Διακριτά Μαθηματικά

1η Γραπτή Εργασία

Χρήστος Τσούφης
03117176

Θέμα 1

α). Η αντιστοίχιση των συντελεστών $(a_0, a_1, \dots, a_d)$ του $p(n)$ με το σύνολο $\mathbb{N}^{d+1}$ είναι 1-1 και επί. Επίσης, κάθε πολυώνυμο αντιστοιχίζεται μοναδικά στους συντελεστές του. Επομένως, το P_d αριθμήσιμο. Το P αποτελείται από αριθμήσιμη ένωση αριθμήσιμων συνόλων επομένως υπάρχει αντιστοίχιση 1-1 και επί $f: P \to \mathbb{N}^{d+2} \to \mathbb{N}$. Άρα και P αριθμήσιμο.

β) Θεωρούμε το σύνολο των συναρτήσεων $f: \mathbb{N} \to \mathbb{N}$ και έστω $(f_n)_{n\in\mathbb{N}}$ μια απαρίθμησή τους. Ορίζουμε την ακολουθία g_n τέτοια ώστε $g(n) = f_n(n)+1$ η οποία ανήκει στο σύνολο. Όμως επειδή έχουμε υποθέσει ότι το σύνολο είναι αριθμήσιμο θα υπάρχει $i \in \mathbb{N}$ τέτοιο ώστε $g(i) = f_i(i) \Leftrightarrow$ $\Leftrightarrow 1 = 0$ που είναι άτοπο. Άρα, υπάρχουν άπειρες συναρτήσεις που δεν ανήκουν στο P.

γ) Ο αλγόριθμος (σε φυσική γλώσσα):

Όσο δεν έχω πρόσβαση στο σύστημα $(x_t' \neq x_t)$:

Μάντεψε $(a_0', a_1', \dots, a_d', x_0', q')$

Δοκίμασε $x_t' = p(x_{t-1}') \bmod q'$. Το x_t' προκύπτει αναδρομικά από τον υπολογισμό των προηγούμενων $x_{t-1}', \dots, x_0'$.

Περίμενε 30 δευτερόλεπτα

Ορθότητα: Εφόσον οι αριθμοί που μαντεύω είναι πάντα φυσικοί και τα σύνολα που θα πάρω είναι άπειρα αριθμήσιμα θα γνωρίζουμε ότι υπάρχει χρονική στιγμή t τέτοια ώστε $x_t' = x_t$.

Θέμα 2

α) 1. Απόδειξη με επαγωγή:

Βάση: Αν $\varphi = A$ τότε δεν χρησιμοποιούνται σύνδεσμοι άρα αυτόματα ισχύει η πρόταση.

υπόθεση: Εστω a, β δύο προτασιακοί τύποι για τους οποίους ισχύει ότι μπορούν να γραφούν μόνο με χρήση του συνδέσμου $|$.

Βήμα: Ισχύουν οι εξής ισοδυναμίες:

$$\neg a \equiv \neg(a \vee a) \equiv a|a$$

$$a \vee \beta \equiv \neg\neg(a\vee\beta) \equiv (a|\beta)|(a|\beta)$$

$$a \wedge \beta \equiv \neg(\neg a \vee \neg\beta) \equiv (a|a)|(\beta|\beta)$$

$$a \rightarrow \beta \equiv \neg a \vee \beta \equiv ((a|a)|\beta)|((a|a)|\beta)$$

$$a \leftrightarrow \beta \equiv (a\rightarrow\beta)\wedge(\beta\rightarrow a)$$

Άρα, όντως όλοι οι τύποι έχουν ισοδύναμη μορφή που χρησιμοποιεί μόνο $|$.

