2014 tavaszi félév
2014. június 1.
v 1.1.1

Készítették:
Mihalovits Ferenc
Viczán Balázs

Diszkrét matematika II. alapfogalmak

1 GRÁFOK

1.1 GRÁFÁBRÁZOLÁSOK

1.1.1 Adjacenciamátrix (szomszédsági mátrix)

Szomszédok felsorolása, csak egyszerű gráfok esetén használható

$$b_{i,j} = \begin{cases} 1, & van\ él\ v_i\ és\ v_j\ között \\ 0, & nincs\ él \end{cases}$$

$$\begin{bmatrix} & v_1 & v_2 & \cdots & v_j \\ v_1 & b_{1,1} & b_{2,1} & \cdots & b_{j,1} \\ v_2 & b_{1,2} & b_{2,2} & \cdots & b_{j,2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ v_i & b_{1,i} & b_{2,i} & \cdots & b_{j,i} \end{bmatrix}$$

1.1.2 Incidenciamátrix

Egy élnek végpontja-e egy pont

$$a_{i,j} = \begin{cases} 1, & ha, v_i\ végpontja\ e_j - nek \\ 0, & egyébként \end{cases}$$

$$\begin{bmatrix} & e_1 & e_2 & \cdots & e_j \\ v_1 & a_{1,1} & a_{2,1} & \cdots & a_{j,1} \\ v_2 & a_{1,2} & a_{2,2} & \cdots & a_{j,2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ v_i & a_{1,i} & a_{2,i} & \cdots & a_{j,i} \end{bmatrix}$$

1.1.3 Éllista felsorolása

Élekhez tartozó csúcsok felírása

e_1	v_1	v_2
e_2	v_3	v_1
e_3	v_5	v_3
e_4	v_4	v_5
e_5	v_6	v_5
e_6	v_7	v_6

1.1.4 Illeszkedési reláció

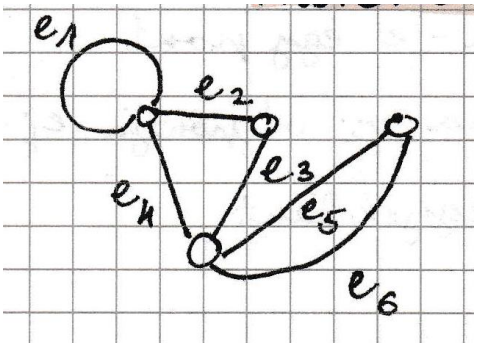
$\varphi: illeszkedési\ reláció$
$V: csúcsok$
$E: élek$
$\varphi(e_1) = \{v_1, v_2\}$

Feladat

Írja fele egy 4 csúcsú teljes gráf adjacenciamátrixát.

$$\begin{bmatrix} & v_1 & v_2 & v_3 & v_4 \\ v_1 & 0 & 1 & 1 & 1 \\ v_2 & 1 & 0 & 1 & 1 \\ v_3 & 1 & 1 & 0 & 1 \\ v_4 & 1 & 1 & 1 & 0 \end{bmatrix}$$

1.2 HUROKÉL, PÁRHUZAMOS ÉL, EGYSZERŰ GRÁF



1.2.1 Hurokél

Olyan él melynek két végpontja megegyezik

$|\varphi(e_1)| = 1$ (mivel a hurokél csak egy csúcsra illeszkedik)

1.2.2 Párhuzamos él

Két él párhuzamos, ha végpontjaik megegyeznek

e_5 és e_6 párhuzamos

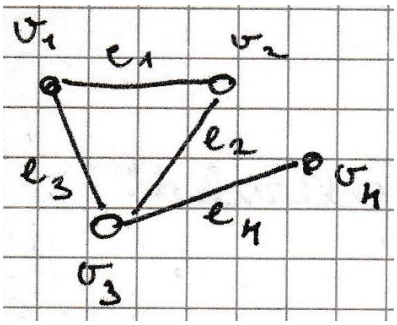
$\varphi(e_5) = \varphi(e_6)$

Feladat

Definiálja az egyszerű gráf fogalmát.

Olyan gráf, amely nem tartalmaz párhuzamos és hurok éleket.

1.3 NYÍLT ILLETVE ZÁRT SÉTA, VONAL, ÚT, KÖR



1.3.1 Séta

- **Nyílt**: az n hosszú séta egy $v_0, e_1, v_1, e_2, v_2 \dots v_{n-1}, e_n, v_n$ sorozat, ahol $\psi(e_i) = (v_{i-1}, v_i)$
  Például:
  $v_2, e_1, v_1, e_1, v_2, e_2, v_3$
- **Zárt**: Ha a kiindulópont egyezik a végponttal
  $v_0 = v_n$
  Például
  v_2, e_1, v_1, e_1, v_2

1.3.2 Vonal

Olyan séta, ahol minden él csak 1x szerepel.

$v_3, e_3, v_1, e_1, v_2, e_2, v_3, e_4, v_4$

1.3.3 Út

Olyan séta, ahol minden csúcs csak 1x szerepel

v_2, e_2, v_3, e_4, v_4

1.3.4 Kör

Olyan vonal, ahol a kezdőcsúcs és végcsúcs egyezik.

Feladat

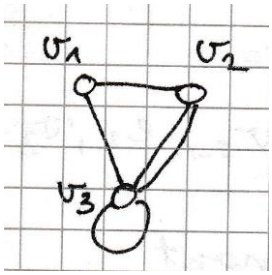
Egy konkrét gráfban adjon meg két sétát adott két csúcs között, melyek közül az egyik út.

1. séta: $v_2, e_1, v_1, e_3, v_3, e_2, v_2, e_2, v_3, e_4, v_4$
2. séta: v_2, e_2, v_3, e_4, v_4

1.4 FOKSZÁM, FOKSZÁMOK ÖSSZEGÉRE VONATKOZÓ ÁLLÍTÁS

1.4.1 Fokszám

A csúcsra illeszkedő élek száma



$$d(v_1) = 2$$

$$d(v_2) = 3$$

$$d(v_3) = 5$$

1.4.2 Fokszámok összege

$$\sum_{v \in V} d(v) = 2 \times |E|$$

Egy gráfban a fokszámok összege megegyezik az élek számának kétszeresével.

