Μαθηματικά Πληροφορικής

2ο Μάθημα

Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Πανεπιστήμιο Αθηνών

Μορφές αποδείξεων

Υπάρχουν πολλά είδη αποδείξεων. Εδώ θα δούμε τα πιο κοινά:

- Εξαντλητική μέθοδος ή μέθοδος επισκόπησης. Όταν το πρόβλημα έχει πεπερασμένο αριθμό περιπτώσεων, τις εξετάζουμε όλες.
- Μαθηματική επαγωγή. Έστω μια πρόταση $P(n)$ που ισχύει για $n = 1$. Αν η $P(n)$ συνεπάγεται την $P(n+1)$, τότε η πρόταση ισχύει για όλους τους φυσικούς.
- Δομική επαγωγή. Επαγωγή όχι στους φυσικούς αριθμούς αλλά σε μια δομή που ορίζεται επαγωγικά.

Μορφές αποδείξεων (συνέχεια)

- Κατασκευαστική απόδειξη ύπαρξης. Δείχνουμε την ύπαρξη ενός στοιχείου δίνοντας ένα αλγόριθμο που το παράγει. Στην ιδία κατηγορία ανήκει και η απόδειξη με αντιπαράδειγμα.
- Μη κατασκευαστική απόδειξη ύπαρξης. Τέτοιες αποδείξεις χρησιμοποιούν μεταξύ άλλων
    - την αρχή του περιστερεώνα και τις γενικεύσεις του
    - την πιθανοτική μέθοδο που βασίζεται στο ότι ένα στοιχείο υπάρχει όταν έχει μη μηδενική πιθανότητα ύπαρξης.
    - την διαγωνιοποίηση του Cantor.

Εξαντλητική μέθοδος

- Σε αυτό το είδος απόδειξης θεωρούμε όλες τις δυνατές περιπτώσεις και τις ελέγχουμε όλες. Αν ο αριθμός των περιπτώσεων είναι πεπερασμένος (και σχετικά μικρός) τότε αυτή είναι συνήθως η πιο κατάλληλη μέθοδος.
- Σήμερα που έχουμε στη διάθεση μας ισχυρούς υπολογιστές, αυτή η μέθοδος μπορεί να χρησιμοποιηθεί σε αρκετά προβλήματα.
- Ας δούμε μερικά παραδείγματα τέτοιων αποδείξεων.

Σκύλος-κατσίκα-χορτάρι

- Ένας βοσκός έχει έναν άγριο σκύλο, μια κατσίκα και ένα δεμάτι χορτάρι και θέλει να χρησιμοποιήσει μια βάρκα για να διασχίσει ένα ποτάμι.
- Η βάρκα είναι μικρή και χωράει μόνο το βοσκό και ένα από τα 3 πράγματα ή ζώα που θέλει να μεταφέρει απέναντι.
- Ο σκύλος θα φάει την κατσίκα και η κατσίκα το χορτάρι αν μείνουν χωρίς το βοσκό στην ίδια όχθη.
- Υπάρχει λυση;
- Ναι. Μπορούμε να τη βρούμε αν δοκιμάσουμε όλους τους συνδυασμούς.

Σκάκι

- Στα προβλήματα *'Ματ σε 3 κινήσεις'* μπορούμε να δοκιμάσουμε όλες τις περιπτώσεις. ($\sim 40^5$.)
- Είναι εφικτά σήμερα τα προβλήματα της μορφής *'Ματ σε 7 κινήσεις'*;
- *Δίνεται η αρχική σκακιέρα. Ματ σε 137 κινήσεις.* Αυτό το πρόβλημα είναι πεπερασμένο, αλλά όχι υπολογιστικά εφικτό.

Όρια της εξαντλητικής μεθόδου

Έστω πως έχουμε 2^n περιπτώσεις.

Οι «σύγχρονοι» υπολογιστές εκτελούν περίπου 2^{30} εντολές / δευτερόλεπτο. Μία ώρα έχει $3600 < 2^{12}$ δευτερόλεπτα, άρα $\sim 2^{42}$ εντολές / ώρα.

Ο ρυθμός αύξησης είναι τεράστιος. Για $n = 48$, θα χρειαζόμασταν 3 μέρες.