2. Οι τύποι είναι οι φ_1 και φ_2. Χρησιμοποιώντας τις ιδιότητες που αποδείχθηκαν έχουμε τις ακόλουθες ισοδυναμίες:

$$\varphi_1 \equiv ((p\vee q)\wedge\neg q)\rightarrow q \equiv (p\wedge\neg q)\vee(q\wedge\neg q)\rightarrow q \equiv q\wedge\neg p\rightarrow q$$

Άρα είναι ταυτολογία εφόσον όταν το αριστερό μέλος είναι αληθές τότε και το q είναι αληθές άρα και το δεξί μέλος είναι αληθές.

$$\varphi_2 \equiv (p\wedge(p\rightarrow q))\wedge(\neg p\vee\neg q) \equiv (p\wedge q)\wedge\neg(p\wedge q)$$

Άρα είναι αντίφαση.

β) Θεωρούμε :
a : ο μπάτλερ λέει αλήθεια
β : ο μάγειρας λέει αλήθεια
γ : ο κηπουρός λέει αλήθεια
δ : ο μάστορας λέει αλήθεια

Οπότε οι προτάσεις γράφονται:

$$\varphi_1 \equiv a\rightarrow\beta \equiv \neg a\vee\beta$$
$$\varphi_2 \equiv \neg\beta\vee\neg\gamma$$
$$\varphi_3 \equiv \gamma\vee\delta$$
$$\varphi_4 \equiv \delta\rightarrow\neg\beta \equiv \neg\delta\vee\neg\beta$$

Πρέπει όλες να αληθεύουν οπότε το a και το β πρέπει να είναι ψευδή, για τα υπόλοιπα όμως δεν προκύπτει κάποιο συμπέρασμα καθώς οι προτάσεις επαληθεύονται αρκεί να λέει αλήθεια ο κηπουρός ή ο μάστορας. Επομένως, ο Πουαρό δεν ξέρει ακριβώς ποιοι λένε αλήθεια και ποιοί ψέματα.

γ) 1.

2. Έστω σύνολο T μη ικανοποιήσιμο. Αυτό συνεπάγεται την αντίφαση. Άρα: $T \models A \wedge \neg A$

Άρα από το (1) υπάρχει πεπερασμένο $T_0 \subseteq T$ ώστε: $T_0 \models A \wedge \neg A$.

Όμως, αφού το T_0 συνεπάγεται την αντίφαση, θα πρέπει να είναι μη ικανοποιήσιμο.

Θέμα 3

α) 1. $\varphi_1 \equiv P(x, c_2) \wedge \forall y \forall z \,(P(y, c_3) \wedge P(z, c_3) \wedge P(y,z) \rightarrow P(g(x,y), g(x,z)))$

2. $\varphi_2 \equiv P(x, c_2) \wedge P(y, c_3) \wedge \forall x' \forall y' \,(P(x', c_2) \wedge P(y', c_3) \wedge$
$((P(g(x',y), g(x,y)) \wedge P(g(x,y), g(x',y))) \rightarrow (P(x',x) \wedge P(x,x'))) \wedge$
$((P(g(x,y'), g(x,y)) \wedge P(g(x,y), g(x,y'))) \rightarrow (P(y',y) \wedge P(y,y'))))$

3. $\varphi_3 \equiv \forall x\,(P(x, c_2) \rightarrow \exists y\,(\neg P(g(x,y), c_4)))$

4. $\varphi_4 \equiv \forall x \forall y\,(P(x, c_2) \wedge P(y, c_3) \rightarrow \exists z \exists w\,(P(g(x,y), f(g(z,y), g(x,w))) \wedge$
$P(f(g(z,y), g(x,w)), g(x,y))))$

5. $\varphi_5 \equiv \forall x \forall y \forall z \forall w\,(P(x, c_2) \wedge P(z, c_2) \wedge P(y, c_3) \wedge P(w, c_3) \wedge$
$(\neg P(z,x) \vee \neg P(w,y)) \rightarrow P(g(x,y), g(z,w)))$.

β) Απόδειξη με επαγωγή:

$\forall n \in \mathbb{N}$, υπάρχει τρόπος να τις εκφράσουμε με τα δεδομένα σύμβολα και σταθερές.

