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

Egy *irányítatlan gráf* vagy röviden *gráf* alatt egy $G = (\varphi, E, V)$ hármast értünk, ahol V a *csúcsok* vagy *szögpontok* halmaza, E az *élek* halmaza, a φ *illeszkedési leképezés* pedig egy E-t a V-beli elemekből álló rendezetlen párok halmazába képező leképezés.

2. Definiálja az „illeszkedik", „végpontja" és „izolált csúcs" fogalmát!

Ha valamely $e \in E$-re és $v \in V$-re $v \in \varphi(e)$, akkor azt mondjuk, hogy e *illeszkedik* v-re, vagy v *végpontja* e-nek. Azokat a csúcsokat, amelyekre nem illeszkedik él, *izolált csúcsoknak* nevezzük.

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

Ha az E halmaz üres, akkor *üres gráfról* beszélünk.
Az élek és csúcsok közötti illeszkedés egy reláció E és V között, amelyet *illeszkedési relációnak* nevezünk.

4. Definiálja csúcsok, illetve élek szomszédosságát!

Két különböző élt *szomszédosnak* nevezünk, ha van olyan csúcs, amelyre mindkettő illeszkedik. Két különböző csúcsot *szomszédosnak* nevezünk, ha van olyan él, amely mindkettőre illeszkedik.

5. Definiálja a hurokél és a párhuzamos élek fogalmát!

Ha egy él csak egy csúcsra illeszkedik, akkor *hurokélnek* nevezzük. Ha $e_1 \neq e_2$ élek ugyanazokra a csúcsokra illeszkednek, akkor *párhuzamos élekről* vagy *többszörös élekről* beszélünk.

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

Ha egy gráf nem tartalmaz sem hurokélt, sem párhuzamos éleket, akkor *egyszerű gráfnak* nevezzük. Ha E és V véges halmazok, akkor a gráfot *végesnek* nevezzük.

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

Ha egy csúcsra csak véges sok él illeszkedik, akkor a csúcs *fokszámán* a rá illeszkedő élek számát értjük, a csúcsra illeszkedő hurokéleket kétszer számolva. Egy $v \in V$ csúcs fokát rendszerint $\deg(v)$-vel vagy $d(v)$-vel jelöljük.
Ha egy gráfban minden csúcs foka n, akkor n-regulárisnak nevezzük; *reguláris gráf* alatt egy olyan gráfot értünk, amely valamely $n \in \mathbb{N}$-re n-reguláris.

8. Mit mondhatunk gráfban a fokszámok összegéről?

Ha $G = (\varphi, E, V)$ egy véges gráf, akkor nyilván

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

9. Definiálja gráfok izomorfiáját!

A $G = (\varphi, E, V)$ és $G' = (\varphi', E', V')$ gráfok *izomorfak,* ha van olyan E-t E'-re képező kölcsönösen egyértelmű f és V-t V'-re képező kölcsönösen egyértelmű g leképezés, hogy minden $e \in E$-re és

minden $v \in V$-re e pontosan akkor illeszkedik v-re, ha $f(e)$ illeszkedik $g(v)$-re, azaz az (f, g) pár tartja az illeszkedési relációt.

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

Ha két gráfnak nem ugyanannyi csúcsa vagy nem ugyanannyi éle van, vagy az egyiknek van olyan tulajdonsága, ami a másiknak nincs meg, például az egyiknek van izolált csúcsa, a másiknak meg nincs, vagy valamely n-re az egyik gráfban nem ugyanannyi n-ed fokú csúcs van, mint a másikban stb., akkor nyilván nem izomorfak.

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

Ha G és G' egyszerű gráfok, és van olyan, a V-t V'-re képező g kölcsönösen egyértelmű leképezés, amely szomszédságtartó, azaz $v, w \in V$ pontosan akkor szomszédosak, ha $g(v)$ és $g(w)$ szomszédosak, akkor G és G' nyilván izomorfak.

12. Definiálja a teljes gráf fogalmát!

Ha egy egyszerű gráfban bármely két különböző csúcsot él köt össze, akkor a gráfot *teljes gráfnak* nevezzük.

13. Hány éle van a teljes gráfnak?

Az n szögpontú teljes gráfnak $\binom{n}{2} = n(n-1)/2$ éle van.

14. Definiálja gráfok Descartes-szorzatát!

Ha $G_i = (\varphi_i, E_i, V_i)$, $i \in I$ gráfok indexelt családja, akkor a $\times_{i \in I} G_i$ *Descartes-szorzatuk* az a $G = (E, V)$ gráf, amelyben a csúcsok halmaza $\times_{i \in I} V_i$, és két csúcs pontosan akkor van összekötve, ha egy kivételével minden koordinátájuk megegyezik, és ha a j-edik koordináták különböznek, akkor a megfelelő csúcsok össze vannak kötve a G_j gráfban.

15. Mondjon példát gráfok Descartes-szorzatára!

Például, ha H_1-ből (H_n: n-dimenziós hiperkocka) n példány Descartes-szorzatát vesszük, H_n-et kapjuk.

16. Definiálja a páros gráf fogalmát!

Egy *páros gráf* egy olyan gráf, amelynél adott a csúcsok V halmazának egy V', V'' diszjunkt halmazokra való felbontása úgy, hogy minden él egyik végpontja az egyik, másik végpontja a másik halmazba esik.

17. Adja meg a „három ház, három kút" gráfot!

Legismertebb példa a „három ház, három kút" gráf, amelynél V' három házból, V'' három kútból áll, és bármely ház és bármely kút között van egy él, de több él nincs. Azt az egyszerű páros gráfot, amelyben $|V'| = m$, $|V''| = n$, és minden V'-beli csúcs minden V''-beli csúccsal össze van kötve, $K_{m,n}$-nel jelöljük.

18. Definiálja a részgráf és a feszített részgráf fogalmát!

A $G' = (\varphi', E', V')$ gráfot a $G = (\varphi, E, V)$ gráf *részgráfjának* nevezzük, ha $E' \subset E$, $V' \subset V$ és $\varphi' \subset \varphi$.
Ha a G' részgráf mindazokat az éleket tartalmazza, amelyek végpontjai V'-ben vannak, azaz ha G' a legbővebb részgráf V'-beli csúcsokkal, akkor G'-t a V' által meghatározott *feszített részgráfnak* nevezzük.

19. Definiálja részgráf komplementerét!

Ha $G' = (\varphi', E', V')$ részgráfja $G = (\varphi, E, V)$ gráfnak, akkor a G'-nek G-re vonatkozó *komplementerén* a $(\varphi|_{E\setminus E'}, E\setminus E', V)$ gráfot értjük.

20. Definiálja az élhalmaz illetve csúcshalmaz törlésével kapott gráfot!

Ha $G = (\varphi, E, V)$ egy gráf és $E' \subset E$, akkor a G-ből az E' *élhalmaz törlésével kapott gráfon* a $G' = (\varphi|_{E\setminus E'}, E\setminus E', V)$ részgráfot értjük.
Ha $G = (\varphi, E, V)$ egy gráf és $V' \subset V$, akkor legyen E' az összes olyan élek halmaza, amelyek illeszkednek valamely V'-beli csúcsra. A G-ből a V' *csúcshalmaz törlésével kapott gráfon* a $G' = G' = (\varphi|_{E\setminus E'}, E\setminus E', V\setminus V')$ részgráfot értjük.

21. Definiálja a séta és a séta hossza fogalmát!

Legyen $G = (\varphi, E, V)$ egy gráf. Egy G-beli n *hosszú séta* v-ből v'-be egy olyan

$$v_0, e_1, v_1, e_2, v_2, \dots, v_{n-1}, e_n, v_n,$$

véges sorozat, amelyre e_i a v_{i-1} és v_i csúcsokra illeszkedő él, ha $1 \le i \le n$ és $v_0 = v$, $v_n = v'$.

22. Definiálja a nyílt és zárt sétát!

Ha $v = v'$, a sétát *zárt sétának* nevezzük, egyébként *nyílt sétának*.

23. Definiálja az út fogalmát!

Egy sétát *útnak* fogunk nevezni, ha a $v_0, v_1, \dots, v_n$ csúcsok mind különbözőek.

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

A nulla hosszú séták mind utak és egyetlen csúcsból állnak.
Az egy hosszú séták utak, ha a bennük szereplő egyetlen él nem hurokél.

25. Definiálja a vonal fogalmát!

Ha a sétában szereplő élek mind különbözőek, akkor *vonalnak* nevezzük.

26. Definiálja a kör fogalmát!

Egy legalább egy hosszú zárt vonalat *körnek* nevezünk, ha kezdő- és a végpont megegyeznek, de egyébként a vonal pontjai különbözőek.

27. Van-e egy illetve kettő hosszú kör?

Az egy hosszú körök egyetlen hurokélt tartalmaznak.
A kettő hosszú körök két különböző, de párhuzamos élt tartalmaznak.

28. Hogyan kaphatunk sétából utat? Fogalmazza meg az állítást!

Bármely G gráfban a különböző v és v' csúcsokat összekötő sétából alkalmasan törölve e_i, v_i párokat, a v-t v'-vel összekötő utat kaphatunk.

29. Fogalmazza meg a séták körök segítségével való előállítására vonatkoztó állítást!

Bármely G gráfban egy legalább egy hosszúságú zárt vonal véges sok páronként éldiszjunkt kör egyesítése.

30. Definiálja az összefüggőség és a komponens fogalmát!

Egy gráfot *összefüggőnek* nevezünk, ha bármely két csúcsa összeköthető sétával (úttal).
Nyilván egy adott gráf csúcsaira az a reláció, hogy két csúcs összeköthető úttal, ekvivalenciareláció a csúcsok halmazán, így meghatároz egy osztályozást. A csúcsok egy ilyen osztálya által meghatározott telített részgráf a gráf egy *komponense*.

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

Két különböző osztályba tartozó csúcs nem lehet szomszédos, így a gráf minden éle hozzátartozik egy komponenshez.

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

Nyilván egy gráf akkor és csak akkor összefüggő, ha minden csúcsa ugyanabba az osztályba tartozik, azaz ha csak egyetlen komponense van.

33. Definiálja a fa fogalmát!

Egy gráfot *fának* nevezünk, ha összefüggő és nincs köre.

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

Egy G egyszerű gráfra a következő feltételek ekvivalensek:

(1) G fa;
(2) G összefüggő, de bármely él törlésével kapott részgráf már nem összefüggő;
(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 hozzávételével kapott gráf már tartalmaz kört.

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

Ha egy G véges gráfban nincs kör, de van él, akkor van legalább két elsőfokú csúcs.

36. 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!

Egy G 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.

37. Definiálja a feszítőfa fogalmát!

Egy G gráf egy *feszítőfája* egy olyan F részgráfja G-nek, amely fa és a csúcsainak halmaza megegyezik G csúcsainak halmazával.

38. Mit állíthatunk feszítőfa létezéséről?

Minden összefüggő véges gráfnak létezik feszítőfája.

39. Mit állíthatunk véges összefüggő gráfban a körök számáról?

Egy $G = (\varphi, E, V)$ összefüggő véges gráfban létezik legalább $|E| - |V| + 1$ kör, amelyek élhalmaza különböző.

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

Legyen $G = (\varphi, E, V)$ egy gráf. Ha v', v'' csúcsok, $V' \subset V$, és minden v'-ből v''-ve vivő útban szerepel valamely $v \in V'$ csúcs, akkor azt mondjuk, hogy V' *elvágja* a v' és v'' csúcsokat.
Ha $E' \subset E$, és minden v'-ből v''-be vivő útban szerepel valamely $e \in E'$ él, akkor azt mondjuk, hogy E' elvágja a v', v'' csúcsokat.

41. Definiálja az elvágó élhalmaz és a vágás fogalmát!

Ha vannak olyan csúcsok, amelyeket az E' élhalmaz elvág, akkor E'-t *elvágó élhalmaznak* nevezzük.
Ha egy elvágó halmaznak nincs olyan valódi részhalmaza, amely ugyancsak elvágó halmaz, akkor *vágásnak* nevezzük.

42. Mit állíthatunk véges összefüggő gráfban a vágások számáról?

Egy $G = (\varphi, E, V)$ összefüggő véges gráfban létezik legalább $|V| - 1$ különböző vágás.

43. Definiálja az erdő fogalmát! Mi az összefüggés a fákkal?

Körmentes gráfot *erdőnek* nevezünk. Egy erdő komponensei nyilván fák, a fák pedig összefüggő erdők.

44. Definiálja a feszítőerdő fogalmát! Hány éle van egy véges gráf feszítőerdőjének?

Egy gráf olan részgráfját, amely a gráf minden komponenséből egy feszítőfát tartalmaz, a gráf *feszítőerdőjének* nevezünk. Egy véges erdő éleinek száma nyilván a csúcsok számának és a komponensek számának különbsége.

45. Definiálja az Euler-vonal fogalmát!

Olyan zárt vonal, amely egy gráf minden élét tartalmazza.

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

Egy összefüggő véges gráfban pontosan akkor létezik zárt Euler-vonal, ha minden csúcs páros fokú. Ha véges összefüggő gráf $2s$ páratlan fokú csúcsot tartalmaz, ahol $s \in \mathbb{N}^+$, akkor a gráf s darab páronként éldiszjunkt nyílt vonal egyesítése.

47. Definiálja a Hamilton-út illetve Hamilton-kör fogalmát!

Egy v-ből v'-be vezető út, amelyen a gráf minden pontja pontosan egyszer szerepel.
Hamilton-körnek egy olyan kört nevezünk, amelyben a gráf minden csúcsa szerepel.

48. Definiálja a címkézett gráf fogalmát!

Ha adott egy $G = (\varphi, E, V)$ gráf, a C_e és C_v halmazok, az *élcímkék*, illetve *csúcsímkék* halmaza, valamint a $c_e: E \to C_e$ és $c_v: V \to C_v$ leképezések, az *élcímkézés*, illetve *csúcscímkézés*, akkor a $(\varphi, E, V, c_e, C_e, c_v, C_v)$ hetest *címkézett gráfnak* nevezzük.

49. Definiálja a súlyozott gráf fogalmát és egy véges részhalmaz súlyát!

Igen gyakori, hogy a $C_e = \mathbb{R}$, illetve $C_v = \mathbb{R}$, ekkor *élsúlyozásról* és *élsúlyozott gráfról*, illetve *csúcssúlyozásról* és *csúcssúlyozott gráfról* beszélünk, és a jelölésből C_e-t, illetve C_v-t elhagyjuk.
Egy (φ, E, V, w) élsúlyozott gráfban egy $E' \subset E$ véges élhalmaz súlya $\sum_{e \in E'} w(e)$. Hasonlóan egy (φ, E, V, w) csúcssúlyozott gráfban egy $V' \subset V$ véges csúcshalmaz súlya $\sum_{v \in V'} w(v)$.

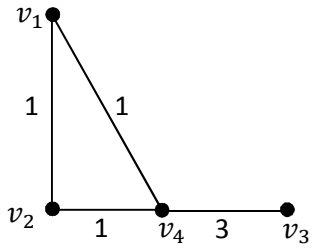
50. Fogalmazza meg a Kruskal-algoritmust és a rá vonatkozó tételt!

Egy w élsúlyozással ellátott véges gráfban az összes csúcsot tartalmazó üres részgráfból indulva, és a már kiválasztott részgráfhoz, amíg lehet, hozzávéve valamely minimális súlyú olyan élt, amellyel a kiválasztott részgráf még nem tartalmaz kört, egy minimális súlyú feszítőerdőt kapunk.

