

Diszkrét Matematika 2 (C)

2014-15 / őszi félév

Jegyzet

Az esetleges elírásokért, hibákért felelősséget nem vállalok!

Javításokat, javaslatokat a következő címre küldhetsz:

blackhawk1990@gmail.com

1. Gráfok alapfogalmai

1. Definiáld a gráf fogalmát!

A G (irányítatlan) gráf egy $G = (\varphi, E, V)$ hármas, ahol E az élek, V a csúcsok halmaza, φ pedig egy az élek halmazából V -beli rendezetlen párokat képező illeszkedési leképezés.

2. Definiáld az „illeszkedik” és a „végpontja” fogalmakat!

Ha egy $G = (\varphi, E, V)$ gráfban tetszőleges $e \in E$ élre $\varphi(e)$ v_1 és $v_2 \in V$ -t adja eredményül, akkor azt mondjuk, hogy v_1 és v_2 csúcs végpontja az e élnek. Ha egy él végpontja egy csúcs, akkor azt mondjuk, illeszkedik rá.

3. Definiáld az izolált csúcs fogalmát!

Izolált csúcsnak nevezünk egy csúcsot, ha nem illeszkedik egy élre sem.

4. Definiáld az üres gráf fogalmát!

Üres gráfnak nevezzük azt a gráfot, melyben nem szerepelnek élek (tehát E halmaz üres).

5. Definiáld az illeszkedési relációt!

Egy $G = (\varphi, E, V)$ gráfban a φ illeszkedési leképezés egy relációt határoz meg az élek és csúcsok között. Ezt a relációt nevezzük illeszkedési relációnak.

6. Definiáld a szomszédos él/csúcs fogalmát!

Két különböző él szomszédos, ha van olyan csúcs, amire mindkettő illeszkedik.

Két különböző csúcs szomszédos, ha van olyan él, ami mindkettőre illeszkedik.

7. Definiáld a hurokél fogalmát!

Olyan él, mely egyetlen csúcsra illeszkedik.

8. Definiáld a párhuzamos él fogalmát!

Két különböző él, melyeknek ugyanazok a végpontjaik, párhuzamos éleknek nevezzük.

9. Definiáld az egyszerű gráf fogalmát!

Egyszerű gráf az a gráf, melyben nincsenek párhuzamos-, és hurokélek.

10. Definiáld a véges/végtelen gráf fogalmát!

Véges gráfnak nevezzük azt a gráfot, ahol az élek és csúcsok halmaza véges. Fordítva végtelen.

11. Definiáld gráfban a fokszám fogalmát!

Egy gráfban az adott csúcsra illeszkedő élek számát - a hurokéleket duplán számolva - a csúcs fokszámának nevezzük. Jelölése $d(v)$.

12. Definiáld az n -reguláris gráf fogalmát!

A gráf minden csúcsának foka n .

13. Definiáld a reguláris gráf fogalmát!

Egy gráf valamilyen $n \in \mathbb{N}$ -re reguláris. Lehet 0 reguláris is, ha pl 1 csúcs van csak a gráfban!

14. Mit mondhatunk irányítatlan gráfban a fokszámok összegéről?

Egy gráfban a csúcsok fokszámának összege megegyezik az élek számának kétszeresével.

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

15. Mikor nevezünk két irányítatlan gráfot izomorfoknak?

$G_1 = (\varphi_1, E_1, V_1)$ és $G_2 = (\varphi_2, E_2, V_2)$ gráfok izomorfak, ha léteznek $f: E_1 \rightarrow E_2$ és $g: V_1 \rightarrow V_2$ bijekciók, hogy $e \in E$ pontosan akkor illeszkedik $v \in V$ -re, ha $f(e) \in E_2$ illeszkedik $g(v) \in V_2$ -re.

16. Definiáld a teljes gráf fogalmát!

Olyan egyszerű gráf, amelyben bármely két csúcs szomszédos.

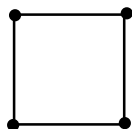
17. Mit jelentenek a C_n , P_n , S_n rövidítések?

C_n (kör): Csúcsai egy szabályos n -szög csúcspontjai és a szomszédos csúcsok vannak összekötve.

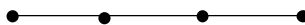
P_n (ösvény): C_{n+1} -ből egy él törlésével kapjuk.

S_n (csillag): Egy szabályos n -szög csúcspontjai a középponttal vannak összekötve.

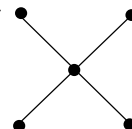
Példa: C_4



Példa: P_3



Példa: S_4



18. Definiáld a páros gráf fogalmát!

$G = (\varphi, E, V)$, ha $V = V' \cup V''$ ($V' \cap V'' = \{\}$) és $\forall e \in E: \varphi(e) = \{v_1, v_2\}$ -re $v_1 \in V'$ és $v_2 \in V''$ (vagy fordítva).

19. Definiáld irányítatlan gráf komplementerének fogalmát!
- Ha $G' = (\varphi', E', V')$ gráf részgráfja a $G = (\varphi, E, V)$ gráfnak, akkor G' -nek a G -re vonatkozó komplementerén a $G'' = (\varphi'_{|E \setminus E'}, E \setminus E', V)$ gráfot értjük.
20. Definiáld az élhalmaz/csúcshalmaz törlésével kapott gráfot!
- A $G = (\varphi, E, V)$ gráfból az $E' \subset E$ elhagyásával kapott gráf a $G' = (\varphi_{|E \setminus E'}, E \setminus E', V)$.
- Legyen $G = (\varphi, E, V)$ gráfra $V' \subset V$ és $E' \subset E$ azon élek halmaza, amelyek illeszkednek V' -beli csúcsra.
- V' elhagyásával kapott gráf: $G' = (\varphi_{|E \setminus E'}, E \setminus E', V \setminus V')$.
21. Definiáld a séta fogalmát!
- A $G = (\varphi, E, V)$ gráfban a $v_1, e_1, v_2, e_2, \dots, v_{n-1}, e_{n-1}, v_n$ sorozatot sétának nevezzük, ha:
- $$v_j \in V, 0 \leq j \leq n$$
- $$e_k \in E, 1 \leq k \leq n$$
- $$\varphi(e_m) = \{v_{m-1}, v_m\}, 1 \leq m \leq n$$
22. Definiáld a zárt séta fogalmát!
- Ha egy sétában a kezdő-, és végpont megegyezik, akkor zárt sétának nevezzük.
23. Definiáld a vonal fogalmát!
- Ha egy sétában nincs élismétlődés, akkor vonalnak nevezzük.
24. Definiáld az út fogalmát!
- Ha egy sétában nincs csúcsmétlődés, akkor útnak nevezzük.
25. Definiáld a kör fogalmát!
- Ha egy zárt vonalban a kezdő és végpont ismétlődésén kívül nincs más csúcsmétlődés, akkor körnek nevezzük.
26. **Mit állíthatunk séta és út kapcsolatáról?**
- Adott $G = (\varphi, E, V)$. Vegyünk egy sétát $v \in V$ -ből $v' \in V$ -be.
- Ekkor a sétából alkalmasan törölve éleket és csúcsokat v -ből v' -be menő utat kapunk.
27. Definiáld az összefüggőség fogalmát!
- Ha $G = (\varphi, E, V)$ és tetszőleges $v_1, v_2 \in V$ esetén létezik út (séta) v_1 és v_2 között, akkor a gráf összefüggő.

28. Definiáld a komponens fogalmát!

Vezessünk be egy $\sim$ relációt a csúcsok halmazán: $v_1, v_2 \in V$ esetén $v_1 \sim v_2$, ha van v_1 és v_2 között út (séta). Mivel egy ekvivalenciareláció osztályoz, a $\sim$ segítségével megkapjuk V egy osztályozását. Az osztályozás által kapott csúcshalmazokon vett részgráfok a komponensek.

29. Mit állíthatunk egy zárt vonalról?

Bármely $G = (V, E, V)$ gráfban egy legalább 1 hosszú zárt vonal véges sok, páronként éldisjunkt kör egyesítése.

Bizonyítások

- Mit mondhatunk irányítatlan gráfban a fokszámok összegéről?

A $G = (V, E, V)$ véges gráfban:

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

Tehát az élek fokszámának összege megegyezik az élek számának kétszeresével.

Bizonyítás: Teljes indukcióval, élszámok szerint:

- $|E| = 0$: $0 = 2 * 0$
- Tegyük fel, hogy $|E| = n$ esetén is igaz az állítás. (Indukciós feltevés)
Állítás: $|E| = n+1$ esetén is igaz. (Indukciós állítás)

Hagyjunk el egy élt a gráfból. Arra a gráfra teljesül az összefüggés, az elhagyott él az egyenlőség mindkét oldalát kettővel növeli.

- Mit állíthatunk séta és út kapcsolatáról?

Állítás: Adott $G = (V, E, V)$. Vegyünk egy sétát $v \in V$ -ből $v' \in V$ -be.

Ekkor a sétából alkalmasan törölve éleket és csúcsokat v -ből v' -be menő utat kapunk.

Bizonyítás: Ha nincs csúcsismétlődés, akkor kész vagyunk.

Különben legyen $v_i = v_j$ ($i < j$)! Hagyjuk el a $v_{i+1} v_{i+2} \dots v_j$ részt a sétából, így egy rövidebb sétát kapunk v -ből v' -be, amelyben kevesebb a csúcsismétlődés. Mivel a séta véges, ez az eljárás véges sok lépésben leáll.

- Mit állíthatunk egy zárt vonalról?

Állítás: Bármely $G = (\varphi, E, V)$ gráfban egy legalább 1 hosszú zárt vonal véges sok, páronként éldiszjunkt kör egyesítése.

Bizonyítás: Ha a triviális csúcsismétlődésen kívül nincs más, akkor a vonal már kör, egyébként egy ismétlődő csúcs első előfordulásától a másodikig haladva egy rövidebb zárt vonalat kapunk. Ezt elhagyva az eredeti vonalból is egy rövidebb zárt vonalat kapunk.

Ezek közül, amelyek nem körök, megismételjük az eljárást. Minden lépésben, ha van még olyan zárt vonal ami nem kör, abból két rövidebb zárt vonalat kapunk, végül csupa kör marad.

- Legyen a $\sim$ a csúcsok halmazán értelmezett reláció, amelyre $v_1 \sim v_2$ pontosan akkor, ha van v_1 kezdőpontú és v_2 végpontú séta a gráfban. Bizonyítsd be, hogy ez a reláció ekvivalenciareláció!

Állítás:

$\sim$ egy ekvivalenciareláció, vagyis reflexív, szimmetrikus és tranzitív.

Bizonyítás:

- reflexív: minden v -re v -ből v -be 0 hosszú út vezet

- szimmetrikus: $v = v_0, e_1, v_2, e_2, \dots, e_n, v_n = v'$ egy út v -ből v' -be akkor $v' = v_n, e_n, v_{n-1}, \dots, e_1, v_0 = v$ egy út v' -ből v -be.

- tranzitív: $v, e_1, \dots, e_n, v'$ út és $v', f_1, \dots, f_n, v''$ út, ekkor a $v, e_1, v', f_1, \dots, f_n, v''$ egy séta v -ből v'' -be, azt pedig tudjuk, hogy sétából lehet utat csinálni.

