

Učinkovito razlikovanje ključev

↓↓↓

JANJA JEREBIC

→ Skoraj vsak izmed nas se je že kdaj znašel v situaciji, ko je s šopom bolj ali manj enakih ključev stal pred zaklenjenimi vrati in iskal pravega. Problem učinkovitega razlikovanja ključev je leta 1979 predstavil Frank Rubin v reviji *Journal of Recreational Mathematics*¹ s spodnjo nalogo, katere rešitev je bila v omenjeni reviji objavljena leta 1980, podana pa je tudi v knjigi z naslovom: *Which Way Did the Bicycle Go?*²

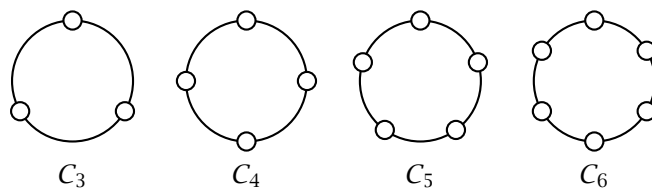
Profesor, ki je slep, ima svoje ključe zbrane na okroglem nosilcu. Na razpolago ima ℓ različnih vrst oznak (obročev) za ključe, ki jih je mogoče ločiti po otipu. Vsako od ℓ oznak lahko uporabi poljubno mnogokrat. Ključev brez oznak profesor ne loči. Koliko ključev ima lahko na nosilcu, da bo ob uporabi ℓ različnih oznak znal izbrati pravega, četudi se mu bo nosilec zavrtel ali obrnil?

Recimo, da želimo na nosilcu imeti točno določeno število ključev. Potem vprašanje zastavimo takole:

Najmanj koliko različnih oznak potrebuje profesor, da bo ločil med svojimi n ključi?

Če ima profesor le en ključ, je jasno, da posebne oznake zanj ne potrebuje. V primeru več ključev je ključ brez oznake označen s tem, da nima dodatne oznake. Zato bomo v nadaljevanju predpostavili, da so vsi ključi označeni. Za en ključ na nosilcu je torej dovolj ena oznaka. Kaj pa, če ima dva ključa? Ker se nosilec lahko obrne ali zavrti, ključev ne bo mogoče

razlikovati, če bosta enako označena. Potrebni sta torej vsaj dve različni oznaki in dve sta tudi dovolj. Jasno je namreč, da bo ključ mogoče vedno prepoznati, če bodo njihove oznake paroma različne. Naša naloga pa je, da poiščemo najmanjše potrebno število različnih oznak za učinkovito razlikovanje med ključi.