Για $n = 100$, $2^{100} = 2^{30}2^{70}$,
άρα χρειαζόμαστε 2^{70} δευτερόλεπτα, δηλαδή $> 2^{58}$ ώρες.
Ένας χρόνος έχει $8760 \simeq 2^{13}$ ώρες.
Άρα χρειαζόμαστε $\sim 2^{58-13} = 2^{45}$ χρόνια. Αυτό είναι παραπάνω από 30 τρισεκατομμύρια χρόνια...

Μα, οι υπολογιστές δεν γίνονται ολοένα ταχύτεροι;

Ποτέ δεν θα γίνουν αρκετά γρήγοροι για να ελέγξουν 2^{100} περιπτώσεις σε λογικό χρόνο.

Αν η ταχύτητα διπλασιαστεί σε $2(2^{30}) = 2^{31}$ εντολές/δευτ., πηγαίνεις από το $n = 30$ στο $n + 1 = 31$. (Αγνοώντας το κόστος για προσπέλαση στη μνήμη και το δίσκο).

Και πρέπει να περιμένεις περίπου 18 μήνες (σύμφωνα με Moore's law) για να συμβεί αυτό. Σε 18 χρόνια από σήμερα, ίσως μπορέσουμε να απαριθμήσουμε $2^{42+12} = 2^{54}$ περιπτώσεις σε μία ώρα.

Μα, οι υπολογιστές δεν γίνονται ολοένα ταχύτεροι;

Οι νόμοι της φυσικής υποδεικνύουν ότι η ταχύτητα των ηλεκτρονικών υπολογιστών δεν θα αυξάνεται για πάντα. Ακόμα και με μαζικό παραλληλισμό, με τεράστιο speedup π.χ., $1000 \simeq 2^{10}$, οι βελτιώσεις θα είναι ελάχιστες.

Για n λίγο παραπάνω από 100, δεν υπάρχει καμία ελπίδα. $2^{250} \simeq 10^{80}$ που είναι ο αριθμός των σωματιδίων στο σύμπαν εντός της εμβέλειας παρατήρησης μας.

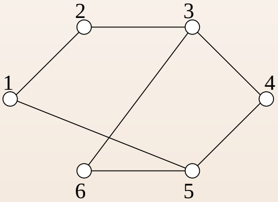
Εκτός εάν;...

Αριθμοί Ramsey

Πρόταση

Σε κάθε ομάδα 6 ατόμων

- *υπάρχουν 3 που γνωρίζονται ανά δυο*
- *ή υπάρχουν 3 που είναι άγνωστοι ανά δυο.*



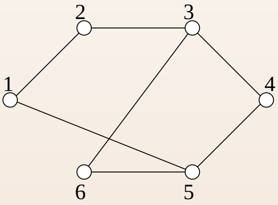
- Απόδειξη: Δοκίμασε όλες τις περιπτώσεις.

Αριθμοί Ramsey

Πρόταση

Σε κάθε ομάδα 6 ατόμων

- *υπάρχουν 3 που γνωρίζονται ανά δυο*
- *ή υπάρχουν 3 που είναι άγνωστοι ανά δυο.*



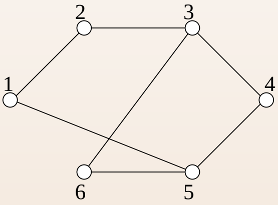
- Το παραπάνω δεν ισχύει για κάθε ομάδα 5 ατόμων. Αντιπαράδειγμα: Οι πέντε κάθονται σε ένα κυκλικό τραπέζι και ο καθένας γνωρίζει μόνο τους διπλανούς του.

Αριθμοί Ramsey

Πρόταση

Σε κάθε ομάδα 6 ατόμων

- *υπάρχουν 3 που γνωρίζονται ανά δυο*
- *ή υπάρχουν 3 που είναι άγνωστοι ανά δυο.*



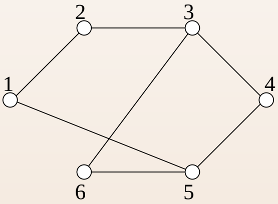
- Το παραπάνω δεν ισχύει για κάθε ομάδα 5 ατόμων. Αντιπαράδειγμα: Οι πέντε κάθονται σε ένα κυκλικό τραπέζι και ο καθένας γνωρίζει μόνο τους διπλανούς του.