2. Fák

30. Definiáld a fa fogalmát!

A fa egy összefüggő, körmentes gráf.

31. **Add meg 3 ekvivalens jellemzését a fa fogalmának!**

Egy $G = (\varphi, E, V)$ egyszerű gráfra a következő feltételek ekvivalensek.

(1) G fa.

(2) G összefüggő, de bármely él törlésével kapott részgráf már nem az.

(3) Ha v és v' a G különböző csúcsai, akkor pontosan egy út van v -ből v' -be.

(4) G -nek nincs köre, de bármilyen új él hozzáadásával kapott gráf már tartalmaz kört.

32. **Mit mondhatunk körmentes gráfban az elsőfokú csúcsokról?**

Ha egy $G = (\varphi, E, V)$ véges gráfban nincs kör, de van él, akkor van legalább két elsőfokú csúcs.

33. **Fogalmazd meg két olyan szükséges és elégséges feltételt arra, hogy egy véges egyszerű gráf fa, amelyben szerepel az élek száma!**

Egy $G = (\varphi, E, V)$ egyszerű, véges n csúcsú gráfra a következő feltételek ekvivalensek:

(1) G fa

(2) G -ben nincs kör és $n-1$ éle van

(3) G összefüggő és $n-1$ éle van

Bizonyítások

- Add meg 3 ekvivalens jellemzését a fa fogalmának!

Egy $G = (\varphi, E, V)$ egyszerű gráfra a következő feltételek ekvivalensek.

(1) G fa.

(2) G összefüggő, de bármely él törlésével kapott részgráf már nem az.

(3) Ha v és v' a G különböző csúcsai, akkor pontosan egy út van v -ből v' -be.

(4) G -nek nincs köre, de bármilyen új él hozzáadásával kapott gráf már tartalmaz kört.

Bizonyítás:

$(1) \rightarrow (2) \rightarrow (3) \rightarrow (4) \rightarrow (1)$

$(1) \rightarrow (2)$ *indirekt:*

G fa, v és v' közti élt elhagyva még mindig összefüggő lenne, de akkor a v-ből v'-be menő utat az elhagyott éllel kiegészítve egy kört kapnánk G-be, ami ellentmondás, mert G fa volt, fa pedig definíció szerint körmentes.

$(2) \rightarrow (3)$ *indirekt:*

Legalább 2 út van v és v' között, legyen v_k és v_k' az első eltérés az utakon, ekkor a (v_{k-1}, v_k) él elhagyható lenne, továbbra is összefüggő lenne, ami pedig ellentmondás.

$(3) \rightarrow (4)$:

Vegyünk hozzá v és v' közé egy élt. v-ből v'-be volt út, az új él bevételeével pedig kör keletkezik, vagyis megszűnt a körmentesség. Ha eredetileg is lenne kör, akkor a kör 2 tetszőleges pontja között 2 út is menne.

$(4) \rightarrow (1)$ *kell:*

Ha nem lenne az, akkor lenne két csúcs, mely nem lenne összekötve. Ha új élt veszek v és v' közé, akkor a (4) alapján kapunk egy kört. Ezt az élt elhagyva aztán mégis lenne út v-ből v'-be.

- Mit mondhatunk körmentes gráfban az elsőfokú csúcsokról?

Állítás: Ha egy $G = (V, E)$ véges gráfban nincs kör, de van él, akkor van legalább két elsőfokú csúcs.

Bizonyítás: Vegyük a gráf egy leghosszabb útját. Ennek a két végpontja elsőfokú. Ha illeszkedne még egy él a végpontra, annak a másik végpontja:

- a leghosszabb útban nem szereplő csúcs: hosszabb utat kapnánk **X**
- a leghosszabb útban szereplő csúcs: kört kapnánk **X**

- Egy egyszerű véges gráfnak n csúcsa van. Fogalmazz meg két olyan szükséges és elégséges feltételt arra, hogy a gráf fa, amelyben szerepel az élek száma!

Tétel: Egy $G = (\varphi, E, V)$ egyszerű, véges n csúcsú gráfra a következő feltételek ekvivalensek:

G fa

G -ben nincs kör és $n-1$ éle van

G összefüggő és $n-1$ éle van

Bizonyítás: Ha $n=1$, akkor triviális. Tegyük fel, hogy n csúcsra igaz.

(1) $\Rightarrow$ (2)

Teljes indukcióval $n \geq 2$ -re:

Legyen $v \in V$ elsőfokú csúcs, hagyjuk el ezt a gráfból.

Ekkor a gráf továbbra is körmentes és összefüggő marad.

$n+1$ -re: A megmaradt gráfnak n csúcsa van és $n-1$ éle, így az eredeti gráfnak n éle.

(2) $\Rightarrow$ (3)

Teljes indukcióval $n \geq 2$ -re:

$n+1$ -re: hagyjunk el egy elsőfokú csúcsot! Marad n csúcs, $n-1$ él és körmentes gráf, így használható az indukciós feltevés.

Feltevés: Az elhagyott csúcsból a szomszédján keresztül tetszőleges csúcsba vezet út.

(3) $\Rightarrow$ (1): Ha van a gráfban kör, hagyjuk el a kör egy élet. Ezt ismételjük, amíg körmentes gráfot nem kapunk. k lépés után az eredmény egy $n-1-k$ élű, összefüggő, körmentes gráf.

De (1) $\Rightarrow$ (2) miatt $n-1$ éle van, tehát $k = 0$.

3. Feszítőfa, Euler-vonal, Hamilton-kör

34. Definiáld a feszítőfa fogalmát!

A feszítőfa olyan részgráf, ami a gráf összes csúcsát tartalmazza és fa.

35. Mikor létezik feszítőfája egy gráfnak?

Ha egy gráf összefüggő, akkor létezik feszítőfája.

36. Mit mondhatunk összefüggő gráfban a körök számáról?

Egy összefüggő gráfban van legalább $|E| = |V| + 1$ kör.

37. Definiáld az élvágó élhalmaz/csúcshalmaz fogalmát!
 Legyen $G = (\varphi, E, V)$ gráf, V' valódi részhalmaza V , $u, v \in V$.
 Azt mondjuk, hogy V' élvágja u -t és v -t, ha bármely u és v közötti útban van V' -beli csúcs.
 V' -t élvágó csúcshalmaznak nevezzük, ha vannak olyan csúcsai G -nek, amelyeket élvág.
38. Definiáld a vágás fogalmát!
 Egy élvágó halmazt vágásnak nevezünk, ha nincs olyan valódi részhalmaza, ami élvágó halmaz.
39. **Mit mondhatunk összefüggő gráfban a vágások számáról?**
 Egy összefüggő $G = (\varphi, E, V)$ gráfban van legalább $|V| - 1$ vágás.
40. Definiáld az erdő fogalmát!
 Körmentes gráfot erdőnek nevezünk. Egy erdő komponensei fák.
 A feszítőerdő egy olyan részgráf, ami az összes csúcsot tartalmazza és erdő. A feszítőerdő komponensei a komponensek feszítőfái.
41. Definiáld az Euler-vonal fogalmát!
 Ha egy vonal a gráf összes élét tartalmazza, akkor Euler-vonalnak nevezzük.
42. **Mit állíthatunk összefüggő gráfban zárt Euler-vonal létezésével kapcsolatban?**
 Egy összefüggő gráfban pontosan akkor van zárt Euler-vonal, ha minden csúcs foka páros.
43. Definiáld a Hamilton-út/kör fogalmát!
 Egy gráfban azt az utat (kört), amely a gráf összes csúcsát tartalmazza, Hamilton-útnak (körnek) nevezzük.
44. Adj meg egy elégséges feltételt Hamilton-kör létezéséről!
 Ha az n csúcsú gráfban minden csúcs foka legalább $n/2$, akkor a gráfban van Hamilton-kör. (Elégséges feltétel, mivel $n \geq 5$ -re C_n -ben van Hamilton-kör, pedig 2-reguláris)

Bizonyítások

- Mikor létezik feszítőfája egy gráfnak?

Állítás: Összefüggő gráfnak van feszítőfája

Bizonyítás: Ha a gráfban van kör, akkor hagyjuk el ennek a körnek egy élét. Folytatva ezt az eljárást körmentes és összefüggő gráfot kapunk, ami fa.

- Mit mondhatunk összefüggő gráfban a körök számáról?

Tétel: Egy összefüggő $G = (\varphi, E, V)$ gráfban van legalább $|E| = |V| + 1$ kör.

Bizonyítás: Vegyük egy feszítőfáját a gráfnak! Legyen a feszítőfa éleinek halmaza F , a további élek halmaza $E \setminus F$. Ha a feszítőfához hozzáveszünk egy $e \in E \setminus F$ élt, az így kapott gráfban lesz kör (korábbi tétel miatt), ez a kör tartalmazza e -t.

$|E \setminus F| = |E| - |F| = |E| - (|V| - 1) = |E| - |V| + 1$, így legalább ennyi kör van G -ben.

Példa: K_4 esetén $6 - 4 + 1 = 3$

- Mit mondhatunk összefüggő gráfban a vágások számáról?

Tétel: Egy összefüggő $G = (\varphi, E, V)$ gráfban van legalább $|V| - 1$ vágás.

Bizonyítás: Vegyük egy feszítőfáját G -nek, ennek élhalmaza legyen F . $E \setminus F$ -hez $e \in F$ -et hozzávéve egy elvágó élhalmazt kapunk. Ez az elvágó halmaz tartalmaz vágást, továbbá ez tartalmazza e -t. Mivel $|F| = |V| - 1$, ezért kész vagyunk.

- Mit állíthatunk összefüggő gráfban zárt Euler-vonal létezésével kapcsolatban?

Tétel: Egy összefüggő gráfban pontosan akkor van zárt Euler-vonal, ha minden csúcs foka páros.

Bizonyítás:

$\Rightarrow$

Menjünk végig a zárt Euler-vonalon, a kezdő és a végpontot leszámítva minden csúcs minden előfordulásakor 2 különböző él szerepel mellette, ezért egy adott csúcs fokszáma kétszerese az előfordulásainak a számának. A kezdő és végpont megegyezik, 1-1 él miatt itt is 2-vel nő a foksám.

$\Leftarrow$

Tetszőleges csúcsból kiindulva kezdjük el felírni egy vonalat, előbb-utóbb visszatérünk a kezdőpontba. Ha ennek a zárt vonalnak az éleit elhagyjuk a gráfból, egy olyan részgráfot kapunk, aminek minden csúcsa páros fokú. Az eljárást folytatva éldiszjunk zárt vonalakat kapunk, amiket összefűzve (az összefüggőség miatt megtehetjük) megkapjuk a zárt Euler-vonalat.

4. Címkezett gráfok, síkba rajzolható gráfok, gráfok színezése, gráfok ábrázolása

45. Definiáld a címkezett gráf, élcímkezett/csúcscímkezett gráf fogalmát!

A $G = (\varphi, E, V, C_v, c_v, C_e, c_e)$ -t címkezett gráfnak nevezzük, ha C_v, C_e halmazok és $c_v: V \rightarrow C_v$, illetve $c_e: E \rightarrow C_e$.

