Θέμα 1 (Διαδικασίες Απαρίθμησης, 2.0 μονάδες)

(α) Μια συνάρτηση $p : N \to N$ είναι πολυωνυμική βαθμού d όταν υπάρχουν φυσικοί $(a_d, a_{d-1}, ..., a_0)$ τέτοιοι ώστε $p(n) = \sum_{l=0}^{d} a_l n^l$, για κάθε $n \in N$.

Συμβολίζουμε με P_d το σύνολο των πολυωνυμικών συναρτήσεων βαθμού d στους φυσικούς και με $P = \bigcup_{d \in N} P_d$ το σύνολο των πολυωνυμικών συναρτήσεων. Να εξετάσετε αν τα σύνολα P_d και P είναι αριθμήσιμα.

Οι διαφορετικές τιμές που παίρνει κάθε a_i είναι αριθμήσιμα άπειρες. Τα a_i είναι $d+1$ στο πλήθος επομένως έχουμε αριθμήσιμα άπειρη ένωση πεπερασμένων συνόλων.
Εφόσσον οι πολυωνυμικές βαθμού $d+1$ είναι αριθμήσιμα άπειρες η ένωσή τους για $d = 1,2,...N$ είναι αριθμήσιμα άπειρη ένωση αριθμήσιμων συνόλων και επομένως το σύνολο όλων των πολυωνυμικών είναι αριθμήσιμα άπειρο.

(β) Χρησιμοποιώντας το (α), να δείξετε ότι υπάρχουν (άπειρες) συναρτήσεις $f : N \to N$ που δεν ανήκουν στο P, δηλ. που δεν μπορούν να εκφραστούν ως πολυωνυμικές συναρτήσεις.

Έστω F το σύνολο όλων των συναρτήσεων από το N στο $\{0,1\}$.
Το F δεν είναι αριθμήσιμο και αποδεικνύεται με διαγωνιοποίηση.

	0	1	2	3	4	5	6	…	*n*
f_0	0	0	1	1	0	1	0	…	0
f_1	1	1	1	0	0	1	1	…	1
…									
f_{n-1}	1	1	1	1	0	0	0	…	1
f_n	1	1	1	1	1	1	1	…	0

Πάντα μπορώ να φτιάξω μία νέα συνάρτηση πως έχει ως τιμές διαφορετικές τιμές από αυτές της διαγωνίου.
Διαισθητικά κάθε συνάρτηση από το σύνολο των φυσικών στο σύνολο με στοιχεία 0 και 1 αντιστοιχεί σε υποσύνολο του συνόλου των φυσικών.

(γ) Ο κωδκός πρόσβασης ενός υπερυπολογιστή είναι ένας φυσικός αριθμός που αλλάζει κάθε δευτερόλεπτο, για λόγους ασφαλείας. Η αλλαγή γίνεται με βάση μια πολυωνυμική συνάρτηση $p : N \to N$ βαθμού d και έναν (πολυψήφιο) πρώτο αριθμό q. Αν ο κωδικός τη χρονική στιγμή t είναι x_t, ο κωδικός την επόμενη χρονική στιγμή είναι $x_{t+1} = p(x_t) \bmod q$. Ο αρχικός κωδικός x_0, οι συντελεστές $(a_d, a_{d-1}, ..., a_0)$ της πολυωνυμικής συνάρτησης p, και ο πρώτος αριθμός q είναι γνωστά μόνο στον διαχειριστή του συστήματος. Γνωρίζετε όμως πόσα δευτερόλεπτα έχουν περάσει από το τελευταίο *reset* και έχετε εντοπίσει ένα κρίσιμο κενό ασφαλείας: αν δοκιμάζετε έναν κωδικό κάθε 30 ή περισσότερα δευτερόλεπτα, αυτό δεν πρόκειται ποτέ να προκαλέσει συναγερμό ή κλείδωμα του συστήματος (όσες φορές και αν αποτύχετε). Να διατυπώσετε μια αλγοριθμική μέθοδο που να παράγει κωδικούς συστηματικά και εγγυάται ότι θα αποκτήσετε πρόσβαση στον υπερυπολογιστή σε πεπερασμένο χρόνο. Να αποδείξετε την ορθότητα της μεθόδου.