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

Minden lépésben az adódó lehetőségek közül az adott lépésben legkedvezőbbek egyikét választjuk.

Példa nem optimális megoldásra:



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

Egy *irányított gráf* alatt egy $G = (\psi, E, V)$ hármast értünk, ahol V a *csúcsok* vagy *szögpontok* halmaza, E az élek halmaza, a ψ *illeszkedési leképezés* pedig egy E-t $V \times V$-be képező leképezés.

53. Definiálja irányított gráfban a kezdőpont és a végpont fogalmát!

Ha $\psi(e) = (v, v')$, akkor azt mondjuk, hogy v az *e kezdőpontja*, v' pedig a *végpontja*.

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

Bármely $G = (\psi, E, V)$ irányított gráfból kapható $G' = (\varphi, E, V)$ irányítatlan gráf úgy, hogy az irányítást „elfelejtjük”, azaz $\psi(e) = (v, v')$ esetén $\varphi(e)$-t $\{v, v'\}$-nek definiálva.

Fontos, hogy mindazokat a fogalmakat, amelyeket irányítatlan gráfokra definiáltunk – ideértve a címkézést, súlyozást, stb. is – használni fogjuk irányított gráfokra is; ilyenkor mindig a megfelelő irányítatlan gráfra gondolunk.

55. Definiálja a gráf irányítása illetve megfordítása fogalmát!

Azt is mondjuk, hogy G a G' egy *irányítása*. (Eddigi jelölésekkel)
$G = (\psi, E, V)$ irányított gráf *megfordításán* azt a $G' = (\psi', E, V)$ irányított gráfot értjük, amelyre $\psi(e) = (v, v')$ esetén $\psi'(e) = (v', v)$.

56. Definiálja a szigorúan párhuzamos élek fogalmát!

Ha az $e_1 \neq e_2$ éleknek ugyanaz a kezdőpontja és a végpontja, akkor *szigorúan párhuzamos élekről* beszélünk.

57. Definiálja az irányított egyszerű gráf és a véges gráf fogalmát!

Legyen $G = (\psi, E, V)$ irányított gráf. Ha E és V véges halmazok, akkor G *véges irányított gráf*. Ha G-ben nincsenek hurokélek és szigorúan párhuzamos élek, akkor G *egyszerű irányított gráf*.

58. Definiálja csúcs befokát és kifokát!

Ha egy csúcs csak véges sok élnek kezdőpontja, akkor ezek számát a csúcs *kifokának* nevezzük.
Hasonlóan, ha egy csúcs csak véges sok élnek végpontja, akkor ezek számát a csúcs *befokának* nevezzük. Egy $v \in V$ csúcs kifokát rendszerint $deg^+(v)$-vel vagy $d^+(v)$-vel, befokát $deg^-(v)$-vel vagy $d^-(v)$-vel jelöljük.

59. Mit mondhatunk irányított gráfokra a fokszámok összegéről?

Ha $G = (\psi, E, V)$ egy véges irányított gráf, akkor nyilván

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

60. Definiálja az irányított ciklus, csillag és teljes gráf fogalmát!

Egy $\vec{C}_n$ *irányított ciklus* csúcsai egy szabályos n-szög csúcsai, például az n-edik egységgyökök, és irányított él megy minden egységgyökből a következőbe (ciklikusan).
Az $\vec{S}_n$ *irányított csillagban* egy szabályos n-szög csúcsaiból visz irányított él a középpontba, plduál az n-edik egységgyökökből a nullába.
Adott csúcshalmaznál az *irányított teljes gráfban* minden csúcsból minden tőle különböző csúcsba visz irányított él. Az n-csúcsú teljes gráfot $\vec{K}_n$ jelöli.

61. Hogyan szemléltethetünk egy relációt irányított gráffal?

Legyen E egy V-beli binér reláció és $\psi(e) = e$, ha $e \in E$, azaz egy csúcsot egy másikkal pontosan akkor kössünk össze, ha az első relációban áll a másodikkal. Ekkor (ψ, E, V) irányított gráf. Így relációk irányított gráfokkal szemléltethetők.

62. Mit értünk irányított gráf éllistás ábrázolásán?

Legyen (ψ, E, V) egy irányított gráf. A csúcsok beolvasásakor minden csúcsnak adunk egy sorszámot, és egy táblázatban (célszerűen egy hashtáblában) eltároljuk ezt a sorszámozást. Minden csúcshoz felépítjük azon élek listáját, amelyeknek ez a csúcs a kezdőpontja: a ψ leképezés olvasásakor, ha az $(e, (v, v'))$ párt olvassuk, akkor az (n, n') párt hozzáfűzzük az n sorszámú csúcs listájához, ahol n a v, az n' a pedig a v' csúcs sorszáma.

63. Definiálja irányított gráfok izomorfiáját!

A $G = (\psi, E, V)$ és $G' = (\psi', E', V')$ irányított gráfok *izomorfak*, ha van olyan E-t E'-re képező kölcsönösen egyértelmű f és a V-t V'-re képező kölcsönösen egyértelmű g leképezés, hogy minden $e \in E$-re vagy $v \in V$ pontosan akkor kezdőpontja e-nek, ha $g(v)$ kezdőpontja $f(e)$-nek, és pontosan akkor végpontja e-nek, ha $g(v)$ végpontja $f(e)$-nek, azaz (f, g) pár tartja a „kezdőpontja" és a „végpontja" relációkat.

64. Definiálja az irányított részgráf és a feszített irányított részgráf fogalmát!

A $G' = (\psi', E', V')$ irányított gráfot a $G = (\psi, E, V)$ irányított gráf *irányított részfájának* nevezzük, ha $E' \subset E$, $V' \subset V$ és $\psi' \subset \psi$.
Ha a G' irányított részgráf mindazokat az éleket tartalmazza, amelyek kezdőpontjai és végpontjai is V'-ben vannak, akkor G'-t a V' által meghatározott *feszített irányított részgráfnak* nevezzük.

65. Definiálja irányított részgráf komplementerét!

Ha $G' = (\psi', E', V')$ irányított részgráfja a $G = (\psi, E, V)$ irányított gráfnak, akkor a G'-nek a G-re vonatkozó *komplementerén* a $(\psi|_{E \setminus E'}, E \setminus E', V)$ gráfot értjük.

66. Definiálja az élhalmaz illetve csúcshalmaz törlésével kapott irányított gráfot!

Ha $G = (\psi, E, V)$ egy irányított gráf és $E' \subset E$, akkor a G-ből az E' *élhalmaz törlésével kapott irányított gráfon* a $G' = (\psi|_{E \setminus E'}, E \setminus E', V)$ irányított részgráfot értjük.
Ha $G = (\psi, E, V)$ egy irányított gráf és $V' \subset V$, akkor legyen E' az összes olyan élek halmaza, amelyeknek kezdőpontja vagy végpontja valamely V'-beli csúcs. A G-ből a V' *csúcshalmaz törlésével kapott irányított gráfon* a $G' = (\psi|_{E \setminus E'}, E \setminus E', V \setminus V')$ részgráfot értjük.

67. Definiálja az irányított séta és az irányított séta hossza fogalmát!

Legyen $G = (\psi, E, V)$ egy irányított gráf. Egy G-beli n *hosszú irányított séta* v-ből v'-be egy olyan

$$v_0, e_1, v_1, e_2, v_2, \dots, v_{n-1}, e_n, v_n,$$

véges sorozat, amelyre e_i kezdőpontja v_{i-1}, végpontja pedig v_i, ha $1 \leq i \leq n$, és $v_0 = v$, $v_n = v'$.

68. Definiálja a nyílt és zárt irányított sétát!

Ha $v = v'$, az irányított sétát *zárt irányított sétának* nevezzük, egyébként *nyílt irányított sétának*.

69. Definiálja az irányított út fogalmát!

Egy irányított sétát *irányított útnak* fogunk nevezni, ha a $v_0, v_1, \dots, v_n$ csúcsok mind különbözőek.

70. Definiálja az irányított kör fogalmát!

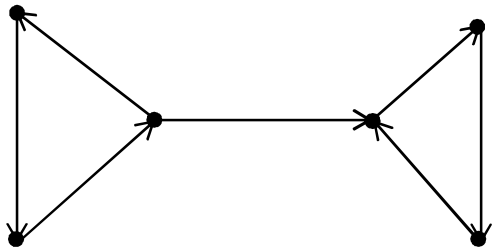
Egy legalább egy hosszú zárt irányított vonalat *irányított körnek* nevezünk, ha a kezdő- és a végpont megegyeznek, de egyébként az irányított vonal pontjai különbözőek.

71. Definiálja az erős összefüggőség és az erős komponens fogalmát!

Egy irányított gráfot *erősen összefüggőnek* nevezünk, ha bármely (v, v') csúcspár esetén vezet irányított út v-ből v'-be (és így, v és v' szerepét megcserélve, v'-ből v-be is).
Nyilván egy adott gráf csúcsaira az a reláció, hogy az egyikből a másikba és a másikból az egyikbe vezet irányított út, ekvivalenciareláció a csúcsok halmazán, így meghatároz egy osztályozást. A csúcsok egy adott osztálya által meghatározott telített irányított részgráf az irányított gráf egy *erős komponense*.

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

Az irányítatlan gráfokkal ellentétben nem feltétlenül tartozik az irányított gráf minden éle valamely erős komponenséhez. Példa:



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

Nyilván egy irányított gráf akkor és csak akkor erősen összefüggő, ha minden csúcs ugyanabba az osztályba tartozik, azaz ha csak egyetlen erős komponense van.

74. Definiálja az irányított fa és gyökere fogalmát!

Az *irányított fa* olyan irányított gráf, amely fa, és van egy csúcsa, amelynek befoka 0, az összes többi csúcs befoka 1.
Azt a csúcsot, amelynek befoka 0, *gyökérnek* nevezzük.

75. Definiálja az irányított fa szintjeit!

Az úthossz szerinti indukcióval adódik, hogy a gyökérből bármely adott csúcsba vezető egyetlen út egyben irányított út is; ennek hossza az adott csúcs *szintje*.

76. Definiálja irányított fában a leveleket!

Irányított fának azokat a csúcsai, amelyek kifoka nulla, *levélnek* nevezzük.

77. Definiálja irányított fában a gyermeke, testvére és szülője fogalmakat!

Ha van olyan él, amelynek v kezdőpontja, v' pedig a végpontja, akkor azt mondjuk, hogy v' a v *gyereke*, illetve hogy v a v' *szülője*.
Ha két csúcsnak ugyanaz a szülője, akkor *testvéreknek* nevezzük őket.

78. Definiálja az irányított részfa fogalmát!

Bármely v csúcsra tekinthetjük azon csúcsok halmazát, amelyekhez vezet irányított út v-ből. Ezek a csúcsok meghatároznak egy feszített irányított részgráfot, amely nyilván irányított fa, és v a gyökere; ezt a v-ben gyökerező *irányított részfának* nevezzük.

79. Definiálja a gyökeres fa fogalmát!

Ha egy irányítatlan fában kijelölünk egy csúcsot, akkor *gyökeres fáról* beszélünk.

80. Definiálja a q-ad rendű fa fogalmát!

Egy *q-ad rendű fa* egy olyan élcímkézett irányított fa, amelyben minden él címkéje egy q-nál kisebb természetes szám, és minden csúcsra a kimenő élek címkéi különböznek.

81. Definiálja a bináris fa fogalmát!

0 vagy 1 helyett bal kimenő élről, illetve jobb kimenő élről, bal gyerekről, illetve jobb gyerekről, részfáról stb. beszélünk.

82. Fogalmazza meg a Dijkstra módszerét leíró tételt!

A (ψ, E, V, w) véges élsúlyozott irányított gráfról tegyük fel, hogy az élsúlyok pozitívak, $s \in V$ és $T \subset V$. Az alábbi algoritmus a csúcshalmazon értelmez egy $d: V \to \overline{\mathbb{R}}$ függvényt, amely $t \in T$ esetén az adott s csúcsból t csúcsba vezető irányított séták súlyának minimuma ($+\infty$, ha nincs ilyen séta):

(1) [Inicializálás.] Legyen $S = \emptyset$, $H = \{s\}$ és $d(s) = 0$; minden más v csúcsra legyen $d(v) = +\infty$. (Az S halmaz a „már kész" csúcsok halmaza, H pedig a „már munkába vett" csúcsok halmaza.)
(2) [Kész?] Ha $T \subset S$, vagy $H = \emptyset$, akkor az algoritmus véget ért.
(3) [S bővítése.] Legyen $t \in H$ egy olyan csúcs, amelyre $d(t)$ minimális. Tegyük át t-t S-be, és minden e élre, amely t-ből $v \in V \backslash S$-be vezet, ha $d(t) + w(e) < d(v)$, akkor legyen $d(v) = d(t) + w(e)$, és ha $v \notin H$, tegyük át v-t H-ba. Menjünk (2)-re.

83. Definiálja a jólszínezés és a kromatikus szám fogalmát!

Egy gráf egy csúcsszínezését *jólszínezésnek* nevezzük, ha a szomszédos csúcsok színe különböző.
A gráf *kromatikus száma* a legkisebb olyan n természetes szám, amelyre a gráf jólszínezhető n színnel; ha nincs ilyen, akkor $+\infty$.

84. Definiálja irányítatlan gráf élmátrixát!

Ha egy $G = (\varphi, E, V)$ véges irányítatlan gráf élei $e_1, \dots, e_n$, csúcsai pedig $v_1, \dots v_m$, akkor az alábbi *élmátrix* egyértelműen megadja a gráfot: $1 \leq i \leq m$ és $1 \leq j \leq n$ esetén: a G irányítatlan gráf élmátrixán az $|a_{i,j}|$ elemekből álló mátrixot értjük.

85. Definiálja az irányított és irányítatlan gráf csúcsmátrixát!

A G irányított véges gráf b *csúcsmátrixában* legyen $b_{i,j}$ a v_i kezdőpontú, v_j végpontú élek száma, ha $1 \leq i, j \leq m$. A megfelelő irányítatlan gráf csúcsmátrixát kicsit másként értelmezzük: ha $1 \leq i, j \leq m$, akkor $i = j$ esetén legyen $b_{i,j}$ a v_i csúcsra illeszkedő hurokélek száma, egyébként pedig legyen a v_i és v_j csúcsokra illeszkedő élek száma.

86. Definiálja egy művelet esetén a homomorfizmus és a homomorf kép fogalmát!

Legyen adott a G és G' halmazokon egy-egy binér művelet; az egyszerűség kedvéért mindegyiket szorzással jelöljük. Egy $\varphi: G \to G'$ művelettartó leképezést *homomorfizmusnak* fogjuk nevezni, és azt mondjuk, hogy $\varphi(G)$ a G *homomorf képe*.

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

Ha a φ homomorfizmus kölcsönösen egyértelmű (injektív), akkor *monomorfizmusnak*, ha pedig G'-re képez (szürjektív), akkor egy G'-re képező *epimorfizmusnak* nevezzük. Ha φ kölcsönösen egyértelmű és G'-re képez (bijektív), akkor azt mondjuk, hogy φ *izomorfizmus* G és G' között.

