ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ	
ΕΑΡΙΝΟ ΕΞΑΜΗΝΟ 2025	**ΣΕΙΡΑ ΑΣΚΗΣΕΩΝ 2**

Αργυρώ Τσίπη

031 19950

Άσκηση 1

1. $\neg((a \Rightarrow (b \Rightarrow \neg a \lor c)) \Leftrightarrow \neg((c \lor d) \land b))$

Αρχικά θα εφαρμόσω για την συνεπαγωγή τον κανόνα $(p \Rightarrow q) = (\neg p \lor q)$:

- $(b \Rightarrow \neg a \lor c) = (\neg b \lor \neg a \lor c)$
- $(a \Rightarrow \neg b \lor \neg a \lor c) = \neg a \lor \neg b \lor \neg a \lor c = \neg a \lor \neg b \lor c$

Άρα έχουμε ως τώρα:
$\neg((\neg a \lor \neg b \lor c) \Leftrightarrow \neg((c \lor d) \land b))$

Θα εξαλείψουμε και τη διπλή συνεπαγωγή με τον κανόνα $p \Leftrightarrow q = (p \land q) \lor (\neg p \land \neg q)$:
- $(\neg a \lor \neg b \lor c) \Leftrightarrow \neg((c \lor d) \land b) = ((\neg a \lor \neg b \lor c) \land \neg((c \lor d) \land b) \lor (\neg(\neg a \lor \neg b \lor c) \land ((c \lor d) \land b))$

Θα βάλουμε και το αρχικό ¬ μέσα:

$\neg (((\neg a \lor \neg b \lor c) \land \neg((c \lor d) \land b)) \lor (\neg(\neg a \lor \neg b \lor c) \land ((c \lor d) \land b))) =$
$(\neg(\neg a \lor \neg b \lor c) \lor ((c \lor d) \land b)) \land ((\neg a \lor \neg b \lor c) \lor \neg((c \lor d) \land b)) =$

$((a \land b \land \neg c) \lor ((c \lor d) \land b)) \land ((\neg a \lor \neg b \lor c) \lor ((\neg c \land \neg d) \lor \neg b))$

$((a \land b \land \neg c) \lor ((c \lor d) \land b)) \land ((\neg a \lor \neg b \lor c) \land ((\neg c \land \neg d) \lor \neg b))$

Για το 1ο μέλος, θα χρησιμοποιήσω τη σχέση $(X \land Y) \lor Z = (X \lor Z) \land (Y \lor Z)$:
- $(a \land b \land \neg c) \lor ((c \lor d) \land b) = [a \lor ((c \lor d) \land b)] \land [b \lor ((c \lor d) \land b)] \land [\neg c \lor ((c \lor d) \land b)] =$

$[a \lor (c \lor d)] \land [a \lor b] \land [b \lor (c \lor d)] \land [b \lor b] \land [\neg c \lor (c \lor d)] \land [\neg c \lor b] =$
$[a \lor c \lor d] \land [a \lor b] \land [b \lor c \lor d] \land [b] \land [\neg c \lor c \lor d] \land [\neg c \lor b]$

Για το 2ο μέλος, θα χρησιμοποιήσω την σχέση $X \lor (A \land B) = (X \lor A) \land (X \lor B)$:
- $(\neg a \lor \neg b \lor c) \lor ((\neg c \land \neg d) \lor \neg b) = (\neg a \lor \neg b \lor c) \lor ((\neg c \lor \neg b) \land (\neg d \lor \neg b)) =$

$[(\neg a \lor \neg b \lor c) \lor (\neg c \lor \neg b)] \land [(\neg a \lor \neg b \lor c) \lor (\neg d \lor \neg b)] =$
$[\neg a \lor \neg b \lor c \lor \neg c] \land [\neg a \lor \neg b \lor c \lor \neg d]$

Άρα, έχουμε τελική έκφραση:
$[a \lor c \lor d] \land [a \lor b] \land [b \lor c \lor d] \land [b] \land [\neg c \lor c \lor d] \land [\neg c \lor b] \land [\neg a \lor \neg b \lor c \lor \neg c] \land [\neg a \lor \neg b \lor c \lor \neg d]$

και μπορούμε να αφαιρέσουμε τις ταυτολογίες όπως c, not c:
$[a \lor c \lor d] \land [a \lor b] \land [b \lor c \lor d] \land [b] \land [d] \land [\neg c \lor b] \land [\neg a \lor \neg b] \land [\neg a \lor \neg b \lor c \lor \neg d]$

