

Kriptografia: RSA zifratze-algoritmoa



Matematika Diskretua
Ana Zelaia Jauregi

- Gako pribatua da, mezu hartzaileak sortua eta ineroa ezkontuan gordeteko duena. Gako hau dabiloak.
 - Gako publikoa: Mezu zifratzeko erabilizten da. Publikoa da eta edonori ematen dira:
- Esan bezala, RSA zifratze-sistema mezu zifratzeko eta deszifratzeko bi gako erabilitzen ditugun.
- Hain modu laburaren alpatutako urtak horiek datozuen ataldean pislak salonduko eta kalkulatzeko saria dabilo, baina konputazioa ezinezkoa geratuko zaio.
- Karria gako pribatua erabiliztea dabilo. Gako publikotik aldatuz gako pribatua lor dabilo, gertatuko balitz ere, berak ez luke mezu ulertuiko, mezu zifratza deszifratzeko modu basatzailea ez den norbaitean eskuineko arriskua beti existzen da. Deha den, hala bidaltzaileak hartzailera erabili dionean, hau da transmisioreen unean, mezuaren orriñala, ulergarria dena, lotutxo du.
- Hartzailera gako pribatua erabiliz mezu deszifratu egongo din, eta deskodetu ondo biltz zifratu egongo du eta mezu zifratza hartzailera bidaliko dio.
 - Bidaltzaileak mezu orriñala zenbakitarrak kodetuko du. Ondoren, gako publikoa era-
- Pribatua ezkontuan gordeteko du.
- Hartzailera gako pribatua eta pribatua aukeztutako ditu, eta mezu zifratua bidali nahi dion edonori, mezu gako publiko hori erabiliz zifratzeko eskatuko dio. Gako emai behariko dituzten urtastak:
- Lagun batetik (bidaltzaileak) beste bat (hartzailera) mezu zifratu bat pasa nahi badio ulertzima geratzen da gainerakoentzat.
- Terrimologiako aldetik esan behar da enkripitatzaea eta zifratza sintonizat erabili ohi sistema da RSA. Oso kriptografiaraztua sistema segurua da eta Zenbak-Teroian oinarritzen da. 1977. Urtean Ronald Rivest, Adi Shamir eta Lenard Adleman-ek sortu zuten kriptografia matematikoen bildez ulertzeko modukoa azalpena, alegia.

1 RSA zifratze-algoritmoa

Kriptografiaren gain ezaguna den RSA algoritmoa Matematika Diskreterua irakasgaiaren aztertzen dugun Zenbak-Teroian oinarritzen da. Orik hauetan oharrari matematikoa lortzen azalpen xumea dator, eskola ordetean Zenbak-Teroiatik buru zuen ikasitako kontzeptu matematikoen bildez ulertzeko moduko azalpena, alegia.

Kriptografa: RSA zifratze-algoritmoa

Matematika Diskreterua

Gako publikoa eta pribatua kalkulatzeko jarraitu beharreko urratsak honakoak dira:

1. Bi zenbaki lehen p eta q aukeratu (100 digitutik gorakoak).
2. Kalkulatu $n = p \times q$.
3. Gako publikoa (n eta r zenbakiak). $m = (p - 1) \times (q - 1)$ izanik, m zenbakiarekin lehen erlatiboa den r zenbaki bat aurkitu behar da, hau da $\text{zkh}(m,r)=1$ beteko duena. r handia aukeratzea gomendatzen da.
4. Gako pribatua (s zenbakia). r gako publikoaren alderantzizkoa modulu m den s balioa aurkitu behar da, hau da, $s = r^{-1} \bmod m$.

Ikus dezagun adibide bat zenbaki txikiak erabiliz:

1. $p = 17$ eta $q = 23$ zenbaki lehenak aukeratuko ditugu.
2. $n = p \times q = 17 \times 23 = 391 \rightarrow \boxed{n = 391}$.
3. Gako publikoa ($n = 391$, r). r zenbakia aukeratzeko:

- $m = (p - 1) \times (q - 1) = (17 - 1) \times (23 - 1) = 16 \times 22 = 352 \rightarrow m = 352$.
- $\text{zkh}(m, r) = 1 \rightarrow \text{zkh}(352, r) = 1 \rightarrow$ adibidez, $\boxed{r=3}$.

r baliorako aukera bat baino gehiago existitzen da. m zenbakiarekin lehen erlatiboa izango den horietako bat aukeratu behar da (guk txikiena, adibidez).

4. Gako pribatua (s). r -ren alderantzizkoa modulu m den s aurkitu behar dugu, $s = r^{-1} \bmod m$, hau da $rs \bmod m = 1$ beteko duena.
- $rs \bmod m = 1 \rightarrow 3s \bmod 352 = 1 \rightarrow \boxed{s=235}$. s balioa Euklidesen algoritmo hedatua erabiliz kalkulatzen da (ikus 2.1. atala).

Hortaz, gako publikoa ($n = 391$, $r = 3$) eta pribatua ($s = 235$) kalkulatuta, RSA zifratze-algoritmoarekin zifratutako mezuak jasotzeko prest dago hartzailca. Egia da gako publikoa den n zenbakia faktorizatuz, p eta q kalkula daitezkeela, eta haien m lortu ondoren, gako pribatua den s balioa kalkulatu. Hori dela eta, derrigorrezkoa gertatzen da p , q eta r zenbakiak oso handiak aukeratzea (ikus 2.2. atala).

1.2 Mezuak kodetzea/deskodetzea (M_i)

Mezu bat zifratu aurretek kodetu egin behar da, hau da, karakterez osatuta dagoen mezu orijinala zenbakitarra bihurtu behar da. Modu berean, zifratuta dagoen mezu bat deszifratu ondoren deskodetu egin beharko da, zenbakietatik abiaturik mezu orijinala osatzen duten karaktereak lortzeko.

Mezuak kodetzeko, kodeketa desberdinak existitzen dira. Kodeketa simple bat alfabetoko 26 karaktereetako 0tik 25erako digituak egokitzea da: $a \leftrightarrow 0, b \leftrightarrow 1, \dots, z \leftrightarrow 25$. Adibidez, "kaixo" mezuari dagokion mezu kodetua horrela idatziko dugu: 10, 0, 8, 23, 14.