88. Definiálja egy művelet esetén az endomorfizmus és az automorfizmus fogalmakat!

Ha $G = G'$ ugyanazzal a művelettel, akkor a homomorfizmusokat *endomorfizmusoknak*, az izomorfizmusokat pedig *automorfizmusoknak* is nevezzük.

89. Definiálja félcsoport esetén a reprezentáció és a hű reprezentáció fogalmát!

Fontos példánk egységelemes félcsoportra egy tetszőleges X halmaz önmagába való leképezéseinek halmaza a függvényösszetétellel mint művelettel. Ha egy félcsoportnak egy ilyen leképezés-félcsoportba való homomorfizmusát tekintjük, akkor a félcsoport *reprezentációjáról* beszélünk. Ha a reprezentáció izomorfizmus, akkor *hű reprezentációról* beszélünk.

90. Adjon meg egy egységelemes félcsoportnak egy hű reprezentációját!

Bármely G egységelemes félcsoportnak könnyen megadhatjuk egy hű reprezentációját: legyen $X = G$, és ha $g \in G$, legyen $\varphi_g(x) = gx$ minden $x \in X$, azaz φ_g a g-vel való balszorzás. A $g \mapsto \varphi_g$ leképezés homomorfizmus, mert minden $x \in X$-re

$$\varphi_{gh}(x) = ghx = \varphi_g(hx) = (\varphi_g \circ \varphi_h)(x).$$

Ha $g \neq h$, akkor $\varphi_g \neq \varphi_h$, mert ha e a G egységeleme, akkor

$$\varphi_g(e) = ge = g \neq h = he = \varphi_h(e),$$

így a reprezentáció hű.

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

A homomorfizmus definíciójánál használt jelölésekkel:

(1) ha G félcsoport, akkor a homomorf képe is félcsoport;
(2) ha G-ben e jobb oldali egységelem, bal oldali egységelem, illetve egységelem, akkor a homomorf képében e képe jobb oldali egységelem, bal oldali egységelem, illetve egységelem;

(3) ha G-ben e egységelem, és g-nek g^* jobb oldali inverze, bal oldali inverze, illetve inverze, akkor a homomorf képében g^* képe a g képének jobb oldali inverze, bal oldali inverze, illetve inverze;
(4) ha G-ben g és h felcserélhetőek, akkor a homomorf képben g és h képei felcserélhetőek.

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

Csoport homomorf képe is csoport. Kommutatív félcsoport homomorf képe is kommutatív félcsoport. Abel-csoport homomorf képe is Abel-csoport.

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

Ha G egy félcsoport, akkor az alábbi feltételek ekvivalensek:

(1) G csoport;
(2) $G \neq \emptyset$ és minden $a, b \in G$ esetén egy és csak egy olyan $x \in G$, illetve $y \in G$ létezik, amelyre $ax = b$, illetve $ya = b$ (elvégezhető az osztás);
(3) $G \neq \emptyset$ és minden $a, b \in G$ esetén létezik olyan $x \in G$, illetve $y \in G$, amelyre $ax = b$, illetve $ya = b$ (a művelet invertálható).

94. Fogalmazza meg csoportban az egyszerűsítési szabályt!

Egy csoportban, ha $ac = bc$ vagy $ca = cb$, akkor $a = b$.

95. Adjon példát műveletre, amelynél elvégezhető az osztás, de nem kapunk csoportot!

Az $\{\alpha, \beta, \gamma\}$ halmazon a

$\cdot$	α	β	γ
α	β	α	γ
β	α	γ	β
γ	γ	β	α

táblázattal megadott művelet elvégezhető az osztás, mégsem kapunk csoportot, mert a művelet nem asszociatív: $(\alpha\beta)\gamma = \alpha\gamma = \gamma$, de $\alpha(\beta\gamma) = \alpha\beta = \alpha$.

96. Adja meg a szorzással mint művelettel tekintett egységnyi abszolút értékű komplex számok csoportjának három valódi részcsoportját!

Az n-edik komplex egységgyökök halmaza bármely $n \in \mathbb{N}$-re csoportot alkot a szorzással és e halmazok mind részhalmazai az egységnyi abszolút értékű komplex számok halmazának.

(1) $\{(1,0); (-1,0)\}$;
(2) $\{(0,1); (0,-1)\}$;
(3) $\{(1,0); (0,1); (-1,0); (0,-1)\}$;
(4) $\{(\sin c, \cos c); (\cos c, \sin c)\}$, $(c \in \mathbb{R})$.

97. Mit értünk kvaterniócsoporton? Kommutatív-e?

A $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ kvaterniók a kvaterniószorzással nem kommutatív csoportot alkotnak.

98. Mit értünk Klein-féle csoporton? Kommutatív-e?

A *Klein-féle csoportot* a szorzótáblájával definiáljuk:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Mivel a szorzótábla szimmetrikus, a művelet kommutatív.

99. Mit értünk diédercsoporton?

Az n oldalú szabályos sokszöget önmagába vivő egybevágóságok (távolságtartó leképezések) az egymás utáni végrehajtással alkotják a D_n *diédercsoportot*.
ε jelöli a $2\pi/n$ szöggel (pozitív irányba) történő forgatást.
Jelöljön τ egy rögzített csúcson átmenő szimmetriatengelyre való tükrözést.
Tehát a diédercsoport

$$D_n = \{e, \varepsilon, \dots, \varepsilon^{n-1}, \tau, \tau\varepsilon, \dots, \tau\varepsilon^{n-1}\}.$$

100. Definiálja a részcsoport, triviális részcsoport és valódi részcsoport fogalmát!

Egy G grupoid egy H részhalmazás részgrupoidnak nevezzük, ha maga is grupoid a G-beli műveletet csak H elemei között tekintve. Ha H a G-beli műveletet csak H elemei között tekintve félcsoport, csoport, stb., akkor *részfélcsoportnak, részcsoportnak*, stb. nevezzük. Számunkra legfontosabb az az eset lesz, amikor H részcsoportja a G csoportnak. (Szokás ennek kifejezésére a $H \leq G$ jelölést használni.) Nyilván ha G csoport, akkor az egész G és a csak az egységelemet tartalmazó egyelemű részhalmaz részcsoportok, ezek a *triviális részcsoportok.* A G-től különböző részcsoportokat *valódi részcsoportnak* nevezzük.

101. Mit értünk komplexusműveleten?

Emlékeztetünk rá, hogy a műveletet a részhalmazok között is értelmeztük, elemenként. Ugyanígy értelmeztük a részhalmazokra az inverzképzést is, elemenként. (Szokás a részhalmazokat *komplexusoknak* is nevezni, és *komplexusműveletekről* beszélni.)

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

Legyen G csoport, és $H \subset G$. Az alábbi feltételek ekvivalensek:

(1) H részcsoport;
(2) a szorzás leszűkítése $H \times H$-ra egy $H \times H$-t H-ba képező leképezés, H tartalmazza G egységelemét, és $H^{-1} \subset H$;
(3) $H \neq \emptyset$, $HH \subset H$ és $H^{-1} \subset H$;
(4) $H \neq \emptyset$ és $H^{-1}H \subset H$.

103. Mit mondhatunk részcsoportok metszetéről és egyesítéséről?

Ha H_γ, $\gamma \in \Gamma$, a G csoport részcsoportjainak egy rendszere, akkor $H = \cap_{\gamma\in\Gamma} H_\gamma$ is részcsoport.

Részcsoportok egyesítése általában nem részcsoport, például a Klein-féle csoportban $\{e, a\}$ és $\{e, b\}$ részcsoportok, de egyesítésük nem az.

104. Definiálja a generátum és a generátorrendszer fogalmát!

Legyen G egy csoport, és $K \subset G$. A K halmaz $\langle K \rangle$ *generátuma* a G összes, K-t tartalmazó részcsoportjának metszete. Ha $G = \langle K \rangle$, akkor azt mondjuk, hogy K a G csoport *generátorrendszere.*

105. Definiálja a ciklikus csoport és generátora fogalmát!

Ha egy csoportnak létezik egyelemű generátorrendszere, akkor *ciklikusnak* nevezzük, az elemet pedig egy *generátorának*.

106. Fogalmazza meg a generátumot leíró állítást!

Az előző definíció jelöléseivel, $\langle K \rangle = \{g_1 g_2 \cdots g_n : n \in \mathbb{N}, g_i \in K \cup K^{-1}, ha\ 1 \leq i \leq n\}$.

107. Mit mondhatunk ciklikus csoport homomorf képéről?

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

108. Definiálja csoport és elem rendjét!

Egy G véges csoport *rendjén* az elemeinek a számát értjük, egyébként azt mondjuk, hogy a csoport rendje végtelen. Egy $g \in G$ *elem rendjén* azt az n legkisebb pozitív egész kitevőt értjük, amelyre $g^n = e$, ha van ilyen, egyébként azt mondjuk, hogy az elem rendje végtelen.

109. Fogalmazza meg a ciklikus csoportok szerkezetét leíró tételt!

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

110. Mi a kapcsolat elem és részcsoport rendje között?

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

111. Mit mondhatunk ciklikus csoport részcsoportjainak ciklikusságáról?

Ciklikus csoport minden részcsoportja is ciklikus.

112. Mit mondhatunk véges ciklikus csoport generátorainak számáról?

Legyen G egy n rendű véges ciklikus csoport, g pedig egy generátoreleme G-nek. Ha $a \in \mathbb{Z}$ és $d = lnko(a, n)$, akkor g^a az egyetlen m-rendű $H = \{g^d, g^{2d}, \dots, g^{md} = e\}$ ciklikus részcsoportot generálja, ahol $n = md$. A G minden részcsoportja előáll így valamely $d|n$-re. A G-nek $\varphi(n)$ generátora van.

113. Definiálja a bal- és jobboldali mellékosztályokat!

Legyen G egy csoport, és legyen H a G egy részcsoportja. Vezessük be az $a \sim b$, ha $ab^{-1} \in H$ relációt. Ez nyilván ekvivalenciareláció. Vizsgáljuk meg az ekvivalenciaosztályokat. Azt állítjuk, hogy $a \in G$ ekvivalenciaosztálya a Ha halmaz. Ha $b \in Ha$, akkor $b = ha$ valamely $h \in H$-ra. Innen $ba^{-1} = h$, azaz $ab^{-1} = h^{-1} \in H$. Megfordítva, ha $a \sim b$, akkor $ab^{-1} = h \in H$, ahonnan $b = h^{-1}a \in H^{-1}a \subset Ha$.
Ha most az $a \sim b$, ha $b^{-1}a \in H$ ekvivalenciarelációt vezetjük be, akkor hasonlóan számolva kapjuk, hogy az a ekvivalenciaosztálya az aH halmaz. Az előző ekvivalenciaosztályokat a G csoport H szerinti *jobb oldali mellékosztályainak*, az utóbbiakat pedig *bal oldali mellékosztályainak* nevezzük.

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

Megjegyezzük, hogy a $Ha \mapsto (Ha)^{-1} = a^{-1}H$ leképezés kölcsönösen egyértelműen képezi le a jobb oldali mellékosztályok halmazát a bal oldali mellékosztályok halmazára, így ezek száma egyszerre véges, és ha véges, akkor megegyezik.

115. Definiálja részcsoport indexét!

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

116. Fogalmazza meg Lagrange tételét!

Ha H a G véges csoport részcsoportja, akkor a H rendjének és indexének a szorzata G rendje.

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

Véges csoportban az elem rendje osztja a csoport rendjét.

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

Prímszámrendű csoport ciklikus.

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

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

120. Definiálja a normálosztó fogalmát!

Ha N részcsoportja G-nek, és minden $a \in G$-re $aN = Na$, akkor N-et *normálosztónak* nevezzük.

121. Adjon meg három olyan csoportot, amelyben minden részcsoport normálosztó!

(1) Abel-csoportban minden részcsoport normálosztó;
(2) Az egész G és a csak az egységelemet tartalmazó egyelemű részhalmaz normálosztó;
(3) Egy kettő indexű N részcsoport mindig normálosztó, mert csak két, bal és egyúttal jobb oldali mellékosztály van, N és $G \backslash N$.

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

Legyen N a G csoport részcsoportja. A következő feltételek ekvivalensek:

(1) N normálosztó;
(2) $a^{-1}Na = N$ minden $a \in G$-re;
(3) $a^{-1}Na \subset N$ minden $a \in G$-re.

123. Mit mondhatunk normálosztók metszetéről és egyesítéséről?

Normálosztók metszete is normálosztó.

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

Legyen G csoport. Ekkor

(1) egy N normálosztó szerinti mellékosztályok a csoportnak a művelettel kompatiblis osztályozását alkotják;
(2) egy N normálosztó szerinti mellékosztályok közötti művelet megegyezik az osztályok mint halmazok komplexusszorzásával;
(3) minden, a művelettel kompatiblis osztályozás esetén az egységelem osztálya normálosztó, és az osztályozás ezen normálosztó szerinti mellékosztályokból áll.

125. Definiálja a faktorcsoport fogalmát és fogalmazza meg a definícióban felhasznált tételt!

Egy G csoportnak egy N normálosztó szerinti mellékosztályai a (komplexus)szorzásra nézve csoportot alkotnak. Ezt a G csoportot az N normálosztó szerinti *faktorcsoportjának* nevezzük, és G/N-el jelöljük.

126. Adjon meg három példát faktorcsoportra!

(1) Ha $N = G$, akkor G/N egyelemű. Ha $N = \{e\}$, akkor az osztályok egyeleműek, így G/N izomorf G-vel.
(2) Bármely $m \in \mathbb{Z}$-re az $m\mathbb{Z}$ normálosztó $\mathbb{Z}$ additív Abel-csoportban, és a faktorcsoport $\mathbb{Z}_m$ additív csoportja.
(3) A kvaterniócsoportban a kételemű $\langle -1 \rangle$ részcsoport szerinti négyelemű faktorcsoport izomorf a Klein-féle csoporttal.

127. Definiálja a csoporthomomorfizmus magját!

Egy G csoportnak egy G' csoportba való φ homomorfizmusánál a *homomorfizmus magján* a G' csoport e' egységelemének a teljes inverz képét értjük, amit $\ker(\varphi)$-vel jelölünk.

128. Fogalmazza meg a homomorfizmustételt csoportokra!

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

129. Definiálja egyműveletes struktúrák direkt szorzatát! Részletezze azt az esetet, amikor az indexhalmaz $\{1, 2, \dots, n\}$! Mit mondhatunk a direkt szorzat algebrai tulajdonságairól?

Legyen G_i $(i \in I)$ egy-egy binér művelettel ellátott halmazok egy indexelt családja. Az egyszerűség kedvéért mindegyik halmazon a műveletet jelöljük szorzással. Ekkor a

$$G = \times_{i \in I} G_i$$

Descartes-szorzatot ellátva az $(ab)_i = a_i b_i$ összefüggéssel definiált művelettel, a G-t a G_i, $i \in I$ család *direkt szorzatának* nevezzük.
A legfontosabb speciális eset az, amikor $I = \{1,2,\dots,n\}$, ekkor a direkt szorzat elemei $a = (a_1, a_2, \dots, a_n)$, $a_i \in G_i$ alakú n-esek. A szorzás definíció szerint koordinátánként történik, így ha $b = (b_1, b_2, \dots, b_n)$ egy másik eleme a direkt szorzatnak, akkor $ab = (a_1 b_1, a_2 b_2, \dots, a_n b_n)$.
Nyilvánvaló, hogy ha minden G_i félcsoport, akkor G is, ha minden G_i kommutatív, akkor G is, ha minden G_i egységelemes, akkor G is, és ha minden G_i csoport, akkor G is.

