

1^η Γραπτή Εργασία – Απαντήσεις

➤ Θέμα 1

a) Το σύνολο $P_d = a_d * x^d + a_{d-1} * x^{d-1} + \dots + a_1 * x + a_0$ των πολυωνυμικών συναρτήσεων βαθμού d μπορεί να αντιστοιχηθεί μονοσήμαντα με τις διατεταγμένες $(d+1)$ -άδες $[a_d \ a_{d-1} \ \dots \ a_1 \ a_0]$, δηλαδή ένα καρτεσιανό γινόμενο $\mathbb{N} \times \mathbb{N} \times \dots \times \mathbb{N} \times \mathbb{N}$ ($d+1$ φορές). Έχουμε αποδείξει όμως πως το καρτεσιανό αυτό γινόμενο καθώς και όσα σύνολα παράγονται από αυτό είναι αριθμήσιμα, αφού \mathbb{N} αριθμήσιμο. Έχοντας απλά υπόψη πως $a_d \neq 0$, αποδείξαμε ότι **το P_d είναι αριθμήσιμο**. Το σύνολο P των πολυωνυμικών συναρτήσεων είναι η ένωση όλων των $P_d \ \forall d$. Επομένως, υπάρχει διαδικασία απαρίθμησης του P μέσω του d . Επίσης, καθένα από τα P_0, P_1 κλπ αποδείξαμε πως είναι αριθμήσιμα (απαρίθμηση έστω μέσω του c). Άρα, έχουμε τον δείκτη (c,d) μέσω του οποίου απαριθμείται κάθε στοιχείο-συνάρτηση του P . Το P δηλαδή αντιστοιχίζεται μονοσήμαντα με ένα καρτεσιανό γινόμενο $\mathbb{N} \times \mathbb{N}$, ένα κατά τα γνωστά αριθμήσιμο σύνολο. Αποδείξαμε πως **το P είναι αριθμήσιμο**.

b) Αρκεί να αποδείξουμε πως το σύνολο όλων των συναρτήσεων $f : \mathbb{N} \rightarrow \mathbb{N}$ είναι μη αριθμήσιμο, αφού αν αφαιρέσουμε από ένα μη αριθμήσιμο σύνολο ένα αριθμήσιμο υποσύνολό του (στην περίπτωσή μας το P), το υπόλοιπο παραμένει προφανώς μη αριθμήσιμο, κάτι που ισοδυναμεί εδώ με το να υπάρχουν άπειρες συναρτήσεις που δεν εκφράζονται σε πολυωνυμική μορφή. Για την απόδειξη θα χρησιμοποιήσουμε την τεχνική της διαγωνιοποίησης, εξετάζοντας τη σχέση των συναρτήσεων με το πεδίο ορισμού τους. Ορίζουμε συνάρτηση $g : \mathbb{N} \rightarrow \mathbb{N}$ ως εξής: $g(n) = \begin{cases} c, & \text{αν δεν ορίζεται το } f_n(n) \\ f_n(n) + c, & \text{αλλιώς} \end{cases}$ με $c \in \mathbb{N}$. Παρατηρούμε πως η g είναι κατά τέτοιο τρόπο φτιαγμένη ώστε να διαφέρει πάντα από οποιαδήποτε άλλη συνάρτηση f , τουλάχιστον σε ένα σημείο όπως φαίνεται από τον δεύτερο κλάδο της. Μάλιστα, αν προσθέσουμε τη g στο σύνολο των συναρτήσεων, μπορούμε με όμοιο τρόπο να παράγουμε μια νέα που θα έχει την ίδια ιδιότητα και δε θα καταμετράται. Συνεπώς, αποδείξαμε πως το σύνολο όλων των συναρτήσεων δεν είναι αριθμήσιμο και κατ' επέκταση πως **υπάρχουν άπειρες συναρτήσεις $f : \mathbb{N} \rightarrow \mathbb{N}$ που δεν μπορούν να εκφραστούν σε πολυωνυμική μορφή**.

c) Πρόσβαση στον υπερυπολογιστή σε πεπερασμένο χρόνο ισοδυναμεί με αλγόριθμο παραγωγής κωδικών με αριθμήσιμο πλήθος βημάτων. Ο υπερυπολογιστής βασίζεται ευτυχώς σε 3 στοιχεία που είναι αριθμήσιμα:

- Το σύνολο των πολυωνυμικών συναρτήσεων βαθμού d είναι αριθμήσιμο όπως αποδείξαμε παραπάνω, άρα είναι και οι $(d+1)$ -άδες των συντελεστών τους.
- Το σύνολο των πρώτων αριθμών όπου ανήκει το q είναι υποσύνολο του \mathbb{N} , άρα αριθμήσιμο.
- Ο αρχικός κώδικας x_0 ανήκει στο αριθμήσιμο σύνολο \mathbb{N} .