Feladat

Van-e olyan gráf, melyben a fokszámok összege 15? Miért?

Nincs, mert a fokszámok összege mindig páros

1.5 RÉSZGRÁF

Feladat

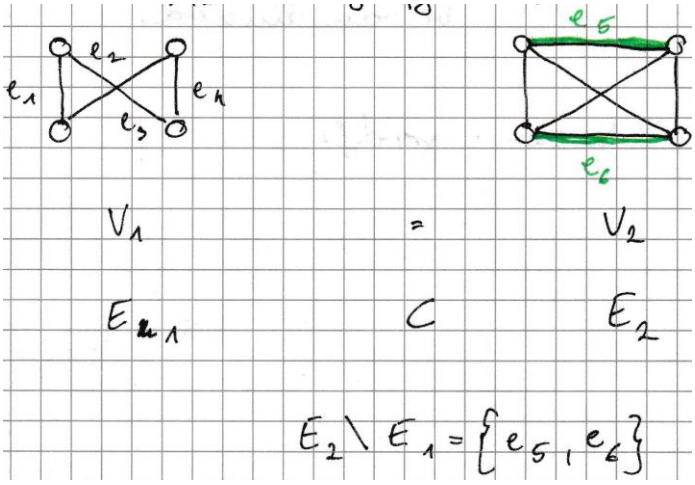
Definiálja a részgráf fogalmát.

$$G_1 = (V_1, E_1, \varphi)$$

$$G_2 = (V_1, E_1, \psi)$$

- $V_1 \subset V_2$
- $E_1 \subset E_2$
- $\varphi \subset \psi \rightarrow e \in E_1 : \varphi(e) = \psi(e)$

$K_{2,2}$ *részgráfja* K_4-nek.



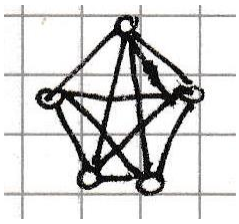
1.6 KONKRÉT GRÁFOK ÉS GRÁF TÍPUSOK ISMERETE

1.6.1 Teljes gráf

Minden csúcs szomszédja az összes többi csúcsnak.

- Jele: K_n
- Csúcsok fokszáma: n-1
- Élszámok: $\binom{n}{2}$

K_5:



1.6.2 Páros gráf

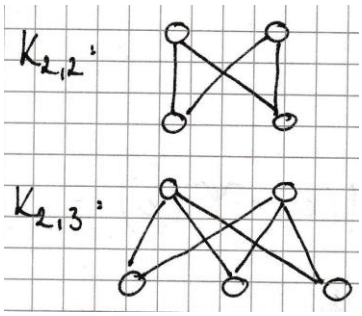
$V = V_1 \cup V_2$ és $V_1 \cap V_2 = \emptyset$

Él csak V_1 és V_2 között van

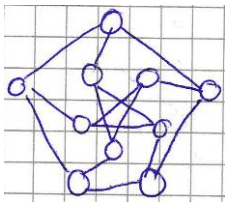
1.6.3 Teljes páros gráf

$K_{n,m}$-t teljes páros gráfnak nevezzük, ha

- $V = V_1 \cup V_2$: $V_1 \cup V_2 = \emptyset$
- $|V_1| = n \qquad |V_2| = m$
- V_1 és V_2 közt minden él be van húzva

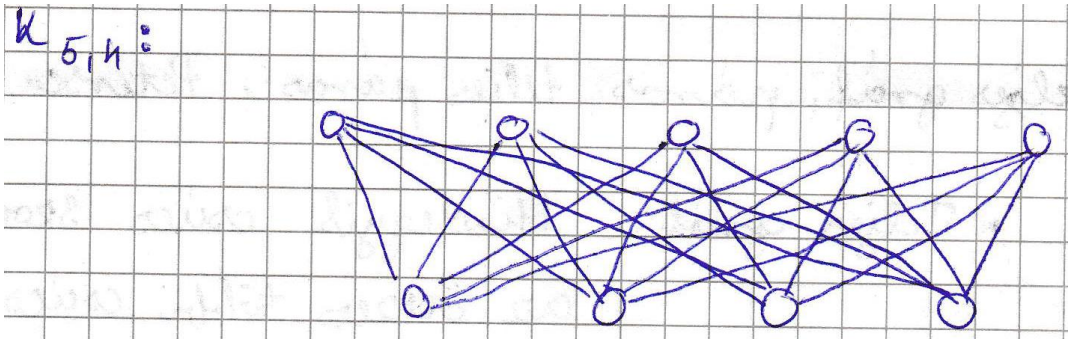


1.6.4 Petersen-gráf



Feladat

Rajzolja fel a Petersen-gráfot és egy teljes páros gráfot 5, illetve 4 elemű csúcsosztályokkal.



1.7 FA, ILLETVE FESZÍTŐFA FOGALMA

1.7.1 Fa

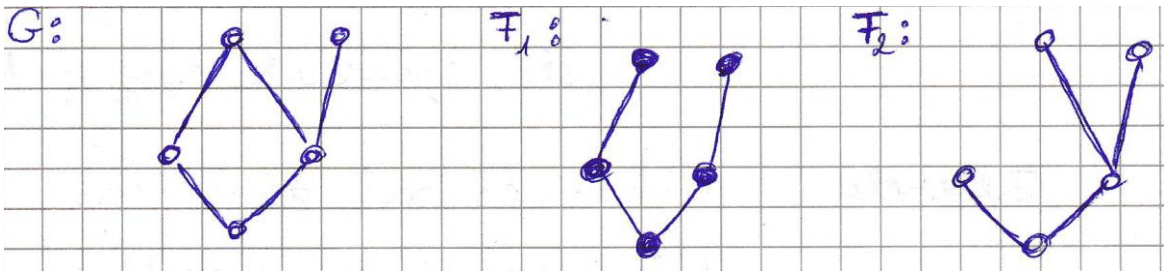
Összefüggő körmentes gráf.

1.7.2 Feszítőfa

Gráf feszítőfája alatt azt a fát értjük, amely tartalmazza az összes csúcsot. Ezt úgy kaphatjuk meg, hogy addig hagyunk el éleket a gráfból, amíg körmentes, de még összefüggő marad. Egy gráfnak több feszítőfája is lehet.

