ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΔΙΑΚΡΙΤΑ ΜΑΘΗΜΑΤΙΚΑ
Διδάσκοντες: Δ.Φωτάκης, Θ. Σούλιου
1η Γραπτή Εργασία, Ημ/νια παράδοσης 15/4/2018

Θέμα 1 (Διαδικασίες Απαρίθμησης 2.0 μον.)

(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 κωδικός 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 (Προτασιακή Λογική 1.6 μον.)

(α) Συμβολίζουμε με $p\,|\,q$ το "ούτε p ούτε q".

1. Να αποδείξετε ότι για κάθε προτασιακό τύπο φ, υπάρχει προτασιακά ισοδύναμος προτασιακός τύπος φ^* που χρησιμοποιεί μόνο το λογικό σύνδεσμο "|".

Ο αληθοπίνακας του $p\,|\,q$ είναι:

p	q	$p\,\|\,q$
T	T	F
T	F	F
F	T	F
F	F	T

Αρκεί να εκφράσω την άρνηση, το λογικό σύνδεσμο "$\wedge$" και το λογικό σύνδεσμο "$\vee$" χρησιμοποιώντας μόνο το λογικό σύνδεσμο "|".

$\neg p \equiv p\,|\,p$

$p \wedge q \equiv \neg p\,|\,\neg q \equiv (p\,|\,p)\,|\,(q\,|\,q)$

$p \vee q \equiv \neg(p\,|\,q) \equiv (p\,|\,q)\,|\,(p\,|\,q)$

2. Είναι κάποια από τις εκφράσεις που ακολουθούν αντίφαση ή ταυτολογία; Εξηγήστε την απάντησή σας.

$$(((p\,|\,q)\,|\,(p\,|\,q)) \wedge (p\,|\,p)) \rightarrow q$$

$$((p\,|\,p)\,|\,((p \rightarrow q)\,|\,(p \rightarrow q))) \wedge (((p\,|\,p)\,|\,(q\,|\,q))\,|\,((p\,|\,p)\,|\,(q\,|\,q)))$$

Η πρώτη είναι ταυτολογία διότι από το προηγούμενο ερώτημα γράφεται ως εξής: $((p \vee q) \wedge \neg p) \rightarrow q$ Η συνεπαγωγή γίνεται ψευδής αν q ψευδής και το πρώτο μέλος αληθές. Καταλήγουμε σε άτοπο. Άρα η συνεπαγωγή είναι πάντα αληθής.

Η δεύτερη είναι αντίφαση γιατί αντίστοιχα γράφεται ως εξής:

$(p \wedge (p \to q)) \wedge \neg(p \wedge q)$ Για να αληθεύει η σύζευξη θα πρέπει να αληθεύει το p καθώς και το q και ταυτόχρονα να αληθεύει το $\neg(p \wedge q)$. Άτοπο επομένως έχουμε αντίφαση.

(β) Ο Ηρακλής Πουαρό ανακρίνει 4 υπόπτους για ένα έγκλημα. Από τις ιστορίες των αυτόπτων μαρτύρων ο Ηρακλής έχει καταλήξει στα εξής:
(i) αν ο μπάτλερ λέει αλήθεια, τότε και ο μάγειρας λέει αλήθεια,
(ii) ο μάγειρας και ο κηπουρός δεν μπορεί να λένε και οι δύο αλήθεια,
(iii) ο κηπουρός και ο μάστορας δεν μπορεί να λένε και οι δύο ψέματα,
(iv) αν ο μάστορας λέει αλήθεια τότε ο μάγειρας λέει ψέματα,
Μπορεί ο Ηρακλής να καταλάβει ποιος λέει αλήθεια και ποιός ψέματα;

