ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΡΟΗΓΜΕΝΑ ΘΕΜΑΤΑ ΑΛΓΟΡΙΘΜΩΝ

(2020-2021)

3η Σειρά Ασκήσεων

Ονοματεπώνυμο:

- Χρήστος Τσούφης

Αριθμός Μητρώου:

- 03117176

Στοιχεία Επικοινωνίας:

- el17176@mail.ntua.gr

1η Άσκηση

Θεωρήστε πως έχουμε ένα γενικευμένο πρόβλημα ανάθεσης m εργασιών σε n άτομα, όπου το i-οστό άτομο μπορεί να αναλάβει μέχρι k_i εργασίες. Επιπλέον, κάποια άτομα απαγορεύεται να πάρουν κάποιες εργασίες (υπάρχει όμως εφικτή ανάθεση) και δίνεται το σύνολο των απαγορευμένων αναθέσεων. Αναγάγετε το γενικευμένο αυτό πρόβλημα στο κλασικό που είδαμε στο μάθημα (αν πιστεύετε ότι γίνεται).

Λύση:

Για το γενικευμένο πρόβλημα ανάθεσης m εργασιών σε n άτομα, όπου το i-οστό άτομο μπορεί να αναλάβει μέχρι k_i εργασίες, και λαμβάνοντας υπόψη το γεγονός ότι κάποια άτομα απαγορεύεται να πάρουν κάποιες εργασίες, μπορεί να θεωρηθεί ότι κάθε ζεύγος απαγορευμένης ανάθεσης του Ι μετατρέπεται σε μη απαγορευμένο ζεύγος στο Ι'.

Όμως, το κόστος για αυτή την μετατροπή είναι τάξεις μεγέθους μεγαλύτερο από το κανονικό κόστος.

Επίσης, σημειώνεται ότι αν το κόστος συμπεριλαμβάνεται στην τελική βέλτιστη λύση για το Ι', τότε δεν υπάρχει λύση για το Ι.

Επομένως, αφού το i-οστό άτομο στο Ι μπορεί να εκτελέσει $k_i > 1$ εργασίες, τότε στο Ι' δημιουργούνται k_i άτομα με κόστη ίδια με του i-οστού ατόμου.

Έτσι, πλέον ο πίνακας του κλασσικού προβλήματος ανάθεσης για το Ι' δεν θα είναι τετραγωνικός αφού θα έχουν προστεθεί γραμμές ή στήλες με μηδενικά.

2η Άσκηση

Έστω A ο n × m πίνακας πρόσπτωσης ενός κατευθυνόμενου γράφου G, δηλ.: A(u, e) = 1 αν e = (u, x) για κάποια κορυφή x, A(u, e) = −1 αν e = (x, u) για κάποια κορυφή x και A(u, e) = 0 διαφορετικά. Δείξτε ότι ο A είναι Totally Unimodular. Χρησιμοποιήστε αυτό για να δείξετε πως σε ένα δίκτυο με ακέραιες χωρητικότητες, η μέγιστη ροή και η ελάχιστη τομή έχουν ακέραιες τιμές.

Λύση:

Ορισμός:

Ένας πίνακας A είναι Totally Unimodular αν κάθε τετραγωνικός υποπίνακας έχει ορίζουσα 0,+1, -1. Αυτό υπονοεί ότι όλα τα entries είναι 0 ή ± 1.

Οι Totally Unimodular πίνακες έχουν καλή συμπεριφορά επειδή πάντα ορίζουν πολύτοπα με ακέραιες κορυφές εφόσον η right-hand πλευρά είναι integer-valued.

Θεώρημα:

Αν A είναι Totally Unimodular και b είναι ένα ακέραιο διάνυσμα, τότε το $P = \{x: Ax \leq b\}$ έχει ακέραιες κορυφές.

Απόδειξη:

Έστω v μια κορυφή του P. Τότε υπάρχει ένας non-singular τετραγωνικός υποπίνακας A' του A τέτοιος ώστε A'v = b'. Έχουμε det(A') = ± 1 αφού A' είναι non-singular. Από τον Cramer's Rule, ισχύει ότι: $v_i = \frac{\det(A'_i|b)}{\det(A')}$ όπου $A'_i|b$ είναι ο A' με το i-οστή στήλη να έχει αντικατασταθεί με το b. Έτσι, vi είναι ακέραια.

Λήμμα:

Για κάθε διμερή γράφο G, ο incidence πίνακας A είναι Totally Unimodular.

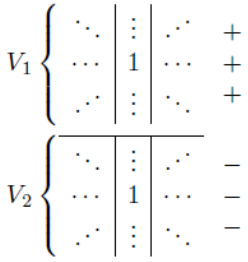
Απόδειξη:

Ο A είναι ένας 0-1 πίνακας, όπου οι στήλες είναι indexed από ακμές και κάθε στήλη έχει ακριβώς δυο 1 που αντιστοιχούν στις δύο κορυφές της ακμής. Με επαγωγή, θα δειχθεί ότι αυτό είναι αληθές για 1×1 πίνακα.