Mezuak kodetzeko beste aukera bat ASCII karaktereen kodeketa erabiltzea da (ikus bibliografia atalean wikipedia erreferentzia). Karaktere imprimagarrien kodeketan kodeketa hamartarrari dagokion zutabea aztertzen baduzu, ikusiko duzu "kaixo" mezu ASCII kodeketa erabiliz horrela geratuko dela: 107, 97, 105, 120, 111.

$$M_5 = 111.$$

Deszifratu ondoren, mezu kodetua lortuko du: $M_1 = 107, M_2 = 97, M_3 = 105, M_4 = 120,$

- $R_5 = 304 \iff M_5 = 304^{235} \bmod 391 = 111.$
- $R_4 = 171 \iff M_4 = 171^{235} \bmod 391 = 120.$
- $R_3 = 265 \iff M_3 = 265^{235} \bmod 391 = 105.$
- $R_2 = 79 \iff M_2 = 79^{235} \bmod 391 = 97.$
- $R_1 = 40 \iff M_1 = 40^{235} \bmod 391 = 107.$

Hartzaileak mezu zifratua deszifratuko du ($s = 235$) gako pribatua erabili zu: $R_5 = 304.$

Hortza, mezu zifratua horrela geratuko da: $R_1 = 40, R_2 = 79, R_3 = 265, R_4 = 171,$

- $M_5 = 111 \iff R_5 = 111^3 \bmod 391 = 304.$
- $M_4 = 120 \iff R_4 = 120^3 \bmod 391 = 171.$
- $M_3 = 105 \iff R_3 = 105^3 \bmod 391 = 265.$
- $M_2 = 97 \iff R_2 = 97^3 \bmod 391 = 79.$
- $M_1 = 107 \iff R_1 = 107^3 \bmod 391 = 40.$

honeko kalkuluak egiten behar dira:

Adibidez, har dezagun "Kaxo" mezuari dagokion ASCII kodetekat: $M_1 = 107, M_2 = 97,$
 $M_3 = 105, M_4 = 120, M_5 = 111.$ Mezu ($n = 391, r = 3$) gako publikoa erabili zu zifratzeko

$$M_i = R_i \bmod n$$

modularreko honeko eragiketaren bidez:

Hortza, n eta s ezagunak izanik, R_i kode zifratu bakotza M_i bilturako da aritmetika Deszifratzea, aldi, gako pribatua den s balioa ezagutzen badan baterrik burutu datteke.

$$R_i = M_i \bmod n$$

eragiketaren bidez:

RSA zifratze-algoritmoearen bidez zifratza R_i bilturazea, aritmetika modularreko honeko eta r balioak erabili M_i kode bakotza R_i bilturako osatzeko duten n deszifratze-prozesuarren bidez desordenatuta duden kodenak ordenatzera lortuko du gako prihatua erabilliz, mezuaz ulergarri bilturako dulearik.

Zifratza gako publiko bat erabillitzuen da, eta mezuaz ulterezina bilturazeta da gako prihatua ezagutzen ez duten edonorentzat. Mezu zifratua jaso duten laguntza prozesuan. Zifratza gako publiko bat erabillitzuen da, eta mezuaz ulterezina bilturazeta da gako prihatua ezagutzen ez duten edonorentzat. Mezu zifratza desordenatua erabili zu zifratze-algoritmoearen bidez desordenatuta duden kodenak ordenatzera lortuko du gako prihatua erabilliz, mezuaz ulergarri bilturako dulearik.

Nolabait eseteko, mezu orrialdeari dagokzion kodenak desordenatua egiten dira zifratze-

dutako pertsonentzat izan ezik, beste guztientzat mezu zifratua ulterezina geratzen da.

Zifratze-algoritmoeak mezuak zifratzea (enkripatzeko) erabilizten dira. Hortza, bainuen-

1.3 Mezu zifratzea/deszifratzea (R_i)

2 Zenbaki teoria eta Aritmetika modularra

Esan dugun bezala, RSA zifratze-algoritmoaren oinarri matematikoan Zenbaki Teoria aurkitzen dugu. Izan ere, gako publikoaren eta pribatuaren kalkuluaren zenbaki lehenekin egiten da lan, zatitzale komunetako handiena kalkulatzen da eta zenbaki baten alderantzizko modularra kalkulatu behar da. Aritmetika modularra mezuak zifratzerakoan eta deszifratzerakoan ere erabili behar da, berreketa modularra kalkulatu behar delako. Zenbaki osoen faktorizazioari buruz ere hitz egin dugu. Atal honetan aipamen berezia egingo diogu alderantzizko modularraren kalkuluari eta zenbaki osoen faktorizazioari. Gainera, frogatuko dugu gako publikoaz zifratutakoa deszifratzea lortuko dela beti gako pribatua erabiliz.

2.1 Alderantzizko modularra

Matematikan, r zenbaki baten alderantzizko zenbakia $\frac{1}{r}$ edo r^{-1} moduan adierazitako beste zenbaki bat da, zeina r balioaz biderkatuz 1 emango duen ($rr^{-1} = 1$). Aritmetika modularrean r zenbaki baten alderantzizkoa modulu m horrela definitzen da: s zenbakia izango da, zeinarentzat $rs \bmod m = 1$ izango den. r zenbaki baten s alderantzizkoa modulu m existitzenko r zenbakiak eta m zenbakiak lehen erlatiboak izan behar dute, hau da, $\text{zkh}(r, m) = 1$ bete behar da. Adibidez, 3 zenbakiaren alderantzizkoa modulu 352 existitzen da, 3 eta 352 zenbaki lehen erlatiboak direlako, $\text{zkh}(3, 352) = 1$.

Zenbaki baten alderantzizko modularra kalkulatzeko Euklidesen algoritmoa erabili ohi da. Izan ere, frogatuta baitago r eta m bi zenbaki oso emanik, honako konbinazio linealeko s eta v koefizienteak existitzen direla:

$$\forall r, m \in \mathbb{Z} \quad \exists s, v \in \mathbb{Z} \quad \text{non} \quad \text{zkh}(r, m) = sr + vm$$

Frogatuta dago, baita, s koefizientea dela r zenbakiaren alderantzizkoa modulu m . Adibidez, $1 = (-117) \times 3 + (1) \times 352$ betetzen denez, esan dezakegu $s = -117$ dela $r = 3$ zenbakiaren alderantzizkoa modulu 352. Negatiboa denez, aritmetika modularra erabili $s = -117 = -117 + 352 = 235$ dela esango dugu. Hortaz, $s = 235$ da $r = 3$ ren alderantzizkoa modulu 352. Egiazta daiteke $3 \times 235 \bmod 352 = 1$ betetzen dela.

RSArako gako publikoa eta pribatua kalkulatzen ditugunean, r gako publikotik abiatuz s gako pribatua kalkulatzen dugu $rs \bmod m = 1$ ebatziz. Aritmetika modularraren ikuspegitik horrek esan nahi duena da, bilatzen dugun s gako pribatua r gako publikoaren alderantzizkoa dela modulu m . Gainera, $\text{zkh}(r, m) = 1$ baldintza ezartzen dugu, bilatzen dugun s hori existitzen dela ziurtatzeko.

