Diskretne Strukture

Gašper Fijavž

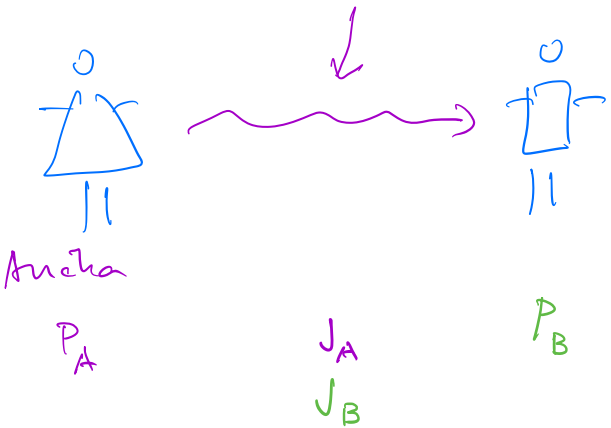
Fakulteta za računalništvo in informatiko
Univerza v Ljubljani

27. december 2021

Asimetrična kriptografija

RSA kriptosistem deluje na principu *javnih* in *privatnih ključev*.

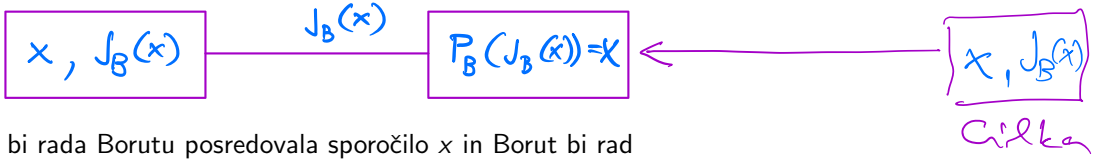
Pogovarjajmo se o dveh uporabnikih *Ančki* in *Borutu*. Vsak izmed njiju ima svoj *privatni ključ* P_A, P_B, ki ga hrani na skrivnem mestu, svoj *javni ključ* J_A, J_B da na vpogled vsem.



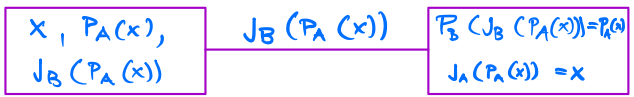
Asimetrična kriptografija

Komunikacija med Ančko in Borutom:

- Ančka bi rada Borutu posredovala sporočilo x:



- Ančka bi rada Borutu posredovala sporočilo x in Borut bi rad bil prepričan, da mu je sporočilo res posredovala Ančka:



Veljati mora:

1. P_A in J_A kot tudi P_B in J_B sta *inverzni preslikavi*.
2. Če poznamo J_A iz tega ne moremo (vsaj ne enostavno) izračunati P_A.

Teoretične osnove

Trditev

Naj bosta p in q različni praštevili. Potem je

$$a \equiv b \pmod{p} \quad in \quad a \equiv b \pmod{q}$$

natanko tedaj, ko je

$$a \equiv b \pmod{pq}.$$

Dokaz

$a-b$ je večkratnik p
$a-b$ je večkratnik q
$\Updownarrow$
$a-b$ je večkratnik $p \cdot q$

Trditev

Naj bosta p in q različni praštevili. Potem za poljubni naravni števili a in k velja

$$a^{k\cdot\varphi(pq)+1} \equiv a^{k\cdot(p-1)(q-1)+1} \equiv a \pmod{pq}$$

$e \cdot d = k \cdot \varphi(p \cdot q) + 1$

p, q

(a, d)

Izrek (Eulerjev)

Naj bo $a \in \mathbb{Z}$, $m \geq 2 \in \mathbb{N}$ in $a \perp m$. Potem je

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

$(a^e)^d \equiv a \pmod{m}$

Izrek (mali Fermatov)