Έστω ότι ισχύει για όλους του (k – 1)×(k – 1) υποπίνακες. Έστω επίσης, A' ένας k×k υποπίνακας του A. Κάθε στήλη στο A' έχει το πολύ δύο 1. Αν καμία στήλη δεν έχει 1, τότε πρέπει να έχει 0 και ο πίνακας να είναι singular. Αν πάλι, κάθε στήλη έχει ακριβώς ένα μη μηδενικό entry, τότε det(A') = ± det(A''), όπου A'' προκύπτει από την διαγραφή της σχετικής σειράς και στήλης κι έτσι θα ισχύει $\det(A'') \in \{0, \pm 1\}$ με επαγωγή.

$$\begin{array}{c|c|c} \ddots & 0 & \iddots \\ \hline \cdots & 1 & \cdots \\ \hline \iddots & 0 & \ddots \end{array}$$

Διαφορετικά, κάθε στήλη έχει ακριβώς δυο 1. Συγκεκριμένα, αφού ο G είναι διμερής, η στήλες μπορούν να είναι χωρισμένες σε V_1, V_2 έτσι ώστε για κάθε στήλη να υπάρχει ακριβώς ένα 1 στο V_1 και στο V_2. Έτσι, αθροίζοντας όλες τις σειρές που αντιστοιχούν στο V1 και αφαιρώντας τις σειρές που αντιστοιχούν στο V2, να προκύπτει 0. Έτσι, A' είναι singular και det(A') = 0.

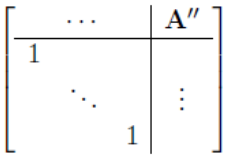


Λήμμα:

Αν A είναι Totally Unimodular, τότε $\begin{bmatrix} A \\ I \end{bmatrix}$ είναι Totally Unimodular.

Απόδειξη:

Από την Determinant Expansion Formula, η ορίζουσα κάθε τετραγωνικού υποπίνακα A' είναι ίση με 0 ή ± det(A''), όπου A'' είναι ένας τετραγωνικός υποπίνακας του A. Εξ ορισμού, det(A'')∈{0, ±1}.



Maximum flow:

Μια κλάση προβλημάτων στην οποία οι σχετικοί πίνακες είναι Totally Unimodular είναι τα προβλήματα Ροής.

Ορισμός:

Για ένα κατευθυνόμενο γράφο G και για μια κορυφή v, ορίζονται τα $\delta_{out}(v) = \{(v, w): (v, w)\in E\}$ και $\delta_{in}(v) = \{(u, v): (u, v)\in E\}$. Ομοίως, για ένα σύνολο κορυφών U, $\delta_{out}(U) = \{(u, v)\in E: u\in U, v\notin V\}$ και $\delta_{in}(W) = \{(v, w)\in E: v\notin W, w\in W\}$.

Ορισμός:

Για ένα κατευθυνόμενο γράφο G με δυο special κορυφές s, t και χωρητικότητα κορυφών c_e, μια s-t ροή είναι μια ανάθεση $x: E \to \mathbb{R}$ έτσι ώστε:

- Για κάθε ακμή e, $0 \le x_e \le c_e$
- Για κάθε κορυφή $v \neq s, t$, $\sum_{e\in\delta_{in}(v)} x_e = \sum_{e\in\delta_{out}(v)} x_e$

Το Maximum Flow Problem είναι το πρόβλημα εύρεσης μια s-t Ροής που να μεγιστοποιεί $\sum_{e\in\delta_{out}(v)} x_e$.

Αυτό το πρόβλημα μπορεί να γραφτεί με τη μορφή πινάκων ως εξής:

Έστω A ένας προσημασμένος incidence πίνακας του G, όπου $A_{v, e} = 1$, $A_{u, e} = -1$ για e = (u, v), και $A_{w, e} = 0$ για $w\notin e$.

Λήμμα:

Ο προσημασμένος πίνακας γειτνίασης ενός κατευθυνόμενου γράφου είναι Totally Unimodular.

Απόδειξη:

Η απόδειξη είναι ίδια με αυτή για διμερείς γράφους. Στην περίπτωση όπου κάθε στήλη του A' περιέχει δυο μη μηδενικές entries, παρατηρείται ότι οι σειρές αθροίζουν στο 0, έτσι det(A') = 0.

Τώρα, το Max Flow πρόβλημα θα γραφτεί σε μορφή πινάκων:

Έστω A' ο πίνακας που προκύπτει από τον A με τις σειρές που αντιστοιχούν στο s, t να έχουν αφαιρεθεί. Η συνθήκη διατήρησης ροής μπορεί να γραφτεί ως $A'x = 0$. Έστω επίσης, w η σειρά που αντιστοιχεί στο t. Τότε, προκύπτει ο ακόλουθο LP: $\max\{w^T x: 0 \le x \le c, A'x = 0\}$.

Από την Total Unimodularity του A, προκύπτει το εξής:

Πόρισμα:

Για $c \in \mathbb{Z}^E$, υπάρχει βέλτιστη ροή με ακέραιες τιμές.

Επίσης, εύκολα πλέον μπορεί να διατυπωθεί και το κλασσικό Max-flow Min-cut Θεώρημα.

Ορισμός:

Ένα s-t κόψιμο αποτελεί ένα οποιοδήποτε σύνολο από ακμές C έτσι ώστε να υπάρχει μη κατευθυνόμενο s-t μονοπάτι στο E\C. Η χωρητικότητα του C είναι $\sum_{e \in C} c_e$.