Συνεπώς, το καρτεσιανό γινόμενο των 3 αυτών στοιχείων είναι αριθμήσιμο σύνολο, κάτι που μας δίνει τη δυνατότητα να προσπελάσουμε όλους τους δυνατούς συνδυασμούς που χρειαζόμαστε για να αποκτήσουμε πρόσβαση στον υπερυπολογιστή. Ο επαναληπτικός αλγόριθμος για αυτή τη διαδικασία είναι ο εξής:

1. Παραγωγή της επόμενης τριάδας στοιχείων μέσω απαρίθμησης. Αναδρομικά, η απαρίθμηση του αντίστοιχου καρτεσιανού γινομένου ξεκινά από τον πρώτο συνδυασμό.
2. Προσδιορισμός της χρονικής στιγμής απόπειρας πρόσβασης $t = t_{old} + 30$ όπου t_{old} η χρονική στιγμή της προηγούμενης απόπειρας. Αναδρομικά, το πρώτο t προσδιορίζεται στα 30 δευτερόλεπτα μετά το reset, τη χρονική στιγμή του οποίου γνωρίζουμε.
3. Προσδιορισμός του $x_{t+1} = P_d(x_t) \bmod q$ με γνωστές όλες τις παραμέτρους. Αναδρομικά, η πρώτη πράξη θα είναι $x_1 = P_d(x_0) \bmod q$. Αν το βήμα υπερβεί τα 30 s για να ολοκληρωθεί, το t θα αυξάνεται ανά 1 δευτερόλεπτο μέχρι την ολοκλήρωση.
4. Δοκιμή του κωδικού x_{t+1} . Αν γίνει δεκτός, ο αλγόριθμος τερματίζει. Αν όχι, επιστρέφουμε στο 1.

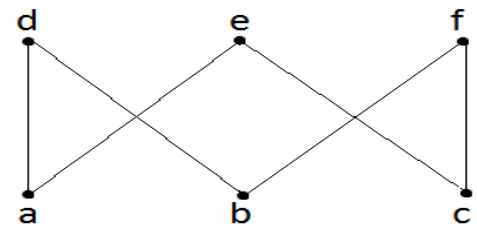
Ο αλγόριθμος είναι πεπερασμένος άρα εγγυάται το «σπάσιμο» του υπερυπολογιστή σε κάποιο χρόνο.

➤ Θέμα 2

- a) Αποδεικνύουμε πρώτα το ορθό: Έστω R μια ανακλαστική και κυκλική διμελής σχέση. Για να είναι σχέση ισοδυναμίας, θα πρέπει να είναι επίσης συμμετρική και μεταβατική. Αν στον ορισμό της κυκλικής ιδιότητας $\forall x \forall y \forall z [(x, y) \in R \wedge (y, z) \in R \rightarrow (z, x) \in R]$ θέσουμε $z = y$, έχουμε: $\forall x \forall y [(x, y) \in R \wedge (y, y) \in R \rightarrow (y, x) \in R]$. Δηλαδή, με δεδομένη την ανακλαστική ιδιότητα $\forall y (y, y) \in R$, παίρνουμε την συμμετρική $\forall x \forall y [(x, y) \in R \rightarrow (y, x) \in R]$. Αν τώρα με βάση την συμμετρική θέσουμε στον ορισμό της κυκλικής όπου $(z, x) \in R$ το $(x, z) \in R$, έχουμε: $\forall x \forall y \forall z [(x, y) \in R \wedge (y, z) \in R \rightarrow (x, z) \in R]$ που είναι ο ορισμός της μεταβατικής ιδιότητας. Επομένως, αν η R είναι ανακλαστική και κυκλική, τότε είναι σχέση ισοδυναμίας. Αποδεικνύουμε τώρα το αντίστροφο: Έστω R μια σχέση ισοδυναμίας (ανακλαστική, συμμετρική και μεταβατική). Πρέπει να δείξουμε ακόμα πως η R είναι κυκλική. Αν με βάση την συμμετρικότητα θέσουμε στον ορισμό της μεταβατικής όπου $(x, z) \in R$ το $(z, x) \in R$, έχουμε: $\forall x \forall y \forall z [(x, y) \in R \wedge (y, z) \in R \rightarrow (z, x) \in R]$ που είναι ο ορισμός της κυκλικής ιδιότητας. Τελικά, αποδεικνύεται πως **μια διμελής σχέση R είναι ανακλαστική και κυκλική ανν είναι σχέση ισοδυναμίας**.