- Ha a címkék halmaza R (valós), akkor súlyozásról beszélünk.
- Ha E' valódi részhalmaza E -nek, akkor E' súlya $\sum_{e \in E'} c_e(e)$
- Ha V' valódi részhalmaza V -nek, akkor V' súlya $\sum_{v \in V'} c_v(v)$
- Igazából c_e illetve c_v helyett szeretjük a súlyozást w -vel jelölni.

46. Definiáld az élsúlyozás/csúcssúlyozás fogalmát!

Élhalmaz súlya: E' részhalmaza E -nek: $w(E') = \sum w(e)$

Csúcshalmaz súlya: V' részhalmaza V -nek: $w(V') = \sum w(v)$

47. Ismertest a Kruskal algoritmust és a rá vonatkozó tételt!

Egy $G = (\varphi, E, V)$ gráf w súlyozással ellátott összefüggő, véges gráfban az összes csúcsot tartalmazó üres részgráfból indulva, és a már kiválasztott részgráf még nem tartalmaz kört, egy minimális súlyú feszítőfát kapunk. A Kruskal-algoritmus egy mohó algoritmus.

48. Definiáld a mohó algoritmus fogalmát, adj példát, amikor nem ad optimális megoldást!

A mohó algoritmuson azt az algoritmust értjük, amely adott döntési helyzetben mindig a lehető legkedvezőbb lehetőséget választja.

Mohó algoritmus nem mindig ad optimális megoldást, például minimális súlyú Hamilton körnél.

49. Mikor nevezünk egy gráfot síkba rajzolhatónak?

Egy $G = (\varphi, E, V)$ gráf síkba rajzolható, ha lerajzolható úgy, hogy élek csak csúcspontban metszhetik egymást.

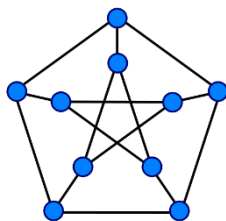
50. Hogy szól Euler tétele síkba rajzolható gráfokról?

Legyen $G = (\varphi, E, V)$ egyszerű, összefüggő, síkba rajzolható gráf, a tartományainak száma: $|T|$.

Ekkor: $|E| + 2 = |V| + |T|$

51. Adj példát nem síkba rajzolható gráfra!

Egy gráf pontosan akkor rajzolható síkba, ha nem tartalmaz K_5 -tel, vagy $K_{3,3}$ -mal topológiailag izomorf részgráfot. Ilyen például a Petersen gráf.



52. Mikor nevezünk két gráfot topologikusan izomorfnak?

G és G' gráfok topologikusan izomorfak, ha az alábbi lépés, vagy fordítottja segítségével véges sok lépéssel a G -ből G' -vel izomorf gráfot kapunk:

Egy másodfokú csúcsot elhagyunk, és a szomszédjait összekötjük.

53. Hogy szól Kuratowski tétele síkgráfokkal kapcsolatosan?

Egy egyszerű véges gráf pontosan akkor síkba rajzolható, ha nincs K_5 -tel vagy $K_{3,3}$ -mal topologikusan izomorf részgráfja.

54. Definiáld az irányított és irányítatlan gráf illeszkedési mátrixát!

$G = (\psi, E, V)$ irányított gráf élmátrixa, avagy illeszkedési mátrixa

$V = \{v_1, v_2, \dots, v_n\}$

$E = \{e_1, e_2, \dots, e_m\}$

A eleme $\{0, \pm 1\}^{n \times m}$

$a_{i,j} =$

- 1 ha v_i kezdőpontja e_j -nek
- -1 ha v_i végpontja e_j -nek, ha e_j nem hurokél

Ha G irányítatlan, akkor $a_{i,j}$ helyett $|a_{i,j}|$ -t vesszük.

55. Definiáld az irányított és irányítatlan gráf csúcsmátrixát!

$b \in \mathbb{Z}_{n \times m}$

Irányított esetben:

$b_{ij} = v_i$ kezdőpontú és v_j végpontú élek száma.

Irányítatlan esetben:

$b_{ii} = A$ v_i -re illeszkedő hurokélek száma,

míg $i \neq j$ esetén $b_{ij} = A$ v_i -re és v_j -re illeszkedő élek száma

56. Hogyan definiáljuk egy gráf kromatikus számát?

Úgy szeretnénk a gráfok csúcsait kiszínezni, hogy a szomszédos csúcsok különböző színűek legyenek. Minden síkba rajzolható gráf legfeljebb négy színnel színezhető.

Egy gráf kromatikus száma az a szám, ahány szín kell legalább a színezéséhez.

Ha a kromatikus szám 1, akkor nincsenek élek.

Ha a kromatikus szám 2, akkor a gráf páros.

Bizonyítások

- Ismertesd a Kruskal algoritmust és a rá vonatkozó tételt!

Bizonyítás: Csak összefüggő gráfra, mert komponensenként véve a minimális súlyú feszítőfákat, együttesen egy minimális súlyú feszítőerdőt adnak.

Legyen F az algoritmus által adott feszítőfa.

Tegyük fel, hogy létezik F_0 , aminek a súlya kisebb. Ha több azonos súlyú ilyen gráf van, akkor közülük azt válasszuk, aminek a legtöbb közös éle van F -fel.

Legyen e olyan éle F_0 -nak, amely nem éle F -nek. Ha e -t hozzávesszük F -hez, keletkezik egy K kör. A K -ban szereplő, tetszőleges e' él súlyára $w(e') \leq w(e)$.

Ha F_0 -ból elhagyjuk azt e élt, akkor z komponensre bomlik. K -nak van olyan e' éle, ami ezt a két komponensre összeköti.

Tekintsük az $F' = F_0 \setminus \{e\} \cup \{e'\}$ -t!

- F' feszítőfa
- Ha $w(e') < w(e)$, akkor F' súlya kisebb F_0 súlyánál. **Ellentmondás!**
- Ha $w(e') = w(e)$, ekkor F' és F súlya azonos, de F' -nek több közös éle van F -el mint F_0 -nak. **Ellentmondás!**

5. Irányított gráfok

57. Definiáld az irányított gráf fogalmát!

A $G = (\psi, E, V)$ irányított gráf, ha E az élek halmaza, V a csúcsok halmaza, ψ pedig illeszkedési leképezés: $E \rightarrow V \times V$

58. Hogyan kaphatunk irányított gráfból irányítatlan?

Bármely $G = (\psi, E, V)$ irányított gráfból kapható egy $G' = (\psi', E', V')$ irányítatlan gráf úgy, hogy az irányítást „elfelejtjük”, azaz $\psi(e) = (v, v')$ esetén $\psi'(e) = \{v, v'\}$ -nek definiálva.

59. Definiáld az irányítás fogalmát!

Egy $G = (\psi, E, V)$ irányított gráfból kapott $G' = (\psi', E', V')$ irányítatlan gráfra azt mondjuk, hogy G a G' egy irányítása.

60. Definiáld a szigorúan párhuzamos élek fogalmát!

$e, e' \in E, e \neq e'$ esetén ha $\psi(e) = \psi(e')$, akkor e és e' szigorúan párhuzamos él.

61. Definiáld a kifok/befok fogalmát!

Ha egy v eleme V csúcs véges sok élnek kezdőpontja, akkor ezek számát a csúcs kifokának nevezzük, és $d^+(v)$ -vel jelöljük.

Ha egy v eleme V csúcs véges sok élnek végpontja, akkor ezek számát a csúcs befokának nevezzük, és $d^-(v)$ -vel jelöljük.

62. Definiáld a nyelő/forrás fogalmát!

Ha egy csúcs kifoka nulla, akkor nyelőnek, ha pedig befoka 0, akkor forrásnak nevezzük.

63. Mit mondhatunk a foksámösszegekről irányított gráfban?

$$\sum_{v \in V} d^+(v) = \sum_{v \in V} d^-(v) = |E|$$

64. Mikor nevezünk két irányított gráfot izomorfnak?

65. Definiáld irányított gráfok izomorfiaját!

$G = (\psi, E, V)$ és $G' = (\psi', E', V')$ gráfok izomorfak, ha léteznek $f: E \rightarrow E'$ és $g: V \rightarrow V'$ bijekciók, úgy hogy v eleme V pontosan akkor kezdőpontja $e \in E$ -nek, ha $g(v)$ kezdőpontja az $f(e)$ -nek, illetve $v \in V$ pontosan akkor végpontja $e \in E$ -nek, ha a $g(v)$ végpontja $f(e)$ -nek.

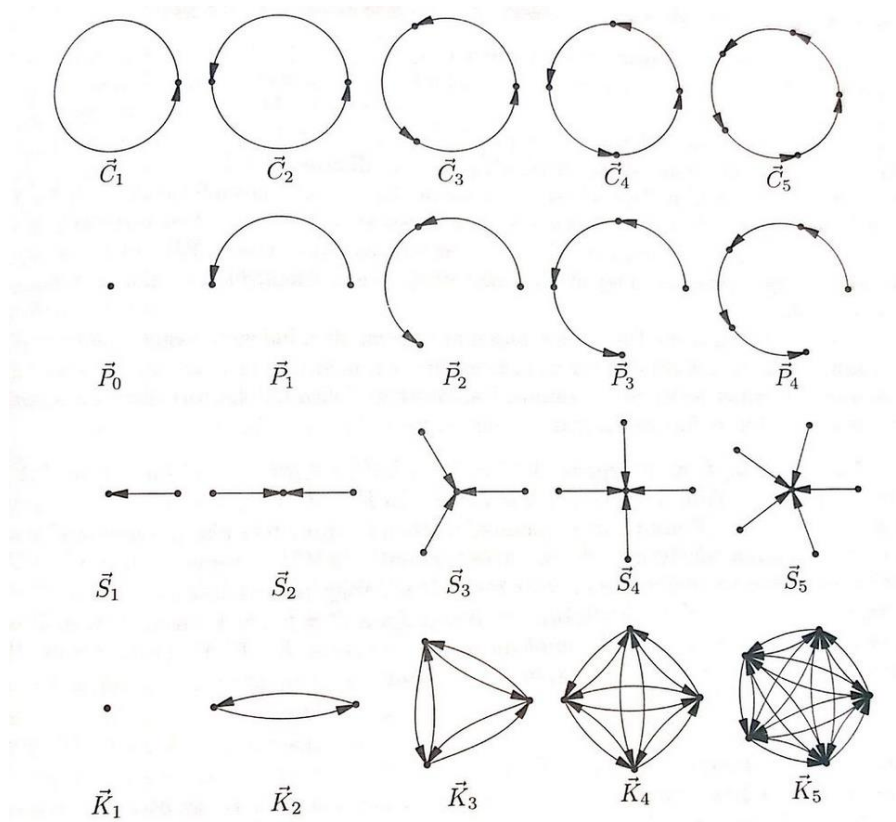
66. Mit jelentenek a C_n , P_n , S_n , K_n rövidítések?

C_n : irányított ciklus csúcsai egy szabványos n -szög csúcsai.

P_n : irányított ösvény, mely C_{n+1} -ből egy él törlésével adódik.

S_n : irányított csillag, melyben egy szabványos n -szög csúcsaiból visz irányított él a középpontba

K_n : irányított teljes gráf



67. Definiáld az irányított részgráf illetve szupergráf fogalmát!

A $G = (\psi, E, V)$ irányított gráfnak a $G' = (\psi', E', V')$ irányított gráf irányított részgráfja, ha V' részhalmaza ψ , E' részhalmaza E és V' részhalmaza V .