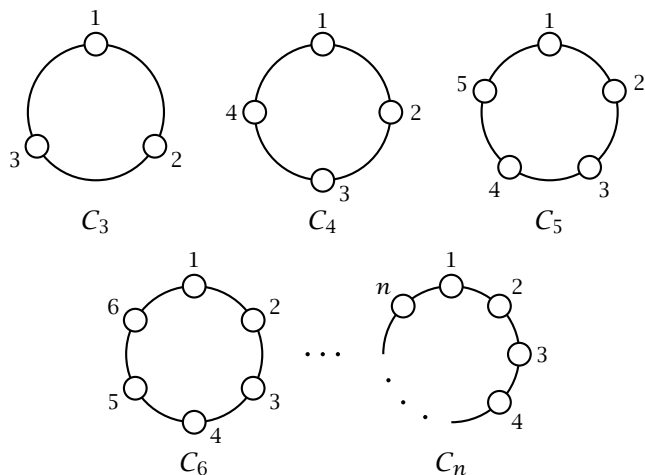


SLIKA 1.
Cikli

Pri reševanju naloge za tri ali več ključev si bomo pomagali z orodji teorije grafov. O osnovnih pojmihi teorije grafov je Presek pisal že v prispevku *Stopnje točk grafov v nalogah*, ki je bil objavljen v drugi številki letnika 26, še več o grafih pa lahko preberete v knjigi R. J. Wilson in J. J. Watkins, *Uvod v teorijo grafov*, Knjižnica Sigma 63, DMFA, Ljubljana, 1997. Okrogli nosilec z n ključi, kjer je $n \geq 3$, bomo identificirali s ciklom na n vozliščih, ki ga označimo s C_n . Vsako vozlišče cikla bo predstavljalo enega od ključev. Na sliki 1 so prikazani cikli C_3 , C_4 , C_5 in C_6 , ki po vrsti predstavljajo nosilce s tremi, štirimi, petimi in šestimi ključi. V ciklu C_n je vsako vozlišče stopnje dva, kar pomeni, da ima natanko dve sosedni vozlišči. Če cikel C_n poljubno zavrtimo ali obrnemo, spet dobimo cikel C_n . Čeprav se položaj vozlišč pri tem lahko spremeni, se strukturne značilnosti grafa ohranijo. Gre torej za bijektivno preslikavo objekta samega vase, ki ohranja sosednost in nesosednost med vozlišči. Rečemo ji *avtomorfizem* ali *simetrija* grafa. Formalno avtomorfizem definiramo takole:

¹Frank Rubin, *Problem 729*, Journal of Recreational Mathematics volume 11, p. 128, 1979.

²J. Konhauser, D. Velleman in S. Wagon, *Which Way Did the Bicycle Go?*, Dolciani series, Mathematical Association of America, Washington, DC, 1996.



SLIKA 2.

Cikli z oštevilčenimi vozlišči

Naj bo G graf z množico vozlišč $V(G)$ in množico povezav $E(G)$. Bijektivna preslikava $\sigma : V(G) \rightarrow V(G)$ je avtomorfizem grafa G natanko tedaj, ko velja $uv \in E(G) \iff \sigma(u)\sigma(v) \in E(G)$.

Avtomorfizem σ grafa G je pravzaprav permutacija njegovih vozlišč, ki ohranja sosednost med vozlišči (zadošča pogoju iz zgornje definicije). O permutacijah je Presek že pisal v tretji številki letnika 16, in sicer v prispevku *O igri petnajst in permutacijah*. Permutacijo σ lahko podamo na več načinov. Eden od njih je prikaz s tabelo, kjer v zgornjo vrstico zapišemo elemente množice $V(G)$, v spodnjo pa njihove slike. Če vozlišča cikla C_n po vrsti označimo s števili $1, 2, \dots, n$, kot je prikazano na sliki 1, potem tabela permutacije $\sigma : V(C_n) \rightarrow V(C_n)$ izgleda takole:

$$\sigma : \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}.$$

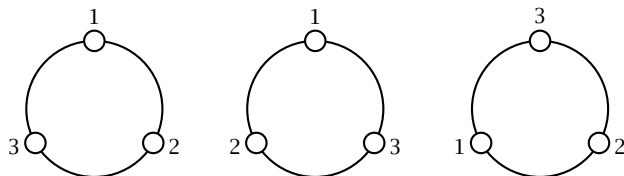
Število vseh permutacij množice z n elementi je enako $n! = n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1$. Permutaciji σ , za katero je $\sigma(i) = i$ za vsak $i = 1, 2, \dots, n$, rečemo *identična permutacija* oz. *trivialni avtomorfizem* (identiteta).

Trije ključi

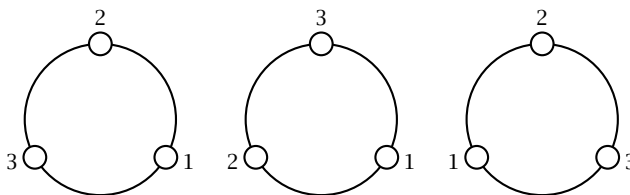
Začeli bomo s primerom treh ključev oz. s ciklom C_3 . Vozlišča cikla C_3 označimo s števili 1, 2 in 3 kot na sliki 2. Spodaj je zapisanih vseh $3! = 6$ permutacij

vozlišč iz množice $V(C_3)$. Hitro lahko ugotovimo, da je vsaka od njih tudi avtomorfizem cikla C_3 , saj ohranja sosednost med vozlišči, kot je prikazano na sliki 3.

$$\sigma_1 : \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_2 : \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \sigma_3 : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$



$$\sigma_4 : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \sigma_5 : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma_6 : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$



SLIKA 3.