Če je p praštevilo in $a \perp p$, potem je

$$a^{(p-1)} \equiv 1 \pmod{p}.$$

Za vse $a \in \mathbb{Z}$ pa velja

$$a^p \equiv a \pmod{p}.$$

Dokaz. Po MFI

$a^{p-1+1} \equiv a^p \equiv a \pmod{p}$ $\Big\}\, a^{p-1}$

$a^{2(p-1)+1} \equiv a^{p-1+1} \pmod{p}$

$a^{3(p-1)+1} \equiv a^{2(p-1)+1} \pmod{p}$

$a^{4(p-1)+1} \equiv a^{3(p-1)+1} \pmod{p}$

$\vdots$

$a^{\ell(p-1)+1} \equiv a^{(\ell-1)(p-1)+1} \pmod{p}$

$a \equiv a^{(p-1)+1} \equiv a^{2(p-1)+1} \equiv \dots \equiv a^{\ell(p-1)+1} \pmod{p}$

$a \equiv a^{(q-1)+1} \equiv a^{2(q-1)+1} \equiv \dots \equiv a^{\ell'(q-1)+1} \pmod{q}$

$\ell = k(q-1)$

$\ell' = k(p-1)$

Kriptografsko ozadje

Sloni na dejstvu, da je *težko* razcepiti naravno število na prafaktorje.

Trenutno se zdi dovolj, da je n 2048 bitno število. Najbolj bi bilo, da bi bili praštevili p in q primerljivi po velikosti, torej 1024 bitni. V desetiškem sestavu to pomeni, da gre za približno 300-mestni števili.

Čez prst je (v povprečju) pri 300 mestnih številih vsako 700-to število tudi praštevilo.

Kako poiskati praštevila?

Praštevila je načeloma težko poiskati, toda obstajajo verjetnosti algoritmi, ki hitro in učinkovito poiščejo naravno število, ki je z veliko verjetnostjo (0.99999999999) praštevilo.

Izrek (mali Fermatov, poenostavljen)

Če je p praštevilo, potem za vse $a \in \mathbb{Z}$ velja

$$a^p \equiv a \pmod{p}.$$

$a = 2, 3, 4, 5, 6, 7, 8, \ldots$

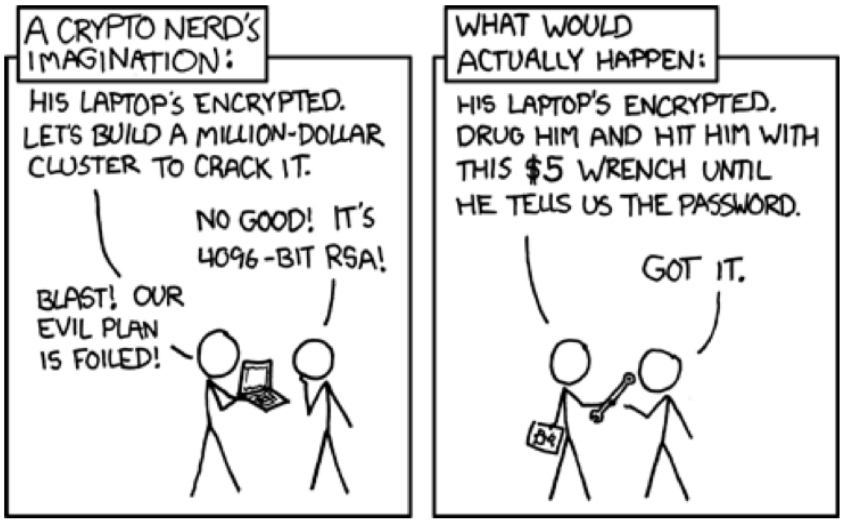
če slučajno najdem a, za katerega

$a^p \not\equiv a \pmod{p}$,

potem z gotovostjo trdim, da p NI praštevilo.

