Diszkrét matek 2 B szakirány beugró kérdések

Készítette: Budai Martin

Források: http://compalg.inf.elte.hu/~vatai/dm2b-pm.html , Járai Antal: Bevezetés a matematikába, saját jegyzet

Gráfok

1. **Definiálja a gráf, csúcsok, élek és illeszkedési leképezés fogalmát.**

   $G=(\varphi,E,V)$ rendezett hármas egy irányítatlan gráf, ahol E az élek halmaza, V a csúcsok halmaza, $\varphi: E \to \mathcal{P}(V)$ illeszkedési leképezés úgy, hogy $\forall e \in E$: $\varphi(e) = \{v_1,v_2\} \subseteq V$.

2. **Definiálja az "illeszkedik", "végpontja" és "izolált csúcs" fogalmakat.**

   Legyen $G=(\varphi,E,V)$ gráf. $\varphi(e) = \{v_1,v_2\}$ esetén az $e \in E$ él illeszkedik a v_1, v_2 csúcsokra, tehát v_1, v_2 végpontjai az e élnek. A $v \in V$ csúcsot izolált csúcsnak nevezzük, ha $\forall e \in E$: $v \notin \varphi(e)$, tehát nincs olyan él, amelynek végpontja a v csúcs.

3. **Definiálja az üres gráf és az illeszkedési reláció fogalmát.**

   Legyen $G=(\varphi,E,V)$ gráf. Ha $E=\emptyset$, akkor G üres gráf. $\varphi: E \to \mathcal{P}(V)$ illeszkedési leképezés úgy, hogy $\forall e \in E$: $\varphi(e) = \{v_1,v_2\} \subseteq V$.

4. **Definiálja csúcsok, illetve élek szomszédosságát.**

   Legyen $G=(\varphi,E,V)$ gráf. $v_1 \neq v_2 \in V$ csúcsok szomszédosak, ha $\exists e \in E$: $\varphi(e)=\{v_1,v_2\}$

5. **Definiálja a hurokél és a párhuzamos élek fogalmát.**

   Legyen $G=(\varphi,E,V)$ gráf. Az $e \in E$ él hurokél, ha $\varphi(e) = \{v\}$, azaz $|\varphi(e)|=1$. Az $e_1 \neq e_2 \in E$ élek párhuzamosak, ha $\varphi(e_1)=\varphi(e_2)$.

6. **Definiálja az egyszerű gráf és a véges gráf fogalmát.**

   Egy gráf egyszerű gráf, ha nem tartalmaz se hurokéleket, se párhuzamos éleket. Egy $G=(\varphi,E,V)$ gráf véges, ha $|E|<\infty$ és $|V|<\infty$.

7. **Definiálja gráfban a fokszám és a reguláris gráf fogalmát.**

Legyen $G=(\varphi,E,V)$ gráf. Ekkor $d(v) = |\{e\in E : v\in\varphi(e)\}| + |\{e\in E : \varphi(e)=\{v\}\}|$ a $v\in V$ csúcs fokszáma. Legyen $n\in\mathbb{N}$, a G gráf n-reguláris, ha $\forall v\in V$: $d(v)=n$. A G gráf reguláris, ha létezik egy olyan $n\in\mathbb{N}$, hogy G n-reguláris.

8. Mit mondhatunk gráfban a fokszámok összegéről?

Egy gráfban a fokszámok összege megegyezik az élek számának kétszeresével.

9. Definiálja gráfok izomorfiáját.

A $G=(\varphi,E,V)$ gráf izomorf a $G'=(\varphi',E',V')$ gráffal, ha létezik $f: E\to E'$ és $g: V\to V'$ bijekció úgy, hogy $\forall e\in E$: $\varphi(e)=\{v_1,v_2\} \Rightarrow \varphi'(f(e)) = \{g(v_1),g(v_2)\}$.

10. Mondjon elégséges feltételt arra, hogy két gráf ne legyen izomorf.

pl. Ha két gráf eltérő számú csúcsokkal rendelkezik, akkor nem lehetnek izomorfak. Ha két gráfban nem ugyanannyi n-ed fokú csúcs van, akkor nem lehetnek izomorfak. stb.

11. Mondjon elégséges feltételt arra, hogy két egyszerű gráf izomorf legyen.

Ha G és G' egyszerű gráfok, és van olyan $g: V\to V'$ bijekció, amely szomszédságtartó, azaz $v,w\in V$ pontosan akkor szomszédosak, ha $g(v)$ és $g(w)$ szomszédosak, akkor G és G' izomorfak.

12. Definiálja a teljes gráf fogalmát.

G egyszerű gráf teljes gráf, ha minden lehetséges éle be van húzva.

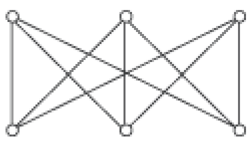
13. Hány éle van egy teljes gráfnak?

$$\binom{n}{2} = \frac{n(n-1)}{2}$$

14. Definiálja a páros gráf fogalmát.

A $G=(\varphi,E,V)$ gráf páros, ha $\exists V',V''\subseteq V$: $V'\cap V'' = \emptyset$ és $V'\cup V'' = V$ és $\forall e\in E$: $\varphi(e) \cap V' \neq\emptyset$ és $\varphi(e) \cap V'' \neq\emptyset$.

15. Adja meg a "három ház, három kút" gráfot.



16. Definiálja a részgráf és a feszített részgráf fogalmát.

G' részgráfja G-nek, ha G' gráf, és $E' \subseteq E$, $V' \subseteq V$ és $\varphi' \subseteq \varphi$. G' feszített részgráfja G-nek, ha $E' = \{e \in E \mid \varphi(e) \subset V'\}$

17. Definiálja részgráf komplementerét.

Legyen G' részgráfja G-nek. G'-nek a G-re vonatkozó komplementere: $\bar{G} = (\varphi_{|E \setminus E'}, E \setminus E', V)$.

18. Definiálja az élhalmaz illetve csúcshalmaz törlésével kapott gráfot.

Az $E' \subseteq E$ élhalmaz törlésével kapott gráf: $(\varphi_{|E \setminus E'}, E \setminus E', V)$.
A $V' \subseteq V$ csúcshalmaz törlésével kapott gráf: $(\varphi_{|E \setminus E'}, E \setminus E', V \setminus V')$,
ahol $E' = \{e \in E : \varphi(e) \cap V' \neq \emptyset\}$.

19. Definiálja a séta és a séta hossza fogalmát.

Legyen $G = (\varphi, E, V)$ gráf, $n \in \mathbb{N}$, n hosszú séta v-ből v'-be ($v, v' \in V$):
$v = v_0, e_1, v_1, e_2, v_2, \ldots, e_{n-1}, v_{n-1}, e_n, v_n = v'$ sorozat úgy, hogy
$\forall 1 \leq i \leq n$: $\varphi(e_i) = \{v_{i-1}, v_i\}$ ($v_i \in V$, $e_i \in E$).

20. Definiálja a nyílt és a zárt sétát.

Ha $v \neq v'$, akkor a séta nyílt, ha $v = v'$, akkor a séta zárt.

21. Definiálja az út fogalmát.

Az n hosszú út egy olyan n hosszú vonal (vagy séta), amelynek minden csúcsa különbözik.

22. Mikor lesz egy nulla illetve egy hosszú séta út?

A nulla hosszú séta egy izolált csúcs, mely megegyezik a nulla hosszú úttal.
Az egy hosszú séta út, ha két csúcsból áll (tehát nem egy hurokélből).

23. Definiálja a vonal fogalmát.

Az n hosszú vonal egy olyan séta, amelyben minden él különbözik.

24. Definiálja a kör fogalmát.

Az n hosszú kör egy legalább 1 hosszú zárt vonal, ahol csak az első és az utolsó csúcs egyezik meg.

25. Van-e egy illetve kettő hosszú kör?

Igen, az egy hosszú kör egy csúcsból és egy hurokélből áll, a kettő hosszú kör pedig két csúcsból, és a köztük lévő két párhuzamos élből áll.

26. Hogyan kaphatunk sétából utat? Fogalmazza meg az állítást.

Ha $G=(\varphi,E,V)$-ben van séta v-ből v'-be ($v\neq v'\in V$), akkor e_i,v_i ($e_i\in E$, $v_i\in V$) párok törlésével utat kapunk v-ből v'-be.

27. Fogalmazza meg a séták körök segítségével való előállítására vonatkozó állítást.

Bármely, legalább 1 hosszú zárt vonal páronként éldiszjunkt körök egyesítése.

28. Definiálja az összefüggőség és a komponens fogalmát.

Legyen $\sim\subseteq V\times V$ reláció úgy, hogy $v\sim v'$ $\Leftrightarrow$létezik séta v-ből v'-be. Ekkor $\sim$ ekvivalencia-reláció, tehát egy osztályzása V-nek. Egy V_i osztály által feszített részgráf az eredeti gráf egy komponense. Egy gráf akkor összefüggő, ha 1 komponensből áll.

29. Igaz-e, hogy egy gráf minden éle valamely komponenshez tartozik?

Igen, a gráf minden éle csak azonos komponensbe tartozó csúcsokat köt össze. Ellenkező esetben létezne séta két különböző komponensbe tartozó csúcs között, ami ellent mond az osztályozásnak.

30. Mi a kapcsolat a komponensek és az összefüggőség között?

Egy gráf akkor összefüggő, ha 1 komponensből áll.

31. Definiálja a fa fogalmát.

A G gráf fa, ha körmentes és összefüggő.

32. Fogalmazzon meg két szükséges és elégséges feltételt arra, hogy egy egyszerű gráf fa legyen.

A következő állítások ekvivalensek egymással:

- G fa
- G összefüggő, de egy él törlése után már nem
- ha v és v' a G gráf különböző csúcsai, akkor pontosan egy út létezik v-ből v'-be
- G körmentes, de 1 él hozzáadása után már nem

33. Egy véges gráfban nincs kör, de van él. Mit állíthatunk fokszámokkal kapcsolatban?

Ekkor kell lennie két olyan csúcsnak, melyeknek fokszáma 1.

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

A következő állítások ekvivalensek egymással:

- G n csúcsú fa
- G-ben nincs kör, és n-1 éle van
- G összefüggő, és n-1 éle van.

35. Definiálja a feszítőfa fogalmát.

Az F gráf feszítőfája a G összefüggő gráfnak, ha F fa, és F csúcsainak a halmaza megegyezik G csúcsainak a halmazával.

36. Mit állíthatunk feszítőfa létezéséről?

Ha G összefüggő, akkor G-nek létezik feszítőfája (valamint, ha G-nek létezik feszítőfája, akkor G összefüggő).