130. Fogalmazza meg a végesen generált Abel-csoportok alaptételét!

Egy véges halmaz által generált Abel-csoport véges sok ciklikus csoport direkt szorzatával izomorf. A tényezők közül véges rendűek választhatók prímhatvány rendűnek. A végtelen rendű tényezők száma és az egyes prímhatványrendek egyértelműen meghatározottak.

131. Fogalmazza meg Cayley tételét!

Bármely G csoport izomorf valamely halmaz permutációinak (a $\circ$ kompozícióval tekintett csoportja) egy részcsoportjával. A halmaz választható G-nek.

132. Definiálja az n-ed fokú szimmetrikus csoportot!

Tetszőleges X halmaz összes permutációinak a $\circ$ művelettel vett csoportját az X szimmetrikus csoportjának neveztük. Az $\{1,2,\dots,n\}$ halmaz összes permutációinak csoportját S_n-nel fogjuk jelölni, és *n-ed fokú szimmetrikus csoportnak* nevezzük.

133. Két véges halmaznak ugyanannyi eleme van. Igaz-e, hogy permutációcsoportjaik izomorfak?

A szimmetrikus csoport szerkezete csak az alaphalmaz elemeinek számától függ: ha φ az X halmaznak az Y halmazra való kölcsönösen egyértelmű leképezése, akkor tudjuk, hogy $f \mapsto \varphi \circ f \circ \varphi^{-1}$ megfeleltetés kölcsönösen egyértelmű leképezése (bijekciója) X összes permutációinak Y összes permutációira. Mivel a permutációk összetételére ez a megfeleltetés művelettartó is, hiszen

$$(\varphi \circ f \circ \varphi^{-1}) \circ (\varphi \circ g \circ \varphi^{-1}) = \varphi \circ f \circ g \circ \varphi^{-1},$$

így X és Y permutációinak csoportjai izomorfak.

134. Írja le S_n elemeinek hagyományos jelölését és adja meg ezzel a jelöléssel a szorzást!

Bár az S_n elemei sorozatok, így egy $p \in S_n$ elemet jelölhetünk $p_1, p_2, \dots, p_n$-nel, szokásosabb a hagyományos jelölés:

$$p = \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix}, q = \begin{pmatrix} 1 & 2 & \dots & n \\ q_1 & q_2 & \dots & q_n \end{pmatrix},$$

azaz minden elem alá odaírjuk a képét.
A két elem szorzata

$$p \circ q = \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ q_1 & q_2 & \dots & q_n \end{pmatrix}$$

$$= \begin{pmatrix} q_1 & q_2 & \dots & q_n \\ p_{q_1} & p_{q_2} & \dots & p_{q_n} \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ q_1 & q_2 & \dots & q_n \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & \dots & n \\ p_{q_1} & p_{q_2} & \dots & p_{q_n} \end{pmatrix}.$$

135. Definiálja a páros és páratlan permutációkat!

Egy

$$p = \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix}$$

alakban írt permutációra legyen k az inverziók száma az alsó sorban, azaz az összes olyan $1 \leq i < j \leq n$ párok száma, amelyekre $p_i > p_j$. A permutációt *páros permutációnak*, illetve *páratlan permutációnak* nevezzük aszerint, hogy k páros vagy páratlan; ez a permutáció paritása.

136. Ismertesse permutációk ciklus jelölését!

Permutációkat egy másik alakban is felírhatunk. Ha $1 \leq i_1, i_2 \dots, i_k \leq n$ különböző természetes számok, jelölje $(i_1, i_2 \dots, i_k)$ azt a permutációt, amely i_1-et i_2-be, i_2-t i_3-ba stb., i_k-t i_1-be viszi, minden más számot pedig fixen hagy. Egy ilyen permutációt k *hosszúságú ciklusnak* nevezünk.

137. Mi a transzpozíció?

A triviális egy (vagy nulla) hosszú ciklusoktól eltekintve a legegyszerűbb ciklusok a kettő hosszú ciklusok, ezeket *transzpozícióknak* nevezzük.

138. Fogalmazza meg a páros illetve páratlan permutációk és a transzpozíciók száma közötti összefüggést leíró tételt!

Egy $p \in S_n$ permutáció pontosan akkor páros, ha előállítható páros sok transzpozíció szorzataként, és pontosan akkor páratlan, ha páratlan sok transzpozíció szorzataként állítható elő.

139. Fogalmazza meg a permutációk szorzatának párosságára vonatkozó tételt!

Az S_n csoportban szorzásban a paritások “mod 2 összeadódnak”: egy páros és egy páratlan permutáció szorzata páratlan, két páros vagy két páratlan permutáció szorzata pedig páros.

140. Definiálja az alternáló csoportokat!

A páros permutációk 2 indexű normálosztót alkotnak S_n-ben, amit A_n-nel jelölünk és n-ed fokú alternáló csoportnak nevezünk.

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

Egy egységelemes integritási tartomány nyilván pontosan akkor test, ha minden nem nulla eleme egység.

142. Definiálja gyűrű karakterisztikáját! Milyen állítást használt?

Nullosztómentes gyűrűben a nem nulla elemek additív rendje megegyezik. Ha ez közös érték végtelen, akkor azt mondjuk, hogy a *gyűrű karakterisztikája* nulla, ha pedig egy véges n érték, akkor azt mondjuk, hogy a *gyűrű karakterisztikája* n. Jelölése: $char(R)$.

143. Igaz-e, hogy egy adott halmazt egy testbe képező függvények gyűrűje is test?

Egy tetszőleges X halmazt egy R gyűrűbe képező összes függvények R^X halmaza a pontonkénti összeadással és szorzással gyűrű. Ha R kommutatív, akkor ez a gyűrű is kommutatív, ha R egységelemes, akkor az R^X gyűrű is egységelemes, de ha R is és X is legalább kételemű, akkor R^X nem nullosztómentes – így nem is test –, még akkor sem, ha R test.

144. Definiálja az endomorfizmusgyűrűt!

Egy tetszőleges A Abel-csoport összes endomorfizmusai egyésgelemes gyűrűt alkotnak a pontonkénti összeadással és a függvények kompozíciójával, mint szorzással; ezt a gyűrűt A *endomorfizmusgyűrűjének* nevezzük.

145. Definiálja két művelet esetén a homomorfizmus és a homomorf kép fogalmát!

Legyen R és R' két-két binér művelettel ellátott halmaz. Az egyszerűség kedvéért R-ben és R'-ben is az első műveletet összeadással, a másodikat pedig szorzással fogjuk jelölni. Az R-nek R'-be való összeadás- és szorzástartó $\varphi: R \to R'$ leképezését *homomorfizmusnak* fogjuk nevezni, és azt mondjuk, hogy $\varphi(R)$ az R *homomorf képe*.

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

Ha φ kölcsönösen egyértelmű (injektív), akkor *monomorfizmusnak*, ha pedig R'-re képez (szürjektív), akkor egy R'-re való *epimorfizmusnak* nevezzük. Ha φ kölcsönösen egyértelmű és R'-re képez (bijektív), akkor φ *izomorfizmus* R és R' között.

147. Definiálja két művelet esetén az endomorfizmus és az automorfizmus fogalmát!

Ha $R' = R$ ugyanazokkal a műveletekkel, akkor a homomorfizmusokat *endomorfizmusoknak*, az izomorfizmusokat *automorfizmusoknak* nevezzük.

148. Mit mondhatunk homomorfizmusnál gyűrű képéről?

Gyűrű homomorf képe is gyűrű.

149. Definiálja gyűrű reprezentációját és hű reprezentációját!

Egy R gyűrűnek egy Abel-csoport endomorfizmusgyűrűjébe való homomorfizmusát R *reprezentációjának* nevezzük. Ha a leképezés monomorfizmus, akkor *hű reprezentációról* beszélünk.

150. Fogalmazza meg nullosztómentes gyűrűben az elemek additív rendjét leíró tételt!

Egy R nullosztómentes gyűrűben a nem nulla elemek additív rendje megegyezik, és vagy végtelen, vagy prímszám.

151. Definiálja gyűrű karakterisztikáját!

Ld.: 142-es kérdés.

152. Definiálja a részgyűrű fogalmát!

Legyen R egy halmaz a $(+,\cdot)$ binér műveletekkel. Az R egy S részhalmazát *részgyűrűnek*, illetve *résztestnek* nevezzük, ha maga is gyűrű, illetve test az adott művelettel.

153. Definiálja a jobbideál, balideál és ideál fogalmát!

Azt a szerepet, amelyet csoportoknál a részcsoportok közül a normálosztók játszottak, a gyűrűk esetében az ideálok veszik át. Az I részgyűrűt *jobbideálnak*, illetve *balideálnak* nevezzük, ha $a \in I$ és $r \in R$ esetén $ar \in I$, illetve $ra \in I$. Ha I egyszerre balideál és jobbideál is, akkor *ideálnak* nevezzük.

154. Definiálja a triviális ideál és a valódi ideál fogalmát!

Nyilván az egész R és a csak a nullelemet tartalmazó egyelemű részhalmaz ideál, ezek a *triviális ideálok*. Az R-től különböző ideálokat *valódi ideálnak* nevezzük.

155. Definiálja az egyszerű gyűrű fogalmát!

Ha egy gyűrűben a triviális ideálokon kívül nincs más ideál, akkor *egyszerű gyűrűnek* nevezzük.

156. Definiálja a generált ideál és a főideál fogalmát!

Egy $A \subset R$ részhalmaz által *generált ideálon* az összes, az A-t tartalmazó ideálok metszetét értjük. Jelölése: (A). Ha egy I ideált egyetlen $a \in R$ generál, azaz $I = (a)$, akkor *főideálnak* nevezzük.

157. Mondjon négy példát $\mathbb{R}^{\mathbb{R}}$ 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 polinomfüggvények stb.

158. Mondjon példát $\mathbb{Z}$-ben ideálra! Főideál-e?

Az egész számok gyűrűjében egy m egész szám többszörösei ideált alkotnak. Ez nyilván főideál, amelyet m (vagy $-m$) generál.

159. Fogalmazza meg egy kommutatív egységelemes gyűrűben a főideálokat leíró állítást!

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

160. Definiálja gyűrűben a mellékosztályokat!

Legyen R egy gyűrű és legyen I egy additív részcsoportja R-nek. Vezessük be az $a \sim b$, ha $a - b \in I$ relációt. Tudjuk, hogy ez az összeadáással kompatibilis ekvivalenciareláció, az $a \in R$ ekvivalenciaosztálya az $I + a$ halmaz. Az ekvivalenciaoszályokat az R gyűrű I szerinti *mellékosztályainak* nevezzük.

161. Fogalmazza meg kompatiblis osztályozások és az ideálok közötti kapcsolatot leíró tételt!

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

162. 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*) nevezzük, és R/I-vel jelöljük.

163. Adjon példát $\mathbb{Z}$ faktorgyűrűjére!

Ha $R = \mathbb{Z}$ és $I = m\mathbb{Z}$, akkor $R/I = \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$.

164. Definiálja gyűrűhomomorfizmus magját!

Egy R gyűrűnek egy R' gyűrűbe való φ homomorfizmusánál a *homomorfizmus magján* az R' gyűrű nullelemének a teljes inverz képét értjük. A φ magját most is $\ker(\varphi)$-vel jelöljük.

165. Fogalmazza meg a homomorfizmustételt gyűrűkre!

Egy R gyűrű egy φ homomorfizmusánál a homomorfizmus magja ideál. Ha R képe R', akkor az $R/\ker(\varphi)$ faktorgyűrű izomorf R'-vel. Az R bármely I ideálja magja valamely homomorfizmusnak, például R kanonikus leképezése R/I-re homomorfizmus, amelynek magja I.

166. Definiálja kétműveletes halmazok direkt szorzatát! Mit mondhatunk a direkt szorzatról?

Legyen $G_i,\ i \in I$ két binér művelettel ellátott halmazok egy indexelt családja. Az egyszerűség kedvéért mindegyik halmazon az első műveletet összeadással, a másodikat pedig szorzással jelöljük. Ekkor a

$$G = \times_{i \in I} G_i$$

Descartes-szorzatot ellátva az $(a+b)_i = a_i + b_i$ és $(ab)_i = a_i b_i$ összefüggéssel definiált műveletekkel, a G-t a G_i család *direkt szorzatának* nevezzük. A direkt szorzat a hatvány általánosítása.
Nyilvánvaló, hogy ha minden G_i gyűrű, akkor G is, ha minden G_i kommutatív, akkor G is, ha minden G_i egységelemes, akkor G is, de soha nem test, még csak nem is nullosztómentes, ha I legalább két G_i nem nullgyűrű.

167. Fogalmazza meg a kommutatív egységelemes gyűrű főideáljait leíró tételt!

Ld.: 159-es kérdés.

168. Fogalmazza meg az oszthatóság és a főideálok kapcsolatát leíró tételt!

Egy R egységelemes integritási tartomány a, b elemeire

(1) $(a) \subset (b)$ akkor és csak akkor, ha $b|a$;
(2) $(a) = (b)$ akkor és csak akkor, ha a és b asszociáltak;
(3) $(a) = R$ akkor és csak akkor, ha a egység.

169. Definiálja a Gauss-gyűrű fogalmát!

Egy R egységelemes integritási tartományt *Gauss-gyűrűnek* nevezünk, ha minden nullától és egységtől különböző elem sorrendtől és egységektől eltekintve egyértelműen felírható irreducibilis elemek (véges) szorzataként, azaz, ha a nem nulla és nem egység, akkor felírható $a = p_1 p_2 \cdots p_n$ alakban, ahol $p_1, p_2, \dots, p_n$ (nem feltétlenül különböző) irreducibilis elemek, és ha $a = q_1 q_2 \cdots q_m$ egy másik előállítás irreducibilis elemek szorzataként, akkor $m = n$, és van olyan $\sigma \in S_n$ permutáció, hogy q_{σ_i} és p_i asszociáltak, ha $i = 1,2, \dots, n$.

170. Gauss-gyűrűben hogyan olvashatók le a faktorizációból az osztók?

A felbontásból leolvashatók a osztói, ezek

$$(1)\ d = \varepsilon' p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

alakúak, ahol ε' egység és $\beta_j \in \mathbb{N}$, $\beta_j \leq \alpha_j$, ha $j = 1,2, \dots, k$, hiszen ha $a = cd$, akkor c és d irreducibilis tényezőkre való felbontásának szorzata a irreducibilis tényezőkre való felbontása kell hogy legyen.

171. Igaz-e, hogy Gauss-gyűrűben létezik legnagyobb közös osztó és legkisebb közös többszörös?

Ha több elemünk van, és mindnek adott az irreducibilis tényezőkre való felbontása, akkor – hasonlóan, mint $\mathbb{Z}$-ben – közös osztóik, valamint közös többszöröseik is leolvashatók, és látjuk, hogy létezik legnagyobb közös osztó és legkisebb közös többszörös.

172. Igaz-e, hogy Gauss-gyűrűben minden irreducibilis elem prím?

Egy Gauss-gyűrűben minden irreducibilis elem prímelem, mert ha a nullától és egységtől különböző p irreducibilis elemre $p|ab$, akkor $ab = 0$, amiből valamelyik nulla, vagy pedig $ab = pd$ valamely $d \neq 0$ elemre, amiből d-t felírva (1) alakban, az ab egy olyan előállítását kapjuk irreducibilis elemek szorzataként, amelyben szerepel p.