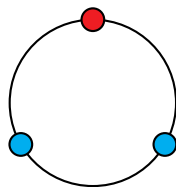
Avtomorfizmi cikla C_3

Najmanj koliko različnih oznak potrebuje profesor, da bo razlikoval tri ključe na okroglem nosilcu? Da je odgovor tri, ste verjetno že ugotovili, kljub temu pa razmislimo zakaj.

Poiskati moramo takšno označitev vozlišč cikla C_3 , ki jo bo ohranjal le trivialni avtomorfizem. To pomeni, da po nobeni netrivialni simetriji nosilca za ključe razporeditev označenih ključev ne bo enaka začetni. Profesor bo zagotovo potreboval vsaj dve različni oznaki, saj v nasprotnem primeru vsak izmed šestih avtomorfizmov ohranja označitev. Toda zakaj dve oznaki nista dovolj? Pri poljubni označitvi treh ključev z dvema različnima oznakama bosta imela dva ključa zmeraj enako oznako. Oznaki bomo na slikah označevali z modro in rdečo barvo.

Oglejmo si sedaj označitev na sliki 4. Predpostavimo, da je profesor iz žepa potegnil nosilec s tako označenimi ključi. Ker ima le en ključ rdečo oznako, ki se po otipu razlikuje od modre oznake, ga bo hitro





SLIKA 4.

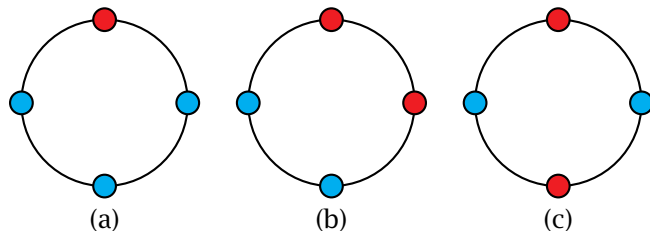
Označitev cikla C_3 z dvema oznakama

prepoznal. Preostala dva ključa imata enaki oznaki. Eden od njiju je sicer na levi in drugi na desni strani rdečega ključa, a kaj, ko ne ve, če in kolikokrat se mu je nosilec obrnil. Zato taka označitev z dvema oznakama ne bo dobra, saj smo našli netrivialno simetrijo cikla C_3 , ki to označitev ohranja. Za ta konkretni primer je to simetrija σ_2 s slike 3. Rečemo tudi, da označitev ni *razlikovalna*. Označitev vozlišč poljubnega grafa G je razlikovalna, če jo ohranja le trivialni avtomorfizem grafa G . Na podoben način kot zgoraj hitro ugotovimo, da nobena označitev vozlišč cikla C_3 z dvema različnima oznakama ni razlikovalna. Profesor bo zato moral vsakega od treh ključev označiti drugače.

Štirje ključ

Ugotovili smo že, da sta za dva ključa potrebni dve različni oznaki, za tri ključa pa tri različne oznake. Bodo zato za štiri ključe potrebne štiri različne oznake? Razmislimo. Graf, ki predstavlja okrogli nosilec s štirimi ključmi, je cikel C_4 . Označitev njegovih vozlišč z eno oznako ni razlikovalna, saj jo ohranjajo vsi avtomorfizmi cikla C_4 . Preden nadaljujete z branjem, jih zapišite. Za razliko od permutacij vozlišč iz množice $V(C_3)$, od katerih vsaka določa avtomorfizem cikla C_3 , je v primeru cikla C_4 le tretjina takih.