37. Mit állíthatunk véges összefüggő gráfban a körök számáról?

Ha G=(φ,E,V) véges összefüggő gráf, akkor G-ben van legalább |E| - |V|+1 kör, különböző élhalmazokkal.

38. Mikor mondjuk, hogy egy csúcshalmaz illetve élhalmaz elvág két csúcsot?

Legyen G=(φ,E,V) gráf. A V'⊆V csúcshalmaz elvágja a v',v''∈V csúcsokat, ha minden v'-ből v''-be vezető úthoz létezik egy olyan v∈V' csúcs, amely eleme az útnak.

Az E'⊆E élhalmaz elvágja a v',v''∈V csúcsokat, ha minden v'-ből v''-be vezető úthoz létezik egy olyan e∈E él, amely eleme az útnak.

39. Definiálja az elvágó élhalmaz és a vágás fogalmát.

Legyen G=(φ,E,V) gráf. Ha létezik v',v''∈V, hogy E'⊆E elvágja őket, akkor E' elvágóhalmaz. Ekkor, ha G összefüggő volt, akkor az E' éleinek törlése után már nem lesz az. Ha E'-nek nincs szűkebb elvágó-részhalmaza, akkor E' vágás.

40. Mit állíthatunk véges összefüggő gráfban a vágások számáról?

Legyen G=(φ,E,V) véges összefüggő gráf. Ekkor létezik legalább |V| - 1 vágás G-ben (ez a szám megegyezik a feszítőfa éleinek számával).

41. Definiálja az erdő fogalmát. Mi az összefüggés a fákkal?

Az erdő egy körmentes gráf, melynek komponensei fák.

42. Definiálja a feszítő erdő fogalmát. Hány éle van egy véges gráf feszítő erdőjének?

A feszítőerdő egy erdő, melynek csúcshalmaza megegyezik a gráf csúcshalmazával. Éleinek száma egyenlő a csúcsok számának és a komponensek számának különbségével.

43. Definiálja az Euler-vonal fogalmát.

Az Euler-vonal egy olyan vonal, amely a gráf összes élét pontosan egyszer tartalmazza. Ha a vonal kezdőcsúcsa megegyezik a végcsúccsal, akkor zárt Euler-vonalról, ha a két csúcs különbözik, akkor pedig nyílt Euler-vonalról beszélünk.

44. Fogalmazza meg a véges összefüggő gráfok vonalak egyesítéseként való előállítására vonatkozó tételt.

Ha véges összefüggő gráf 2s páratlan fokú csúcsot tartalmaz ($s \in \mathbb{N}^+$), akkor a gráf s darab páronként éldiszjunkt nyílt vonal egyesítése.

45. Definiálja a Hamilton-út illetve Hamilton-kör fogalmát.

A Hamilton-út (illetve –kör) egy olyan út (illetve kör), amely a gráf összes csúcsát pontosan egyszer tartalmazza (kör esetében a kezdő és a végcsúcs megyezik).

46. Definiálja a címkézett gráf fogalmát.

A $G=(\varphi,E,V,c_e,C_e,c_v,C_v)$ élcímkézett gráf, ahol c_e: $E \rightarrow C_e$ élcímkézés, c_v: $V \rightarrow C_v$ csúcscímkézés, C_e az élek címkehalmaza, C_v a csúcsok címkehalmaza. Attól függően, hogy a gráf él- vagy csúcscímkézett, c_e és C_e vagy c_v és C_v elhagyható.

47. Definiálja a súlyozott gráf fogalmát és egy véges részhalmaz súlyát.

A $G=(\varphi,E,V,C_e,C_v,w)$ élcímkézett gráf súlyozott gráf, ha C_e vagy C_v a valós számok halmaza. A $w: E\to\mathbb{R}$ vagy $w: V\to\mathbb{R}$ az élek, illetve csúcsok súlyát meghatározó függvény. Az $E'\subseteq E$ részhalmaz súlya: $\sum_{e\in E'} w(e)$.

48. Fogalmazza meg a Kruskal algoritmust és a rá vonatkozó tételt.

A Kruskal algoritmus megadja egy $G=(\varphi,E,V,w)$súlyozott gráf minimális súlyú feszítőerdőjét. Az algoritmus így néz ki:

0. Init: $S:=\emptyset$
1. ha nincs olyan $e\in E$, hogy $S\cup\{e\}$ körmentes marad, az algoritmus leáll
2. ha létezik olyan $e\in E$, hogy $S\cup\{e\}$ körmentes marad, akkor $S:=S\cup\{e\}$, ahol $w(e)$ minimális
3. goto 1

49. Mit értünk mohó algoritmuson? Mondjon példát, amikor egy mohó algoritmus nem ad optimális megoldást.

A mohó algoritmus minden lépésben az adódó lehetőségek közül az adott lépésben legkedvezőbbek egyikét választja ki. A mohó algoritmus nem ad optimális megoldást pl. az utazóügynök problémájára, ahol egy gráfban kell minimális súlyú Hamilton-kört keresnünk.

50. Definiálja az irányított gráf, csúcsok, élek és illeszkedési leképezés fogalmát.

Legyen $G=(\psi,E,V)$ irányított gráf, ahol E az élek halmaza, V a csúcsok halmaza, ψ pedig az illeszkedési függvény, $\psi: E\to V\times V$ úgy, hogy $\forall e\in E$: $\psi(e)=(v_1,v_2)$.

51. Definiálja irányított gráfban a kezdőpont és a végpont fogalmát.

Legyen $G=(\psi,E,V)$ irányított gráf, ahol ψ az illeszkedési függvény, $\psi: E\to V\times V$ úgy, hogy $\forall e\in E$: $\psi(e)=(v_1,v_2)$. Ekkor az e élnek v_1 kezdőpontja, v_2 végpontja.

52. Hogyan kaphatunk irányított gráfból irányítatlan gráfot? Miért használhatjuk irányított gráfokra az irányítatlan gráfokra definiált fogalmakat?

Ha $G=(\psi,E,V)$ irányított gráf és $G'=(\varphi,E,V)$ irányítatlan gráf, ahol $\psi(e)=(v_1,v_2) \Rightarrow \varphi(e) = \{v_1,v_2\}$, akkor G' a G-hez tartozó irányítatlan gráf, illetve G a G' egy irányítása. Ezért használhatjuk az irányítatlan gráfra vonatkozó definíciókat irányított gráfokra is.

53. Definiálja a gráf irányítása illetve megfordítása fogalmát.

Ha $G=(\psi,E,V)$ irányított gráf és $G'=(\varphi,E,V)$ irányítatlan gráf, ahol $\psi(e)=(v_1,v_2) \Rightarrow \varphi(e) = \{v_1,v_2\}$, akkor G' a G-hez tartozó irányítatlan gráf, illetve G a G' egy irányítása.

A $G=(\psi,E,V)$ irányított gráf megfordítása a $G'=(\psi',E,V)$ irányított gráf, ha $\psi(e)=(v,v') \Leftrightarrow \psi'(e) = (v',v)$ $(e\in E,\ v,v'\in V)$.

54. Definiálja a szigorúan párhuzamos élek fogalmát.

Legyen $G=(\psi,E,V)$ irányított gráf. Az $e_1\neq e_2\in E$ élek szigorúan párhuzamosak, ha $\psi(e_1)=\psi(e_2)$.

55. Definiálja az egyszerű gráf és a véges gráf fogalmát irányított gráf esetén.

A $G=(\psi,E,V)$ irányított gráf egyszerű gráf, ha nem tartalmaz párhuzamos és hurok éleket, illetve véges, ha $|E|<\infty$ és $|V|<\infty$.

56. Definiálja csúcs befokát és kifokát.

Legyen $G=(\psi,E,V)$ irányított gráf, $S\subseteq V$.
$E^-(S)=\{e\in E \mid \exists v\in V\setminus S \text{ és } v'\in S \text{ hogy } \psi(e)=(v,v')\}$
$E^+(S)=\{e\in E \mid \exists v'\in V\setminus S \text{ és } v\in S \text{ hogy } \psi(e)=(v,v')\}$

Ekkor $v\in V$ befoka: $d^-(v)=|E^-(\{v\})| + |\{e\in E : \psi(e)=(v,v)\}|$
kifoka: $d^+(v)=|E^+(\{v\})| + |\{e\in E : \psi(e)=(v,v)\}|$

57. Mit mondhatunk irányított gráfokra a fokszámok összegéről?

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

58. Hogyan szemléltethetünk egy relációt irányított gráffal?

Legyen $R\subseteq A\times B$ reláció. Ekkor a relációt szemléltethetjük egy olyan $G=(\psi,V)$ irányított gráffal, melyre $A\cup B = V$, $\psi=R$. Mivel a relációban egy rendezett pár csak egyszer fordulhat elő (halmaz lévén), így az élek halmaza elhagyható.

59. Definiálja irányított gráfok izomorfiáját.

$G=(\psi,E,V)$ irányított gráf izomorf a $G'=(\psi',E',V')$ irányított gráffal, ha léteznek $f: E\to E'$ és $g: V\to V'$ bijekciók úgy, hogy:
$\psi(e)=(v,v') \Leftrightarrow \psi'(f(e))=(g(v),g(v'))$.

60. Definiálja az irányított részgráf és a feszített irányított részgráf fogalmát.

$G'=(\psi',E',V')$ irányított részgráfja $G=(\psi,E,V)$-nek, ha $\psi'\subseteq\psi$, $E'\subseteq E$, $V'\subseteq V$. Ha $E'=\{e\in E : \psi(e)\in V'\times V'\}$, akkor ez a V' által feszített irányított részgráf.

61. Definiálja irányított részgráf komplementerét.

G'-nek a G-re vonatkozó komplementere: $(\psi|_{E\setminus E'}, E\setminus E', V)$.

62. Definiálja az élhalmaz illetve csúcshalmaz törlésével kapott irányított gráfot.

Az $E'\subseteq E$ élhalmaz törlésével kapott gráf: $(\psi|_{E\setminus E'}, E\setminus E', V)$.

A $V'\subseteq V$ csúcshalmaz törlésével kapott gráf: $(\psi|_{E\setminus E'}, E\setminus E', V\setminus V')$,
ahol: $E'=\{e\in E : \psi(e)=(v_1,v_2) \Rightarrow v_1\in V'$ vagy $v_2\in V'\}$.

63. Definiálja az irányított séta és az irányított séta hossza fogalmát.

Az n hosszú irányított séta a $v_0,e_1, \dots ,e_n,v_n$ sorozat, ahol $\psi(e_i)=(v_{i-1},v_i)$ $(1\leq i\leq n, i\in\mathbb{N})$.