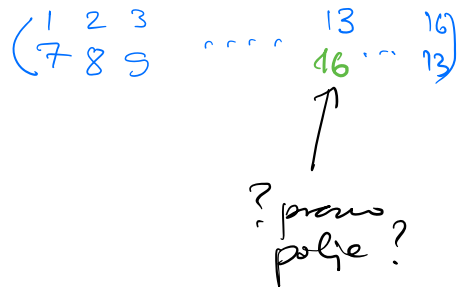
Kaj pravi Randall Munroe? RSA ni vsemogočen.

http://xkcd.com/538/



Igra 15

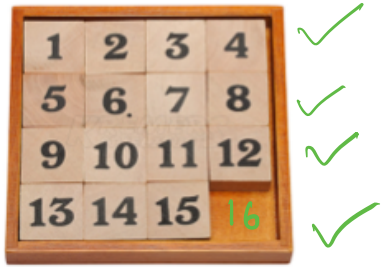
Igro 15 igramo na kvadratni igralni površini, na kateri je 15 ploščic s številskimi oznakami in eno *prazno polje*.



Naš cilj je, da s premikanjem ploščic dosežemo *ciljno pozicijo*, v kateri so številke po poljih urejene po velikosti.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 7 & 8 & 9 & 10 & 6 & 1 & 2 & 11 & 5 & 4 & 3 & 2 & 16 & 15 & 14 & 13 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \end{pmatrix} = \mathrm{id}$$



Zgled igre 15

$\pi * \tau_1 * \tau_2 * \tau_3 = id$

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 16 & 10 & 12 & 13 & 14 & 11 & 15 \end{pmatrix} *$$

$(10 \quad 16) *$

$(11 \quad 16) *$

$(15 \quad 16)$

$=$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \end{pmatrix}$$

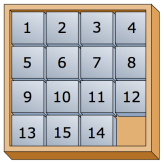
- Poteza je množenje s transpozicijo.
  (zadnja poteza je transpozicija, obratno pa ni res)
- Igra ... množenje začetne pozicije s potezami
- Uspešna igra ... končam z identiteto

$\pi = id * \tau_3 * \tau_2 * \tau_1$

Igra 15 in parnost

Denimo, da ima začetna pozicija π_z *prazno polje desno spodaj*.
Koliko potez ima igra, če jo uspešno zaključimo?
Kakšna mora biti *parnost* π_z, če igro uspešno zaključimo?

Branko Gradišnik *(Igre: volčje in ovčje)* predlaga naslednje ...



je LIHA permutacija

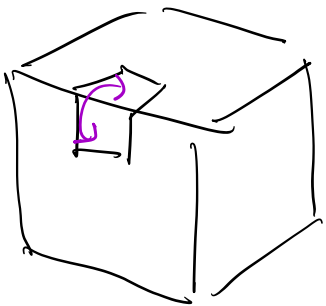
potez v LEVO =
potez v DESNO

potez NAVZGOR =
potez NAVZDOL

Uspešni igri je SODO število potez!

$\pi_z = id * \tau_k * \tau_{k-1} * \tau_{k-2} * \dots * \tau_2 * \tau_1$

↳ je SODA permutacija.

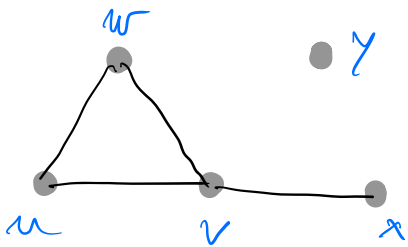


Kaj je graf

(Neusmerjen, enostaven) Graf je urejen par $G = (V, E)$, kjer je

- V neprazna končna množica *točk (vozlišč)* grafa G in
- E množica povezav grafa G, pri čemer je vsaka povezava *par* točk (povezava je množica dveh različnih točk).

Zgled:
$V = \{u, v, w, x, y\}$ $\quad E = \{\{u, v\}, \{u, w\}, \{v, w\}, \{v, x\}\}$



Pisava: Namesto $e = \{u, v\}$ pišemo krajše $e = uv$ ali $e = vu$. V tem primeru pravimo, da sta točki u in v *krajišči* povezave e. Pravimo tudi, da sta u in v *sosednji*, kar označimo z $u \sim v$.

