Μαθηματικά Πληροφορικής 2011-2012

4ο Σύνολο Ασκήσεων

Λυσεις

Πρόβλημα 1.

1. $n = pq = 7 \cdot 11 = 77$.
2. $\varphi(n) = (p-1)(q-1) = (7-1)(11-1) = 60$.
3. Επιλύοντας την εξίσωση $e \cdot d = 1 \mod \varphi(n) \iff 7 \cdot d = 1 \mod 60$, βρίσκουμε ένα $d = 43$.
4. Το δημόσιο κλειδί της Αλίκης είναι το $(n, e) = (77, 7)$ και το $(p, q, d) = (7, 11, 43)$ είναι το μυστικό της.
5. Ο Βασίλης κρυπτογραφεί και στέλνει στην Αλίκη το μήνυμα $M = 31$, αφού $T^e = 3^7 = 31 \mod 77$.
6. Η Αλίκη αποκρυπτογραφεί το αρχικό μήνυμα $T = 3$ από το μήνυμα $M = 31$, αφού $M^d = 31^{43} = 3 \mod 77$.

Πρόβλημα 2. Αφού $f(n) = O(g(n))$, υπάρχουν σταθερές $n_0 \in \mathbb{N}$ και $c \in \mathbb{R}^+$ τέτοιες ώστε

$$f(n) \leq c \cdot g(n) \quad \text{για κάθε } n \geq n_0.$$

Χωρίς βλάβη μπορούμε να θεωρήσουμε πως $c > 1$ (αλλιώς αντικαθιστούμε απλά την σταθερά c με την $\max\{c, 1\}$ και η σχέση συνεχίζει να ισχύει λόγω της φοράς της ανισότητας). Παίρνοντας λογαρίθμους και στα δύο μέλη της παραπάνω ισότητας έχουμε πως για κάθε $n \geq n_0$,

$$\log f(n) \leq \log(cg(n)) = \log c + \log g(n)$$

και αφού $g(n) \geq 2$, δηλαδή $\log g(n) \geq 1$, έχουμε

$$\log f(n) \leq (\log c + 1) \log g(n),$$

όπου $\log c + 1 > 0$ (αφού $c > 1$), που σημαίνει πως πράγματι $\log f(n) = O(\log g(n))$.

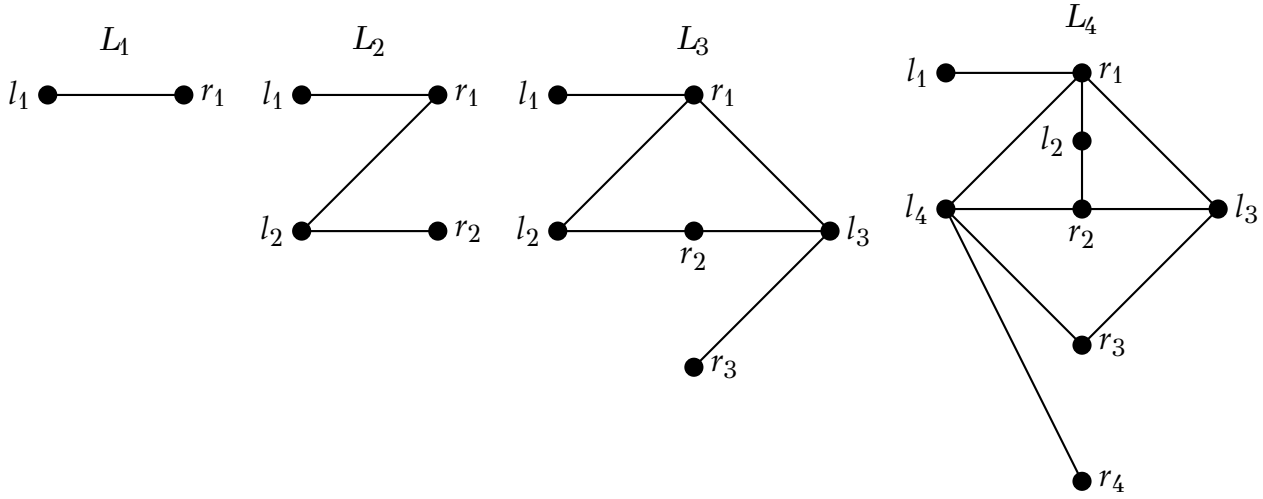
Εάν αφαιρέσουμε τον περιορισμό $g(n) \geq 2$, η πρόταση *δεν* ισχύει. Για παράδειγμα, θεωρείστε τις συναρτήσεις $f(n) = 2$ και $g(n) = 2^{\frac{1}{n}} < 2$ για $n > 1$. Τότε, είναι $\log f(n) = \log 2 = 1$ και $\log g(n) = \log 2^{\frac{1}{n}} = \frac{1}{n}$, και δεν ισχύει $1 = O(\frac{1}{n})$ αφού $\frac{1}{n} \to 0$.