- b) Το **διάγραμμα Hasse** με τα δοσμένα χαρακτηριστικά είναι το εξής:

- c) Η σχέση R είναι ανακλαστική και μεταβατική εξ ορισμού, δεν είναι όμως αντισυμμετρική, αφού για $n = 12 = 2 * 2 * 3$ και $m = 18 = 2 * 3 * 3$, $(n, m) \in R$ και $(m, n) \in R$. Επομένως, **η R δεν είναι σχέση μερικής διάταξης**.



- d) P είναι lattice ανν κάθε ζεύγος στοιχείων του **έχει ελάχιστο άνω φράγμα και μέγιστο κάτω φράγμα**. Σε πρωτοβάθμια λογική: $\text{lattice}(P) \equiv \forall x \forall y [P(x, x) \wedge (P(x, y) \wedge P(y, x) \rightarrow x = y) \wedge \forall z (P(x, z) \wedge P(y, z) \rightarrow P(x, z))] \wedge \exists c [P(c, x) \wedge P(c, y) \wedge \forall d ((P(d, x) \wedge P(d, y)) \rightarrow P(d, c))] \wedge \exists m [P(x, m) \wedge P(y, m) \wedge \forall n ((P(x, n) \wedge P(y, n)) \rightarrow P(m, n))]$ $\{P(x, y) \equiv x \leq y \text{ ως poset}\}$

➤ Θέμα 3

- a) Για τους A, B : Αν ο A ήταν ευγενής και έλεγε την αλήθεια, τότε και ο B θα ήταν ευγενής λόγω της δήλωσης του A . Ο B όμως λέει πως ο A είναι απατεώνας, άτοπο εν προκειμένω. Άρα **ο A είναι απατεώνας** και κατ' επέκταση **ο B είναι ευγενής**. Για τους C, D : Δεν μπορεί να είναι και οι 2 ευγενείς αφού κατά δήλωσή τους θα έπρεπε να είναι απατεώνες. Επίσης, δεν μπορεί να είναι και οι 2 απατεώνες, αφού κατά το αντίστροφο της δήλωσής τους θα έπρεπε να είναι ευγενείς. Άρα, **ένας ακριβώς από τους 2 είναι απατεώνας**. Αυτό συμβαδίζει με τις δηλώσεις τους αφού αν ο ένας είναι ευγενής, ο άλλος θα είναι απατεώνας, επιβεβαιώνοντας την ευγένεια του πρώτου. Για τους X, Y : Υπάρχουν 4 πιθανοί συνδυασμοί (EE, EA, AE, AA). Αν ο X απαντούσε ΝΑΙ δε θα μπορούσαμε να αποφανθούμε μεταξύ EE, EA και AA. Αν αντίθετα απάντησε ΟΧΙ, καταλήγουμε στην AE, αφού δεν μπορεί να είναι ευγενής και επίσης δε μπορεί να μην είναι κανένας ευγενής. Άρα, **ο X απάντησε ΟΧΙ όντας απατεώνας, ενώ ο Y είναι ευγενής**.
- b) Οι δηλώσεις των B, Γ είναι πάντα αληθείς καθώς ο καθένας από τους A, B, Γ μπορεί να είναι είτε ευγενής είτε απατεώνας είτε κατάσκοπος. Επομένως, ο μόνος που μπορεί να είναι απατεώνας είναι ο A . Αν αυτός τώρα είχε δηλώσει ότι ο Γ είναι απατεώνας, δε θα μπορούσαμε να αποφανθούμε αν ο Γ είναι ευγενής ή κατάσκοπος. Αν όμως ο A είχε δηλώσει ότι ο Γ είναι κατάσκοπος, μεταξύ ευγενή και απατεώνα, μπορούμε να συμπεράνουμε πως ο Γ είναι ευγενής. Επομένως, **ο ανακριτής συνέλαβε τον B ως κατάσκοπο. Ο A δήλωσε «Ο Γ είναι κατάσκοπος»**.