68. Definiáld a feszített/telített irányított részgráf fogalmát!

$G = (\psi, E, V)$ -nek irányított részgráfja $G' = (\psi', E', V')$ feszített irányított részgráf, ha E' minden olyan élt tartalmaz E -ből, amelynek kezdő-, és végpontja is V' -ben szerepel.

69. Definiáld irányított gráf komplementerének fogalmát!

Ha $G = (\psi, E, V)$ -nek a $G' = (\psi', E', V')$ irányított részgráfja, ekkor G' -nek G -re vonatkozó komplementere $G'' = (\psi \setminus E', E \setminus E', V)$.

70. Definiáld az élhalmaz/csúcshalmaz törlése fogalmát irányított gráf esetén!

Ugyanúgy működik, mint irányítatlan esetben.

71. Definiáld az irányított séta fogalmát!
 A $G = (\psi, E, V)$ irányított gráfban egy n hosszú irányított séta alatt egy $v_0, e_1, v_1, e_2, \dots, v_{n-1}, e_n, v_n$ sorozatot értünk, ahol:
- v_j eleme V , $(0 \leq j \leq n)$
 - e_k eleme E , $(1 \leq k \leq n)$
 - $\psi(e_m) = (v_{m-1}, v_m)$, $(1 \leq m \leq n)$
72. Definiáld a zárt/nyílt irányított séta fogalmát!
 Zárt, ha kezdő-, és végpontja megegyezik, ellenkező esetben nyílt.
73. Definiáld az irányított vonal fogalmát!
 Olyan irányított séta, melyben nincs éliszmétlődés.
74. Definiáld az irányított út fogalmát!
 Olyan irányított séta, melyben nincs csúcsismétlődés.
75. Definiáld az irányított kör fogalmát!
 Olyan irányított séta, melyben nincs éliszmétlődés, valamint csak egy csúcsismétlődés van benne (kezdő-, és végpont).
76. Definiáld az erősen összefüggő gráf fogalmát!
 Irányított gráf erősen összefüggő, ha bármely csúcsából bármely csúcsába vezet irányított út.
77. Definiáld az erős komponens fogalmát!
 Bevezetünk egy relációt a csúcsok halmazán: $v_1, v_2 \in V$ -re $v_1 \sim v_2$, ha vezet irányított út v_1 -ből v_2 -be és vezet irányított út v_2 -ből v_1 -be. Ez egy ekvivalenciareláció, így meghatároz egy osztályozást a csúcsok halmazán. Az egyes osztályok által meghatározott telített részgráfok az úgynevezett erős komponensek.
78. Definiáld az irányított fa fogalmát!
 Egy $G = (\psi, E, V)$ irányított gráfot irányított fának nevezünk, ha f_a : van egy csúcs, melynek befoka 0, a többi befoka pedig 1.
79. Definiáld a gyökér fogalmát irányított fában!
 Irányított fában a 0 befokú csúcsot gyökérnek nevezzük.
80. Definiáld a szint fogalmát irányított fában!
 A gyökérből az adott csúcsba vezető út hosszát a csúcs szintjének nevezzük.

81. Definiáld a magasság fogalmát irányított fában!
A csúcsok szintjeinek a maximuma.
82. Definiáld a gyerek/szülő/testvér fogalmát irányított fában!
Ha $\psi(e) = (v, v')$, akkor v szülője v' -nek, illetve v' gyereke v -nek. Ha két csúcs szülője közös, akkor ők testvérek.
83. Definiáld a levél fogalmát irányított fában!
Ha a csúcsnak 0 a kifoka, akkor levélnek nevezzük.
84. Definiáld a gyökeres fa fogalmát!
Írányítatlan fa egy v csúcsának kijelölésével egy v gyökerű fáról beszélünk. Ez a fa egyértelműen irányítható úgy, hogy irányított fát kapjunk.
85. Definiáld az irányított részfa fogalmát!
Adott $v \in V$ csúcsához tekinthetjük azon csúcsok halmazát, amik végpontjai v -ből induló irányított útnak az általuk meghatározott feszített részgráf a v -ben gyökerező irányított részfa.

Bizonyítások

- Mit mondhatunk a fokszámok összegéről irányított gráfban?

$$\sum_{v \in V} d^+(v) = \sum_{v \in V} d^-(v) = |E|$$

Nyilván igaz lesz a feltevés, mivel egy újabb él hozzáadása az irányított gráfhoz mindhárom összeget eggyel fogja növelni.

- Legyen $\sim$ a csúcsok halmazán értelmezett reláció, amelyre $v_1 \sim v_2$ pontosan akkor, ha van v_1 kezdőpontú és v_2 végpontú irányított séta és v_2 kezdőpontú és v_1 végpontú irányított séta is a gráfban. Bizonyítsd be, hogy ez a reláció ekvivalenciareláció!

Egy relációt ekvivalenciarelációnak nevezünk, ha a reláció reflexív, szimmetrikus és tranzitív is.

- Reflexív, mivel minden $v \in V$ esetén $v \sim v$
- Szimmetrikus, mivel minden $v_1, v_2 \in V$ esetén $v_1 \sim v_2 \Rightarrow v_2 \sim v_1$
- Tranzitív, mivel minden $v_1, v_2, v_3 \in V$ esetén, ha $v_1 \sim v_2 \wedge v_2 \sim v_3 \Rightarrow v_1 \sim v_3$

- Bizonyítsd be, hogy egy irányított fában a gyökérből bármely adott csúcsba vezető út egyben irányított út is!
???

6. Algebrai alapok, polinomokkal kapcsolatos alapfogalmak

86. Definiáld a (belső) művelet fogalmát!

Legyen A egy halmaz, ekkor az A halmazon értelmezett n változós (belső) műveleten egy $*$: $A^n \rightarrow A$ leképezést értünk, ahol A^n az A halmaz önmagával vett n -szeres Descartes szorzata.

87. Definiáld az asszociativitás fogalmát!

Legyen G halmaz, $*$ pedig egy művelet a halmazon.

A $*$ művelet asszociatív G -n, ha bármely $g_1, g_2, g_3 \in G$ esetén teljesül, hogy:

$$g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3.$$

Ha $*$ asszociatív G -n, akkor $(G, *)$ félcsoporth.

88. Definiáld a kommutativitás fogalmát!

Legyen G halmaz, $*$ pedig egy binér művelet a halmazon.

A $*$ művelet kommutatív G -n, ha bármely $g_1, g_2 \in G$ esetén $g_1 * g_2 = g_2 * g_1$.

89. Definiáld a félcsoporth fogalmát!

Ha egy binér művelet egy halmazon asszociatív, akkor a halmaz a művelettel félcsoporthot alkot.

90. Definiáld az egységelem fogalmát!

91. Definiáld a bal oldali semleges elem/jobb oldali semleges elem fogalmát!

Legyen G halmaz, $*$ pedig egy művelet a halmazon.

A G egy s elemét bal, illetve jobb oldali semleges elemnek nevezzük, ha $s * g = g$, illetve $g * s = g$,

minden $g \in G$ -re. Ha s bal és jobb oldali semleges elem is egyben, akkor semleges elemnek nevezzük.

92. Definiáld a monoid fogalmát!

Egy semleges elemes félcsoporthot monoidnak nevezünk.

93. Definiáld a nullelem fogalmát!

Egy halmazban nullelemnek nevezzük azt az elemet, mely adott G halmazon tetszőleges $*$ műveletre $n * g = n$ és $g * n = n$ minden $g \in G$ esetén. Tehát a művelet elvégzésével a nullelemet kapjuk.

94. Definiáld a bal oldali inverz/jobboldali inverz/inverz fogalmát!
 Legyen $(G, *)$ grupoid s eleme G pedig semleges elem, akkor
 g_b eleme G baloldali inverze g -nek, ha $g_b * g = s$.
 g_j eleme G jobboldali inverze g -nek, ha $g * g_j = s$.

 g^{-1} inverze g -nek, ha baloldali és jobboldali inverz is.
95. Definiáld a csoport fogalmát!
 $(G, *)$ grupoidot csoportnak nevezzük, ha félcsoport, vagyis $*$ asszociatív a G -n, létezik semleges elem, valamint minden elemnek létezik inverze.
96. Definiáld az Abel-csoport fogalmát!
 Ha $(G, *)$ csoport és $*$ kommutatív G -n, akkor G Abel-csoport.
97. Definiáld a gyűrű fogalmát!
 Legyen $(R, +, *)$ két binér műveletes struktúra. $(+, *: R_2 \rightarrow R, *: R_2 \rightarrow R)$ gyűrű, ha:
 - $(R, +)$ Abel-csoport
 - $(R, *)$ félcsoport
 - Teljesül a $*$ műveletnek a $+$ -ra vonatkozó mindkét oldali disztributivitása:
 $x * (y + z) = x * y + x * z$ és $(y + z) * x = y * x + z * x$
98. Definiáld a disztributivitás fogalmát!
 Legyen $(R, +, *)$, és $k, m, n \in R$, ekkor:
 $k * (m + n) = (k * m) + (k * n)$
99. Definiáld az egységelemes gyűrű fogalmát!
 Legyen R egy halmaz, mely a $(+, *)$ binér műveletekből álló párral gyűrűt alkot. Ezt egységelemes gyűrűnek nevezzük, ha a szorzásnak van egységeleme.
100. Definiáld a nullosztópár fogalmát!
 Ha x, y egy R gyűrű nullától különböző elemei, és $xy = 0$, akkor azt mondjuk, hogy x és y egy nullosztópár.
101. Definiáld a nullosztómentes gyűrű fogalmát!
 Egy legalább kételemű gyűrűt nullosztómentesnek nevezünk, ha nincsenek benne nullosztópárok.
102. Definiáld az integritási tartomány fogalmát!
 Kommutatív, nullosztómentes gyűrűt integritási tartománynak nevezünk.

103. Adj példát véges és végtelen testre!
 Véges például $\mathbb{Z}_3$.
 A komplex számok halmaza végtelen.
104. Definiáld az egység fogalmát!
 Egységnek nevezzük egy R egységelemes integritási tartomány azon elemeit, melyeknek van a szorzásra nézve inverzük. Az egységek a szorzásra nézve Abel-csoportot alkotnak, a gyűrű egységcsoportját.
105. Definiáld az irreducibilis elem fogalmát!
 Legyen R egységelemes integritási tartomány. Egy $0 \neq a \in R$ elemet felbonthatatlannak (vagy irreducibilisnek) nevezünk, ha nem egység, és csak triviális módon írható fel szorzatként, tehát $a = bc$, $b, c \in R$ esetén b vagy c egység. Ez azzal ekvivalens, hogy a -nak nincs más osztója, mint az egységek és az asszociáltjai.
106. Definiáld a karakterisztika fogalmát!
 Egy nullosztómentes gyűrűben a nem nulla elemek additív rendje megegyezik és ez vagy egy p prímszám, vagy végtelen. A gyűrű karakterisztikája véges esetben p , különben 0 .
107. Definiáld a polinomokat a műveletekkel!
 Legyen R gyűrű. R feletti polinom egy olyan végtelen $(f_0, f_1, f_2, \dots)$ sorozat, amelynek csak véges sok tagja nem nulla és $f_j \in R$.