Αριθμοί Ramsey

Πρόταση

Σε κάθε ομάδα 6 ατόμων

- *υπάρχουν 3 που γνωρίζονται ανά δυο*
- *ή υπάρχουν 3 που είναι άγνωστοι ανά δυο.*



- Το παραπάνω δεν ισχύει για ομάδες των 5 ατόμων. Αντιπαράδειγμα: Οι πέντε κάθονται σε ένα κυκλικό τραπέζι και ο καθένας γνωρίζει μόνο τους διπλανούς του.

Αριθμοί Ramsey

Μπορούμε να γενικεύσουμε την πρόταση

Θεώρημα

Σε καθε σύνολο 18 ατόμων υπάρχουν 4 που γνωρίζονται ανά δυο ή υπάρχουν 4 που είναι άγνωστοι ανά δυο.

Απόδειξη.

Δοκίμασε όλες τις περιπτώσεις. Όμως τώρα οι περιπτώσεις είναι πάρα πολλές. □

Αριθμοί Ramsey

Θεώρημα

Σε κάθε σύνολο 49 ατόμων υπάρχουν 5 που γνωρίζονται ανά δυο ή υπάρχουν 5 που είναι άγνωστοι ανά δυο.

Απόδειξη.

Η εξαντλητική μέθοδος δεν μπορεί να χρησιμοποιηθεί γιατί σήμερα είναι υπολογιστικά ανέφικτη. $\square$

Μαθηματική επαγωγή

Έστω $P(n)$ μια υπόθεση που αφορά τους φυσικούς αριθμούς. Για να αποδείξουμε την υπόθεση με επαγωγή

- Δείχνουμε ότι ισχύει για $n = 1$: $P(1)$
- Δείχνουμε για κάθε n: αν ισχύει για n τότε θα ισχύει για $n + 1$:
$$P(n) \Rightarrow P(n+1)$$

Παράδειγμα - H_k

- Ο αρμονικός αριθμός H_k ορίζεται σαν

$$H_k = 1 + \frac{1}{2} + \frac{1}{3} + \cdots \frac{1}{k}$$

- Τι μεγέθους είναι ο H_k;

Παράδειγμα - H_k

Λήμμα

Να δειχτεί ότι για κάθε φυσικό n: $H_{2^n} \leq 1 + n$.

Απόδειξη.

Βάση της επαγωγής: Για $n = 1$ έχουμε $H_{2^1} = H_2 = 3/2$ και $1 + n = 2$ και επομένως το λήμμα ισχύει: $3/2 \leq 2$.
Επαγωγική υπόθεση: Υποθέτουμε ότι το λήμμα ισχύει για κάποιο φυσικό αριθμό n: $H_{2^n} \leq 1 + n$.
Επαγωγικό βήμα: Θα δείξουμε ότι ισχύει για $n + 1$, δηλαδή ότι $H_{2^{n+1}} \leq 1 + (n + 1)$. $\square$

Παράδειγμα - H_k

Απόδειξη (συνέχ.)

Έχουμε

$$\begin{aligned} H_{2^{n+1}} &= 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^{n+1}} \\ &= (1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^n}) + (\frac{1}{2^n+1} + \cdots + \frac{1}{2^{n+1}}) \\ &= H_{2^n} + (\frac{1}{2^n+1} + \cdots + \frac{1}{2^{n+1}}) \\ &\leq (1+n) + (\frac{1}{2^n} + \cdots + \frac{1}{2^n}) \\ &= (1+n) + 2^n \frac{1}{2^n} = (1+n) + 1 = 1 + (n+1). \end{aligned}$$

$\square$

Μαθηματική επαγωγή - γενικεύσεις

Κάποιες κοινές παραλλαγές της επαγωγής

- Η βάση δεν είναι πάντα για $n = 1$. Π.χ., για θεωρήματα της μορφής «Για κάθε φυσικό αριθμό $n \geq 4$: ...» η βάση είναι $n = 4$.
- Η επαγωγική υπόθεση είναι ότι η πρόταση ισχύει για **όλους** τους μικρότερους αριθμούς:

$$P(1), \ldots, P(n) \Rightarrow P(n+1)$$

Αυτή είναι η λεγόμενη Ισχυρή Επαγωγή.