Κάθε 30 secs "μαντεύω" τα $a_d, a_{d-1}, ..., a_0, x_0, q$ και υπολογίζω το x_t τη χρονική στιγμή t την οποία γνωρίζω.

$x_1 = p(x_0) \bmod q$

$x_2 = p(x_1) \bmod q$

...

$x_t = p(x_{t-1}) \bmod q$

Αν δεν βρω το passwd συνεχίζω "μαντεύοντας" το επόμενο σύνολο

$a_d, a_{d-1}, ..., a_0, x_0, q$.

Τα $a_d, a_{d-1}, ..., a_0, x_0, q$ παίνουν τιμές από το σύνολο των φυσικών και επομένως όλα τα διαφορετικά σύνολα που θα πάρω είναι αριθμήσιμα άπειρα.

Θέμα 2 (Διμελείς Σχέσεις, 2.0 μονάδες)

(α) Μία διμελής σχέση R είναι *κυκλική* αν για κάθε τριάδα στοιχείων x, y, z, $(x,y) \in R \wedge (y,z) \in R \Rightarrow (z,x) \in R.$ Να δείξετε ότι μια σχέση R είναι ανακλαστική και κυκλική αν και μόνο αν η R είναι σχέση ισοδυναμίας.

(β) Να σχεδιάσετε διάγραμμα Hasse ενός μερικώς διατεταγμένου συνόλου το οποίο έχει 3 minimal και 3 maximal στοιχεία, και κάθε στοιχείο του είναι είτε μεγαλύτερο είτε μικρότερο από (ακριβώς) δύο άλλα στοιχεία.

(γ) Ορίζουμε μία σχέση R στο σύνολο των θετικών φυσικών ως εξής: Για κάθε $m,n \in N_+, (n,m) \in R$ αν και μόνο αν κάθε πρώτος παράγοντας του n είναι και πρώτος παράγοντας του m. Είναι η R σχέση μερικής διάταξης; Να αιτιολογήσετε κατάλληλα τον ισχυρισμό σας.

(δ) Θεωρούμε μια πρωτοβάθμια γλώσσα με ένα διμελές κατηγορηματικό σύμβολο P. Να διατυπώσετε μία πρόταση που να δηλώνει ότι (η διμελής σχέση με την οποία ερμηνεύουμε) το P είναι lattice.

(α) **κυκλική και ανακλαστική $\Rightarrow$ ισοδυναμίας**

$\forall a(a,a) \in R$, άρα για κάθε ζεύγος $(a,b) \in R \Rightarrow (b,a) \in R$ (εφαρμογή της κυκλικής ιδιότητας). Επομένως R συμμετρική.

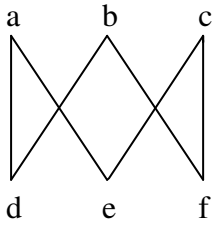
$\forall a,b,c((a,b) \in R \wedge (b,c) \in R \rightarrow (c,a) \in R)$ και επειδή R συμμετρική $(a,c) \in R$.

Επομένως R μεταβατική.

ισοδυναμίας $\Rightarrow$ κυκλική και ανακλαστική

Επειδή η R είναι μεταβατική για κάθε τριάδα $x, y, z,$ λόγω της μεταβατικής ιδιότητας ισχύει πως $(x,y) \in R \wedge (y,z) \in R \Rightarrow (x,z) \in R.$ Η R όμως είναι και συμμετρική επομένως $(z,x) \in R.$

(β)



(γ) Για να είναι σχέση μερικής διάταξης θα πρέπει να ισχύει η αντισυμμετρική ιδιότητα. Το 6 και το 12 έχουν τους ίδιους πρώτους παράγοντες και επομένως $(6,12) \in R$ και $(12,6) \in R$ αλλά το 6 δεν είναι ίσο με το 12.