64. Definiálja a nyílt és a zárt irányított sétát.

Az n hosszú $v_0,e_1, \dots ,e_n,v_n$ irányított séta nyílt, ha $v_0\neq v_n$, különben zárt.

65. Definiálja az irányított út fogalmát.

Az irányított út egy olyan irányított séta, hogy a csúcsok nem ismétlődnek.

66. Definiálja az irányított kör fogalmát.

Az irányított kör egy olyan legalább 1 hosszú irányított vonal, hogy csak az első és az utolsó csúcs egyezik meg.

67. Definiálja az erős összefüggőség és az erős komponens fogalmát.

$G=(\psi,E,V)$ irányított gráf erősen összefüggő, ha minden $v,v'\in V$-hez létezik irányított út v-ből v'-be.

Legyen $\sim$ reláció úgy, hogy ha létezik irányított út v-ből v'-be, akkor $v\sim v'$. Ekkor $\sim$ ekvivalencia-reláció, tehát V-nek egy osztályozása. A V osztályai által meghatározott telített irányított részgráfok az erős komponensek. (Az erősen összefüggő gráfnak pontosan egy erős komponense van.)

68. Igaz-e, hogy egy irányított gráf minden éle valamely erős komponenshez tartozik?

Nem, mivel az erős összefüggőség függ az élek irányítottságától is, így lehetséges, hogy egy összefüggő irányított gráf nem erősen összefüggő.

69. Mi a kapcsolat az erős komponensek és az erős összefüggőség között?

Az erősen összefüggő gráf pontosan egy erős komponensből áll.

70. Definiálja az irányított fa és gyökere fogalmát.

A $G=(\psi,E,V)$ irányított gráf irányított fa, ha körmentes, illetve létezik egy $r\in V$ csúcsa, melyből az összes $v\in V$ csúcs elérhető egy irányított úttal, befoka 0, és minden más csúcsának befoka 1. Ekkor az r csúcsot a fa gyökerének nevezzük.

71. Definiálja a irányított fa szintjeit.

Az irányított fa minden csúcsához egyértelműen létezik egy irányított út a fa gyökeréből. Ennek az útnak a hossza egyenlő a csúcs szintjével.

72. Definiálja irányított fában a leveleket.

Egy irányított fában azokat a csúcsokat, melyeknek kifoka 0, leveleknek hívjuk.

73. Fogalmazza meg a Dijkstra algoritmust és a rá vonatkozó tételt.

A Dijkstra algoritmus megadja egy adott csúcsból egy adott csúcshalmaz csúcsaihoz vezető minimális súlyú irányított utakat. Az algoritmus csak akkor ad megfelelő eredményt, ha az összes él súlya pozitív. Az algoritmus bemenete: $G=(\psi,E,V,w)$ élsúlyozott irányított gráf, $s\in V$ kiinduló csúcs, $T\subseteq V$ célcsúcsok. A kimenet egy $d: V\to\overline{\mathbb{R}_0^+}=\mathbb{R}_0\cup\{+\infty\}$ függvény, ahol minden $t\in T$-re $d(t)$ egyenlő az s-ből t-be vezető út minimális súlyával. Az algoritmus így néz ki:

0. init: $S:=\emptyset$, $H:=\{s\}$, $d(s):=0$, $\forall v\in V\setminus\{s\}$: $d(v):=+\infty$
   (S: kész csúcsok, H: feldolgozásra váró csúcsok)
1. amíg nem $T\subseteq S$ vagy $H=\emptyset$
   - legyen $t\in H$ úgy, hogy $d(t)=\min\{d(v) : v\in H\}$
   - $H:=H\setminus\{t\}$, $S:=S\cup\{t\}$
   - minden e élre, amelynek egyik végpontja t, másik végpontja $v\in V\setminus S$:
     1. ha $d(t)+w(e)<d(v)$, akkor $d(v):=d(t)+w(e)$
     2. ha $v\notin H$, akkor $H:=H\cup\{v\}$

74. Mikor mondjuk, hogy egy gráf egy $X \subset R^n$ halmazban rajzolható?

Legyen $X \subseteq \mathbb{R}^n$, γ: $[0,1] \to X$ folytonos függvény egy görbe. Ha $x \neq y \in (0,1)$ esetén $\gamma(x) \neq \gamma(y)$, akkor a görbe egyszerű.

Legyen $G=(\psi,E,V)$ irányított gráf, G $X \subseteq \mathbb{R}^n$-be rajzolása az (f,g) pár, ha f: $V \to X$ injektív és $\forall e \in E$: g_e egyszerű görbe, $g_e(0)=f(v_1)$ és $g_e(1)=f(v_2)$, ha $\psi(e)=(v_1,v_2)$, és rng(f), $g_e((0,1))$ páronként diszjunktak.

75. Mit mondhatunk a gráfok R^3-beli rajzolhatóságáról?

Minden egyszerű véges gráf rajzolható $\mathbb{R}^3$-ban.

76. Mi a kapcsolat a síkba és a gömbre rajzolható gráfok között?

Egy gráf síkba rajzolható akkor és csak akkor, ha $X \subseteq \mathbb{R}^3$ gömbfelületre rajzolható.

77. Fogalmazza meg az Euler formulát.

$G=(\psi,E,V)$ egyszerű véges összefüggő síkba rajzolható gráfra teljesül az alábbi összefüggés: $|V|+t = |E|+2$, ahol t a gráf élei által határolt tartományok száma.

78. Definiálja a jól színezés fogalmát.

A G gráf jól színezhető k színnel, ha a csúcsok színezhetők legfeljebb k színnel úgy, hogy a szomszédos csúcsok színei különböznek ($k \in \mathbb{N}$).

79. Definiálja a kromatikus számot.

A G gráf kromatikus száma $c=\min\{k : G \text{ k-színezhető}\}$. Tehát a kromatikus szám megadja, hogy egy gráf legkevesebb hány színnel színezhető.

Csoportok

80. Definiálja egy művelet esetén a homomorfizmus és a homomorf kép fogalmát.

Legyen (G,·), (G',·') két félcsoport. Ekkor a φ: G → G' művelettartó leképezést homomorfizmusnak nevezzük, és φ(G) a G homomorf képe.

81. Definiálja egy művelet esetén a monomorfizmus, az epimorfizmus és az izomorfizmus fogalmát.

Legyen (G,·), (G',·') két félcsoport. Ekkor a φ: G → G' homomorfizmust monomorfizmusnak nevezzük, ha φ injektív, epimorfizmusnak nevezzük, ha φ szürjektív, és izomorfizmusnak nevezzük, ha φ bijektív.

82. Definiálja egy művelet esetén az endomorfizmus és az automorfizmus fogalmát.

Legyen (G,·), (G',·') két félcsoport. Ha G' = G, akkor ha φ: G→G' homomorfizmus, akkor endomorfizmusnak, ha izomorfizmus, akkor automorfizmusnak nevezzük.

83. Mit mondhatunk homomorfizmusnál félcsoport, egységelem, inverz és felcserélhető elemek esetén?

Ha G félcsoport, akkor a homomorf képe is félcsoport. Ha G-ben *e* jobboldali egységelem, baloldali egységelem, vagy egységelem, akkor a homomorf képében *e* szintén jobboldali egységelem, baloldali egységelem, vagy egységelem. Ha G-ben *e* egységelem, és g-nek g* jobboldali inverze, baloldali inverze, illetve inverze, akkor a homomorf képében g* képe a g képének jobboldali inverze, baloldali inverze, illetve inverze. Ha G-ben g és h felcserélhetőek, akkor a homomorf képben g és h képei felcserélhetőek.

84. Mit mondhatunk homomorfizmusnál csoport, kommutatív félcsoport és Abel-csoport esetén?

Csoport homomorf képe is csoport, kommutatív félcsoport homomorf képe is kommutatív félcsoport, illetve Abel-csoport homomorf képe is Abel-csoport.

85. Adjon meg szükséges és elégséges feltételeket arra, hogy egy félcsoport csoport legyen.

Ha G egy félcsoport, akkor az alábbi feltételek ekvivalensek:

- G csoport
- $G \neq \emptyset$, $\forall a,b \in G : \exists!\, x \in G : ax=b$ és $\exists!\, y \in G : ya=b$ (elvégezhető az osztás)
- $G \neq \emptyset$, $\forall a,b \in G : \exists\, x \in G : ax=b$ és $\exists\, y \in G : ya=b$ (a művelet invertálható)

86. Fogalmazza meg csoportban az egyszerűsítési szabályt.

$(G, \cdot)$ csoportban $ac=bc$ vagy $ca=cb \Rightarrow a=b$

87. Adjon példát invertálható műveletre, amellyel nem kapunk csoportot.

$(\mathbb{N}^+, \cdot)$

88. Adja meg a szorzással mint művelettel tekintett egységnyi abszolút érték komplex számok csoportjának három valódi részcsoportját.

Bármely n-edik egységgyökök halmaza a szorzás művelettel ($n \geq 2$).

89. Mit értünk a Klein-féle csoporton? Kommutatív-e?

A Klein-csoportot definiáljuk a szorzótáblájával:

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

A szorzótábla szimmetrikus, tehát a művelet kommutatív.

90. Mit értünk diédercsoporton?

A szabályos *n* oldalú sokszögek önmagába vivő egybevágóságainak (távolságtartó leképezéseinek) csoportját.

91. Definiálja a részcsoport, triviális részcsoport és valódi részcsoport fogalmát.

Legyen $(G,\cdot)$ csoport, $H \subseteq G$, ekkor H részcsoport, ha a $H \times H$-ra leszűkített művelettel részcsoportot alkot. A legtágabb részcsoport $H=G$, a legszűkebb részcsoport $H=\{e\}$ (ahol e az egységelem), ezek a triviális részcsoportok. A H valódi részcsoportja G-nek, ha $H \neq G$.

92. Adjon meg szükséges és elégséges feltételeket arra, hogy egy csoport egy részhalmaza részcsoport legyen.

Legyen (G,·) csoport, H⊆G, ekkor az alábbi állítások ekvivalensek:

- H≤G (H részcsoportja G-nek)
- ·: H×H → H és G egységeleme eleme a H halmaznak és H^{-1}⊆ H
- H≠∅ és H·H ⊆ H és H^{-1}⊆ H
- H≠∅ és H^{-1}·H ⊆ H

93.Mit mondhatunk részcsoportok metszetéről és egyesítéséről?