Preverimo sedaj, ali obstaja razlikovalna označitev vozlišč cikla C_4 z dvema oznakama. Na slikah ju bomo označili z rdečo in modro barvo. Glede na število oznak posamezne barve sta možnosti dve, $1 + 3$ in $2 + 2$, pri čemer sta pri drugi možnosti mogoči dve različni razporeditvi oznak. Če upoštevamo še vse simetrije cikla C_4 , obstajajo le tri različne označitve njegovih vozlišč z dvema različnima oznakama. Priказane so na sliki 5. Je katera od njih razlikovalna? Odgovor je ne. Predstavlajte si, da so vozlišča cikla C_4 označena s števili od 1 do 4 kot na sliki 2. Potem



SLIKA 5.

Označitve cikla C_4 z dvema oznakama

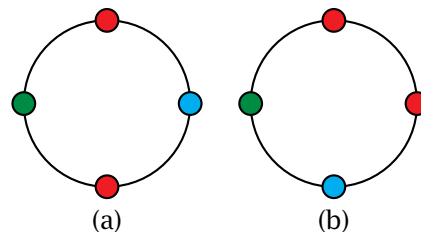
lahko za vsako od označitev (a), (b) in (c) najdemo netrivialni avtomorfizem, ki jo ohranja:

$$(a) : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \quad (b) : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$(c) : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

Kaj pa, če uporabimo tri različne oznake? Modri in rdeči dodajmo še zeleno. Pri vsaki taki označitvi bosta zmeraj dve vozlišči enako označeni. Če upoštevamo še različne razporeditve oznak in simetrije grafa, ugotovimo, da obstajata le dve različni označitvi vozlišč cikla C_4 s tremi različnimi oznakami. Priказani sta na sliki 6.

Netrivialnega avtomorfizma, ki ohranja označitev 6(a), ni težko najti. A veste, kateri je? Za označitev 6(b) na prvi pogled ni videti, da bi tak avtomorfizem obstajal. Razmislimo sedaj, kaj mora veljati za avtomorfizem grafa na sliki 6(b), ki ohranja njegovo označitev. Ker avtomorfizem ohranja označitev, se lahko vozlišče določene barve preslika le v vozlišče



SLIKA 6.

Označitvi cikla C_4 s tremi oznakami

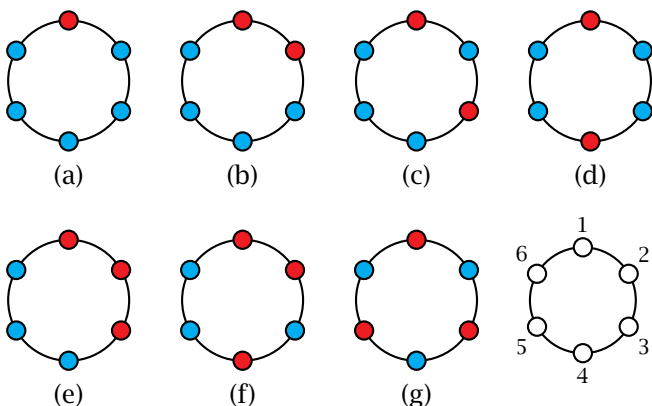
enake barve. To pomeni, da mora tak avtomorfizem fiksirati vozlišči modre in zelene barve (ju preslikati sami vase), saj sta edini vozlišči take barve. Ostneta še vozlišči rdeče barve. Avtomorfizem, ki fiksira tudi ti dve vozlišči, je identiteta, avtomorfizem, ki bi zamenjal rdeči vozlišči in hkrati fiksiral modro in zeleno vozlišče, pa ne obstaja. Avtomorfizmi ohranjajo sosednost med vozlišči in zato zamenjava rdečih vozlišč, ki imata paroma različne barve sosednih vozlišč, ni mogoča. S tem smo dokazali, da je označitev s slike 6(b) razlikovalna označitev cikla C_4 s tremi oznakami, in ugotovili, da profesor za učinkovito razlikovanje med štirimi ključi na okroglem nosilcu ne bo potreboval štirih, ampak le tri različne oznake.