Θεώρημα:

Η μέγιστη ροή ενός s-t κοψίματος ισούται με την ελάχιστη χωρητικότητα ενός s-t κοψίματος.

Απόδειξη:

Από την LP δυϊκότητα, προκύπτει:

$$\max\{w^T x: A'x = 0, 0 \le x \le c\} = \min\{c^T y: A'^T z + y \ge w, z \in \mathbb{R}^{V\{s.t\}}, y \in \mathbb{R}_+^E\}$$

Αφού A' είναι TUM, προκύπτουν ακέραιες βέλτιστες λύσεις x* και (y*, z*) για το πρωτεύον και το δυϊκό LP.

Για απλοποίηση της περιγραφής, επεκτείνεται το z* σε διάνυσμα στο $\mathbb{R}^V$, όπου $z_s^* = 0$ και $z_t^* = -1$. Έτσι, προκύπτει $A^T z^* + y^* = A'^T z^* - w + y^* \ge 0$. Παρατηρείται ότι το y* πρέπει να είναι όσο το δυνατόν μικρότερο, το οποίο σημαίνει ότι $y_{uv}^* = \max\{z_u^* - z_v^*, 0\}$, λαμβάνοντας υπόψη το constraint για e = (u, v).

Ορίζεται $U = \{u \in V: z_u^* \ge 0\}$. Τότε, υπάρχει $s \in U$, $t \notin U$, έτσι ώστε $\delta_{out}(U)$ να είναι s-t κόψιμο. Αφού z_u^* είναι ακέραιοι, θα ισχύει ότι $y_{uv}^* \ge z_u^* - z_v^* \ge 1$ για κάθε $(u, v) \in \delta_{out}(U)$. Έτσι, $OPT = c^T y \ge \sum_{e \in \delta_{out}(U)} c_e$.

Προφανώς, $\sum_{e \in \delta_{out}(U)} c_e \ge \sum_{e \in \delta_{out}(s)} x_e = OPT$, οπότε τελικά όλες οι ανισότητες είναι ισότητες.

3η Άσκηση

Αποδείξτε το Θεώρημα Lagrange. Ειδικότερα, αποδείξτε ότι για πεπερασμένη ομάδα G, και υποομάδα $H \subseteq G$, δύο (δεξιά) σύμπλοκα της H είτε ταυτίζονται είτε είναι ξένα μεταξύ τους, και έχουν ίδια πληθικότητα με την H.

1ος Τρόπος Λύσης:

Πρόταση:

Έστω μια πεπερασμένη ομάδα $(G, \cdot)$. Αν το $H \subseteq G$ είναι υποομάδα της G, τότε $|H| \mid |G|$.

Απόδειξη:

Έστω ένα στοιχείο $g \notin H$. Έστω επίσης, το σύνολο $H_g = \{g \cdot a: a \in H\}$.

Προφανώς, αν $a_1 \neq a_2$, τότε και $g \cdot a_1 \neq g \cdot a_2$ και εφαρμόζοντας την πράξη με τον αντίστροφο του g και χρησιμοποιώντας το associativity: $g^{-1} \cdot g \cdot a_1 = g^{-1} \cdot g \cdot a_2 \Rightarrow a_1 = a_2$ που είναι άτοπο.

Τα H_g και H δεν έχουν τομή, αφού εάν είχαν, τότε $g \cdot h_1 = h_2 \Rightarrow g = h_2 \cdot h_1^{-1} \in H$ που είναι επίσης άτοπο καθώς από υπόθεση $g \notin H$. Επομένως, όλα τα στοιχεία του H_g είναι ανά δύο διαφορετικά.

Επιπλέον, το H_g έχει ένα στοιχείο για κάθε στοιχείο του H, άρα $|H_g| = |H|$.

Για την κάλυψη όλου του G, θα ακολουθηθεί η εξής διαδικασία. Αρχικά επιλέγεται ένα $g_1 \notin H$ και σχηματίζεται το H_{g1}. Ύστερα, επιλέγεται ένα $g_2 \notin H \cap H_{g1}$ και σχηματίζεται το H_{g2} κ.ο.κ.

Τα σύνολα H_{gi} είναι ανά δύο ξένα μεταξύ τους. Πράγματι, έστω $g_1 \cdot h_1 = g_2 \cdot h_2$:

$$g_1 \cdot h_1 = g_2 \cdot h_2 \Rightarrow g_1 = g_2 \cdot (h_2 \cdot h_1^{-1})$$

Όμως, $h_2 \cdot h_1^{-1} \in H$, οπότε εξ' ορισμού, $g_1 = g_2 \cdot (h_2 \cdot h_1^{-1}) \in H_{g2}$ που είναι άτοπο αφού $g_1 \notin H_{g2}$.

Έστω ότι χρησιμοποιήθηκαν k σύνολα εκτός του H για να καλυφθεί το G. Τότε, επειδή είναι ξένα μεταξύ τους:

$$\cup_{i=1}^{k} H_{gi} \cup H = G \Rightarrow |H| + \sum_{i=1}^{k} |H_{gi}| = |G| \xrightarrow{|H|=|H_{gi}|} (k+1)|H| = |G| \Rightarrow |H| \mid |G|$$

2ος Τρόπος Λύσης:

Πρόταση:

Κάθε 2 cosets μια υποομάδας H συνόλου G είτε ταυτίζονται είτε είναι ξένα μεταξύ τους.