2. $\boldsymbol{\exists x.\forall y.(P (x, y) \lor (\neg\exists z.(\exists w.P (z, z) \lor Q(w)) \Rightarrow (\forall z.P (y, z) \land Q(z))))}$

Αρχικά, θα αντικαταστήσω τις συνεπαγωγές με τον κανόνα $(p \Rightarrow q) = (\neg p \lor q)$:
$\boldsymbol{\exists x.\forall y.(P (x, y) \lor [\neg\neg\exists z.(\exists w.P (z, z) \lor Q(w)) \lor (\forall z.P (y, z) \land Q(z))])}$

Απλοποιώ τη διπλή άρνηση και δίνω ξεχωριστά ονόματα στις μεταβλητές:
$\boldsymbol{\exists x.\forall y.(P (x, y) \lor [\exists z1.(\exists w.P (z1, z1) \lor Q(w)) \lor \forall z2.(P (y, z2) \land Q(z2))])}$

Φέρνω όλους τους τελεστές μπροστά:
$\boldsymbol{\exists x.\forall y.\exists z1.\exists w.\forall z2. (P (x, y) \lor [(P (z1, z1) \lor Q(w)) \lor (P (y, z2) \land Q(z2))])}$

$\exists x.\forall y.\exists z1.\exists w.\forall z2.\ (P(x, y) \vee P(z1, z1) \vee Q(w) \vee (P(y, z2) \wedge Q(z2)))$

Κάνω skolemization:

$\exists x.\forall y.\exists z1.\exists w.\forall z2.\ (P(x, y) \vee P(z1, z1) \vee Q(w) \vee (P(y, z2) \wedge Q(z2)))$

$\forall y.\forall z2.\ (P(a, y) \vee P(f1(y), f1(y)) \vee Q(f2(y)) \vee (P(y, z2) \wedge Q(z2)))$

Θα εφαρμόσουμε την ιδιότητα $A\vee(B\wedge C)\equiv(A\vee B)\wedge(A\vee C)$:

$\forall y.\forall z2.\ [\ P(a, y) \vee P(f1(y), f1(y)) \vee Q(f2(y)) \vee P(y, z2)\ ] \wedge [\ P(a, y) \vee P(f1(y), f1(y)) \vee Q(f2(y)) \vee Q(z2)\ ]$

<u>Άσκηση 2</u>

1.

Ανακλαστική reflexive

Για κάθε στοιχείο ισχύει η σχέση με τον εαυτό του

$\forall x P(x,x)$

Μη ανακλστική non-reflexive

Υπάρχει τουλάχιστον ένα στοιχείο που δε σχετίζεται με τον εαυτό του

$\exists x\ \neg P(x,x)$

Αντιανακλαστική irreflexive

Κανένα στοιχείο δεν σχετίζεται με τον εαυτό του

$\forall x\ \neg P(x,x)$

Συμμετρική symmetric

Αν ένα στοιχείο σχετίζεται με ένα άλλο, τότε και το δεύτερο σχετίζεται με το πρώτο

$\forall x\ \forall y(P(x,y) \to P(y,x))$

Μη συμμετρική non symmetric

Υπάρχει ένα ζεύγος στοιχείων τέτοιο ώστε η σχέση ισχύει από το ένα προς το άλλο και όχι αντίστροφα

$\exists x\ \exists y(\ P(x,y) \wedge \neg P(y,x))$

Αντισυμμετρική antisymmetric

Αν δυο στοιχεία σχετίζονται και αμφίδρομα, τότε είναι το ίδιο στοιχείο

$\forall x\ \forall y(P(x,y) \wedge P(y,x) \to x=y)$

Ασύμμετρη asymmetric

Αν το ένα σχετίζεται με το άλλο, τότε το αντίστροφο δεν ισχύει

$\forall x\ \forall y(P(x,y) \to \neg P(y,x))$

Μεταβατική transitive

Αν το ένα σχετίζεται με ένα δεύτερο και το δεύτερο με ένα τρίτο τότε σχετίζεται και το πρώτο με το τρίτο

$\forall x\ \forall y\ \forall z\ ((P(x,y)\wedge P(y,z)) \to P(x,z))$

2.