(δ) Για να είναι lattice θα πρέπει για κάθε ζεύγος στοιχείων να υπάρχει μέγιστο κάτω φράγμα και ελάχιστο άνω φράγμα. Ορίζουμε αρχικά το μέγιστο κάτω φράγμα:

$SUP(x,y,z) = P(x,z) \wedge P(y,z) \wedge \forall w((P(x,w) \wedge P(y,w)) \rightarrow P(z,w))$

Ομοίως για το ελάχιστο άνω φράγμα:

$INF(x,y,z) = P(z,x) \wedge P(z,y) \wedge \forall w((P(w,x) \wedge P(w,y)) \rightarrow P(w,z))$

και η πρόταση που δηλώνει ότι το P είναι lattice

$\forall x \forall y(\exists z SUP(x,y,z) \wedge \exists w INF(x,y,w))$

Για λόγους πληρότητας θα έπρεπε να προσθέσουμε εδώ και τις ιδιότητες της μερικής διάταξης γιατί το lattice αναφέρεται σε σχέση μερικής διάταξης. Επομένως θέλουμε επιπλέον ανακλαστικότητα, αντισυμμετρικότητα και μεταβατικότητα.

$$\forall x P(x,x) \wedge \forall x \forall y ((P(x,y) \wedge P(y,x)) \rightarrow x = y) \wedge \forall x \forall y \forall z ((P(x,y) \wedge P(y,z)) \rightarrow P(x,z))$$

και συνολικά η πρόταση που δηλώνει πως το P είναι lattice είναι η ακόλουθη:

$$\forall x P(x,x) \wedge \forall x \forall y ((P(x,y) \wedge P(y,x)) \rightarrow x = y) \wedge \forall x \forall y \forall z ((P(x,y) \wedge P(y,z)) \rightarrow P(x,z))$$
$$\wedge \forall x \forall y (\exists z SUP(x,y,z) \wedge \exists w INF(x,y,w))$$

Θέμα 3 (Προτασιακή Λογική, 1.2 μονάδες)
(α)Επισκέπτεσθε ένα νησί όπου κατοικούν δύο είδη ανθρώπων, οι ευγενείς που λένε πάντα την αλήθεια, και οι απατεώνες που λένε πάντα ψέματα. (i)Πρώτα συναντάτε δύο κατοίκους του νησιού, τον Α και τον Β. Ο Α λέει ότι "Είμαστε και οι δύο ευγενείς". Ο Β λέει ότι "Ο Α είναι απατεώνας". Τι είναι οι Α και Β; (ii)Στη συνέχεια συναντάται τους C και D. Ο C λέει ότι "Ο D είναι απατεώνας", και ο D λεέι ότι "Ο C είναι απατεώνας". Πόσοι από τους C και D είναι απατεώνες; (iii)Λίγο παρακάτω συναντάτε τους Χ και Υ. Ρωτάτε τον Χ "Υπάρχει κάποιος ευγενής μεταξύ σας;" Αυτός αποκρίνεται, και η απάντησή του είναι τέτοια ώστε να μπορείτε να αποφανθείτε με σιγουριά για τους Χ και Υ. Τι απάντησε ο Χ, και τι είναι οι Χ και Υ;

(i) Ο Α δεν μπορεί να λέει αλήθεια γιατί τότε ο Β θα έλεγε αλήθεια και ο Α θα ήταν απατεώνας. Επομένως ο Α είναι απατεώνας. Κατά συνέπεια ο Β είναι ευγενής.
(ii) Αν ο C λέει αλήθεια τότε ο ίδιος είναι ευγενής και ο D απατεώνας. Διαφορετικά ο C είναι απατεώνας και ο D ευγενής. Άρα έχουμε έναν ευγενή και έναν απατεώνα.
(iii) Αν ο Χ απάντησε όχι τότε ο Χ είναι απατεώνας και άρα λέει ψέματα και κατά συνέπεια ο Υ είναι ευγενής. Αν ο Χ απάντησε ναι δεν μπορούμε να αποφανθούμε. Άρα ο Χ απάντησε όχι.