Ha H_γ, γ∈Γ, a G csoport részcsoportainak egy rendszere, akkor $H = \bigcap_{\gamma \in \Gamma} H_\gamma$ is részcsoport. Részcsoportok egyesítése általában nem részcsoport (pl. Klein-csoportban az {e,a} és {e,b} részcsoportok egyesítése nem részcsoport).

94.Definiálja a generátum és a generátorrendszer fogalmát.

Legyen (G,·) csoport, K⊆G. Ekkor $\langle K \rangle = \bigcap\{H \leq G \mid K \subseteq H\}$ generátum, és mivel részcsoportok metszete is részcsoport, $\langle K \rangle \leq G$.

Ha $\langle K \rangle = G$, akkor K a G generátorrendszere.

95.Definiálja a ciklikus csoport és generátora fogalmát.

Ha $G = \langle \{g\} \rangle = \langle g \rangle$ $(g \in G)$, akkor G ciklikus csoport, és g a G generátora.

96.Fogalmazza meg a generátumot leíró állítást.

$$\langle K \rangle = \{g_1 \cdot g_2 \cdot \ldots \cdot g_n \mid n \in \mathbb{N}, g_i \in K \cup K^{-1}, ha\ 1 \leq i \leq n\}$$

Az üres szorzat (n=0 eset) az e egységelem. Az állításból következik, hogy $\langle K \rangle = \langle K^{-1} \rangle$.

97.Mit mondhatunk ciklikus csoport homomorf képéről?

Ha g ∈ G, akkor $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$. Egy ciklikus csoport homomorf képe is ciklikus, és egy generátor képe generálja a homomorf képet.

98.Definiálja csoport és elem rendjét.

Legyen (G,·) csoport. Ekkor a csoport rendje egyenlő a G halmaz elemszámával (|G|), ha az véges. Végtelen halmaz esetén a csoport rendje végtelen. Legyen g ∈ G, a g elem rendje $\sigma(g) = \min\{n \in \mathbb{N}^+ \mid g^n = e\}$, ha létezik ilyen n, különben végtelen.

99.Fogalmazza meg a ciklikus csoportok szerkezetét leíró tételt.

Végtelen ciklikus csoport izomorf az egész számok additív csoportjával ($\mathbb{Z}$,+); n elemű ciklikus csoport izomorf a modulo n maradékosztályok $\mathbb{Z}_n$ additív csoportjával ($\mathbb{Z}_n$,+). Speciálisan a ciklikus csoportok kommutatívak.

100. Mi a kapcsolat elem és részcsoport rendje között?

Véges rendű elem rendje megegyezik az általa generált ciklikus csoport rendjével.

101. Mit mondhatunk ciklikus csoport részcsoportjairól?

Ciklikus részcsoport minden részcsoportja is ciklikus.

102. Mit mondhatunk véges ciklikus csoport részcsoportjai generátorainak számáról?

Legyen G egy n rendű véges ciklikus csoport. Ekkor G-nek $\varphi(n)$ generátora van. (Ahol φ az Euler-függvény, tehát $\varphi(n)$ az n-nél nem nagyobb, n-nel relatív prímek számát adja meg.)

103. Definiálja a bal- és jobboldali mellékosztályokat.

Legyen $(G,\cdot)$ csoport, $H \leq G$, $a,b \in G$. Ekkor:

- $a \sim_{jobb} b \Leftrightarrow ab^{-1} \in H$ jobb oldali mellékosztályok
- $a \sim_{bal} b \Leftrightarrow b^{-1}a \in H$ bal oldali mellékosztályok

mivel a fenti relációk ekvivalenciarelációk.

104. Mi a kapcsolat a bal- és a jobboldali mellékosztályok között?

Létezik $Ha \mapsto (Ha)^{-1} = a^{-1}H$ bijekció jobb- és baloldali mellékosztályok között. A jobb- és baloldali mellékosztályok száma, ha véges, megegyezik.

105. Definiálja részcsoport indexét.

A H részcsoport G-beli indexét $[G : H]$-val jelöljük. Ha véges sok jobb oldali mellékosztály van, akkor azok száma a H indexe, egyébként H indexe végtelen.

106. Fogalmazza meg Lagrange tételét.

Ha H a G véges csoport részcsoportja, akkor H rendjének és indexének szorzata G rendje: $|H|\cdot[G : H] = |G|$.

107. Mi a kapcsolat elem rendje és a csoport rendje között?

Véges csoportban elem rendje osztja a csoport rendjét.

108. Fogalmazzon meg olyan tételt, amely lehetővé teszi, hogy egy csoport rendjéből a ciklikusságára következtessünk.

Ha a csoport rendje prímszám, akkor a csoport ciklikus.

109. Adjon meg szükséges és elégséges feltételt arra, hogy egy csoportnak ne legyen nem triviális részcsoportja.

Egy nem egyelemű csoportnak csak triviális részcsoportjai vannak pontosan akkor, ha prímszámrendű.

110. Definiálja a normálosztó fogalmát.

Legyen $(G,\cdot)$ csoport, $N \leq G$ normálosztó (vagy normális részcsoport, vagy invariáns részcsoport), ha $\forall a \in G$: $aN = Na$. Jelölés: $N \lhd G$

111. Adjon meg három olyan csoportot, amelyben minden részcsoport normálosztó.

Ha G Abel-csoport, akkor minden részcsoportja normálosztó. Pl. $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$

112. Adjon meg szükséges és elégséges feltételeket arra, hogy egy részcsoport normálosztó legyen.

Legyen $(G,\cdot)$ csoport, $N \leq G$. Ekkor a következő állítások ekvivalensek:

- N normálosztó
- $\forall a \in G$: $a^{-1}Na = N$
- $\forall a \in G$: $a^{-1}Na \subset N$

113. Mit mondhatunk normálosztók metszetéről és egyesítéséről?

Normálosztók metszete és egyesítése is normálosztó.

114. Fogalmazza meg kompatibilis osztályozások és a normálosztók közötti kapcsolatot leíró tételt.

Legyen $(G,\cdot)$ csoport. Ekkor:

- egy N normálosztó szerinti mellékosztályok a csoportnak a művelettel kompatibilis osztályozását adják

- egy N normálosztó szerinti mellékosztályok közötti művelet megegyezik az osztályok, mint halmazok komplexusszorzásával
- minden, a művelettel kompatibilis osztályozás esetén az egységelem osztálya normálosztó, és az osztályozás ezen normálosztó szerinti mellékosztályokból áll.

115. Definiálja a faktorcsoport fogalmát és fogalmazza meg a definícióban felhasznált tételt.

$N \lhd G$, N szerinti mellékosztályok a komplexusszorzással csoportot alkotnak, és ezt a csoportot N normálosztó szerinti faktorcsoportnak hívják. Jelölés: G/N

116. Adjon meg három példát faktorcsoportra.

A $\mathbb{Z}_p$ maradékosztályok az összeadással, ahol p prímszám.

117. Fogalmazza meg a homomorfizmus–tételt csoportokra.

Egy G csoport egy φ homomorfizmusánál a homomorfizmus magja normálosztó, és a G/ker(φ) faktorcsoport izomorf φ(G)-vel. A G bármely N normálosztója magja valamely homomorfizmusnak: G-nek G/N-re való kanonikus leképezése homomorfizmus, melynek magja N.

118. Definiálja csoportok direkt szorzatát.

Legyen $(G_i,\times_i)$ csoport ($i\in I$). Ekkor $G =\times_{i\in I} G_i$ a halmazok direktszorzata a $(a\times b)_i := a_i \times_i b_i$ ($a,b\in G$) művelettel a G_i, $i \in I$ család direkt szorzata.

119. Fogalmazza meg a véges Abel–csoportok alaptételét.

Egy véges Abel-csoport véges sok ciklikus csoport direkt szorzatával izomorf. A tényezők választhatók prímhatvány rendűnek. A prímhatvány rendek egyértelműen meghatározottak.

$$|G| = n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

ahol p_i különböző prímek, és $\alpha_i>0$ és $G = G_1\times G_2\times \ldots \times G_r$, $|G_i| = p_i^{\alpha_i}$

Gyűrűk és testek

120. Igaz–e hogy egy egységelemes integritási tartomány akkor és csak akkor test, ha minden nem nulla eleme egység?

Igen, egy egységelemes integritási tartomány pontosan akkor test, ha minden nem nulla eleme egység.

121. Igaz–e hogy egy véges integritási tartomány test?

Igen, mert rögzített nem nulla elemmel végigszorozva a nem nulla elemeket jobbról, illetve balról, mindegyiket megkapjuk, így a nem nulla elemek körében az ax=b és az ya=b egyenletek megoldhatók.

122. Definiálja a Gauss–egészek gyűrűjét. Igaz–e, hogy két egység van?

Gauss-egészek: $\mathbb{Z}[i] = \{a + bi : a,b \in \mathbb{Z}\}$. Nem igaz, mert a Gauss-egészek között 4 egység van: 1,-1,i,-i.

123. Igaz–e, hogy egy adott halmazt egy testbe képző függvények gyűrűje is test?

Nem igaz. Egy X halmazt egy R gyűrűbe képző összes függvények R^X halmaza a pontonkénti összeadással és szorzással együtt gyűrű. Ha R kommutatív, akkor ez a gyűrű is kommutatív, valamint ha R egységelemes, akkor a gyűrű is egységelemes. Viszont ha R és X legalább kételeműek, akkor R^X nem nullosztómentes, tehát nem lehet test. Az állítás akkor sem igaz, ha R test.

124. Definiálja két művelet esetén a homomorfizmus és a homomorf kép fogalmát.

Legyenek $(R,+,\cdot)$ és $(R',+',\cdot')$ gyűrűk, $\varphi: (R,+,\cdot) \mapsto (R',+',\cdot')$ leképezés mindkét műveletre művelettartó. Tehát:
$\varphi(x+y) = \varphi(x) +' \varphi(y)$
$\varphi(x\cdot y) = \varphi(x)\cdot'\varphi(y)$
Ekkor φ gyűrűhomomorfizmus, és $(R,+,\cdot)$-nak $(R',+',\cdot')$ homomorf képe.

125. Definiálja két művelet esetén a monomorfizmus, az epimorfizmus és az izomorfizmus fogalmát.

Legyenek $(R,+,\cdot)$ és $(R',+',\cdot')$ gyűrűk, $\varphi: (R,+,\cdot) \mapsto (R',+',\cdot')$ homomorfizmus. Ha φ injektív, akkor monomorfizmus, ha φ szürjektív, akkor epimorfizmus, ha pedig φ bijektív, akkor izomorfizmus.