173. Definiálja az euklideszi gyűrű fogalmát!

Egy R egységelemes integritási tartományt *euklideszi gyűrűnek* nevezünk, ha a nem nulla elemein értelmezve van egy $\mathbb{N}$-beli értékű φ függvény úgy, hogy

(1) ha $a, b \in R$, $b \neq 0$, akkor van olyan $q, r \in R$, hogy $a = bq + r$ és $r = 0$, vagy $r \neq 0$ és $\varphi(r) < \varphi(b)$;
(2) $\max\{\varphi(a), \varphi(b)\} \leq \varphi(ab)$ minden $a, b \in R$, $a \neq 0$, $b \neq 0$ esetén.

174. Fogalmazza meg az euklideszi gyűrűben az egységeket és az asszociáltakat leíró tételt!

Euklideszi gyűrűben pontosan azok az elemek az egységek, amelykre φ értéke minimális értéket vesz fel. Az a, b nem nulla elemekre $b|a$ esetén egyrészt $\varphi(b) \leq \varphi(a)$, másrészt egyenlőség pontosan akkor teljesül, ha a és b asszociáltak.

175. Fogalmazza meg a bővített euklideszi algoritmust gyűrűben!

A következő eljárás egy R euklideszi gyűrűben meghatározza az $a, b \in R$ elemek egy d legnagyobb közös osztóját, valamint az $x, y \in R$ elemeket úgy, hogy $d = ax + by$ teljesüljön. (Az eljárás során végig az $ax_n + by_n = r_n$, $n = 0{,}1$ ….)

(1) [Inicializálás.] Legyen $x_0 \leftarrow e$, a gyűrű egységeleme, $y_0 \leftarrow 0$, $r_0 \leftarrow a$, $x_1 \leftarrow 0$, $y_1 \leftarrow e$, $r_1 \leftarrow b$, $n \leftarrow 0$.
(2) [Vége?] Ha $r_{n+1} = 0$, akkor $x \leftarrow x_n$, $y \leftarrow y_n$, $d \leftarrow r_n$, és az eljárás véget ért.
(3) [Ciklus.] Legyen $r_n = q_{n+1}r_{n+1} + r_{n+2}$, ahol $r_{n+1} = 0$ vagy $\varphi(r_{n+2}) < \varphi(r_{n+1})$, legyen $x_{n+2} \leftarrow x_n - q_{n+1}x_{n+1}$, $y_{n+2} \leftarrow y_n - q_{n+1}y_{n+1}$, $n \leftarrow n + 1$, és menjünk (2)-re.

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

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

177. 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 euklideszi gyűrű Gauss-gyűrű.

178. Definiálja a hányadostest fogalmát! Milyen állítást használt?

Legyen R a nullgyűrűtől különböző integritási tartomány. Az $R \times (R\backslash\{0\})$ halmazon vezessük be az $(a, b) \sim (a', b')$, ha $ab' = a'b$ ekvivalenciarelációt, az $(a, b) + (a', b') = (ab' + a'b, bb')$ összeadást és az $(a, b)(a', b') = (aa', bb')$ szorzást. A műveletek kompatibilisek az ekvivalenciarelációval, és az ekvivalenciaosztályok testet alkotnak, amelyet az R *hányadostestének* nevezünk.

179. Hogyan ágyazható be egy integritási tartomány a hányadostestébe?

Az előző tétel jelöléseivel, az R integritási tartomány beágyazható a hányadostestébe: bármely rögzített $b \neq 0$-ra $x \in R$-hez a (bx, b) osztályát rendelve ugyanazt a monomorfizmust kapjuk.

180. Definiálja az egyhatározatlanú polinom fogalmát!

Legyen R gyűrű. Az (egyhatározatlanú) polinomokról az az elképzelésünk, hogy $\sum_{i=0}^{n} f_i x^i$ alakú véges összegek, ahol x a "határozatlan", $n \in \mathbb{N}$, $f_i \in R$, ha $0 \leq i \leq n$, az összeadás és szorzás pedig tagonként történik.

181. Definiálja az egyhatározatlanú polinomok összeadását és szorzását!

Az előbbi definíció könnyen pontossá tehető az alábbi módon: ha $f = (f_0, f_1 \dots)$ és $g = (g_0, g_1 \dots)$ is R-beli végtelen sorozatok, azaz $R^{\mathbb{N}}$ elemei, akkor összegüket az $f + g = (f_0 + g_0, f_1 + g_1 \dots)$ sorozatként, szorzatukat pedig azon $h = (h_0, h_1 \dots)$ sorozatként definiálva, amelyre

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

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

Az $a \mapsto (a, 0,0, \dots)$ leképezés R-nek a polinomok gyűrűjébe való monomorfizmusa, értékkészletének elemei a *konstans polinomok*, ezeket R elemeivel azonosíthatjuk.

183. Definiálja polinom együtthatóit, főegyütthatóját és fokszámát!

A továbbiakban $f = (f_0, f_1, \dots, f_n, 0,0, \dots)$ polinomot kényelmi okokból a szokásos $f = f_0x^0 + f_1x^1 + f_2x^2 + \cdots + f_nx^n$ alakba írjuk. Az f_i neve az i-ed fokú tag *együtthatója*. Ha kikötjük, hogy $f_n \neq 0$, és minden n-nél alacsonyabb fokú tag is szerepel a felírásban, akkor f_n a polinom *főegyütthatója*, n pedig a polinom *foka*, jelölése $\deg(f)$.

184. Definiálja a lineáris polinomokat!

A legfeljebb elsőfokú polinomok a *lineáris polinomok*.

185. Definiálja a monom fogalmát egy határozatlan esetén!

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

186. Definiálja a főpolinom fogalmát!

Ha egy polinom főegyütthatója R egységeleme, akkor *főpolinomnak* nevezzük.

187. Mit mondhatunk polinomok szorzatának főegyütthatójáról?

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

188. Mit mondhatunk polinomok szorzatának fokáról?

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

189. Definiálja polinom helyettesítési értékét és gyökét!

Egy $f = f_0 + f_1x + \cdots + f_nx^n$ polinomnak az $r \in R$ helyen felvett *helyettesítési értékén* az $f(r) = f_0 + f_1r + \cdots + f_nr^n \in R$ elemet értjük. Ha f helyettesítési értéke az r helyen nulla, akkor azt mondjuk, hogy az r az f *gyöke*.

190. Definiálja a polinomhoz tartozó polinomfüggvényt! Tartozhat-e különböző polinomokhoz ugyanaz a polinomfüggvény?

Az $r \mapsto f(r)$ leképezést az f polinomhoz tartozó *polinomfüggvénynek* hívjuk.
Két különböző polinomhoz tartozhat ugyanaz a polinomfüggvény. Például, ha az R gyűrű véges, de nem a nullgyűrű, akkor végtelen sok polinom van $R[x]$-ben, míg csak véges sok R-et R-be képező függvény létezik.

191. Fogalmazza meg a maradékos osztás tételét polinomokra!

Legyen R egységeelemes integritási tartomány, $f, g \in R[x]$, $g \neq 0$, és tegyük fel, hogy g főegyütthatója egység R-ben. Ekkor egyértelműe léteznek olyan $q, r \in R[x]$ polinomok, amelyekre $f = gq + r$, ahol $\deg(r) < \deg(g)$.

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

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

193. Fogalmazza meg a gyöktényező leválasztására vonatkozó állítást!

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

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

Ha $f \neq 0$, akkor f-nek legfejlebb $\deg(f)$ gyöke van.

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

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

196. 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.

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

Az, hogy egy polinomnak hány gyöke van, függ attól, hogy milyen gyűrű felett tekintjük, azaz hol keressük a gyököt. Például az $1 - x^2$ polinomot $\mathbb{Z}$, $\mathbb{Q}$, illetve $\mathbb{R}$ felett tekintve nincs gyöke, $\mathbb{C}$ felett két gyöke van, i és $-i$, ha $\mathbb{Z}_p$ felett tekintjük, ahol p prímszám, akkor $p = 2$ esetén egy gyöke van.

198. Definiálja egy polinom algebrai deriváltját!

Legyen R gyűrű. Egy $f = f_0 + f_1x + f_2x^2 + \cdots + f_nx^n \in R[x]$ polinom *algebrai deriváltján* vagy röviden deriváltján az $f' = f_1 + 2f_2x + 3f_3x^2 + \cdots + nf_nx^{n-1} \in R[x]$ polinomot értjük.

199. Egy polinom hatványa oszt egy polinomot. Mit mondhatunk, mi osztja a deriváltat?

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

200. Definiálja polinom többszörös gyökét!

Legyen R egységelemes integritási tartomány, $f \in R[x]$, $f \neq 0$ és $n \in \mathbb{N}^+$. Azt mondjuk, hogy $c \in R$ az f egy *n-szeres gyöke*, ha $(x - c)^n | f$, de $(x - c)^{n+1} \nmid f$.

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

A derivált gyöke nyilván nem feltétlenül gyöke a polinomnak (például $x^2 + 1$-nek 0 nem gyöke, de a deriváltjának igen).

202. Lehet-e egy polinom n-szeres gyöke a deriváltjának is legalább n-szeres gyöke?

A polinom n-szeres gyöke lehet a deriváltnak több, mint $n-1$-szeres gyöke is: ha p prím, $a \in \mathbb{Z}_p$, $n \in \mathbb{N}$, $p \nmid n$, akkor $f = (x-a)^p((x-a)^n + 1) \in \mathbb{Z}_p[x]$-nek az a egy p-szeres gyöke, míg $f' = n(x-a)^{p+n-1}$-nek $(p+n-1)$-szeres gyöke.

203. Írja le az egységeket test feletti polinomok körében!

Az egységek a nem nulla konstans polinomok.

204. Hogyan kaphatunk test feletti polinomgyűrűből testbővítést? Írja le az eljárást részletesen!

Legyen F test, és $f \in F[x]$ egy n-ed fokú ($n \in \mathbb{N}^+$) főpolinom. A $\tilde{F} = F[x]/(f)$ gyűrűben minden mellékosztályban a legalacsonyabb fokú polinom fokszáma kisebb, mint n, és csak egy n-nél alacsonyabb fokú polinom van (mivel a mellékosztály bármely két polinomjának különbsége többszöröse f-nek); ez meghatározható úgy, hogy a mellékosztály tetszőleges g elemére veszzük az f-fel való osztásánál adódó r maradékot. Jelölje $\tilde{x} \in F[x]$ polinom osztályát $F[x]/(f)$-ben. A $\tilde{F}$ gyűrű elemei egyértelműen felírhatók $a_0 + a_1\tilde{x} + \cdots + a_{n-1}\tilde{x}^{n-1}$ alakban, ahol $a_0, a_1, \ldots, a_{n-1} \in F$. Így F részteste $\tilde{F}$-nak, más szóval $\tilde{F}$ bővítése F-nek. Az így megkapható testbővítéseket *algebrai testbővítésnek* nevezzük.

205. Mit mondhatunk véges testek elemszámáról?

Bármely véges test elemeinek száma prímhatvány, ahol a prím a test karakterisztikája.

206. 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 $c^q = e$.

207. Hogyan kaphatunk véges testeket? Írjon le olyan eljárást, amely minden lehetséges elemszámra véges testet ad! Írja le a tételt, amiből ez következik!

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

208. Írja le Wedderburn tételét!

Véges ferdetest kommutatív, tehát test.

209. Írja le az irreducibilis polinomokat a $\mathbb{C}$ feletti polinomok körében!

A komplex számtest felett az algebra alaptétele szint mindn $\mathbb{C}[x]$-beli nem konstans polinomnak van gyöke, így a gyöktényező leválasztására vonatkozó állítás szerint pontosan az elsőfokú polinomok az irreducibilisek.

210. Írja le az irreducibilis polinomokat a $\mathbb{R}$ feletti polinomok körében!

A valós számtest felett irreducibilisek az elsőfokú polinomok és azok a másodfokú polinomok, amelyeknek nincs valós gyöke.

211. Mit tud a $\mathbb{Q}$ feletti irreducibilis polinomokról?

A racionális számtest felett bonyolultabb a helyzet. Vannak polinomok, például $x^2 - 2$, amelyek $\mathbb{Q}$ felett irreducibilisek, bár $\mathbb{R}$ felett nem. $\mathbb{Q}[x]$-ben minden $n \in \mathbb{N}^+$-ra van olyan n-ed fokú polinom, amely irreducibilis.

212. Igaz-e, hogy $\mathbb{Z}[x]$ euklideszi gyűrű?

A $\mathbb{Z}[x]$ gyűrű nem tehető euklideszi gyűrűvé. Ha ugyanis euklideszi gyűrűvé tudnánk tenni, akkor a 2 és x polinomok legnagyobb közös osztója, amely létezik és 1, előállítható lenne $1 = 2u + xv$ alakban valamely $u, v \in \mathbb{Z}[x]$ polinomokkal, ami nem lehetséges, mert a jobb oldal konstans tagja páros.

213. Igaz-e, hogy $\mathbb{Z}[x]$ Gauss-gyűrű?

Igen, mivel $\mathbb{Z}$ Gauss-gyűrű, ezért $\mathbb{Z}[x]$ is az.

214. Fogalmazza meg Gauss tételét egyértelmű faktorizációs tartományokról!

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

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

215. Ismertesse a Lagrange-interpolációt!

Az R egységelemes integritási tartománynak $c_0, c_1, \dots, c_n$ különböző elemei, $d_0, d_1, \dots, d_n$ pedig tetszőleges elemei R-nek, akkor legfeljebb egy olyan legfejlebb n-ed fokú f polinom létezik, amelyre $f(c_j) = d_j$, $j = 0,1, \dots, n$. Ha R test, akkor mindig létezik is ilyen polinom, és az alábbi *Lagrange-iterpolációs 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 $f(x) = \sum_{j=0}^{n} d_j l_j(x)$.

216. Ismertesse a Lagrange-interpoláció felhasználását titokmegosztásra!

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 (és 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 $t + a_1 x^1 + a_2 x^2 + \cdots + a_{m-1} x^{m-1}$ polinom $y_1, y_2, \dots, y_n$ értékeit az $1,2, \dots, n$ helyeken. Ezen y_j-k a titokrészek: bármelyik m titokrészből a polinom megkapható Lagrange-interpolációval, így adódik a konstans tag, azaz titok, de kevesebb részből könnyen láthatóan nem.

217. Ismertesse a Kronecker-eljárást!

Ha R egy (végtelen) Gauss-gyűrű, amelyben rendelkezésünkre áll egy eljárás, amellyel akármelyik elem osztóit meg tudjuk határozni, valamint vannak eljárások a műveletek elvégzésére (például, ha

$R = \mathbb{Z}$), akkor egy $f \in R[x]$ polinomnak meghatározhatjuk az irreducibilis faktorait. Ha $f = gh$, akkor bármely $c \in R$-re $f(c) = g(c)h(c)$, így $g(c)|f(c)$. Legyen K az R hányadosteste. Választva különböző $c_0, c_1, \dots, c_n$ elemet R-ben, bármely R-beli $d_j|f(c_j)$, $j = 0,1, \dots, n$ értékekhez Lagrange-interpolációval meghatározhatjuk azt az egyetlen $g \in K[x]$ polinomot, amelyre $\deg(g) \leq n$ és $g(c_j) = d_j$, azaz $g(c_j)|f(c_j)$, $j = 0,1, \dots, n$. Ha $g \in R[x]$ és osztja f-et, akkor megtaláltuk f egy osztóját, és f helyett a hányadossal folytatjuk. Ha $n = 0$-va indulunk, és egyesével növeljük n-et, akkor csak irreducibilis polinomosztókat fogunk találni. Ha $n \leq \lfloor \deg(f)/2 \rfloor$-ig nem találtunk osztót, akkor f irreducibilis.