Műveletek:

$$f = (f_0, f_1, f_2, \dots)$$

$$g = (g_0, g_1, g_2, \dots)$$

$$f + g = (f_0 + g_0, f_1 + g_1, f_2 + g_2, \dots)$$

$$f * g = h = (h_0, h_1, h_2, \dots) \text{ ahol}$$

$$h_n := \sum_{i+j=n} f_i g_j = \sum_{i=0}^n f_i * g_{n-i}$$

108. Definiáld a konstans polinom fogalmát!
 Azt az f polinomot, melyre $\deg(f) \leq 0$, konstans polinomnak nevezzük.

109. Definiáld a főegyüttható és a polinom fokának fogalmát!

Ha R egységelemes, akkor legyen $x = (0, 1, 0, 0, \dots)$. $x^i = (0, 0, 0, \underbrace{1}_{i.\text{elem}}, 0, 0, \dots)$.

$$f = (f_0, f_1, f_2, \dots) = \sum_{i \geq 0} f_i x^i = f_0 + f_1 x + f_2 x^2 + f_3 x^3 + \dots + f_n x^n.$$

Ekkor f_n a főegyüttható és $n = \deg(f)$ az f foka.

110. Definiáld a nullpolinomot!

A nullpolinom ($0 = (0, 0, 0, \dots)$) esetén $\deg(0) = -\infty$.

111. Definiáld a lineáris polinom fogalmát!

Legyen $f(x) = \sum_{i=0}^n f_i x^i$, $f_n \neq 0$, $\deg(f) = n$, $f_n x^n$ a fő tag. Az ilyen alakú polinomot monomnak nevezzük.

Ha $\deg(f) \leq 1$, akkor az f lineáris polinom.

112. Definiáld a monom fogalmát!

Legyen $f(x) = \sum_{i=0}^n f_i x^i$, $f_n \neq 0$, $\deg(f) = n$, $f_n x^n$ a fő tag. Az $f_k x^k$ alakú polinomot monomnak nevezzük.

113. Definiáld a főpolinom fogalmát!

Ha egy polinom főegyütthatója 1, akkor főpolinomnak nevezzük.

114. Mit mondhatunk polinomok összegének/szorzatának fokáról?

Adott f, g polinomok esetén $\deg(f + g) \leq \max(\deg(f), \deg(g))$.

Továbbá $\deg(f * g) \leq \deg(f) + \deg(g)$ és gyűrű fölötti nullosztómentes polinomok esetén utóbbi esetben egyenlőség van.

115. Definiáld a helyettesítési érték fogalmát!

116. Definiáld a gyök fogalmát!

Az $f(x) = \sum_{i=0}^n f_i x^i$ ($f_n \neq 0$) polinom r helyen vett helyettesítési értéke:

$$f(r) := \sum_{i=0}^n f_i r^i$$

Ha $f(r) = 0$, akkor azt mondjuk, hogy r gyöke f -nek.

117. Definiáld a polinomfüggvény fogalmát!

Legyen R gyűrű, f egy $R[x]$ -beli polinom, r a gyűrű egy eleme. Ekkor az $r \rightarrow f(r)$, $R \rightarrow R$ függvényt az f -hez tartozó polinomfüggvénynek hívjuk. Két különböző polinomnak lehet ugyanaz a polinomfüggvénye.

118. Adj példát, amikor különböző polinomokhoz ugyanaz a polinomfüggvény tartozik!
 $\mathbb{P}_{\mathbb{Z}_3}$ felett az x és x^3 polinomok polinomfüggvénye ugyanaz, mégis két különböző polinom.

Bizonyítások

- Mit mondhatunk polinomok összegének/szorzatának fokáról?

Adott f, g polinomok esetén $\deg(f + g) \leq \min(\deg(f), \deg(g))$.

Továbbá $\deg(f * g) \leq \deg(f) + \deg(g)$ és gyűrű fölötti nullosztómentes polinomok esetén utóbbi esetben egyenlőség van.

Bizonyítás:

Legyen $\deg(f) = n, \deg(g) = k$!

$j > \max(n, k)$ esetén $f_j = g_j = 0$, így $f_j + g_j = 0$. (Összegre vonatkozó becslés)

$$j > n + k \text{ esetén } h = f * g - re: \quad h_j = \sum_{m+l=j} f_m * g_l,$$

$m \leq n$ esetén $l = j - m > n + k - m \geq k$. (Szorzatra vonatkozó becslés)

$$h_{n+k} = \sum_{n+l=n+k} f_n * g_l = f_n * g_k \neq 0$$

7. Polinomok maradékos osztásának tétele és következményei

119. Hogyan szól a polinomok maradékos osztásának tétele?

Legyen R egységelemes integritási tartomány (kommutatív, nullosztómentes gyűrű).

$f, g \in \mathbb{R}[x], g$ főegyütthatója egység, ekkor egyértelműen létezik $q, r \in \mathbb{R}[x]$, hogy $f = g * q + r$ és $\deg(r) < \deg(g)$.

120. Mit jelent a gyöktényező leválasztása?

Ha $f \neq 0$ és c az f gyöke, akkor valamely $q \neq 0$ polinomra $f = (x - c)q$.

121. Hány gyöke lehet egy polinomnak?

Ha $f \neq 0$, akkor legfeljebb $\deg(f)$ gyöke lehet.

122. Mit mondhatunk két, $n+1$ helyen megegyező, legfeljebb n -ed fokú polinomról?

Ha két n -ed fokú polinom $n+1$ helyen ugyanazt az értéket veszi fel, akkor ők egyenlők.

123. Mit mondhatunk végtelen $\mathbb{R}$ esetén a polinomfüggvényekről?

Ha $\mathbb{R}$ nem véges, akkor két $\mathbb{R}[x]$ -beli polinomhoz nem tartozhat ugyanaz a polinomfüggvény.

124. Ismertesd a bővített Euklideszi algoritmust!

Legyen $\mathbb{R}$ test, $f, g \in \mathbb{R}[x]$ és $g \neq 0$!

Az algoritmus kiszámolja az $(f, g) = d$ legnagyobb közös osztót.

Továbbá olyan $u, v \in \mathbb{R}[x]$ polinomokat, amikre $d = u * f + v * g$.

$u_{-1}(x) = 1$	$v_{-1}(x) = 0$
$u_0(x) = 0$	$v_0(x) = 1$
$u_1(x) = 1$	$v_1(x) = -q_1(x)$
$u_k(x) = u_{k-2}(x) * q_k(x) + u_{k-1}(x)$	$v_k(x) = v_{k-2}(x) - q_k(x) * v_{k-1}(x)$

$$f(x) = q_1(x) * g(x) + r_1(x)$$

$$g(x) = q_2(x) * r_1(x) + r_2(x)$$

$$r_1(x) = q_3(x) * r_2(x) + r_3(x)$$

$\vdots$

$$r_{n-2}(x) = q_n(x) * r_{n-1}(x) + r_n(x)$$

$$r_{n-1}(x) = q_{n+1}(x) * r_n(x) + 0$$

Az eljárás véget ér, mert a $\deg(r_1) > \deg(r_2) > \dots > \deg(r_n)$.

Indukcióval belátható, hogy:

$$v_k(x) = u_k(x)f(x) + v_k(x) * g(x)$$

Emiatt ha $d|f$ és $d|g \Rightarrow d|r_k$ (bármely k -ra teljesül).

Másrészt:

$$r_n \mid r_{n-1} \mid r_{n-2} \mid \dots$$

$$r_n \mid g, r_n \mid f$$

$\Rightarrow r_n$ a legnagyobb közös osztó.

125. Ismertesd a Horner-elrendezést!

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, a_n \neq 0$$

Célja a polinom adott helyen vett helyettesítési értékének gyors számolása.

Táblázatos formában:

	a_n	a_{n-1}	...	a_j	a_{j-1}	a_0	
c	-	$c_{n-1} = a_n$		c_j	$c_{j-1} = c_j * c + a_j$		$c_0 * c + a_0 = f(c)$

126. Adj példát olyan polinomra, amelynek különböző polinomgyűrűben különböző számú gyöke van!
???

Bizonyítások

- Hogyan szól a polinomok maradékos osztásának tétele?

Legyen R egységelemes integritási tartomány (kommutatív, nullosztómentes gyűrű).

$f, g \in \mathbb{R}[x], g \neq 0$ és tegyük fel, hogy főegyütthatója egység R -ben.

Ekkor egyértelműen léteznek olyan $q, r \in \mathbb{R}[x]$ polinomok, hogy

$$f = g * q + r \text{ és } \deg(r) < \deg(g).$$

Bizonyítás:

Fokszám szerinti indukcióval:

$$\text{Legyen } f = \sum_{i=0}^n f_i * x^i, g = \sum_{i=0}^k g_i * x^i, \text{ ahol } f_i \neq 0 \text{ és } g_k \neq 0.$$

Ha $n < k$, akkor $q = 0, r = f$ megfelelő választás.

$$f^* := f - f_n * g_k^{-1} * g * x^{n-k}.$$

- Mit jelent a gyöktényező leválasztása?

Ha $f \neq 0$ és c az f gyöke, akkor valamely $q \neq 0$ polinomra $f = (x - c)q$.

Bizonyítás:

A maradékos osztás tételét alkalmazva $g = x - c$ választással $f = (x - c)q + r$.

Ha $r \neq 0$ lenne, akkor $\deg(r) = 0$ miatt a c helyen az egyik oldal helyettesítési értéke nulla, a másiké nem nulla lenne.

- Hány gyöke lehet egy polinomnak?

Ha $f \neq 0$, akkor f – nek legfeljebb $\deg(f)$ gyöke lehet.

Bizonyítás:

Fokszám szerinti indukcióval:

Ha $\deg(f) = 0$, igaz az állítás.

Ha $\deg(f) > 0$, és c egy gyök, akkor $f = (x - c)g$, ahol $1 + \deg(g) = \deg(f)$.

Ha d az f egy gyöke, akkor vagy $d - c = 0$, azaz $d = c$, vagy d gyöke g – nek, ahonnan következik az állítás.

- Mit mondhatunk két, $n+1$ helyen megegyező, legfeljebb n -ed fokú polinomról?

Ha két, legfeljebb n – ed fokú polinom $n + 1$ különböző helyen ugyanazt az értéket veszi fel, akkor megegyezik.

Bizonyítás:

A két polinom különbsége legfeljebb n -ed tagú és $n+1$ gyöke van. Az előző állítás miatt ez csak akkor fordulhat elő, ha a nullpolinom a különbség, így tényleg egyenlők a polinomjaink.

- Mit mondhatunk végtelen R esetén a polinomfüggvényekről?

Ha R végtelen, akkor két különböző polinomhoz nem tartozik ugyanaz a polinomfüggvény.

Bizonyítás:

Egyébként a különbségpolinomnak végtelen sok gyöke lenne.