Έστω πως ο μπάτλερ λέει αλήθεια. Τότε και ο μάγειρας λέει αλήθεια (λόγω του (i)). Λόγω του (ii) ο κηπουρός δε λέει αλήθεια. Λόγω του (iii) ο μάστορας λέει αλήθεια. Λόγω του (iv) ο μάγειρας λέει ψέματα. Άτοπο.
Έστω πως ο μπάτλερ λέει ψέματα. Δεν μπορούμε να αποφανθούμε για το μάγειρα. Υποθέτουμε πως ο μάγειρας λέει αλήθεια. Καταλήγουμε σε άτοπο όπως πριν. Υποθέτουμε πως ο μάγειρας λέει ψέματα. Σε αυτή την περίπτωση ο κηπουρός μπορεί να λέει αλήθεια ή ψέματα ομοίως και ο μάστορας. Ο Πουαρώ δεν μπορεί να αποφανθεί.

(γ) Έστω Τ ένα άπειρο σύνολο προτασιακών τύπων, και έστω φ αυθαίρετα επιλεγμένος προτασιακός τύπος. Να δείξετε ότι:
1. Αν $T \models \varphi$, τότε υπάρχει πεπερασμένο $T_0 \subseteq T$ τέτοιο ώστε $T_0 \models \varphi$.
Από το Θεώρημα Πληρότητας, αν $T \models \varphi$, τότε $T \mid\!- \varphi$. Η τυπική απόδειξη του φ από τις υποθέσεις T, προκύπτει σε πεπερασμένο πλήθος βημάτων. Επομένως μπορεί να χρησιμοποιεί μόνο ένα πεπερασμένο υποσύνολο υποθέσεων του T. Έστω λοιπόν T_0 το πεπερασμένο υποσύνολο όλων των υποθέσεων στο T που χρησιμοποιούνται στην τυπική απόδειξη $T \mid\!- \varphi$. Με βάση τον ορισμό του T_0, έχουμε ότι $T_0 \mid\!- \varphi$. Χρησιμοποιώντας το Θεώρημα Εγκυρότητας, καταλήγουμε ότι $T_0 \models \varphi$.
2. Αν το Τ είναι μη ικανοποιήσιμο, τότε υπάρχει πεπερασμένο $T_0 \subseteq T$ που δεν είναι ικανοποιήσιμο.
Εφόσον Τ μη κανοποιήσιμο, $T \models \varphi$ για κάθε προτασιακό τύπο φ. Σύμφωνα με το προηγούμενο ερώτημα υπάρχει πεπερασμένο υποσύνολο $T_0 \subseteq T$ τέτοιο ώστε $T_0 \models \varphi$. Αυτό σημαίνει πως το σύνολο $T_0 \cup \{\neg\varphi\}$ είναι μη ικανοποιήσιμο, για κάθε προτασιακό τύπο φ. Στην περίπτωση που επιλέξουμε το φ να είναι αντίφαση, το $\neg\varphi$ είναι ταυτολογία. Κατά συνέπεια, το T_0 είναι αναγκαστικά μη ικανοποιήσιμο.

Θέμα 3 (Κατηγορηματική Λογική 2.1 μονάδες)

Θέλουμε να εκφράσουμε ιδιότητες που μπορεί να έχει ένας πίνακας $A \in N^{20\times 30}$. Είμαστε στο σύμπαν των θετικών ακεραίων εφοδιασμένο με το διμελές κατηγορηματικό σύμβολο P, δύο συναρτησιακά σύμβολα $f(x,y)$ και $g(x,y)$, και τέσσερις σταθερές c_1, c_2, c_3 και c_4. Ερμηνεύουμε το $P(x,y) \equiv x \leq y$, το $f(x,y) = x + y$, το $g(x,y) = A[x,y]$, τις σταθερές $c_1 = 1$, $c_2 = 20$, $c_3 = 30$ και $c_4 = 40$.
α) Σε αυτή την ερμηνεία να διατυπώσετε:
1. Τύπο $\varphi_1(x)$ που δηλώνει ότι τα στοιχεία της x-οστής γραμμής του πίνακα A είναι ταξινομημένα σε αύξουσα σειρά.

