Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών
Προηγμένα Θέματα Αλγορίθμων (Ροή Λ) – Εαρινό Εξάμηνο 2018-2019
Αβραμίδης Κλεάνθης – 03115117

3η Σειρά Ασκήσεων – Απαντήσεις

- **Άσκηση 1**

Καλούμαστε να αποδείξουμε το Finite Subgroup Test. Το ευθύ μέρος αποδεικνύεται με προφανή τρόπο καθώς εξ ορισμού, το H είναι υποομάδα του G όταν είναι υποσύνολό του και κλειστό ως προς την πράξη της ομάδας. Μένει λοιπόν να αποδείξουμε ότι η κλειστότητα ως προς την πράξη της ομάδας συνεπάγεται την ιδιότητα της υποομάδας:

Ένα σύνολο $H \subseteq G$ είναι υποομάδα του G αν ισχύουν τα εξής:

- Το H είναι μη κενό (μπορούμε να το υποθέσουμε εδώ χωρίς βλάβη της γενικότητας)
- Το H είναι κλειστό ως προς την πράξη της ομάδας (το έχουμε εδώ ως υπόθεση)
- Για κάθε στοιχείο x του H θα πρέπει να ορίζεται ο αντίστροφός του x^{-1} (μένει να το δείξουμε)

Καταρχάς, αν $a = e$ (ουδέτερο στοιχείο), τότε εξ ορισμού $a^{-1} = a \in H$. Συνεπώς θεωρούμε $a \neq e$. Έστω η ακολουθία $a, a^2, a^3, \dots$ Λόγω κλειστότητας από υπόθεση, κάθε στοιχείο της ακολουθίας αυτής θα ανήκει στο H. Επειδή όμως το H είναι πεπερασμένο, ως υποσύνολο του πεπερασμένου συνόλου G, δε θα είναι όλα τα στοιχεία της ακολουθίας διαφορετικά. Υποθέτουμε λοιπόν $a^i = a^j$ για $i > j$ χβγ. Θα ισχύει $a^{i-j} = e$ κι επειδή $a \neq e$: $i - j > 1$:

$$e = a^{i-j} = aa^{i-j-1} \rightarrow a^{i-j-1} = a^{-1}$$

Επειδή $i - j > 1$ θα ισχύει $i - j - 1 \geq 1$ άρα $a^{i-j-1} = a^{-1} \in H$. Συνεπώς αποδείξαμε το ζητούμενο.

- **Άσκηση 2**

Θα αποδείξουμε πρώτα πως κάθε 2 cosets μιας υποομάδας H συνόλου G είτε ταυτίζονται είτε είναι ξένα μεταξύ τους. Θα επικεντρωθούμε χωρίς βλάβη της γενικότητας στα right cosets, καθώς ανάλογη απόδειξη υφίσταται και για τα left cosets. Έστω Ha, Hb δύο right cosets και έστω ότι δεν είναι ξένα. Τότε θα μοιράζονται ένα κοινό στοιχείο c για το οποίο θα ισχύει $c = ha = h'b$ με $h, h' \in H$ (βλ. ορισμό coset από διαφάνειες μαθήματος). Από αυτή τη σχέση λαμβάνουμε $a = h^{-1}h'b$ κι επειδή το H είναι υποομάδα, $h^{-1}h' = h'' \in H$. Θα έχουμε

$$a = h''b \rightarrow Ha = H(h''b) = (Hh'')b = Hb$$

Συνεπώς τα 2 cosets ταυτίζονται, αν δεν είναι ξένα. Για την απόδειξη θεωρήσαμε ότι $Hh'' \equiv H$. Αυτό μπορούμε να το αποδείξουμε ως εξής: Το $h'' = g$ είναι όπως είπαμε στοιχείο του H. Θα ισχύει όμως και το εξής:

$$g' = g'(g^{-1}g) = (g'g^{-1})g \in Hg = Hh''$$

το οποίο μας λέει πως το H ανήκει στο Hh''. Τελικά τα 2 σύνολα ταυτίζονται και η απόδειξη ολοκληρώνεται.