Oznake: $V = V(G)$ ... množica točk grafa G
$E = E(G)$ ... množica povezav grafa G

$H = (U, F)$

$V(H) = U$ → množica točk grafa H

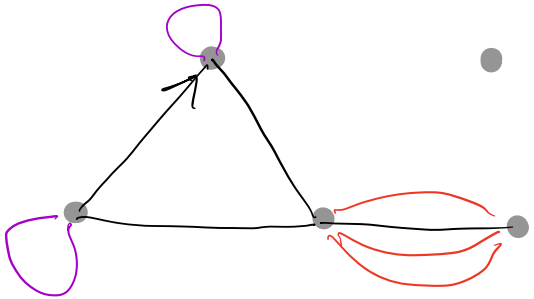
$E(H) = F$ → množica povezav grafa H

Drugi razredi grafov

Drugi razredi grafov:

- *multigraf* . . . dovolimo vzporedne povezave.
- *psevdo graf* . . . in zanke.
- *usmerjen graf* . . . povezave so usmerjene.

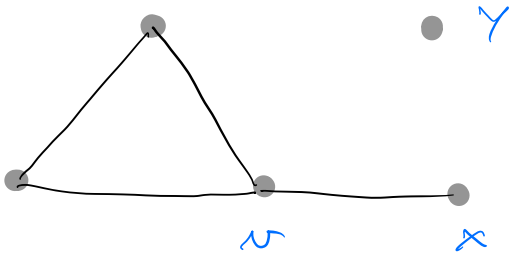
Naši grafi so grafi *simetričnih relacij brez zank*.



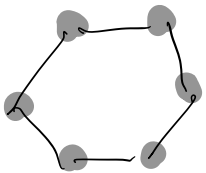
Stopnje točk

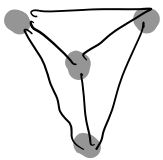
Stopnja točke $v \in V(G)$ je število povezav, ki imajo v za krajišče.
Stopnjo točke v označimo z $\deg(v)$.
Točki stopnje 0 je *izolirana točka*, točki stopnje 1 pravimo tudi *list* grafa.

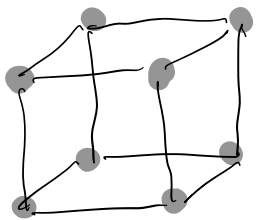
Graf G je *d-regularen*, če so vsa vozlišča grafa G stopnje d.
3-regularnim grafom pravimo tudi *kubični grafi*.



$\deg(v) = 3$
$\deg(x) = 1$
$\deg(y) = 0$
$\deg(u) = 2$





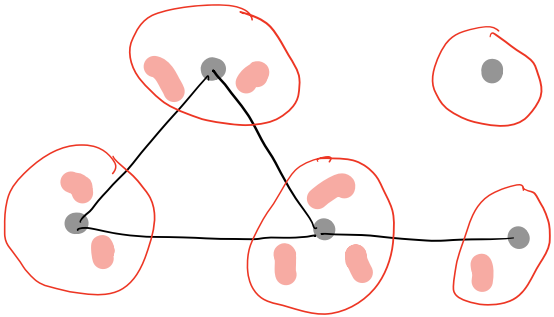


Stopnje točk

Izrek (Lema o rokovanju)

Naj bo G graf z n točkami in m povezavami. Potem je

$$\sum_{i=1}^{n} \deg(v_i) = 2 \cdot m$$



Posledica

V vsakem grafu je sodo mnogo točk lihe stopnje.