2.2 Zenbaki osoen faktorizazioa

RSA zifratze-algoritmoan gako publikoa (n eta r balioak) eta gako pribatua (s balioa) matematikoki erlazionaturik daude; n eta r balioak ezagututa, nahikoa izango litzateke n balioaren faktorizazioa kalkulatzea p eta q lortzeko, eta horietatik m kalkulatuz, r balioaren alderantzizkoa kalkulatzea modulu m . Gako publikotik gako pribatua kalkulatzea lortzen bada, RSA enkriptatzeko sistemak porrot egin duela esango dugu.

Teorikoki hala da, baina praktikan gako publikoa ezagutu arren, oso zaila gertatzen da gako pribatua kalkulatzea, n balioaren faktorizaziorako ez delako algoritmo eraginkorrik existitzen, n hori oso handia den kasuan. Gaur egun, oso zaila da 200 digitu dituen zenbaki oso bat zenbaki lehenetan faktorizatzea, baina aldi berean 100 digitu dituen zenbaki lehen pare bat aurkitzea eta bi zenbaki horien biderkadura kalkulatzea ez da oso zaila. Hori da RSA enkriptatzeko sistemaren arrakastaren oinarria.

Hurrela lortzen da zifratutako R^i , kodera deszifratzea, eta M^i , berreskurtatzea. Oso zaila bada ere, gerta liteke $\text{zkh}(M^i, n) > 1$ izatea. Halakoretan ere Fermat-en teorema txikia erabiltz frogatzea da. M^i , berreskurtatzeko M^i , berreskurtatzen dela.

Ondorioz, $M_{\phi(n)}^i \equiv 1 \pmod{n}$ $\leftarrow (M_{\phi(n)}^i)^k \equiv 1 \pmod{n}$ $\leftarrow M^i \cdot 1 \pmod{n} = M^i$

Teorema. (Euler) $a, n \in \mathbb{Z}_+$ lehen erlatiboa izanik, $\text{zkh}(a, n) = 1$, $a_{\phi(n)} \equiv 1 \pmod{n}$.

$\text{zkh}(M^i, n) = 1$ denean, Euler-en teorema aplikatzen da.

$M_{\phi(n)}^i \pmod{n} \leftarrow M_{i+k\phi(n)}^i \pmod{n} \leftarrow M^i M_{\phi(n)}^i \pmod{n} \leftarrow M^i \pmod{n}$

eta s ekarren alderantzikoa, $rs \equiv 1 \pmod{n}$ $\leftarrow rs = 1 + k\phi(n)$, $k \in \mathbb{Z}$

$(M^i)^s \pmod{n} \leftarrow M_s^i \pmod{n}$

$R^i = M_s^i \pmod{n}$ berriketa modulararen bidez lortu dugunek,

$R_s^i \pmod{n}$

Hurretz, egin ditzagun kalkulua. R^i , kude zifratua deszifratzea:

- $rs \equiv 1 \pmod{n}$ betetzen da, hau da, $rs = 1 + k\phi(n)$, $k \in \mathbb{Z}$ izanik.
- larrauen existentziari buruzko teorema. r eta s ekarren alderantzikoa diriez, $s = r^{-1} \pmod{n}$ existitiko dela (ikus artimelka modulararen alderantzikoa modulu-gu, $\text{zkh}(m, r) = 1$, baldintza horrek berriatzen baitu alderantzikoa modularra den).
- zenbaikia askerratzekoan mirekum lehen erlatiboa den zenbakia bat askerratu diu-

izendatu dugu Eulerren fintzia, $m = \phi(n)$.

- lehen desberdinien biderkadura den kasuan $\phi(n) = (p-1)(q-1)$. m notazioaz
- Ondoren, n zenbaikiaren Eulerren fintzia kalkulatu dugun. Dakigunez, n bi zenbaiki

- p eta q bi zenbaiki lehen askerratu eta $n = p \times q$ kalkulatu dugu.

biribiliduz,

Kontuan izan behar da, r eta s zenbakiek ez direla edonola askerratuak izan. La-

da, zifratua zegotenak deszifratzea lortuko dugula? Nola frogatzea?

Zeragatik dakigun berriketa modular horren bidez hasierako M^i , lortuko dugula? Hau

$M^i = R_s^i \pmod{n}$

Hurrela, n eta s ezagutuak izanik, R^i , kude zifratua M^i , biderkiko da hurrela. Deszifratzea, aldi, gako probabilitua den s balioa ezagutzen basa berakarril burutu datiket.

$R^i = M^i \pmod{n}$

kalkulatu:

Esan dugunez, RSA zifratze-algoritmoearen bidez zifratzea zero da: gako Publikoa osatzeari duteen n eta r balioak erabiliz M^i , kude basotza R^i , biderketa modularra. Erantzuna berrehalakoa da. Eulerren teorema betetzen delako. Ikarus dezagun polikago.

2.3 Zeragatik fintzioak du RSA zifratze-algoritmoeak?

Bibliografia

1. Wikipedian eta Telekomunikazio hiztegian:
 - <http://eu.wikipedia.org/wiki/Kriptografia>
 - http://eu.wikipedia.org/wiki/Zifratze_algoritmo
 - <http://en.wikipedia.org/wiki/RSA>
 - <http://eu.wikipedia.org/wiki/ASCII>
 - http://es.wikipedia.org/wiki/Inverso_multiplicativo
 - http://es.wikipedia.org/wiki/Factorización_de_enteros
 - http://es.wikipedia.org/wiki/División_por_tentativa
 - <http://www.telekomunikaziohiztegia.org/definizioa.asp?Kodea=E68789&Hizkuntza=E&hizk=eusk>
 - <http://www.telekomunikaziohiztegia.org/definizioa.asp?Kodea=E55930&Hizkuntza=E&hizk=eusk>
2. Rivest, Shamir, Adleman - The RSA Algorithm Explained
<http://www.youtube.com/watch?v=b57zGAkNIc>
3. "Kode sekretuak (I, II, III)". Patxi Angulo, Elhuyar Zientzia eta Teknika, 78. (1993)
<http://www.aldizkaria.elhuyar.org/erreportajeak/kode-sekretuak-i-ii-iii/>
4. "Kodeen liburua. Simon Singh, Elhuyar Fundazioa, ISBN: 978-84-92457-78-6. Jatorrizko izenburua: "The Code Book".
<http://www.europapress.es/euskera/noticia-elhuyar-fundazioak-simon-singh-idazlearen-the-code-book-liburua-argitaratu-du-euskaraz-20121106134209.html>
5. "Enkriptazioa gure inguruko gauza guztieta dago". Elhuyar Zientzia eta Teknika, 291. alea (2012).
<http://aldizkaria.elhuyar.org/elkarrizketak/enkriptazioa-gure-inguruko-gauza-guztietan-dago/>
6. "Interneteko esploitza"artikulua Berria egunkarian (2003).
http://paperekoaberria.info/iritzia/2003-07-15/006/014/interneteko_esploitza.htm
7. "Kriptografia"artikulua Gara egunkarian (2008).
<http://ikusimakusi.net/eu/2008/kriptografia/>
8. "Kriptografia: Idazkera Ezkutuaren Artea", Domingo Ramirez-Alzola, Matematika saila, EKAIA (2004), UPV/EHU
<http://www.ehu.es/ojs/index.php/ekaia/article/download/2457/2049>
9. **Breaking the Code: Biography of Alan Turing** (Derek Jacobi, BBC, 1996)
http://en.wikipedia.org/wiki/Breaking_the_Code
<http://www.youtube.com/watch?v=S23yie-779k> → pelikula
"Breaking the Code"(1996). A biography of the English mathematician Alan Turing, who was one of the inventors of the digital computer and one of the key figures in the breaking of the Enigma code, used by the Germans to send secret orders to their U-boats in World War II.