126. Definiálja két művelet esetén az endomorfizmus és az automorfizmus fogalmát.

Legyenek (R,+,·) és (R',+',·') gyűrűk, φ: (R,+,·) ↦ (R',+',·') homomorfizmus. Ha R'=R ugyanazokkal a műveletekkel, akkor φ endomorfizmus, ha emellett φ izomorfizmus is, akkor automorfizmus.

127. Mit mondhatunk homomorfizmusnál gyűrű képéről?

Gyűrű homomorf képe is gyűrű.

128. Definiálja gyűrű karakterisztikáját. Milyen állítást használt?

Nullosztómentes (R,+,·) gyűrűben minden nem nulla elem additív rendje egyenlő, és ez vagy p prím, vagy ∞. Ha az additív rend véges p prímszám, akkor a gyűrű karakterisztikája char(R)=p, különben char(R)=0.

129. Fogalmazza meg a gyűrűk karakterisztikájára vonatkozó tételt.

Ha char(R)=n>0 ⇒∀a,b∈R: $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = a^n + b^n$

130. Definiálja a részgyűrű fogalmát.

Legyen (R,+,·) halmaz két művelettel (nem feltétlenül gyűrű!) és S⊆R. S részgyűrű, ha (S,+,·) gyűrű a műveletek S-re való megszorításával. Ha R is gyűrű, akkor S≤R, és ekkor R az S bővítése.

131. Definiálja a jobbideál, balideál és ideál fogalmát.

Legyen (R,+,·) gyűrű, I≤R. Ekkor:

- I jobb ideál, ha ∀r∈R ∀a∈I: ar ∈ I ⇔ Ir ⊆ I
- I bal ideál, ha ∀r∈R ∀a∈I: ra ∈ I ⇔ rI ⊆ I
- I ideál, ha jobb és bal ideál is

132. Definiálja a triviális ideál és a valódi ideál fogalmát.

Legyen (R,+,·) gyűrű. Ekkor R és {0} triviális ideálok. Ha R≠I ideál, akkor I valódi ideál.

133. Definiálja az egyszerű gyűrű fogalmát.

Az egyszerű gyűrű csak triviális ideálokat tartalmaz.

134. Definiálja a generált ideál és a főideál fogalmát.

Legyen $(R,+,\cdot)$ gyűrű, $A \subseteq R$. Az A által generált ideál:
$(A) = \bigcap\{I \subseteq R : I \text{ ideál és } A \subseteq I\}$.

Ha $|A|=1$, akkor (A) főideál.

135. Mondjon négy példát R^R részgyűrűjére.

A valós változós valós értékű függvények $\mathbb{R}^{\mathbb{R}}$ gyűrűjében részgyűrűt alkotnak például a korlátos függvények, a folytonos függvények, a korlátos folytonos függvények, a polinom-függvények, stb.

136. Mondjon példát Z-ben ideálra. Főideál–e?

$\mathbb{Z}$-ben ideált alkotnak például egy $m \in \mathbb{Z}$ szám többszörösei. Ez főideált alkot, melyet m (vagy –m) generál.

137. Definiálja gyűrűben a mellékosztályokat.

Legyen $(R,+,\cdot)$ gyűrű, I additív részcsoportja R-nek, $\sim$ ekvivalencia-reláció úgy, hogy $\forall a,b \in R$: $a \sim b \Leftrightarrow a-b \in I$. A $\sim$ által létrehozott ekvivalencia-osztályok a mellékosztályok: $\{I + a : a \in R\}$.

138. Fogalmazza meg kompatibilis osztályozások és az ideálok közötti kapcsolatot leíró tételt.

Egy R gyűrű egy I ideál szerinti mellékosztályai a gyűrűnek mindkét műveletével kompatibilis osztályozását alkotják. Minden, mindkét művelettel kompatibilis osztályozás esetén a nulla osztálya ideál, és az osztályozás ezen ideál szerinti mellékosztályokból áll.

139. Definiálja a faktorgyűrű fogalmát és fogalmazza meg a definícióban felhasznált tételt.

Egy R gyűrűnek egy I ideál szerinti mellékosztályai az összeadásra és a szorzásra nézve gyűrűt alkotnak. Ezt a gyűrűt az R gyűrű I ideál szerinti maradékosztály-gyűrűjének (vagy faktorgyűrűjének, illetve hányadosgyűrűjének) nevezzük, és R/I-vel jelöljük.

140. Fogalmazza meg a homomorfizmus–tételt gyűrűkre.

Egy R gyűrű egy φ homomorfizmusánál a homomorfizmus magja ideál. Ha R képe R’, akkor az R/ker(φ) maradékosztály-gyűrű izomorf R’-vel. Az R bármely I ideálja magja valamely homomorfizmusnak, például R kanonikus leképezése R/I-re homomorfizmus, melynek magja I.

141. Adjon példát Z faktorgyűrűjére.

Legyen R=ℤ és m∈ℤ. Ekkor egy egész számhoz a modulo m vett maradékosztályát rendelő leképezés homomorfizmus, amelynek magja I=mℤ, képe pedig R/I = $\mathbb{Z}_m$.

142. Fogalmazza meg egy kommutatív egységelemes gyűrűben a főideálokat leíró állítást.

Egy R kommutatív egységelemes gyűrűben az a∈R elem által generált főideálra: (a) = aR. Speciálisan a nulla által generált főideál: {0}, az egységelem által generált főideál: R.

143. Fogalmazza meg egy egységelemes integritási tartományban az oszthatóság és a generált főideálok kapcsolatát leíró állítást.

Egy R egységelemes integritási tartomány minden a,b elemére igazak a következő állítások:

- (a) ⊂ (b) ⇔ b|a
- (a) = (b) ⇔ a és b asszociáltak
- (a) = R ⇔ a egység

144. Definiálja a Gauss–gyűrű fogalmát.

Az R egységelemes integritási tartomány Gauss-gyűrű (vagy egyértelmű faktorizációs tartomány), ha minden a∈R, a≠0, a≠ε (egység) sorrendtől és asszociáltságtól eltekintve felírható irreducibilis elemek szorzataként.

145. Gauss–gyűrűben hogyan olvashatók le a faktorizációból az osztók?

Gauss-gyűrűben kiolvashatók az elemek osztói a következő módon: $a = \varepsilon\, p_1^{\alpha_1}\, p_2^{\alpha_2} \dots\, p_k^{\alpha_k}$, ahol ε egység, p_i páronként különböző irreducibilis elemek, $\alpha_i \in \mathbb{N}^+$.

146. Igaz–e hogy Gauss–gyűrűben létezik legnagyobb közös osztó és legkisebb közös többszörös?

Igen, mivel az $a = \varepsilon\, p_1^{\alpha_1}\, p_2^{\alpha_2} \dots\, p_k^{\alpha_k}$ felírásból leolvashatók a osztói is: d|a ⇔ $d = \varepsilon'\, p_1^{ß_1}\, p_2^{ß_2} \dots\, p_k^{ß_k}$ (ahol $ß_i \in \mathbb{N}$, $ß_i \le \alpha_i$, ε' egység). Így kiolvasható a legnagyobb közös osztó és a legkisebb közös többszörös is.

147. Igaz–e hogy Gauss–gyűrűben minden irreducibilis elem prím?

Igen, Gauss-gyűrűben p akkor és csak akkor prím, ha p irreducibilis.

148. Definiálja az euklideszi gyűrű fogalmát.

Az R egységelemes integritási tartomány euklideszi gyűrű, ha létezik egy $\varphi: R\setminus\{0\}\to\mathbb{N}$ függvény, hogy:

- $\forall 0\neq a,b\in R\ \exists q,r\in R$: $r=0$ vagy ($r\neq 0$ és $\varphi(r) < \varphi(b)$ és $a=qb+r$)
- $\forall 0\neq a,b\in R$: $\max\{\varphi(a),\varphi(b)\} \leq \varphi(ab)$

(megjegyzés: tehát működik a bővített euklideszi algoritmus)

149. Fogalmazza meg az euklideszi gyűrűben az egységeket és az asszociáltakat leíró tételt.

R euklideszi gyűrű esetén:

- ε egység $\Leftrightarrow$ $\varphi(\varepsilon)=\min\{\varphi(x) : x\in R\setminus\{0\}\}$
- $a,b\in R$ és $b|a \Rightarrow$
  - $\varphi(b) \leq \varphi(a)$
  - $\varphi(b) = \varphi(a) \Leftrightarrow$ a és b asszociáltak

150. Fogalmazza meg a bővített euklideszi algoritmust euklideszi gyűrűben.

Ha $(R,+,\cdot)$ euklideszi gyűrű, akkor R-ben működik az euklideszi algoritmus.
$\forall a,b\in R\ \exists d=\mathrm{lnko}(a,b) = (a,b)$ és $\exists x,y\in R$: $d=ax+by$
Az algoritmus:

0. init: $x_0:=e$, $y_0:=0$, $r_0:=a$, $n:=0$, $x_1:=0$, $y_1:=e$, $r_1:=b$
1. vége? Ha $r_{n+1}= 0$ akkor $d:=r_n$, $x:=x_n$, $y:=y_n$
2. ciklus:
   $r_n:= q_{n+1} \cdot r_{n+1} + r_{n+2}$
   $x_{n+2}:= x_n - q_{n+1} \cdot x_{n+1}$
   $y_{n+2}:= y_n - q_{n+1} \cdot y_{n+1}$
   $n:=n+1$
   goto 1

Mivel $r_2=0$ vagy $\varphi(r_{n+2}) < \varphi(r_{n+1})$, azaz $\varphi(r_n)$ szigorúan monoton csökken és $\varphi: R\to\mathbb{N}$, ezért az algoritmus terminál.
Az algoritmus invariánsa: $ax_n + by_n = r_n$

151. Mi a kapcsolat euklideszi gyűrűben a prímelemek és az irreducibilis elemek között?

Egy euklideszi gyűrű egy eleme pontosan akkor irreducibilis, ha prímelem.

152. Fogalmazza meg euklideszi gyűrűben a faktorizációra vonatkozó tételt.

Euklideszi gyűrű minden nem nulla és nem egység eleme sorrendtől és asszociáltságtól eltekintve egyértelműen felírható felbonthatatlan elemek szorzataként, azaz az euklideszi gyűrű egyben Gauss-gyűrű is.

153. Definiálja a hányadostest fogalmát. Milyen állítást használt?

Legyen R integritási tartomány, és legyen az R×R\{0} halmazon ~ reláció úgy, hogy (a,b)~(a',b') ⇔ ab' = a'b.

Legyen + olyan, hogy (a,b)+(a',b') = (ab'+a'b, bb').
Legyen · olyan, hogy (a,b) · (a',b') = (aa', bb').