Ανακλαστική (Reflexive):

Σύνολο: $A=\{1,2,3\}$

Σχέση: $P=\{(1,1),(2,2),(3,3),(1,2),(2,1)\}$

Κάθε στοιχείο σχετίζεται με τον εαυτό του.

Μη Ανακλαστική (Non-reflexive):

Σύνολο: $A=\{1,2,3\}$

Σχέση: $P=\{(1,1),(2,3)\}$
Το 2 και το 3 δεν σχετίζονται με τον εαυτό τους ⇒ δεν είναι πλήρως ανακλαστική.

Αντιανακλαστική (Irreflexive):
Σύνολο: $A=\{1,2,3\}$
Σχέση: $P=\{(1,2),(2,3)\}$
Κανένα (x,x) δεν ανήκει στη σχέση.

Συμμετρική (Symmetric):
Σύνολο: $A=\{a,b\}$
Σχέση: $P=\{(a,b),(b,a)\}$
Αν a σχετίζεται με b, τότε και b με a.

Μη Συμμετρική (Non-symmetric):
Σύνολο: $A=\{1,2\}$
Σχέση: $P=\{(1,2)\}$
(1,2) ανηκει P, αλλά (2,1) δεν ανηκει P

Αντισυμμετρική (Antisymmetric):
Σύνολο: $A=\{1,2,3\}$
Σχέση: $P=\{(1,1),(2,2),(3,3),(1,2)\}$
Δεν υπάρχουν διαφορετικά $x \neq y$ με $(x,y)\in P$ και $(y,x)\in P$

Ασύμμετρη (Asymmetric):
Σύνολο: $A=\{a,b,c\}$
Σχέση: $P=\{(a,b),(b,c)\}$
Για κάθε $(x,y)\in P$, δεν υπάρχει (y,x)

Μεταβατική (Transitive):
Σύνολο: $A=\{1,2,3\}$
Σχέση: $P=\{(1,2),(2,3),(1,3)\}$
Εφόσον (1,2) και(2,3) υπάρχουν, πρέπει να υπάρχει και (1,3)

3.
Ιδιότητες Σχέσης Ισοδυναμίας:
Μια σχέση P P είναι σχέση ισοδυναμίας αν ικανοποιεί:

Ανακλαστικότητα: $\forall x\ P(x,x)$
Συμμετρία: $\forall x,y,\ P(x,y)\rightarrow P(y,x)$
Μεταβατικότητα: $\forall x,y,z,\ (P(x,y)\wedge P(y,z))\rightarrow P(x,z)$

Ιδιότητες Σχέσης Ολικής Διάταξης:
Μια σχέση P είναι ολική διάταξη αν ικανοποιεί:
Αντισυμμετρία: $\forall x,y,\ (P(x,y)\wedge P(y,x))\rightarrow x=y$
Μεταβατικότητα: $\forall x,y,z,\ (P(x,y)\wedge P(y,z))\rightarrow P(x,z)$
Ολικότητα (Συγκρισιμότητα): $\forall x,y,\ P(x,y)\vee P(y,x)$

Σύγκρουση Ιδιοτήτων:
Η σχέση ισοδυναμίας είναι συμμετρική, ενώ η ολική διάταξη είναι αντισυμμετρική.
Η συμμετρία επιτρέπει: $x\sim y\Rightarrow y\sim x$, ακόμα κι αν $x \neq y$
Η αντισυμμετρία λέει: Αν $x \leq y$ και $y \leq x$, τότε πρέπει να είναι $x=y$

Άρα δεν μπορούν να ισχύουν και οι δύο ταυτόχρονα

Εξαίρεση το Τριβιακό Μοντέλο:
Αν το σύνολο έχει μόνο ένα στοιχείο Α={a}, τότε:
Η σχέση P={(a,a)} είναι ταυτόχρονα:
Ανακλαστική, συμμετρική, μεταβατική. Άρα ισοδυναμία.
Και αντισυμμετρική, ολική (καθώς δεν υπάρχουν δύο διαφορετικά στοιχεία για να παραβιαστεί η συγκρισιμότητα). Άρα ολική διάταξη.

4.
Υπόθεση: μπορεί να υπάρχει σύνολο Α με 2 στοιχεία α<>β (διαφορετικά μεταξύ τους) τέτοιο ώστε μια σχέση P να είναι και ισοδυναμία και ολική διάταξη.
Από συμμετρία έχουμε ότι αν P(α.β) τότε και P(β,α)
Από αντισυμμετρία έχουμε ότι αν P(α,β) και P(β,α) τότε πρέπει α=β
άτοπο, αφού ορίσαμε α<>β.
Άρα δεν υπάρχει σύνολο Α με 2 στοιχεία α<>β: P ισοδυναμία και ολική διάταξη.