Feladat

Adja meg egy adott gráf két különböző feszítőfáját.



1.8 FÁK JELLEMZÉSE EKVIVALENS TULAJDONSÁGGAL

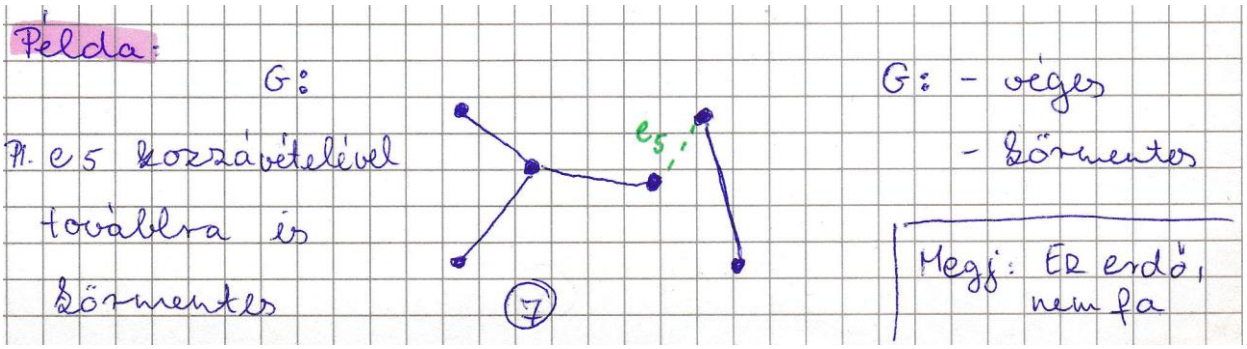
1. G fa
2. G összefüggő, bármely él elvételével nem lesz összefüggő.
3. G-ben $u \neq v$ csúcsok esetén pontosan egy út van v és u között.
4. G-nincs köre, de él hozzátételével kör keletkezik.

Feladat

Igaz-e, hogy minden véges körmentes gráf fa? Miért?

Nem igaz!

Létezik véges körmentes gráf, amihez él hozzátételével továbbra is körmentes lesz. (4-es szabály)



1.9 EULER-VONAL ÉS LÉTEZÉSÉNEK FELTÉTELE

1.9.1 Euler-vonal

Olyan vonal, ahol minden élt érintünk egy gráfban.

1.9.2 Létezésének feltétele

Akkor, és csak akkor van Euler-vonal egy gráfban, ha a páratlan fokszámú csúcsok száma 0 vagy 2.

Feladat

Van-e Euler-vonal a Petersen-gráfban? Miért?

Nincs, mert mind a 10 csúcsának foka páratlan.

1.10 HAMILTON-KÖR, HAMILTON-ÚT

1.10.1 Hamilton-kör

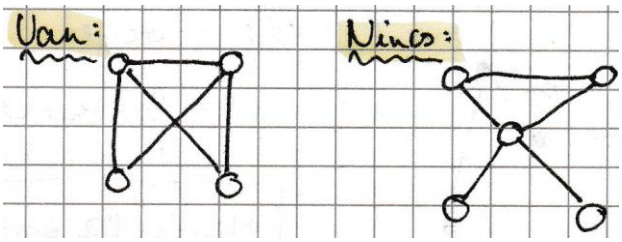
Olyan kör, ami minden csúcsot pontosan egyszer érint egy gráfban

1.10.2 Hamilton-út

Olyan út, ami minden csúcsot pontosan egyszer érint egy gráfban

Feladat

Adjon meg egy-egy gráfot, melyben nincs, illetve van Hamilton-kör.



1.11 Irányított séta, vonal, út, kör

Minden esetben $G = (V, E, \psi)$ egy irányított gráf.

1.11.1 Irányított séta

n hosszú irányított séta egy $v_0, e_1, v_1, e_2, v_2 \dots v_{n-1}, e_n, v_n$ sorozat, ahol $\psi(e_i) = (v_{i-1}, v_i)$

1.11.2 Irányított vonal

Olyan irányított séta, ahol minden él csak 1x szerepel.

1.11.3 Irányított út

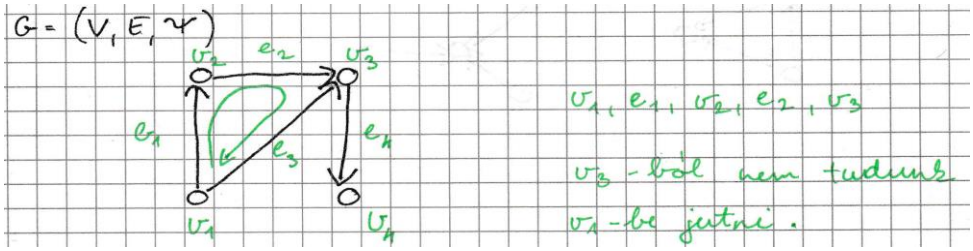
Olyan irányított séta, ahol minden csúcs csak 1x szerepel.

1.11.4 Irányított kör

Olyan irányított vonal, ahol a kezdőcsúcs és végcsúcs egyezik.

Feladat

Adjon meg egy olyan irányított gráfot, mely tartalmaz kört, de irányított kört nem.



1.12 Összefüggőség, erős összefüggőség, komponens, erős komponens

1.12.1 Összefüggő

Egy gráf összefüggő, ha minden u, v esetén van séta u – ból v –be.

1.12.2 Erősen összefüggő

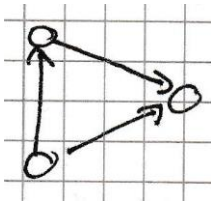
Erősen összefüggő egy gráf, ha minden u, v esetén van irányított séta u -ból v -be.

1.12.3 Komponens

Egy v csúcs komponense egy gráfnak, ha minden u –ra fenn áll $v \sim u$: v -ból van séta u -ba.

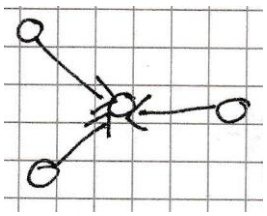
1.12.4 Erős komponens

Egy v csúcs erős komponense egy gráfnak, ha minden u –ra fenn áll $v \sim u$: v -ból van irányított séta u –ba és vissza.