Pet ključev

Obravnavo primera s petimi ključi prepustimo zainteresiranemu bralcu, ki naj dokaže, da so za razlikovanje med petimi ključi na okroglem nosilcu prav tako potrebne (in zadostne) tri različne oznake.

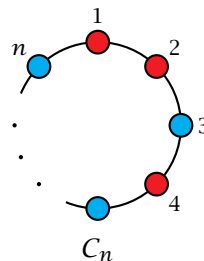
Šest ali več ključev

Bodo tri oznake potrebne tudi, če imamo na nosilcu šest ključev? Oglejmo si še ta primer. Da potrebujemo vsaj dve oznaki, je očitno. Vse možne označitve cikla C_6 z dvema oznakama (do simetrije natančno) so prikazane na sliki 7.



SLIKA 7.

Označitve cikla C_6 z dvema oznakama



SLIKA 8.

Označitev cikla C_n , $n > 6$, z dvema oznakama

Pričakovali bi, da bomo za vse primere hitro našli avtomorfizem, ki ohranja označitev. Toda za označitev (f) na sliki 7 je videti, da takega avtomorfizma ni (za vse ostale obstaja – poišcite ga!). Osredotočimo se sedaj na označitev (f) in si oglejmo njene posebnosti. Prva od teh je, da obstaja le eno rdeče vozlišče (4) z dvema modrima sosedama (3 in 5), od koder sledi, da ga avtomorfizem, ki ohranja označitev, mora fiksirati. Prav tako obstaja le eno modro vozlišče (3) z dvema rdečima sosedama (2 in 4), ki se bo zato tudi preslikalo samo vase. Vsako vozlišče v ciklu ima natanko dve sosedni vozlišči. Če avtomorfizem neko vozlišče fiksira, lahko ta isti avtomorfizem njegovi sosedni vozlišči bodisi fiksira bodisi zamenja. Če je eno od sosednih vozlišč fiksno, mora biti tudi drugo. Z zaporedno uporabo zgornjega razmisleka po vrsti ugotovimo, da so poleg vozlišč 3 in 4 fiksna še vozlišča 2, 5, 1 in 6 cikla C_6 s slike 7(f). Pri tem je bilo ključno to, da smo našli dve sosedni vozlišči cikla, ki ju mora poljuben avtomorfizem, ki ohranja označitev, fiksirati.

Predstavljajte si sedaj, da med vozlišči 5 in 6 cikla s slike 7(f) vrinemo še poljubno dolgo verigo modrih vozlišč in na ta način dobimo označen cikel C_n , kjer je $n > 6$ (slika 8). Tak cikel spet vsebuje natanko eno rdeče vozlišče z dvema modrima sosedama in natanko eno modro vozlišče z dvema rdečima sosedama. Zato mora avtomorfizem, ki ohranja označitev, ti dve vozlišči fiksirati. Omenjeni vozlišči sta poleg tega še sosedni. Ker ima vsako od njiju natanko dve sosedni vozlišči, od katerih je eno fiksno, mora biti tudi drugo fiksno. S tem posopkom nadaljujemo in ugotovimo, da je edini avtomorfizem cikla C_n , ki ohranja označitev s slike 8, identiteta. Rezultat je dokaj presenetljiv. Pričakovali bi, da bomo za





razlikovanje med več ključi potrebovali več različnih oznak, a se je izkazalo drugače – če ima profesor na okroglem nosilcu šest ali več ključev, bo za učinkovito razlikovanje med njimi potreboval le dve različni oznaki.