Απόδειξη:

Η απόδειξη θα γίνει για τα right cosets καθώς ανάλογη είναι και η απόδειξη για τα left cosets.

Έστω Ha, Hb δύο right cosets και έστω ότι δεν είναι ξένα. Τότε, θα έχουν ένα κοινό στοιχείο, έστω c, για το οποίο θα ισχύει $c = ha = h'b$ με $h, h' \in H$. Από αυτή τη σχέση προκύπτει $a = h^{-1}h'b$. Επειδή το H είναι υποομάδα, $h^{-1}h' = h'' \in H$, οπότε: $a = h''b \Rightarrow Ha = H(h''b) = (Hh'')b = Hb$.

Συνεπώς, τα 2 cosets ταυτίζονται, αν δεν είναι ξένα.

Για την απόδειξη χρησιμοποιήθηκε το εξής: $Hh'' \equiv H$. Αυτό ισχύει, διότι το $h'' = g \in H$ οπότε:

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

Αυτό σημαίνει πως το H ανήκει στο Hh''.

Πρόταση:

Κάθε σύμπλοκο του H θα είναι ίδιας πληθικότητας με αυτό.

Απόδειξη:

Έστω η συνάρτηση $f: H \rightarrow Ha$, με τύπο $f(h_i) = h_ia$ που είναι 1-1 και επί:

$$f(h_i) = f(h_j) \rightarrow h_ia = h_ja \rightarrow h_i = h_j$$

Οπότε, προκύπτει πως το πλήθος των στοιχείων ενός coset είναι ίδιο με το πλήθος στοιχείων του H.

Απόδειξη Θ. Lagrange:

Έστω H υποομάδα του πεπερασμένου συνόλου G, με πληθικότητες $|H| = m$ και $|G| = n$.

Επομένως, κάθε coset του H θα έχει επίσης m στοιχεία.

Χρησιμοποιώντας την 1η ιδιότητα που αποδείχθηκε, διαμερίζεται το G ως εξής:

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

Δηλαδή, αν r ο αριθμός των στοιχείων κάθε coset της διαμέρισης, τότε $n = rm$, οπότε θα ισχύει πράγματι ότι:

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

4η Άσκηση

Bonus άσκηση (προαιρετική):
https://courses.corelab.ntua.gr/pluginfile.php/494/mod_resource/content/2/BONUS_CRYPTO.pdf

Σημείωση: αγνοήστε την ημερομηνία παράδοσης που αναγράφεται στην εκφώνηση.

Λύση:

Έστω G το σύνολο των ανθρώπων της Βασιλοπροσγείωσης.

Έστω η πράξη $(\cdot)$: $G \times G \rightarrow G$ τέτοια ώστε η $(G, \cdot)$ να είναι ομάδα ώστε να χρησιμοποιηθούν οι ιδιότητες των αλγεβρικών ομάδων. Έτσι, ορίζεται $(\cdot)$: $G \times G \rightarrow G$, για την οποία το $a \cdot b = c$ σημαίνει ότι ο άνθρωπος c τραυμάτισε τον a με το μαχαίρι του b.

Πρόταση:

Θα δειχθεί ότι η $(G, \cdot)$ είναι ομάδα.

Απόδειξη:

Κλειστότητα:

Η πράξη είναι κλειστή, αφού το αποτέλεσμα είναι ένας άνθρωπος που πάντα ανήκει στο G.

Ουδέτερο στοιχείο:

Το ουδέτερο στοιχείο της πράξης είναι ο Καλικάντζαρος αφού "ο Καλικάντζαρος είχε ένα μαχαίρι που ο κάθε ένας χρησιμοποίησε για να τραυματίσει τον εαυτό του". Δηλαδή, αν K ο Καλικάντζαρος, $\forall A \in G: A \cdot K = A \Rightarrow K = e$.

Αντίστροφος:

Ο αντίστροφος κάθε ανθρώπου είναι ο θανάσιμος εχθρός του. Πράγματι, "ο Καλικάντζαρος τραυμάτισε κάθε έναν με το μαχαίρι του θανάσιμου εχθρού του", δηλαδή αν E(A) ονομαστεί ο θανάσιμος εχθρός του ανθρώπου A, $\forall A \in G: A \cdot E(A) = e \Rightarrow E(A) = A^{-1}$.

Προσεταιριστικότητα:

Είναι γνωστό ότι για κάθε τριάδα ανθρώπων $a, b, c \in G$, "ο άνθρωπος που τραυμάτισε τον τρίτο χρησιμοποιώντας το μαχαίρι αυτού που τραυμάτισε τον δεύτερο με το μαχαίρι του πρώτου, είναι ο ίδιος άνθρωπος που χρησιμοποίησε το μαχαίρι του πρώτου για να τραυματίσει αυτόν που τραυμάτισε τον τρίτο με το μαχαίρι του δεύτερου". Αναλυτικότερα, αυτός που τραυμάτισε τον δεύτερο με το μαχαίρι του πρώτου: $(b \cdot a)$. Αυτός που τραυμάτισε τον τρίτο χρησιμοποιώντας το μαχαίρι του $(b \cdot a)$: $c \cdot (b \cdot a)$. Αυτός που τραυμάτισε τον τρίτο με το μαχαίρι του δεύτερου: $(c \cdot b)$. Τέλος, αυτός που χρησιμοποίησε το μαχαίρι του a για να τραυματίσει τον $(c \cdot b)$: $(c \cdot b) \cdot a$.