Feladat

Adjon meg két olyan gráfot, melyek összefüggőek, de nem erősen összefüggőek.



2 POLINOMOK

2.1 POLINOM, FOK, FOKSZÁMTÉTEL

2.1.1 Polinom

Legyen R egy kommutatív gyűrű, akkor $(a_0, a_1, a_2 \dots)$ azon végtelen sorozatok halmazát, ahol csak véges sok nem 0 elem van, polinomnak hívjuk. (Izomorfoktól eltekintve.)

Legyen R egy kommutatív gyűrű, akkor az $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ ahol $a_n \dots a_0 \in R$ formális kifejezések a polinomok, ezek halmaza $R[x]$.

A két definíció ekvivalens, kinek melyikhez van gusztusa.

2.1.2 Fok

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = f(x)$$

Ha $a_n \neq 0 \implies a_n$ a fő együttható és $f(x)$ foka $\deg\ f(x) = n$.

2.1.3 Fokszámtétel

Ha $\deg f(x) = n$, $\deg g(x) = m$, akkor $\deg\big(f(x) \cdot g(x)\big) \leq n + m$.

Ha R nullosztó-mentes, akkor $\deg\big(f(x) \cdot g(x)\big) = n + m$

Feladat

Mekkora lehet két polinom szorzatának foka? Mondjon példát, amikor éles, illetve amikor nem éles a korlát!

Éles: $\mathbb{Z}_7$: $(2x + 1)(4x + 1)$

Ha elvégezzük a szorzást:

$$(2x + 1)(4x + 1) = 8x^2 + 6x + 1 = x^2 + 6x + 1$$

Mivel a főegyüttható 8 volt vettük a 7-ttel vett osztási maradékát, így x^2 maradt.

Nem éles: $\mathbb{Z}_8$: $(2x + 1)(4x + 1)$

Megint elvégezzük a szorzást:

$$(2x + 1)(4x + 1) = 8x^2 + 6x + 1 = 6x + 1$$

Most mivel $\mathbb{Z}_8$ felett vagyunk, 8-cal kell osztani, így a főegyüttható 0 lesz és az x^2 kiesik.

$$\deg\big(f(x) \cdot g(x)\big) = 1$$

$$n + m = 2$$

2.1.4 Polinomfüggvény

Ha $f(x) \in R[x]$, akkor az f-hez tartozó polinomfüggvény: $\forall x \in R: x \to f(x)$

Feladat

Mondjon példát két különböző polinomra, melyek ugyanazt a polinomfüggvényt határozzák meg!

$\mathbb{Z}_2$ felett $f(x) = x$ és $g(x) = x^2$-hez ugyan az a polinomfüggvény tartozik.

2.1.5 Polinomok maradékos osztása

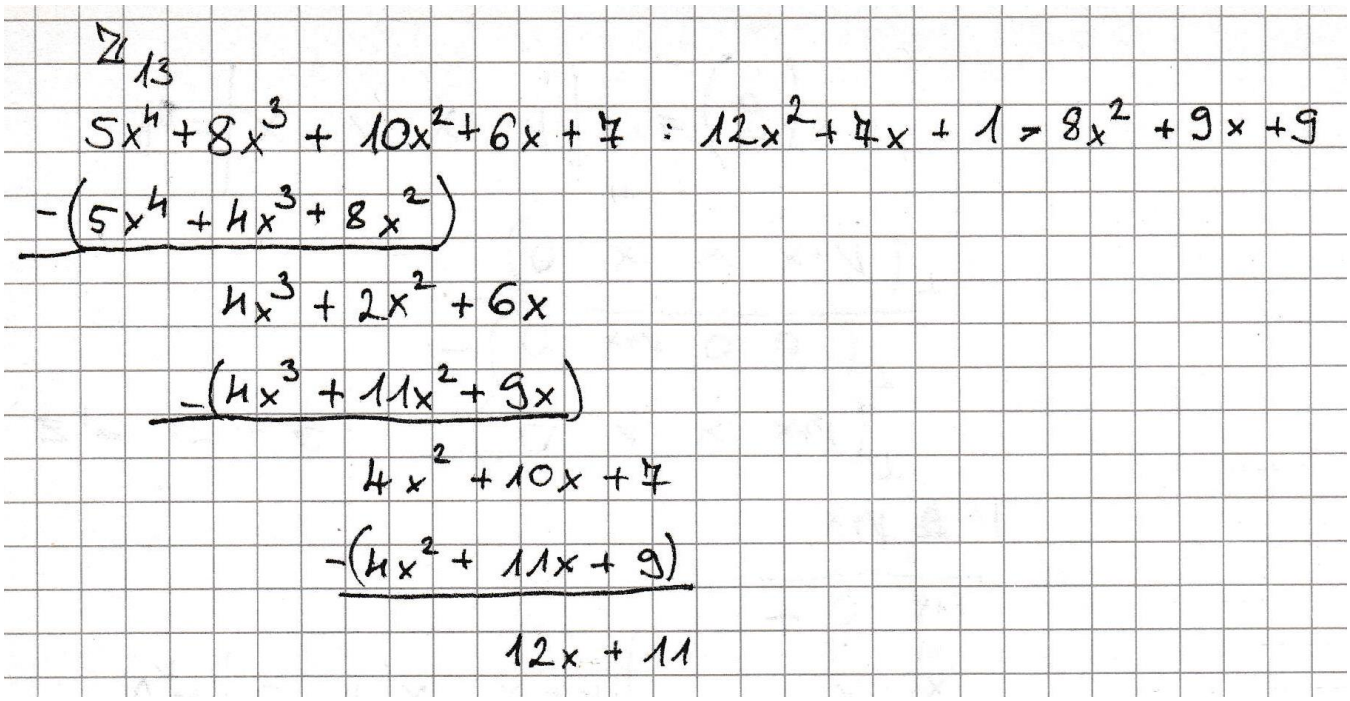
Legyen R egységelemes integritási tartomány, továbbá $f(x), g(x) \in R[x]: g \neq 0, g(x)$ fő együtthatója olyan elem, amivel lehet osztani.
Ekkor $\exists!\, q(x), r(x) \in R[x]$

$$f(x) = g(x) \cdot q(x) + r(x)$$

úgy, hogy deg $\big(r(x)\big) <$ deg $(g(x))$.