Posledica

Naj bo G d-regularen graf z n točkami in m povezavami. Potem je

$$n \cdot d = 2 \cdot m$$

Dokaz:

je sodo število → $d_1 + d_2 + d_3 + \ldots + d_n$

(število lihih členov je sodo)

Izomorfizem grafov

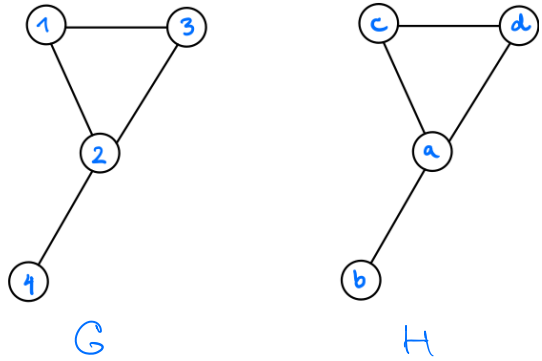
Grafa G_1 in G_2 sta *izomorfna*, če obstaja preslikava $f : V(G_1) \to V(G_2)$, za katero velja:

1. f je bijektivna in
2. $u \sim_{G_1} v \Leftrightarrow f(u) \sim_{G_2} f(v)$.

V tem primeru pravimo, da je f *izomorfizem* grafov G_1 in G_2, ter pišemo $G_1 \cong G_2$.

Trditev

Izomorfizem ohranja število točk, število povezav, stopnje točk, število trikotnikov, ...