<u>Άσκηση 3</u>
1.
Αρχικά, ορίζουμε το κατηγόρημα G(x), που δηλώνει ότι το στοιχείο χ ανήκει στο σύνολο G και μια συνάρτηση f(x,y) που δείχνει την πράξη x.y
Για να ορίσουμε την ομάδα:

Κλειστότητα:
αν x ανήκει G και y ανήκει G, τότε f(x,y) ανήκει G.
∀x ∀y(G(x) Λ G(y) -> G(f(x,y)))

Προσεταιριστικότητα:
Για κάθε x,y,z που ανήκουν στο G, ισχύει f(x,f(y,z)) = f(f(x,y),z).
∀x∀y∀z (G(x) Λ G(y) Λ G(z) -> f(x,f(y,z)) = f(f(x,y),z))

Ουδέτερο στοιχείο
Υπάρχει e ανήκει G, τέτοιο ώστε για κάθε x ανήκει G, f(e,x) = x & F(x,e) = x.
G(e) Λ ∀x(G(x) -> (f(e,x) = x Λ f(x,e) = x)).

Αντίστροφο στοιχείο
Για κάθε x ανήκει G, υπάρχει y: f(x,y) = e και f(y,x) = e.
∀x(G(x) - > ∃y(G(y) Λ f(x,y) = e Λ f(y,x) = e))

2.
Εάν υπάρχουν δύο στοιχεία e1 kai e2 στο G τέτοια ώστε και τα δύο να είναι ουδέτερα τότε πρεέπει να ισχύει ότι είναι ίσα.

Υπόθεση και τα δύο στοιχεία είναι ουδέτερα
G(e1) Λ ∀x(G(x) -> (f(e1,x) = x Λ f(x,e1) = x))
G(e2) Λ ∀x(G(x) -> (f(e2,x) = x Λ f(x,e2) = x))

Αφου e1 ουδέτερο: f(e1,e2)=e2
Αφου e2 ουδέτερο: f(e1,e2)=e1
άρα f(e1,e2)=e1=e2

3.
Εις άτοπον απαγωγή
Υπόθεση: έστω ότι e1, e2 neutral & e1 <> e2

Ορίζουμε neautral= G(x) Λ ∀a(G(a) -> (f(x,a) = a Λ f(a,x) = a))
Αφου e1 ουδέτερο: f(e1,e2)=e2
Αφου e2 ουδέτερο: f(e1,e2)=e1

f(e1,e2)= e1 Λ f(e1,e2)= e2 => e1=e2

(1)	f(e1 ,e2)=e2 (από neutral του e1)
(2)	f(e1 ,e2)=e1 (από neutral του ε2)
(3)	e1 =e2 ≡¬(e1 =e2)
(4)	**Reflexivity**: x=x
(5)	**Symmetry**: x=y→y=x≡¬(x=y)∨y=x
(6)	**Transitivity**: x=y∧y=z→x=z≡¬(x=y)∨¬(y=z)∨x=z

Από (1),(2): f(e1,e2)= e1 Λ f(e1,e2)= e2 => e1=e2 (7)
Από (3): ¬(e1 =e2)
από (7),(3): e1=e2 Λ ¬(e1 =e2) => ⊥
αντίφαση άρα η υπόθεσή μας είναι άτοπη. Άρα e1=e2.

4.
Ορισμοι

Ουδέτερο στοιχείο:
neutral(E) :- forall(A, f(E, A, A)), forall(A, f(A, E, A)).

Ισότητα:
equal(X, X).
equal(X, Y) :- equal(Y, X). (Συμμετρία)
equal(X, Z) :- equal(X, Y), equal(Y, Z). (Μεταβατικότητα)

Base case
neutral(e1).
neutral(e2).

Στόχος για απόδειξη
:- not(equal(e1, e2)).