Feladat

Ossza el maradékosan az $5x^4 + 8x^3 + 10x^2 + 6x + 7 \in \mathbb{Z}_{13}[x]$ polinomot a $12x^2 + 7x + 1 \in \mathbb{Z}_{13}[x]$ polinommal!

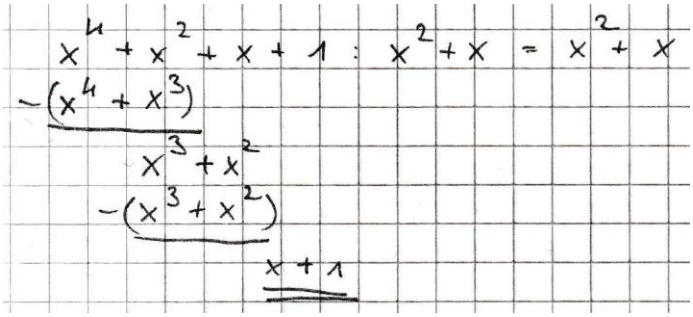


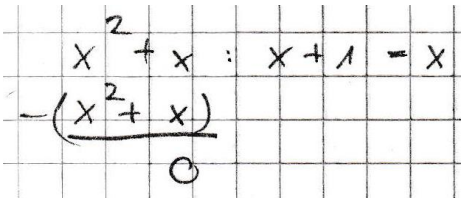
2.1.6 Polinomok legnagyobb közös osztója

Legyen $f(x), g(x) \in R[x]$ (ahol R egységelemes integritási tartomány). Akkor $d(x) \in R[x]$ egy legnagyobb közös osztójuk, ha $d(x)|f(x), d(x)|g(x)$, továbbá, ha $h(x)|f(x), h(x)|g(x) \Longrightarrow h(x)|d(x)$.

Feladat

Számolja ki az $x^4+x^2+x+1, x^2+x \in \mathbb{Z}_2[x]$ polinomok legnagyobb közös osztóját!





2.1.7 Horner-elrendezés

Általános képlet:

	a_n	a_{n-1}	a_{n-2}	$\cdots$	a_0
c	$c_{n-1}=a_n$	$c_{n-2}=c\cdot c_{n-1}+a_{n-1}$	$c_{n-3}=c\cdot c_{n-2}+a_{n-2}$	$\cdots$	$f(c)$

Feladat

Ossza el maradékosan az $(i+1)x^3-ix^2+x+1 \in \mathbb{C}[x]$ polinomot $x+i \in \mathbb{C}[x]$ polinommal a Horner elrendezés segítségével!

	$i+1$	$-i$	1	1
$-i$	$i+1$	$(-i)\cdot(i+1)+(-i)=(1-i)+(-i)=1-2i$	$-i-1$	$-1+i+1=i$

$$f(x)=(x+i)\big((i+1)x^2+(1-2i)x-i-1\big)+i$$

A hányados $\big((i+1)x^2+(1-2i)x-i-1\big)$, a maradék i.

2.1.8 Algebrai derivált

Legyen R integritási tartomány. Egy $f=f_0+f_1x+f_2x^2+\cdots+f_nx^n \in R[x]$ polinom algebrai deriváltja, vagy röviden deriváltja a $f'=f_1+2f_2x+3f_3x^2+\cdots+nf_nx^{n-1} \in R[x]$ polinom.

Tulajdonságait leíró tétel

1) konstans polinom deriváltja a nulla polinom
2) az x polinom deriváltja az egységelem
3) $(f+g)'=f'+g'$, ha $f,g \in R[x]$ (additív)
4) $(f\cdot g)'=f'g+fg'$, ha $f,g \in R[x]$ (szorzat differenciálási szabálya)

Feladat

Van-e olyan hatodfokú polinom, melynek a 0 polinom a deriváltja?

Van, $\mathbb{Z}_6$-ban a hatodfokú tag (f_6x^6) egy $0\cdot f_6x^5$ taggá alakul, így kiesik, ezért x^6 deriváltja 0.

2.1.9 Többszörös gyökök

Ha $(x-c)^n | f$, de $(x-c)^{n+1} \nmid f$ akkor azt mondjuk, hogy c n-szeres gyöke f polinomnak. $c \in R, f \in R[x]$

Feladat

Mutasson példát $\mathbb{Z}_3$ fölött olyan polinomra, melynek van többszörös gyöke!

Gondolkozzunk visszafele: az f polinom, aminek van többszörös gyöke, felírható így is:

$$(x-c)^n \cdot g = f$$

Tehát annyi a dolgunk, hogy választunk egy c-t (az egyszerűség kedvéért legyen 2, aminek ellentettje 1), választunk egy n-t, (most 2-t) ami azt jelzi hányszoros gyök legyen és hasraütésre írunk egy szimpatikus g polinomot is (ne bonyolítsuk nagyon, legyen a $2x+1$). Nincs más dolgunk, mint felírni és kiszámolni az f-t.

$$(x+1)^2 \cdot (2x+1) = (x+1) \cdot (2x^2 + x + 2x + 1) = (x+1) \cdot (2x^2 + 1) = (2x^3 + x + 2x^2 + 1)$$

Tehát végül a megfejtés a $(2x^3 + x + 2x^2 + 1)$ polinom, aminek 2-szeres gyöke a $(x+1)$. Lépések:

1) $(2x+1)$-t beszoroztam $(x+1)$-tel
2) $x + 2x = 3x$, de mivel $\mathbb{Z}_3$ felett vagyunk ezért ez a tag kiesik.
3) $(2x^2+1)$-t megszoroztam $(x+1)$ polinommal

2.1.10 Irreducibilis polinomok

K test, $f(x) \in K[x]$ irreducibilis, ha $f(x) = g(x) \cdot h(x)$ esetén vagy $g(x)$ vagy $h(x)$ konstans polinom.

Feladat

Mutasson példát olyan polinomra, mely irreducibilis $\mathbb{Q}$ fölött, de nem irreducibilis $\mathbb{R}$ fölött!