Επομένως, από την πληροφορία της εκφώνησης, $\forall\, a, b, c \in G: c \cdot (b \cdot a) = (c \cdot b) \cdot a$

Οπότε, η πράξη $(\cdot)$ είναι προσεταιριστική στο G.

Από τα παραπάνω, η $(G, \cdot)$ είναι ομάδα.

(i) Επειδή η τάξη της G είναι πρώτος αριθμός ($2^{19} – 1$), η (G, ·) είναι αβελιανή ομάδα, δηλαδή ισχύει για αυτή και η αντιμεταθετική ιδιότητα. Επιπλέον, είναι γνωστό πως η Δρακομάνα τραυμάτισε τον Γιάννη τον Χιονιά με το μαχαίρι του Τζοφραίου του Αντιπαθητικού, δηλαδή Γ·Τ = Δ. Επειδή η ομάδα είναι αβελιανή, θα ισχύει και: Τ·Γ = Δ, δηλαδή η Δ = Δρακομάνα ήταν εκείνη που τραυμάτισε τον Τ = Τζοφραίο με το μαχαίρι του Γ = Γιάννη του Χιονιά.

(ii) Είναι γνωστό ότι η Δρακομάνα και ο Τζοφραίος είναι θανάσιμοι εχθροί, δηλαδή Δ·Τ = Τ·Δ = e. Έστω Χ, ο άνθρωπος που τραυμάτισε την Δρακομάνα με το μαχαίρι της. Θα ισχύει: Δ·Δ = Χ. Αν πολλαπλασιαστεί από δεξιά με τον Τ που είναι αντίστροφος της Δ, τότε: Δ = Χ·Τ. Από το προηγούμενο ερώτημα είναι γνωστό ότι Δ = Γ·Τ, οπότε: Γ·Τ = Χ·Τ. Αν πολλαπλασιαστεί από δεξιά με τον αντίστροφο του Τ και εφαρμοστεί η προσεταιριστική, προκύπτει: $Γ·(T^{-1}·T) = Χ·(T^{-1}·T) ⇒ Χ = Γ$.

Συνεπώς, ο Γιάννης ο Χιονιάς ήταν εκείνος που τραυμάτισε την Δρακομάνα με το μαχαίρι της.

(iii) Έστω Β το ζητούμενο πρόσωπο. Εκείνος που τραυμάτισε τον Γιάννη τον Χιονιά με το ίδιο του το μαχαίρι είναι ο Γ·Γ. Αντίστοιχα, αυτός που τραυμάτισε τον Τζοφραίο με το ίδιο του το μαχαίρι είναι ο Τ·Τ. Ο Β χρησιμοποίησε το μαχαίρι του Γ·Γ για να τραυματίσει τον Τ·Τ: (Τ·Τ)·(Γ·Γ) = Β. Εάν εφαρμοστεί η προσεταιριστική, τότε: Β = Τ·(Τ·Γ)·Γ. Είναι γνωστό ότι Τ·Γ = Δ, οπότε Β = Τ·Δ·Γ. Τέλος, οι Τ και Δ είναι αντίστροφοι, οπότε Β = Γ.

Συνεπώς, το ζητούμενο πρόσωπο είναι ο Γιάννης ο Χιονιάς.

5η Άσκηση

Αποδείξτε ότι στην περίπτωση όπου $n = p^e$, $e > 1$, p πρώτος, ο έλεγχος Miller-Rabin (ουσιαστικά ο έλεγχος Fermat) επιτυγχάνει με πιθανότητα > 1/2. Συγκεκριμένα, αποδείξτε ότι για περισσότερα από τα μισά $b \in \mathbb{Z}_n : b_n - 1 \not\equiv 1 \pmod n$.

Υπόδειξη: θεωρήστε γνωστό το γεγονός ότι η ομάδα $U(\mathbb{Z}_n)$ είναι κυκλική για $n = p^e$, $e > 0$, p περιττό.

1ος Τρόπος Λύσης:

Πρόταση:

Αρχικά, θα δειχθεί ότι υπάρχει κάποιο $x \in \mathbb{Z}_n^*$ τέτοιο ώστε $x^{n-1} \not\equiv 1 \pmod n$.