➤ Θέμα 4

- $\forall x \exists y [S(x) \wedge C(y) \wedge E(x, y)]$
- $\exists y \exists z [C(y) \wedge P(x) \wedge C(z) \wedge y \neq z \wedge T(x, y) \wedge T(x, z) \wedge \forall d (C(d) \wedge T(x, d) \rightarrow d = y \vee d = z)]$
x: Καθηγητής
- $\forall x \forall y [S(x) \wedge S(y) \wedge x \neq y \wedge F(x, y) \rightarrow \exists z (C(z) \wedge E(x, z) \wedge E(y, z))]$
- $\forall x [S(x) \wedge C(y) \wedge C(z) \wedge E(x, y) \rightarrow \neg E(x, z)]$
y: Διακριτά Μαθηματικά & z: Αριθμητική Ανάλυση
- $\forall x \forall y \forall z [S(x) \wedge P(y) \wedge C(z) \wedge T(y, z) \wedge E(x, z) \rightarrow F(x, y)]$

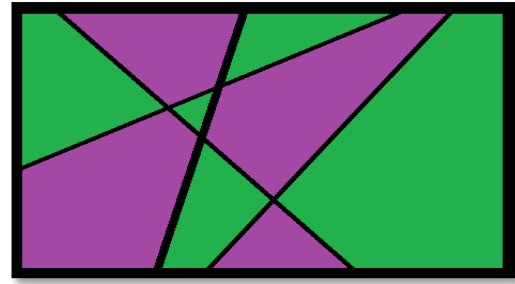
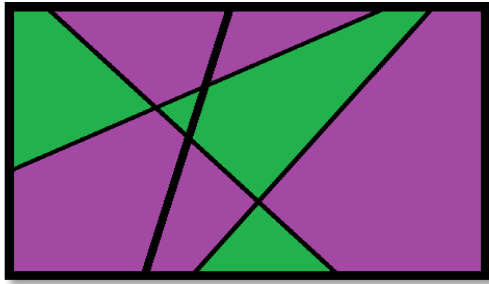
➤ Θέμα 5