Οι αριθμοί Fibonacci

Οι αριθμοί Fibonacci ορίζονται ως εξής:

$$F_0 = 1, \quad F_1 = 1,$$

και για κάθε $n \geq 2$:

$$F_n = F_{n-1} + F_{n-2}.$$

Λήμμα

Να δειχτεί ότι για κάθε ακέραιο $n \geq 0$,

$$F_n \leq \phi^n,$$

όπου $\phi = \frac{1+\sqrt{5}}{2} = 1.618\ldots$ *είναι η χρυσή τομή.*

Θεώρημα

Για κάθε θετικό ακέραιο n: $\frac{1}{2}\phi^n \leq F_n \leq \phi^n$.

Συνδυαστική ερμηνεία των αριθμών Fibonacci

Ορίζουμε J_n ως τον αριθμό των τρόπων να γράψουμε το n ως άθροισμα ακολουθιών που αποτελούνται από 1 και 2. Π.χ., $J_4 = 5$ γιατί

$$1+1+1+1 = 1+1+2 = 1+2+1 = 2+1+1 = 2+2.$$

Ομοίως $J_1 = 1, J_2 = 2, J_3 = 3$ κοκ. Ορίζουμε $J_0 := 1$, και παίρνουμε (πώς;) για κάθε $n \geq 2$:

$$J_n = J_{n-1} + J_{n-2}$$

Άρα $J_n = F_n$, για κάθε n. *Ισοδύναμα*, J_n είναι ο αριθμός των τρόπων να ανέβεις μια σκάλα με n σκαλοπάτια αν κάθε φορά ανεβαίνεις ένα ή δύο σκαλιά ...

Οι αριθμοί Fibonacci

Θεώρημα

Να δειχτεί ότι για κάθε ακέραιους $n, m \geq 1$, οι αριθμοί Fibonacci ικανοποιούν τη σχέση

$$F_{n+m} = F_n F_m + F_{n-1} F_{m-1}.$$

Το θεώρημα μας επιτρέπει να υπολογίσουμε ένα αριθμό Fibonacci χωρίς να υπολογίσουμε όλους τους προηγούμενους.

$$F_{2k+1} = F_{k+1}F_k + F_kF_{k-1} = (F_k + F_{k-1})F_k + F_kF_{k-1} = F_k^2 + 2F_kF_{k-}$$

$$F_{2k} = F_kF_k + F_{k-1}F_{k-1} = F_k^2 + F_{k-1}^2$$

Παράδειγμα:

$$F_{31} = F_{15}^2 + 2F_{15}F_{14}$$

$$F_{15} = F_7^2 + 2F_7F_6$$

$$F_{14} = F_7^2 + F_6^2 \qquad F_7 = \dots, F_6 = \dots$$

(Επαγωγικές) Αποδείξεις στη Στοιχειώδη Αριθμοθεωρία

Ορισμός

Ένας θετικός ακέραιος $p > 1$, καλείται πρώτος αν δεν μπορεί να γραφτεί ως γινόμενο δύο ακεραίων a, b με $1 < a, b < p$.

Θεώρημα

Κάθε θετικός ακέραιος $n \geq 2$ μπορεί να γραφτεί ως γινόμενο πρώτων αριθμών.

Μέγιστος Κοινός Διαιρέτης

Για $a, b \in \mathbb{Z}$, λέμε ότι ο a διαιρεί τον b (συμβολίζεται με $a \mid b$), αν υπάρχει $k \in \mathbb{Z}$, τέτοιο ώστε $b = ka$.

Ορισμός

Για $a, b \in \mathbb{Z}$, ο μέγιστος κοινός διαιρέτης των a και b (συμβολίζεται με $\gcd(a, b)$), ορίζεται ως ο μεγαλύτερος ακέραιος d τ.ω. $d \mid a$ και $d \mid b$.

Εξ ορισμού, όλοι οι ακέραιοι διαιρούν το 0. Άρα $\gcd(0, b) = b$. Ορίζουμε $\gcd(0, 0) := 0$.