Βάση: Για $n=1$, ισχύει $n = c_1$.

Υπόθεση: Έστω ότι το $n = n_0 \geq 1$ εκφράζεται με τα δεδομένα.

Βήμα: Αν $n = n_0 + 1$ τότε $n = f(n_0, c_1)$.

Οπότε, δεν απαιτούνται οι υπόλοιπες σταθερές.

Θέμα 4ο

α) 1. $\varphi = \forall x P(x,x) \land \forall x \forall y (P(x,y) \to \forall z (P(x,z) \lor P(z,y))) \to \forall x \forall y (P(x,y) \lor P(y,x))$

$1^{η}$ ιδιότητα: $\forall x P(x,x)$ είναι αληθής (ανακλαστική ιδιοτ.)

$2^{η}$ ιδιότητα: $\forall x \forall y (P(x,y) \to \forall z (P(x,z) \lor P(z,y)))$

θέτοντας $y = x$: $\forall x (P(x,x) \to \forall z (P(x,z) \lor P(z,x)))$

Άρα, η φ είναι λογικά έγκυρη.

2. $\psi = \forall x P(x,x) \land \forall x \forall y (P(x,y) \to \forall z (P(x,z) \lor P(z,y))) \to \exists x \forall y P(x,y)$

Επαγωγή:

Βάση: Για $n=1$ το μοναδικό στοιχείο είναι το a. Σε αυτήν την περίπτωση ισχύει το δεξιό μέλος, αφού το a σχετίζεται με κάθε άλλο στοιχείο του σύμπαντος, δηλαδή με τον εαυτό του λόγω της πρώτης ιδιότητας (ανακλαστική).

Υπόθεση: Έστω ότι για κάθε σύμπαν με αριθμό στοιχείων $n \leq n_0$ αν ισχύουν οι πρώτες δύο ιδιότητες, τότε: $\exists x \forall y P(x,y)$.

Βήμα: Για σύμπαν με πλήθος στοιχείων $n = n_0 + 1$ ισχύουν οι πρώτες δύο ιδιότητες.

Έστω b ένα στοιχείο του σύμπαντος

$P(b,b)$ αληθής λόγω ανακλαστικής ιδιοτ. ($1^{η}$ ιδιοτ.)

$P(b,b) \Rightarrow \forall z (P(b,z) \lor P(z,b))$ ($2^{η}$ ιδιοτ.)

$P(b,x) \lor P(x,b)$ αληθής, προκύπτει από αντικατάσταση $z = x$

Οπότε, είτε το b σχετίζεται με το στοιχείο που σχετίζεται με όλα τα υπόλοιπα είτε αυτό σχετίζεται με το b.

Έστω $P(b,x)$ αληθής, τότε

$P(b,x) \Rightarrow \forall z (P(b,z) \lor P(z,x))$ ($2^{η}$ ιδιοτ.)

$P(b,b) \Rightarrow \forall z (P(b,z) \lor P(z,b))$ ($2^{η}$ ιδιοτ.)

Για να ισχύουν και τα δύο θα πρέπει $\forall z P(b,z)$.

Επομένως, το νέο στοιχείο που σχετίζεται με όλα είναι το b.

Η άλλη περίπτωση είναι τετριμμένη καθώς το x ήδη συσχετιζόταν με όλα τα άλλα.

3. Μια ερμηνεία που δεν αποτελεί μοντέλο της φ είναι το σύμπαν των ακεραίων με $P(x,y) \equiv x \leq y$. Προφανώς, ισχύει η ανακλαστική ιδιότητα και επίσης αν $P(x,y)$ αληθές τότε για οποιοδήποτε z ισχύει $P(x,z) \lor P(z,y)$ αφού είτε το z θα είναι μικρότερο ή του y είτε θα είναι αναγκαστικά μεγαλύτερο του y οπότε σίγουρα θα είναι και μεγαλύτερο του x.