ΘΔΟ ?- neutral(e1), neutral(e2), not(equal(e1, e2)).
Υπόθεση equal(e1,e2) οδηγεί σε άτοπο.
Αφου e1 ουδέτερο: f(e1,e2)=e2
Αφου e2 ουδέτερο: f(e1,e2)=e1

equal(f(e1,e2),e1)∧equal(f(e1,e2),e2)⇒equal(e1,e2)
f(e1,e2),e1 σημαίνει ότι δίνει e1
f(e1,e2),e2 σημαίνει ότι δίνει e2
equal(e1,e2) = equal(e2,e1) = e1= e2

αντίφαση, άρα άτοπη υπόθεση. Άρα ε1=ε2.

5.
Αξιώματα Ομάδας:
Κλειστότητα: Για κάθε a, b ∈ G, ισχύει a · b ∈ G.
Συνδετικότητα: Για κάθε a, b, c ∈ G, ισχύει a · (b · c) = (a · b) · c.
Ουδέτερο στοιχείο: Υπάρχει e ∈ G τέτοιο ώστε για κάθε a ∈ G, ισχύει e · a = a και a · e = a.
Αντίστροφο στοιχείο: Για κάθε a ∈ G, υπάρχει a^{-1} ∈ G τέτοιο ώστε a · a^{-1} = e και a^{-1} · a = e.
Απόδειξη:
Έστω a, b ∈ G. Θέλουμε να βρούμε c ∈ G τέτοιο ώστε a · c = b.
Από το αξίωμα ύπαρξης αντίστροφου στοιχείου, υπάρχει a^{-1} ∈ G τέτοιο ώστε a^{-1} · a = e.
Θέτουμε c = a^{-1} · b, και ελέγχουμε:
a · c = a · (a^{-1} · b)
= (a · a^{-1}) · b (συνδετικότητα)
= e · b
= b (ουδετερότητα)
Άρα όντως υπάρχει στοιχείο c = a^{-1} · b ∈ G τέτοιο ώστε a · c = b.

6.
Αξιώματα Ομάδας:
Κλειστότητα: Για κάθε a, b ∈ G, ισχύει a · b ∈ G.
Συνδετικότητα: Για κάθε a, b, c ∈ G, ισχύει a · (b · c) = (a · b) · c.
Ουδέτερο στοιχείο: Υπάρχει e ∈ G τέτοιο ώστε για κάθε a ∈ G, ισχύει e · a = a και a · e = a.
Αντίστροφο στοιχείο: Για κάθε a ∈ G, υπάρχει a^{-1} ∈ G τέτοιο ώστε a · a^{-1} = e και a^{-1} · a = e.

Θέλουμε ∀a ∈G ∀b ∈G ∃c∈G f(a,c) = b
Έστω a,b∈G.
Από το αξίωμα αντιστροφου στοιχείου : υπάρχει α^-1 ανήκει G τέτοιο ώστε: f(a^-1, a) = e
Μέσω της συνδετικότητας έχω c = f(a^-1, b)
και υπολογίζω
f(a,c) = f(a,f(a^-1,b)) = f(f(a,a^-1),b) = f(e,b) = b

7.
ΘΔΟ: ∀a∀b(G(a)∧G(b)⇒∃c(G(c)∧f(a,c)=b))
σε prolog: ?- G(a), G(b), f(a, c) = b, G(c).

Από G(a) γνωρίζουμε ότι υπάρχει a^-1 με f(a,a^-1)=e
Ορίζουμε c = f(a^-1,b) και G(c)
Και υπολογίζουμε f(a,c) = f(a,f(a^-1,b)) = f(f(a,a^-1),b) = f(e,b) = b

Κώδικας σε prolog
% Ορισμός ουδέτερου στοιχείου
neutral(e).

% Κλειστότητα ομάδας: Αν a, b ∈ G τότε f(a,b) ∈ G
% όλα τα στοιχεία που αναφέρουμε είναι στο G.

```prolog
g(e).
g(a).
g(b).
g(c).
g(inv_a).

% Ουδέτερο στοιχείο
f(e, X, X) :- g(X).
f(X, e, X) :- g(X).

% Αντίστροφο στοιχείο: f(A, inv_A, e) και f(inv_A, A, e)
f(a, inv_a, e).
f(inv_a, a, e).

% Ορισμός πράξης f(A, B, C) σημαίνει C = A·B
f(inv_a, b, c) :- g(b), g(c).

% Εύρεση αντιστρόφου (πχ για a)
inverse(a, inv_a).
inverse(inv_a, a).

% βρες c
find_c(A, B, C) :-
   inverse(A, A_inv),
   f(A_inv, B, C),
   g(C),
   f(A, C, B).
```