Razlikovalno število grafa

Zgoraj predstavljeni problem so raziskovalci pred približno dvajsetimi leti posplošili tako, da nosilec za ključe ni bil več nujno okrogel in da so definirali **razlikovalno število** poljubnega grafa G , $D(G)$ kot najmanjše število d , za katerega obstaja razlikovalna označitev grafa G z d različnimi oznakami. Koncept razlikovalnega števila je bil vpeljan v članku M. O. Albertson in K. L. Collins, *Symmetry breaking in graphs*, Electron. J. Combin. 3(1996), R18. Danes smo torej določili razlikovalno število ciklov in ugotovili, da je $D(C_3) = D(C_4) = D(C_5) = 3$ ter $D(C_n) = 2$ za $n \geq 6$. O znanih razlikovalnih številih drugih grafov pa več kdaj drugič.

× × ×

Naloga

↓↓↓

MARKO RAZPET

→ Izračunaj

$$\blacksquare 6^2 - 5^2, 56^2 - 45^2, 556^2 - 445^2, 5556^2 - 4445^2.$$

Nato rezultate posploši na razliko kvadratov oblike

$$\blacksquare \underbrace{55\dots 5}_n 6^2 - \underbrace{44\dots 4}_n 5^2.$$

Rešitev

Uporabimo enakost $a^2 - b^2 = (a - b)(a + b)$ in dobimo:

$$\blacksquare 6^2 - 5^2 = (6 - 5)(6 + 5) = 1 \cdot 11 = 11,$$

$$\blacksquare 56^2 - 45^2 = (56 - 45)(56 + 45) = 11 \cdot 101 = 1111,$$

$$\blacksquare 556^2 - 445^2 = (556 - 445)(556 + 445) = 111 \cdot 1001 = 111111,$$

$$\blacksquare 5556^2 - 4445^2 = (5556 - 4445)(5556 + 4445) = 1111 \cdot 10001 = 11111111.$$

Predvidevamo, da velja enakost

$$\blacksquare \underbrace{55\dots 5}_n 6^2 - \underbrace{44\dots 4}_n 5^2 = \underbrace{11\dots 1}_{2n+2}. \quad (1)$$

Če hočemo (1) zares izpeljati, ne le uganiti, se moramo spomniti, kaj desetiški mestni zapis števil pomeni. 1949 je npr. le krajši zapis števila $1 \cdot 10^3 + 9 \cdot 10^2 + 4 \cdot 10 + 9$. Brez težav pa lahko krajše izrazimo vsoto $S_n = 1 + q + q^2 + \dots + q^n$, kjer je q poljubno število, ki ni enako 1, n pa poljubno naravno število. Ker je $qS_n = q + q^2 + q^3 + \dots + q^n + q^{n+1} = S_n - 1 + q^{n+1}$, dobimo S_n iz enačbe $qS_n = S_n + (q^{n+1} - 1)$:

$$\blacksquare S_n = 1 + q + q^2 + \dots + q^n = \frac{q^{n+1} - 1}{q - 1}.$$

V posebnem primeru $q = 10$ je

$$\blacksquare 1 + 10 + 10^2 + \dots + 10^n = \frac{1}{9}(10^{n+1} - 1). \quad (2)$$

Enakost (1) lahko sedaj z uporabo mestnega zapisa in (2) preverimo tako:

$$\begin{aligned} \blacksquare \underbrace{55\dots 5}_n 6^2 - \underbrace{44\dots 4}_n 5^2 &= \\ &= (\underbrace{55\dots 5}_n 6 - \underbrace{44\dots 4}_n 5)(\underbrace{55\dots 5}_n 6 + \underbrace{44\dots 4}_n 5) = \\ &= \underbrace{11\dots 1}_{n+1} \cdot \underbrace{100\dots 01}_n = \\ &= (10^n + \dots + 10 + 1)(10^{n+1} + 1) = \\ &= \frac{1}{9}(10^{n+1} - 1)(10^{n+1} + 1) = \frac{1}{9}((10^{n+1})^2 - 1) = \\ &= \frac{1}{9}(10^{2n+2} - 1) = \\ &= 1 + 10 + \dots + 10^{2n+1} = \underbrace{11\dots 1}_{2n+2}. \end{aligned}$$

× × ×