(β) Ένας ανακριτής προσπαθεί να ξεχωρίσει έναν κατάσκοπο μεταξύ τριών υπόπτων (ας τους ονομάσουμε Α, Β και Γ. Ο ανακριτής γνωρίζει πως ένας από τους τρεις είναι ευγενής (και λέει πάντα αλήθεια), ένας είναι απατεώνας (και λέει πάντα ψέματα) και ένας είναι κατάσκοπος (μπορεί να λέει είτε αλήθεια είτε ψέματα). Ο Α δήλωσε είτε ότι "Ο Γ είναι απατεώνας" είτε ότι "Ο Γ είναι κατάσκοπος". Εμείς δεν γνωρίζουμε τι από τα δύο δήλωσε ο Α, γιατί δεν ακούσαμε καλά, αλλά ο ανακριτής άκουσε και κατέγραψε τη δήλωσή του. Ο Β δήλωσε ότι "Είτε ο Α είναι κατάσκοπος είτε ο Α είναι απατεώνας είτε ο Α είναι ευγενής". Ο Γ δήλωσε ότι "Είτε ο Β είναι κατάσκοπος είτε ο Β είναι απατεώνας είτε ο Β είναι ευγενής". Ο ανακρτής συνέλαβε τον κατάσκοπο. Ποιός ήταν ο κατάσκοπος; Ποιά ήταν η δήλωση του Α;

Οι δηλώσεις των Β και Γ είναι αληθείς. Άρα ο ένας είναι ευγενής και ο άλλος είναι κατάσκοπος. Κατά συνέπεια ο Α είναι απατεώνας και επομένως είπε ψέματα. Αν ο Α δήλωσε πως ο Γ είναι απατεώνας ο Γ πρέπει να είναι ευγενής ή κατάσκοπος και δεν μπορεί με αυτή τη δήλωση ο ανακριτής να αποφανθεί. Αν όμως είπε πως ο Γ είναι κατάσκοπος τότε ο Γ είναι ευγενής και ο κατάσκοπος είναι ο Β.

Θέμα 4 (Κατηγορηματική Λογική, 1.6 μονάδες)

Έστω πρωτοβάθμια γλώσσα με κατηγορηματικά σύμβολα τα $C(x)$, $S(x)$, $P(x)$, $T(x,y)$, $E(x,y)$ και $F(x,y)$ τα οποία ερμηνεύουμε ως "το x είναι μάθημα" (για το $C(x)$), "ο x είναι φοιτητής" (για το $S(x)$), "ο x είναι καθηγητής" (για το $P(x)$), "ο καθηγητής x διδάσκει το μάθημα y" (για το $T(x,y)$), "ο φοιτητής x παρακολουθεί το μάθημα y" (για το $E(x,y)$), και "οι x και y είναι φίλοι μεταξύ τους" (για το $F(x,y)$). Σε αυτή την ερμηνεία, να διατυπώσετε ότι:

1. Υπάρχει μάθημα που το παρακολουθούν όλοι οι φοιτητές.

$$\exists x(C(x) \wedge \forall y(S(y) \rightarrow E(y,x)))$$

2. Ο καθηγητής x διδάσκει ακριβώς 2 μαθήματα.

$$P(x) \wedge \exists y \exists z(C(y) \wedge C(z) \wedge y \neq z \wedge T(x,y) \wedge T(x,z) \wedge \forall w(C(w) \wedge T(x,w)) \rightarrow w = y \vee w = z)$$

το x είναι ελεύθερη μεταβλητή

3. Όταν δύο φοιτητές είναι φίλοι, τότε παρακολουθούν τουλάχιστον ένα μάθημα μαζί.

$$\forall x \forall y(S(x) \wedge S(y) \wedge F(x,y) \rightarrow \exists z(C(z) \wedge E(x,z) \wedge E(y,z)))$$

4. Όσοι φοιτητές παρακολουθούν το μάθημα "Διακριτά Μαθηματικά" δεν παρακολουθούν το μάθημα "Αριθμητική Ανάλυση".

Έχουμε 2 σταθερές d για τα διακριτά μαθηματικά και a για την αριθμητική ανάλυση $\forall x((S(x) \wedge E(x,d)) \rightarrow \neg E(x,a))$

5. Αν ένας φοιτητής παρακολουθεί όλα τα μαθήματα ενός καθηγητή, τότε αυτοί είναι φίλοι.

$$\forall x \forall y[(S(x) \wedge P(y) \wedge \forall z((C(z) \wedge T(y,z)) \rightarrow E(x,z))) \rightarrow F(x,y)]$$

Θέμα 5 (Κατηγορηματική Λογική, 2.4 μονάδες)