8. Polinomok algebrai deriváltja, véges testek, racionális gyökteszt, Lagrange-interpoláció

127. Definiáld az algebrai derivált fogalmát!

Legyen az $\mathbb{R}$ gyűrű, az $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{R}[x]$

*algebrai deriváltja $f'(x) = n * a_n * x^{n-1} + (n - 1)a_{n-1}x^{n-2} + \dots + 2a_2 * x + a_1 \in \mathbb{R}[x]$*

128. Milyen tulajdonságokkal rendelkezik az algebrai derivált?

(1) konstans polinom deriváltja a nulla polinom

(2) az x polinom deriváltja az egységelem

(3) $(f + g)' = f' + g'$, ha $f, g \in R[x]$ (additivitás)

(4) $(fg)' = f'g + fg'$, ha $f, g \in R[x]$ (szorzat differenciálási szabálya)

129. Definiáld a többszörös gyök fogalmát!

Legyen $\mathbb{R}$ egységelemes integritási tartomány, $f \in \mathbb{R}[x]$, $c \in \mathbb{R}$, $n \in \mathbb{N}$, $n \geq 1$.

c az f -nek n -szeres gyöke, ha $(x - c)^n \mid f$, de $(x - c)^{n+1} \nmid f$.

Megjegyzés:

Ekvivalens azzal, hogy $f(x) = (x - c)^n \cdot g(x)$, ahol $g(c) \neq 0$.

130. Milyen kapcsolat van egy polinom gyökei illetve a deriváltjának a gyökei között?

Legyen R egységelemes integritási tartomány, f egy $R[x]$ -beli polinom, c pedig az f -nek egy n -szeres gyöke.

Ekkor c az f' -nek is legalább $(n-1)$ -szeres gyöke, és ha a gyűrű karakterisztikája nem osztja n -t, akkor pontosan $(n-1)$ -szeres gyöke.

131. Adj példát olyan polinomra, amelynek van olyan n -szeres gyöke, ami a deriváltjának is n -szeres gyöke!
???

132. Mik lehetnek egy primitív egész együtthatós polinom racionális gyökei?

???

133. Ismertesd a Lagrange-interpolációt!

Legyenek R egységelemes integritási tartománynak $c_0, c_1, \dots, c_n$ különböző elemei, $d_0, d_1, \dots, d_n$ pedig tetszőleges elemei. Ekkor legfeljebb egy olyan legfeljebb n -ed fokú f polinom létezik, melyre $f(c_j) = d_j$, ha $j = 0, 1, \dots, n$. Ha R test, akkor mindig létezik is ilyen polinom.

Legyen

$$l_j(x) = \frac{\prod_{i \neq j} (x - c_i)}{\prod_{i \neq j} (c_j - c_i)}$$

a j -edik Lagrange interpolációs alappolinom, és legyen $f(x) = \sum_{j=0}^n d_j l_j(x)$.

134. Hogyan használható a Lagrange-interpoláció titokmegosztásra?

Legyen $m, n \in \mathbb{N}^+$, $m < n$. Tegyük fel, hogy egy $t \in \mathbb{N}$, $t < T$ titkot n részre akarunk szétosztani úgy, hogy bármelyik m részből a titok visszaállítható legyen, de kevesebből semmi információt ne lehessen kapni a titokról. Válasszunk egy T -nél (és lehetőleg n -nél is) nagyobb p prímet és véletlen $a_1, a_2, \dots, a_{m-1} \in \mathbb{Z}_p$ együtthatókat, majd számítsuk ki a $\mathbb{Z}_p$ feletti $t + a_1 x^1 + a_2 x^2 + \dots + a_{m-1} x^{m-1}$ polinom $y_1, y_2, \dots, y_n$ értékeit az $1, 2, \dots, n$ helyeken. Ezek az y_j -k a titokrészek: bármelyik m titokrészből a polinom megkapható Lagrange-interpolációval, így adódik a konstans tag, azaz a titok.

Bizonyítások

- Milyen kapcsolat van egy polinom gyökei illetve a deriváltjának a gyökei között?
- Mik lehetnek egy primitív egészegyütthatós polinom racionális gyökei?

9. Polinomok irreducibilitása

135. Hogyan jellemezhetőek test fölötti polinomgyűrűben az egységek?

F test fölötti polinomgyűrűben az egységek azon f polinomok, amikre $\deg(f) = 0$ (nemnulla konstans polinom).

136. Mit mondhatunk test fölötti elsőfokú polinomokról a gyökökkel kapcsolatban?

Ha F test, $F \in F[x]$, $\deg(f) = 1$, akkor létezik $c \in F: f(c) = 0$ (azaz c gyök).

137. Mit mondhatunk a lineáris polinomokról test fölötti polinomgyűrűben irreducibilitás szempontjából? ???

138. Hogyan jellemezhetőek a $\mathbb{C}$ fölötti irreducibilis polinomok?

$f \in \mathbb{C}[x]$, $\deg(f) \geq 2$ esetén f felbontható.

139. Hogyan jellemezhetőek az $\mathbb{R}$ fölötti irreducibilis polinomok?

$f \in \mathbb{R}[x]$ irreducibilis pontosan akkor, ha $\deg(f) = 1$, vagy $\deg(f) = 2$ és nincsen valós gyöke.

140. Mit mondhatunk véges testekről az elemszámmal kapcsolatosan?

???

141. Definiáld a primitív polinom fogalmát!

Egy polinomot primitív polinomnak nevezünk, ha az együtthatóinak a legnagyobb közös osztója 1.

Például: $f(x) = 4 \in \mathbb{Z}[x]$, $\deg(f) = 0$. $f(x) = 2 \cdot 2$

142. Hogy szól a Schönemann-Eisenstein-tétel egész együtthatós polinomokra?

Legyen $f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$, $a_n \neq 0$, $n \geq 1$ primitív polinom.

Ha létezik p prímszám, amire:

$$\begin{aligned} p &\nmid a_n \\ p &\mid a_j, 0 \leq j < n \\ p^2 &\nmid a_0 \end{aligned}$$

akkor $f(x)$ irreducibilis $\mathbb{Z}[x]$ – ben.

143. Hogyan szól a Gauss-tétel egész együtthatós polinomokra?

Ha $f(x)$ legalább elsőfokú primitív polinom, akkor $f(x)$ irreducibilis $\mathbb{Z}[x]$ -ben pontosan akkor, ha $f(x)$ irreducibilis $\mathbb{Q}[x]$ -ben.

Bizonyítások

- Hogyan jellemezhetőek test fölötti polinomgyűrűben az egységek?

F test fölötti polinomgyűrűben az egységek azon f polinomok, amikre $\deg(f) = 0$ (nemnulla konstans polinom).

Bizonyítás:

$\deg(f) = 0 \Rightarrow f = a_0 \neq 0, a_0 \in F$ egység, így egység $F[x]$ – ben is. 0 nyilván nem egység.

Ha $\deg(f) \geq 1, f \cdot a = 1 \Rightarrow \deg(f) + \deg(a) = 0$, ilyen a nem létezik, ezért f nem egység.

- Mit mondhatunk test fölötti elsőfokú polinomokról a gyökökkel kapcsolatban?

Ha F test, $F \in F[x], \deg(f) = 1$, akkor létezik $c \in F: f(c) = 0$ (azaz c gyök).

Bizonyítás:

???

- Mit mondhatunk a lineáris polinomokról test fölötti polinomgyűrűben irreducibilitás szempontjából?

??

- Hogyan jellemezhetőek a $\mathbb{C}$ fölötti irreducibilis polinomok?

$f \in \mathbb{C}[x], \deg(f) \geq 2$ esetén f felbontható.

Bizonyítás:

Az algebra alaptétele miatt van gyök, gyöktényezőt kiemelve pedig a hányados legalább elsőfokú, így tehát kaptunk nemtriviális szorzat-előállítást.

- Hogyan jellemezhetőek az $\mathbb{R}$ fölötti irreducibilis polinomok?

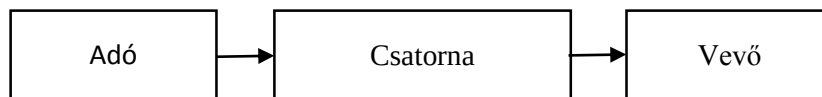
???

10. Kódolás

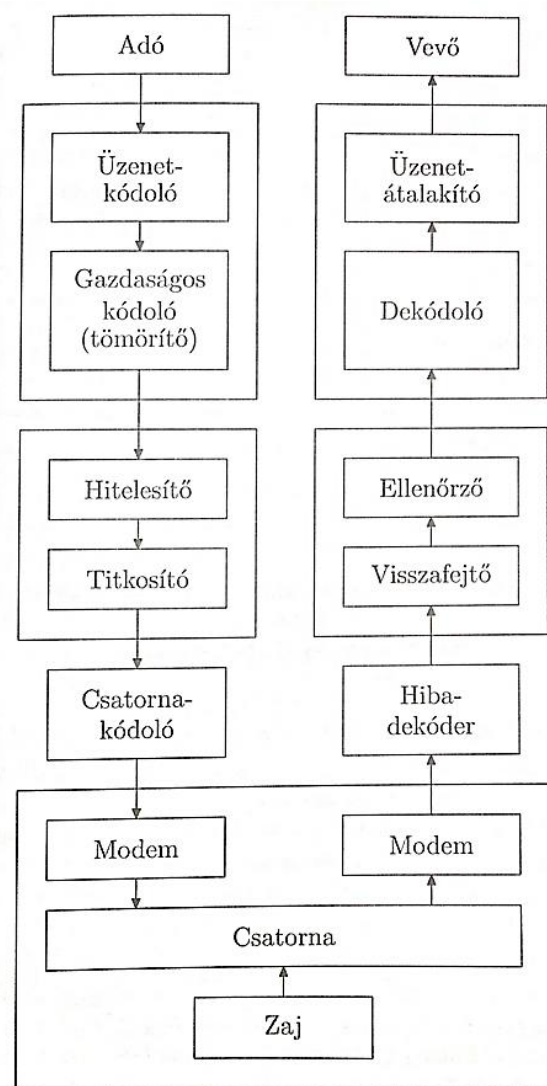
144. Definiáld a kódolás fogalmát!

Üzenetek halmazát egy másik (tárolható, küldhető formátumú) halmazra képezzük.

145. Add meg a kommunikáció vázlatos ábráját!



146. Add meg a kommunikáció részletes ábráját!



147. Definiáld az információ fogalmát!

Új ismeret, az általa megszüntetett bizonytalansággal mérjük.

148. Definiáld a gyakoriság/relatív gyakoriság fogalmát!

149. Definiáld az eloszlás fogalmát!

Legyen az összes különböző üzenet $a_1, a_2, \dots, a_m$ ($m \in \mathbb{N}^+$). Ha az a_i üzenet k_i -szer fordul elő, akkor azt mondjuk, hogy gyakorisága k_i , relatív gyakorisága pedig $p_i = k_i/n > 0$.

A $p_1, p_2, \dots, p_m$ szám-m-est az üzenetek eloszlásának nevezzük. Nyilván $\sum_{i=1}^m p_i = 1$.

150. Definiáld üzenet egyedi információtartalmát!

Az a_i üzenet egyedi információtartalmának célszerű definíciója $I_i = -\log_r p_i$, ahol r egy 1-nél nagyobb valós szám. A logaritmus alapja az információ egysége. Amennyiben az alap 2, akkor az információ egysége a bit.