1. Η πρόταση ψ_1 δηλώνει πως κάθε τριάδα στοιχείων που έχει τη μεταβατική και την συμμετρική ιδιότητα και που από κάθε στοιχείο μπορούμε να πάμε σε κάποιο άλλο, έχει την ανακλαστική ιδιότητα. Αυτό είναι πάντα αληθές, αφού αξιοποιώντας τις 2 πρώτες ιδιότητες μπορούμε ξεκινώντας από το x να επιστρέψουμε σε αυτό άμεσα. Επιπλέον, αυτό γίνεται καθολικά μιας και πάντα μπορούμε να φύγουμε από οποιοδήποτε στοιχείο, σύμφωνα με την τελευταία ιδιότητα. Επομένως **η ψ_1 είναι λογικά έγκυρη**. Από την πρόταση ψ_2 εξετάζουμε τον πρώτο όρο της σύζευξης: $\exists x \forall y (P(y) \rightarrow R(y, x))$. Επιλέγουμε ερμηνεία στο \mathbb{N} με $P(y) \equiv y \neq 0$, $R(y, x) \equiv y \leq x$. Ο όρος δηλώνει τώρα ότι υπάρχει φυσικός αριθμός για τον οποίο κάθε μη μηδενικός φυσικός είναι μικρότερός του, προφανώς ψευδής, άρα ψευδής (λόγω σύζευξης) και η πρόταση ψ_2 . Εφόσον βρήκαμε αντιπαράδειγμα, μπορούμε να συμπεράνουμε πως **η ψ_2 δεν είναι λογικά έγκυρη**. Σύμφωνα με την ίδια ερμηνεία, η πρόταση ψ_3 δηλώνει ότι για κάθε ζεύγος μη μηδενικών φυσικών αριθμών, όπου ο ένας είναι γνήσια μεγαλύτερος του άλλου, υπάρχει ένας τρίτος που είναι γνήσια μεγαλύτερος του μικρότερου και γνήσια μικρότερος του μεγαλύτερου. Αυτό δεν είναι αληθές στην περίπτωση 2 διαδοχικών φυσικών, επομένως **η ψ_3 δεν είναι λογικά έγκυρη**.
2. Εξετάζουμε την ερμηνεία στο σύνολο \mathbb{N} με $P(y) \equiv y$ άρτιος διψήφιος, $R(y, x) \equiv y \geq x$. Ο πρώτος όρος της ψ_2 δηλώνει τώρα ότι υπάρχει φυσικός αριθμός για τον οποίο κάθε άρτιος διψήφιος είναι μεγαλύτερός του, δηλαδή ότι είναι μονοψήφιος. Συνολικά η ψ_2 δηλώνει ότι υπάρχει μονοψήφιος φυσικός που είναι μεγαλύτερος από κάθε άλλο αριθμό που είναι επίσης μονοψήφιος (επανάληψη της μορφής του πρώτου όρου). Ο μονοψήφιος αυτός υπάρχει και είναι το 9, οπότε η ψ_2 ικανοποιείται. Η ψ_3 για αυτή την ερμηνεία δηλώνει ότι για κάθε ζεύγος άρτιων διψήφιων αριθμών, όπου ο ένας είναι γνήσια μεγαλύτερος του άλλου, υπάρχει ένας τρίτος αυθαίρετος αριθμός που είναι γνήσια μεγαλύτερος του μικρότερου και γνήσια μικρότερος του μεγαλύτερου, δηλαδή ότι ανάμεσα σε 2 άρτιους διψήφιους υπάρχει ένας άλλος φυσικός αριθμός. Αυτό είναι προφανώς αληθές. Επομένως, **η ερμηνεία στο \mathbb{N} με $P(y) \equiv y$ άρτιος διψήφιος, $R(y, x) \equiv y \geq x$ ικανοποιεί τις ψ_2, ψ_3** .
3. Σύμφωνα με την ερμηνεία που δίνεται, ο όρος $\exists x \forall y (P(y) \rightarrow R(y, x))$ δηλώνει ότι κάθε πεπερασμένο σύνολο του $2^{\mathbb{N}}$ είναι υποσύνολο ενός συνόλου x . Αυτό σημαίνει ουσιαστικά πως το x είναι ένα μη πεπερασμένο σύνολο στο $2^{\mathbb{N}}$. Συνολικά, η ψ_2 δηλώνει ότι υπάρχει μη πεπερασμένο σύνολο στο $2^{\mathbb{N}}$ που είναι υποσύνολο κάθε μη πεπερασμένου συνόλου στο $2^{\mathbb{N}}$, δηλαδή ότι υπάρχει ελάχιστο μη πεπερασμένο υποσύνολο του $2^{\mathbb{N}}$. Η πρόταση αυτή είναι ψευδής, καθώς το δυναμοσύνολο του \mathbb{N} δεν είναι αριθμήσιμο, άρα θα μπορούμε πάντα να βρίσκουμε ένα υποσύνολό του που δε θα είναι πεπερασμένο. Συνεπώς **η ψ_2 δεν ικανοποιείται**. Η ψ_3 δηλώνει ότι για κάθε ζεύγος πεπερασμένων συνόλων στο $2^{\mathbb{N}}$, όπου το ένα είναι γνήσιο υποσύνολο του άλλου, υπάρχει σύνολο στο $2^{\mathbb{N}}$ που δεν είναι υποσύνολο του ενός και υπερσύνολο του άλλου. Οι προϋποθέσεις αυτές πληρούνται καθώς το τρίτο σύνολο υπάρχει (θα είναι ξένο προς τα άλλα δύο). Συνεπώς **η ψ_3 ικανοποιείται**.