Πρόβλημα 3. Παρατηρούμε πως για κάθε $n \geq 1$, ο γράφος L_n είναι διμερής (και συνεκτικός), με $|V| = n + n = 2n$ και $|E| = \sum_{i=1}^{n} \sum_{j=1}^{i} 1 = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$, οπότε έχουμε την εξής αναγκαία συνθήκη[1] για να είναι επίπεδος:

$$|E| \leq 2|V| - 4 \iff \frac{n(n+1)}{2} \leq 2 \cdot 2n - 4 \iff n^2 - 7n + 8 \leq 0 \iff n \in \left[\frac{7+\sqrt{17}}{2}, \frac{7-\sqrt{17}}{2}\right],$$

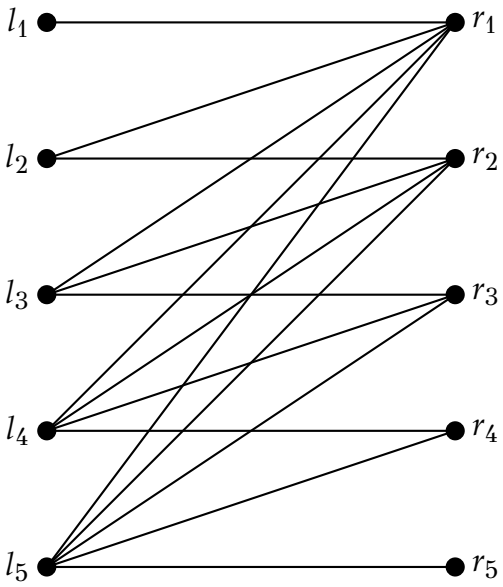
και αφού ο n είναι φυσικός, συμπεραίνουμε πως για $n \geq 6$ ο γράφος L_n *δεν* είναι επίπεδος.

Ας εξετάσουμε τώρα τις περιπτώσεις για $n = 1, 2, \ldots, 5$. Θα δείξουμε πως για $n \leq 4$ οι γράφοι είναι επίπεδοι, ενώ για $n = 5$ δεν είναι. Πράγματι, οι επίπεδοι σχεδιασμοί των L_1, L_2, L_3 και L_4 φαίνονται παρακάτω:

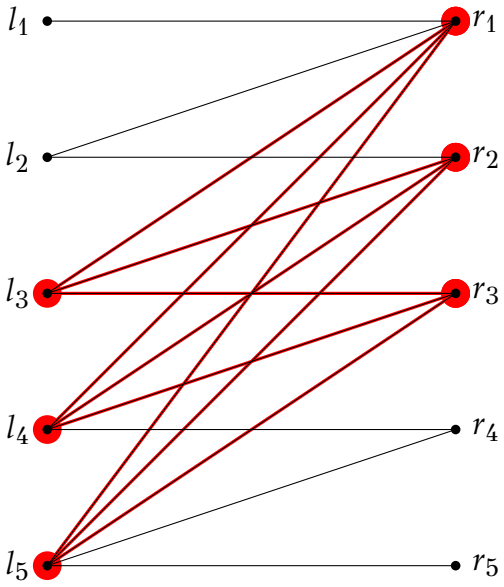


Για τον L_5 τώρα, ένας τρόπος να δούμε πως *δεν* είναι επίπεδος είναι το ότι ο *μη* επίπεδος γράφος $K_{3,3}$ είναι υπογράφος του, όπως φαίνεται και στο παρακάτω σχήμα:

[1] "Σε κάθε συνεκτικό διμερή επίπεδο γράφο ο αριθμός των κόμβων n και των ακμών m ικανοποιεί την σχέση $m \leq 2n - 4$." (σελ. 117 σημειώσεων μαθήματος) Παρατηρείστε πως "σιωπηλά" υποθέτουμε σε αυτό το θεώρημα πως $m \geq 4$ έτσι ώστε να μπορεί να αποδειχθεί από το τύπο του Euler. Σε αντίθετη περίπτωση, αν δηλαδή $m \leq 3$, ο γράφος μας είναι έτσι κι αλλιώς τετριμμένα επίπεδος.



Ο γράφος L_5



Ένας $K_{3,3}$ υπογράφος του

Πρόβλημα 4. Ο νέος αλγόριθμος επιστρέφει την σωστή απάντηση, αν και μόνο αν η σωστή απάντηση επιστρέφεται σε τουλάχιστον δύο από τις τρεις *ανεξάρτητες* εκτελέσεις του αρχικού αλγορίθμου (στην ίδια είσοδο). Αυτό το ενδεχόμενο (που είναι ουσιαστικά ένα πείραμα ρίψης ενός νομίσματος με πιθανότητα επιτυχίας q) έχει πιθανότητα τουλάχιστον

$$\sum_{m=2}^{3} \binom{3}{m} q^m (1-q)^{3-m} = \binom{3}{2} q^2(1-q) + \binom{3}{3} q^3 = q^2(3-2q).$$

Επιλύοντας την ανίσωση $q^2(3-2q) > q$ λοιπόν, βλέπουμε πως ο νέος αλγόριθμος έχει μεγαλύτερη πιθανότητα επιτυχίας αν και μόνο αν η αρχική πιθανότητα επιτυχίας είναι πάνω από 50%, δηλαδή όταν $q \in \left(\frac{1}{2}, 1\right)$.