Aurkibidea

Konbinatoria

Sarrera

Oinarriko zenbaketa-erregelak

Aldakuntzak. Errepikatuzko aldakuntzak

Permutazioak. Errepikatuzko permutazioak

Irakasgai: Matematika Diskretua
Titulazioa: Informatikaren Ingeniaritzako Gradua
Informatika fakultatea
Donostia

1

Konbinatoria

- Konbinatoria multzo finitu baten elementuak hautatzeko edota ordenatzeko dauden era desberdinak aztertzen dituen matematikaren alorra da.
- Kontuan hartu behar izaten diren baldintzak:
 - Multzoko elementu guztiak hartu? Ala batzuk bakarrik...
 - Elementuak errepikia daitezke?
 - Ordenak eragina al du?
- Problemak ebazteko era desberdinak egon daitezke.
- Sarri problema bat problema txikiagotan deskonposa daiteke: batuketa-errengela, biderketa-errengela.

1. Oinarriko zenbaketa-erregelak

Oinarriko zenbaketa-erregelak

Definizioa (Batzuketa-errengela)

Ataza bat m modu desberdinetara burutu badaiteke eta beste ataza bat n modu desberdinetara, eta bi ataza horiek aldiberean burutzea posiblea ez bada, orduan bi ataza horietako edozein burutzeko $m + n$ modu desberdin daude.

Definizioa (Biderketa-errengela)

Prozedura bat bi urratsetan deskonposa badaiteke, lehenengo urratserako m emaitza posible badaude, eta emaitza horietako bakoitzerako n emaitza badaude bigarren urratsean, orduan prozedura osorako $m \times n$ emaitza posible daude.

2. Aldakuntzak. Errepikatuzko aldakuntzak

2

Oinarriko zenbaketa-erregelak

Aldakuntza: Errepikatuzko aldakuntzak

Definizioa (Aldakuntzak)

n elementu ezberdin izanik, n horien arteko r elementuren ordenamendu bakoitzak r tamainako aldakuntza bat da. n objekturekin osa daitekeen r tamainako aldakuntza kopurua:

$$V(n, r) = n \cdot (n - 1) \dots (n - r + 1) = \frac{n!}{(n - r)!} \quad \text{non } 0 \leq r \leq n$$

Definizioa (Errepikatuzko aldakuntzak)

n elementurekin r tamainako aldakuntzak osatzean elementuak errepikatuta agertzea posible bada, orduan errepikatuzko aldakuntza dela esaten da. Errepikatuzko aldakuntzetaan $r \geq n$ izan daiteke. n objekturekin osa daitekeen r tamainako errepikatuzko aldakuntza kopurua:

$$VR(n, r) = n^r \quad \text{non } 0 \leq r$$

ALDAKUNTZAK, ERREPİKATUZKO ALDAKUNTZAK⁵

Konbinazioak: Errepikatuzko konbinazioak

Definizioa (Konbinazioak)

n objektu izanik, n horien artekik r objekturen aukeraketa bakoitzaz r tamainako konbinazioa dela esaten da, eta $C(n, r)$ notazioaz adierazten da. r objektuen aukeraketa egitean ordenak ez du garrantziarik. Konbinazio kopurua honela kalkulatzen da:

$$C(n, r) = \frac{V(n, r)}{P(r)} = \binom{n}{r} = \frac{n!}{(n - r)! \cdot r!}$$

Definizioa (Errepikatuzko konbinazioak)

n objekturen artean r aukeratzerakoan objektuak errepikatuta ager bidaitezke, konbinazioa errepikatuzkoa dela esaten da, eta $CR(n, r)$ notazioaz adierazten da. $r \geq n$ izan daiteke. Kopurua:

$$CR(n, r) = C(n + r - 1, r) = \binom{n + r - 1}{r}, \quad r \geq 0 \quad \text{izanik}$$

Permutazioak: Errepikatuzko permutazioak

Definizioa (Permutazioak)

n elementu izanik, n elementu horien ordenazioak n elementuren permutazioak dira, hau da, n elementuren n tamainako aldakuntzak dira. n elementurekin osa daitekeen permutazio kopurua hau da:

$$P(n) = V(n, n) = n!$$

Definizioa (Errepikatuzko permutazioak)

n elementu izanik, 1 motakoak n_1 badaude, 2 motakoak n_2, \dots, r motakoak n_r , non $n_1 + n_2 + \dots + n_r = n$ betetzen den, n elementu horien ordenazioak errepikatuzko permutazioak dira. Errepikatuzko permutazio kopurua horrela kalkulatzen da:

$$PR_{n_1, \dots, n_r}(n) = \frac{n!}{n_1! \dots n_r!}, \quad \text{non } n_1 + \dots + n_r = n \quad \text{den}$$

PERMUTAZIOAK, ERREPİKATUZKO PERMUTAZIOAK⁶

Bibliografia

- Matemáticas Discreta y Combinatoria. Una Introducción con aplicaciones. Ralph P. Grimaldi. Addison-Wesley Iberoamericana. Capítulo 1: "Principios fundamentales del Conteo"
- Lur Entziklopedia Tematikoa. Gai Unibertsalak, Matematika, Konbinatoria. <http://www.euskaraeuskadi.net/r59-lurconte/eu/contendos/articulo/c1804eu.d1804001/1804001.html>
- Maths is Fun. Combinations and Permutations Calculator. <http://www.mathsisfun.com/combinatorics/combinations-permutations-calculator.html>
- Wolfram Mathworld. The web's most extensive mathematics resource. <http://mathworld.wolfram.com/Combinatorics.html> <http://mathworld.wolfram.com/Combination.html> <http://mathworld.wolfram.com/Permutation.html>

