Aalto-yliopisto

Gripenberg, Potka, Pöllänen, Tuhkanen, Ääri

MS-A0401 Diskreetin matematiikan perusteet
2. välikoe 22.10.2015

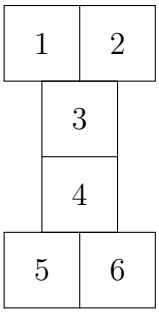
Kirjoita jokaiseen koepaperiin nimesi, opiskelijanumerosi ym. tiedot !
Laskimia tai taulukoita ei saa käyttää tässä kokeessa!

1. U ja V käyttävät RSA-algoritmia keskinäisessä viestinnässään. U:n julkinen avain on (n_U, k_U) ja yksityinen avain (n_U, d_U). V:n julkinen avain on (n_V, k_V) ja yksityinen avain (n_V, d_V) ja molemmat pitävät tietenkin yksityiset avaimensa salassa muilta. Lisäksi he käyttävät allekirjoituksia varten hajautusfunktiota h. Jos nyt U saa V:ltä viestin, joka salattuna on x ja lisäksi allekirjoituksen, joka on s, niin mitä U:n pitää laskea, jotta hän voisi olla varma siitä, että V on viestin lähettäjä?

Ratkaisu: U purkaa salauksen yksityisellä avaimellaan ja laskee $y = \mod(x^{d_U}, n_U)$. Tämän jälkeen hän laskee alkuperäsen viestin y hajautusarvon $h(y)$ jonka jälkeen hän purkaa allekirjoituksen salauksen V:n julkisella avaimella eli hän laskee $z = \mod(s^{k_V}, n_V)$. Jos nyt $z = h(y)$ niin U voi luottaa siihen, että V on viestin lähettäjä.

---

2. Alla olevan kuvion rotaatioilla ja peilauksilla saadaan permutaatiot $p_1 = (1)$, $p_2 = (1\ 6)(2\ 5)(3\ 4)$, $p_3 = (1\ 2)(5\ 6)$ ja $p_4 = (1\ 5)(2\ 6)(3\ 4)$.



(a) Mitä pitäisi osoittaa, jotta tulisi todistetuksi, että yllä mainitut permutaatiot muodostavat ryhmän? (Sinun ei tarvitse suorittaa näitä laskuja!)
(b) Määritä tämän ryhmän sykli-indeksi.
(c) Määritä Pólyan lauseen avulla monellako, ryhmän toiminnnan suhteen ei-ekvivalentilla, tavalla kuvion ruudut voidaan värittää kahdella värillä.

Ratkaisu: (a) Koska tietyn joukon alkioiden kaikki permutaatiot muodostavat ryhmän on siis osoitettava, että permutaatiot $\{p_1, p_2, p_3, p_4\}$ muodotavat aliryhmän (kun laskutoimituksena on funktioiden yhdistäminen). Koska kyseinen joukko on äärellinen niin tässä tapauksessa riittää tarkistaa, että jos i ja $j \in \{1, 2, 3, 4\}$ niin löytyy $k \in \{1, 2, 3, 4\}$ siten, että $p_i \circ p_j = p_k$. (Jos emme halua käyttää hyväksi sitä tosiasiaa, että joukko on äärellinen niin meidän pitää todeta, että jokaisella $j \in \{1, 2, 3, 4\}$ pätee $p_j^{-1} = p_j$.)

(b) Permutaatioiden ratojen pituudet ovat

p_1 : 6 rataa, joissa on 1 alkio
p_2 : 3 rataa, joissa on 2 alkiota
p_3 : 2 rataa, joissa on 1 alkio, 2 rataa, joissa on 2 alkiota
p_4 : 3 rataa, joissa on 2 alkiota

Näin ollen sykli-indeksi on

$$\zeta_{G,X}(t_1, t_2) = \frac{1}{4}(t_1^6 + 2t_2^3 + t_1^2 t_2^2).$$

(c) Pólyan luseen nojalla saamme

$$\zeta_{G,X}(2, 2) = \frac{1}{4}(2^6 + 2 \cdot 2^3 + 2^4) = \frac{1}{4}(64 + 16 + 16) = 24$$

erilaista väritystä jos käytämme 2:ta väriä.

3.

(a) Osoita, että jos kahdella yksinkertaisella ja suuntaamattomalla verkolla ei ole sama kromaattinen luku niin ne eivät ole isomorfiset.
(b) Määritä lukujen 38 ja 48 suurin yhteinen tekijä Eukleideen algoritmin avulla.