β) Θα αποδείξουμε ότι υπάρχει ερμηνεία για την οποία δεν ισχύει η συνεπαγωγή. Έστω ότι σύμπαν είναι οι φυσικοί και $P(x,y) \equiv y=x+1$. Αφού αποδεχθούν οι ιδιότητες του αριστερού μέλους θα δείξουμε ότι σε αυτήν την ερμηνεία δεν ισχύει το δεξί μέλος.

- $\forall x \neg P(x,x)$: δεν υπάρχει x ώστε $x = x+1$.
- $\exists x \forall y \neg P(y,x)$: υπάρχει x με το οποίο δεν σχετίζεται κανένα άλλο στοιχείο, το 0.
- $\forall x \forall y \forall z (P(x,y) \wedge (x,z) \to y=z)$: αν $y=x+1$ δεν υπάρχει $z \neq x$ ώστε $y=z+1$ γιατί $z<x=y-1 \Rightarrow y>z+1$ και $z>x=y-1 \Rightarrow y<z+1$.
- $\forall x \forall y \forall z (P(y,x) \wedge P(z,x) \to y=z)$: ομοίως, δεν υπάρχει $z \neq y$ ώστε $z=x+1$.

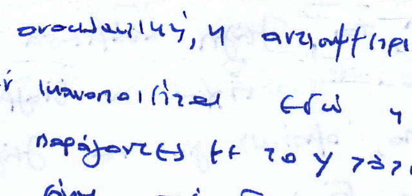
Όμως, δεν υπάρχει τέτοιο στοιχείο που να μην σχετίζεται με κανένα πέρα από τον αριθμό των φυσικών, αν ένας αριθμός είναι φυσικός τότε και ο επόμενός του είναι φυσικός.

Θέμα 5

α) Ευθύ: Η R είναι ανακλαστική. Έστω x,y στοιχεία με xRy. Όμως η R είναι και κυκλική. Επομένως $xRy \wedge yRy \Rightarrow yRx$ επομένως συμμετρική. Τέλος, είναι μεταβατική διότι είναι κυκλική και συμμετρική επομένως, για κάθε x,y,z τέτοια ώστε $xRy \wedge yRz \Rightarrow zRx \Rightarrow xRz$. Άρα η R σχέση ισοδυναμίας.

Αντίστροφα: Έστω R σχέση ισοδυναμίας, τότε τετριμμένα για κάθε x είναι xRx. Επίσης για κάθε x,y,z τέτοια ώστε $xRy \wedge yRz \Rightarrow xRz \Rightarrow zRx$. Άρα η R ανακλαστική και κυκλική.

β) Διάγραμμα Hasse:



γ) Αρκεί να ικανοποιείται η ανακλαστική, η αντισυμμετρική και η μεταβατική ιδιότητα για να είναι σχέση ______. Δεν ικανοποιείται εδώ η αντισυμμετρική γιατί αν ένας αριθμός x έχει τους ίδιους πρώτους παράγοντες με το y τότε και το y έχει τους ίδιους πρώτους παράγοντες με το x. Άρα δεν είναι σχέση διάταξης.

Θέμα 6

α) Μέσω επαγωγής αποδεικνύεται ότι οι n ευθείες που χωρίζουν το επίπεδο σε περιοχές μπορούν να χρωματιστούν μόνο με δύο χρώματα ώστε δυο γειτονικές να μην έχουν το ίδιο χρώμα. Έστω $P(n)$ η παραπάνω πρόταση.

Βάση: Για $n=1$, είναι προφανές ότι αν χρωματίσουμε τις 2 περιοχές με 2 διαφορετικά χρώματα, θα ισχύει

υπόθεση: Για κάποιο συγκεκριμένο $n \geq 1$ δεχόμαστε ότι ισχύει η $P(n)$.