GRAFOAK eta ZUHAITZAK

1. Grafoak

1. *Grafoak*
 - 1.1. *Sarrera.*
 - 1.2. *Definizioak.*
 - 1.3. *Erpinen graduak.*
 - 1.4. *Ibilaldiak grafoetan.*
 - 1.5. *Grafoei lotutako matrizeak.*
 - 1.6. *Azpigrafoak, grafo osagarria.*
 - 1.7. *Grafo isomorfismoa.*
 - 1.8. *Kate eta zirkuitu eulertarrak.*
 - 1.9. *Bide eta ziklo hamiltondarak.*
2. *Zuhaitzak*
 - 2.1. *Sarrera.*
 - 2.2. *Definizioak eta propietateak.*
 - 2.3. *Errodun zuhaitzak.*

1

1.1. Sarrera

Grafo teoriaren sorerra: 1736. Euler.
Königsberg-eko zazpi Zubien problema:
7 Zubien bidez komunikatutako 4 zonalde.
Zubi bakoitsetik behin pasata hasierako puntura itzuli.

1.2 Definizioak

- Grafo zuzendua: $G = (V, E)$ bikotea, non
- V multzo finitu ez hutsa erpin multzoa den.
 - $E \subseteq V \times V$ ertz multzoa den (erpin bikote ordenatuak).

1.2.1. Ertza emanik:

- ertz a eta b erpinekin intzidenteak.
- a eta b erpinak albokoak dira.
- a erpina ertzaren jatorria da.
- b erpina ertzaren amaiera da.
- Baldin $a = b$ orduan (a, a) begizta da.

3

1.2.2. Ertza emanik:

- Helburua: Elkarren artean erlazionatuta dauden objektu kopuru finitua duten egoerak eredutzea.
- Aplikazioak informatikan: sareen diseinua, zirkuitu integratuena diseinua, etab.

Erpin bakartua: ertz intzidenterik ez duena.

4

Definizioak

Grafo ez zuzendua: ertzak erpin bilkete ez ordenatuak dira. Ertzen noranzkoak ez da kontuan hartzen, $(a, b) \in E \Rightarrow (b, a) \in E$.
 Ertz ez zuzendua: $\{(a, b), (b, a)\}$.
 Begizta: $\{a, a\} = (a, a)$.

Izan bedi $G = (V, E)$ grafo zuzendua, dagokion grafo ez zuzendua: ertzen norantzka kontuan hartu gabe G -tik lortutako grafoa (ertz bakotza behin bakarrik).

$G = (V, E)$ multigrafo: existitzen badira $a, b \in V$, $a \neq b$ bi erpin, beren artean ertz bat baino gehiago dutelarik.
 Anizkoitzasuna: $(a, b) \{ (a, b) \}$ moduko ertz kopurua.
 k -grafoa: k anizkoitzasuna baino handiagoa duen ertzik ez dago.
 Kontrakorik esaten ez bada, grafoa simplea da, ez multigrafoa.

5

1.3. Erpinen graduak

- $G = (V, E)$ grafo zuzendua eta $a \in V$ erpina.
- a -ren graduerdialk:
 $d^+(a) = \#\{b \mid (a, b) \in E\}$: jatorria a -n (irteera gr.).
 $d^-(a) = \#\{b \mid (b, a) \in E\}$: amaiera a -n (sarrera gr.).
- a -ren gradua: $d(a) = d^+(a) + d^-(a)$.

- $G = (V, E)$ grafo ez zuzendua eta $a \in V$ erpina.
 a erpinaren gradua: $d(a) = a$ -rekin intzidenteak diren ertzen kopurua. (Erpinean $\{a, a\}$ begizta badago, bi ertz intzidentetzat hartuko ditugu). a erpina zintzilikatua: $d(a) = 1$. a erpina bakartua: $d(a) = 0$.

6

Erpinen graduak

Teorema
 Izan bedi m ertz duen $G = (V, E)$ grafo ez zuzendua.

$$\sum_{x \in V} d(x) = 2m$$

- x_0, x_1, \dots, x_p erpinak,
 - e_1, \dots, e_p ertzak. $e_i = \{x_{i-1}, x_i\}$
- Ibilaldiaren luzera: ertz kopurua, p .
- Baldin $p = 0$ orduan $x = y$: Ibilaldi nabaria.
 - Baldin $x = y$ eta $p \geq 1$: Ibilaldi itxia.
 - Baldin $x \neq y$: Ibilaldi irekia.

$G = (V, E)$ grafo ez zuzendu errregularra: erpin guztiek gradu bera dute. k -errregularra: erpin guztiek k gradua dute.

7

1.4. Ibilaldiak grafoetan

$G = (V, E)$ grafo ez zuzendua eta $x, y \in V$ erpinak izanik
 G -ko $x - y$ ibilaldia: honelako sekuentzia finitura

$$x = x_0, e_1, x_1, e_2, x_2, e_3, \dots, e_{p-1}, x_{p-1}, e_p, x_p = y$$

- x_0, x_1, \dots, x_p erpinak,
 - e_1, \dots, e_p ertzak. $e_i = \{x_{i-1}, x_i\}$
- Ibilaldiaren luzera: ertz kopurua, p .
- Baldin $p = 0$ orduan $x = y$: Ibilaldi nabaria.
 - Baldin $x = y$ eta $p \geq 1$: Ibilaldi itxia.
 - Baldin $x \neq y$: Ibilaldi irekia.

8

Ibilaldiak grafoetan

Izan bedi $G = (V, E)$ grafo ez zuzenduko $x - y$ ibilaldia:

- Katea: Ertz errepikaturik ez dago.
- Zirkuitua: Kate itxia ($x = y$).
- Bidea: Erpin errepikaturik ez dago.
- Zikloa: Bide itxia ($x = y$).

Akordioa: Zirkuituetan gutxienez ertz bat. Zikloetan gutxienez 3 ertz desberdin.

Grafo zuzenduetan: ibilaldi zuzenduak, kate zuzenduak, bide zuzenduak, etab.

9

Ibilaldiak grafoetan

$G = (V, E)$ grafo ez zuzendua izanik, V -ren gaineko erlazio hau baliokidetasun erlazioa da.