Απόδειξη:

Έστω ότι $\forall\, x \in \mathbb{Z}_n^*$: $x^{n-1} \equiv 1 \pmod n$. Είναι γνωστό ότι η $\mathbb{Z}_n^*$ είναι κυκλική, επομένως έχει κάποιο γεννήτορα g για τον οποίο θα ισχύει $\text{ord}(g) = |\mathbb{Z}_n^*| = \varphi(n)$. Από υπόθεση, ισχύει $\forall x$: $x^{n-1} \equiv 1 \pmod n$, οπότε και για το g θα ισχύει:

$g^{n-1} \equiv 1 \pmod n \Rightarrow g^{n-1} \equiv g^0 \pmod n \Rightarrow n - 1 \equiv 0 \pmod{\varphi(n)} \Rightarrow \varphi(n) \mid n - 1$

Εύκολα αποδεικνύεται ότι για δυνάμεις πρώτων αριθμών, η συνάρτηση φ του Euler έχει την ακόλουθη μορφή: $\varphi(p^e) = p^{e-1}(p - 1)$. Επομένως, ισχύει: $\varphi(n) \mid n - 1 \Rightarrow p^{e-1}(p - 1) \mid p^e - 1$

Αυτό είναι άτοπο αφού το p διαιρεί το $p^{e-1}(p - 1)$ αλλά όχι το $p^e - 1$.

Τελικά, υπάρχει κάποιο $x \in \mathbb{Z}_n^*$ τέτοιο ώστε $x^{n-1} \not\equiv 1 \pmod n$.

Έστω το σύνολο $B = \{b \in \mathbb{Z}_n^* : b^{n-1} \equiv 1 \pmod n\}$. Το B προφανώς είναι κλειστό ως προς τον πολλαπλασιασμό mod n:

$$\begin{cases} a^{n-1} \equiv 1 \pmod n \\ b^{n-1} \equiv 1 \pmod n \end{cases} \Rightarrow (ab)^{n-1} \equiv 1 \pmod n \Rightarrow (ab) \in B$$

Άρα, το B είναι υποομάδα του $\mathbb{Z}_n^*$ και μάλιστα γνήσια υποομάδα αφού αποδείχθηκε ότι υπάρχει $x \in \mathbb{Z}_n^*$: $x^{n-1} \not\equiv 1 \pmod n$.

Συνεπώς, από το θεώρημα Lagrange, $|B| \mid |\mathbb{Z}_n^*| \Rightarrow |B| \leq \frac{|\mathbb{Z}_n^*|}{2}$

2ος Τρόπος Λύσης:

Πρόταση:

Έστω ο έλεγχος Miller-Rabin για $n = p^a$, όπου $a > 1$. Οι περιπτώσεις αποτυχίας του αλγορίθμου είναι λύσεις του $a^{p-1} \equiv 1 \bmod n$ και συγκροτούν ομάδα υπό την πράξη του πολλαπλασιασμού mod n.

Απόδειξη:

Έστω $a \in \{2, 3, \ldots, n-1\}$ ένα Miller-Rabin nonwitness. Επειδή a και n είναι σχετικά πρώτοι, το Θεώρημα Euler λέει ότι $a^{\varphi(n)} \equiv 1 \bmod n$. Από την ιδιότητα του nonwitness προκύπτει $a^k \equiv 1 \bmod n$ ή $a^{2^i k} \equiv -1 \bmod n$. Από αμφότερες τις περιπτώσεις προκύπτει $a^{n-1} \equiv 1 \bmod n$. Άρα, το a mod n διαιρεί το $(\varphi(n), n-1) = (p^{a-1}(p-1), p^a - 1) = p - 1$ αφού p και $p^a - 1$ είναι σχετικά πρώτοι και $p - 1$ διαιρεί το $p^a - 1$. Τελικά, $a^{p-1} \equiv 1 \bmod p^a = n$. Ομοίως, αν $a^{p-1} \equiv 1 \bmod p^a$ τότε $p - 1 = 2^f l$, $f \geq 1$, και l περιττός. Το $p - 1$ είναι παράγοντας του $p^a - 1 = 2^e k$, οπότε $f \leq e$, $l|k$.

Επειδή, $(a^l)^{2^f} \equiv 1 \bmod p^a$, η τάξη του $a^l \bmod p^a$ είναι 2^j για $j \in \{0, \ldots, f\}$. Αν $j = 0$, τότε $a^k \equiv 1 \bmod p^a$ με $l|k$. Αν $j > 0$, τότε $x := (a^l)^{2^{j-1}}$ ικανοποιεί το $x \not\equiv 1 \bmod p^l$. Θα ισχύει όμως, $x^2 \equiv 1 \bmod p^l$. Οπότε, θα ισχύει $p^l \mid (x+1)(x-1)$ και το πολύ ένας εκ των όρων του δεξιού μέλους θα διαιρείται από το p. Δηλαδή, $p^l \mid (x+1)$ ή $p^l \mid (x-1)$ ώστε $x \not\equiv \pm 1 \bmod p^l \rightarrow x \equiv (a^l)^{2^{j-1}} \equiv -1 \bmod p^l$, $l|k$ και k περιττός.

Υψώνοντας και τα δύο μέλη στην k/l δύναμη, προκύπτει τελικά: $a^{2^i k} \equiv -1 \bmod p^a$.

Πρόταση:

Η πιθανότητα να έχουμε nonwitness είναι μικρότερη από 50%.