Megint gondolkozzunk visszafele: kell egy olyan szám, ami benne van $\mathbb{R}$-ben, de nincs benne $\mathbb{Q}$-ban. Legyen ez mondjuk a $\sqrt{2}$, de lehetne e, vagy akár π is. Ezek után fel kell írni azt a két polinomot, amire felbontjuk az eredeti polinomunkat, ami majd a megoldás lesz.

$$\left(x-\sqrt{2}\right)\left(x+\sqrt{2}\right) = (x^2 - 2)$$

Tehát a (x^2-2) mint láttuk, felbontható $\mathbb{R}$-ben, viszont mivel a $\sqrt{2}$ nincs benne $\mathbb{Q}$-ban ezért ott felbonthatatlan, azaz irreducibilis.

3 TESTEK, TESTBŐVÍTÉSEK

3.1 KONGRUENCIA POLINOMOK KÖRÉBEN

Legyen K test, $f(x), g(x), h(x) \in K[x]$

$$g(x) \equiv h(x) mod\ f(x)$$

ha $f(x) | g(x) - h(x)$

Feladat

Igaz-e $\mathbb{Z}_5$ felett az alábbi kongruencia $x^3 + 2x^2 + 1 \equiv 3x^4 + 2\ mod\ x^2 + x + 2$?

Nem, mivel ha elvégezzük a két maradékos osztást ($g(x)$: $f(x)$ és $h(x)$: $f(x)$) akkor látjuk, hogy két különböző maradékot kapunk, így nem kongruens a két polinom $f(x)$-re.

3.1.1 Véges testek alaptétele

1. Ha K egy véges test, akkor K elemszáma prímhatvány.
2. Minden q prímhatványhoz egyértelműen tartozik q elemű test: $\mathbb{F}_q$

Feladat

Van-e 6, 7, illetve 8 elemű test?

Megjegyzésben leírtak alapján, csak olyan véges test van ahol az elemszám prím, vagy prímhatvány.

Mivel a 6 nem prímhatvány, ilyen elemű test nem létezik, 7 és 8 viszont igen.

3.1.2 Véges testek struktúra tétele

- Legyen $q = p^n$ prímhatvány
  $$\mathbb{F}_q^+ = (\mathbb{F}_q, +) \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \ldots \times \mathbb{Z}_p$$
  azaz $\mathbb{F}_q^+$ $\mathbb{Z}_p$ feletti n dimenziós vektortér
- $\mathbb{F}_q^\times = (\mathbb{F}_q / \{0\}, \cdot) \cong \mathbb{Z}_{q-1}$
  azaz van olyan $g \in \mathbb{F}_q^\times$
  $$\mathbb{F}_q^\times = \{g^n : 0 \leq n < q\}$$

Feladat

Legyen $\mathbb{F}_{25} \cong \mathbb{Z}_5[x]/(x^2 + x + 2)$! Mennyi lesz $25 \cdot x$, illetve x^{25}?

$25x$: $\mathbb{Z}_5$ miatt maradékosan osztom 5-tel, ezért $25x = 0x = 0$

4 ÜZENETKÓDOLÁS

4.1 BETŰNKÉNTI KÓDOLÁS

Legyen A halmaz kódolandó ABC, B halmaz a kódABC. A betűnkénti kódolás a $\varphi: A \to B^*$ leképezés.
$\psi(a_1, a_2 \dots a_n) = \varphi(a_1), \varphi(a_2) \dots \varphi(a_n)$ ha $a_1, a_2 \dots a_n \in A$

Példa:

$$A = \{a, b, c, d\}$$
$$B = \{0,1\}$$
$$\varphi(a) = 01$$
$$\varphi(b) = 0010$$
$$\varphi(c) = 10$$
$$\varphi(d) = 111$$

Feladat

Betűnkénti kódolások-e az alábbi $\boldsymbol{\varphi_1, \varphi_2}: \{\boldsymbol{a, b, c, d}\} \to \{\mathbf{0}, \mathbf{1}\}^+$ leképezés:

- $\varphi_1(a) = 0, \quad \varphi_1(b) = 01, \quad \varphi_1(c) = 10, \quad \varphi_1(d) = 00$
- $\varphi_2(a) = 1, \quad \varphi_2(b) = 01, \quad \varphi_2(c) = 001, \quad \varphi_2(d) = 0001$

Mindkettő betűnkénti kódolás

4.2 KÓDTULAJDONSÁGOK

4.2.1 Felbontható

$\varphi\ A \to B^+$ injektív leképezés által meghatározott $\psi\ A^+ \to B^+$ kódolás

a) ψ felbontható, ha φ injektív (egyértelműen dekódolható)
b) prefix, ha $rng\ \psi$ prefixmentes, azaz nem létezik $\nexists \alpha, \beta \in B^+, \alpha \in rng\ \psi, \alpha\beta \in rng\psi$
c) egyenletes, ha $rng\ \psi$ minden eleme ugyan olyan hosszú
d) vesszős, ha van olyan $\vartheta \in B^+$ami minden kódsornak szufixe, de nem infixe vagy prefixe

Feladat

Az alábbi kódok milyen tulajdonságokkal rendelkeznek:

- $\varphi_1(a) = 0, \quad \varphi_1(b) = 10, \quad \varphi_1(c) = 10, \quad \varphi_1(d) = 110$
- $\varphi_2(a) = 1, \quad \varphi_2(b) = 01, \quad \varphi_2(c) = 001, \quad \varphi_2(d) = 0001$

φ_1: nem felbontható, mert nem injektív ugyanis „b”-t és „c”-t nem tudjuk dekódolni.