$x \sim y$ baldin eta soilik baldin $x - y$ ibilaldia badago

Baliokidetasun klaseak: V_1, \dots, V_q

G -ren ossgaiak: $G_1 = (V_1, E_1), \dots, G_q = (V_q, E_q)$
non $i = 1, \dots, q$, eta E_i diren V_i baliokidetasun klase bakotzeko erpinei intzidente diren ertz guztiak osatutako multzoak.

G -ren osagai kopurua: $\kappa(G)$.

G konektatua baldin eta soilik baldin $\kappa(G) = 1$.

Ibilaldiak grafoetan

Teorema.

Izan bedi $G = (V, E)$ grafo ez zuzendua eta $x, y \in V$ bi erpin, $x \neq y$. $x - y$ ibilaldia existitzen da baldin eta soilik baldin $x - y$ bidea existitzen bada.

$G = (V, E)$ grafo ez zuzendua konektatua: $x, y \in V$ edozein bi erpinetarako $x \neq y$ izanik, $x - y$ bidea baldin badago beti.

Grafo zuzendu konektatua: Dagokion grafo ez zuzendua konektatua bada.
Grafo ez konektatua: kontrako kasuan.

10

1.5 Grafoei lotutako matrizeak

Izan bedi $G = (V, E)$ begizta gabeko grafo ez zuzendua, $V = \{x_1, \dots, x_n\}$.
Albokotasun matrizea: $n \times n$ tamainako $A = (a_{ij})$ matrizea

$$a_{ij} = \begin{cases} 1 & \text{baldin } x_i, x_j \text{ albokoak} \\ 0 & \text{baldin } x_i, x_j \text{ ez albokoak} \end{cases}$$

A simetrikoa da. Diagonal nagusian: 0-ak.

$$d(x_i) = \sum_{j=1}^n a_{ij} = \sum_{j=1}^n a_{ji}$$

Teorema

Izan bitez $G = (V, E)$ begiztarik gabeko grafo ez zuzendua, $V = \{x_1, \dots, x_n\}$ eta A dagokion albokotasun matrizea. A^p matrizeko (i, j) elementua: p luzerako $x_i - x_j$ ibilaldi kopurua.

11

12

1.6 Azpografoak. Grafo osagarria

Izan bedi $G = (V, E)$ grafoa (zuzendua edo ez)
 $G_1 = (V_1, E_1)$ grafoa G -ren azpografo da baldin

- $\emptyset \neq V_1 \subseteq V$
- $E_1 \subseteq E$ (E_1 -eko ertza bakoitza V_1 -eko erpinekin intzidentea da).
- $G = (V, E)$ grafoa emanik (zuzendua edo ez); $\emptyset \neq U \subseteq V$.
 U erpin azpimultzoak induzitutako G -ren azpografoa ($< U >$):

- Erpin multzoa: U
- Ertz multzoa: $E \cap (U \times U)$ (U -ko erpinekin intzidente diren E -ko ertzak).

13

Azpografoak. Grafo osagarria

- $G = (V, E)$ (zuzendua edo ez).
- $x \in V$ erpina kenduz gero, $G - x = (V_1, E_1)$
 - $V_1 = V - \{x\}$
 - $E_1: x$ erpinari intzidente diren ertzak ezik, E -ko gainontzeko ertza guztiak.
 - ($G - x$ grafoa V_1 -ek induzitutako azpografoa da).
 - $e \in E$ ertza kenduz gero, $G - e = (V_1, E_1)$
 - $V_1 = V$
 - $E_1 = E - \{e\}$

- $V = \{x_1, \dots, x_n\}$ erpin multzoa izanik.
- V -ren gaineko grafo osotua (K_n): erpinen arteko ertz guztiak dituen begizta gabeko grafo ez zuzendua, hau da,
 - $(\forall x, y \in V) \quad x \neq y \implies \{x, y\}$ ertza existitzen da

14

Azpografoak. Grafo osagarria

- Izan bedi $G = (V, E)$ begizta gabeko grafo ez zuzendua,
 $V = \{x_1, \dots, x_n\}$.
- G -ren osagarria: $\overline{G} = (V, \overline{E})$ begizta gabeko grafoa, non G -ko erpinak dauden eta $\overline{E}: K_n$ grafoan dauden eta E -n ez dauden ertzak.

Baldin $G = K_n$ orduan \overline{G} : grafo nulua (n erpin, 0 ertz).

$G = (V, E)$ zatibiko grafoa: grafo ez zuzendua, begizta gabea, non erlazioa da.

- Existitzen dira V_1, V_2 non $V_1 \cup V_2 = V$, $V_1 \cap V_2 = \emptyset$
- G -ko $\{x, y\}$ ertza bakoitzas $x \in V_1$ eta $y \in V_2$.

Horretaz gain, $(\forall x \in V_1, \forall y \in V_2) \exists \{x, y\}$ ertza, orduan G zatibiko grafo osotua. V_1 -ek n_1 erpin badu eta V_2 -k n_2 ,

$$G = K_{n_1, n_2}$$

Azpografoak. Grafo osagarria

- $G = (V, E)$ (zuzendua edo ez).
- $x \in V$ erpina kenduz gero, $G - x = (V_1, E_1)$
 - $V_1 = V - \{x\}$
 - $E_1: x$ erpinari intzidente diren ertzak ezik, E -ko gainontzeko ertza guztiak.
 - ($G - x$ grafoa V_1 -ek induzitutako azpografoa da).
 - $e \in E$ ertza kenduz gero, $G - e = (V_1, E_1)$
 - $V_1 = V$
 - $E_1 = E - \{e\}$

1.7 Grafo isomorfismoa

- $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ grafo ez zuzenduak emanik,
 $f: V_1 \longrightarrow V_2$ funtzioa grafo isomorfismoa da baldin
- f bijektiboa.
 - $(\forall x, y \in V_1) \{x, y\} \in E_1 \iff \{f(x), f(y)\} \in E_2$, hau da, erpinen arteko albokotasunak mantentzen baditu.

G_1 eta G_2 isomorfoak. $G_1 \cong G_2$.

Isomorfia erlazioa grafoen multzoaren gaineko baliokidetasun erlazioa da.

- G_1 eta G_2 isomorfoak: funtsean berdinak. Erpinen izenean eta grafoak marratzeko moduan desberdintzen dira solik; erpin kopuru bera, ertza kopuru bera, gradu bereko erpin kopuru bera, ziklo kopuru bera, etab.

16

1.8 Kate eta zirkuitu eulertarrak

Kate eta zirkuitu eulertarrak

Izan bedi $G = (V, E)$ grafo ez zuzendua, erpin bakarturik gabea.

- Zirkuitu eulertarra: G grafoko ertz guztietatik behin eta bakarrik behin igarotzen den zirkuitua.
- Kate eulertarra: G grafoko ertz guztietatik behin eta bakarrik behin igarotzen den kate irekia.