Απόδειξη:

Θα αποδειχθεί το ζητούμενο δείχνοντας ότι τα nonwitnesses περιέχονται σε κανονική υποομάδα των αντιστρέψιμων αριθμών mod n. Μια 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 (δεν περιέχει το 1 και το n – 1) ενώ περιλαμβάνει και όλους τους μη αντιστρέψιμους αριθμούς mod n σε αυτό το διάστημα. Δηλαδή, το πλήθος των επιτυχιών του αλγόριθμου είναι άνω του 50%, έστω W. Όμως, πρέπει να αφαιρεθούν τα 1, n – 1 αφού δεν μπορεί να είναι witnesses. Έτσι, $\frac{W}{n-1} > \frac{1}{2} \rightarrow \frac{W}{n-3} > \frac{W}{n-1} > \frac{1}{2}$ που είναι το ζητούμενο.

Πρόταση:

Τα nonwitnesses περιέχονται σε κανονική υποομάδα των αντιστρέψιμων αριθμών mod n.

Απόδειξη:

Χρησιμοποιώντας τη μορφή του n που δίνεται στην εκφώνηση, αποδείχθηκε πως τα Miller-Rabin nonwitnesses είναι λύσεις του $a^{p-1} \equiv 1 \bmod n$ και συγκροτούν ομάδα με την πράξη του πολλαπλασιασμού mod n. Αυτό το a δεν διαιρείται από το p και υπάρχουν αντιστρέψιμοι αριθμοί mod n με τάξη ώστε να διαιρούνται από p, π.χ. το 1+ p.

Εν κατακλείδι, με τους παραπάνω ισχυρισμούς ολοκληρώνεται η απόδειξη.

6η Άσκηση

Διατυπώστε παραμετρικό αλγόριθμο για το πρόβλημα Dominating Set με παράμετρο το μέγεθος του κυρίαρχου συνόλου. Είναι ο αλγόριθμός σας FPT; Εξηγήστε. Αλλάζει κάτι αν θεωρήσουμε ως παράμετρο και τον μέγιστο βαθμό του γράφου εισόδου Δ;

1ος Τρόπος Λύσης:

Ένας προφανής παραμετρικός αλγόριθμος για το Dominating Set με παράμετρο το μέγεθος του κυρίαρχου συνόλου είναι ο έλεγχος όλων των συνόλων k κόμβων για να διαπιστωθεί εάν αποτελούν dominating set. Υπάρχουν συνολικά $\binom{n}{k} < n^k$ τέτοια σύνολα και απαιτούνται O(n' + m') = O(n + n·k) για να γίνει έλεγχος εάν κάποιο είναι dominating set. Επομένως, συνολικά θα χρειαστούν $O(k \cdot n^{k+1})$.

Αυτός ο αλγόριθμος είναι πολυωνυμικός για κάθε σταθερά k, ωστόσο δεν είναι FPR αφού ο εκθέτης του n εξαρτάται από το k, δηλαδή η πολυπλοκότητα δεν είναι της μορφής $f(k) \cdot n^c$.

Αν θεωρηθεί ως παράμετρος ο μέγιστος βαθμός του γραφήματος, δεν αλλάζει κάτι αφού όπως φάνηκε, το Dominating Set είναι W[2]-complete, επομένως δεν είναι FPT εκτός και αν W[2] ≡ FPT.

2ος Τρόπος Λύσης:

Για τον παραμετρικό αλγόριθμο αρχικά για παράμετρος θεωρείται το μέγεθος του Dominating Set, έστω k. Εξαντλητικά, παράγονται όλα τα μεγέθους k υποσύνολα κορυφών του γράφου και ελέγχονται γραμμικά σε καθένα από αυτά εάν είναι Dominating Set του γράφου. Οπότε, θα προκύψουν συνολικά $\binom{n}{k} = O(n^k)$ σύνολα για να ελεγχθούν σε γραμμικό χρόνο το καθένα. Επομένως, η συνολική πολυπλοκότητα του προτεινόμενου αλγορίθμου είναι $O(n^k)$.

Για να είναι ένας αλγόριθμος FPT πρέπει να έχει χρονική πολυπλοκότητα της μορφής $O(f(k)n^{O(1)})$. Όμως, ο παραπάνω αλγόριθμος δεν είναι σε αυτή τη μορφή και μάλιστα είναι αδύνατο να βρεθεί FPT αλγόριθμος για το Dominating Set Problem αφού το πρόβλημα ανήκει στην κλάση W[2] και αυτό θα σήμαινε W[1] = W[2].

Αν προστεθεί ως παράμετρος και το φράγμα Δ στον βαθμό του γράφου εισόδου, τότε ουσιαστικά είναι η περίπτωση ενός Δ-degenerate γράφου. Έτσι, μπορεί να προκύψει FPT αλγόριθμος.

Αρχικά, επιλέγεται ο undominated κόμβος ελάχιστου βαθμού. Ο κόμβος είτε θα βρίσκεται στη λύση είτε ένα υποσύνολο των γειτόνων του. Έπειτα, σημειώνονται οι dominated κόμβοι, διαγράφεται ο αρχικός και επαναλαμβάνεται η διαδικασία. Τελικά, προκύπτει Dominating Set, με πολυπλοκότητα $O(\Delta^k n)$ οπότε θα είναι και FPT.

7η Άσκηση

Διατυπώστε έναν FPT αλγόριθμο για το πρόβλημα q-coloring (αν ένας γράφος μπορεί να χρωματιστεί με q χρώματα, q σταθερά, ανεξάρτητη της εισόδου) με παράμετρο το treewidth k. Θεωρήστε ότι σας δίνεται και η αντίστοιχη tree decomposition [1, Άσκηση 7.18.c].