Az így definiált + és · műveletek kompatibilisek a ~ szerinti osztályzással, és (R×R\{0}, +, ·) testet alkot, és ez R hányados teste.

154. Hogyan ágyazható be egy integritási tartomány a hányadostestébe?

R integritási tartomány beágyazható a hányadostestébe egy φ: x→(bx,b) (b≠0, x∈R) monomorfizmussal.

Polinomok

155. Definiálja az egyhatározatlanú polinom fogalmát.

Legyen R gyűrű. Az egyhatározatlanú polinomok $\sum_{i=0}^{n} f_i x^i$ alakú véges összegek, ahol x a „határozatlan", n∈ℕ, f_i∈ℝ, ha 0≤i≤n, az összeadás és a szorzás pedig tagonként történik.

156. Definiálja egyhatározatlanú polinomok összeadását és szorzását.

Ha f=(f_0, f_1, …) és g=(g_0,g_1,…) is R gyűrűbeli végtelen sorozatok, azaz $R^{\mathbb{N}}$ elemei, akkor definiáljuk összegüket az f + g =(f_0+g_0, f_1+g_1, …) sorozatként, szorzatukat pedig azon h=(h_0,h_1,…) sorozatként, amelyre:

$$h_k = \sum_{i=0}^{k} f_i g_{k-i} = \sum_{j=0}^{k} f_{k-j} g_j = \sum_{i+j=k} f_i g_j$$

157. Hogyan azonosíthatjuk a gyűrű elemeit bizonyos polinomokkal? Hogy hívjuk ezeket a polinomokat?

Az $a \mapsto (a, 0, 0, \ldots)$ leképezés R gyűrűnek a polinomok gyűrűjébe való monomorfizmusa, értékkészletének elemei a konstans polinomok, ezeket R elmeivel azonosítjuk.

158. Definiálja polinom együtthatóit, főegyütthatóját és fokszámát.

Legyen $f=f_0 + f_1x + f_2x^2 + \ldots + f_nx^n$ $(n\neq 0)$ polinom. Ekkor $f_n=LC(f)$ az f polinom főegyütthatója, az f_i $(0\leq i<n)$ az f polinom együtthatói, és $\delta(f)=n$ az f polinom foka. Speciális esetben, ha $f=0$, akkor $\delta(0)=-\infty$.

159. Definiálja a lineáris polinomokat.

A legfeljebb elsőfokú polinomokat lineáris polinomoknak nevezzük.

160. Definiálja a monom fogalmát egy határozatlan esetén.

Azokat a polinomokat, amelyek f_ix^i alakba írhatók, monomoknak nevezzük.

161. Definiálja a főpolinom fogalmát.

Ha egy polinom főegyütthatója az R gyűrű egységeleme, akkor főpolinomnak (vagy normális polinomnak) nevezzük.

162. Mit mondhatunk polinomok szorzatának főegyütthatójáról?

Ha az R gyűrű nullosztómentes, akkor két nem nulla polinom szorzatának a főegyütthatója a főegyütthatók szorzata.

163. Mit mondhatunk polinomok szorzatának fokáról?

Ha az R gyűrű nullosztómentes, akkor két nem nulla polinom szorzatának a foka a fokok összege.

164. Definiálja polinom helyettesítési értékét és gyökét.

Egy $f = f_0 + f_1x + f_2x^2 + \ldots + f_nx^n$ polinomnak az $r\in R$ helyen vett helyettesítési értékén az $f(r) = f_0 + f_1r + f_2r^2 + \ldots + f_nr^n \in R$ elemet értjük. Ha az f helyettesítési rétéke az r helyen nulla, akkor r az f gyöke.

165. Definiálja a polinomhoz tartozó polinomfüggvényt. Tartozhat–e különböző polinomokhoz ugyanaz a polinomfüggvény?

Az $r \mapsto f(r)$ leképezést az f polinomhoz tartozó polinomfüggvénynek nevezzük. Előfordulhat, hogy két különböző függvényhez ugyanaz a polinomfüggvény tartozik.

166. Fogalmazza meg a maradékos osztás tételét polinomokra.

Legyen R egységelemes integritási tartomány, $f,g \in R[x]$, $g \neq 0$, $LC(g)=\varepsilon$ (egység R-ben). Ekkor $\exists!\ q,r \in R[x] : f = q \cdot g + r$ és $\delta(r) < \delta(g)$.

167. Fogalmazza meg a gyöktényező leválasztására vonatkozó állítást.

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

168. Legfeljebb hány gyöke van egy polinomnak? Fogalmazza meg az állítást.

Ha $f \neq 0$ polinom, akkor f-nek legfeljebb $\delta(f)$ gyöke van.

169. Milyen esetben kölcsönösen egyértelmű a megfeleltetés a polinomok és a polinomfüggvények között? Fogalmazza meg az állítást.

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

170. Milyen esetben alkotnak a polinomok euklideszi gyűrűt? Fogalmazza meg az állítást.

Ha R test, akkor $0 \neq f \mapsto \delta(f)$ függvénnyel R[x] euklideszi gyűrű.

171. Ismertesse a Horner–elrendezést.

A maradékos osztás tételét alkalmazva az f és a $g=x-c$ polinomra azt kapjuk, hogy $f = (x-c)q + r$, ahol r konstans, értéke $f(c)$. Így $n-1$ szorzással és ugyanannyi összeadással megkaphatjuk $f(c)$-t.

172. Mondjon példát, amikor egy adott másodfokú polinomnak nulla, egy illetve két gyöke van.

Például az $1+x^2$ polinomnak $\mathbb{Z}$, $\mathbb{R}$, vagy $\mathbb{Q}$ felett nincs gyöke, $\mathbb{Z}_2$-ben egy gyöke van: 1, $\mathbb{C}$ felett pedig két gyöke van: i és –i.

173. Definiálja polinom algebrai deriváltját.

Legyen R gyűrű. Az $f = (f_0, f_1, f_2, \ldots, f_n, 0, 0, \ldots) \in R[x]$ polinom algebrai deriváltja: $f' = (f_1, 2f_2, 3f_3, \ldots, nf_n, 0, 0, \ldots) \in R[x]$.

174. Milyen négy tulajdonsággal jellemezhető a polinomhoz az algebrai deriváltját rendel leképezés?

Legyen R egységelemes integritási tartomány, $f,g \in R[x]$. Ekkor igazak az alábbi állítások:

- $f = f_0$ konstans $\Rightarrow f' = 0$
- $f = x \Rightarrow f' = e$
- $(f+g)' = f' + g'$
- $(f \cdot g)' = f' \cdot g + f \cdot g'$

175. Az f,g polinomokra $g^n|f$. Mit állíthatunk f'-ről? Fogalmazza meg az állítást.

Legyen R egységelemes integritási tartomány, $f,g \in R[x]$ és $n \in \mathbb{N}^+$. Ekkor, ha $g^n|f$, akkor $g^{n-1}|f'$.

176. Hogyan kaphatunk egy polinomból négyzetmentes polinomot? Fogalmazza meg az állítást.

Ha R test, $f \neq 0$, és d az f és az f' egyik legnagyobb közös osztója, akkor $q=f/d$ négyzetmentes, azaz egyetlen legalább elsőfokú g polinomnak a négyzetével sem osztható.

177. Definiálja polinom többszörös gyökét.

Legyen R egységelemes integritási tartomány, $f \in R[x]$, $f \neq 0$ és $n \in \mathbb{N}^+$. Ekkor azt mondjuk, hogy $c \in R$ az f egy n-szeres gyöke, ha $(x-c)^n|f$, de $(x-c)^{n+1}\nmid f$. Ez azzal ekvivalens, hogy $f=(x-c)^n g$, ahol g-nek c nem gyöke.

178. Mi a kapcsolat a polinom gyökei és a deriváltjának a gyökei között? Fogalmazza meg az állítást.

Legyen R egységelemes integritási tartomány, $f \in R[x]$, $n \in \mathbb{N}^+$ és $c \in R$ az f egy n-szeres gyöke. Ekkor c az f'-nek legalább $(n-1)$-szeres gyöke, és ha $\mathrm{char}(R) \nmid n$, akkor pontosan $(n-1)$-szeres gyöke.

179. Lehet–e egy polinom n-szeres gyöke a deriváltnak is legalább n-szeres gyöke?

Igen, a polinom n-szeres gyöke lehet a deriváltnak több, mint $(n-1)$-szeres gyöke.

Legyen p prím, $a \in \mathbb{Z}_p$, $n \in \mathbb{N}$, $p \nmid n$. Ekkor az $f=(x-a)^p((x-a)^n + 1) \in \mathbb{Z}_p[x]$-nek az a egy p-szeres gyöke, míg f'-nek $(p+n-1)$-szeres gyöke.

180. Írja le az egységeket test feletti polinomok körében.

Az egységek a nem nulla konstans polinomok.

181. Hogyan kaphatunk véges testeket?

$\mathbb{F}_q$ a q elemű véges test: $\mathbb{F}_q = \mathbb{Z}_p[x] \,/\, (f)$ ahol:

- $q = p^n$
- p prím
- $f \in \mathbb{Z}_p[x]$ irreducibilis polinom, minden együtthatója mod p
- $LC(f)=1$ és $\delta(f) = n$

182. Fogalmazza meg a véges testek elemszámát leíró tételt.

Minden q prímhatványhoz létezik $\mathbb{F}_q$ q elemű véges test. q prímhatvány ekvivalens azzal, hogy létezik egy olyan $n \in \mathbb{N}$, hogy $q=p^n$, ahol p prím a test karakterisztikája.

183. Fogalmazza meg a véges test nem nulla elemei multiplikatív csoportjának szerkezetét leíró tételt.

Véges test nem nulla elemeinek multiplikatív csoportja ciklikus. Ha a véges testnek q eleme van, akkor bármely c elemére $c^q=c$.

184. Van–e minden prímhatványhoz olyan elemszámú véges test?

Igen. Bármely $q=p^n$ (p prím, $n \in \mathbb{N}^+$) prímhatványra létezik q elemű véges test.

185. Írja le az irreducibilis polinomokat a C feletti polinomok körében.

$\mathbb{C}[x]$-ben az irreducibilis polinomok a lineáris polinomok.

186. Írja le az irreducibilis polinomokat az R feletti polinomok körében.

$\mathbb{R}[x]$-ben az irreducibilis polinomok az olyan másodfokú polinomok, melyeknek nincs valós gyöke, és a lineáris polinomok.

187. Mit tud a Q feletti irreducibilis polinomokról?

Vannak olyan polinomok, melyek $\mathbb{Q}$ felett irreducibilisek, viszont $\mathbb{R}$ felett nem. Minden $n \in \mathbb{N}^+$-ra van olyan n-ed fokú polinom, amely irreducibilis $\mathbb{Q}$ felett.