218. Definiálja a racionális függvényeket!

Ha R integritási tartomány, akkor $R[x]$ is, így képezhetjük a hányadostestét; ezt $R(x)$-el jelöljük, és az elemeit R feletti *racionális függvényeknek* nevezzük.

219. Fogalmazza meg a parciális törtekre bontás tételét $1/g$ alakú racionális függvényekre!

Legyen K test, $g_1, g_2, \dots, g_n \in K[x]$ legalább elsőfokú páronként relatív prím polinomok, $g = g_1 g_2 \cdot \dots \cdot g_n$. Ekkor léteznek olyan

$$f_1, f_2, \dots, f_n \in K[x]$$

polinomok, amelyekkel (a hányadostestben)

$$\frac{1}{g} = \frac{f_1}{g_1} + \frac{f_2}{g_2} + \dots + \frac{f_n}{g_n}.$$

220. Fogalmazza meg a parciális törtekre bontás tételét f/g alakú racionális függvényre két alakban!

Ha $h \in K[x]$, akkor léteznek olyan $h_j \in K[x]$ polinomok, amelyekkel

$$\frac{h}{g} = \frac{h_1}{g_1} + \frac{h_2}{g_2} + \dots + \frac{h_n}{g_n}.$$

Ez felírható

$$\frac{h}{g} = p + \frac{h_1}{g_1} + \frac{h_2}{g_2} + \dots + \frac{h_n}{g_n}$$

alakban is, ahol $p \in K[x]$, és $\deg(h_j) < \deg(g_j)$, ha $j = 1, \dots, n$.

221. Fogalmazza meg a parciális törtekre bontás tételét u/v^k alakú racionális függvényekre!

Ha a $g_1, g_2, \dots, g_n$ polinomokat a g-nek irreducibilis polinomok szorzataként történő előállításából kaptuk, akkor az előző kérdésben szereplő törtek u/v^k alakúak, ahol $\deg(u) < \deg(v^k)$. Ezek a törtek felírhatók

$$\frac{u}{v^k} = \frac{u_k}{v^k} + \frac{u_{k-1}}{v^{k-1}} + \dots + \frac{u_1}{v}$$

alakban, ahol $\deg(u_j) < \deg(v)$, ha $j = 1, \dots, k$.

222. Definiálja a többhatározatlanú polinom fogalmát!

Legyen R gyűrű, $n \in \mathbb{N}$. Az R feletti *n-határozatlanú polinom* gyűrűjét n szerinti rekurzióval definiáljuk: ha $n = 0$, legyen $R[x_1, x_2, \dots, x_n] = R$, az egyhatározatlanú polinomok gyűrűjét már definiáltuk, ha pedig $n > 1$, akkor legyen $R[x_1, x_2, \dots, x_n] \coloneqq R[x_1, x_2, \dots, x_{n-1}][x_n]$, azaz az n határozatlanú polinomok olyan polinomjai x_n-nek, amelynek együtthatói az $x_1, x_2, \dots, x_{n-1}$ határozatlanok polinomjai.

223. Hogyan azonosíthatjuk a gyűrű elemeit bizonyos többhatározatlanú polinomokkal?

Könnyen látható, hogy az n-határozatlanú polinomok

$$\sum_{i_1, i_2, \dots, i_n} f_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

alakú összegek, ahol $x_1, x_2, \dots, x_n$ a "határozatlanok" és $f_{i_1, i_2, \dots, i_n} \in R$. Az $a \in R$ elemhez hozzárendelve azt az f polinomot, amelyre $f_{0,0,\dots,0} = a$ és $f_{i_1, i_2, \dots, i_n} = 0$ egyébként, az R egy olyan leképezését kapjuk a polinomok gyűrűjébe, amely nyilván monomorfizmus, értékkészletének elemei a konstans polinomok, ezeket R elemeivel azonosíthatjuk.

224. Definiálja a többhatározatlanú polinom együtthatóit, tagjainak multifokát és fokát!

Az

$$f_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

tagot *monomnak* nevezzük, $f_{i_1, i_2, \dots, i_n}$ az *együtthatója*, $(i_1, i_2, \dots, i_n)$ a *multifoka,* $i_1 + \cdots + i_n$ pedig a *foka*.

225. Definiálja a többhatározatlanú monom fogalmát!

Ld.: előző kérdés.

226. Definiálja a többhatározatlanú polinom fokát! Milyen megállapodások mellett egyértelmű egy többhatározatlanú polinom felírása?

Az n-határozatlanú polinomok jelölésére a hagyományos

$$\sum_{i_1 + i_2 + \cdots + i_n \leq m} f_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

felírást fogjuk használni. Mivel a felírásból a nulla együtthatójú tagokat szokás elhagyni, illetve a felíráshoz további nulla együtthatójú tagok adhatók hozzá, a felírás nem egyértelmű. Egyértelművé válik azonban, ha kikötjük, hogy m minimális legyen, és minden m-nél nem magasabb fokú tag – egyszer – szerepeljen. Ez a minimális m a polinom *foka*, jelölése $\deg(f)$.

227. Definiálja a többhatározatlanú lineáris polinomokat!

A legfeljebb elsőfokú polinomok a *lineáris polinomok*.

228. Definiálja a többhatározatlanú homogén polinomokat!

Ha egy polinom minden (nem nulla) tagjának ugyanaz a k a foka, akkor k-adfokú *homogén polinomnak* nevezzük.

229. Hogyan írhatjuk fel két többhatározatlanú polinom összegének, illetve szorzatának az együtthatóit?

A definícióból adódik, hogy az összeadás és szorzás tagonként történik: ha

$$g = \sum_{i_1+i_2+\cdots+i_n \le m} g_{i_1,i_2,\ldots,i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

egy másik polinom, akkor az összegük az

$$f + g = \sum_{i_1+i_2+\cdots+i_n \le m} (f_{i_1,i_2,\ldots,i_n} + g_{i_1,i_2,\ldots,i_n}) x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

polinom, szorzatuk pedig az a $h = fg$ polinom, amelyre

$$h_{k_1,k_2,\ldots,k_n} = \sum_{i_1+j_1=k_1,\ldots,i_n+j_n=k_n} f_{i_1,i_2,\ldots,i_n} g_{j_1,j_2,\ldots,j_n}.$$

230. Milyen esetben lesz a többhatározatlanú polinomok gyűrűje nullosztómentes?

Ha az R gyűrű nullosztómentes, akkor az $R[x_1, x_2, \ldots, x_n]$ gyűrű is nullosztómentes.

231. Mit mondhatunk két többhatározatlanú polinom szorzatának fokáról?

Két polinom szorzatának a foka a fokok összege.

232. Milyen esetben lesz a többhatározatlanú polinomok gyűrűje Gauss-gyűrű? Fogalmazza meg az állítást!

Ha R egy Gauss-gyűrű, $n \in \mathbb{N}$, akkor $R[x_1, x_2, \ldots, x_n]$ is Gauss-gyűrű.

233. Definiálja a gyakoriság és a relatív gyakoriság fogalmát!

Tegyük fel, hogy egy információforrás nagy számú, összesen n üzenetet bocsát ki. 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 azt mondjuk, hogy *gyakorisága* k_i, *relatív gyakorisága* pedig $p_i = k_i/n > 0$.

234. Definiálja az egyedi üzenet információtartalmát! Mi a bit?

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 egységét határozza meg. Amennyiben az alap 2, akkor az információ egysége a *bit*.

235. 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 *entrópiáját* a

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

összefüggéssel értelmezzük.

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

Bármilyen eloszláshoz tartozó entrópiára

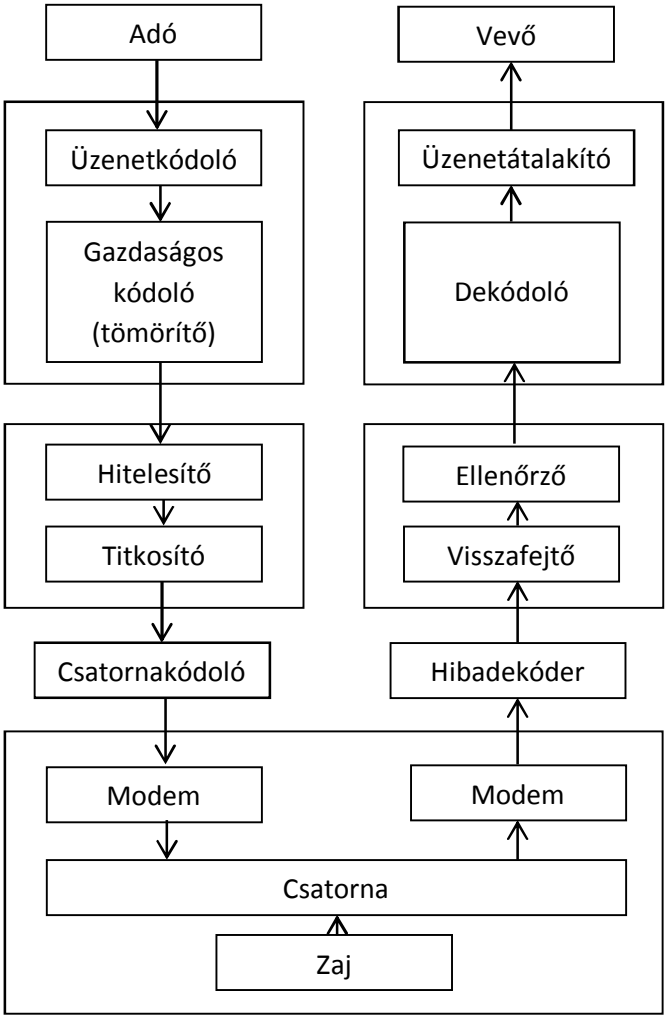
$$H_r(p_1, p_2, \dots, p_m) \leq \log_r m,$$

és egyenlőség pontosan akkor teljesül, ha $p_1 = p_2 = \cdots = p_m = 1/m$.

237. Mi a forráskódolás? Mik a részei?

Az üzenetkódolást és a gazdaságos kódolást együttesen nevezik *forráskódolásnak*.

238. Rajzolja fel az üzenetátvitel részletes sémáját!



239. Ismertesse a betűnkénti kódolást!

A betűnkénti kódolás során az eredeti üzenetet meghatározott módon egymáshoz átfedés nélkül csatlakozó részekre bontjuk, egy-egy ilyen részt egy szótár alapján kódolunk, és az így kapott kódokat az eredeti sorrendnek megfelelően egymáshoz láncoljuk. Az általánosság csorbítása nélkül feltehetjük, hogy a szótár alapján kódolandó elemi üzenetek egy A ábécé (a kódolandó ábécé) betűi, és egy-egy ilyen betű kódja egy másik (az előbbitől nem feltétlenül különböző) B ábécé, a kódoló ábácé, vagy kódábécé betűivel felírt szó, vagyis ezen ábécéből vett betűk véges hosszúságú sorozata, a sorozat elemeit egyszerűen egymás mellé írva. A továbbiakban mindkét ábécéről feltesszük, hogy nem üres és véges. Ha a B ábécé egyelemű, kételemű, háromelemű stb., akkor rendre unáris, bináris, ternáris, stb., kódról beszélünk. Az A ábécé betűivel felírható összes (legalább egy betűt tartalmazó) szó halmazát A^+, míg az egyetlen betűt sem tartalmazó üres szóval (jele: $\emptyset$ vagy λ) kibővített halmazt A^* jelöli. Az előbbiek alapján a betűnkénti kódolást egy $\varphi: A \to B^*$ leképezés határozza meg, amelyet természetes módon terjesztünk ki egy $\psi: A^* \to B^*$ leképezéssé: ha $a_1 a_2 \dots a_n = \alpha \in A^*$ (tehát $n \in \mathbb{N}$, és $a_i \in A$, ha $1 \leq i \leq n$), akkor α kódja $\psi(\alpha) = \varphi(a_1)\varphi(a_2) \dots \varphi(a_n)$; $rng(\psi)$ elemei a kódszavak.

240. Definiálja a prefix, infix és szuffix fogalmát!

Legyen α, β és γ az A ábécével felírt három szó. Ekkor α *prefixe* (vagy előtagja) és γ *szuffixe* (vagy utótagja) az $\alpha\gamma$ szónak, β pedig *infixe* (vagy belső tagja) $\alpha\beta\gamma$-nak.

241. Ismertesse a kód és kódfa kapcsolatát!

A betűnkénti kódolás szemléletesen és egyértelműen adható meg egy irányított fa segítségével. Legyen $\varphi: A \to B^*$ egy betűnkénti kódolás. Tetszőleges szóhalmaz, így a φ értékkészletében lévő kódszavak összes prefixeinek halmaza is részbenrendszett a „prefixe” relációra. Készítsük el ennek a relációnak a Hasse-diagramját. Nyilván egy irányított fát kapunk, amelynek gyökere az üres szó, és 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 vezető él színe legyen b. Nyilván bármely csúcs esetén a csúcsból kivezető élek mind különböző színűek.

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

Tegyük fel, hogy az infektív $\varphi: A \to B^+$ leképezés $rng(\varphi)$ értékkészlete B^+ prefixmentes részhalmaza. Ekkor a φ által meghatározott $\psi: A^* \to B^*$ betűnkénti kódolás nyilván könnyen dekódolható, mert ha egymás után érkeznek a kódábécé betűi, és nézzük az addig beérkezett szimbólumokból összeálló szót, akkor amint ez kiadja a kódolandó ábécé valamey betűjének kódját, azonnal dekódolható is, hiszen a folytatásával kapott jelsorozat már egyetlen betűnek sem lehet a kódja. Ezen dekódolási módszer miatt szokás az ilyen kódot *prefix kódnak* nevezni.
Egy betűnkénti kód *egyenletes kód*, ha a betűk kódjainak hossza azonos. Mivel ilyen kód nyilván prefix, ezért felbontható, így mindig van felbontható kód.
Egy betűnkénti kód *vesszős kód*, ha van olyan ϑ szó, a vessző, hogy ϑ minden kódszónak szuffixe, de egyetlen kódszó sem áll elő $\alpha\vartheta\beta$ alakban nem üres β szóval. Egy vesszős kód prefix kód, mert a vessző egyértelműen jelzi a beérkezett jelsorozatban egy-egy kódszó végét, és ha ezt folytatjuk, aakkor már biztosan nem kapunk kódszót, hiszen ebben a meghosszabbított sorozatban a vesszú valódi infix lenne.

243. 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: bár φ injektív, ψ nem.

244. Adjon példát fejthető, de nem prefix kódra!

Legyen $\varphi(a) = 10$, $\varphi(b) = 1$ és $\varphi(c) = 00$.