151. Definiáld az entrópia fogalmát!

Egy eloszlás entrópiáját a

$$H_r(p_1, \dots, p_m) = - \sum_{i=1}^m p_i \log_r p_i$$

összefüggéssel értelmezzük.

152. Milyen korlát adható az entrópiára?

Bármilyen eloszláshoz tartozó entrópiára $H_r(p_1, p_2, \dots, p_m) \leq \log_r m$, és egyenlőség pontosan akkor teljesül, ha $p_1 = p_2 = \dots = p_m = 1/m$.

153. Definiáld a betűnkénti kódolást!

Adott egy A (véges) halmaz – kódolandó ábécé – és egy B (véges) halmaz – kódábécé. Ekkor a betűnkénti kódolás egy $\varphi: A \rightarrow B^*$ leképezés.

154. Definiáld a prefix, infix, szuffix fogalmát!

Legyenek $\alpha, \beta, \gamma \in A^*$. Ekkor α prefixe $\alpha\gamma$ -nak, γ szuffixe $\alpha\gamma$ -nak, és β infixe $\alpha\beta\gamma$ -nak.

155. Definiáld a triviális prefix/infix/suffix fogalmát!

Ha α egy szó, akkor az üres szó és α mind prefixe, mind szuffixe, mind pedig infixe α -nak. Ezek az α triviális prefixei, triviális szuffixei és triviális infixei.

156. Definiáld a valódi prefix/infix/suffix fogalmát!

A prefix, szuffix, illetve infix valódi prefix, valódi szuffix, illetve valódi infix, ha nem egyezik meg α -val.

157. Definiáld a prefixmentes halmaz fogalmát!

Szavak egy halmaza prefixmentes halmaz, ha nincs benne két olyan különböző szó, hogy egyik a másik prefixe.

158. Definiáld a kódfa fogalmát!

A betűnkénti kódolás szemléletesen és egyértelműen adható meg egy irányított fa segítségével. Legyen $\varphi: A \rightarrow B^+$ egy betűnkénti kódolás. Tetszőleges szóhalmaz, így a φ értékkészletében lévő összes prefixeinek halmaza is részbenrendezett a „prefixe” relációra. Készítsük el ennek a relációnak a Hasse-diagramját. Egy irányított fát kapunk, aminek a gyökere az üres szó, továbbá minden szó a hosszának megfelelő szinten van.

A fa éleit színezzük úgy B elemeivel, hogy ha $\beta = \alpha b$ valamely $b \in B$ -re, akkor az α -ból β -ba menő él színe legyen b . Nyilván bármely csúcs esetén a csúcsból kivezető élek mind különbözőek. A kódfa csúcsait is kiszínezhethetjük, az $a \in A$ kódjának megfelelő csúcs színe legyen a , azon csúcsok színe, melyek nincsenek az értékkészletben, legyen üres.

159. Definiáld a felbontható kód fogalmát!

Egy kód felbontható, ha $\varphi: A^* \rightarrow B^*$ injektív.

160. Definiáld a prefix kód fogalmát!

Olyan kód, amelyik prefixmentes.

161. Definiáld az egyenletes/fix hosszúságú/blokk kód fogalmát!

Minden kódszó egyforma hosszú.

162. Definiáld a vesszős kód fogalmát!

Van egy külön karakter a B kódábécében, a „vessző”, mely minden kódszó végén szerepel, de csak ott.

163. Adj példát nem prefix, de felbontható kódra!

???

164. Hogyan szól a McMillan egyenlőtlenség és a megfordítása?

Legyen A, B két véges ábécé, $\varphi: A \rightarrow B^+$ injektív leképezés, $K = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ betűnkénti kód úgy, hogy a kódszavak hosszai $l_1, l_2, \dots, l_n$. Ha K felbontható és $|B| = r$ (kód ábécé elemszáma), akkor

$$\sum_{i=1}^n r^{-l_i} \leq 1. \quad (*)$$

Fordítva:

Ha $l_1, l_2, \dots, l_n$ pozitív egészek, amikre teljesül $(*)$, akkor A -nak van B elemeivel olyan kódolása, ami felbontható és a kódszavak hosszai $l_1, l_2, \dots, l_n$. Sőt, van ilyen prefix kód is!

165. Definiáld az általános szóhosszúságot!

Legyen $A = \{a_1, \dots, a_n\}$ a kódolandó ábécé, $p_1, \dots, p_n$ a betűk eloszlása, $\varphi: A \rightarrow B^+$ egy betűnkénti kódolás, l_i az a_i kódjának hossza. Ekkor $\bar{l} = \sum_{i=1}^n p_i l_i$ a kód átlagos szóhosszúsága.

166. Definiáld az optimális kód fogalmát!

Ha adott elemszámú ábécével és eloszlással egy felbontható betűnkénti kód átlagos szóhosszúsága minimális, akkor optimális kódnak nevezzük.

167. Mit mondhatunk optimális kód létezésével kapcsolatosan?

Válasszunk egy tetszőleges felbontható kódot, és legyen ennek átlagos szóhosszúsága l . Mivel $p_i l_i > l$ esetén a kód nem lehet optimális, elég azon kódokat tekintenünk, amelyekre $l_i \leq l/p_i$, ha $i = 1, \dots, n$. Ilyen kód csak véges sok van, így van köztük minimális átlagos hosszúságú.

168. Hogyan szól Shannon tétele zajmentes csatornákra?

Adott $(p_1, p_2, \dots, p_m)$ eloszlás mellett felbontható kód esetén $H_r(p_1, \dots, p_m) \leq \bar{l}$.

169. Mit mondhatunk Shannon kód létezéséről?

$m > 1$ esetén van olyan prefix kód, melyre $\bar{l} < H_r(p_1, \dots, p_m) + 1$.

170. Hogyan konstruálunk Huffman-kódot?

Az $a_1, a_2, \dots, a_n$ üzenetek eloszlása legyen $(p_1, p_2, \dots, p_n)$. Legyen a jelkészlet r elemű. Rendezzük valószínűség szerint csökkenő sorrendbe az üzeneteket.

Legyen $n - 2 = (r - 1)q + m$: $0 \leq m < r - 1$.

Legyen $t = m + 2$, helyettesítsük az utolsó t üzenetet egy új betűvel, a megfelelő valószínűségek összege legyen az új betűhöz tartozó valószínűség.

Ezután ismételjük a redukciót, de most már minden lépésben r darab üzenettel csökkentjük a halmazt. Ha legfeljebb r üzenetet kaptunk, ezek kódjai legyenek a megfelelő jelek. Ezután a redukciónál visszafelé haladva, ha volt összevonás, a következő karakter kiegészítésével kapjuk a kódot.

Példa a következő oldalon.

Példa:

Kódolandó ábécé: { a, b, c, d, e, f, g, h, i, j }

Eloszlások: { 0.17(a), 0.02(b), 0.13(c), 0.02(d), 0.01(e), 0.31(f), 0.02(g), 0.17(h), 0.06(i), 0.09(j) }

Kódoló ábécé: { 0, 1, 2 }

n := 10

r := 3

$$8 = (3-1) * 4 + 0 \Rightarrow m = 0 \Rightarrow t = 2$$

Sorba rendezünk eloszlások szerint csökkenő sorrendben:

F: 0,31 A: 0,17 H: 0,17 C: 0,13 J: 0,09 I: 0,06 B: 0,02 D: 0,02 G: 0,02 E: 0,01	F: 0,31 A: 0,17 H: 0,17 C: 0,13 J: 0,09 I: 0,06 (G, E): 0,03 B: 0,02 D: 0,02	F: 0,31 A: 0,17 H: 0,17 C: 0,13 J: 0,09 ((G, E), B, D): 0,07 I: 0,06	F: 0,31 <i>(J, ((G, E), B, D), I): 0,22</i> A: 0,17 H: 0,17 C: 0,13	<i>(A, H, C): 0,47</i> F: 0,31 <i>(J, ((G, E), B, D), I): 0,22</i>
--	---	---	--	--

Kódolás:

(A, H, C)	0	A: 00, H: 01, C: 02		
F	1			
(J, ((G, E), B, D), I)	2	J: 20, ((G, E), B, D): 21, I: 22	(G, E): 210, B: 211, D: 222	G: 2100, E: 2101

A	00
B	211
C	02
D	212
E	2101
F	1
G	2100
H	01
I	22
J	20

Entrópia ~ 1,73

Átlagos kódhossz ~ 1,79

Bizonyítások

- Milyen korlát adható az entrópiára?

Bármilyen eloszláshoz tartozó entrópiára $H_r(p_1, p_2, \dots, p_m) \leq \log_r m$, és egyenlőség pontosan akkor teljesül, ha $p_1 = p_2 = \dots = p_m = 1/m$.

Bizonyítás:

Mivel $r > 1$ esetén $-\log_r$ szigorúan konvex függvény,

$$-H_r(p_1, \dots, p_m) = \sum_{i=1}^m p_i \log_r p_i = - \sum_{i=1}^m p_i \log_r \left(\frac{1}{p_i} \right) \geq -\log_r \left(\sum_{i=1}^m p_i / p_i \right) = -\log_r m.$$

- Hogyan szól Shannon tétele zajmentes csatornára?

Adott $(p_1, p_2, \dots, p_m)$ eloszlás mellett felbontható kód esetén $H_r(p_1, \dots, p_m) \leq \bar{l}$.

- Mit mondhatunk Shannon kód létezéséről?

$m > 1$ esetén van olyan prefix kód, melyre $\bar{l} < H_r(p_1, \dots, p_m) + 1$.

Bizonyítás:

Válasszunk olyan $l_1, l_2, \dots, l_m$ természetes számokat, amelyekre $r^{-l_i} \leq p_i < r^{-l_i+1}$, $1 \leq i \leq m$.

Ekkor $\sum_{i=1}^m r^{-l_i} < \sum_{i=1}^m p_i = 1$, ezért a McMillan egyenlőtlenség megfordítása miatt van prefix kód az adott l_i hosszakkal. $l_i < 1 - \log_r(p_i)$.

$$\bar{l} = \sum_{i=1}^m p_i * l_i < \sum_{i=1}^m p_i (1 - \log_r(p_i)) = \sum_{i=1}^m \underbrace{p_i}_1 - \sum_{i=1}^m \underbrace{p_i * \log_r(p_i)}_{H_r(p_1, \dots, p_m)}.$$

11. Hibakorlátozó kódolás

171. Definiáld a t-hibajelző kód fogalmát!

Egy kód t-hibajelző, ha minden olyan esetben jelez, ha az elküldött és megkapott szó legfeljebb t helyen tér el. Egy kód pontosan t-hibajelző, ha t-hibajelző, de nem t+1-hibajelző, azaz van olyan t+1 hiba, amelyet a kód nem jelez.

172. Definiáld a Hamming-távolságot!

Legyen A véges halmaz, $u, v \in A^n$ (azaz n betűből álló szavak).

Ekkor $d(u, v) = |\{i: 1 \leq i \leq n, u_i \neq v_i\}|$ az u és v Hamming-távolsága.

173. Hogyan működik az ISBN kódolása?

Legyen $d_1, d_2, \dots, d_n$ decimális számjegyek egy sorozata, $n \leq 10$.