Πριν το Θ. Lagrange θα χρειαστεί να δείξουμε και ότι κάθε σύμπλοκο του H θα είναι ίδιας πληθικότητας με αυτό. Θεωρούμε την αντιστοίχιση $f: H \rightarrow Ha$ με τύπο $f(h_i) = h_i a$ που είναι κατά προφανή τρόπο onto καθώς και 1-1:

$$f(h_i) = f(h_j) \rightarrow h_i a = h_j a \rightarrow h_i = h_j$$

Από αυτά προκύπτει πως το πλήθος των στοιχείων ενός coset είναι ίδιο με το πλήθος στοιχείων του H. Αποδεικνύουμε τώρα το Θεώρημα Lagrange:

Έστω H υποομάδα του πεπερασμένου συνόλου G, με πληθικότητες $|H| = m$ και $|G| = n$. Συνεπώς κάθε coset του H θα έχει επίσης m στοιχεία. Χρησιμοποιώντας την πρώτη ιδιότητα που δείξαμε μπορούμε να διαμερίσουμε το G:

$$|G| = |g_1 * H| + |g_2 * H| + \cdots + |g_r * H| = |H| + |H| + \cdots + |H| = r|H| = rm$$

Αν δηλαδή r ο αριθμός των στοιχείων σε κάθε coset της διαμέρισης, τότε $n = rm$, οπότε θα ισχύει πράγματι ότι

$$|G| = |G/H| * |H|$$

- **Άσκηση 3**

Μοντελοποιούμε το πρόβλημα ως εξής: Έστω G το σύνολο των ατόμων του βασιλείου και έστω η πράξη $x * y$ που ορίζεται ως «το άτομο x του βασιλείου τραυμάτισε το άτομο y του βασιλείου». Ορίζουμε δηλαδή την ομάδα $(G,*)$ για την οποία αναγνωρίζουμε τις παρακάτω ιδιότητες:

Καταρχάς η ομάδα είναι κλειστή ως προς την πράξη της. Έπειτα, υπάρχει ουδέτερο στοιχείο τέτοιο, ώστε: $x * e = x$. Στην περίπτωσή μας το ουδέτερο στοιχείο είναι ο Καλικάντζαρος, αφού όποιος τραυματίζει με το μαχαίρι του, τραυματίζει τον εαυτό του. Υπάρχει επίσης ο αντίστροφος x^{-1} κάθε στοιχείου x του G. Στην περίπτωσή μας αντίστροφο στοιχείο είναι ο θανάσιμος εχθρός, αφού κάθε άνθρωπος τραυματίστηκε με το μαχαίρι του θανάσιμου εχθρού του από τον Καλικάντζαρο. Τέλος, παρατηρούμε πως ισχύει η προσεταιριστικότητα $(x * y) * z = x * (y * z)$ αφού ο y τραυματίζεται με το μαχαίρι του z. Με βάση αυτά τα δεδομένα και θεωρώντας Δ=Δρακομάνα, Γ=Γιάννης Χιονάς, Τ=Τζοφραίος Αντιπαθητικός, έχουμε τα εξής πορίσματα:

i. Έχουμε από υπόθεση ότι $\Gamma * T = \Delta$. Επίσης, $|G| = 2^{19} - 1$, δηλαδή η τάξη της ομάδας είναι περιττός αριθμός. Επομένως η ομάδα είναι κυκλική και η τάξη κάθε στοιχείου διαιρεί την τάξη της:

$$|G| = |g| \in G \ \rightarrow \ g \ \gamma\varepsilon\nu\nu\acute{\eta}\tau o\rho\alpha\varsigma$$

Συνεπώς ισχύει η αντιμεταθετική ιδιότητα: $T * \Gamma = \Delta$. Συνεπώς η απάντηση είναι πάλι η Δρακομάνα.

ii. Αναζητούμε το $\Delta * \Delta$. Ισχύει $\Delta * T = e$ και $\Gamma * T = \Delta$:

$$(\Gamma * T) * \Delta = \Delta * \Delta \ \rightarrow \ \Gamma * (T * \Delta) = \Gamma * (\Delta * T) = \Gamma * e = \Delta * \Delta$$

Τελικά $\Delta * \Delta = \Gamma$ άρα ο Γιάννης ο Χιονάς.