188. Igaz–e, hogy Z[x] euklideszi gyűrű?

$\mathbb{Z}[x]$ nem euklideszi gyűrű.
Például legyen $f=x$, $g=2$. Ekkor $(f,g)=1$, és nem létezik olyan $u,v \in \mathbb{Z}[x]$, hogy $1=uf+gv$.

189. Igaz–e, hogy Z[x] Gauss–gyűrű?

Igen, $\mathbb{Z}[x]$ Gauss-gyűrű.

190. Fogalmazza meg Gauss tételét egyértelmű faktorizációs tartományokról.

Legyen R egy Gauss-gyűrű, K pedig a hányadosteste. Ekkor:

- ha egy $f \in R[x]$ polinom előállítható két nem konstans g,h polinom szorzataként K[x]-ben, akkor R[x]-ben is előállítható két g^*,h^* polinom szorzataként, amelyekre g és g^*, illetve h és h^* asszociáltak K[x]-ben, azaz egymásnak K-beli konstansszorosai.
- R[x] is Gauss-gyűrű.

191. Ismertesse a Lagrange–interpoláiót.

Ha R egységelemes integritási tartománynak $c_0, c_1, \ldots, c_n$ különböző elemei, $d_0, d_1, \ldots, d_n$ pedig tetszőleges elemei R-nek, akkor legfeljebb egy olyan legfeljebb n-ed fokú f polinom létezik, amelyre $f(c_j)=d_j$ $(0 \leq j \leq n)$.

Ha R test, akkor mindig létezik is ilyen polinom, és az alábbi Lagrange interpolációs eljárással megkapható. 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 $f(x) = \sum_{j=0}^{n} d_j l_j(x)$.

192. Ismertessen egy titokmegosztási eljárást.

A Lagrange interpoláció titokmegosztásra is felhasználható. 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, a t maximális lehetséges T értékénél is nagyobb p prímet és véletlen $a_1, a_2, \ldots, a_{m-1} \in \mathbb{Z}_p$ együtthatókat, majd számítsuk ki a $\mathbb{Z}_p$ feletti $t + a_1x + a_2x^2 + \ldots + a_{m-1}x^{m-1}$ polinom $y_1, y_2, \ldots, y_n$ értékeit az 1, 2, …, n helyeken. Ezen y_j-k a titokrészek.

Bármelyik m titokrészből a polinom megkapható Lagrange-interpolációval, így adódik a konstans tag, azaz a titok, de kevesebb részből nem.

193. Ismertesse a Kronecker–eljárást.

Ha R egy Gauss-gyűrű, amelyben rendelkezésünkre áll egy eljárás, amellyel akármelyik elem osztóit meg tudjuk határozni, valamint vannak eljárások a műveletek elvégzésére, akkor egy $f \in R[x]$ polinomnak meghatározhatjuk az irreducibilis faktorát.

Ha $f=gh$, akkor bármely $c \in R$-re $f(c) = g(c)h(c)$, tehát $g(c)|f(c)$. Legyen K az R hányadosteste. Választva különböző $c_0, c_1, \ldots, c_n \in R$ elemeket, bármely R-beli $d_j|f(c_j)$ $(j=0,1,\ldots,n)$ értékekhez Lagrange-interpolációval meghatározhatjuk azt az egyetlen $g \in K[x]$ polinomot, amelyre $\delta(g) \leq n$ és $g(c_j)=d_j$, azaz $g(c_j)|f(c_j)$ $(j=0,1,\ldots,n)$.

Ha $g \in R[x]$ és osztja f-et, akkor megtaláltuk f egy osztóját, és f helyett a hányadossal folytatjuk.

Ha $n=0$-val indulunk, és egyesével növeljük n-et, akkor csak irreducibilis polinomosztókat fogunk találni. Ha $n \leq \lfloor \delta(f)/2 \rfloor$-ig nem találtunk osztót, akkor f irreducibilis. Az elsőfokú faktorok megadják a K-beli, és ezáltal az R-beli gyököet is.

194. Fogalmazza meg a véges testek alaptételét.

Bármely $q=p^n$ (p prím, $n \in \mathbb{N}^+$) prímhatványra a q elemű véges testek izomorfak.

195. Hogyan kaphatunk véges testeket? Írjon le olyan eljárást, amely minden véges testet megad.

Legyen $\mathbb{F}_q$ egy q elemű véges test. Egy $\mathbb{F}_q$ feletti d-ed fokú irreducibilis polinom akkor és csak akkor osztja $x^{g^n} - x$-et, ha $d|n$.

Kódolás

196. Definiálja a gyakoriság és a relatív gyakoriság fogalmát.

Az összes ténylegesen előforduló különböző üzenet legyen $a_1, a_2, \ldots, a_m$ ($m \in \mathbb{N}^+$). Ha az a_i üzenet k_i-szer fordul elő, akkor gyakorisága k_i, relatív gyakorisága epdig $p_i = k_i/n > 0$.

197. Definiálja egyedi üzenet információtartalmát. Mi a bit?

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

198. Definiálja az eloszlás és az entrópia fogalmát.

Egy m tagú eloszlás egy pozitív valós számokból álló $p_1, p_2, \ldots, p_m$ sorozat, amelyre $\sum_{i=1}^{m} p_i = 1$.

Az eloszlás entrópiája: $H_r(p_1, \ldots, p_m) = -\sum_{i=1}^{m} p_i log_r p_i$.

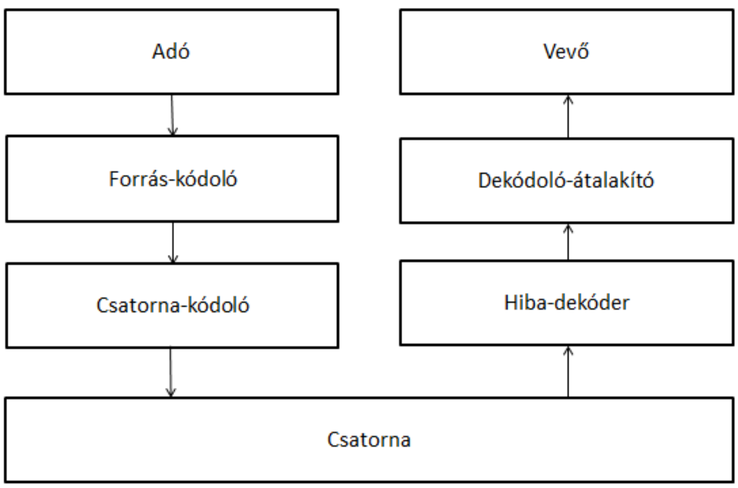
199. Adja meg a pontos felső korlátot eloszlás entrópiájára. Mikor teljesül egyenlőség?

Legyen $p_1, \ldots, p_m$ egy eloszlás. Ekkor $H_r(p_1, \ldots, p_m) \leq \log_r m$. Egyenlőség akkor áll fenn, ha minden i-re $p_i = 1/m$.

200. Mi a forráskódolás? Mik a részei?

Legyen ψ: $A \rightarrow B^*$ kódolás, ahol A az üzenetek halmaza, B a kódoló ábécé, B^* pedig a B-beli véges sorozatok halmaza.

201. Rajzolja fel az üzenetátvitel részletes sémáját.



202. Ismertesse a betűnkénti kódolást.

Legyen ψ: $A^* \rightarrow B^*$ betűnkénti kódolás, φ: $A \rightarrow B^*$ ahol ψ a φ természetes kiterjesztése, azaz $\alpha=(a_1, a_2, \ldots, a_n) \in A^*$ és $\psi(\alpha)=\varphi(a_1)\ \varphi(a_2) \ldots\ \varphi(a_n)$. ψ felbontható, ha ψ és φ is injektív.

203. Definiálja a prefix, infix és szufix fogalmát.

Legyen α, β, γ az A ábécével felírt három szó. Ekkor α prefixe és γ szufixe az $\alpha\gamma$ szónak, β pedig infixe a $\alpha\beta\gamma$ szónak.

204. Ismertesse a kód és a kódfa kapcsolatát.

A betűnkénti kódolás szemléltethető kódfával. Legyen φ: $A \rightarrow B^*$ betűnkénti kódolás. Ekkor az összes, rngφ-ben lévő kódszavak összes prefixének halmaza részbenrendezett a „prefixe" relációra. Ennek a relációnak a Hasse-diagramja (ami egy irányított fa, melynek gyökere az üres szó) a kódolás kódfája.

205. Definiálja a prefix, egyenletes és vesszős kódot. Mi a kapcsolatuk?

Legyen φ: $A \rightarrow B^+$ betűnkénti kód.

- φ prefix kód, ha rngφ prefix mentes, azaz $\alpha,\beta \in$ rngφ és $\alpha \neq \beta$ esetén $\alpha \nleq \beta$.
- φ vesszős kód, ha létezik $\theta \in B^+$, hogy θ szufixe minden kódszónak, viszont egyiknek sem infixe.
- φ egyenletes kód, ha a betűk kódjának hossza azonos.
- Vesszős kód egyben prefix kód is.

206. Adjon példát nem dekódolható kódra.

Legyen $\varphi(a)=10$, $\varphi(b)=1$ és $\varphi(c)=01$.
Ekkor $\psi(ab)=\varphi(a)\varphi(b)=101=\varphi(b)\varphi(c)=\psi(bc)$. Tehát ez a kód nem dekódolható, mivel φ injektív, de ψ nem.

207. Adjon példát fejthető, de nem prefix kódra.

Legyen $\varphi(a)=10$, $\varphi(b)=1$ és $\varphi(c)=00$. Ez a kód egyértelműen megfejthető, de nem prefix kód.

208. Fogalmazza meg a McMillan–egyenlőtlenséget tartalmazó tételt.

Legyen $A=\{a_1, \ldots, a_n\}$ és B két ábécé, B elemeinek száma $r \geq 2$, és $\varphi: A \rightarrow B^+$ injektív leképezés. Ha a φ által meghatározott betűnkénti kódolás felbontható, akkor $l_j=|\varphi(a_j)|$ jelöléssel: $\sum_{j=1}^{n} r^{-l_j} \leq 1$.

Fordítva, ha az $l_1, \ldots, l_n$ olyan pozitív számok, hogy az egyenlőtlenség teljesül, akkor van az A-nak a B elemeivel való olyan felbontható, sőt prefix kódolása, hogy az a_j betű kódjának hossza l_j.