Grafo eulertarra: zirkuitu eulertarra badu.

Teorema

$G = (V, E)$ grafo ez zuzendua eta erpin bakartu gabea.
 G -ko kate eulertarra da baldin eta soilik baldin konektatua bada eta

Izan bedi $G = (V, E)$ grafo ez zuzendua, erpin bakarturik gabea.
 G eulertarra da baldin eta soilik baldin G konektatua bada eta
 G -ko erpin guztien gradua bikoitia bada.

17

1.9 Bide eta ziklo hamiltondarra

Bide eta ziklo hamiltondarra

$G = (V, E)$ grafo ez zuzendua.
Erpin kopuria $= n \geq 3$.

- Ziklo hamiltondarra: erpin guztiak dituen zikloa.
 - Bide hamiltondarra: erpin guztiak dituen bide irekia.
- Ziklo hamiltondar bat ertz bat kentzean bide hamiltondarra lortzen da.
- Grafo hamiltondarra: ziklo hamiltondarra duen grafoa.

Korolarioa

$G = (V, E)$ ez zuzendua eta erpin bakartu gabea.
 G -ko kate eulertarra du baldin eta soilik baldin konektatua bada eta zehazki gradu bakoitiko bi erpin baditu.

Teorema

$G = (V, E)$ grafo zuzendua, erpin bakartu gabea.
 G -ko zirkuitu eulertar zuzendua du baldin eta soilik baldin konektatua bada eta edozein $x \in V$ erpinerako $d^+(x) = d^-(x)$ betetzen bada.
(Zirkuitu eulertar zuzendua: G -ko ertz bakoitzetik behin bakarrik pasatzten den zirkuitu zuzendua).

18

- G grafoa hamiltondarra bada, orduan G konektatua da eta $x \in V$ erpin guztiak $d(x) \geq 2$ gradua dute.
- Baldin $a \in V$ eta $d(a) = 2$ orduan a erpinarekin intzidenteak diren bi ertzak ziklo hamiltondarrean daude.
- Baldin $a \in V$ eta $d(a) > 2$ orduan ziklo hamiltondarra eraikitzeko, behin a erpinetik pasa garela ez ditugu a -ra intzidente diren eta erabili ez ditugun ertzak kontuan izango.
- G -rentzat ziklo hamiltondarra eraikitze-prozesuan erpin guztiak ez dituen ziklo bat ezin daiteneke itxi.

19

Kate eta zirkuitu eulertarrak

Izan bedi $G = (V, E)$ grafo ez zuzendua, erpin bakarturik gabea.

- Zirkuitu eulertarra: G grafoko ertz guztietatik behin eta bakarrik behin igarotzen den zirkuitua.
- Kate eulertarra: G grafoko ertz guztietatik behin eta bakarrik behin igarotzen den kate irekia.

Grafo eulertarra: zirkuitu eulertarra badu.

Teorema

$G = (V, E)$ grafo ez zuzendua eta erpin bakartu gabea.
 G -ko kate eulertarra du baldin eta soilik baldin konektatua bada eta

Izan bedi $G = (V, E)$ grafo ez zuzendua, erpin bakarturik gabea.
 G eulertarra da baldin eta soilik baldin G konektatua bada eta
 G -ko erpin guztien gradua bikoitia bada.

17

1.9 Bide eta ziklo hamiltondarra

Bide eta ziklo hamiltondarra

$G = (V, E)$ grafo ez zuzendua.
Erpin kopuria $= n \geq 3$.

- Ziklo hamiltondarra: erpin guztiak dituen zikloa.
 - Bide hamiltondarra: erpin guztiak dituen bide irekia.
- Ziklo hamiltondar bat ertz bat kentzean bide hamiltondarra lortzen da.
- Grafo hamiltondarra: ziklo hamiltondarra duen grafoa.

Korolarioa

$G = (V, E)$ ez zuzendua eta erpin bakartu gabea.
 G -ko kate eulertarra du baldin eta soilik baldin konektatua bada eta zehazki gradu bakoitiko bi erpin baditu.

Teorema

$G = (V, E)$ grafo zuzendua, erpin bakartu gabea.
 G -ko zirkuitu eulertar zuzendua du baldin eta soilik baldin konektatua bada eta edozein $x \in V$ erpinerako $d^+(x) = d^-(x)$ betetzen bada.
(Zirkuitu eulertar zuzendua: G -ko ertz bakoitzetik behin bakarrik pasatzten den zirkuitu zuzendua).

18

- G grafoa hamiltondarra bada, orduan G konektatua da eta $x \in V$ erpin guztiak $d(x) \geq 2$ gradua dute.
- Baldin $a \in V$ eta $d(a) = 2$ orduan a erpinarekin intzidenteak diren bi ertzak ziklo hamiltondarrean daude.
- Baldin $a \in V$ eta $d(a) > 2$ orduan ziklo hamiltondarra eraikitzeko, behin a erpinetik pasa garela ez ditugu a -ra intzidente diren eta erabili ez ditugun ertzak kontuan izango.
- G -rentzat ziklo hamiltondarra eraikitze-prozesuan erpin guztiak ez dituen ziklo bat ezin daiteneke itxi.

20

Bide eta ziklo hamiltondarra

Grafo hamiltondarra karakterizatzeko ez dago beharrezko eta nahikoan den baldintzarik.

Teorema

Izan bedi $G = (V, E)$ begizta gabeko grafo ez zuzendua, n ≥ 3 erpinekoa. Baldin

$$\forall x, y \in V \quad (x \neq y) \quad d(x) + d(y) \geq n - 1$$

orduan G -k bide hamiltondarra du.

Korolarioa

Izan bedi $G = (V, E)$ begizta gabeko grafo ez zuzendua, n erpin dituena. Baldin

$$\forall x \in V, \quad d(x) \geq \frac{n-1}{2}$$

orduan G -k badu bide hamiltondarra.

21

Bide eta ziklo hamiltondarra

Teorema
Izan bedi $G = (V, E)$ begizta gabeko grafo ez zuzendua, n ≥ 3 erpinekoa. Baldin

$$\forall x, y \in V \quad (x, y \text{ ez albokoak}) \quad d(x) + d(y) \geq n$$

orduan G hamiltondarra da.

Korolarioa

$G = (V, E)$ begizta gabeko grafo ez zuzendua, n ≥ 3 erpinekoa. Baldin

$$\forall x \in V \quad d(x) \geq \frac{n}{2}$$

orduan G hamiltondarra da.