Αλγόριθμος για το Μέγιστο Κοινό Διαιρέτη

$$\gcd(a,b) = \begin{cases} a & \text{αν } b = 0 \\ \gcd(b, a \bmod b) & \text{αν } b > 0. \end{cases}$$

Αλγόριθμος του Ευκλείδη

function $\textsc{Euclid}(a, b)$ ▷ Υποθέτουμε ότι $a \geq b$
    if $b = 0$ **then**
        return a ▷ $gcd(a, 0) = a$
    else
        $\delta \leftarrow \textsc{Euclid}(b, a \bmod b)$ ▷ $gcd(a, b) = gcd(b, a \bmod b)$
        return δ
    end if
end function

Ορθότητα του Αλγορίθμου του Ευκλείδη

Θα αποδείξουμε με τη σειρά τις εξής προτάσεις.

Λήμμα (Bézout)

Έστω $a, b \in \mathbb{Z}$*, όχι και οι δύο μηδέν. Τότε* $\gcd(a, b) = \min\{ax + by \mid x, y \in \mathbb{Z},\ ax + by > 0\}$.

Λήμμα

Αν $d \mid a$ *και* $d \mid b$*, τότε* $d \mid \gcd(a, b)$.

Θεώρημα

Για ακέραιους $a \geq 0$ *και* $b > 0$, $\gcd(a, b) = \gcd(b, a \bmod b)$.

Πολυπλοκότητα του Αλγορίθμου του Ευκλείδη

- Πόσα βήματα κάνει ο αλγόριθμος για να υπολογίσει τον μέγιστο κοινό διαιρέτη δυο αριθμών; Εξαρτάται από τους αριθμούς. Θέλουμε μια εκτίμηση για τη χειρότερη περίπτωση.
- Το Θεώρημα του Lamé (δεν θα το αποδείξουμε) λέει ότι ο αριθμός των διαιρέσεων, ή ισοδύναμα οι φορές που υπολογίζουμε το $a \bmod b$, είναι λιγότερες από $k-1$ όταν $a > b \geq 1$ και $b < F_k$.
- Εδώ θα δείξουμε ένα πιο απλό αποτέλεσμα.

Πολυπλοκότητα του Αλγορίθμου του Ευκλείδη

Παρατηρούμε ότι ο αριθμός των διαιρέσεων ισούται με τον αριθμό r των αναδρομικών κλήσεων που εκτελεί ο αλγόριθμος. Συνεπώς ο αριθμός βημάτων του αλγορίθμου είναι $O(r)$.

Θεώρημα

Για κάθε θετικούς ακέραιους a, b με $a \geq 2$ και $a \geq b$, ο αριθμός των διαιρέσεων του αλγόριθμου του Ευκλείδη δεν ξεπερνά το $2\lfloor \log a \rfloor$.

Θεμελιώδες Θεώρημα της Αριθμοθεωρίας

Λήμμα

Αν $a \mid bc$ *και* $\gcd(a, b) = 1$, *τότε* $a \mid c$.

Λήμμα

Αν p *πρώτος και* $p \mid bc$, *τότε* $p \mid b$ *ή* $p \mid c$.

Λήμμα

Αν p *πρώτος και* $p \mid a_1 a_2 \ldots a_n$, *τότε ο* p *διαιρεί κάποιο* a_i.

Θεώρημα

Κάθε θετικός ακέραιος $n \geq 2$ *μπορεί να γραφτεί με μοναδικό τρόπο ως γινόμενο πρώτων αριθμών:*

$$n = p_1 \cdot p_2 \ldots p_j, \ (p_1 \leq p_2 \leq \ldots \leq p_j).$$

Ισχυροποίηση της πρότασης

Κάποιες φορές για να αποδείξουμε μια πρόταση με μαθηματική επαγωγή, παραδόξως μας συμφέρει να την ισχυροποιήσουμε. Παράδειγμα:

Πρόταση

$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2.$

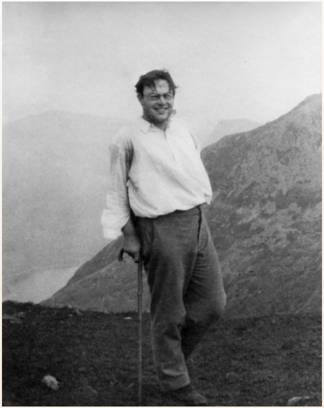
Απόδειξη.