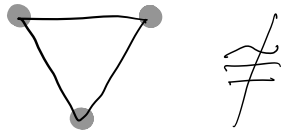


$V(G) = \{1, 2, 3, 4\}$

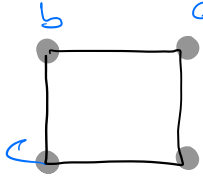
$V(H) = \{a, b, c, d\}$

$f : V(G) \to V(H)$

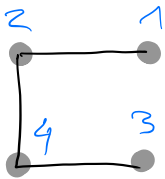
x	$f(x)$
1	d
2	a
3	c
4	b



$\not\cong$



$\not\cong$



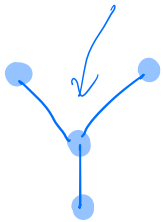
$f(1) = a$

$f(2) = b, d$

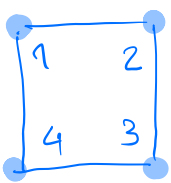
$f(3) = c$

$f(4) = c$ //

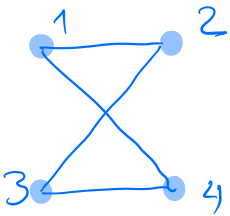
točka st 3

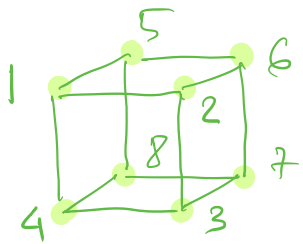


$\not\cong$

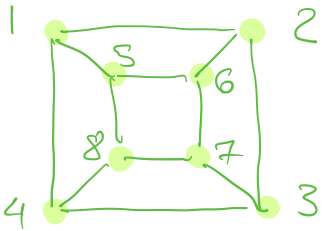


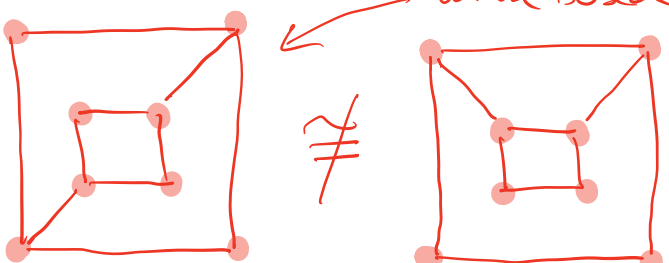
$\cong$





$\cong$





$\not\cong$

ima sosed stopnje 2

8 točk

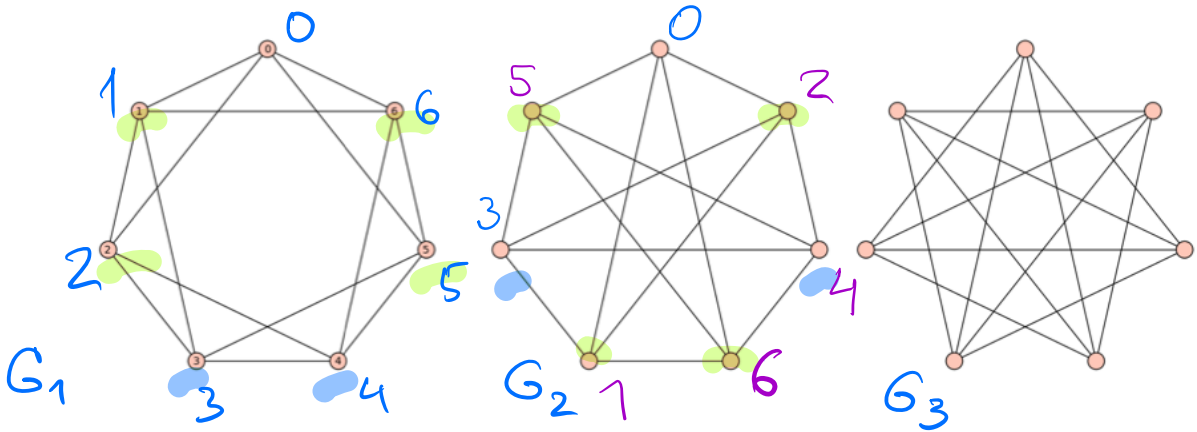
10 povezav

2, 2, 2, 2, 3, 3, 3, 3 zaporedje stopenj

ima sosedi stopnje 2

Ali so izomorfni?

$G_1 \cong G_2$?



Simetrije: rotacija (za $\frac{1}{7}$ polnega kota) in zrcalo (navpična simetrala)

0 in 3 (oranžni v srednjem grafu) sta zaradi simetrij izbrani tako, kot narisano.

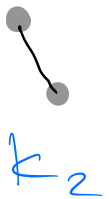
Polni grafi

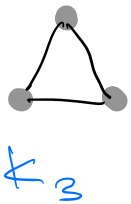
Graf je *poln*, če sta vsaki njegovi točki sosedi. Poln graf na n točkah označimo s K_n.

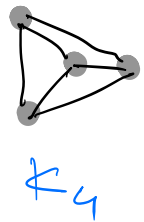
$V(K_n) = \{v_1, v_2, \ldots, v_n\}$ $\quad$ $|V(K_n)| = n$

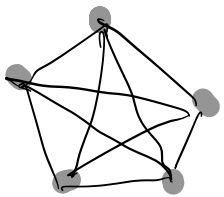
$E(K_n) = \{v_i v_j \,;\, 1 \leq i < j \leq n\}$ $\quad$ $|E(K_n)| = \frac{n(n-1)}{2}$

$\deg(v_1) = n - 1$ $\quad$ K_n je $(n-1)$-regularen graf.







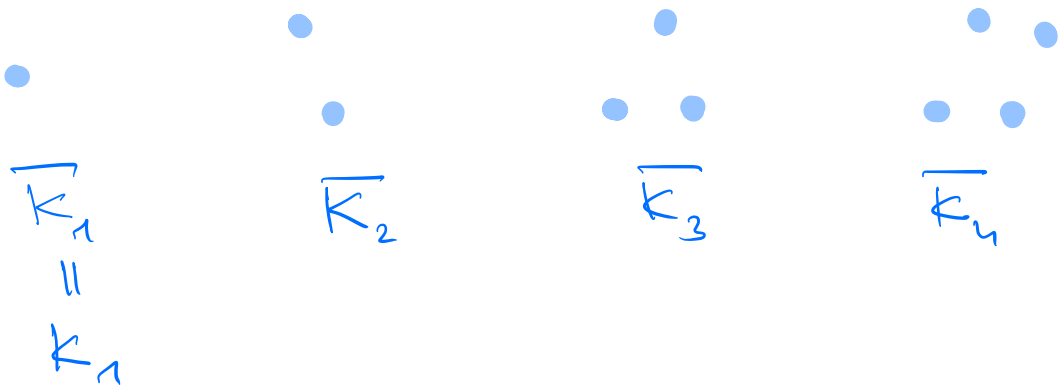


Prazni grafi

Graf je *prazen*, če nobeni njegovi točki nista sosedi. Prazen graf na n točkah označimo s $\overline{K_n}$.