$\varphi_1(x) = \forall y(P(f(y,c_1),c_3) \to P(g(x,y),g(x,f(y,c_1))))$

2. Τύπο $\varphi_2(x,y)$ που δηλώνει ότι το στοιχείο στη θέση (x,y) του πίνακα A έχει τιμή διαφορετική από αυτές των στοιχείων που βρίσκονται στην ίδια στήλη ή στην ίδια γραμμή με αυτό.

$$\varphi_2(x,y) = \forall z((P(z,c_3) \wedge y \neq z) \to g(x,y) \neq g(x,z)) \wedge \forall z((P(z,c_2) \wedge x \neq z) \to g(x,y) \neq g(z,y))$$

3. Πρόταση που δηλώνει ότι σε κάθε γραμμή του A υπάρχει στοιχείο που η τιμή του ξεπερνά το 40.

$$\forall x(P(x,c_2) \to \exists y(P(y,c_3) \wedge \neg P(g(x,y),c_4)))$$

4. Πρόταση που δηλώνει ότι η τιμή κάθε στοιχείου του πίνακα A μπορεί να γραφτεί σαν άθροισμα των τιμών δύο στοιχείων του A, ένα στην ίδια γραμμή και ένα στην ίδια στήλη με το αρχικό.

$$\forall x \forall y((P(x,c_2) \wedge P(y,c_3)) \to \exists z \exists w(P(z,c_2) \wedge P(w,c_3) \wedge g(x,y) = f(g(x,w),g(z,y))))$$

5. Πρόταση που δηλώνει ότι η τιμή κάθε στοιχείου του πίνακα A είναι μικρότερη ή ίση της τιμής κάθε στοιχείου που βρίσκεται σε μεγαλύτερη στήλη ή σε μεγαλύτερη γραμμή από αυτό.

$$\forall x \forall y \forall z \forall w((P(x,c_2) \wedge P(y,c_3) \wedge P(z,c_2) \wedge P(w,c_3)) \to ((P(x,z) \wedge P(y,w)) \to P(g(z,w),g(x,y))))$$

β) Αν δεν υπήρχαν οι σταθερές c_2, c_3 και c_4 θα μπορούσαμε να τις εκφράσουμε με κάποιο τρόπο χρησιμοποιώντας τα υπόλοιπα σύμβολα (δηλ. τη σταθερά c_1, το κατηγορηματικό σύμβολο P και τα συναρτησιακά σύμβολα f και g);

Μπορούμε να γράψουμε το c_2 χρησιμοποιώντας μια νέα σταθερά τη c^* της οποίας η τιμή είναι 10. Εκφράζουμε τη c^* με τη βοήθεια της c_1 και του συναρτησιακού συμβόλου f. $c^* = f(f(f(f(c_1,c_1),f(c_1,c_1)),f(f(c_1,c_1),f(c_1,c_1))),f(c_1,c_1))$

Έτσι $c_2 = f(c^*,c^*)$, $c_3 = f(f(c^*,c^*),c^*)$, $c_2 = f(f(c^*,c^*),f(c^*,c^*))$

Θέμα 4 (Κατηγορηματική Λογική 2.5 μονάδες)

(α) Έστω μία πρωτοβάθμια γλώσσα με ένα διμελές κατηγορηματικό σύμβολο P. Θεωρούμε τις προτάσεις:

$$\varphi = \forall x P(x,x) \wedge \forall x \forall y(P(x,y) \to \forall z(P(x,z) \vee P(z,y))) \to \forall x \forall y(P(x,y) \vee P(y,x))$$
$$\psi = \forall x P(x,x) \wedge \forall x \forall y(P(x,y) \to \forall z(P(x,z) \vee P(z,y))) \to \exists x \forall y P(x,y)$$

1. Να διερευνήσετε τη λογική εγκυρότητα της φ.