Ας χρησιμοποιήσουμε επαγωγή και ας υποθέσουμε ότι η πρόταση ισχύει για κάποιο n. Προσθέτουμε και στα δυο μέλη το $\frac{1}{(n+1)^2}$. Αλλά, τώρα το δεξί μέλος είναι $2 + \frac{1}{(n+1)^2}$ που δεν είναι μικρότερο του 2. Η προσέγγιση αυτή αποτυγχάνει.

Είναι εύκολο όμως να δείξουμε την πιο ισχυρή πρόταση

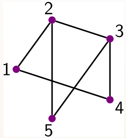
$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}. \quad \square$$

Θεωρία Ramsey



Frank P. Ramsey (1903-1930)

Γραφήματα



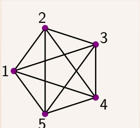
Γράφημα G με σύνολο κορυφών V και σύνολο ακμών E είναι ένα ζεύγος (V, E) όπου

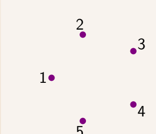
$$E \subseteq \{\{u, v\} \mid u, v \in V\}$$

δηλαδή μια ακμή είναι ένα μη διατεταγμένο ζεύγος κορυφών.

Ορισμός (Πλήρες / Κενό)

$G = (V, E)$ καλείται πλήρες (κλίκα) αν $E = \{\{u, v\} \mid u, v \in V\}$ και κενό (ανεξάρτητο σύνολο) αν $E = \varnothing$.





Θεωρία Ramsey

Θεώρημα (Ramsey)

Για κάθε φυσικό k, υπάρχει φυσικός $R(k)$ τέτοιος ώστε κάθε γράφημα με $R(k)$ ή περισσότερες κορυφές περιέχει ένα πλήρες υπογράφημα με k κορυφές ή ένα κενό υπογράφημα με k κορυφές.

Η πρόταση για κάποιο k δεν φαίνεται να συνεπάγεται την πρόταση για κάποιο $k+1$.
Αν όμως γενικεύσουμε το θεώρημα, τότε μπορούμε να το αποδείξουμε με επαγωγή.

Θεώρημα (Ramsey)

Για κάθε θετικούς ακέραιους $k, m \geq 2$ υπάρχει φυσικός $R(k, m)$ τέτοιος ώστε κάθε γράφημα με $R(k, m)$ ή περισσότερες κορυφές περιέχει ένα πλήρες υπογράφημα με k κορυφές ή ένα κενό υπογράφημα με m κορυφές.

Απόδειξη Θεωρήματος Ramsey

Θεώρημα (Ramsey)

Για κάθε θετικούς ακέραιους $k, m \geq 2$ υπάρχει φυσικός $R(k, m)$ τέτοιος ώστε κάθε γράφημα με $R(k, m)$ ή περισσότερες κορυφές περιέχει k-κλίκα ή m-ανεξάρτητο σύνολο.

Η επαγωγική απόδειξη απαιτεί λίγη προσοχή στις αρχικές συνθήκες.

Πρόταση

Για κάθε θετικούς ακέραιους $k, m \geq 2$, $R(k, 2) = k$ και $R(2, m) = m$.

Θα αποδείξουμε το Θεώρημα του Ramsey με ισχυρή επαγωγή στο άθροισμα $k + m$.
ΒΑΣΗ: Για $k + m = 4$, ισχύει από την Πρόταση. Ομοίως και για $k + m = 5$, αφού τότε ο ένας από τους k, m ισούται με 2.

Απόδειξη Θεωρήματος Ramsey

ΒΑΣΗ: Για $k+m=4$ και $k+m=5$, ισχύει από την Πρόταση.

ΕΠΑΓΩΓΙΚΗ ΥΠΟΘΕΣΗ: Ισχύει για $k,m \geq 2$ με $k+m \geq 5$.

ΕΠΑΓΩΓΙΚΟ ΒΗΜΑ: Θα δείξουμε για αριθμούς $k,m \geq 2$ με $k+m \geq 6$. (Άρα χβτγ $k,m \geq 3$).
Η επαγωγική υπόθεση διασφαλίζει την ύπαρξη των $R(k-1,m)$ και $R(k,m-1)$ (αφού $k+m-1 \geq 5$, και $k-1, m-1 \geq 2$).

Θα δείξουμε ότι υπάρχει το $R(k,m)$ και μάλιστα

$$R(k,m) \leq R(k-1,m) + R(k,m-1) + 1.$$