$V(\overline{K_n}) = \{v_1, v_2, \ldots, v_n\}$	$\lvert V(\overline{K_n})\rvert = n$
$E(\overline{K_n}) = \emptyset$	$\lvert E(\overline{K_n})\rvert = 0$
$\deg(v_1) = 0$	$\overline{K_n}$ je 0-regularen graf.

$\overline{K_1} = K_1$



Polni dvodelni grafi

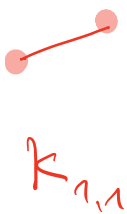
$K_{m,n}$ je *polni dvodelni graf* na $n+m$ točkah. Vsebuje dva *barvna razreda* s po n in m točkami, točki sta sosedi natanko tedaj, ko sta v različnih barvnih razredih.

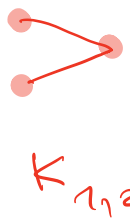
$V(K_{m,n}) = \{v_1, v_2, \ldots, v_m, u_1, u_2, \ldots, u_n\}$ $\quad |V(K_{m,n})| = m+n$

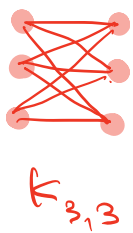
$E(K_{m,n}) = \{v_i u_j \,;\, 1 \le i \le m \text{ in } 1 \le j \le n\}$ $\quad |E(K_{m,n})| = m \cdot n$

$\deg(v_1) = n\,,\ \deg(u_1) = m$ $\quad K_{n,n}$ je n-regularen.

$K_{1,1} = K_2$







Cikli

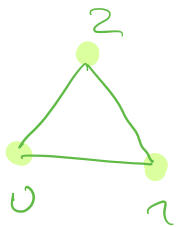
Cikel na $n \geq 3$ točkah označimo s C_n.

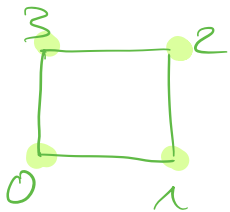
$V(C_n) = \{v_1, v_2, \ldots, v_n\}$ $\quad |V(C_n)| = n$

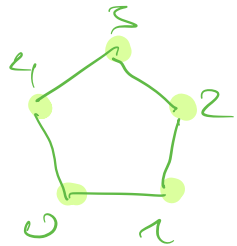
$E(C_n) = \{v_1v_2, v_2v_3, \ldots, v_{n-1}v_n, v_nv_1\}$ $\quad |E(C_n)| = n$

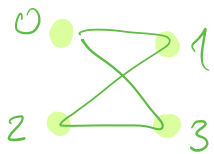
$\deg(v_1) = 2$ $\quad C_n$ je 2-regularen graf.

$C_3 = K_3, C_4 = K_{2,2}$







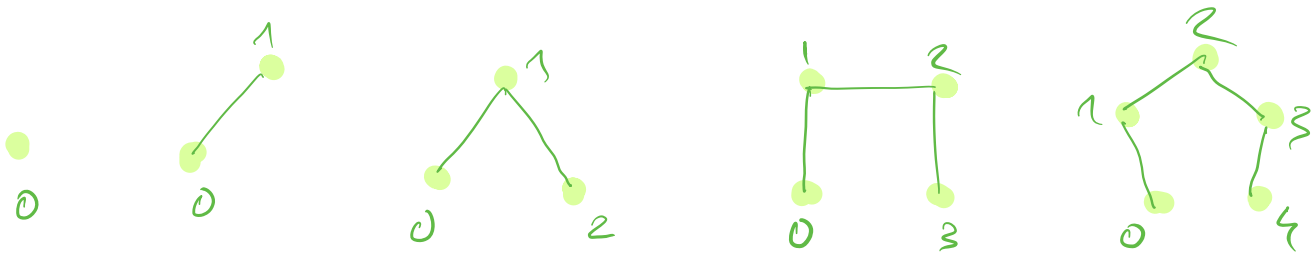


Poti

Pot na n točkah označimo s P_n.