Ratkaisu: (a) Teemme vastaoletuksen, että verkot $[V_1, E_1]$ ja $[V_2, E_2]$ ovat isomorfiset vaikka niiden kromaattiset luvut k_1 ja k_2 ovat erisuuret. Oletamme esimerkiksi että $k_1 > k_2$ ja että $\psi : V_1 \to V_2$ on bijektio siten, että $\{a, b\} \in E_1$ jos ja vain jos $\{\psi(a), \psi(b)\} \in E_2$. Jos nyt $\omega : V_2 \to \{v_1, \ldots, v_{k_2}\}$ on verkon $[V_2, E_2]$ solmujen väritys niin $\omega \circ \psi : V_1 \to \{v_1, \ldots, v_{k_2}\}$ on verkon $[V_1, E_1]$ solmujen väritys koska jos $\{a, b\} \in E_1$ niin $\{\psi(a), \psi(b)\} \in E_2$ ja koska ω on verkon $[V_2, E_2]$ solmujen väritys niin $\omega(\psi(a)) \neq \omega(\psi(b))$ eli $(\omega \circ \psi)(a) \neq (\omega \circ \psi)(b)$ ja olemme löytäneet verkon $[V_1, E_1]$ värityksen jossa on k_2 väriä mikä on ristiriidassa sen kanssa, että verkon $[V_1, E_1]$ kromaattinen luku on $k_1 > k_2$.
(b) Eukleideen algoritmin avulla saamme

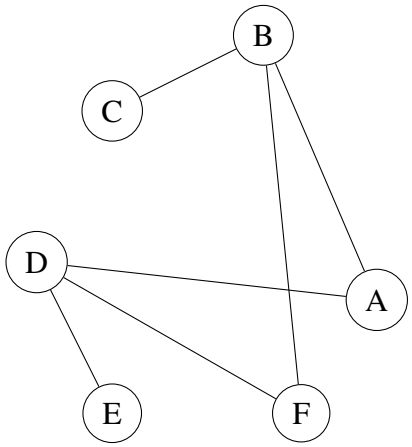
$$\begin{aligned} 48 &= 1 \cdot 38 + 10, \\ 30 &= 3 \cdot 10 + 8, \\ 10 &= 1 \cdot 8 + 2, \\ 8 &= 4 \cdot 2 + 0, \end{aligned}$$

josta näemme, että suurion yhteinen tekijä on 2.

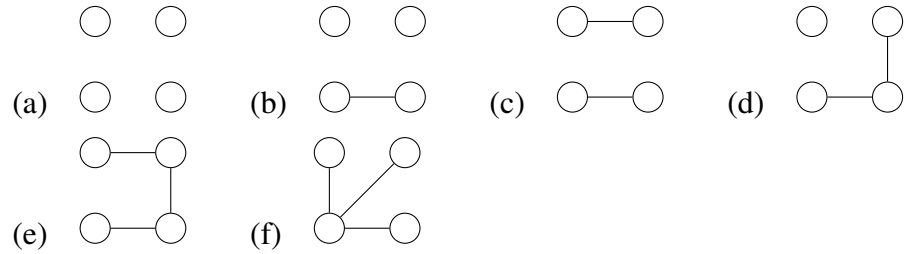
4.

(a) Piirrä kuvat kaikista yksinkertaisista suuntaamattomista ei-isomorfisista verkoista, joissa on 4 solmua ja jotka ovat metsiä (eli jokaisesta solmusta on korkeintaan yksi yksinkertainen polku jokaiseen toiseen solmuun).

(b) Määritä alla olevassa verkossa Hamilton-polku tai selitä mistä nähdään ettei sellaista löydy.



Ratkaisu: (a) Ei-isomorfiset metsät, joissa on 4 solmua ovat



(b) Tässä verkossa ei ole Hamiltonin polku (joka siis kulkisi täsmälleen kerran jokaisen solmun kautta) koska jos sellainen olisi niin ensimmäinen solmu olisi joko C (jolloin viimeinen olisi E) tai E (jolloin viimeinen olisi C). Silloin polku olisi $[C, B, X, Y, D, E]$ (tai $[E, D, X, Y, B, C]$) missä X on joko A tai F ja Y vastaavasti F tai A. Mutta tämä ei ole mahdollista koska solmujen A ja F välillä ei ole kaari.