Βήμα: Για $n:=n+1$ θα δείξουμε ότι $P(n) \rightarrow P(n+1)$. Πράγματι, αν χαράξουμε μία νέα ευθεία στο σχήμα θα "διχοτομηθούν" ορισμένες περιοχές. Οι νέες περιοχές εκατέρωθεν της ευθείας έχουν το ίδιο χρώμα. Εργαζόμαστε ως εξής: Έστω ότι χωρίζεται το επίπεδό μας στα δυο ημιεπίπεδα εκατέρωθεν της ευθείας. Στο ένα εκ των δύο αντιστρέφουμε τα χρώματα οπότε οι περιοχές που συνορεύουν με την ευθεία έχουν αμφότερες διαφορετικό χρώμα και γνωρίζουμε λόγω της υπόθεσης ότι χρωματίζονται με δύο χρώματα και επομένως στον γράφο δεν θα υπάρχει κύκλος περιττού μήκους. Συνεπώς, το γράφημά μας είναι διμερές.

β) Έστω $b_{l,n}$ μια ακολουθία που σε κάθε ζεύγος l,n αντιστοιχίζει το πολύ τον αριθμό από ζεύγη δυαδικών μήκους l ενός συνόλου n στοιχείων που διαφέρουν κατά ένα μόνο ψηφίο.

Βάση: Για $l=1$, τα μόνα δυνατά σύνολα είναι τα $\{0\}, \{1\}, \{0,1\}$. Τα πρώτα δύο με $n=1$ έχουν $0=\frac{1}{2}\log_2 1$ ζεύγη, ενώ το τρίτο με $n=2$ έχει $1=\frac{2}{2}\log_2 2$ ζεύγη.

υπόθεση: $b_{l,n} \leq \frac{n}{2}\log_2 n \quad \forall l \leq l_0, \ 1 \leq n \leq 2^l$.

Βήμα: Για $l=l_0+1$ διαμερίζουμε το $S, |S|=n$, σε δύο ξένα σύνολα S_0 και S_1 ώστε το πρώτο να περιέχει τα στοιχεία του S που τελειώνουν σε 0 και το δεύτερο τα στοιχεία του S που τελειώνουν σε 1. Αν $|S_0|=n_0$, $|S_1|=n_1$ τότε $n_0+n_1=n$ και $n_0 \leq 2^{l_0}$, $n_1 \leq 2^{l_0}$, γιατί με σταθερό το ένα ψηφίο από τα l_0+1 απομένουν l_0 που αλλάζουν τιμές. Άρα, τα ζεύγη ανάμεσα σε στοιχεία μόνο του S_0 είναι το πολύ ίσα με όσα θα είχε αν διαγράφαμε το τελευταίο ψηφίο, δηλαδή $b_{l_0+1,n_0}=b_{l_0,n_0}$, ομοίως για τα ζεύγη ανάμεσα σε στοιχεία του S_1, $b_{l_0+1,n_1}=b_{l_0,n_1}$. Επίσης, για κάθε στοιχείο του S_0 υπάρχει το πολύ ένα στοιχείο του S_1 ώστε να σχηματίζουν ζεύγος, γιατί τα στοιχεία των δύο συνόλων διαφέρουν τουλάχιστον κατά ένα ψηφίο και υπάρχουν μόνο δύο δυαδικοί αριθμοί που να διαφέρουν μόνο κατά το τελευταίο ψηφίο, άρα από τα ζεύγη είναι το πολύ $\min(n_0,n_1)$. Το S έχει αυτά τα ζεύγη που αποτελούνται από στοιχεία του S_0 ή μόνο του S_1 ή και των δύο, άρα:

$b_{l_0+1,n} \leq b_{l_0,n_0}+b_{l_0,n_1}+\min(n_0,n_1) \Rightarrow$

$\Rightarrow b_{l_0+1,n} \leq \frac{n_0}{2}\log_2 n_0 + \frac{n_1}{2}\log_2 n_1 + \min(n_0,n_1) \leq$

$\leq \frac{n_0+n_1}{2}\log_2(n_0+n_1) = \frac{n}{2}\log_2 n$