Egészítsük ki a sorozatot egy $n + 1$ – edik számjeggyel, amelynek értéke

$$d_{n+1} = \sum_{j=1}^m j d_j \bmod 11;$$

ha $b_{n+1} = 10$, akkor az X „római számjegy”. Ha valamelyik számjegyet elírjuk, akkor az összefüggés nyilván nem teljesülhet.

174. Mi az a paritásbites kód?

Adjunk meg egy n hosszú, 0-1 sorozatot. Ezt egészítsük ki egy $n+1$ -edik bittel, mely legyen 1, ha páratlan sok 1-es van az n hosszú sorozatban, különben legyen 0.

Pl.:

$(0,0,0) \mapsto (0,0,0,0)$

$(1,1,1) \mapsto (1,1,1,1)$

$(1,0,1) \mapsto (1,0,1,0)$

$(b_1, b_2, \dots, b_k) \mapsto (b_1, b_2, \dots, b_k, \sum_{i=1}^n b_i \bmod 2)$

Ez a kód egy 1-hibajelző kód.

175. Mi az a kétdimenziós paritásbites kód?

$b_{0,0}$	...	$b_{0,j}$	...	$b_{0,n-1}$	$b_{0,n}$
$\vdots$		$\vdots$		$\vdots$	$\vdots$
$b_{i,0}$	...	$b_{i,j}$	...	$b_{i,n-1}$	$b_{i,n}$
$\vdots$		$\vdots$		$\vdots$	$\vdots$
$b_{m-1,0}$	...	$b_{m-1,j}$	...	$b_{m-1,n-1}$	$b_{m-1,n}$
$b_{m,0}$	...	$b_{m,j}$	...	$b_{m,n-1}$	$b_{m,n}$

2 hibát jelez

1 hibát javít

Pl.: Mágnesszalag

176. Mit jelent a minimális távolságú dekódolás?

Egy adott szóhoz azt a kódszót rendeljük, amelyik hozzá legközelebb van. Több ilyen szó esetén az egyiket (de mindig ugyanazt) választjuk.

177. Definiáld a t -hibajavító kód fogalmát!

Egy kód t -hibajavító, ha minden olyan esetben helyesen javít, amikor egy elküldött kódszó legfeljebb t helyen változik meg. A kód pontosan t -hibajavító, ha t -hibajavító, de nem $t+1$ -hibajavító, azaz van olyan $t+1$ hibával érkező üzenet, amelyet a kód helytelenül javít, vagy nem javít.

178. Mi az az ismétléses kód?

Legyen egy binárisan kódolt üzenethalmazunk, és küldjük el az üzenetet úgy, hogy minden egyes bitet megháromszorozunk, azaz ugyanazt a bitet háromszor egymás után küldjük. A vétel helyén a három összetartozó bit közül legalább kettő azonos lesz, így a minimális távolságú dekódolás esetén a vett három bithez a többségi döntés alapján rendelünk egy bitet.

179. Fogalmazd meg a Singleton-korlátra vonatkozó állítást!

Legyen $K \subseteq A^n, |A| = q, d(K) = d$.

Ekkor: $|K| \leq q^{n-d+1}$.

180. Definiáld az MDS-kód fogalmát!

Ha egy Singleton-korláton teljesül az egyenlőség, akkor maximális távolságú szeparábilis kódnak, azaz MDS-kódnak nevezzük.

181. Fogalmazd meg a Hamming-korlátra vonatkozó állítást!

Legyen $K \subseteq A^n, |A| = q, K$ t -hibajavító.

Ekkor:

$$|K| * \sum_{j=0}^t \binom{n}{j} * (q-1)^j \leq q^n$$

182. Definiáld a perfekt kód fogalmát!

Ha a Hamming korlát egyenlőséggel teljesül, perfekt kódról beszélünk.

Bizonyítások

- Fogalmazd meg a Singleton-korlátra vonatkozó állítást!

Legyen $k \subseteq A^n, |A| = q, d(K) = d$.

Ekkor: $|K| \leq q^{n-d+1}$.

Bizonyítás:

Mivel a minimális távolság d , így az utolsó $d-1$ karaktert elhagyva mindig különböző szavakat kapunk. Ezek hossza $n-d+1$, azaz $n-d+1$ hosszú szavak száma $q^{n-d+1} \Rightarrow |K| \leq q^{n-d+1}$.

- Fogalmazd meg a Hamming-korlátra vonatkozó állítást!

Legyen $K \subseteq A^n, |A| = q, K$ t -hibajavító.

Ekkor:

$$|K| * \sum_{j=0}^t \binom{n}{j} * (q-1)^j \leq q^n$$

Bizonyítás:

Ha a kód t -hibajavító, akkor egy kódszó t -sugarú környezetében lévő szót az adott kódszóra javítunk.

Ugyanaz a szó nem lehet két különböző kódszó t -sugarú környezetében, mert akkor a kód nem lenne t -hibajavító, így ezek a környezetek diszjunktak.

Egy kódszó t -sugarú környezetében lévő szavak száma:

$$\sum_{j=0}^t \binom{n}{j} (q-1)^j$$

12. Lineáris kódolás

183. Definiáld a lineáris kód fogalmát!

Legyen F véges test a betűk halmaza, F^n az n hosszú szavak halmaza. Ha $K \leq F^n$ és K altér, akkor K -t lineáris kódnak nevezzük.

Legyen $k = \dim(K)$, d a kód távolsága, a test elemeinek száma pedig q . Ekkor a kódot $[n, k, d]_q$ kódnak nevezzük.

184. Definiáld a kódszó súlyát!

Egy $u \in A^n$ szó súlya: $w(u) = d(u, (0, 0, \dots, 0))$ ami nem más, mint a nem-nulla koordináták száma.

Megjegyzés: $d(x)$ az x kód távolságát jelöli.

185. Definiáld a kód súlyát!

Egy k kód súlya $w(k) = \min(d(u)), 0 \neq u \in k$

Megjegyzés: $d(x)$ az x kód távolságát jelöli.

186. Definiáld a generátormátrix fogalmát!

Legyen $G: F_q^k \rightarrow F_q^n$ lineáris leképezés, $G \in F_q^{n \times k}$.

Ekkor $K = \text{Im}(G)$ esetén a G a K kód generátormátrixa.

187. Definiáld az ellenőrző mátrix fogalmát!

Legyen $G \in F_q^{n \times k}$ egy kód generátormátrixa. Egy $H \in F_q^{(n-k) \times n}$ mátrix a kód egy ellenőrző mátrixa, ha $H * v = 0, v$ kódszó ($n - k$ dimenziós nullvektor).

188. Mi a kapcsolat a generátormátrix és ellenőrző mátrix között?

H ellenőrző mátrix $\Leftrightarrow \text{Ker}(H) = \text{Im}(G)$ (Im = képtér, Ker = magtér)

189. Definiáld a szisztematikus kódolás fogalmát!

190. Definiáld az üzenetszegmens fogalmát!

191. Definiáld a paritászegmens fogalmát!

Egy kódolás szisztematikus, ha a kódszó első k karaktere megfelel az eredeti kódolandó szónak. Ekkor az első k karakter az üzenetszegmens, az $n-k$ karakter pedig az úgynevezett paritászegmens.

192. **Mi a kapcsolat a szisztematikus kód generátormátrixa és ellenőrző mátrixa között?**

Legyen $G \in F_q^{n \times k}$ egy szisztematikus kód generátormátrixa $G = \begin{pmatrix} I_k \\ \dots \\ P \end{pmatrix}$.

Ekkor a $H = (-P : I_{n-k})$ egy ellenőrzőmátrix.

193. **Mi a kapcsolat az ellenőrző mátrix és a kód távolsága között?**

Legyen H egy $[n, k, d]_q$ kód ellenőrző mátrixa.

Ha H -nak bármely l oszlopa lineárisan független, akkor $l < d$.

194. Írd le a szindróma dekódolást!

???

195. Adj meg egy bináris Hamming-kódot!

???

Bizonyítások

- Mi a kapcsolat szisztematikus kód generátormátrixa és ellenőrző mátrixa között?

Legyen $G \in F_q^{n \times k}$ egy szisztematikus kód generátormátrixa $G = \begin{pmatrix} I_k \\ \dots \\ P \end{pmatrix}$.

Ekkor a $H = (-P : I_{n-k})$ egy ellenőrzőmátrix.

Bizonyítás:

$$H * G = (-P : I_{n-k}) * \begin{pmatrix} I_k \\ \dots \\ P \end{pmatrix} = -P + P = 0 \in F_q^{(n-k) \times k}.$$

$$(H * G)_{ij} = 0$$

$$H(Gv) = (H * G)v = 0$$

$$K = \text{Im}(G) \subseteq \text{Ker}(H)$$

$$\left. \begin{array}{l} \dim(\text{Im}(G)) = k \\ \dim(\text{Ker}(H)) \leq k \end{array} \right\} \Rightarrow \dim(\text{Im}(G)) = \dim(\text{Ker}(H))$$

- Mi a kapcsolat az ellenőrző mátrix és a kód távolsága között?

Legyen H egy $[n, k, d]_q$ kód ellenőrző mátrixa.

Ha H – nak bármely l oszlopa lineárisan független, akkor $l < d$.

Bizonyítás:

Legyen d a minimális súlyú, nem 0 kódszó súlya. Legyen ez a szó $v = (v_1, v_2, \dots, v_n)^T$.

Ekkor, ha $H = (l_1, l_2, \dots, l_n) (l_i \in F_q^n)$, akkor $0 = H * v = \sum_i v_i \cdot h_i$.

Ha itt a v súlya s , akkor az nem nulla koordinátákhoz tartozó s db oszlop összefüggő.

Megfordítva:

Ha van s db összefüggő vektor, akkor $\sum u_{\phi'} * h_{\phi'} = 0$ ($u_{\phi'} - k$ között s db nem nulla szerepel)

Így kapunk egy s súlyú kódszót $= d(u) = s > d$

Tehát ha találunk l db lineárisan összefüggő oszlopot H – ban és l – nek kevesebb oszlopa

H – nak.

lineárisan független, akkor a kódtávolsága ≥ 2

13. Polinomkódolás

196. Definiáld a ciklikus kód fogalmát!

???

197. Definiáld a polinomkódolás fogalmát!

Lineáris kódnál a k hosszú kódolandó szavak tekinthetők F_q feletti, k -nál alacsonyabb fokú polinomnak is, a betűket nullától indexelve. Ha a kódolást úgy végezzük, hogy ezt a $p(x)$ polinomot beszorozzuk egy rögzített m -ed fokú $g(x)$ polinommal ($m \in \mathbb{N}^+$), akkor lineáris kódot és kódolást kapunk, $n = m + k$ hosszú kódszavakkal, mivel a $p \mapsto pg$ leképezés kölcsönösen egyértelmű. Az ilyen típusú lineáris kódolást polinomkódolásnak nevezzük.

198. Mit mondhatunk a lineáris ciklikus kód és a polinomkódolás kapcsolatáról?

???

199. Milyen kapcsolat van egy $[n, k]$ lineáris ciklikus kód generátorpolinomja és x^n-1 között?

???

Bizonyítások

- Mit mondhatunk a lineáris ciklikus kód és a polinomkódolás kapcsolatáról?

???

- Milyen kapcsolat van egy $[n, k]$ lineáris ciklikus kód generátorpolinoma és x^n-1 között?

???