iii. Ζητάμε να μάθουμε ποιος τραυμάτισε αυτόν που τραυμάτισε τον Τζοφραίο με το ίδιο του το μαχαίρι $(T * T)$ με το μαχαίρι αυτού που μαχαίρωσε τον Γιάννη με το ίδιο του το μαχαίρι $(\Gamma * \Gamma)$. Συνεπώς ζητάμε το $(T * T) * (\Gamma * \Gamma)$. Έχουμε:

$$(T * T) * (\Gamma * \Gamma) = T * (T * \Gamma) * \Gamma = \ T * \Delta * \Gamma = (T * \Delta) * \Gamma = e * \Gamma = \Gamma$$

Άρα η απάντηση είναι ο Γιάννης ο Χιονάς.

- **Άσκηση 4**

Θεωρούμε έλεγχο Miller-Rabin για $n = p^\alpha$ όπου $\alpha > 1$. Θα αποδείξουμε καταρχάς ότι οι περιπτώσεις αποτυχίας του αλγόριθμου είναι λύσεις του $a^{p-1} \equiv 1 \, mod \, n$ και συγκροτούν ομάδα υπό την πράξη του πολλαπλασιασμού mod n. Έστω $a \in \{2,3, \dots, n-1\}$ ένα Miller-Rabin nonwitness. Επειδή α και n είναι σχετικά πρώτοι, το θεώρημα του Euler μας λέει ότι $a^{\varphi(n)} \equiv 1 \, mod \, n$. Από την ιδιότητα του nonwitness προκύπτει $a^k \equiv 1 \, mod \, n$ ή $a^{2^i k} \equiv -1 \, mod \, n$. Από αμφότερες τις περιπτώσεις λαμβάνουμε $a^{n-1} \equiv 1 \, mod \, n$. Συνεπώς το $a \, mod \, n$ διαιρεί το

$$(\varphi(n), n-1) = (p^{\alpha-1}(p-1), p^\alpha - 1) = p - 1$$

αφού p και $p^\alpha - 1$ είναι σχετικά πρώτοι και $p-1$ διαιρεί το $p^\alpha - 1$. Τελικά $a^{p-1} \equiv 1 \, mod \, p^\alpha = n$. Ανάποδα, αν θεωρήσουμε ότι $a^{p-1} \equiv 1 \, mod \, p^\alpha$ μπορούμε να γράψουμε $p - 1 = 2^f l, \ f \geq 1, \ l \, odd$. Το $p-1$ είναι παράγοντας του $p^\alpha - 1 = 2^e k$, συνεπώς $f \leq e, \ l | k$. Από τη στιγμή που $\left(a^l\right)^{2^f} \equiv 1 \, mod \, p^a$, η τάξη του $a^l \, mod \, p^a$ είναι 2^j για $j \in \{0, \dots, f\}$. Αν $j = 0$ τότε $a^k \equiv 1 \, mod \, p^a$ με $l | k$. Αν τώρα $j > 0$ τότε $x \coloneqq \left(a^l\right)^{2^{j-1}}$ ικανοποιεί το $x \not\equiv 1 \, mod \, p^l$. Θα ισχύει όμως $x^2 \equiv 1 \, mod \, p^l$. Συνεπώς $p^l | (x+1)(x-1)$ και το πολύ ένας εκ των όρων του δεξιού μέλους θα διαιρείται από το p. Δηλαδή $p^l | (x+1)$ ή $p^l | (x-1)$ ώστε $x \not\equiv \pm 1 \, mod \, p^l \ \rightarrow x \equiv a^{l 2^{j-1}} \equiv -1 \, mod \, p^l$. $l | k$ και k περιττός. Ανεβάζοντας κάθε πλευρά στη k/l δύναμη και λαμβάνουμε αποτέλεσμα:

$$a^{2^i k} \equiv -1 \, mod \, p^\alpha$$

Θα αποδείξουμε τώρα ότι για αυτή τη διάταξη, η πιθανότητα να έχουμε nonwitness είναι μικρότερη από 50%. Συγκεκριμένα θα αποδείξουμε το ζητούμενο δείχνοντας ότι τα nonwitnesses περιέχονται σε κανονική υποομάδα των αντιστρέψιμων αριθμών mod n. Μία υποομάδα μιας ομάδας έχει μέγεθος ίσο το πολύ με το μισό της, συνεπώς οι επιτυχίες του αλγόριθμου γενικά για n\in{1,…,n-1} περιλαμβάνουν τουλάχιστον τους μισούς αντιστρέψιμους αριθμούς mod n (δε περιέχει το 1 και το n-1) ενώ περιλαμβάνει και όλους τους μη αντιστρέψιμους αριθμούς mod n σε αυτό το διάστημα (υπάρχουν αφού γενικά n σύνθετος). Δηλαδή το πλήθος των επιτυχιών του αλγόριθμου είναι άνω του 50%, έστω W. Θα πρέπει να εξαιρέσουμε όμως τα 1, n-1 αφού δε μπορεί να είναι witnesses. Επομένως:

$$\frac{W}{n-1} > \frac{1}{2} \;\rightarrow\; \frac{W}{n-3} > \frac{W}{n-1} > \frac{1}{2}$$

που είναι το ζητούμενο. Μένει να δείξουμε πως τα nonwitnesses περιέχονται σε κανονική υποομάδα των αντιστρέψιμων αριθμών mod n. Αξιοποιούμε εδώ τη μορφή του n όπως δίνεται στην εκφώνηση. Αποδείξαμε πριν πως για αυτή τη μορφή τα Miller-Rabin nonwitnesses είναι λύσεις του $a^{p-1} \equiv 1 \, mod \, n$ και συγκροτούν ομάδα υπό την πράξη του πολλαπλασιασμού mod n. Ένα τέτοιο α δεν διαιρείται από το p, ενώ υπάρχουν αντιστρέψιμοι αριθμοί mod n με τάξη ώστε να διαιρούνται από p, πχ το 1+p. Αυτό αρκεί προκειμένου να συνάγουμε το ζητούμενο.

- **Άσκηση 5**

Θεωρούμε παράμετρο του προβλήματος το μέγεθος του Dominating Set, έστω k. Δουλεύοντας εξαντλητικά, μπορούμε να παράγουμε όλα τα μεγέθους k υποσύνολα κορυφών του γράφου και να ελέγξουμε γραμμικά σε καθένα από αυτά αν είναι Dominating Set του γράφου. Θα έχουμε $\binom{n}{k} = O(n^k)$ σύνολα για να ελέγξουμε σε γραμμικό χρόνο το καθένα. Συνεπώς η συνολική πολυπλοκότητα του προτεινόμενου αλγόριθμου είναι $O(n^k)$.

Για να ανήκει ένας αλγόριθμος στην FPT θα πρέπει να έχει χρονική πολυπλοκότητα της μορφής $O(f(k)n^{O(1)})$ κάτι που δεν ισχύει για τον προτεινόμενο. Μάλιστα, είναι αδύνατο να βρεθεί FPT αλγόριθμος για το Dominating Set Problem καθώς ως γνωστόν το πρόβλημα ανήκει στην κλάση W[2] και αυτό θα σήμαινε FPT=W[1]=W[2]. Σε περίπτωση που προσθέσουμε σαν παράμετρο και το φράγμα Δ στον βαθμό του γράφου εισόδου θεωρούμε ουσιαστικά την περίπτωση ενός Δ-degenerate γράφου. Σε αυτή την περίπτωση μπορεί να εξαχθεί FPT αλγόριθμος: Επιλέγουμε τον undominated κόμβο ελάχιστου βαθμού. Για τον κόμβο αυτό υπάρχουν 2 περιπτώσεις, είτε ο κόμβος θα βρίσκεται στη λύση, είτε ένα υποσύνολο των γειτόνων του. Σημειώνουμε τους dominated κόμβους, διαγράφουμε τον αρχικό και επαναλαμβάνουμε. Καταλήγουμε προφανώς σε Dominating Set, με πολυπλοκότητα $O(\Delta^k n)$. Ο αλγόριθμος λοιπόν ανήκει στο FPT αφού έχει πολυπλοκότητα της μορφής $O(f(k)n^{O(1)})$.