φ_2: vesszős, prefix, tehát felbontható (1 a vessző)

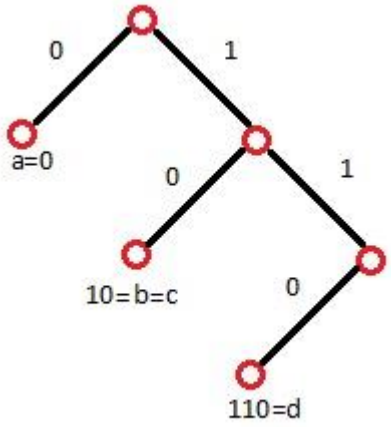
4.3 KÓDFA

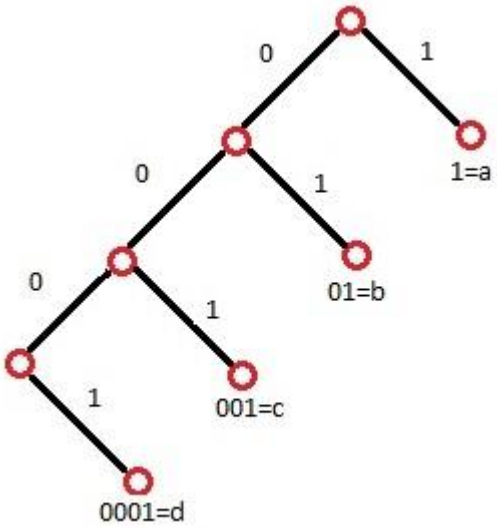
Egy adott $\varphi\ A \to B^+$ betűnkénti kódoláshoz egy irányított címkézett fát rendelünk hozzá: csúcsok, összes kódszó $(rng\ \varphi)$ illetve ezek összes prefixe, speciálisan az üres szó is.

Feladat

Mi lesz az alábbi kódok fája?

- $\varphi_1(a) = 0,$ $\varphi_1(b) = 10,$ $\varphi_1(c) = 10,$ $\varphi_1(d) = 110$
- $\varphi_2(a) = 1,$ $\varphi_2(b) = 01,$ $\varphi_2(c) = 001,$ $\varphi_2(d) = 0001$





5 HIBAJAVÍTÓ KÓDOLÁS

5.1 T-HIBAJELZŐ KÓDOK

5.1.1 Mikor mondjuk, hogy egy kód t-hibajelző?

Egy kód t-hibajelző, ha t darab hibát képes jelezni, de t+1-et már nem.

Feladat

Hány hibajelző az alábbi négyszeres ismétléses kód: adott $\boldsymbol{a} \in \{\mathbf{0}, \mathbf{1}, \mathbf{2}\}$ esetén $\boldsymbol{a} \to (\boldsymbol{a}, \boldsymbol{a}, \boldsymbol{a}, \boldsymbol{a})$?

3, mert egy kód $d - 1$ hibajelző, ahol d a kód távolságát jelenti.

Kód távolsága: a kódszavak közötti minimális távolság (itt 4), ami nem 0.

5.1.2 Hamming távolság

Definiálja a Hamming távolságot, és mondja ki annak tulajdonságait!

A kódábécé két egyforma hosszú sorának, u-nak és v-nek a Hamming távolsága $d(u, v)$, azon poziciók száma, ahol eltérnek.

a) $d(u, v) \geq 0$
b) $d(u, v) = 0 \Longrightarrow u = v$
c) $d(u, v) = d(v, u)$
d) $d(u, v) \leq d(u, z) + d(v, z)$

Feladat

Mennyi lesz a $(\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}), (\mathbf{3}, \mathbf{2}, \mathbf{1}, \mathbf{0}) \in \{\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}\}^{\mathbf{4}}$ szavak távolsága?

4, mert 4 helyen térnek el a kódszavak.

5.1.3 Kódtávolság

Definiálja a kódtávolság fogalmát!

Legyen $K \subset A^n$, ekkor a K kód távolsága $d(K) = min\,\{d(u, v),\ u, v \in K,\ u \neq v\}$

Feladat

Mennyi lesz az alábbi négyszeres ismétléses kód kódtávolsága: adott $\boldsymbol{a} \in \{\mathbf{0}, \mathbf{1}, \mathbf{2}\}$ esetén $\boldsymbol{a} \to (\boldsymbol{a}, \boldsymbol{a}, \boldsymbol{a}, \boldsymbol{a})$?

4, mert az összes kódszó 4 helyen különbözik.

5.1.4 t-hiba javító kódok

Mikor mondjuk, hogy egy kód t-hibajavító?

Egy kód t-hibajavító, ha t hibát javítani tud, de t+1-t már nem.

Feladat

Hány hibajavító az alábbi négyszeres ismétléses kód: adott $\boldsymbol{a} \in \{\mathbf{0}, \mathbf{1}, \mathbf{2}\}$ esetén $\boldsymbol{a} \to (\boldsymbol{a}, \boldsymbol{a}, \boldsymbol{a}, \boldsymbol{a})$?

1, mert $t < d/2$ hibát tud javítani egy kód. A $d = 4$.

5.1.5 Lineáris kódok

Mikor mondjuk, hogy egy kód lineáris?

Egy C kódot lineáris kódot nevezünk, ha a C halmaz lineáris tér. (Összeadásra, konstanssal szorzásra zárt)

Feladat

Lineáris-e az alábbi bináris kódolás:

$$(c_1, c_2) \to (c_1, c_2, c_1, c_1 \cdot c_2)$$

Nem lineáris, mert összegre nem zárt.

5.1.6 Generátormátrix

Definiálja a generátormátrix fogalmát!

Legyen G $\mathbb{F}_q^k \to \mathbb{F}_q^n$ lineáris transzformáció, G teljes rangú (azaz G injektív). Ekkor $G: \mathbb{F}_q^{n \times k}$ egy kód generátormátrixa.

Feladat

Adja meg az alábbi lineáris bináris kód generátormátrixát:

$$(c_1, c_2) \to (c_1, c_2, c_1 + c_2, c_1, c_2)$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

5.1.7 Ellenőrző mátrix

Definiálja az ellenőrző mátrix fogalmát!

Egy $H \in \mathbb{F}_q^{(n-k) \times n}$ mátrixot egy $K[n, k, d]_q$ kód ellenőrző mátrixának nevezzük, ha $c \in K \Leftrightarrow Hc = 0$.

Feladat

Adja meg az alábbi lineáris bináris kód generátormátrixát: (szerintem itt ellenőrző mátrixra gondol)

$$(c_1, c_2) \rightarrow (c_1, c_2, c_1 + c_2, c_1, c_2)$$

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

5.1.8 Ciklikus kódok

Definiálja a ciklikus kódokat!