Δεδομένου ότι κάθε στοιχείο του σύμπαντος (έστω x) "δείχνει" στον εαυτό του ο δεύτερος όρος του λογικού συνδέσμου "$\wedge$" για $y = x$ λέει πως κάθε στοιχείο του σύμπαντος συνδέεται με το x προς τη μία ή την άλλη κατεύθυνση. Σε αυτή την περίπτωση κάθε 2 στοιχεία του σύμπαντος συνδέονται προς τη μία ή την άλλη κατεύθυνση. Επομένως είναι λογικά έγκυρη.

2. Χρησιμοποιώντας μαθηματική επαγωγή στον πληθάριθμο του σύμπαντος, να δείξετε ότι κάθε ερμηνεία σε πεπερασμένο σύμπαν αποτελεί μοντέλο της ψ.

Η πρόταση λέει πως ΑΝ κάθε στοιχείο του σύμπαντος έχει την ανακλαστική ιδιότητα και ΑΝ για κάθε ζεύγος στοιχείων (a,b) που σχετίζονται ισχύει πως για κάθε στοιχείο του σύμπαντος υπάρχει συσχέτιση του a με αυτό ή αυτού με το b τότε υπάρχει στοιχείο που σχετίιζεται με όλα τα στοιχεία του σύμπαντος (ελάχιστο).

Για σύμπαν με ένα στοιχείο ισχύει. Έστω πως ισχύει για σύμπαν με k στοιχεία και έστω a το ελάχιστο στοιχείο. Συμβολίζουμε με x_i τα στοιχεία με τα οποία συσχετίζεται το a. Θα αποδείξουμε πως ισχύει για σύμπαν με $k+1$ στοιχεία. Αν το a σχετίζεται με το τελευταίο στοιχείο που προσθέσαμε έστω b τότε το a εξακολουθεί να παίζει το ρόλο του ελάχιστου στοιχείου. Αν όχι τότε η συχέτιση θα υπάρχει προς την αντίθετη κατεύθυνση δηλ το b σχετίζεται με το a. Σε αυτή την περίπτωση ισχύει $P(a,x_i)\rightarrow P(a,b)\vee P(b,x_i)$ και επειδή $P(a,b)$ δεν είναι αληθής θα είναι η $P(b,x_i)$ για όλα τα x_i. Επομένως το b θα παίξει το ρόλο του ελάχιστου στοιχείου.

3. Να διατυπώσετε ερμηνεία που δεν αποτελεί μοντέλο της ψ.

Σύμπαν οι φυσικοί αριθμοί και κατηγορηματικό σύμβολο $P(x,y)=x\leq y$

(β) Θεωρούμε μια πρωτοβάθμια γλώσσα με ένα διμελές κατηγορηματικό σύμβολο P. Να διερευνήσετε τη λογική εγκυρότητα της παρακάτω πρότασης:

$$\xi=\begin{pmatrix}\forall x\neg P(x,x)\wedge\exists x\forall y\neg P(x,y)\wedge\\ \forall x\forall y\forall z(P(x,y)\wedge P(x,z)\rightarrow y=z)\wedge\\ \forall x\forall y\forall z(P(y,x)\wedge P(z,x)\rightarrow y=z)\end{pmatrix}\rightarrow\exists x\forall y\neg P(x,y)$$

Η πρόταση λέει πως ΑΝ κανένα στοιχείο δεν σχετίζεται με τον εαυτό του και ΑΝ υπάρχει minimal και ΑΝ κάθε στοιχείο σχετίζεται με ένα στοιχείο το πολύ και το πολύ ένα στοιχείο σχετίζεται με αυτό τότε υπάρχει maximal. Είναι προφανές πως σε πεπερασμένο σύμπαν αυτό ισχύει (ουσιαστικά έχω πεπερασμένες αλυσίδες που δεν έχουν κοινά στοιχεία). Σε άπειρο σύμπαν όπως αυτό των φυσικών αριθμών και με ερμηνεία του κατηγορηματικού συμβόλου $P(a,b)=a<b$ δεν υπάρχει maximal. Επομένως η ξ δεν είναι λογικά έγκυρη.