245. Fogalmazza meg a McMillan-egyenlőtlenséget tartalmazó tételt!

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

$$\sum_{j=1}^{n} r^{-l_j} \leq 1.$$

246. Definiálja az átlagos szóhosszúság és az optimális kód fogalmát!

Legyen $A = \{a_1, \dots, a_n\}$ a kódolandó ábécé, $p_1, \dots, p_n$ a betűk eloszlása, $\varphi: A \to B^+$ 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*. Ha adott elemszámú ábécével és eloszlással egy felbontható kód átlagos szóhosszúsága minimális, akkor *optimális kódnak* nevezzük.

247. Van-e mindig optimális kód betűnkénti kódolsánál?

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 szóhosszúságú.

248. Fogalmazza meg Shannon tételét zajmentes csatornára!

Az előző definíció jelöléseivel legyen B elemeinek száma r. ha a betűnkénti kódolás felbontható, akkor $H_r(p_1, \dots, p_n) \leq \bar{l}$, ahol H_r az eloszlás entrópiája.

249. Ismertesse egy optimális kód kódfájának tulajdonságait!

(1) A kódfában csak az $L - 1$-edik (L: a kódszavak hosszának maximuma) szinten lehet csonka csúcs, és még a csonka csúcsokból is legalább két él indul ki.
(2) van olyan optimális prefix kód, amelynek kódfájában lefeljebb egy csonka csúcs van.

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

(1) egy optimális prefix kód, amelynek kódfájában akkor nincs csonka csúcs, ha $r \equiv n \pmod{r-1}$, azaz
$$r = 2 + ((n-2) \bmod (r-1)),$$
ha pedig egy csonka csúcs van, akkor annak m kifokára $m \equiv n \pmod{r-1}$, azaz
$$m = 2 + ((n-2) \bmod (r-1));$$
(2) ha $n \leq r$, akkor egybetűs kódszavakat választva optimális prefix kódot kapunk;
(3) legyen $\beta_1, \dots, \beta_n$ az r-elemű kódábécével megadott, a $p_1, \dots, p_n$ eloszláshoz tartozó optimális prefix kód, amelynek a kódfájában nincs csonka csűcs. Ha $2 \leq m \leq r$, és valamely $1 \leq k \leq n$-re a $p_{n+1}, \dots, p_{n+m}$ pozitív valós számokra $\sum_{i=1}^{m} p_{n+i} = p_k$, továbbá

$$\max\{p_{n+1}, \dots, p_{n+m}\} \leq \min\{p_1, \dots, p_n\},$$

akkor

$$\beta_1, \dots, \beta_{k-1}, \beta_{k+1}, \dots, \beta_n, \beta_k b_1, \dots, \beta_k b_m,$$

ahol $b_1, \dots, b_m$ a B különböző elemei, a

$$p_1, \dots, p_{k-1}, p_{k+1}, \dots, p_n, p_{n+1}, \dots, p_{n+m}$$

"finomított" eloszláshoz tartozó optimális prefix kód.

251. Írja le, hogyan konstruálhatunk Huffman-kódot!

Optimláis kódot ad az úgynevezett *Huffman-kód*, amelyet az előző tétel pontjai alapján tudunk megszerkeszteni. Rendezzük a relatív gyakoriságok csökkenő sorrendjében a betűket, majd osszuk el $n-2$-t $r-1$-gyel, és legyen m a maradék plusz 2. Első lépésben 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 a sorozatban. Ezek után ismételjük meg az előző redukciót, de most már minden lépésben r betűvel csökkentve 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 kiegészítésével kapjuk.

252. Írja le, mit érhetünk el a kódolandó ábécé kiterjesztésével!

Azt, hogy egy felbontható kódban az egy betűre jutó átlagos szóhosszúság tetszőleges mértékben megközelítse az entrópia értékét, azaz az elméleti alsó határt.

253. 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. A szótár állandó (statikus) vagy változó (dinamikus).

254. Ismertesse a paritásbites kódot!

A legegyszerűbb hibajelző kód a *paritásbites kód*. Legyen például az üzetenhalmaz n-bites bináris jelsorozatok halmaza, és egészítsük ki ezeket a jelsorozatok egy $n+1$-edik bittel, az úgynevezett paritásbittel: amennyiben egy üzenetben az 1-esek száma páratlan, akkor írjunk a bitsorozat végére egy 0-t, míg az ellenkező esetben egy 1-et (vagy fordítva, de egy adott kódban mindig úgyanazon szabály szerint). Az így kiegészített, $n+1$-bites szavak mindegyikében páratlan sok 1-es van. Ha most egy ilyen kódszót elküldünk, és a vevőhöz olyan szó érkezik, amelyben az egyesek száma páros, akkor biztos, hogy nála hiba történt az átvitel során. Ha viszont az egyetek száma páratlan, akkor úgy kell tekintenünk (de nem állíthatjuk), hogy nem történt hiba.

255. Definiálja a t-hibajelző és pontosan t-hibajelző 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.

256. Definiálja kód távolságát és súlyát!

A kódábécé két egyforma hosszú szavának *kód távolsága* $d(C)$, a különböző kódszópárok távolságainak minimuma, ahol C a kódszavak halmaza, röviden a kód.
Ha a kódábécé egy A additív Abel-csoport, akkor a *kód* $w(C)$ *súlya* a nem nulla kódszavak súlyainak minimuma (ha van nem nulla kódszó, azaz a csoport nem egyelemű).

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

A továbbiakban egy kód távolságát d és a súlyát w jelöli. A bevezetett távolságfogalommal egy kód akkor és csak akkor t-hibajelző, ha $t < d$, és akkor és csak akkor pontosan t-hibajelző, ha $t = d - 1$, tehát nagyobb távolság nagyobb hibajelző képességet jelent.

258. Ismertesse a minimális távolságú dekódolást!

A hibajavításhoz meg kell adni egy úgynevezett döntési függvényt, amely bármely lehetséges jelsorozathoz hozzárendel egy és csak egy kódszót. (Az is lehetséges, hogy nem minden szó esetén akarunk dönteni.) Ezt a döntési függvényt kell úgy meghatároznunk, hogy a döntési hiba, tehát az a hiba, hogy egy beérkezett jelsorozathoz nem a ténylegesen elküldött kódot rendeljük, a lehető legkisebb legyen. Az ilyen döntési függvény által meghatározott dekódolást *minimális távolságú dekódolásnak* mondjuk.

259. Definiálja a t-hibajavító és pontosan 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.

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

Egy d távolságú kód esetén minimális távolságú dekódolással $t < d/2$ hiba esetén biztosan jól döntünk, hiszen a háromszög-egyenlőtlenség következtében az eredetileg elküldött kódszótól különböző bármely más kódszó biztosan $d/2$-nél több helyen tér el a vett szótól. Viszont $t \geq d/2$ esetén nincs olyan döntési függvény, amely t-hibajavító.

261. Ha legfeljebb t hibát javítani, legfeljebb s hibát pedig jelezni akarunk, mekkora kódtávolság szükséges?

Ha $t + s < d$, akkor minimális távolságú dekódolással minden t-hiba kijavítható és minden s-hiba jelezhető.

262. Mi az ismétléses kód? Mi a hátránya?

Legyen egy binárisan kódolt üzenethalmazunk, és küldjük el az üzenetet úgy, hogy minden egyes bitet megháromszorozunk, azaz ugyanazt a bitet háromszor egymás után küldjük. Ilyen kódot nem sikerült még konstruálni, és még ha sikerülne is, akkor is használhatatlan lenne a gyakorlatban, olyan nagy lenne a kódszava hossza, és olyan nagy lenne a kódszavak száma.

263. Ismertesse a kétdimenziós paritásellenőrzést!

A korábban tárgyalt paritáselemes kód segítségével könnyen tudunk egy minimális távolságú dekódolással 1-hibajavító kódot konstruálni. Legyenek az üzenetek n-bites szavak, és tegyük fel, hogy

m üzenetünk van. Egészítsünk ki minden kódszót egy paritásbittel például páratlan paritásúvá, majd m ilyen kódszóból alkossunk blokkot. Írjuk egymás alá a blokk $n+1$-bites kódszavait, és most az egy-egy oszlopban álló m-bites sorozatokat egészítsük ki egy-egy paritásbittel, például páros paritásúvá. Az így kapott $n+1$-bites szóval kiegészítve a blokkot kapjuk az eredeti m üzenet kódját.

264. Mi az a Hamming-korlát?

Ha egy q elemű ábécé bizonyos n hosszú szavaiból álló C kód t-hibajavító, akkor bármely két kódszóra a tőlük legfeljebb t távolságra lévő szavak halmazai diszjunktak. Mivel egy kodszótól j távolsgára pontosan $\binom{n}{j}(q-1)^j$ szó van, azt kapjuk, hogy

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

Ez a *Hamming-korlát* a kódszavak számára adott t-nél.

265. Mikor nevezünk egy kódot tökéletesnek?

Ha a Hamming-korlátnál egyenlőség teljesül, akkor a kódot *tökéletesnek* nevezzük.

266. Mi a Singleton-korlát?

Ha egy q elemű ábécé bizonyos n hosszú szavaiból álló C kód távolsága d, akkor minden kódszóból elhagyva $d-1$ betűt (ugyanarról a $d-1$ helyről), még mindig különböznek a kódszavak, de csak $n-d+1$ hosszúak. Innen a kódszavak számára azt kapjuk, hogy $|C| \leq q^{n-d+1}$, másként $d \leq (n+1)/\log_q(|C|)$; ez a *Singleton-korlát*.

267. Mi az MDS-kód? Mi indokolja az elnevezést?

Ha a Singleton-korlátnál egyenlőség áll fent, a kódot maximális távolságú szeparábilis kódnak, *MDS-kódnak* nevezzük. Az elnevezést az indokolja, hogy (bármely) rögzített $d-1=n-k$ helyen álló betűket elhagyva a kódszavakból, q^k különböző szó marad, ezért a kódolást végezhetjük úgy, hogy az üzeneteket leképezzük ezekre a szavakra, majd az adott $d-1=n-k$ helyen kiegészítjük ellenőrző betűkkel, így az ellenerző betűk elválaszthatók a kódoló betűktől.

268. 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 bármly 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. Ha nem lényeges d, illetve q megadása, akkor elhagyható a jelölésből.

269. Definiálja a generátormátrix, ellenőrző mátrix és a szindróma fogalmát!

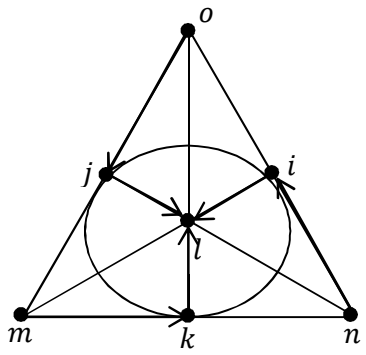
A K véges test feletti $[n,k]$ lineáris kódnál célszerű a kódolást egy K^K-t $C \subset K^n$-re képező G (kölcsönösen egyértelmű) lineáris leképezésnek választani, ahol C a kódszavak k-dimenziós altere. Ezt a leképezést mátrixával jellemezhetjük, ez a kódolás *generátormátrixa*.

A hibajavításra használható egy (tetszőleges) $H: K^n \to K^{n-k}$ szürjektí lineáris leképezés, amelynek a magja C; egy ilyen leképezést ellenőrző leképezésnek, mátrixát a kód egy *ellenőrző mátrixának* nevezzük. Ha $v \in K^n$, akkor a v-hez tartozó $s = Hv$ vektor, *szindróma* pontosan akkor nulla, ha v kódszó, azaz $v \in C$.

270. Ismertesse a szindróma-dekódolást!

Egy lineáris kód esetén a minimális távolságú dekódolás egy megvalósítása. Az előző pont jelöléseivel, ha $s \in K^{n-k}$, tekintsük a $H^{-1}(s)$ halmaz egy olyan $e(s)$ rögzített vektorát, amelynek súlya az adott mellékosztályban minimális. Ezeket az $e(s)$ vektorokat mellékosztály-vezetőnek fogjuk nevezni. Ha $c \in K^n$ egy kódszó, $v \in K^n$ a vett szó, $e = v - c$ a hiba, és ha $w(e) < d/2$, tehát ha a hiba minimális távolságú dekódolással javítható, akkor $He(s) = s = Hv - Hc = He - 0 = He$, így e és $e(s)$ ugyanabban a mellékosztályban vannak. A mellékoszály-vezető választása miatt $w\big(e(s)\big) \leq w(e)$, ahonnan $w\big(e - e(s)\big) \leq w(e) + w\big(-e(s)\big) = w(e) + w\big(e(s)\big) < d$. De $H\big(e - e(s)\big) = 0$, így a különbség kódszó, tehát $e = e(s)$, így $c = v - e(s)$, a hibát kijavítottuk.

271. Ismertesse a Fano-kódot!



Az ábrán látható Fano-sík felhasználható hibajavító kód megkonstruálására. Megszámozva a pontokat 1-től 7-ig, a kódszavak az egyenesekhez tartoznak: olyan bitsorozatok, amelyekben az adott egyenesre illeszkedő pontoknak megfelelő bitek egyesek, a többi nulla, illetve ezek egyekre komplemensei. Kódszó még a csupa nulla illetve csupa egy bitsorozat. Mint könnyen ellenőrizhető, hogy így egy $[7,4,3]_2$ lineáris kódot kapunk, melynek kódszavai: 1110000, 1001100, 0101010, 0011001, 1000011, 0100101, 0100110, 0000000, 0001111, 0110011, 1010101, 1100110, 0111100, 1011010, 1011001, 1111111. A Fano-kód súlya, tehát távolsága is 3. Könnyen ellenőrizhető, hogy 1-hibajavító tökéletes kód (és 1-hibajelző), de nem MDS-kód.

272. Ismertesse a polinomkódokat!

Lineáris kódnál a k hosszú kódolandó szavak tekinthetők $\mathbb{F}_q$ 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 $p \mapsto pg$ leképezés kölcsönösen egyértelmű. Az ilyen típusú lineáris kódolást *polinomkódolásnak* nevezzük.

273. Ismertesse a CRC-t!

Egyszerű, csak hibajelzésre használatos, $\mathbb{F}_2$ feletti polinomkódok az úgynevezett *CRC,* vagyis "ciklikus ellenőrzés" kódok.

274. Adja meg Reed-Solomon-kód esetén a kódolást!

Legyen most K egy tetszőleges véges test, alkossák az ábécét ennek elemei, a K elemszámát jelölje q. Legyen a K^* egy α elemének multiplikatív rendje n. Ekkor az α^i, $0 \leq i < n$ elemek páronként különböznek, és mindegyik gyöke a $z^n - 1 \in K[z]$ polinomnak, ezért megadják ezen polinom összes gyökét. Így $z^n - 1 = \prod_{i=0}^{n-1}(z - \alpha^i)$. Legyen $0 < k < n, m = n - k$ és $g = \prod_{i=1}^{m}(z - \alpha^i)$. Ez a polinom egy K fölötti m-edfokú főpolinom, és nyilván osztója $z^n - 1$ polinomnak. A g mint generátorpolinom által megadott $[n, k]_q$ polinomód a g (vagy az α) által generált *Reed-Solomon-kód*.

275. Adjon meg Reed-Solomon-kód esetén egy ellenőrző mátrixot!

Reed-Solomon-kód esetén az ellenőrző mátrix egy Vandermonde-determinánsú mátrix lesz.