- **Άσκηση 6**

Έστω γράφημα G, δέντρο T του G και $V = \bigcup_{t \in T} V_t$ ένα tree decomposition του G. Έστω $H \leq G$ μια κλίκα του G. Καλούμαστε να αποδείξουμε πως κάθε κλίκα εμπεριέχεται σε κάποιο V_t του V, ισοδύναμα $tw(G) \geq w(G) - 1$ όπου $tw(G)$ το treewidth και $w(G)$ το μέγεθος της μέγιστης κλίκας. Θα το αποδείξουμε με επαγωγή.

Καταρχάς το ζητούμενο ισχύει κατά προφανή τρόπο για $w(G) = 2$, από τον ορισμό του treewidth. Υποθέτουμε επίσης πως ισχύει για $w(G) = k$ και θεωρούμε κλίκα S μεγέθους $k + 1$. Επιλέγουμε έναν κόμβο της κλίκας, έστω u, και θεωρούμε $S_0 = S - \{u\}$. Από υπόθεση, υπάρχει $t \in T$ τέτοιο ώστε $S_0 \in V_t$. Έστω T_0 το σύνολο όλων αυτών των t. Αν κάποιο V_t από αυτά περιέχει το u, η απόδειξη ολοκληρώνεται καθώς $S \subseteq V$. Αν όχι: Το σύνολο $T - T_0$ είναι δάσος. Αν $t_1, t_2 \in T - T_0$ ανήκουν σε διαφορετικές συνεκτικές συνιστώσες και $u \in V_{t_1} \cap V_{t_2}$ τότε θα πρέπει να περιέχεται και στο μονοπάτι που τα συνδέει, σε όλους τους κόμβους. Ένα τέτοιο μονοπάτι ωστόσο θα περιείχε το T_0, άτοπο. Συνεπώς υπάρχει μοναδική συνεκτική συνιστώσα C του $V_{t_1} \cap V_{t_2}$ που περιέχει το u. Μάλιστα, u και T_0 συνδέονται με μοναδική ακμή (t_0, c_0).

Για κάθε $u \in S_0$ υπάρχει $t \in T$ τέτοιο ώστε η ακμή να ανήκει στο V_t. Αυτό προκύπτει από τον ορισμό του tree decomposition καθώς πρόκειται για ακμή της κλίκας S. Συνεπώς κάθε u πρέπει να ανήκει στο C. Το μονοπάτι από κάθε τέτοιο κόμβο στο t_0 θα πρέπει να περιλαμβάνει την ακμή και να περνάει από το c_0. Επειδή επιπλέον $u \in V_{t_0}$ έχουμε ότι $u \in V_{c_0}$ για όλα τα u. Αυτό όμως σημαίνει ότι $c_0 \in T_0$, άτοπο.

- **Άσκηση 7**

Ένα tree decomposition χαρακτηρίζεται nice αν κάθε «υπερκόμβος» x ανήκει σε μια από τις εξής κατηγορίες:

- Leaf: Δεν έχει παιδιά, οπότε $|B_x| = 1$
- Introduce: Έχει ένα παιδί y και ισχύει $|B_x| = |B_y| \cap \{v\}$ για κάποιο κόμβο του v
- Forget: Έχει ένα παιδί y και ισχύει $|B_x| = |B_y| \setminus \{v\}$ για κάποιο κόμβο του v
- Join: Έχει 2 παιδιά y_1, y_2 με $|B_x| = |B_{y_1}| = |B_{y_2}|$

όπου B_x το σύνολο των κόμβων που περιέχονται στον υπερκόμβο x. Αποδεικνύεται ότι ένα tree decomposition (treewidth k) γραφήματος n κόμβων μπορεί να μετατραπεί σε nice έχοντας $O(kn)$ κόμβους, σε χρόνο $O(k^2 n)$. Εφαρμόζουμε αυτή τη διαδικασία στο προκείμενο πρόβλημα του q-coloring και λαμβάνουμε ένα nice tree decomposition. Για κάθε υπερκόμβο x και χρωματισμό που δηλώνεται ως $c: B_x \to \{1,2,\dots,q\}$ μπορούμε να υπολογίσουμε την boolean συνάρτηση $E[x,c]$ που αληθεύει ανν το c επεκτείνεται σε q-coloring του υποδέντρου του x. Ο υπολογισμός γίνεται αποδοτικά μέσω δυναμικού προγραμματισμού. Με βάση το decomposition έχουμε:

- Leaf: Εξ ορισμού ισχύει $E[x,c] = T$
- Introduce: Με βάση τον παραπάνω ορισμό, αν $c(v) \neq c(u)$ για κάθε γείτονα u του v, τότε $E[x,c] = E[y,c']$ όπου το c' προκύπτει από το c περιορισμένο στο B_y
- Forget: $E[x,c] = T$ αν $E[y,c'] = T$ για ένα εκ των q επεκτάσεων του c στο B_y
- Join: $E[x,c] = E[y_1,c] \wedge E[y_2,c]$

Υπάρχουν το πολύ q^{k+1} υποπροβλήματα για κάθε κόμβο του γραφήματος και κάθε υποπρόβλημα είναι επιλύσιμο όπως παρατηρούμε σε πολυωνυμικό χρόνο ως προς το treewidth. Η συνολική πολυπλοκότητα του αλγορίθμου για γράφημα n κόμβων είναι $O\left(k^2 n + kn * q^{k+1} * k^{O(1)}\right) = O\left(nq^k k^{O(1)}\right)$. Η τελική πολυπλοκότητα είναι της μορφής $O\left(f(k)n^{O(1)}\right)$ συνεπώς ο αλγόριθμος ανήκει στην κλάση FPT.

- **Άσκηση 8**

Θέλουμε να εκφράσουμε σε Monadic Second Order Logic την έκφραση «G δεν περιέχει το H ως minor». Πέραν της άρνησης, θα πρέπει να εκφράσουμε την ιδιότητα του H να είναι minor του γραφήματος G. Αυτό εξασφαλίζεται με 3 ιδιότητες για δεδομένα σύνολα κόμβων V_h του H. Πρώτον, τα σύνολα αυτά είναι συνεκτικά. Δεύτερον, είναι ανά 2 ξένα. Τρίτον, αν υπάρχει ακμή (h_1, h_2) στον H τότε θα υπάρχει και ακμή (u,v) με u να ανήκει στο σύνολο κόμβων του h_1 και v να ανήκει στο σύνολο κόμβων του h_2. Η έκφραση λοιπόν σε MSO_2 είναι η ακόλουθη:

- Πρώτη Ιδιότητα: $A \equiv \exists V_{h_1}, \dots, V_{h_n}. \left(\wedge_{1 \le i \le n} \left(\left(\exists h. h \in V_{h_i}\right) \wedge conn(V_{h_i})\right)\right)$
- Δεύτερη Ιδιότητα: $B \equiv \exists V_{h_1}, \dots, V_{h_n}. \left(\wedge_{1 \le i < j \le n} \neg \exists h. \left(h \in V_{h_i} \wedge h \in V_{h_j}\right)\right)$
- Τρίτη Ιδιότητα: $C \equiv \exists V_{h_1}, \dots, V_{h_n}. \left(\wedge_{(i,j) \in E(H)} \exists u, v. \left(u \in V_{h_i} \wedge v \in V_{h_j} \wedge edge(u,v)\right)\right)$

Τελικά $notMinor(H) \equiv \neg(A \wedge B \wedge C)$.

- **Πηγές ~ Βιβλιογραφία**

[1] Διαφάνειες Μαθήματος για Παραμετρικούς Αλγόριθμους και Miller-Rabin

[2] Paul D. Humke: Lagrange's Theorem: Statement and Proof, April 5, 2012

[3] Keith Conrad: Cosets and Lagrange's Theorem, The Miller-Rabin Test

[4] M. Cygan, F.V. Fomin, etc: Parameterized Algorithms, Springer 2016

[5] F.V. Fomin, M. Pilipczuk, etc: Kernelization and Sparseness: the case of Dominating Set

[6] Br. Courcelle, Joost Engelfriet. Graph structure and monadic second-order logic. A languagetheoretic approach. Cambridge University Press, pp.728, 2012, Encyclopedia of Mathematics and its applications, Vol. 138