Θέμα 5 (Διμελείς Σχέσεις 1.5 μον.)

(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.

κυκλική και ανακλαστική $\Rightarrow$ ισοδυναμίας

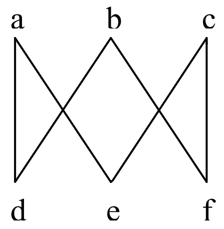
$\forall a(a,a)\in R$, άρα για κάθε ζεύγος $(a,b)\in R\ \Rightarrow(b,a)\in R$ (εφαρμογή της κυκλικής ιδιότητας). Επομένως R συμμετρική.

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

ισοδυναμίας ⇒ 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) 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.

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.

Θέμα 6 (Μαθηματική Επαγωγή, 1.8 μον.)

(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. Έστω $S=\{a_1, a_{2,} ..., a_n\}$ ένα σύνολο $n \geq 1$ διαφορετικών δυαδικών συμβολοσειρών μήκους $k \geq 1$. Να δείξετε (με μαθηματική επαγωγή στο μήκος k των συμβολοσειρών) ότι το S περιέχει το πολύ $\frac{n}{2}\log_2 n$ (μη διατεταγμένα) ζευγάρια διαφορετικών συμβολοσειρών που διαφέρουν μεταξύ τους σε ένα δυαδικό ψηφίο. Π.χ. το σύνολο $S=\{00,01,10,11\}$ περιέχει 4 τέτοια ζευγάρια, τα $(00,01),(00,10),(01,11),(10,11)$. Αντίστοιχα, το σύνολο $S=\{000,001,010,100\}$ περιέχει 3 τέτοια ζευγάρια, τα $(000,001),(000,010),(000,100)$.

Σε κάθε στοιχείο του συνόλου S προσθέτω στην αρχή ένα ακόμη ψηφίο και παίρνω $2n$ στοιχεία. Από τα n που το πρώτο τους ψηφίο είναι το 0 αφαιρώ κάποια. Έστω απομένουν x. Αυτά που διαφέρουν σε ένα ψηφίο είναι το πολύ $\frac{x}{2}\log_2 x$.
Ομοίως το πλήθος αυτών που διαφέρουν σε ένα ψηφίο και έχουν σαν πρώτο ψηφίο το 1 είναι το πολύ $\frac{y}{2}\log_2 y$.
Αυτά που διαφέρουν κατά 1 μεταξύ αυτών που έχουν πρώτο ψηφίο το 0 και αυτών που έχουν το 1 είναι το πολύ $\min(x,y)$.
Θέλουμε να αποδείξουμε πως :

$$\frac{x}{2}\log_2 x+\frac{y}{2}\log_2 y+\min(x,y)\leq\frac{x+y}{2}\log_2(x+y)$$

Για την απόδειξη της παραπάνω ανισότητας, θεωρούμε (χωρίς βλάβη της γενικότητας) ότι $x \leq y$. Οπότε αρκεί να δείξουμε ότι:
$x\log_2 x+y\log_2 y+2x\leq(x+y)\log_2(x+y)$, για κάθε $0<x\leq y$.
Η παραπάνω, είναι ισοδύναμη με την

$$2x\leq x\log_2\left(1+\frac{y}{x}\right)+y\log_2\left(1+\frac{x}{y}\right)$$

Αφού $0<x\leq y$, αρκεί να δείξουμε ότι:

$$2x\leq x\left(\log_2\left(1+\frac{y}{x}\right)+\log_2\left(1+\frac{x}{y}\right)\right)=x\log_2\left(\left(1+\frac{y}{x}\right)\left(1+\frac{x}{y}\right)\right)$$

Η τελευταία ανισότητα ισχύει γιατί $x>0$ και $(1+z)\left(1+\frac{1}{z}\right)\geq 4$, για κάθε $z>0$.