276. Definiálja a hibahelypolinomot és a hibaértékpolinomot!

Legyen adott egy $[n, k, d]_q$ Reed-Solomon-kód, $m = n - k$, $d = n - k + 1 = m + 1$, $g = \prod_{i=1}^{m}(z - \alpha^i)$ a kód generátorpolinomja, e a hibavektor, és $L(z) = \prod_{\{j:e_j \neq 0\}}(1 - \alpha^j z)$ az úgynevezett *hibahelypolinom.* Legyen $E(z) = \sum_{\{j:e_j \neq 0\}} \alpha^j e_j L_j(z)$ az úgynevezett *hibaérték-polinom*, ahol $L_j(z) = L(z)/(1 - \alpha^j z)$, ha $e_j \neq 0$.

277. Hogyan történik a hibahelypolinom és a hibaértékpolinom ismeretében a Reed-Solomon-kód dekódolása?

Ha még $E(z)$-t is ismerjük, akkor a hiba javítható is, mert rögzített j esetén $L_i(\alpha^{-j})$ akkor és csak akkor nem nulla, ha $i = j$, ezért $E(\alpha^{-j}) = \alpha^j e_j L_j(\alpha^{-j})$, így

$$e_j = \frac{E(\alpha^{-j})}{\alpha^j L_j(\alpha^{-j})}.$$

278. Fogalmazza meg a tételt, amely lehetővé teszi a hibahelypolinom és a hibaértékpolinom meghatározását!

Legyen $s(z)$ a szindrómához tartozó polinom. Az előző pont jelöléseivel tegyük fel, hogy a hibahelyek száma, azaz $L(z)$ fokszáma legfeljebb $m/2$ (ami azzal ekvivalens, hogy kisebb, mint $d/2$, azaz hibajavítás egyáltalán végezhető). Alkalmazzuk a bővített euklideszi algoritmust az $a(z) = z^m$ és $b(z) = s(z)$ polinomokra. Az ottani jelölésekkel legyen ℓ a legkisebb index, amelyre $\deg(r_\ell) < m/2$, és legyen $r_\ell = ax_\ell + by_\ell$. Ekkor $y_\ell(0) \neq 0$, és $L(z) = y_\ell(z)/y_\ell(0)$, $E(z) = r_\ell(z)/y_\ell(0)$.

279. Definiálja a számítási eljárás fogalmát!

Egy *számítási eljárás* alatt egy $C = (Q, Q_b, Q_k, f)$ négyest értünk, ahol Q az állapotok (tetszőleges) halmaza, a $Q_b \subset Q$ és $Q_k \subset Q$ részhalmazai a bemeneti állapotok, illetve kimeneti állapotok halmazai, az $f: Q \to Q$ átmeneti függvény pedig Q_k elemeit pontonként fixen hagyja, azaz $f(q) = q$, ha $q \in Q_k$.

280. Definiálja a szimulálást!

Azt mondjuk, hogy a $C' = (Q', {Q'}_b, {Q'}_k, f')$ számítási eljárás a $C = (Q, Q_b, Q_k, f)$ számítási eljárást szimulálja, ha van olyan $g: Q_b \to {Q'}_b$ függvény, a bemeneti kódolás, olyan $h: Q' \to Q$ függvény, az állapotdekódolás és olyan $k: Q' \to \mathbb{N}^+$ függvény, hogy

(1) ha $x \in Q_b$, akkor a C számítási eljárás pontosan akkor adja az y eredményt, ha van olyan $y' \in {Q'}_k$, hogy $g(x)$ bemenettel a C' számítási eljárás az y' eredményt adja, és $h(y') = y$;
(2) ha $q' \in Q'$, akkor $f\big(h(q')\big) = h({f'}^{k(q')}(q'))$, ahol ${f'}^{k(q')}$ azt jelenti, hogy az f' leképezést $k(q')$-ször ismételjük, azaz a $q' \in Q'$-nek megfelelő $h(q') \in Q$ állapotból ha egy lépést teszünk C-ben, az megfelel, annak, hogy q'-ből $k(q')$ lépést teszünk C'-ben.

281. Definiálja a nagy ordót!

Legyen $f: \mathbb{N} \to \mathbb{R}$ egy számsorozat. Jelölje $O(f)$ mindazon $g: \mathbb{N} \to \mathbb{R}$ számsorozatok halmazát, amelyekre van olyan (g-től függő) $C \in \mathbb{R}^+$ konstans és $N \in \mathbb{N}$ index, hogy $|g(n)| \leq C|f(n)|$, ha $n \geq N$.

282. Definiálja a Turing-gépet!

Egy Turing-gép $k \geq 1$ számú szalagból és egy vezérlőegységből áll. A szalagok mindkét irányban végtelen sok mezőre vannak osztva. Minden mezőn egy-egy betű van egy véges ábécéből, úgy, hogy véges sok mező kivételével minden mezőn a _ szóköz (vagy üres) jel áll.
A vezérlőegység véges sok, úgynevezett "belső állapot" egyikében lehet. A belső állapotok között van egy s kezdő állapot és egy h befejező állapot. Minden szalaghoz tartozik egy író-olvasó fej. Kezdetben a vezérlőegység az s kezdőállapotban van. Minden lépésben minden fej elolvassa azt a jelet, amely éppen a fej alatt van, majd három dolog történik az éppen leolvasott jelektől és a vezérlőegység belső állapotától függően: minden fej felülírja az olvasott jelet (lehet, hogy ugyanarra, ami volt), minden fej egymástól függetlenül elmozdul egy mezővel jobbra vagy balra, vagy helyben marad, és a vezérlőegység átmegy egy másik belső állapotba (lehet, hogy ugyanabba, amelyben volt). Ha gép a h befejező állapotba jut, a gép megáll (anélkül hogy bármit is tenne a szalagokkal).
Matematikailag egy T Turing-gép egy $T = (B, A, \varphi)$ hármas, ahol az A, B véges halmazok a szalagábécé illetve a belső állapotok halmaza, _ $\in A$, $s, h \in B$ és

$$\varphi: B \times A^k \to B \times A^k \times \{<, =, >\}^k$$

egy tetszőleges leképezés.

283. Definiálja a Turing-gép bemenetét és kimenetét!

Az előző definíció jelöléseivel egy Turing-gép aktuális állapotát egy

$$q = (b, \alpha_1, \beta_1, \alpha_2, \beta_2, \dots, \alpha_k, \beta_k) \in B \times (A^*)^{2k}$$

sorozat írja le, ahol $\alpha_i \in A^*$ szó az i-edik szalagon szereplő betűk balról jobbra felsorolva az első nem üres jellel kezdve és a fej alatti betűvel végezve, a $\beta_i \in A^*$ szó pedig az i-edig szalagon jobbról balra olvasott betűk az első nem üres jellel kezdve és a fejtől jobbra álló betűvel végezve; mindkettő lehet üres. Mindig feltesszük, hogy az induláskor minden β_i az üres szó, tehát az α_i-k a bemeneti szavak, a fejek a bemenet jobb szélén állnak. Megálláskor az α_i szavakat, azaz a fejektől balra lévő rész teikintjük kimenetnek.

284. Fogalmazza meg a Turing-gép csökkentett jelkészlettel történő szimulálására vonatkozó tételt!

Legyen $T = (B, A, \varphi)$ egy Turing-gép, és A' egy tetszőleges véges ábécé, amelynek legalább két eleme van. Ekkor T szimulálható olyan T' Turing-géppel, amelynek ábécéje A'. Ha egy számítás során a T gép t lépést tesz, akkor a T' gép $O(t)$ lépést tesz.

285. Ismertesse szavak kódolását számmá és vissza!

Sokszor szükség van arra, hogy egy Turing-gép bemeneti szavait számnak tekintsük. Ilyenkor mindig feltesszük, hogy a gép A ábécéje a $\{0,1,\dots,r-1\}$ számjegyekből áll, és 0 az üres jel. Egy A^*-beli $\alpha = a_n a_{n-1} \dots a_0$ bemeneti szó vagy az üres szó, vagy nem 0-val kezdődik, és r alapú számrendszerben az $|\alpha|_r = \sum_{i=0}^{n} a_i r^i$ számot reprezentálja. Az $\alpha \mapsto |\alpha|_r$ leképezés kölcsönösen egyértelműen képezi le A^* nem 0-val kezdődő szavait $\mathbb{N}$-re. Ha csak A_0^*-beli szavakat akarunk számmá kódolni, akkor az $\alpha \mapsto |\alpha|_{r-1}$ leképezést használhatjuk, ahol természetesen $\alpha = a_n a_{n-1} \dots a_0$ esetén $|\alpha|_{r-1} = \sum_{i=0}^{n} a_i (r-1)^i$, de itt a jegyek között már $r-1$ is szerepel, annak ellenére, hogy $r-1$ alapú számrendszert használunk. Az $\alpha \mapsto |\alpha|_{r-1}$ leképezés kölcsönösen egyértelműen képezi le A_0^*-ot $\mathbb{N}$-re, ami indukcióval könnyen belátható. Egy unáris kódban felírt n szám Turing-gép általi konvertálása egy $\alpha \in A_0^*$ szóvá, amire $|\alpha|_{r-1} = n$ vagy fordítva, hasonlóan végezhető, mint az unáris-bináris konverzió.

286. Fogalmazza meg a Turing gép egyszalagos géppel történő szimulálására vonatkozó tételt!

Legyen $T = (B, A, \varphi)$ egy Turing-gép k szalaggal. Ekkor T szimulálható olyan egyszalagos S Turing-géppel, amelynek ábécéje szintén A. Ha egy számítás során a T gép t lépést tesz, akkor az S gép $2kt(2t+3) = O(t^2)$ lépést tesz.

287. Fogalmazza meg a szemétgyűjtésre vonatkozó tételt!

Legyen $T = (B, A, \varphi)$ egy Turing-gép. Ekkor T módosítható egy azonos szalagszámú S Turing-géppé, amely szimulálja T működését, és ugyanazokkal az A_0^*-beli bemeneti szavakkal indítva, mint T-t, ugyanazokat az A_0^*-beli kimeneti szavakat produkálja, de nem hagy "szemetet", azaz a kimeneti szavakon kívül a szalagok mezője üres. Ha egy számítás során a T gép t lépést tesz, és elolvassa a bemenetét (azaz a számítás során a bemenet minden mezőjén járt fej), akkor az S gép $O(t^2)$ lépést tesz.

288. Fogalmazza meg az univerzális Turing-gépekkel kapcsolatban tanult tételt!

Legyen A egy (legalább kételemű) ábécé, $k \geq 1$. Van olyan $k+1$ szalagos U Turing-gép A ábécével, hogy bármely k szalagos $T = (B, A, \varphi)$ Turing-gépre a T bemenetét felírva az U első k szalagjára, a $k+1$-edig szalagra pedig egy, csak a φ-től függő $\omega \in A^*$ "programot" írva (amelynek utolsó betűje nem üres jel, és legfeljebb $6k+4$ üres jelet tartalmaz egymás mellett), U szimulálja T működését (az első k szalagján). Ha A-nak legalább három eleme van, akkor U-t úgy is választhatuk, hogy a programok ne tartalmazzanak üres jelet. Ha T egy bemeneten t lépést tesz, akkor U a szimulálást $O(t)$ lépésben végzi.

289. Ismertesse a RAM-gépet!

A *RAM-gép* a valódi számítógépekhez közelebb álló gépmodell. Az M memória minden $M[k]$ ($k \in \mathbb{Z}$) rekesze tetszőleges egész számot tárolhat, de egyszerre mindig csak véges sok nem nulla értéket

tárol. A gépnek három regisztere van: az A akkumulátor, a B regiszter és az I indexregiszter; ezek tartalma is egész szám. Van még egy programmemória, ennek rekeszei természetes számokkal vannak indexelve, és utasításokat tartalmaznak.

290. Mi a logaritmikus költség?

RAM-gépnél egy lépés idejét nem egységnyinek vesszük, hanem annyinak, amennyi az adott lépésben (operandusonként, illetve eredményként) szereplő összes egész szám bitjei számának összege, ahol minden számnál egy bitet számolunk az előjelre. Így a 0 egybites, a $0 \neq n \in \mathbb{Z}$ szám bitjeinek száma pedig $2 + \lfloor \log|n| \rfloor$. Emiatt szokás *logaritmikus költségű* RAM-gépről is beszélni.

291. Fogalmazza meg a Turing-gép RAM-géppel történő szimulálására vonatkozó tételt!

Bármely egyszalagos Turing-gép szimulálható RAM-gépen. Ha a Turing-gép lépésszáma n, akkor a RAM-gép $O(n)$ lépést tesz $O(\log n)$ jegyű számokkal, tehát a RAM-gép végrehajtási ideje $O(n \log n)$.

292. Fogalmazza meg a RAM-gép Turing-géppel történő szimulálására vonatkozó tételt!

Egy RAM-gépen írt programhoz van olyan négyszalagos Turing-gép, amely szimulálja a program működését, és ha a RAM-gép elolvassa a bemenetét és futásideje n, akkor a Turing-gép lépésszáma $O(n^2)$.

293. Ismertesse a tárolt programú gépet!

Egy másik a valódi számítógépekhez közel álló számítógépmodell a *tárol programú gép*. A memória ugyanolyan, mint a RAM-gépnél, de most a program is a memóriában van. A gépnek csak egy regisztere van, az A akkumulátor.

294. Ismertesse a félszalagos Turing-gépet!

Néha a Turing-gépet úgy szokás definiálni, hogy a szalagjai csak az egyik irányban végtelen. Ha a gép balra haladva bármelyik szalagján “lelép” a szalagról. akkor úgy tekintjük, hogy “elszállt”: soha nem jut el a halt állapotba (még akkor sem, ha éppen abba ment volna át).

295. Fogalmazza meg a félszalagos Turing-gép Turing-géppel történő szimulálására vonatkozó tételt!

Bármely félszalagos Turing-géphez létezik Turing-gép ugyanazzal a szalagszámmal és ábécével, amely a félszalagos Turing-gépet szimulálja, és ha az n lépést tett, akkor legfejlebb $O(n)$ lépést tesz.

296. Fogalmazza meg a Turing-gép félszalagos Turing-géppel történő szimulálására vonatkozó tételt!

Bármely Turing-géphez létezik félszalagos Turing-gép gép ugyanazzal a szalagszámmal és ábécével, amely a Turing-gépet szimulálja, és ha az n lépést tett, akkor legfeljebb $O(n)$ lépést tesz.

297. Ismertesse a korlátozott gépmodelleket!

Ha egy Turing-gépre különböző megszorításokat teszünk, *korlátozott gépmodelleket* kapunk. Például feltehetjük, hogy vannak “csak bemenet” szalagok, amelyeken a gép nem írhat, és csak balra léphet, vannak “csak kimenet” szalagok, amelyeket a gép írhat, de csak jobbra léphet rajtuk, és vannak

veremtárak vagy vermek, amelyeken a gép írhat és olvashat, valamint balra is, jobbra is léphet, de ha balra lép, akkor törölnie kell, amit olvasott (azaz üres jelet kell a helyére írni); ezek a szalagok szolgálhatnak bemenetként és kimenetként is.

298. Fogalmazza meg a Turing-gép kétveremtáras géppel történő szimulálására vonatkozó tételt!

Bármely egyetlen félszalaggal rendelkező T Turing-géphez létezik olyan V kétveremtáraas gép, amelynek mindkét veremtára félszalag, a Turing-gépet szimulálja ugyanazzal az ábécével, és ha az n lépést tett, akkor legfeljebb $O(n)$ lépést tesz.