$V(P_n) = \{v_1, v_2, \ldots, v_n\}$	$\lvert V(P_n)\rvert = n$
$E(P_n) = \{v_1v_2, v_2v_3, \ldots, v_{n-1}v_n\}$	$\lvert E(P_n)\rvert = n-1$
$\deg(v_1) = 1, \deg(v_2) = 2$	če $n \geq 3$.

$P_1 = K_1 = \overline{K_1}, P_2 = K_2 = K_{1,1}, P_3 = K_{2,1}$

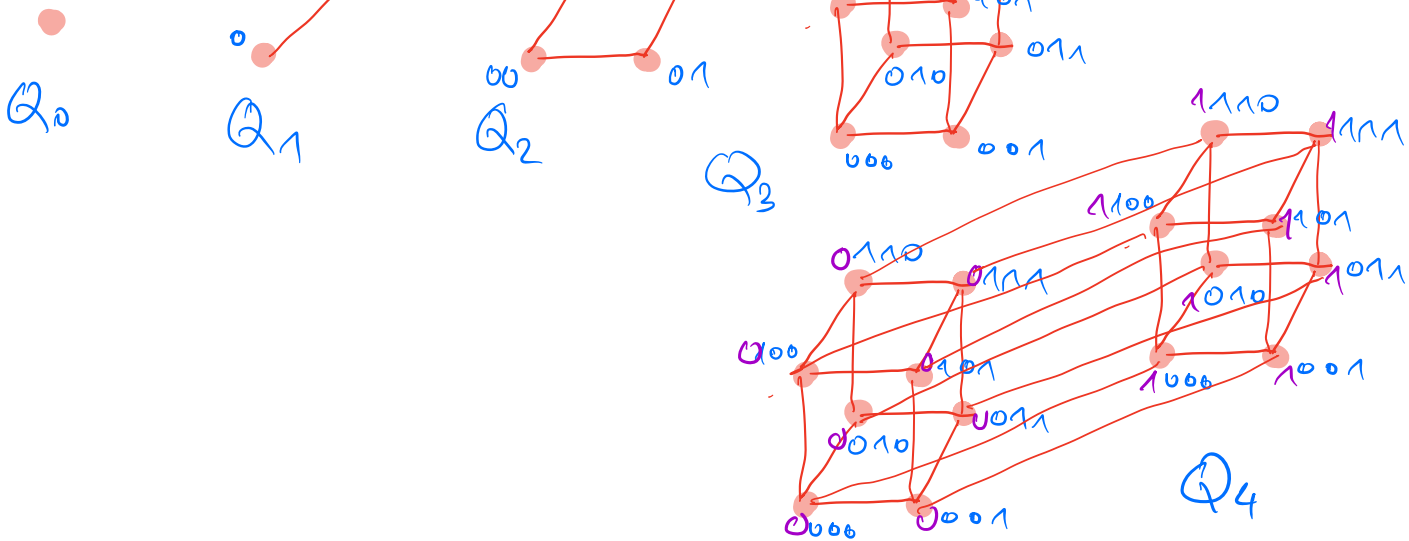


Hiperkocke

Točke *d-razsežne hiperkocke* Q_d so zaporedja ničel in enic dolžine d. Dve takšni točki-zaporedji sta sosedi, če se razlikujeta v natanko enem členu.

$|V(Q_d)| = 2^d$
$|E(Q_d)| = d \cdot 2^{d-1}$
Q_d je d-regularen graf.

$Q_0 = K_1, Q_1 = K_2, Q_2 = C_4$



Operacije z grafi

Poznamo naslednje elementarne operacije z grafi:

- *odstranjevanje povezave:* $G \mapsto G - e$
- *dodajanje povezave:* $G \mapsto G + f$
- *odstranjevanje točke:* $G \mapsto G - v$