22

Bide eta ziklo hamiltondarra

Teorema
Baldin $G = (V, E)$ hamiltonarra, orduan edozein $V' \subset V$ azpimultzortzentzat, $\emptyset \neq V' \neq V$,

$$\kappa(G - V') \leq |V'|$$

Izan bedi $T = (V, E)$ begizta gabeko grafo ez zuzendua.

- $(G - V' = (V_1, E_1)$ non $V_1 = V - V'$ eta E_1 multzoan V' -ko erpinekin intzidente diren ertzaek ezik gainontzeko E ko ertz guztia daude).
- Grafo konektatu baten zuhaitz sortzaile esaten zaio zuhaitza den azpografo sortzaile orori.

Bide eta ziklo hamiltondarra

Teorema
Izan bedi $G = (V, E)$ begizta gabeko grafo ez zuzendua, n ≥ 3 erpinekoa. Baldin

$$\forall x, y \in V \quad (x, y \text{ ez albokoak}) \quad d(x) + d(y) \geq n$$

orduan G hamiltondarra da.

Korolarioa

$G = (V, E)$ begizta gabeko grafo ez zuzendua, n ≥ 3 erpinekoa. Baldin

$$\forall x \in V \quad d(x) \geq \frac{n}{2}$$

orduan G hamiltondarra da.

23

Zuhaitzak

2.1 Sarrean.

2.2 Definiziak

- Hastapenak: Kirchhoff (1847). Cayley (1857).
- Aplikazioak: Datu egiturak, sailkapen teknikak, kodifikazio teoria, optimizazio problemak...

Izan bedi $T = (V, E)$ begizta gabeko grafo ez zuzendua.

- Zuhaitza da baldin konektatua bada eta ziklorik ez badu.
- Basoa da baldin grafoaren osagai bakoitza zuhaitza bada.
- Grafo konektatu baten zuhaitz sortzaile esaten zaio zuhaitza den azpografo sortzaile orori.

24

Zuhaitzak

2.2 Proprietateak

Teorema

T zuhaitzaren edozein bi erpin a eta b, $a \neq b$ emanik, $a - b$ bide bat eta bakarra dago erpin hauen artean.

Ondorioz, T zuhaitzari ertz bat kenduz deskonektatu egiten da eta zuhaitz diren bi osagai konektatu sortuko dira.

Teorema

G grafo ez zuzendua izanik, G konektatua da baldin eta soilik baldin zuhaitz sortzailea badu.

Teorema

T zuhaitzak n erpin eta m ertz baditu, orduan $n = m + 1$.

25

2.3 Errodon zuhaitzak

Izan bedi T grafoa.

- T zuhaitz zuzendua: zuhaitz ez zuzendu bateko ertzei noranzkoa emanaz lortzen den grafo zuzendua.
- T errodon zuhaitza: r erpina badago, erro deitua, 0 sarrera gradua duena ($d^-(r) = 0$), eta beste x erpin guztien sarrera gradua 1 bada ($d^-(x) = 1$).

Zuhaitz errodonetarako terminologia:

- Hostoa: 0 irteera gradua duten v erpinak: $d^+(v) = 0$.
- Gainontzekoak barne erpinak dira.
- v erpina zuhaitzaren / mailan dago, baldin r errrotik v erpinerako bidearen luzera / bada. Hostoen mailarik handienari zuhaitzaren altuera esaten zaio.
- Zuhaitz errodonak (v_1, v_2) ertza badu, v_1 erpina v_2 -ren ama da; v_2 erpina v_1 -en alaba.
- Baldin v_1 -etik v_2 -rako bide zuzendua badago, v_1 erpina v_2 -ren arbasoa da eta v_2 erpina v_1 -en ondorengoa.

Zuhaitzak

2.2 Proprietateak

Teorema

T zuhaitzak $n \geq 2$ erpin baditu, orduan gutxienez 2 erpin zintzilikatu (bat gradukoak) ditu.

Teorema

Izan bedi $G = (V, E)$ begizta gabeko grafo ez zuzendua, n erpin eta m ertz dituena. Honakoak baliokideak dira.

- i) G zuhaitza da.
- ii) G grafoak ez du ziklorik eta $n = m + 1$.
- iii) G konektatua da eta $n = m + 1$.

26

Errodon zuhaitzak

Izan bitez $T = (V, E)$ zuhaitz erroduna, $p \in \mathbb{Z}^+$ ($p \geq 1$).

- T zuhaitz p -tarra: $d^+(x) \leq p$ edozein $x \in V$ -rako, hau da, barne erpin bakoitzak gehienez p alaba baditu.
- T zuhaitz p -tar osotua: $d^+(x) = 0$ edo $d^+(x) = p$ edozein $x \in V$, hau da, barne erpin bakoitzak zehazki p alaba baditu.

Teorema

Izan bedi $T = (V, E)$ zuhaitz p -tar osotua, n erpin dituena, hauetatik h hostoak eta i barne erpinak izanik. Honako erlazioak betetzen dira.

- $n = p \cdot i + 1$
- $h = (p - 1) \cdot i + 1$

27

28

ZUHAITZAK

1. Aurkitu $K_{2,3}$ grafoaren zuhaitz sortzaile bat.
2. Baldin G grafo ez zuzendua konektatua bada eta 30 ertz baditu, zenbat erpin ditu gehienez?
3. Zuhaitz batek $2k$ erpin ditu gradu batekoak, $3k$ erpin bi gradukoak eta k erpin hiru graduokoak. Kalkulatu k , erpin kopurua eta ertz kopurua. Marratzu honetako zuhaitz bat.
4. Nolako zuhaitzek dituzte zehazki bi erpin zintzilikatu?
5. Zuhaitz batean v_1 erpin zintzilikatu baditugu, lau erpin 2 graduokoak, erpin bat 3 graduokoak, bi 4 graduokoak, eta bat 5 graduokoak, kalkulatu v_1 .
6. G grafo ez zuzenduak v erpin, e ertz eta k osagai baditu, frogatu $e \geq v - k$ betetzen dela.
7. Izan bedi $T = (V, E)$ zuhaitza, $|V| = n$ erpin dituena. Zuhaitz honetako erpin guziak 1 edo 3 graduokoak dira. Frogatuzazu 3 graduoko $\frac{n-2}{2}$ erpin dagoela.
8. Izan bedi T , $n = 21$ erpindun zuhaitza, erpinen graduak 1, 3, 5 edo 6 izanik. Demagun T zuhaitzak 15 hosto eta 6 graduoko erpin bakarra dituela. 5 graduoko zerbat erpin ditu?
9. Izan bedi $T = (V, E)$ zuhaitza. Frogatuzazu T zuhaitzean $k > 2$ graduoko erpin bat baldin badago, orduan badagela gutxienez k erpin zintzilikatu.