➤ Θέμα 6

- a) Χρησιμοποιούμε μαθηματική επαγωγή στο πλήθος n των ευθειών. **Επαγωγική Βάση:** Για $n = 1$ έχουμε επίπεδο που χωρίζεται σε 2 ημιεπίπεδα από μια ευθεία. Προφανώς το καθένα μπορεί να χρωματιστεί με διαφορετικό χρώμα, άρα η ιδιότητα ισχύει. **Επαγωγική Υπόθεση:** Υποθέτουμε ότι η ιδιότητα ισχύει για n ευθείες, δηλαδή οι περιοχές στις οποίες χωρίζεται ένα επίπεδο από n ευθείες μπορούν να χρωματιστούν με 2 διαφορετικά χρώματα, ώστε καμία να μη γειτονεύει με περιοχή ίδιου χρώματος. **Επαγωγικό Βήμα:** Θα αποδείξουμε την ιδιότητα για $n + 1$ ευθείες, χαράζουμε δηλαδή άλλη μια ευθεία στο επίπεδο. Παρατηρούμε πως οι μόνες περιοχές που δεν τηρούν τη ζητούμενη ιδιότητα είναι αυτές που γειτονεύουν μέσω της νέας ευθείας, στην ακμή μάλιστα επαφής τους με αυτή. Διαλέγουμε το ένα από τα 2 ημιεπίπεδα στα οποία χωρίζει η νέα ευθεία το επίπεδο και αντιστρέφουμε τον χρωματισμό των περιοχών του. Η ιδιότητα προφανώς διατηρείται εκεί όπου ίσχυε ήδη, ενώ πλέον και οι περιοχές που συνορεύουν με τη νέα ευθεία έχουν διαφορετικό χρωματισμό από αυτές με τις οποίες γειτονεύουν μέσω αυτής στο άλλο ημιεπίπεδο. Η διαδικασία γίνεται καλύτερα αντιληπτή στα σχήματα της επόμενης σελίδας. Συνεπώς, η ιδιότητα ισχύει για $n + 1$ ευθείες.

Έτσι: **οι περιοχές στις οποίες χωρίζεται ένα επίπεδο από ευθείες μπορούν να χρωματιστούν με 2 διαφορετικά χρώματα, ώστε καμία να μη γειτονεύει με περιοχή ίδιου χρώματος, ανεξαρτήτως πλήθους των ευθειών.**



b) Χρησιμοποιούμε μαθηματική επαγωγή στο πλήθος n των πόλεων. Επαγωγική Βάση: Για $n = 2$ έχουμε ένα δίκτυο 2 πόλεων (A, B) που συνδέονται εξ ορισμού μονομερώς (έστω $A \rightarrow B$). Υπάρχει προφανώς μετάθεση $[A B]$ κατά την οποία κάθε πόλη (A) συνδέεται απευθείας με την επόμενη της (B). Επαγωγική Υπόθεση: Υποθέτουμε ότι για n πόλεις A_1, A_2, \dots, A_n που συνδέονται απευθείας και μονομερώς ανά ζεύγη, υπάρχει αντίστοιχη μετάθεση με δείκτη αρίθμησης για ευκολία το n ($A_1 \rightarrow A_2 \rightarrow \dots \rightarrow A_n$). Επαγωγικό Βήμα: Θα αποδείξουμε ότι υπάρχει αντίστοιχη μετάθεση για $n+1$ πόλεις, προσθέτουμε δηλαδή στο δίκτυο την πόλη C που συνδέεται οδικά απευθείας και μονομερώς με όλες τις προηγούμενες. Με δεδομένη τη μετάθεση για τις n πόλεις, στην περίπτωση που υπάρχει σύνδεση $A_n \rightarrow C$, προσθέτουμε απλά τη νέα πόλη στο τέλος της μετάθεσης και η ιδιότητα τηρείται. Αν δεν υπάρχει αυτή η σύνδεση, θα υπάρχει η $C \rightarrow A_n$, θα πρέπει δηλαδή η πόλη να τοποθετηθεί κάπου πριν την τελευταία στη μετάθεση. Σε αυτή τη περίπτωση θα ελεγχθεί με όμοιο τρόπο η σύνδεση με την πόλη A_{n-1} . Αν η σύνδεση καταλήγει στη C τότε την τοποθετούμε αμέσως μετά την A_{n-1} (θα οδηγεί μετά αναγκαστικά στην A_n). Αν όχι, επαναλαμβάνουμε την ίδια διαδικασία σαρώνοντας προς τα κάτω τη μετάθεση. Ο αλγόριθμος είναι πεπερασμένος, καθώς στην ακραία περίπτωση που η σύνδεση με την A_0 δεν έχει κατάληξη τη C , θα υπάρχει η $C \rightarrow A_0$ οπότε η C θα τοποθετηθεί στην αρχή της μετάθεσης. Η ιδιότητα δηλαδή θα διατηρηθεί για τις $n + 1$ πόλεις.

Σε κάθε περίπτωση λοιπόν αποδείχθηκε πως **υπάρχει μετάθεση πόλεων, που συνδέονται απευθείας και μονομερώς ανά ζεύγη, τέτοια ώστε κάθε πόλη να οδηγεί απευθείας στην επόμενη της στη μετάθεση.**