Egy K $\subset F_g^n$ kód ciklikus, ha $(c_0, c_1, c_2 \dots c_{n-1})^T \in K \Longrightarrow (c_{n-1}, c_0, c_1, c_2, \dots c_{n-2})^T \in K$

Feladat

Ciklikus-e a {000,010,100,111} kód?

Nem, mivel szerepelnie kellene benne a 001 kódszónak.

5.1.9 Polinom kódok

Legyen K $[n, k, d]_q$ lineáris kód, most $K \subset \mathbb{F}_q[x]$. Legyen K ciklikus kód, és legyen $g(x) \in K$ olyan kódpolinom ami 1-főegyütthatós (normált, $g(x)$ minimum fokú polinom K-ban).

- Most K polinom kód
- $g(x)$ a kód generátorpolinomja
- ellenőrző polinomja: $h(x) = \frac{x^n - 1}{g(x)}$

5.1.10 CRC kódok

A bináris, ciklikus, lineáris kódokat (bináris polinom kódok) CRC kódoknak hívjuk (Cyclic Redundancy Check).

Feladat

Mondjon példát CRC kódra (n, k paraméterek és a generátor polinom megadásával)!

- $n = 7$ (CRC kód hossza)
- $k = 4$ (u hossza)
- generátor polinom: $g(x) = x^3 + x^2 + 1$
- $u = 0001 \Longrightarrow u(x) = 0 \cdot 1 + 0 \cdot x + 0 \cdot x^2 + 1 \cdot x^3 = x^3$

$$r(x) = x^{n-k} \cdot u(x) \; mod \; g(x) \Rightarrow r(x) = x^{7-4} \cdot x^3 \; mod \; x^3 + x^2 + 1 \Rightarrow$$

$$r(x) = (x^2 + 1) \cdot (x^2 + 1) = (x^2 + 1)^2 = x \cdot x^3 + 1 \equiv x \cdot (x^2 + 1) + 1 =$$

$$= x^3 + x + 1 \equiv x^2 + 1 + x + 1 \equiv x^2 + x$$

Mert: $(x^3 + x^2 + 1) \equiv 0 \; mod \; (x^3 + x^2 + 1) \Rightarrow x^3 \equiv -x^2 - 1 \equiv x^2 + 1$

$$v(x) = x^{n-k} \cdot u(x) + r(x) = x^3 \cdot x^3 + x^2 + x = x^6 + x^2 + x \Longrightarrow v = 0110001$$

5.1.11 Reed-Solomon-kód

Legyen $\mathbb{F}_q$ q elemű test. Legyen $\alpha \in F_q^x$ α rendje n $\alpha^n = 1,\ \alpha^r \neq 1, 0 < r < n$, ekkor $n|q-1$ (tipikus választás α-ra : $n = q-1$). Most α^i hatványok ($0 \leq i < n$) gyökei az $x^{n-1} \in H_q[x]$ polinomok.

Speciálisan:

$$x^{n-1} = \prod_{i=0}^{n-1}(x - \alpha^i)$$

Legyen $0 < m < n$, legyen $k = n - m$. Legyen g(x)= $\prod_{i=1}^{m}(x - \alpha^i)$, most $g(x)|x^n - 1$
A Reed-Solomon-kód $g(x)$-el generált $[n, k]_q$ polinom kód.

6 GAZDASÁGOS KÓDOLÁS

6.1.1 McMillian egyenlőtlenség

- Ha K kód felbontható és $|B| = r$, akkor $\sum_{i=1}^{n} r^{-li} \leq 1$
- Ha az egyenlőtlenség teljesül, akkor van olyan prefix kód, ahol a kódszavak hosszai $l_1, l_2 \dots l_n$

Feladat

Létezik-e olyan bináris felbontható kód, ahol a kódszavak hossza 2, 2, 2, 3, 3, 4?

$$\frac{1}{2^2} + \frac{1}{2^2} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^3} + \frac{1}{2^4} \leq 1$$

6.1.2 Átlagos kódhossz

Legyen az $A = \{a_1 \dots a_n\}$ a kódolandó szavak halmaza. Legyen $p_1, p_2 \dots p_n$ az adott karakterek előfordulásának valószínűsége ($0 < p_i \leq 1 \ \sum_{i=1}^{n} p_i \ = 1$). Ekkor a kódolás átlagos kódhossza: $l = \sum_{i=1}^{n} p_i \cdot l_i$.

Feladat

Mennyi lesz annak a kódnak az átlagos kódhossza, ahol a kódhosszak rendre 2, 2, 2, 3, 3, a betűk valószínűségei rendre 0; 34, 0; 3, 0; 22, 0; 07, 0; 07

$$2 \cdot 0{,}34 + 2 \cdot 0{,}3 + 2 \cdot 0{,}22 + 3 \cdot 0{,}07 + 3 \cdot 0{,}07 \ = \ Átlagos\ szóhossz$$

6.1.3 Entrópia

Az adott kód entrópiája (az információ mennyiség): $-\sum_{i=1}^{n} p_i \cdot log_q p_i$

Feladat

Mennyi lesz annak a forrásnak az entrópiája, ahol a betűk valószínűségei $\mathbf{0,34}$; $\mathbf{0,3}$; $\mathbf{0,22}$; $\mathbf{0,07}$; $\mathbf{0,07}$!

$$0{,}34 \cdot log_2 0{,}34 \ + \ 0{,}3 \cdot log_2 0{,}3 \ + \ 0{,}22 \cdot log_2 0{,}22 \ + \ 0{,}07 \cdot log_2 0{,}07 \ + \ 0{,}07 \cdot log_2 0{,}07 \ = 2{,}068$$

6.1.4 Shanonn tételek

Entrópia < átlagos szóhossz < Entrópia +1.

6.1.5 Huffman kód

Lényege a tökéletes kód konstruálása. Bináris Huffmann konstruálása:

a) rendezzük csökkenő sorrendbe a gyakoriságokat
b) 2 legkisebbet vonjuk össze a gyakoriság összeadásával
c) oldjuk meg rekurzívan az összevonás utánira
d) az összevont csúcs alá írjuk be azokat, amikből gyártottunk

Ha $r > 2$
Első lépésben $m = 2 + ((n-2) \ mod \ (r-1))$ összevonás, utána r-esével vonjuk össze.