209. Definiálja az átlagos szóhosszúság és az optimális kód fogalmát.

Legyen $A=\{a_1,\ldots,a_n\}$ ábécé, $p_1, \ldots, p_n$ relatív gyakorisággal $\varphi: A \rightarrow B^+$ injektív, és $|B|=r \geq 2$ ($0 \leq p_i \leq 1$, $\sum p_i = 1$), akkor az átlagos szóhossz:

$$\bar{l} = \sum_{i=1}^{n} p_i |\varphi(a_i)|$$

A kód optimális, ha $\bar{l}$ minimális.

210. Van–e mindig optimális kód betűnkénti kódolásnál?

Igen, minden betűnkénti kódhoz megkonstruálható optimális kód.

211. Fogalmazza meg Shannon tételét zajmentes csatornára.

Legyen $p_1, \ldots, p_n$ relatív gyakorisággal $\varphi: A \rightarrow B^+$ betűnkénti kód, és $|B|=r \geq 2$ ($0 \leq p_i \leq 1$, $\sum p_i = 1$). Ekkor $n>1$ esetén van olyan prefix kód, amelyre:
$\bar{l} < H_r(p_1, \ldots, p_n) + 1$.

212. Ismertesse egy optimális kód kódfájának tulajdonságait.

A szokásos jelölésekkel legyen $n>1$. Tekintsünk gy optimális prefix kódot, és legyen a kódszavak hosszának maximuma L. Ekkor:

- ha $p_i > p_j$ akkor $l_i \leq l_j$
- a kódfában csak az (L–1)-edik szinten van csonka csúcs, és még a csonka csúcsokból is legalább 2 él indul ki
- van olyan optimális prefix kód, melynek kódfájában legfeljebb 1 csonka csúcs van
- egy optimális prefix kód kódfájában pontosan akkor nincs csonka csúcs, ha $r \equiv n \ (mod\ r-1)$, azaz:

$$r = 2 + ((n-2) mod\ (r-1))$$

- ha egy csonka csúcs van, akkor annak m kifokára $m \equiv n\ (mod\ r - 1)$, azaz:

$$m = 2 + ((n - 2) mod\ (r - 1))$$

213. Fogalmazza meg azt a három állítást, amelynek alapján optimális kód konstruálható.

- egy optimális prefix kód kódfájában pontosan akkor nincs csonka csúcs, ha $r \equiv n\ (mod\ r - 1)$, azaz:

  $$r = 2 + \big((n - 2) mod\ (r - 1)\big),$$

  ha egy csonka csúcs van, akkor annak m kifokára $m \equiv n\ (mod\ r - 1)$, azaz:

  $$m = 2 + ((n - 2) mod\ (r - 1))$$

- ha $n \leq r$, akkor egybetűs kódszavakat választva optimális prefix kódot kapunk
- legyen $\beta_1, \ldots, \beta_n$ az r-elemű kódábécével megadott, a $p_1, \ldots, p_n$ eloszláshoz tartozó optimális prefix kód, amelynek a kódfájában nincs csonka csúcs. Ha $2 \leq m \leq r$, és valamely $1 \leq k \leq n$-re $p_{n+1}, \ldots, p_{n+m}$ pozitív valós számokra $\sum_{i=1}^{m} p_{n+i} = p_k$, továbbá $\max\{ p_{n+1}, \ldots, p_{n+m} \} \leq \min\{ p_1, \ldots, p_n \}$, akkor $\beta_1, \ldots, \beta_{k-1}, \beta_{k+1}, \ldots, \beta_n, \beta_k b_1, \ldots, \beta_k b_m$, ahol $b_1, \ldots, b_m$ a B különböző elemei, a $p_1, \ldots, p_{k-1}, p_{k+1}, \ldots, p_n, p_{n+1}, \ldots, p_{n+m}$ „finomított” eloszláshoz tartozó optimális prefix kód.

214. Írja le, hogyan konstruálunk Huffman–kódot.

Rendezzük a relatív gyakoriságok csökkenő sorrendjében a betűket, majd osszuk el (n–2)-t (r–1)-gyel, és legyen m a maradék plusz 2.

Helyettesítsük a sorozat m utolsó betűjét egy újabb betűvel, amelyhez az elhagyott betűk relatív gyakoriságainak az összegét rendeljük, és az így kapott gyakoriságoknak megfelelően helyezzük el az új betűt sorozatban.

Ismételjük meg az előző redukciót úgy, hogy minden lépésben r betűvel csökkentjük a kódolandó halmazt, mígnem már csak r betű marad.

Most a redukált ábécé legfeljebb r betűt tartalmaz, és ha volt redukció, akkor pontosan r betűt. Ezeket a kódoló ábécé elemeivel kódoljuk, majd a redukciónak megfelelően visszafelé haladva, az ott összevont betűk kódját az összevonásként kapott betű már meglévő kódjának a kódoló ábécé különböző betűivel való kiegészítését kapjuk.

215. Írja le, mit érhetünk el a kódolandó ábécé kiterjesztésével.

A kódolandó ábécé kiterjesztésével elérhetjük, hogy egy felbontható kódban az egy betűre jutó átlagos szóhosszúság tetszőlegesen megközelítse az entrópia értékét, ami az elméleti alsó határ.

216. Ismertesse a szótárkódok alapgondolatát.

A szótárkódok alapgondolata, hogy egy $\varphi \in A^* \to B^*$ szótárt használunk fel a kódolásra, amelynek értelmezési tartománya tartalmazza A-t, azaz a kódolandó ábécét.

217. Ismertesse a paritásbites kódot.

A paritásbites kód a legegyszerűbb hibajelző kód. Az n-bites bináris jelsorozatokat kiegészítjük egy (n+1)-edik bittel, az ún. paritásbittel. Amennyiben egy üzenetben az 1-esek száma páratlan, akkor a bitsorozat végére egy 0-t, ellenkező esetben egy 1-et írunk. (vagy fordítva, a lényeg, hogy következetes legyen)

218. Definiálja a *t*-hiba jelző és pontosan *t*-hiba jelző kód fogalmát.

Egy kód t-hibajelző, ha minden olyan esetben jelez, amikor egy elküldött kódszó legfeljebb t helyen változik meg.

A kód pontosan t-hibajelző, ha t-hibajelző, de nem (t+1)-hibajelző, azaz van olyan t+1 hiba, amelyet a kód nem jelez.

219. Definiálja kód távolságát és súlyát.

Legyen d: $A^n \times A^n \to \mathbb{N}$ függvény. Ekkor az u,v kódszavak távolsága: $d(u,v)=|\{i : u_i \neq v_i\}|$, ahol $u=(u_1, u_2, \ldots, u_n)$ és $v=(v_1, v_2, \ldots, v_n)$.

A kód távolsága $d(C) = d = \min\{d(u,v) \mid u,v \in C \text{ és } u \neq v\}$.

Legyen (A,+) Abel-csoport, ahol 0 a nullelem. Ekkor az $u=(u_1, u_2, \ldots, u_n) \in A^n$ szó súlya: $w(u) = |\{i : u_i \neq 0\}|$.

A kód súlya $w(c) = w = \min\{w(u) \mid u \in C \text{ és } u \neq \bar{o}\}$

220. Mi a kapcsolat a kód távolsága és hibajelző képessége között?

Legyen d a kód távolsága. Ekkor a kód d–1 hibát jelez.

221. Ismertesse a minimális távolságú dekódolást.

Egy adott szóhoz mindig a legközelebbi kódszót rendeljük. Ha több ilyen is létezik, akkor kiválasztunk közülük egyet, és mindig azt rendeljük hozzá.

222. Definiálja a *t*-hibajavító és pontosan *t*-hibajavító kód fogalmát.

Egy kód t-hibajavító, ha tud javítani minden, legfeljebb t darab hibát. Egy kód pontosan t-hibajavító, ha t-hibajavító, és van t+1 hiba, amit nem tud javítani.

223. Mi a kapcsolat a kód távolsága és hibajavító képessége között?

Legyen d a kód távolsága. Ekkor a kód $\left\lfloor\frac{d-1}{2}\right\rfloor$ hibát javít.

224. Definiálja a lineáris kód fogalmát és a kapcsolódó jelöléseket.

Ha K véges test, akkor a K elemeiből alkotott rendezett n-esek a komponensenkénti összeadással, valamint az n-es minden elemének ugyanazzal az elemmel való szorzásával egy K feletti n-dimenziós K^n lineáris teret alkotnak. Ennek a térnek bármely altere egy lineáris kód.

Ha az altér k-dimenziós, a kód távolsága d és a test elemeinek száma q, akkor az ilyen kódot $[n, k, d]_q$ kódnak nevezzük.

Singleton korlátja $k \leq n-d+1$, kódsebessége k/n.

225. Ismertesse a kétdimenziós paritásellenőrzést.
226. Mi a Hamming–korlát?

Ha egy q elemű ábécé bizonyos n hosszú szavaiból álló C kód t-hibajavító, akkor igaz a következő egyenlőtlenség:

$$|C| \cdot \sum_{j=0}^{t} \binom{n}{j} (q-1)^j \leq q^n = |A^n|$$

227. Mi a Singleton–korlát?

Ha egy q elemű ábácé n hosszú szavaiból álló C kód távolsága d, akkor:

$$d \leq \frac{n+1}{log_q|C|} \Leftrightarrow |C| \leq q^{n-d+1}$$

228. Mi az MDS–kód és miért hívják így?

Az MDS a Maximum Distance Separable rövidítése, mely maximális távolságú szeparábilis kódot jelent. Egy kód MDS kód, ha a C kód q elemű ábécén, n hosszú szavainak távolsága d, és a Singleton-korlát egyenlőtlenségeiben egyenlőség van, tehát:

$$d = \frac{n+1}{log_q|C|}\ \text{és}|C| = q^{n-d+1}$$

229. Definiálja a generátormátrix, ellenőrző mátrix és s szindróma fogalmát.

Egy $C=[n, k, d]_q$ lineáris kód G generátor mátrixa egy olyan $K^{n\times k}$ mátrix, hogy:

- C=Im(G)
- ha az u üzenet kódolása v, akkor: v=Gu
- G oszlopai bázisa C-nek

A H hibaellenőrző mátrix egy $K^{(n-k)\times n}$ mátrix, hogy C=ker(H).

Ha $v \in K^n$, akkor a v-hez tartozó s=Hv vektor, a szindróma pontosan akkor nulla, ha v kódszó, azaz $v \in C$.

230. Ismertesse a szindróma–dekódolást.
231. Ismertesse a Fano–kódot.
232. Ismertesse a polinomkódokat.
233. Ismertesse a CRC-t.

Cyclic Redundancy Check kód. Ciklikus és bináris kód.