Έστω πρωτοβάθμια γλώσσα με ένα μονομελές κατηγορηματικό σύμβολο P και ένα διμελές κατηγορηματικό σύμβολο R. Θεωρούμε τις παρακάτω προτάσεις:

$$\psi_1 \equiv \left[\forall x \forall y \forall z \left(R(x,y) \wedge R(y,z) \rightarrow R(x,z)\right) \wedge \forall x \forall y \left(R(x,y) \rightarrow R(y,x)\right) \wedge \forall x \exists y R(x,y)\right] \rightarrow \forall x R(x,x)$$

$$\psi_2 \equiv \exists x \left[\forall y \left(P(y) \rightarrow R(y,x)\right) \wedge \forall y \left(\forall z \left(P(z) \rightarrow R(z,y)\right) \rightarrow R(x,y)\right)\right]$$

$$\psi_3 \equiv \forall x \forall y \left[P(x) \wedge R(x,y) \wedge P(y) \wedge \neg R(y,x) \rightarrow \exists z \left(\neg R(z,x) \wedge \neg R(y,z)\right)\right]$$

1. Να διερευνήσετε αν οι προτάσεις ψ_1, ψ_2 και ψ_3 είναι λογικά έγκυρες.
2. Να δώσετε μια ερμηνεία των κατηγορηματικών συμβόλων P και R στο σύνολο N των φυσικών αριθμών ώστε να ικανοποιούνται οι προτάσεις ψ_2 και ψ_3.
3. Να διερευνήσετε αν οι προτάσεις ψ_2 και ψ_3 ικανοποιούνται στην ερμηνεία με σύμπαν το δυναμοσύνολο του N, με το $P(x)$ να δηλώνει ότι "το x είναι πεπερασμένο σύνολο" και το $R(x,y)$ να δηλώνει ότι "το x είναι υποσύνολο του y".

1. ψ_1: η μεταβατικότητα σε συνδυασμό με τη συμμετρικότητα δίνει όλα τα ζεύγη (a,a) για τα οποία ξεκινά βελάκι από το a. Επιπλέον δίνεται πως από κάθε στοιχείο ξεκινά βελάκι. Αυτές οι σχέσεις έχουν την ανακλαστική ιδιότητα.
ψ_2: στην ακόλουθη ερμηνεία η ψ_2 δεν ικανοποιείται:
Σύμπαν οι φυσικοί, $P(x)$: $x > 0$ και $R(x,y)$: $x < y$
Στους φυσικούς δεν υπάρχει μέγιστο.
ψ_3: στην ακόλουθη ερμηνεία η ψ_3 δεν ικανοποιείται:
Σύμπαν οι φυσικοί, $P(x)$: $x > 0$ και $R(x,y)$: $x \leq y$
Αν $x = 3$ και $y = 4$ δεν υπάρχει φυσικός που να μην είναι μικρότερος ή ίσος του 3 και να μην είναι μεγαλύτερος ή ίσος του 4. Δεν υπάρχει φυσικός μεγαλύτερος του 3 και μικρότερος του 4 (δεν υπάρχει ενδιάμεσο στοιχείο).

2. Ορίζω ως σύμπαν τους φυσικούς, $P(x)$: $x < 1000$ και $R(x,y)$: $x < y$.
Για την ψ_2 αναζητώ τον ελάχιστο φυσικό που είναι μεγαλύτερος όλων των φυσικών που έχουν την ιδιότητα P (δηλαδή είναι μικρότεροι του 1000). Και αυτός είναι ο 1000.
Για την ψ_3 αναζητώ για όλους τους φυσικούς x, y που είναι μικρότεροι του 1000 κάποιον φυσικό που να μην είναι μικρότερος του πρώτου και να μην είναι μεγαλύτερος του δεύτερου. Το ρόλο του z σε αυτή την περίπτωση θα μπορούσε να παίξει είτε το x είτε το y.

3. Για την ψ_2 στην ερμηνεία που δίνεται το ρόλο του μέγιστου κάτω φράγματος παίζει η ένωση όλων των πεπερασμένων υποσυνόλων.
Για την ψ_3 το ρόλο του z θα μπορούσε να παίξει οποιοδήποτε σύνολο ξένο ως προς τα y και x. Επομένως ικανοποιούνται και οι δύο προτάσεις.