Λύση:

Αναζητείται ένας FPT αλγόριθμος για το q-coloring (q σταθερά), χρησιμοποιώντας ως παράμετρο το treewidth k. Αποδεικνύεται ότι ένα tree decomposition (treewidth k) γραφήματος n κόμβων μπορεί να μετατραπεί σε nice έχοντας O(k·n) κόμβους, σε χρόνο $O(k^2 \cdot n)$. Έτσι, εν προκειμένω, προκύπτει ένα nice tree decomposition. Ο υπολογισμός γίνεται αποδοτικά μέσω δυναμικού προγραμματισμού.

Ορίζεται το υποπρόβλημα D[x, S] όπου x ένας κόμβος του nice decomposition και S κάποιος χρωματισμός των κόμβων στο bag B_x. Το D[x, S] θα είναι true αν και μόνο αν το υποδέντρο που έχει ρίζα το x μπορεί να χρωματιστεί με q χρώματα εφόσον οι κόμβοι του B_x χρωματίζονται σύμφωνα με το S.

Έτσι, διακρίνονται οι παρακάτω περιπτώσεις για τον κόμβο x του nice decomposition:

- Leaf: Ο κόμβος x δεν έχει παιδιά και $|B_x| = 1$. Τότε, D[x, S] = true για κάθε χρωματισμό S.

- Introduce: Ο κόμβος x έχει ένα παιδί y με ακριβώς μια λιγότερη κορυφή στο bag του (δηλαδή $B_x = B_y \cup \{u\}$). Για τον υπολογισμό του D[x, S], αρχικά ελέγχεται αν υπάρχει κάποιος γείτονας του v στο B_x στον οποίο το S αναθέτει το ίδιο χρώμα. Αν δεν παραβιάζεται αυτό, αρκεί να λυθεί αναδρομικά το D[y, S'] όπου S' είναι το S περιορισμένο στο $B_x \setminus \{u\}$.

- Forget: Ο κόμβος x έχει ένα παιδί y με ακριβώς μια περισσότερη κορυφή στο bag του (δηλαδή $B_x = B_y \setminus \{u\}$). Για τον υπολογισμό του D[x, S]. αρκεί να λυθεί αναδρομικά το D[y, S'] για τα q σύνολα S' που είναι η επέκταση του S στο $B_x \cup \{u\}$ ώστε το u να παίρνει όλα τα χρώματα.

- Join: Ο κόμβος x έχει δυο παιδιά y_1, y_2 με $B_x = B_{y1} = B_{y2}$, οπότε: $D[x, S] = D[y_1, S] \wedge D[y_2, S]$.

Υπάρχουν το πολύ q^{k+1} υποπροβλήματα για κάθε κόμβο του γραφήματος και κάθε υποπρόβλημα είναι επιλύσιμο σε πολυωνυμικό χρόνο ως προς το treewidth. Συνολικά, υπάρχουν $q^k \cdot n$ υποπροβλήματα και στην χειρότερη περίπτωση (Forget) απαιτείται O(q·k) για κάθε ένα. Συνεπώς, η συνολική πολυπλοκότητα για γράφημα n κόμβων είναι $O(k^2 \cdot n + k \cdot n \cdot q^{k+1} \cdot k^{O(1)}) = O(n \cdot q^k \cdot k^{O(1)}) = O(q^{k+1} \cdot k \cdot n)$. Δηλαδή, το q-coloring με παράμετρο το treewidth έχει την μορφή $O(f(k)n^{O(1)})$ και άρα θα είναι FPT.

8η Άσκηση

Bonus άσκηση (προαιρετική): λύστε την Άσκηση 7.24 από το [1]. Θα χρειαστεί να μελετήσετε, μεταξύ άλλων, τις ενότητες 2.5, 3.1 και 3.2.

"Obtain an algorithm for Vertex Cover running in time $1.3803^k k^{O(1)} + O(m\sqrt{n})$ *by combining branching in degree 4 vertices, the 2k vertex kernel of Theorem 2.21, and the fact that agraph on n vertices of maximum degree 3 has pathwidth at most* $\frac{n}{6} + o(n)$*, and a path decomposition of such width can be constructed in polynomial time (see [3])"*

Λύση:

–

Resources:

1. *https://theory.stanford.edu/~jvondrak/MATH233B-2017/lec3.pdf*
2. *Διαφάνειες Μαθήματος για Παραμετρικούς Αλγόριθμους και Miller-Rabin*
3. *Paul D. Humke: Lagrange's Theorem: Statement and Proof, April 5, 2012*
4. *Keith Conrad: Cosets and Lagrange's Theorem, The Miller-Rabin Test*
5. *Marek Cygan, Fedor V. Fomin, Lukasz Kowalik, Daniel Lokshtanov, Dániel Marx, Marcin Pilipczuk, Michal Pilipczuk, and Saket Saurabh. Parameterized Algorithms. Springer, 2016.*
6. *Fomin, F.V., Kaski, P.: Exact exponential algorithms. Communications of the ACM 56(3), 80-88 (2013).*
7. *F.V. Fomin, M. Pilipczuk, etc: Kernelization and Sparseness: the case of Dominating Set*