποδυνάμωσης της μετασυνθήκης

$$\frac{\{P\}C\{R\} \quad R \Rightarrow Q}{\{P\}C\{Q\}}$$

- Κανόνες σύζευξης και διάζευξης

$$\frac{\{P_1\}C\{Q_1\} \quad \{P_2\}C\{Q_2\}}{\{P_1 \wedge P_2\}C\{Q_1 \wedge Q_2\}}$$

$$\frac{\{P_1\}C\{Q_1\} \quad \{P_2\}C\{Q_2\}}{\{P_1 \vee P_2\}C\{Q_1 \vee Q_2\}}$$

Αξιωματική σημασιολογία (ix)

- Κανόνας σύνθετων εντολών

$$\frac{\{P\}C_1\{R\} \quad \{R\}C_2\{Q\}}{\{P\}C_1;C_2\{Q\}}$$

- Παράδειγμα

$$\{X=x \wedge Y=y\}R:=X\{R=x \wedge Y=y\}$$

$$\{R=x \wedge Y=y\}X:=Y\{R=x \wedge X=y\}$$

$$\{R=x \wedge X=y\}Y:=R\{Y=x \wedge X=y\}$$

$$\{X=x \wedge Y=y\}R:=X;X:=Y\{R=x \wedge X=y\}$$

$$\{X=x \wedge Y=y\}R:=X;X:=Y;Y:=R\{Y=x \wedge X=y\}$$

Αξιωματική σημασιολογία (X)

- Κανόνας του *if*

$$\frac{\{P \wedge S\} C_1 \{Q\} \quad \{P \wedge \neg S\} C_2 \{Q\}}{\{P\} \text{if } S \text{ then } C_1 \text{ else } C_2 \{Q\}}$$

- Παράδειγμα

$\{y > 1\} \text{if } x > 0 \text{ then } y := y - 1 \text{ else } y := y + 1 \{y > 0\}$

Αξιωματική σημασιολογία (xi)

- Κανόνας του **while**

$$\frac{\{P \wedge S\} C \{P\}}{\{P\} \text{while } S \text{ do } C \{P \wedge \neg S\}}$$

- Η συνθήκη P λέγεται **αναλλοίωτη** (invariant)
- Παράδειγμα

```
{n ≥ 0} p := 1; i := 2;  
while i ≤ n do (p := p * i; i := i + 1) {p = n!}
```