Θέμα 6 (Μαθηματική Επαγωγή, 1.8 μονάδες)
(α) Θεωρούμε n ευθείες που διαιρούν το επίπεδο σε περιοχές. Χρησιμοποιώντας μαθηματική επαγωγή στο πλήθος n των ευθειών, να δείξετε ότι αυτές οι περιοχές μπορούν να χρωματιστούν με δύο χρώματα ώστε αν δύο περιοχές είναι γειτονικές, αυτές να έχουν διαφορετικό χρώμα (δύο περιοχές θεωρούνται γειτονικές αν το "σύνορό" τους είναι ένα ευθύγραμμο τμήμα, όχι μόνο ένα σημείο).

Για $n=1$ ισχύει
Έστω πως ισχύει για $n=k$. Θα πρέπει να δείξουμε πως ισχύει για $n=k+1$
Χαράζουμε την νέα ευθεία. Η πλευρά που βρίσκεται δεξιά της νέας ευθείας είναι χρωματισμένη με δύο χρώματα και λόγω επαγωγής (για $n=k$) οι γειτονικές περιοχές έχουν διαφορετικό χρώμα.
Στις περιοχές αριστερά της ευθείας αντιστρέφω τα χρώματα. Άρα και αυτή η πλευρά λόγω επαγωγής για $n=k$ έχει περιοχές που αν είναι γειτονικές έχουν διαφορετικό χρώμα.
Οι περιοχές των δύο πλευρών που χωρίζονται από την νέα ευθεία επίσης έχουν διαφορετικό χρώμα λόγω του ότι πριν χαράξω την νέα ευθεία είχαν το ίδιο και όταν την χάραξα αντέστρεψα τα χρώματα των περιοχών της μιας πλευράς.

(β) Θεωρούμε μία χώρα με $n \geq 2$ πόλεις, όπου για κάθε ζευγάρι διαφορετικών πόλεων $x, y,$ υπάρχει απευθείας οδική σύνδεση (μονής κατεύθυνσης) είτε από την x στην y είτε από την y στην x. Να δείξετε, χρησιμοποιώντας μαθηματική επαγωγή, ότι σε κάθε τέτοια χώρα, υπάρχει μία μετάθεση $t_1,...t_n$ των πόλεων ώστε κάθε πόλη (εκτός της τελευταίας) να συνδέεται απευθείας με την επόμενή της στη μετάθεση, δηλ. για κάθε $i=1,...,n-1,$ να υπάρχει απευθείας οδική σύνδεση από την πόλη t_i στην πόλη t_{i+1}.

Για 2 πόλεις t_1 και t_2 ισχύει εφόσσον υπάρχει οδική σύνδεση μεταξύ τους.
Έστω πως ισχύει για n πόλεις και χβγ θεωρώ πως η διάταξη είναι από την t_1 στην t_n.
Για την t_{n+1} διακρίνουμε τις εξής περιπτώσεις:
$1^{η}$ Η t_{n+1} να "δείχνει" στην t_1. Σε αυτή την περίπτωση η t_{n+1} είναι η πρώτη πόλη στην διάταξη και ακολουθούν t_1 έως t_n.
$2^{η}$ Η t_n να δείχνει στην t_{n+1}. Επομένως η διάταξη ξεκινά από την t_1 και καταλήγει στην t_{n+1}.
$3^{η}$ Η t_1 να "δείχνει" στην t_{n+1} και η t_{n+1} να "δείχνει" στην t_n. Εφόσσον όλες οι πόλεις συνδέονται με την t_{n+1} ελέγχουμε όλες τις πόλεις ξεκινώντας από την t_1 και σταματούμε στην πρώτη προς την οποία "δείχνει" η t_{n+1} (στη χειρότερη περίπτωση αυτή θα είναι η τελευταία). Έστω οι πόλεις $t_1,...t_i$ έχουν κατεύθυνση προς την t_{n+1} και η t_{i+1} συνδέεται με την t_{n+1} προς την αντίθετη κατεύθυνση. Τότε η διάταξη θα είναι $t_1,...,t_i,t_{n+1},t_{i+1},...,t_n$.